OWASP

Open Web Application Security Project

Application Security Guide For CISOs

Version 1.0 (November 2013)

Project Lead and Main Author

Marco Morana

Co-authors, Contributors and Reviewers

Tobias Gondrom, Eoin Keary, Andy Lewis, Stephanie Tan and Colin Watson

Chief Information Security Officers (CISOs) are responsible for application security from governance, compliance and risk perspectives. The Application Security Guide For CISOs seeks to help CISOs manage application security programs according to their own roles, responsibilities, perspectives and needs. Application security best practices and OWASP resources are referenced throughout the guide.

Foreword

This guide has been supported by the OWASP project reboot program and developed in alignment with OWASP core values reflected in the openness of the content, innovative ideas and concepts, global reach to the application security community and integrity of the contents that are published as strictly vendor neutral and un-biased by specific commercial interests. This guide has also been developed in respect of the OWASP core values such as to "Promote the implementation of and promote compliance with standards, procedures, controls for application security" and the OWASP principles of delivering free and open content, not for profit interests and a risk based approach for improving application security. The leader of the OWASP Application Security Guide for CISOS project is Marco Morana that developed the original contents of this guide with contributions from Colin Watson, Eoin Keary, Tobias Gondrom and Stephanie Tan. This project is being developed by the OWASP in parallel with the CISO Survey project lead by Tobias Gondrom.

The objective is to run these two projects in sync and use the results of the 2013 CISO Survey to tailor the guide to the specific CISOs needs by highlighting which OWASP projects/resources address these needs. The November 2013 version of the OWASP Application Security Guide for CISOs was presented at the 2013 AppSec USA Conference, held in New York City on November 18-23, 2013.

Contents

Preamble to Guide 1
Introduction *3*
Executive Summary *5*
The CISO Guide 11
Part I : Reasons for Investing in Application Security *13*
Part II : Criteria for Managing Application Security Risks *31*
Part III : Application Security Program *57*
Part IV : Metrics For Managing Risks & Application Security Investments *77*
Supporting Information 85
References *87*
About OWASP *91*
CISO Guide Appendixes 93
Appendix A: Value of Data & Cost of an Incident *95*
Appendix B: Quick Reference to OWASP Guides & Projects *99*

List of Figures

Figure 1 Risk Mitigation Strategy Based on Event Likelihood and Impact 22
Figure 2 Analysis Indicating That 1-2 Year Roadmaps Support Obtaining Proper Security Investment; Shorter and Longer Roadmaps Do Not (OWASP CISO Survey 2013) 24
Figure 3 Chart Indicating How the Cost of Investment in Software Security Measures Against Failure Costs Due to Incidents that Exploit Software Vulnerabilities. 29
Figure 4 Diagram Indicating How Attackers Can take Different Pathways Through An Application to do Harm (OWASP Top Ten Web Application Risks 2013) 35
Figure 5 The Calculation of Business Risk 36
Figure 6 Threat Agents 38
Figure 7 Example Security Processes Built Into a Waterfall SDLC 65
Figure 8 Business Functions and Related Security Practices Within Open Software Assurance Maturity Model (OWASP Open SAMM v1.0) 66
Figure 9 Three Key Questions for the Security Strategy 68
Figure 10 Inputs for Developing the Security Strategy 69
Figure 11 Elements of the Security Strategy 71
Figure 12 Analysis of Application Security Roadmap Durations (OWASP CISO Survey 2013) 72
Figure 13 An Illustration of OWASP's Project Categories 73
Figure 14 People, Processes and Technology Controls Support Application Security 74
Figure 15 Example Vulnerability Categorization Trend Chart 82
Figure 16 Chart Illustrating How the Cost Of Testing and Managing Software Bugs Vary with Stage of SDLC 83

List of Tables

Table 1 The OWASP Risk Framework Applied to Web 2.0 Technologies 53
Table 2 CISO Functions Mapped to OWASP Guides and Other Projects 99

Preamble to Guide

Introduction

Among application security stakeholders, Chief Information Security Officers (CISOs) are responsible for application security from governance, compliance and risk perspectives. This guide seeks to help CISOs manage application security programs according to CISO roles, responsibilities, perspectives and needs. Application security best practices and OWASP resources are referenced throughout this guide. OWASP is a non profit organization whose mission is "making application security visible and empowering application security stakeholders with the right information for managing application security risks".

This CISO guide is written to help CISOs that are responsible for managing application security programs from the information security and risk management perspectives. From the information security perspective, there is a need to protect the organization assets such as the citizen, client and customer sensitive data, the databases where this data is stored, the network infrastructure where the database servers reside and last but not least, the applications and software used to access and process this data. Besides business and user data, applications and software are among the assets that CISOs seek to protect. Some of these applications and software provide business critical functions to customers that generate revenues for the organization. Examples include applications and software that provide customers with business services as well as applications and software that are sold as products to the clients. In the case where software applications are considered business critical information assets, these should receive a specific focus in human resources, training, processes, standards and tools. The scope of this guide is the security of web applications and the security of the components of the architecture such as the security of web servers, application servers and databases. This does not include other aspects of security that are not related to the specific application. Such as the security of the network infrastructure that supports the applications and constitutes a valued asset whose security properties such as confidentiality, integrity and availability need to be protected as well.

Objectives

This guide helps CISOs manage application security risks by considering the exposure from emerging threats and compliance requirements. This guide helps:

- Make application security visible to CISOs
- Assure compliance of applications with security regulations for privacy, data protection and information security
- Prioritize vulnerability remediation based upon risk exposure to the business
- Provide guidance for building and managing application security processes
- Analyze cyber-threats against applications and identify countermeasures
- Institute application security training for developers and managers
- Measure and manage application security risks and processes

Target Audience

- Chief Information Security Officers (CISOs)
- Senior security management
- Senior technology management

Executive Summary

The fact that applications ought to be considered company's assets is "per se" a good reason to put applications in scope for compliance with information security policies and standards. The impact of compliance with information security policies and standards for applications typically depends on the classification of the asset-data stored by the application, the type of exposure of the application to the users (e.g. internet, intranet, extranet) and the risk of the functionality that the application supports with the data (e.g. access to confidential data, transfer of money, payments, users administration etc). From an information security perspective, applications should be in scope for organizations specific vulnerability assessments and application security requirements. The security validations and certifications of applications follow specific security requirements such as the secure design, secure coding and secure operations. These are often part of the goals of application security standards. Therefore, compliance is a critical aspect of application security, and of CISOs responsibilities, but not the only one. Application security spans other security domains that CISOs are responsible for. These can be summarized as (GRC) Governance, Risk and Compliance.

- From the governance perspective, CISOs are responsible for institute application security processes, roles and responsibilities to manage them, and software security training and awareness for software developers such as defensive coding and vulnerability risk management for information security officers/managers.
- From the risk management perspective, the risks managed by the CISOs also include application security risks, such as the risks of specific threats targeting applications that process confidential user data by seeking to exploit gaps in security controls as well as vulnerabilities in applications.
- Among CISOs security domains, compliance with regulations and security standards is often the one that gets the most attention from the organization's executive management. The aim of this guide, is to help CISOs fulfill compliance requirements as well as to use compliance requirements as one of the reasons for justifying investments in application security. For some organizations, managing risks of security incidents such as credit card fraud, theft of personal identifiable information, theft of intellectual property and confidential data is what gets most of the executive management attention, especially when the organization has been impacted by data breach security incidents.

Part I: Reasons for Investing in Application Security

In this digital era, public and private organizations serve an increasing number of citizens, clients, customers and employees through web applications. Often these web applications provide “highly trusted services” over the internet, including functions that bear high risk for the business. These web applications are the target of an ever-increasing number of fraudsters and cyber-criminals. Many incidents result in a denial of online access, breach of customer data and online fraud.

Chief Information Security Officers (CISOs) are tasked to enforce application security measures in order to avoid, mitigate and reduce security risks affecting the organization's ability to deliver on its mission. This evolving threat landscape further drives audit, legal and compliance requirements. CISOs must create a business case for investing in an application security program. The business case should be mapped to the security threats on the business and the program services necessary to serve as a countermeasure. Industry security spending benchmarks and quantitative risk calculations provide support to security investment budget requests.

Part II: Criteria for Managing Application Security Risks

CISOs must prioritize security issues in order to identify areas needing attention first. To make informed decisions on how to manage application security risks, CISOs often need to assess the costs of fixing known vulnerabilities and adoption of new countermeasures and to consider the risk mitigation benefits of doing so. Costs vs. benefits trade offs are critical to decide on which application security measures and security controls to invest in to reduce the level of risk. Often CISOs need to explain to executive management the risks to applications and to articulate the potential business impacts for the organization in case applications are attacked and confidential data is breached. Security risks are business risks only when all three risk characteristics exist:

- Viable threat
- Vulnerability that may be exposed
- Asset of value

To systematically prioritize risks for investment, CISOs should consider a risk scoring methodology known as the Common Vulnerability Scoring System Version 2.0 (CVSSv2). To help regularly communicate application risk to the business executives, CISOs may consider providing "emerging cyber-threat awareness" reports to executive management.

Communicating to business executives

CISOs need to be real about cyber-threat risks and present to the business the overall picture of information security risks, not just compliance and vulnerabilities, but also security incidents and threat intelligence of threat agents targeting the organization information assets including for applications. The ability to communicate risks to the business empowers CISOs to articulate the business case for application security and justify additional spending in application security measures. This justification needs to consider the economical impact of security incidents compared with the costs of unlawful non compliance. Today's costs to the business due to the economical impacts of security incidents are much higher than the costs of non-compliance and failing audits. Often the severity of the impact of security incidents might costs CISOs their jobs and the company losing reputation and revenues.

Threat modeling

A top-down approach to identifying threats and countermeasures, CISOs should consider a threat modeling technique also described in Part III. The threat modeling technique allows the target application to be decomposed to reveal its attack surface and subsequently its relevant threats, associated countermeasures, and finally, its gaps and weaknesses.

Handling new technology

New application technologies and platforms such as mobile applications, Web 2.0, and cloud computing services offer different threats and countermeasure techniques. Changes to applications are also a source of potential risks, especially when new or different technologies are integrated within applications. As applications evolve by offering new services to citizens, clients, customers and employees, it is also necessary to plan for mitigation of new vulnerabilities introduced by the adoption and implementation of new technologies such as mobile devices, web 2.0 and new services such as cloud computing. Adopting a risk framework to evaluate the risks introduced by new

technologies is essential to determine which countermeasures to adopt to mitigate these new risks. This guide will provide guidance for CISOs on how to mitigate risks of new threats against applications, as well as of vulnerabilities that might be introduced by the implementation of new technologies.

- Mobile applications
  - Example concerns: lost or stolen devices, malware, multi-communication channel exposure, weak authentication
  - Example CISO actions: Meeting mobile security standards, tailoring security audits to assess mobile application vulnerabilities, secure provisioning, and application data on personal devices.
- Web 2.0
  - Example concerns: securing social media, content management, security of third party technologies and services
  - Example CISO actions: security API, CAPTCHA, unique security tokens in form posts, and transaction approval workflows.
- Cloud computing services
  - Example concerns: multi-tenant deployments, security of cloud computing deployments, third party risk, data breaches, denial of service malicious insiders
  - Example CISO actions: cloud computing security assessment, compliance-audit assessment on cloud computing providers, due diligence, encryption in transit and at rest, and monitoring.

Today's threat agents seek financial gain such as by attacking applications to compromise users' sensitive data and company's proprietary information for financial gain, fraud as well as for competitive advantage (e.g. through cyber espionage). To mitigate the risks posed by these threat agents, it is necessary to determine the risk exposure and factor the probability and the impact of these threats as well as to identify the type of application vulnerabilities that can be exploited by these threat agents. The exploit of some of these application vulnerabilities might severely and negatively impact the organization and jeopardize the business.

Part III: Application Security Program

From the risk management strategic point of view, the mitigation of application security risks is not a one time exercise; rather it is an ongoing activity that requires paying close attention to emerging threats and planning ahead for the deployment of new security measures to mitigate these new threats. This includes the planning for the adoption of new application security activities, processes, controls and training. When planning for new application security processes and controls, it is important for CISOs to know on which application security domains to invest, in order for the business to deliver on its missions.

To build and grow an application security program, CISOs must:

- Map business priorities to security priorities
- Assess the current state using a security program maturity model
- Establish the target state using a security program maturity model

Map business priorities to security priorities

All security priorities must be able to be mapped to business priorities. This is the first step towards establishing the relevance of every security initiative and shows business management how security supports the mission. It also demonstrates to security staff how the staff supports the mission.

Assess the current state using a security program maturity model

Accessing process maturity is a prerequisite for adoption of application security and software security processes. One criteria that is often adopted by organizations is to consider the organization's capabilities in application security domains and the maturity of the organization in operating in these domains. Examples of these application security domains include application security governance, vulnerability risk management, regulatory compliance and application security engineering; such as to design and implement secure applications. Specifically in the case of application security engineering, adopting software security assurance is often necessary when there is not direct control on implementing the security of such software since it is produced by a third party vendor. A factor to consider in this case is to measure the software security assurance using a maturity model. A pre-requisite for measuring software security assurance is the adoption of a Secure Software Development Lifecycle (S-SDLC). At high level, S-SDLC consists of embedding "build security in" security activities, training and tools within the SDLC. Examples of these activities might include software security processes/tools such as architectural risk analysis/ threat modeling, secure code reviews/static source code analysis, application security testing/application vulnerability scanning and secure coding for software developers. A reference to OWASP software assurance maturity model as well as to the several OWASP projects dedicated to software security and S-SDLC are provided in this guide as well.

Establish the target state using a security program maturity model

Not all organizations need to be at the highest maturity. The maturity should be at a level that it can manage the security risk that affects the business. Obviously, this varies among organizations and is driven by the business and what it accepts as risk as part of continuous collaboration and transparency from the security organization.

Once a target state is identified, CISOs should build a roadmap that identifies its strategy for addressing known issues as well as detecting and mitigating new risks.

OWASP provides several projects and guidance for CISOs to help develop and implement an application security program. Besides reading this section of the guide, see the Appendix B: Quick Reference to OWASP Guides & Projects for more information on the type of security engineering domain activities that can be incorporated within an application security program.

Part IV: Metrics For Managing Risks & Application Security Investments

Once application security and software security investments are made, it is important for CISOs to measure and report the status of governance, risk and compliance of the application security program to Executive Management. Furthermore, CISOs need to show the effectiveness of the application security program investment and its impact on business risk.

CISOs also need metrics to manage and monitor the people, processes, and technologies that make up the application security program. Example metrics for measuring governance, risk and compliance of application security processes are also included.

Security metrics consist of three categories:

- Application security process metrics
- Application security risk metrics
- Security in the SDLC metrics

Application security process metrics

These support informed decisions to decide where to focus the risk mitigation effort and to manage application security risks more effectively. These risk management goals are usually very organization specific and depend on the type of organization and the industry sector that the organization does business with, to decide which application security risks should be prioritized for action.

- How well is the organization meeting security policies, technical standards, and industry practices?
- How consistently are we executing security SLAs? By application? By division? By channel?

Application security risk metrics

- Vulnerability risk management metrics - What is the Mean Time to Repair on an annual basis? On a monthly basis? By application? By division? What are the known security issues in production?
- Security incident metrics - What security issues have been exploited? Were they known issues that were released in production? What was the cost to the business?
- Threat intelligence reporting and attack monitoring metrics - Which applications are receiving more attacks than others? Which applications have upcoming expected peak usage?

Security in the SDLC metrics

One often neglected aspect when spending on software security is the economics of dealing with insecure software applications. The investment in software security to identify and fix security issues prior to release of software in production actually pays for itself because it saves the organization money. Patching vulnerabilities after applications are released into production is very expensive; it is much cheaper than to invest in secure architecture reviews to identify design flaws and remediate them prior to coding, as well as to invest in secure code reviews to identify and fix security bugs in software during coding, and to ensure that releases are configured correctly.

- Metrics for risk mitigation decisions - What is the Mean Time to Repair by an application's risk category? Does it meet expectations? What is the risk heat map by application? By division? By channel?
- Metrics for vulnerability root causes identification - What are the root causes of vulnerabilities for each application? Is there a systemic issue? Which security practices have

been best adopted by each development team? Which development teams need more attention?

- Metrics for software security investments - Which SDLC phase have identified the most security issues? What is the maturity of the corresponding security practices in each SDLC phase? What is the urgency for more security people, process, and technologies in each SDLC phase? What are the cost-savings between security testing versus downstream vulnerability penetration testing? What are the cost-savings between issues identified in each phase?

The CISO Guide

Part I : Reasons for Investing in Application Security

I-1 Executive Summary

In this digital era, public and private organizations serve an increasing number of citizens, customers and employees through web applications. Often these web applications provide "highly trusted services" over the internet, including functions that bear high risk for the business. These web applications are the target of an ever-increasing number of fraudsters and cyber-criminals. Many incidents result in a denial of online access, breach of customer data and online fraud.

Chief Information Security Officers (CISOs) are tasked to enforce application security measures in order to avoid, mitigate and reduce security risks affecting the organization's ability to deliver on its mission. This evolving threat landscape further drives audit, legal and compliance requirements. CISOs must create a business case for investing in an application security program. The business case should be mapped to the security threats on the business and the program services necessary to serve as a countermeasure. Industry security spending benchmarks and quantitative risk calculations provide support to security investment budget requests.

I-2 Introduction

Applications have grown increasingly critical in organizations. Oftentimes delivering critical services with legal and regulatory requirements. For bank customers, these are feature rich functions that allow them to open bank accounts, pay bills, apply for loans, book resources and services, transfer funds, trade stocks, view account information, download bank statements and others. This online experience is convenient for people: it allows them to perform the same financial transactions as being at the branch/office/outlet, but with the added convenience of conducting these transactions remotely from their home computer or mobile phone. At the same time, this convenience for customers comes at a price to the financial organizations involved in developing and maintaining these applications. For example, online banking and commerce sites have become the target of an increased number of fraudsters and cyber-criminals and victims of security incidents. Several of these incidents resulted in a denial of online access, breaches of data and online fraud.

In the case of data breach incidents, often these attacks from fraudsters and cyber-criminals involve the exploitation of applications such as SQL injection to compromise the data stored in the application database and cross site scripting to execute malicious code such as malware on the user's browser. The targets of these attacks are both the data and the application business functions for processing this data. In the case of online banking applications, the data targeted by hacking and malware include personal data of individuals, bank account data, credit and debit card data, online credentials such as passwords and PINs and last but not least, alteration of data in on-line financial transactions such as transfers of money to commit fraud. Verizon's 2012 data breach investigations report identifies hacking and malware as the most prominent types of attack, yielding stolen passwords and credentials, and thus posing a major threat to any organization that trades online.

To cope with this increase of incidents targeting applications, such as denial of services and data breaches often caused by hacking and malware, Chief Information Security Officers (CISOs) have been called by company's executives such as the Chief Information Officer (CIO), Legal Counsel or Chief Financial Officer (CFO) to build and enforce application security measures to manage application security risks to the organization. For financial organizations for example, the increasing threat to applications such as online banking applications, challenges CISOs to enforce additional application security controls and increase the investment in application security to cope with the increasing risk.

Due to the evolving threat landscape and increased pressure from audit, legal and compliance, in the last decade, investments in application security have been a growing proportion of overall information security and information technology budgets. This trend is also captured in applications security surveys such as the 2009 OWASP Security Spending Benchmarks Project Report that, for example, stated "Despite the economic downturn, over a quarter of respondents expected application security spending to increase in 2009 and 36% expected to remain flat". Furthermore, in the 2013 OWASP CISO Survey, about 87% of respondents indicated that application security investment would either increase or remain constant. Nevertheless, making the business case for increasing the budget for application security today remains a challenge because of the recession economy and prioritization of spending for development of new application features and platforms (e.g. mobile devices), initiatives to expand service uptake or profitability, and marketing to attract new customers and retain existing customers. Ultimately, in today's recession type of economic climate and in a scenario of slow growth in business investments including the company's built-in software, it is increasingly important for CISOs to articulate the "business case" for investment in application security. Since it also appears to be a disconnect between organization's perceived threats (application security threats are greatest) yet spending on network and infrastructure security is still much higher, we would like to shed some light on the business impact of data breaches due to application vulnerability exploits and how much these might cost to organizations. Typically, additional budget allocation for application security includes the development of changes in the application to fix the causes of the incident (e.g. fixing vulnerabilities) as well as rolling out additional security measures such as preventive and detective controls for mitigating risks of hacking and malware and limiting the likelihood and impact of future data breach incidents.

CISOs can build a business case for additional budget for application security today for different reasons; some directly tailored to the specific company risk culture or appetite for risk; others tailored to application security needs. Some of these needs can be identified by the analysis of the results of application security surveys. To assess these needs, readers of this guide are invited to participate in the OWASP CISO Survey so that the contents of this guide can be tailored to the needs of CISOs participating in the survey.

2013 CISO Survey: Growing Focus

An increased perception of risk of application targeted threats and shifts the organization investment from the traditional network security to application security. In comparison of the application security budget to the company's annual budget:

- **47% of CISOs have seen an increase**
- **39% consider it relatively constant**
- **13% have seen a decrease**

The budgeting for application security measures might depend on different factors such as compliance with security policies and regulations, operational risks management including the risks due to application vulnerabilities and the response of security incidents involving applications. For the sake of this guide we will focus on the following areas to target application security spending:

- Compliance with security standards, security policies and regulations;
- Identification and remediation of application vulnerabilities;
- Implementation of countermeasures against emerging threats targeting applications.

Nevertheless, assuming the business cases can be made along these goals, CISOs today still have the difficult task to determine “how much” money should the company spend for application security and “where” that is on “which security measures” to spend it. Regarding the how much, often it gets down to how much is needed to invest to satisfy compliance requirements and pass the auditor’s check. When the focus is compliance, the focus is to develop and implement application security standards and map these security requirements to current projects. When the focus is vulnerability risk management, the main goal is to fix high risk vulnerabilities and to reduce the residual risk to an acceptable value for the business. When the focus is security incident management, the focus is how to investigate and analyze the suspected security breaches and recommend corrective actions. When the focus is application security awareness, the focus is on institute application security training for the workforce.

For today’s CISO there is an increased focus on making decisions for mitigating risks. Both for mitigating real risks (e.g. incidents, vulnerability exploits) and for mitigating non-compliance risks (e.g. unlawful non-compliance), the question for CISOs is "where" and "how" to prioritize the spending of the application security budget. Often the question is which countermeasure, application security process, activity, or security tool yields “more bang for the money” for the organization. Regarding the "where" it comes down to balance correctly different application security and risk domains - to name the most important ones: business

governance, security risk management, operational management that includes network security, identity management, access control and incident management. Since as a discipline, application security encompasses all these domains, it is important to consider all of them and look at the application security investment from different perspectives.

I-3 Information Security Standards, Policies and Compliance

Identifying standards, policies and other mandates in scope for compliance

One of the main factors for funding an application security program is compliance with information security standards, policies and regulations mandated by applicable industry standards regulatory bodies. Initially, it is important for the CISO to define what is in the scope for compliance and how it affects application security. Depending on the industry sector and the geographical location in which the organization operates, there will be several different types of security requirements that the organization needs to comply with. The impact of these requirements is also on the applications that manage and process data whose security falls under the scope of these standards and regulations. The impact on applications consists of performing scheduled risks assessment and to report the status on compliance to the auditors.

Examples of data security and privacy standards that apply to applications in the US include:

- Payment Card Industry (PCI) Data Security Standard (DSS) for payment card merchants and processors
- FFIEC guidelines for US financial organizations whose applications allow clients and consumers to bank online and conduct transactions such as payments and money transfers
- FISMA law for US federal government agencies whose systems and applications need to provide information security for their operations and assets
- HIPAA law for securing privacy of health data whose applications handle patient records in the U.S. healthcare industry
- GLBA law for US financial institutions whose applications collect and store individuals' personal financial information
- US State Data Breach Disclosure laws for organizations whose applications store and process US state resident Personal Identifiable Information (PII) data when this data is lost or stolen in clear (e.g. un-encrypted)
- FTC privacy rules for organizations whose applications handle private information of consumers in the US as well as when operating in EU countries to comply with "Safe Harbor" rules

OWASP provides several projects and guidance for CISOs to help develop and implement policies, standards and guidelines for application security. Please consult the Appendix B: Quick Reference to OWASP Guides & Projects for more information.

Capturing application security requirements

PCI DSS

Most of the applications that carry out payment transactions such as merchant type of e-commerce applications that handle credit cardholder data are required to comply with the Payment Card Industry Data Security Standard PCI DSS. The requirements for the protection of cardholder data when it is stored by the application includes several PCI DSS requirements such as rendering or encrypting the Primary Account Number (PAN) and masking the PAN when it is displayed. The PCI-DSS requirement for card authentication data such as PIN, CVC2/CVV2/CIDs is not to store these data at all, even in encrypted form after a payment has been authorized. Credit cardholder data needs to be protected with encryption when it is transmitted over open networks. These requirements for protection of cardholder personal account numbers and cardholder authentication data motivate the CISO to document internal security requirements to comply with these provisions and to adopt application security measures and assessments to verify that these requirements are met by the applications that are in scope. Besides protection of cardholder data, PCI-DSS has provisions for the development and maintenance of secure systems and applications, for testing security

systems and processes and for the testing of applications for common vulnerabilities such as those defined in the OWASP Top Ten.

The need of compliance with the PCI DSS requirements can be a reason to justify an additional investment in technology and services for application security testing: examples include source code security reviews with SAST (Static Analysis Security Testing) assessment/tools and application security reviews with DAST (Dynamic Analysis Security Testing) assessments. For a merchant that develops and maintains a web application such as an e-commerce web site that handles credit card payments, the main question is whether to allocate budget to application security measures and activities to comply with PCI DSS or to incur in fines (e.g. up to $ 500,000 when credit cardholder data is either lost or stolen). From this perspective, unlawful noncompliance with regulations and standards might be treated as another risk by the organization and as any other risk, this could be mitigated, transferred or accepted. If the risk of being non-compliant is accepted, CISO should consider that the data breach risk, because of not implementing basic security controls such as data encryption but also input validation, might be much higher than non-compliance risk.

Example: T.J.Maxx non-compliance with PCI DSS

T.J.Maxx was non-compliant with PCI DSS when 94 million credit card numbers were compromised in a data breach. Yet, the non-compliance costs for failing to encrypt or truncate card numbers and remediate application vulnerabilities, such as SQL injection, were less of the overall costs incurred by the businesses impacted by this security incident. In the case of T.J Maxx credit card data breach incident, the economical costs incurred by T.J. Maxx because of the incident were a factor of at least a thousand times higher (if not more) than the costs of not compliance with PCI-DSS: several hundreds of millions of US dollars vs. several hundreds of thousands of US dollars.

FFIEC

In the U.S. banking sector, applications that handle sensitive customer information and are allowed to process financial transactions such as to transfer money between different bank accounts (e.g. electronic wires) must comply with Federal Financial Institutions Examination Council (FFIEC) guidelines for online authentication. Requirements include strong authentication such as multi-factor authentication (MFA).

Business drivers for application security investment

Federal Financial Institutions Examination Council (FFIEC) requirements for authentication of online banking sites can justify budgeting for application security measures to secure design, implement and test the provision of MFA controls in the application.

GLBA

For US consumers, privacy is regulated under different laws and regulations depending on the industry sectors. In the US financial sectors, laws that govern consumers privacy include GLBA laws and FTC rules. From a GLBA compliance perspective, financial applications need to provide disclosure to application users of which PII is collected, processed and stored and how it is shared among the financial institution businesses and affiliates including third parties. From an FTC compliance perspective, organizations that store consumer PII need to disclose their due diligence security practices to consumers and can be considered liable when

such practices are not followed as in the case of a breach of consumer's private information and in a clear breach of the license agreements with the consumers. Because privacy laws in the US mostly require acknowledging to consumer that the personal data is protected, the impact of security is limited to notifications, acknowledgements and "opt out" controls. Exceptions are cases where privacy controls are implemented as application privacy settings (e.g. as in the case of Facebook), and offered to users of the application as "opt in controls" to comply with the FTC Safe Harbor rules.

Privacy laws

In general, applications that store and process data that is considered personal and private by country specific privacy laws need to protect such data when it is stored or processed. What is considered private information varies country by country. For countries that are part of the European Union (EU) for example, personal data is defined in EU directive 95/46/EC, for the purposes of the directive: Article 2a: "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

For most of the US States, protection of personal identifiable information (PII) is driven by data breach notification laws such as SB1386 where PII is more narrowly defined than in the EU directive as the individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number. (2) Driver's license number or State Identification Card number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. For purposes of these laws, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Applications that process and store data that is considered personal private data by EU privacy laws or PII by US States data breach notification laws, need to implement security controls such as authentication, authorization, encryption, logging and auditing to protect the confidentiality, availability and integrity of this data. These information security requirements are typically part of the information security policy enforced by the organization. These security requirements, indirectly translate in security requirements for applications that store and process data that is either considered confidential or confidential PII. Budgeting application security programs for complying with personal and consumer data privacy requirements is justifiable both as internal compliance with information security policy, as well as for mitigating the reputation damage to the organization in the case this data is either lost or compromised. In addition to reputation damage, organizations might incur regulatory fines and legal costs because of non-compliance with local privacy laws.

I-4 Risk Management

Risk management is certainly one of the core CISO functions. The purpose of this section of the guide is to help CISOs in developing, articulating and implementing a risk management process. OWASP also provides documentation guides that can be useful for CISOs to implement a risk management strategy for applications. After reading this section, consult Appendix B for a reference to OWASP guides and projects.

Proactive vs. reactive risk management

Proactive risk management consists of focusing on mitigating the risks of threat events before these might possibly occur and negatively impact the organization. Organizations, whose focus is proactive risk management, plan to protect mission critical assets including applications ahead of potential threats targeting them. Proactive risk mitigation activities for applications include focusing on threat intelligence to learn about threat agents, application threat modeling to learn how the application can be protected by attacks from different threat agents, security testing and fixing of potential vulnerabilities in the application as well as in the source code before these are exploited by potential attackers. A pre-requisite for proactive risk management is to have an inventory of the mission critical applications with associated risk profiles that allow CISOs to identify the critical digital assets such as data and functions that need to be prioritized and planned for proactive risk mitigation activities. CISOs whose organizations focus on proactive risk mitigation measures have typically adopted a risk mitigation strategy and act upon information from threat intelligence and monitored security events and alerts to raise the bar on acceptable technical and business risks. CISOs whose focus is proactive risk mitigation usually require the roll out of additional countermeasures ahead of new threats and new compliance requirements.

Reactive risk management consists of responding to risk events as they occur to mitigate negative impacts to the organization. Examples of reactive risk management activities include security incident response, security incident investigations and forensics and fraud management. In the case of application security, reactive risk management activities include vulnerability patch management, fixing application vulnerabilities in response to reported security incidents or when these are identified by third parties, performing application risk assessment due to occasional (not planned) requirements to satisfy specific compliance and audit requirements. CISOs whose organizations focus on reactive risk management typically spend more focus on responding to unplanned risk management events. Often the focus of reactive risk management is "damage containment" to “stop the bleeding” and less focus is dedicated to planning for risk mitigation ahead of potential negative events targeting applications. Typically organizations whose focus is on reactive risk management have their CISOs spending most of their time on incident response and management and remediating application vulnerabilities either ahead of production releases or patching applications that are already released in production. When the prime focus of the CISO function is on reactive risk management, it is important to recognize that reactive risk mitigation, even if it cannot always be avoided because security incidents happen, is not cost effective since the cost of remediating issues after they have been either reported or exploited by an attacker is several factors of magnitude higher than identifying and fixing the same by adopting preventive risk mitigation measures.

A proactive risk mitigation approach is preferable to a reactive risk mitigation approach when making the business case for application security. A proactive risk mitigation approach might consist on using the opportunity of a required technology upgrade of a application to introduce new functionality or when an old application reaches end of life, and needs to migrate to a newer system/platform. Designing new features to applications represents an opportunity for CISOs to demand upgrade security technology to new standards and implement stronger security measures as well.

Asset centric risk management

CISOs whose information security policies are derived for compliance with information security standards such as ISO 17799/ISO 27001 include asset management as one of the security domains that need to be

covered. In the case when these assets include the applications, assets management requires an inventory of the applications that are managed by the organization in order to implement a risk management approach. This inventory includes information on the type of applications, the risk profile for each application, the type of data that is stored and processed, patching requirements and the security assessments such as vulnerability testing that are required. This inventory of applications is also critical to track application security assessments and risk management processes conducted on the application, the vulnerabilities that have been identified and fixed as well as the ones that are still open for remediation. The risk profile that is assigned to each application can also be stored in the application inventory tool: depending on the inherent risk of the application that depends on the classification of the data and the type of functions that the application provides, it is possible to plan for risk management and the prioritization of the mitigation of existing vulnerabilities as well as for the planning for future vulnerability assessments and application security assessment activities. One of the application security activities that take advantage of asset centric risk management is application threat modeling. From an architecture perspective, assets consist of several components such as application servers, application software, databases and sensitive. Through application threat modeling, it is possible to identify threats and countermeasures for the threats affecting each asset. CISOs whose focus is on asset risk management, should consider implementing application threat modeling as proactive application security and asset centric risk management activity.

Technical vs. business risk management

When deciding how to mitigating the application security risks it is important to make the trade off between technical risks and business risks. Technical risks are the risks of either technical vulnerabilities or control gaps in an application whose exploit might cause a technical impact such as lost and compromised data, server/host compromise, unauthorized access to an application data and functions, denial or disruption of service as examples. Technical risks can be measured as the impact of confidentiality, integrity and availability of the asset caused by a technical event/cause such as vulnerability that is identified by an application security assessment. The managing of these technical risks typically depends on the type of the vulnerability and the risk rating assigned to it, also referred to as "severity" of the vulnerability. The severity of the vulnerability can be calculated based upon risk scoring methods such as FIRST's CVSS, while the type of vulnerability can be classified based upon the group that the vulnerability falls into such as using MITRE's CWE. CISOs can use the risk scoring of a vulnerability reported as HIGH, for example, to prioritize such vulnerability for mitigation ahead of vulnerabilities that are scored as MEDIUM or LOW risk. In making this technical vulnerability risk management decision, CISO won't consider the economical impact of the vulnerability to the business, such as in the case the value of the asset impacted by the vulnerability is either lost or compromised.

Business risk management occurs when the value of the asset is taken into account to determine the impact to the organization. This requires the association of technical risk of the vulnerability with the asset value to quantify the risk. The risk can be factored as the likelihood of the asset being compromised and the business impact caused by the exploit of the vulnerability. For example, in the case that a high risk technical vulnerability such as SQL injection (assumed is fully, 100% exposed as a pre-authentication issue) is exploited, the business impact can be determined as impact to an asset, such as data, that is classified as sensitive data and whose value if compromised is estimated as $ 250/data record (e.g. based upon either internal incident cost estimates or publicly reported estimates). The aggregated value of the sensitive data of 100,000 records stored in a database that could be exploited by SQL injection is therefore $ 25 Million. If the probability of a sensitive data compromise due to the exploit of SQL injection vulnerability is estimated as 10 % (1 successful data breach incident caused by SQL injection every ten years) the potential economical impact is a loss of $ 2,500,000. Based upon these estimates, it is possible to calculate how much to budget in application security measures (e.g. detective and preventive controls) for mitigating the risks to the business.

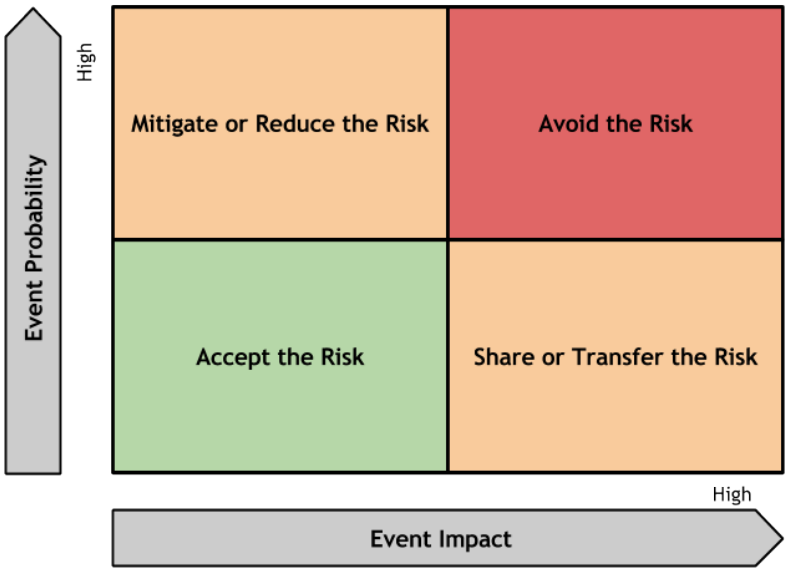
It should be noted that estimating business risks is much more difficult than estimating technical risks since business risk estimates require estimates of the likelihood of specific types of security incidents (e.g. data

breaches) as well as the estimates of the monetary losses (e.g. loss of revenue, legal-compliance costs, incident cause repair costs) caused by that incident. Typically these estimates are not easy to make in absence of specific data and calculation tools that can factor the frequency of security data breach incidents and keep records of direct and indirect costs suffered by the organization as a result of these security incidents. Nevertheless, statistical data of data breach incidents, estimates of the costs of data breach incidents as well as data breach quantitative risk calculators might help. The Appendix A Value Data & Cost of an Incident provides examples, formulations and online calculators to help CISOs assigning monetary value to information assets and determine the monetary impact for the organization in the case where such assets will be lost because of a security incident. The purpose of these quantitative risk calculations is to help CISOs decide how much is reasonable to spend in application security measures to reduce the business impacts for the organization in the case of data breach incident.

Risk management strategies

Once security risks have been identified and assigned a qualitative value such as high, medium and low risk, the next step for the CISO is to determine what to do with that risk. To decide "what to do with the risks" CISOs usually rely upon their organization's risk management processes and risk mitigation strategy. Risk management processes are usually different for each type of organization. At high level, risk management depends on the risk mitigation strategy that is adopted by the organization. Depending on the assessment of the level of risk impact and probability, for example, an organization might decide to accept the risks whose likelihood and impact are low, mitigate or reduce the risks (e.g. by applying security measures) that have high probability and low impact, transfer or share the risks (e.g. to/with a third party such as through contractual agreements) that are of low probability and high impact and avoid the risks (e.g. such as not to implement high risk functions, not to adopt high risk technologies) that have high probability and impact. A visual example of this risk mitigation strategy factored by event likelihood and impact is shown in the diagram below.

Figure 1 RISK MITIGATION STRATEGY BASED ON EVENT LIKELIHOOD AND IMPACT



In the case high risks cannot be avoided because of business decisions requiring to mitigate them, and risks cannot be transferred to third parties through contractual agreements and cyber insurance, a possible risk strategy for the organization could be to mitigate all risks that are medium and high and accept (e.g. do nothing) only the ones whose residual risk (e.g. the risk left after either measures or compensating control are either applied or considered) are low. Risk mitigation strategies can also factor business risks using qualitative risk analysis that factor risks such as probability and economical impacts. Once the risk has been determined, the next step is to decide which risk the organization is willing to accept, mitigate, transfer or to avoid. For the risks that the organization is willing to accept it is important for CISOs to have a risk acceptance process that qualifies the low level of risk based upon the presence of compensating controls and that can be signed off by him and executive management. For the risks that are chosen for risk mitigation, it is important to determine which security measures/corrective actions are deemed acceptable by the organization and to decide which of these measures are most effective in reducing risks by minimizing the costs (e.g. highest benefit vs. minimum security measure total costs). This is where the risk mitigation strategy needs to consider the cost of potential security incidents, such as data breaches, to decide how much is reasonable for the organization to budget for investments in application security measures. An important aspect of the risk strategy for CISOs is to decide which security measures work best together as "pluribus unum" that includes applying preventive and detective controls to provide a defence in depth of the application's assets. Finally, for the risks that are either transferred or shared with a third party, it is important for the CISO to work with legal to make sure risk-liability clauses are documented in the legal agreements and service license agreements are signed by the organization with the third party service provider/legal entity.

Threat analysis and awareness of emerging threats

Making the business case for additional spending on application security measures is not always justifiable without risk data from the analysis of the impact of emerging threats and the increased level of risks that needs to be mitigated. Threat analysis data allow informed risk management decisions. In the absence of such data, the management is left with subjective considerations about threats.

Subjective considerations about threats are most often decisions based upon Fear, Uncertainty and Doubt (FUD). Acting upon FUD to mitigate risks posed by emerging threats is late-coming and ineffective. Example actions based on FUD include, but are not limited to:

- Fear of data breaches
- Fear of failing audit and compliance
- Uncertainty regarding business threats
- Doubts about effectiveness of existing security measures in light of recent security incidents

The intent of this part of the guide, is to help CISOs to create an additional business case for application security investment based upon objective threat analysis instead of subjective considerations. From a compliance with standards perspective, objective considerations are based upon a rationale for investing in applications security that includes complying with new security standards and regulations that impact applications. From a threat analysis perspective, objective considerations are based upon data regarding the business impact of emerging threat agents seeking to compromise applications for financial gain. Specifically regarding making the case for mitigation of risks, it is necessary for CISOs to avoid assumptions and back the case with data such as reports and analysis of cyber-threats and security incidents, costs of data breaches to estimate liability and quantitative calculations of risk based upon estimates of probability and impacts. Based upon risk calculations and data breach cost estimates, it is possible for the CISO to articulate how much the organization should invest in application security and to determine in which specific measures to invest.

From a fear perspective it is true that CISOs can also exploit the momentum, being this either a negative or positive event, but this is part of a reactive risk management approach and low maturity in dealing with risks.

Often application security spending can be triggered by a negative event such as a security incident, since this shifts senior management's perception of risk. However, CISOs should find that using a one to two year roadmap to drive security investment would be more effective as found in the 2013 OWASP CISO Survey.

Figure 2 ANALYSIS INDICATING THAT 1-2 YEAR ROADMAPS SUPPORT OBTAINING PROPER SECURITY INVESTMENT; SHORTER AND LONGER ROADMAPS DO NOT (OWASP CISO SURVEY 2013)

Security Investment is...	3 months	6 months	1 year	2 years	3 years	5 years+	Grand Total
Decreasing	1.69%	3.39%	5.08%	1.69%	3.39%	3.39%	18.64%
Increasing as a % of total expenditures	3.39%	1.69%	18.64%	16.95%	3.39%	0.00%	44.07%
Relatively constant	5.08%	3.39%	11.86%	10.17%	3.39%	3.39%	37.29%
Grand Total	10.17%	8.47%	35.59%	28.81%	10.17%	6.78%	100.00%

In this case, the money is probably already being spent to limit the damage, such as to remediate the incident and implement additional countermeasures. The main question then is what further investment in application security will reduce the likelihood and impact of another similar incident happening in the future. One approach is to focus on applications that might become a target for future attacks.

Addressing the business concerns after a security incident

The implementation of a security incident response process is an essential activity for every CISO. Such security incident response process requires the identification of a point of contact for security issues, the adoption of a security issue disclosure process and the creation of an informal security response team(s). In the case of a security incident, CISOs are often tasked to conduct root cause analysis for incidents, collect per-incident metrics and recommend corrective actions. In Appendix B we provide CISOS with a quick reference to OWASP guides & projects to help CISOs investigating and analyzing suspected and actual application security incidents and recommend corrective actions.

Once the root causes of the incident have been identified and corrective actions have been taken to contain the impact of the security incident, the main question for CISOs is what should be done to prevent similar security incidents to occur in the future. If an application has been targeted by an attack and sensitive data was either lost or compromised the main question is to whether similar applications and software might be also at risk of similar attacks and incidents in the future. The main question for the CISO is which application security measures and activities should be targeted for spending to mitigate the risks of breaches of sensitive data due to malware and hacking attacks to applications and software that are developed and managed by the organization.

After these measures are selected, the next question is how much should be spent in countermeasures. From the costs vs. benefit perspective, application security spending matching all of the costs of the business impact of a possible data breach is not justifiable since it will cost the business as much as doing nothing hence with no risk benefit for investing in countermeasures. The main question for the CISOs is therefore how much should be spent to reduce the risk of a data breach incident at a fraction of the cost of implementing a security measure: if not 100%, is it 50%, 25% or 10% of all possible monetary losses? Also,

how will I estimate the monetary losses of a security incident? Which methods should I use? Does the loss estimate include non-monetary losses such as reputation loss?

The goals of the following sections of the guide are to help CISOs in budgeting of application security measures for mitigating risks of data breach incidents by analyzing the risks of data breach incidents, monetizing the economical impacts and estimating the likelihood and the business impacts. Only after this "risk due diligence" work is done is it possible to determine the costs and compare with the risk mitigation benefits and decide in which security measures to invest. In Appendix A of this guide we provide a quick reference to assign monetary value to information assets and to determine the monetary impact of a security incident based upon statistical data. After measures are implemented it is important to measure and monitor security and the risks. In Appendix B we provide examples of OWASP projects that can help the CISO to measure and monitor security and risks of application assets within the organization.

Budgeting of application security measures for mitigating risks of data breach incidents

For guiding the CISOs in making decisions on "how much money the organization needs to budget for application security" we will focus on risk mitigation criteria rather than other factors such as percentage of the overall Information Technology (IT) budget and year over year budget allocation for applications security as a fraction of overall information security budget that includes compliance and operational-governance costs. A risk based application security budgeting criteria documented in this guide consist of the following:

- Estimate of the impact of the costs incurred in the event of an security incident
- Quantitative risk calculation of the annual cost for losses due to a security incident
- Optimization of the security costs in relation to cost of incidents and cost of security measures
- The return of security investment in application security measures

We shall explain in the following sections of this guide each of these criteria and how they can be used for quantifying how much money to spend on application security measures.

Analyzing the risks of data breach incidents

There are two important factors to determine the risk of a security incident: these are the negative impact caused by the security incident and the likelihood (probability) of the incident. To obtain an estimate of the impact of the costs incurred in the event of a security incident, the key factor is the ability to ascertain the costs incurred due to the security incident. Examples of negative impacts to an organization because of a security incident might include:

- Reputation loss such as, in the case of publicly traded company, a drop in stock price as consequence of announced security breach;
- Loss of revenue such as in the case of denial of service to a site that sells services or goods to clients and customers;
- Loss of data that is considered an asset for the company such as users' confidential data, Personal Identifiable Information (PII), authentication data, and trading secrets/intellectual property data;
- Inability to deliver a statutory service to citizens;
- Adverse impact on individuals whose data has been exposed.

Monetizing the economical impacts of data breach incidents

In the case of a security incident that caused a loss of sensitive customer or employee data such as personal identifiable information, debit and credit card data, the costs incurred by the organization that suffered the loss include several operational costs also referred as failure costs. In the case of a financial services company,

these are the costs for changing account numbers, remission costs for issuance of new credit and debit cards, liability costs because of fraud committed by the fraudster using the stolen data such as for illicit payment transactions and withdrawal of money from ATMs. Often times, the determination of such "failure" costs is not directly quantifiable by an organization, such as when this monetary loss is not directly caused by a security incident, hence ought to be estimated as a possible impact. In this case, CISOs can use statistical data to determine the possible liability costs to the company in case of data loss incident. By using reported statistical data from data loss incidents, it is possible to estimate the costs incurred by companies to repair the damage caused by a security incident that resulted in losses of sensitive data or identity loss.

The value of data will be different for each organization, but values in the range of $500 to $2,000 per record seem to be common.

Data value: $200 to $2,000 per record

We will use this range for the remaining discussion, but each CISO needs to come up with some valuation of their own that can then be used to calculate the impact of a data loss.

Note: Appendix A Value of Data & Cost of an Incident contains a detailed discussion, examples and a data breach calculation tool to estimate the cost of a data breach based upon statistical data.

Estimating the likelihood of data breach incidents

One of the challenges of the calculation of the burden to the company because of a potential data loss is to get an accurate estimate of the amount of the loss x victim and of the probability or likelihood of such loss occurring. Statistical data about reported data loss incidents to breach notification letters sent to various jurisdictions in the United States collected by the Open Security Foundation's (OSF) DataLossDB show that the percentage of 2010 data loss incidents breaching a web interface is 9% and the percentage that reported as being a hack is 12%, fraud 10% and virus 2%. The highest reported incident by breach type is stolen laptop with 13% of all reported incidents.

The data from OSF DataLossDB related to web as type of breach differ from the statistics of the Verizon's 2011 data breach investigations report where hacking (e.g. brute force, credential guessing) and malware (e.g. backdoors, keyloggers/form grabbers, spyware) represent the majority of threats for security breaches (50% and 49% respectively) and attacks against applications represent 22% of all attack vectors and 38% as percent of records being breached.

These differences might be explained by the fact that the Verizon study is based upon a subset of data from the U.S Secret Service and does not include, for example, cases related to theft and fraud that are instead counted on the overall OSF DataLoss DB statistical data. Furthermore, according to the Verizon report; "the scope of the survey was narrowed to only those involving confirmed organizational data breaches". In the case of OSF, survey data includes data breaches covered by U.S State data breach notification law such as when resulting in disclosure of customer's Personal Identifiable Information (PII) and reported by organizations with notification letters sent to various jurisdictions in the United States.

Quantification of the business impact of data breach incidents

In the cases when the impact of an occurred data breach due to a security incident are not being recorded and notified to the public in compliance with the data breach notification laws enforced by different countries and jurisdictions, it is necessary to estimate it based upon risk estimate calculations. Besides the calculation of liability costs based upon the value of data (refer to Appendix A Value of Data & Cost of an Incident for

estimate the value of data), quantitative risk analysis can be used to estimate the spending for application security measures on the yearly basis such as by calculating the impact of a security incident on an annual basis. Quantitative risks can be calculated by the assessment of the Single Loss Expectancy (SLE) or probability of a loss as a result of a security incident and the Annual Rate of Occurrence (ARO) or the annual frequency of the security incident. By using quantitative risk analysis and using publicly available reports of data breaches, CISOs can estimate the amount that a given organization managing an application would loose and therefore should spend on application security measures to mitigate the risk of a data loss due to the exploitation of an application vulnerability. The accuracy of this risk estimate depends on how reliable and pertinent the data breach incident is to application security. It is therefore important to choose the data carefully as this is being reported as being caused by an exploit of application vulnerabilities such as SQL injection (e.g. Sony and TJX Max data breaches).

The SLE can be calculated with the following formula:

SLE = AV x EF

Where, AV is the Asset Value (AV) and EF is the Exposure Factor (EF). The EF represents the percentage of the asset loss because of the realization of a threat or an incident. In the case of the 2003 US Federal Trade Commission (FTC) incident data this represents the amount of the population that suffered identity fraud and is 4.6%.

Assuming the AV of 1 million accounts of $ 655,000,000 ($655 per account based upon 2003 FTC data) and an exposure factor of 4.6%, the estimated SLE of the data breach incident is $ 30,130,000. Assuming a frequency of 1 attack every 5 years such as in the case of TJX Inc data breach incident (discovered in mid-December 2006 and due to SQL injection exploits) the ARO is 20%. Hence the estimated annual loss or Annual Loss Expectancy (ALE) can be calculated using the formula:

ALE = ARO x SLO

The calculated Annual Loss Expectancy (ALE) for data loss incident is therefore $ 6,026,000/year over 10 years.

Considering costs and benefits of application security measures before making investments

Now the question is if using quantitative risk analysis leads to an estimate of the optimal investment for application security measures. The honest answer is, not necessarily. The correct answer is to use cost vs. benefit analysis to determine the optimal value. By comparing the costs of security incidents against the costs of security measures, it is possible to determine when this maximizes the benefit, that is, the overall security of the application.

In the case of software security costs for example, the cost due to software security failures including security incidents decreases as the company spends more money in security measures as shown in (FIG 1). The assumption is that an increased investment in security measures translates to less risk and a reduced impact for the business. This is based on the assumption that risks are decreasing when investments in security are increasing. The other assumption is that investments are directed toward effective risk mitigation security measures. To decide which security measures are risk mitigation effective and should be invested in, it is implied that CISOs have done a risk analysis to identify the most cost effective security measures (e.g. processes, technical controls, tools, training and awareness etc.) and selected the ones that reduce the risk the

most and cost the least to implement, deploy and maintain. Note: this might not always be true as more spending in security measures does not always translate into increased risk mitigation: for example spending more on anti-virus protection won't reduce the risk of malware compromise as malware is designed to evade virus signature detection systems.

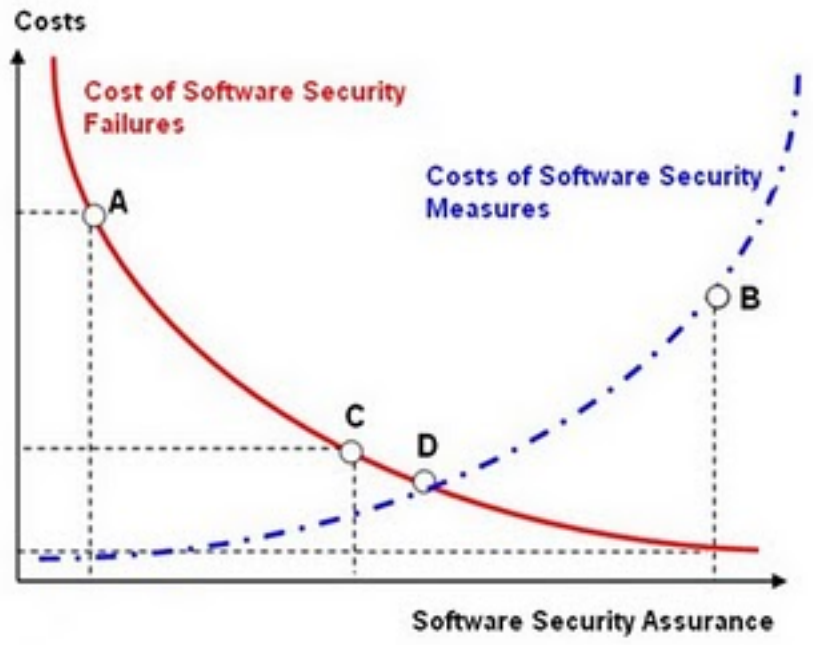
It is of the upmost importance to consider the effectiveness of security measures in mitigating the possible impact of specific threats before deciding if it is cost effective to invest in them. In part II of this guide we provide guidance to help CISOs identify which vulnerabilities should be prioritized for fixing and which security measures are most effective in mitigating specific threats targeting web applications. Before making decisions on which security measures to invest please consult Part II "Criteria for Managing Application Security Risks".

With these assumptions, the more money spent on security measures to prevent security incidents the less money will be lost in a security incident when this occurs; such as costs to recover from security incident, fix vulnerabilities, implement new measures and paying for regulatory fines, contract liability costs and legal costs. The assumption is that, because of an increase in spending in protective and detective security controls, testing and fixing vulnerabilities and other measures, security incidents will be less likely to occur and when they occur will have a reduced impact for the organization. In the case of applications, the implementation of security measures falls under the scope of the application security program. CISOs can look at Part III "Application Security Program" of this guide to learn which security processes, tools and training should be considered prior to investing in application security measures.

With these caveats, as more money is spent in application security a point could be reached when the costs outweigh the benefits. This is obviously not the objective of risk management and a limit that should not be reached if possible as this will undermine the whole risk mitigation strategy and put pressure on CISOs to justify their budgets. A sound risk mitigation strategy is rather the one that seeks to identify at which value of security investment the benefits for the business will be maximized while the impacts will be minimized. This value is the optimal value of investment in security measures and can be estimated by measuring the costs incurred because of security incidents as well as the investment in security measures. By assuming that such cost measurement metrics have been adopted by the organization, it would be possible to determine if an increase of budget in mitigating the risks correlates with a reduced number of security incidents and reduced overall impact caused by these security incidents. In Part IV of this guide we provide guidance to CISO for establishing "Metrics for Managing Risks & Application Security Investments". In absence of such metrics to determine the optimal value of application security investments, CISOs can look at some research studies that point to the optimal investment when the cost of security measures is approximately 37% of the estimated losses. For our example, assuming the total estimated losses of $ 6,026,000/year due to data loss incidents, the optimal expense for security measures, using this empirical value from the study, is $ 2,229,620/year.

At the point (A) in the figure below, the costs due to software security failures exceed of several order of magnitude the expenditure in countermeasures and the assurance on the security of the software is very low, on the contrary in (B) the costs of security measures outweigh the costs due to the software failures, the software can be considered very secure but too much money is spent for software security assurance. In point (C) the cost of losses is nearly two times larger costs of security measures while in point (D) the costs due to incidents is equal to the cost of the security measures. The optimal value for spending of security measures is the one that minimizes both the cost of incidents and security measures and maximizes the benefit or the security of the software.

Figure 3 CHART INDICATING HOW THE COST OF INVESTMENT IN SOFTWARE SECURITY MEASURES AGAINST FAILURE COSTS DUE TO INCIDENTS THAT EXPLOIT SOFTWARE VULNERABILITIES.



Analyzing security measures as investments

For most organizations today's application security is not seen as an investment but as a cost imposed by necessity to comply with standards and regulations. Some organizations might justify spending on application security because of risk management requirements, others because of increased awareness of the exposure to threats from cyber criminals, fraudsters and hacktivists. Some organizations might consider the cost saving that investment in security provides as shorter "time to market" as they will release a security product earlier than the competition. Some organizations might realize that spending in security for web applications might increase the level of trustworthiness that customers have in the web applications they are accustomed to use and help retain these customer business as well as sell them more services: these organizations might see spending on application security in a positive light as an investment and not as a cost. For organizations that consider security as investment and not as a cost, it is important to determine the most efficient way to spend the application security budget from the perspective of this being an investment. If the CISO considers application security spending as an investment rather than an expense, for example, the budget can be justifiable as additional savings the company gets because of less money spent on dealing with security incidents.

An example of this "money saving thinking" could be "if I spend a total of $$ in security measures to prevent security incidents in the next two years I will save a total of $$ in possible losses, fixing vulnerabilities and other direct and indirect costs caused by an estimated number of security incidents in the next two years". One of the methods to calculate the savings in terms of investment in security is the Return on Security Investment (ROSI). The use of ROSI can help CISOs to determine if the investment in countermeasures to thwart specific cyber-attacks is justifiable as a long term security investment: if the ROSI is not positive, the investment is not justifiable while if it is null, it does not yield any savings or investment returns.

There are several empirical formulas to calculate ROSI; one is to factor the savings for the data losses avoided over the total cost of the security controls/measures. Assuming the Total Cost of Ownership (TCO) for the cost of security control/measure is $ 2,229,620 (previously calculated as optimal value of expense in security controls for SQL injection mitigation per year) that includes development costs and acquisition of the new technologies, processes, tools as well as operating and maintenance costs, it is possible to calculate the savings in security incident costs. The ROSI can be calculated using the following empirical formula:

ROSI = [(ALE x % of control effectiveness) - cost of controls]/cost of controls

With this ROSI formula, assuming a pre calculated ALE (Annual Loss Expectancy) for security incidents caused by exploit of SQL injection vulnerabilities is $ 6,026,000 and that the effectiveness of the risk control mitigation is 75% (e.g. assume for example, in the case of a SQL injection, risk mitigation as defence in depth such as different layers of controls that include use of prepared statements/stored procedures in source code as well as filtering of malicious characters at the web server and application server), the cost of security controls is $ 2,229,620, the ROSI to the company is 102% per year. With this value of return of security investment, the spending in security control measures is worth it and will make the company save money each year. The best use of ROSI is to compare alternative investments in security measures such as to decide whether to invest in the development of a new countermeasure or extending the capabilities of an existing one.

As a comparative measurement for example, ROSI can be used by CISOs to determine which application security process is more efficient or yields the organization the higher savings and returns on the investment during the life-span of a Software Development Life-Cycle (SDLC). According to research of Soo Hoo (IBM) of the ROSI of the various security activities in the SDLC, the maximum return of investment (21%) (e.g. a savings of $ 210,000 on an investment of a $ 1 Million in Secure Software Development Lifecycle (S-SDLC) program) is when most of the money is invested in activities that can identify and allow to remediate security defects during the design phase of the SDLC such as architectural risk analysis and application threat modeling. The return of investment is lower (at 15%) when the defects are identified and remedied during the implementation (code) phase of the SDLC such as with source code analysis and even lower (at 12%) when these are identified and remedied during the testing-validation phase of the SDLC such as with ethical hacking/pen tests. By using the ROSI as comparative metrics for investments for SSDLC activities, the most cost effective investment in application security is therefore in activities that can identify defects as early as possible, such as requirements and design phase of the SDLC. In essence, the more CISOs think about investing in application security programs and especially security requirement engineering activities such as threat modeling/architectural risk analysis activities and secure code reviews the more they'll save on the costs of implementing and fixing security issues with other activities such as penetration testing.

Conclusion

Finally, it is important to notice that the cost estimates using the risk and cost empirical formulas dealt in this guide are as good as the reliability of data values that are used. The more accurate are these data values the more accurate are the cost estimates. Nevertheless, when these risk-cost criteria are used consistently and based upon tested quantitative risk calculations and reliable data can be used by CISO for objective risk and cost considerations to decide if the investment in application security measures is financially justifiable. These risk and cost considerations can also be used by CISOs to either defend their budgets in light of cost cutting measures or ask for more budget. Today an increased budget in application security can be justified in light of the increased exposure of web applications to the risk and monetary losses caused by security incidents. Since investment in application security has to be justified in business terms, these risk-cost criteria can be used for business cases as well as to decide how much to spend and where to spend in application security measures.

Part II : Criteria for Managing Application Security Risks

II-1 Executive Summary

CISOs must prioritize security issues in order to identify areas needing attention first. To make informed decisions on how to manage application security risks, CISOs often need to assess the costs of fixing known vulnerabilities and adoption of new countermeasures and to consider the risk mitigation benefits of doing so. Costs vs. benefits trade offs are critical to decide on which application security measures and security controls to invest in to reduce the level of risk. Often CISOs need to explain to executive management the risks to applications and to articulate the potential business impacts for the organization in case applications are attacked and confidential data is breached. Security risks are business risks only when all three risk characteristics exist:

- Viable threat
- Vulnerability that may be exposed
- Asset of value

To systematically prioritize technical risks for remediation, CISOs should consider a risk scoring methodology known as the Common Vulnerability Scoring System Version 2.0 (CVSSv2). To help regularly communicate application risk to the business executives, CISOs may consider providing "emerging cyber-threat awareness" reports to executive management.

Communicating to business executives

CISOs need to be real about cyber-threat risks and present to the business the overall picture of information security risks, not just compliance and vulnerabilities but also security incidents and threat intelligence of threat agents targeting the organization information assets including for applications. The ability to communicate risks to the business empowers CISOs to articulate the business case for application security and justify additional spending in application security measures. This justification needs to consider the economical impact of security incidents compared with the costs of unlawful non compliance. Today's costs to the business due to the economical impacts of security incidents are much higher than the costs of non-compliance and failing audits. Often the severity of the impact of security incidents might cost CISOs their jobs and the company losing reputation and revenues.

Threat modeling

A top-down approach to identifying threats and countermeasures, CISOs should consider a threat modeling technique also described in Part III. The threat modeling technique allows the target application to be decomposed to reveal its attack surface and subsequently its relevant threats, associated countermeasures, and finally, its security control gaps and design flaws.

Handling new technology risks

New application technologies and platforms such as mobile applications, Web 2.0, and cloud computing services offer different threats and countermeasure techniques. Changes to applications are also a source of potential risks especially when new or different technologies are integrated within applications. As applications evolve by offering new services to citizens, clients, customers and employees, it is also necessary to plan for mitigation of new vulnerabilities introduced by the

adoption and implementation of new technologies such as mobile devices, web 2.0 and new services such as cloud computing. Adopting a risk framework to evaluate the risks introduced by new technologies is essential to determine which countermeasures to adopt to mitigate these new risks. This guide will provide guidance for CISOs on how to mitigate risks of new threats against applications as well as of vulnerabilities that might be introduced by the implementation of new technologies.

- Mobile applications
    - Example concerns: lost or stolen devices, malware, multi-communication channel exposure, weak authentication
    - Example CISO actions: Meeting mobile security standards, tailoring security audits to assess mobile application vulnerabilities, secure provisioning, and application data on personal devices.
- Web 2.0
    - Example concerns: securing social media, content management, security of third party technologies and services
    - Example CISO actions: security API, CAPTCHA, unique security tokens in form posts, and transaction approval workflows.
- Cloud computing services
    - Example concerns: multi-tenant deployments, security of cloud computing deployments, third party risk, data breaches, denial of service malicious insiders
    - Example CISO actions: cloud computing security assessment, compliance-audit assessment on cloud computing providers, due diligence, encryption in transit and at rest, and monitoring.

Today's threat agents seek financial gain such as by attacking applications to compromise users' sensitive data and company's proprietary information for financial gain, fraud as well as for competitive advantage (e.g. through cyber espionage). To mitigate the risks posed by these threat agents, it is necessary to determine the risk exposure and factor the probability and the impact of these threats as well as to identify the type of application vulnerabilities that can be exploited by these threat agents. The exploit of some of these application vulnerabilities might severely and negatively impact the organization and jeopardize the business.

II-2 Introduction

Once an application has been targeted by an attack and the organization has suffered either a data breach incident or fraud as result of it, it is important to understand the root causes (e.g. vulnerabilities, control gaps) of the incident and to invest in security measures that will prevent such incident from occurring again. In this section of the guide, we address how to target spending to mitigate the risk posed by specific attacks and vulnerability exploits that caused data breach incidents. As best practice, we are not advocating to fix only vulnerabilities that might have been the cause of the incident even if these are the ones that need to be prioritized first for remediation to limit further damage. Vulnerabilities that might have been already exploited to attack the application certainly represent the highest probability to be also exploited in future targeted attacks.

The main question for the CISO is also to whether the same vulnerabilities can be used in attacks in the future against applications that have a similar functionality and type of data. Nevertheless, the application might have other types of vulnerabilities that might be opportunistically exploited by an attacker. These are vulnerabilities that either enable or facilitate an attacker to conduct the attacks against applications. The main point is that since the risk of data breaches and online fraud are a factor of likelihood and impact of vulnerabilities, it is important to consider likelihood and impact as factors to determine which issues to target for spending. In general, vulnerabilities are prioritized based upon technical risks not business impact, for example, vulnerabilities that yield high technical risks are prioritized for remediation over low risk ones. A vulnerability of high technical risk can be SQL injection, for example, independently from the data asset and the value that such asset has for the organization. Clearly if that SQL injection vulnerability is affecting either authentication or confidential data it might represent a very different risk to the organization than a SQL injection vulnerability that might affect data that is considered of low risk for the organization such as marketing research data, for example. The impact might be more of reputation risk in this case rather than data breach risk.

In part I of this guide we provide business cases that CISOs can use to request budget for application security. Application security budget typically need to cover several information security and risk governance needs. Besides the usual need to spend for compliance with information security standards, policies and regulations, CISOs might advocate additional budget to address mitigation of increased risks of data breach incidents. One critical factor is to quantify the impact of the data breach incident that already occurred. This implies that the CISOs are authorized to access data in relation to data breach incidents such as incident reports filed by the Security Incident Response Teams (SIRT), data from legal in relation to law suits and regulatory fines and fraud data that includes amount of money losses incurred because of online fraud. All this type of information is essential to determine the overall impact. In absence of this data, the best the CISO can do is to use data breach incident data from public sources and data breach incident reports. In part I of this guide, we provided some examples of how this data can be used to estimate impact. We documented what are the critical factors to estimate impacts of data breaches: these as the value of the data assets (e.g. citizen, client, employee or customer confidential and personal identifiable information, credit cards and bank account data) and the liability for the organization in case these assets are lost. Once the potential business impact of a data breach is estimated, the next step is to determine how much should be spent to mitigate the risk. At high level, this is a risk strategy decision that depends on the organization risk culture and the organization priorities for mitigating risks.

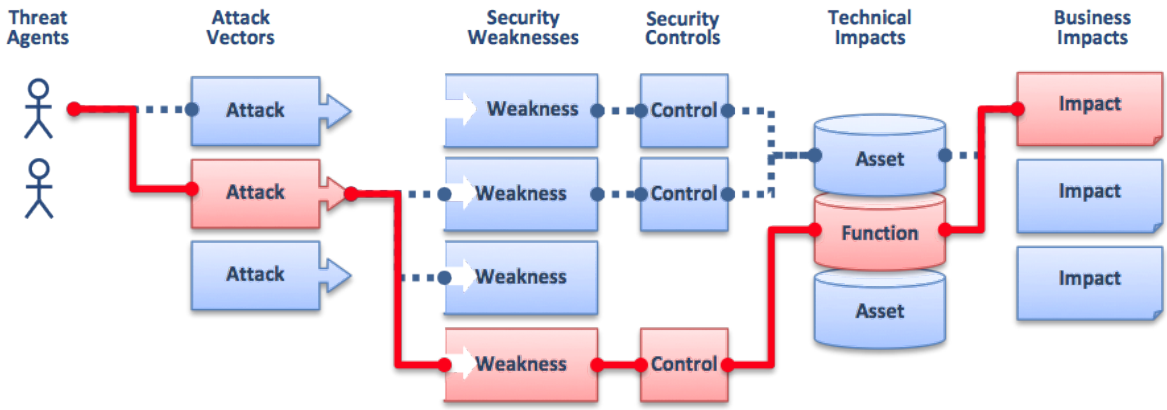
Depending on the type of organization, the number one priority can be "to not to be caught in unlawful non-compliance" such as in case of suffering a data breach and additionally failing to comply with compliance with PCI-DSS standards. This can be the case of a small company that provides online payment processing services and who could lose business from credit card issuers and additional fines, law suits and audit and legal costs. For an organization such as an engineering or research organization whose patents and trading secrets are critical assets, the protection from internal threats of commercial or country sponsored spying might represent number one priority. In general, it is important to address application security as a business

enabler for protecting digital assets whose value is represented in terms of costs of security measures vs. benefits in protecting the digital assets. In part I of the guide we present one criteria that can be used as the one that optimizes spending by maximizing risk mitigation value while minimizing the security costs. Another criteria, is to consider security not as a tax but as an investment, this criteria is the Return of Investment in Security (ROSI). The ROSI can be used for making both tactical and strategic risk mitigation decisions. Tactically, ROSI can be used to decide which security measures should be targeted for spending by considering the cost vs the effective of the measure in mitigating the impact of the data loss. Strategically, ROSI can be used to decide which application security activities to invest in the SDLC such as the ones that will bring money savings in the long term.

II-3 Defining Risk

Before we discuss how to manage application security risks, we need to use a consistent terminology. According to the OWASP Top Ten Risks to Web Applications, the characterization of risk of vulnerability is as such "Attackers can potentially use many different paths through your application to do harm to your business or organization. Each of these paths represents a risk that may, or may not, be serious enough to warrant attention."

Figure 4 DIAGRAM INDICATING HOW ATTACKERS CAN TAKE DIFFERENT PATHWAYS THROUGH AN APPLICATION TO DO HARM (OWASP TOP TEN WEB APPLICATION RISKS 2013)



This section will discuss:

- Prioritizing Overall Risk
- Understanding Risk Drivers
  - Threat Agents
  - Attacks, Weaknesses (Vulnerabilities), and Controls (Countermeasures)

II-4 Prioritizing Overall Risk

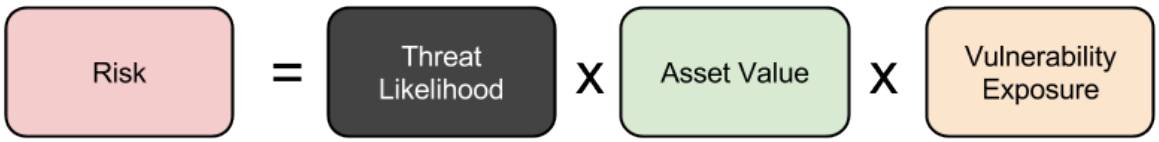
Prioritizing risks from known vulnerabilities is a reactive but tangible approach to managing clear business risk. These risk characteristics are useful to CISOs for determining the risks to the business of a threat agent exploiting either vulnerabilities or control weaknesses and gaps to compromise an asset and cause a negative impact to the business. To note that the value of the asset has nothing to do with the asset's cost of financial value is the relative value that the organization places into the asset in the case this asset is either lost or compromised.

Business risk occurs when there is a likelihood (probability) of a threat to the system, a vulnerability, and an asset of value.

Business risk from security issues is driven by:

- Threat Likelihood (TL) - probability of the occurrence of the threat
- Vulnerability Exposure (VE) - probability of the exposure of the vulnerability to the threat
- Asset Value (AV) - business impact

Figure 5 THE CALCULATION OF BUSINESS RISK



CISOs should use a consistent approach to characterizing technical risks to known vulnerabilities. This can be accomplished using a risk scoring methodology such as the Common Vulnerability Scoring System Version 2.0 (CVSSv2). There are many in use today, CVSSv2 is one such methodology. When using a risk scoring methodology, it is critical to not only score a vulnerability based on likelihood and business impact, but also its context within your organization. This allows CISOs to prioritize risks to drive application security investment. OWASP is the primary source to provide organizations with the top ten web application risks that need to be mitigated. The testing of OWASP Top 10 might require organizations to routinely perform security testing of these vulnerabilities in web applications. Once the vulnerabilities are identified and the severity assigned to these, it is important to have a vulnerability management process that allows managers to prioritise the fixes of these vulnerabilities by risk severity but also by the business impacts they might cause in the case these will be exploited by an attacker. However, vulnerabilities are just one aspect of risk mitigation for application security risks.

About CVSSv2: A Methodology to Prioritize Risk

Online Calculator - http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2

CVSSv2 guide - http://www.first.org/cvss/cvss-guide.html

This risk scoring system utilizes multiple data points to assess risk:

- **Base Metrics**
  - **Access Vector (AV)**
  - **Access Complexity (AC)**
  - **Authentication (Au)**
  - **Confidentiality Impact (C)**
  - **Integrity Impact (I)**
  - **Availability Impact (A)**
- **Temporal Metrics**
  - **Exploitability (E)**
  - **Remediation Level (RL)**
  - **Report Confidence (RC)**
- **Environmental Metrics**
  - **Collateral Damage Potential (CDP)**
  - **Target Distribution (TD)**
  - **Security Requirements (CR, IR, AR)**

II-5 Understanding Risk Drivers: Threats and Countermeasures

CISOs should adopt a threat modeling technique to drive risk scoring. Per OWASP's Application Threat Modeling (https://www.owasp.org/index.php/Application_Threat_Modeling), "threat modeling is an approach for analyzing the security of an application. It is a structured approach that enables you to identify, quantify, and address the security risks associated with an application."

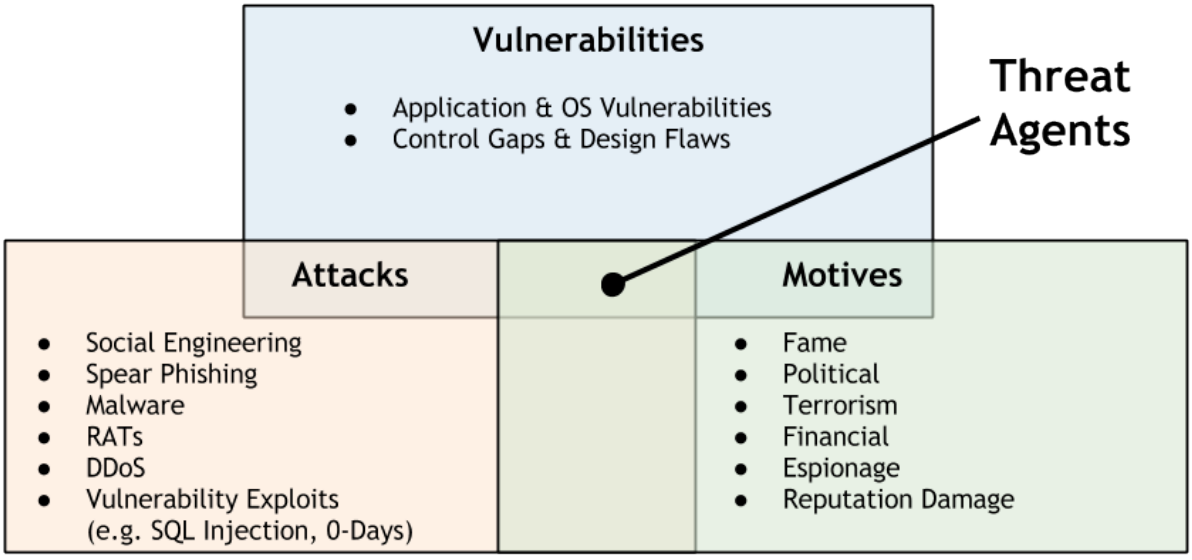
About threat agents

A threat agent (https://www.owasp.org/index.php/Category:Threat_Agent) "is used to indicate an individual or group that can manifest a threat. It is fundamental to identify who would want to exploit the assets of a company, and how they might use them against the company." A threat agent can be defined as the function of his capabilities, intentions and past activities:

Threat Agent = Capabilities + Intentions + Past Activities

A threat agent can be characterized as the intersection between the agent's motives, the specific type of attacks used and the vulnerabilities that are exploited.

Figure 6 THREAT AGENTS



The growing maturity of threat agents

By identifying the threat agent intentions and the capabilities such as the types of attacks used against applications and the vulnerabilities that are exploited, CISOs can assess likelihood and business impact. As cyber threats evolve, it is important to understand what these threat agents are, their intentions and the past activities (e.g. the type of attacks used by them). By analyzing how threats evolve, CISO can adapt application security measures to mitigate the risks of these threats.

In the past decade, threat agents have radically changed and matured. Historically, threat agents began as an opportunistic venture -- targeting anyone with a vulnerability, regardless of asset value. Today's threats are targeted, usually known as the Advanced Persistent Threat.

- Script kiddies, worms and virus authors
- Fraudsters & cyber-criminals
- Hacktivists
- Cyber-spies
- Advanced persistent threat (APT) agents

Script kiddies, worms and virus authors

Between the years 2000 and 2005, the main threats agents could be characterized as the so called "script kiddies" seeking to gain notoriety by hacking into government systems using easy-to-find techniques and scripts to search for and exploit weaknesses in other computers as worm and virus authors seeking to spread them for causing notable major computer disruptions and get famous as a result. Historically, the primary targets of these threat agents weren't websites but computer hosts for the sake of getting notoriety by infecting them with viruses and worms. Notable script kiddie of the late 90s includes Jonathan James, known as "cOmrade" on the Net, that pleaded guilty to intercepting 3,300 emails, stealing passwords, and nicking data by using network sniffers installed by compromising servers of US Dept of Defense with backdoors. In the year 2000, Jeanson James Ancheta created a worm that allowed him to infect as many computers on the Internet as he could with off-the-shelf Remote Access Trojans (RATs). Over time, he amassed about 40,000 worm-infected remote access computers (also known as bots). In the same year 2000, Onel Deguzman authored the ILOVEYOU virus that spread by emails to 10 million hosts worldwide costing companies an estimated $ 5.5 billion dollars for cleaning it. In the year 2000, a 15 year script kiddie, Michael Calce known as "mafia boy" takes down eBay, Amazon and CNN websites for 90 minutes by accidental use of a file sharing tool. Notable worm author of the year 2004 is Sven Jascham author of the Sasser worm that is estimated to have impacted 10 million hosts. The impact of the Sasser worm included disabling hosts for satellite communications, disabling hosts for operation of air lines trans-Atlantic flights and disabling hosts for financial organizations and hospitals. Today CISOs need to be on the threat alert for today's script kiddies threat agents using readily available tools that look for common exploits of known vulnerabilities to expose them to the public. CISOs need to make sure that systems and applications are not vulnerable to these easy exploits since this might severely impact the organization operations when critical hosts are infected and disabled as well as damage the company reputation when news of these exploits are posted on social media (e.g Twitter).

Fraudsters & cyber-criminals

In the years between 2005 and 2010, the motives of the threat agents shifted from hacking for fame and notoriety to hacking for financial gain. During this period, the targets of the attacks also shifted from hosts to websites and the motives for the attacks changed from causing disruption using viruses and worms to stealing confidential and sensitive data such as personal data for identity theft and credit and debit card data for credit card fraud. In the year 2007 for example, Albert Gonzales and other three conspirators succeeded in stealing 130 million credit card numbers from Heartland Payment Systems, a New Jersey card payment processor; 7-Eleven, the Texas-based convenience store chain; and Hannaford Brothers, a Maine-based supermarket chain. The attackers used SQL Injection attacks that resulted in the placement of malware to sniff the network for credit card data used at retail stores. They later engaged in ATM fraud by encoding the data on the magnetic stripes of blank cards and withdrawing tens of thousands of dollars at a time from ATMs.

- In 2010, a cyber-criminal gang of 37 Russian hackers succeeded in stealing $ 3 million from online bank accounts by infecting online bank users PCs with the ZEUS banking Trojan. The ZEUS Trojan is specifically designed to steal banking information by using man in the browser, key logging and

attacking online banking applications by hijacking the session and by taking over the victim bank accounts.

- In 2012, banking malware became more sophisticated when malware named "GameOver" was designed to steal user's online banking credentials by defeating common methods of multi factor authentication employed by financial institutions as well as to perform wire transfers using the victims' credentials without requiring any interaction from the victim during the attack. For CISOs at financial institutions, understanding how these threat agents and malware attacks seek to compromise user's online credentials and bypass multi factor authentication is critical in determining which countermeasures can be deployed to protect the financial institutions from these attacks. Often CISOs at financial organizations subscribe to "threat intelligence services" so that they are notified when customer's online credentials and bank and credit card data have been recovered from Zeus Command and Control and "dropping" servers. Typically these alerts are the outcome of ZEUS malware hosted botnets being taken down by law enforcement. Based upon this information, CISO can inform the businesses to take actions to limit the impact, such as notifying the customers and suspending and replacing credit and bank accounts.

Hacktivists

In the years between 2010 and 2012, a new class of threat agents emerged that seek to attack government and corporate websites for political motives. These are computer hacker groups, such as Lulzec and Anonymous. In 2011, Lulzec claimed responsibility for compromising user accounts and credit card data users of the Sony's PlayStation Network while Anonymous claimed responsibility for defacing the site of the company HBGary federal and publishing several thousand of client's emails. These threat agents are commonly referred to as "hacktivists" and seek to attack websites not for financial gain but for exposing corporate and government owned information to the public. It is important for CISOs to notice, that according to the 2012's Verizon Data Breach Investigation Report (released on March, 22nd 2012), even if hacktivists caused a small percentage of incidents (3%) hence affecting a low probability, overall, they account for the largest impact in terms of volume of data records compromised (58%). According to the Verizon's report, hacktivists are more likely to attack large organizations rather than small ones since these provide them with the most return of investment (i.e. from the attacker's perspective) in terms of data that can be compromised and disclosed to public. CISOs in large private and public (e.g. Government) organizations that have a known public brand should consider the risk of confidential data (e.g. names, last names and emails) and confidential personal identifiable data (e.g. names, last names and card numbers) as high risk. CISOs responsible for the security of both government and corporate hosted and managed websites that store customer's confidential and personal identifiable information, might likely become the target of hacktivists for political reasons and need to worry about reputation damage impacts also resulting from public disclosure of website vulnerabilities. Hacktivists often engage in attacking the organization's employees and customers with spear phishing and their websites with SQL injection, Cross Site Scripting and web service vulnerability exploits for the sake to steal and post the compromised information online. Another type of attack that CISOs managing government and corporate websites need to worry about are disruptions due to Distributed Denial of Service (DDoS) attacks. Typically, Hacktivists target websites with DDoS hosted at financial and government organizations for political reasons. For example, several credit card sites such as Mastercard.com and Visa.com were attacked in 2011 by Anonymous with DDoS in retaliation of removing WikiLeaks operators among the VISA's and MasterCard's clients.

Cyber-spies

Since the years 2011 and 2012, besides hacktivists, fraudsters and cyber-criminals, another class of new threat agents that some of the CISO of international organizations, governments, financial, defense and high tech engineering type of companies need to deal with are cyber-spies seeking to compromise websites for stealing top secrets, financial restricted and intellectual property type of information such as company's trading secrets. These type of attacks often involve the use of Remote Access Tools (RATs) as publicly revealed by McAfee in the operation Shady RAT report. In this 2011 study, it is reported that these type of attacks went

on for several years starting in mid-2006, impacting "at least 72 organizations, including defense contractors, businesses worldwide, the United Nations and the International Olympic Committee". These type of cyber espionage attacks involved the use "spear-phishing email containing an exploits sent to an individual with the right level of access at the company, and the exploit, when opened, in an unpatched system, will trigger a download of the implant malware". Spyware malware typically execute and initiate a backdoor communication channel to the C&C web server and interpret the instructions encoded in the hidden comments embedded in the webpage code." Besides spear-phishing, cyber espionage tools can spread also by compromising web servers via SQL injection (http://www.mcafee.com/uk/about/night-dragon.aspx), infected USBs, and infected hardware or software. The analysis of some of the most recently used cyber-spying malware seems to indicate that these are developed by countries engaged in cyber espionage. In 2012 for example, Kaspersky labs identified a cyber-spying malware such as "Gauss" that bear code similarities with other cyber-espionage tools such as Flame and cyber-war tools like Stuxnet. According to Kaspersky, Gauss is "designed to steal sensitive data, with a specific focus on browser passwords, online banking account credentials, cookies, and specific configurations of infected machines.

Advanced persistent threat (APT) agents

Often cyber-espionage activities are associated with APTs (Advanced Persistent Threats). APTs are characterized by advanced that is use sophisticated methods, such as zero-day exploits and persistent that is, the attackers return to target systems over and over again with a long term objective of achieving his goals without detection. Historical APTs include operation Aurora targeting Google, Juniper, Rackspace and Adobe companies as well as operation Nitro, Lurid, Night Dragon, Stuxnet and DuQu. CISOs of government organizations as well as corporations whose protection of intellectual property and confidential and restricted information constitute a primary concern, need to be aware they might become the target of APTs seeking to target employees and customers with spear phishing to infect PCs with spyware, as well as to exploit system and web application vulnerabilities like SQL injection for installation and dissemination of cyber espionage tools.

About attacks and vulnerabilities

In this section of the guide we will describe how to proactively manage the risks posed by specific types of attacks, such as threat agents whose motives and attack goals have been previously analyzed. Typically, risk mitigation consists of fixing vulnerabilities as well as applying new countermeasures. The choice of which vulnerabilities are critical to mitigate starts first with the understanding of the threat scenarios and the threat agents motives, especially of hacking and malware and how these threat agents might adversely target applications leading to compromise of the data assets as well as of critical business functions. One critical tool that CISOs can use to prioritize risk is the use of risk frameworks that factor the threat agents, the technical risks posed by application vulnerabilities that the threat agent seeks to exploit and the business impacts. The risk profile of each application is different depending on the inherent values of the asset whose business impact depends upon and the likelihood as the application might be targeted by a threat agent. After vulnerabilities are prioritized for remediation, it is important to consider the effectiveness of existing countermeasures and identify any gaps in risk mitigation measures that require the CISO to consider new countermeasures. The control gap analysis can be used to determine which countermeasures need to be implemented based upon security principles. The principle of defense in depth can be used to identify gaps and these gaps can be filled by applying countermeasures. To decide on which countermeasures to invest, CISOs should consider both the costs and the effectiveness of new countermeasures in mitigating the risks. To decide how much should be spent in countermeasures, the calculation of potential financial losses as factor of likelihood and impact to determine the financial liability can also be used as criteria.

Script kiddies attacks

In the case of script kiddies, the attacks that CISO need to be prepared to defend from are the ones seeking to run scripts and off the shelf vulnerability scanning tools for the sake of identifying application

vulnerabilities. Among the script kiddies goals are to probe websites for common vulnerabilities and when these are identified, they often seek to disclose them to the public for fame and notoriety.

Since script kiddies often seek to identify vulnerabilities and not necessarily to exploit them for data compromise, the impact for the business is often reputation damage. Assuming that this vulnerability discovery is limited to running vulnerability scanning tools, the main vulnerabilities that CISOs need to worry about are the ones that are most common, more precisely, the ones that OWASP Top 10 characterizes as 'widespread" and "easy to detect" such as cross site scripting (OWASP A2 XSS), Cross Site Request Forgery (OWASP A5-CSRF) and security misconfigurations (OWASP A6-Config.). Other these vulnerabilities are disclosed to the public without contacting the organization whose web application has been identified to be vulnerable. When these are disclosed to public, they might obviously also increase the risk to the organization since these might be exploited to compromise the website as well as the data. It is therefore important that CISOs pay close attention to script kiddies threat and remediate this type of vulnerabilities. In some cases, these vulnerabilities are published in a public accessible database after the owners of the vulnerability have been contacted and offered help to remediate. For example xssed.org collects and validates information about XSS vulnerabilities and publicly tracks them for remediation as well as offers a service to notify organizations when these vulnerabilities are released to public.

CISOs cannot assume that reputation damage is just restricted to the organization's vulnerabilities being released to the public since vulnerabilities can be occasionally exploited for defacing the website and publishing unauthorized content. Examples of vulnerabilities that can be exploited for defacing includes exploit of file injection vulnerabilities such as Cross Frame Scripting (XFS), that is part of (OWASP A1:Injection) group. For mitigating the risk of these vulnerabilities, CISOs need to invest in vulnerability scanning tools for testing them before the web application is released into the production environment. Additionally, the focus should be given to building secure software whose components and libraries such as the OWASP ESAPI (Enterprise Security API) "a free, open source, web application security control library that makes it easier for programmers to write lower-risk applications."

Besides investing in vulnerability testing and secure software to mitigate the risk of reputation type impacts, CISOs can also invest in attack monitoring and detection measures such as WAF (Web Application Firewalls). Since these types of vulnerabilities are easy to identify and widespread among web applications, they are also the ones that websites are most probed for, therefore knowing when a web application is a target of a script kiddie attack can be used for further monitor the activities and issue alerts in case the attacks are not limited to probing the website but to try to exploit the vulnerability of compromised data.

Fraudsters and cyber-criminals attacks

Fraudsters and cyber-criminals attack websites that represent an opportunity for them for financial gain. Examples are websites that process credit card payments such as e-commerce websites, websites that allow access to credit and debit card data as well as bank accounts and perform financial transactions and wire transfers, such as online banking websites and any website that stores and collects private information, such as Personal Identifiable Information of an individual. Besides committing fraud by attacking the financial transactions such as payments and money transfers that the websites supports, other types of attacks that are sought by fraudsters are the ones that are allowed unauthorized access to sensitive data, such as credit and debit card data that can be used for card non present financial transactions and to counterfeit cards, as well as personal identifiable information that can be used for impersonating the victim for identity theft.

By taking into consideration these attacker financial goals, any vulnerability that allows the fraudster/cyber-criminal to control payments and money transfers as well as to gain unauthorized access to sensitive data is very likely to be the target for an exploit. First and for most, these are vulnerabilities that can be exploited for gaining un-authorized access to e-commerce and financial type of applications. These include exploit of weak authentication and session management vulnerabilities (OWASP A3- Broken Authentication and Session

Management) since the exploit might allow for compromised credentials for accessing the web applications such as username and passwords as well as SessionIDs for impersonating the victim. Other likely vulnerability exploits might include the exploit of the Cross Site Request Forgery (OWASP-A5-CSRF) vulnerability to ride the session for performing un-authorized financial transactions such as payments and money transfers. Among the most damaging web application vulnerabilities that fraudsters and cyber-criminals might seek to exploit are SQL injection (OWASP- A1-Injection), access to sensitive data by manipulating unprotected parameters such as direct references (OWASP A4 Insecure direct object reference), exploit of failure of the web application to restrict URL access (OWSP A8-Failure to Restrict URL Access), poor or non-existent cryptographic controls to protect confidential data in storage (OWASP A7-Insecure Crypto Storage) and in transit (OWASP A9-Insufficient Transport layer protection. In the case the CISOs are responsible for managing risks of inherently risky websites such as e-commerce, online banking and sites that process confidential and personal information such as for insurance, loans, credit they need to focus on testing and fixing these vulnerabilities since these are the most likely to be exploited and cause the highest business impact.

Application layer intrusion detection rules (IDS) can also be embedded within the web application as OWASP ESAPI or in the web server such as a WAF (Web Application Firewall) can log and monitor suspicious activity and trigger alerts for potential fraud attempts.

Application threat analysis and modeling is the key activity for determining the exposure of applications to threats and to determine how to protect the data from the impact of these threats. From a threat analysis perspective, after threat agents and their motives and attacks are identified it is important to analyze the probable attack scenarios, identify the attack vectors used and the vulnerabilities that can be exploited. An attack tree can help to translate the attacker goals into the means to realize these goals. From the attacker perspective, the main goal is to pursue attacks that are easier and cheaper to conduct and have the highest probability to succeed rather than otherwise. For example, consider that credit card and account data can be purchased from cyber-criminal organizations on the black market and if it is easier, cheaper and less risky for a fraudster than to break into an application, this is probably what a fraudster will do. If the website that stores credit card data has open vulnerabilities that are easily exploitable to get credit card data, probably the fraudster will attack this website first instead. From a CISOs perspective, fixing of application vulnerabilities that can be exploited by a fraudster can be justified as reduced opportunity for exploiting them. Attack trees can also be useful to understand the realization of possible threats by following the same attack patterns used by a fraudster. This allows for the identification of any weaknesses and points of least resistance for an attacker to pursuit. For example, if applications are accessible through different data interfaces and channels, the fraudster will focus on the ones that offer the least resistance and greatest opportunity for compromised data, such as mobile instead of web channels. As one of the security principles is "you are only as secure as your weakest point", identifying where these weakest points are is critical in the assessment of the security of any system exposed to attacks, including applications. The identification of the data entry points for a given application, internal and external, is critical to determine the attack surface of the application and is usually identified as part of the application threat modeling assessment.

Another critical analysis that is part of application threat modeling is to analyze which threats can be realized by exploiting a certain class of vulnerabilities so that CISOs can focus on applying countermeasures for mitigating these vulnerabilities. An in depth analysis of threats impacting applications and software is best conducted by using threat trees and risk frameworks. These are formal methods that allow for mapping threats to vulnerabilities and countermeasures. OWASP has included guides for application threat modeling as well as reference to "threat trees" and "threat-countermeasures" frameworks that can be used for this threat analysis.

Business logic attacks

A class of vulnerabilities that are often exploited by fraudsters and not tested in applications are design flaws and logical vulnerabilities. One of the main reasons these are not tested is because automated vulnerability scanning tools do not understand the business logic of the application to be able to identify them. In absence of specific manual security tests that test for possible use and abuse cases of the application, for example, these type of vulnerabilities are most likely not identified and remediated and might cause serious financial losses and business impacts when are exploited. Examples of attacks that exploit these vulnerabilities are the so called "business logic attacks". Examples of business logic attacks that exploit design flaws in applications include bypassing role base access controls to gather unauthorized confidential data and to perform un-authorized financial transactions, attacking the logic of shopping carts to alter the price of an item before check out and alter the shipping address of a purchased item before credit card validations are completed during a check out. Typically, business logic attacks exploit input validation vulnerabilities such as in missing validation of parameters in business transactions (e.g. Role ID, RuleIDs, PriceIDs), weak enforcement of controls for transaction workflows, flaws in committing financial transactions before all checks are done and misconfigurations of Role Based Access Controls (RBAC) and business policy rules. Most of these vulnerabilities need to be tested manually based upon use and mis-use cases, a technique that is considered part of application threat modeling and also documented in OWASP Application Threat Modeling methodology.

Often design flaws are to be found in how application security controls are designed and require specific security testing to identify them. For example, this is the case of flaws in the design of password resets, use of guessable challenge questions in multi-factor authentication, session management flaws allowing sessions to not expire or not close, misconfiguration of authorizations and access controls. These design flaws usually fall under the class of common vulnerabilities such as OWASP A3 Broken Authentication and Session Management, OWASP A4 Insecure Direct Object Reference, OWASP A6 Security Mis-Configurations and OWASP A8 Failure To Restrict URL access and can be tested for specific manual tests. OWASP provides specific guidelines for security testing applications for vulnerabilities as well. A class of vulnerabilities also exploited for business logic attacks includes the insufficient anti-automation (WASC 21). This is a vulnerability that can be exploited by attackers to spam online registrations, posting of information using automation tools, but also for fraud such as to automatically enumerate and validate credit card data such as numbers and PINs using automated scripts that test the application error codes and success responses.

The most important criteria for CISOs to protect from business logic attacks is not to assume that the testing of design flaws and business logic flaws is covered under normal vulnerability scans and security tests. Design and business logic flaws is a class of vulnerabilities that requires to be tested by deriving specific security tests from use and abuse cases produced by security teams specifically engaged in threat modeling applications. CISOs should consider the investment in application threat modeling process specifically for identifying and testing this class of vulnerabilities when these are not identified and tested by other security processes.

Phishing attacks

Since often one of the attack techniques adopted by fraudsters and cyber-criminals is social engineering the victim to select malicious links serving malware, exploits of web application vulnerabilities that facilitate phishing the victim with malicious links might also be targeted. These attacks include using Cross Site Scripting (A2: XSS) vulnerabilities to run malicious scripts that can steal cookies and run keyloggers. Another web application vulnerability that can be used for tricking a victim to visit a malicious site and get infected with malware is OWASP A10: invalidated redirects and forwards. Additional vulnerabilities that facilitate malware installation through phishing include XFS exploits for click jacking attacks. These attacks trick a victim into performing undesired actions by clicking on a concealed malicious link. These are vulnerabilities that CISOs can prioritize for remediation since they facilitate the installation of malware on the victim's PC. Since the identification of these vulnerabilities often require manual security testing such as manual ethical hacking/penetration testing as well as manual source code review to identify these vulnerabilities in the

source code, it is critical for the CISO to invest in hiring and train pen testers as well as software developers with secure coding skills as well as secure code review processes, secure coding standards and static source code analysis tools.

"Man in the browser" and "man in the middle" attacks

Unfortunately, identifying and fixing these vulnerabilities is not a guarantee of immunity from attack of fraudsters but of a minimum level of software security assurance. Resilient software today requires the CISO to consider investment in countermeasures to protect web applications from another class of attacks such as Man in the Browser (MiTB) and Man in the Middle (MiTM). Through MiTB, fraudsters can collect confidential, authentication and credit/card data from the victim by injecting HTML fields in the browser outside the control of the web application. Additionally, the victim's logging credentials are collected through key loggers and sent to the fraudster's for impersonating the victim. In a money transfer session for example, the fraudster will connect to the victim's PC from his command and control server and hijack the session to transfer money to an account under the control of the attacker (e.g. money mule account). Through, MiTM, fraudsters will redirect the victim to a malicious site whose web traffic and data will be under the control of the attacker.

To protect e-commerce and financial web applications from MiTB and MiTM attacks, CISOs need to adopt a defense in depth approach that includes different layers of controls at the client-PC layer, at the web server and web application server layer as well as at the backend databases and services layers. At the client PC layer, investing in user's information and awareness on malware threats is very important. Simple measures such as keeping browsers and PCs up to date and patched as well as hardened with limited user's privileges and with a limited number of applications installed (e.g. ideally with no email and no Facebook installed on PC) can limit the chances of malware infections. Pointed security information embedded in the website login web pages can keep warning users about malware risks every time they login.

Additionally, CISOs can invest in providing anti-malware client software for free to their clients since this is more effective in detecting and protecting the PC than traditional anti-virus. Assuming the client PC/browser has been compromised with banking malware, additional countermeasures that CISO might consider includes adding additional identity validation controls for high risk transactions such as in the case of wire transfers and payments. These include positive pay, dual verification & authorizations, anomaly and fraud detection. Since the online channel is assumed compromised by the attacker, using out of band transaction validation/authentication for payments and financial transactions with two way notification confirmation via independent mobile/voice channels puts the citizen/client/customer/employee in control of the transaction and allows them to reject transactions that either cannot be confirmed or whose integrity of transaction parameters have been modified by the attacker and cannot be validated. Detection measures such as receiving out of band alerts for financial transactions as well as auditing and logging and monitoring of web traffic with WAF and SIEM and using behavioral fraud detection to detect abnormal transaction rates/parameters might also allow CISOs to receive reports on detected malware based transactional events and to recommend proactive actions to limit the impact of financial losses (e.g. suspend the accounts that are flagged as suspicious till further validation).

When deciding on which countermeasures to deploy for mitigating the risk of MiTB and MiTM attacks, CISOs might need to conduct trade-offs between the risk, the effectiveness of these countermeasures and the costs. The countermeasures that cost the least and mitigate MiTB and MiTM attacks the most can be prioritized for investment. Typically client based anti-malware software can be effective in mitigating the malware risks at the front door and it is rather inexpensive to acquire and deploy if this cost does not include the total cost of maintenance of the solution for a large user population. Security awareness campaigns for customers can be the least expensive measure but might not be that affective since often customers do not pay attention to security warnings. Acquiring and deploying out of band authentication and out of band transaction validation/authorization can be expensive, but it offers strong mitigation against man in the

middle attacks and can be a viable option to protect high risk transactions. Implementation of fraud detection systems for monitoring malicious traffic might be expensive to implement and maintain and need to be justified on the case by case basis. For example, if it is known that some web applications are constantly under attack from malware and impacted by fraud, investing in fraud detection systems might be justifiable due to the tested capability of fraud detection systems to detect attacks earlier than with other methods (e.g. looking at transaction logs that feed to SIEMs). CISOs can select which web applications should be put in scope for remediation of vulnerabilities sought by fraudsters and implementation of new countermeasures against MiTB and MiTM attacks based upon the risk profile of the application. The risk profile of the web application can be a function of the value of the data assets and the risk of the transactions that the web application provides to customers. A control gap analysis can be used to identify gaps in protective and detective controls and to determine the degree of risk mitigation that can be obtained when these are implemented. Once the security measures are adopted, a calculation of the residual risk highlights whether the risk can be accepted or needs to be reduced further by implementing additional controls.

Denial of service attacks

Denial of Service (DoS) attacks might severely impact the availability of website to users. Depending on the type of services that the website provide to customers, a loss of service might result in a considerable revenue loss for the organization. CISOs should consider the mitigation of the risk of denial of service attacks as top priority, especially for web applications that generate considerable revenue and whose availability is considered critical by the organization.

DoS attacks can be facilitated by web application vulnerabilities, OWASP included DoS as one of OWASP Top Ten vulnerabilities in 2004 (OWASP A9:DoS) but this was dropped in 2007 due to the MITRE ranking in 2006. Nevertheless, even if it is no longer part of the OWASP top ten in 2010, depending on the exposure and the value of the assets impacted, denial of service vulnerabilities might represent a high risk for the organization and prioritized for mitigation. At the application level, a denial of service might be the result of exploits of OWASP A1 injection vulnerabilities, specifically vulnerabilities allowing injections of SQL, XPATH and LDAP commands can cause the web application to crash. At the user level, denial of service attacks can target the usability of the application by a registered user, for example attackers can use scripts to lock user accounts upon guessing valid userIDs and force user accounts to lock upon several un-successful attempts. In absence of temporary account locks (e.g. the user account will unlock automatically in 24 hours), this attack cause users to not be able to log on. A side effect of this is customers calling customer support seeking to unlock their user accounts, possibly flooding the call centers with account unlock calls. At a source code level, DoS attacks might occur because of attack vectors exploiting insecure code issues causing exhaustion of computer resources. These are insecure coding issues such as failing to release memory from allocated resources (e.g. object's memory) when exiting programs and causing the application to crash as a result. Examples include exploiting of insecure code with NULL pointer deference and improper termination, exploiting uncaught exceptions and exploiting weaknesses when processing XML files causing the XML parsing process to exhaust memory with malicious recursive XML files. In the cases when the application source code is written in programming languages that allow programmers to manage memory such as C, C++, coding errors in the handling of memory allocations and use of unsafe functions might expose the source code and the application to possible exploit of buffer overflow vulnerabilities to cause the application to crash or to take control. Buffer overflow vulnerabilities can also be exploited at server level because of attacks seeking to exploit web and application servers that are unpatched and vulnerable to buffer overflows. CISOs need to make sure that application and source code vulnerabilities that could be exploited for denial of service are in the scope of security testing since these are typically covered by static and dynamic application security testing tools.

Distributed denial of service attacks

At the transport-network layer, denial of service typically seeks to exploit network layer protocol type vulnerabilities such as by spoofing packets for the sake of flooding network traffic. A type of denial of service

attack called Distributed Denial of Service (DDoS) typically seeks to flood the target web server with an unusually high level of data traffic sent from a coordinated and controlled network of bots. Because of the unusual network traffic that the web server is asked to handle, it might not be able to serve all the requests over the network and deny the requests of service to the users of the application. At the most outer layer that is the edge of the internet it is possible to filter the malicious traffic before it attacks the internal layer that is the data center where the application is hosted and other countermeasures are implemented. As the DDoS attacks take place, defense in depth allows the organization to be alerted and prepare new filtering blocking rules for malicious traffic. But applying the principle of defense in depth, even if it can slow down attackers, it is not enough and other defensive security principles need to be followed when deploying countermeasures as well. Such as to consider control of security of the weakest point, consider the simplicity and openness of the security mechanism so it can be managed and vetted securely, apply security as the lowest privilege for users' access are all essential for the security of the design of security controls of applications and software.

Well known DDoS attacks originating from bots include “Ping of Death” bots that create huge electronic packets and send them to victims, “Mailbomb” bots that send a massive amount of e-mails, crashing e-mail server, Smurf Attack” bots that send Internet Control Message Protocol (ICMP) messages to reflectors to amplificy the attack, and “Teardrop” bots that send malformed pieces of packets that crash a system trying to recombine them.

Today's script kiddies, hacktivists, cyber-criminals and country sponsored attackers use open source DDoS attack tools and bots against possible targets. The typical, likely targets for DDoS attacks are public and private organizations with high visibility. General objectives of these attacks are to cause disruptions, get noticed and damage the company reputation. Specific motives for conducting DDoS attacks varies depending on the type of threat agents and their motives. Script kiddies might use DDoS attacks for opportunistic motives such as to exploit denial of service vulnerabilities and gain notoriety, hacktivists might use DDoS attacks for political reasons and to get attention from public media. Fraudsters and cyber-criminals might use DDoS attacks to derail attention from other attacks such as in the case of an account take over attack seeking to defraud online bank customers. State sponsored cyber-attackers might use DDoS attacks for economic and military reasons such as in the case of disrupting the operation of another country’s government operated website.

The impact of DDoS attacks in terms of reputation and revenue loss to private and public organizations varies greatly depending on the type of website targeted by the attack, the duration of the attack and the number of individuals and customers affected. The business impact of DDoS attacks can be estimated as a function of the loss of revenue caused by the loss of services to customers and individuals when the website is taken down. According to the "2011 Second Annual Cost of Cyber Crime Study Benchmark Study By Ponemon Institute" that involved 50 organizations and U.S. companies, the impact of DDoS is estimated to be an average annual cost of $187,506. This cost is weighted by the frequency of the attack incidents for all benchmarked companies. Another survey from CA Technologies including 200 companies in North America as well as Europe, estimated the cost of downtime because of a denial of service of about $150,000 annually. These cost estimates, are just order of magnitudes since business impacts vary greatly depending on the type of online services affected and the volume of the online business affected by the DDoS attacks. For a very large e-business company like Amazon for example, whose business generated $ 48 billion in revenues for the year 2011, assuming that most of Amazon's revenues are generated online, a denial of service of just one hour DDoS attack might cost several millions of dollars in revenue loss. CISOs whose companies generate a significant part of their revenues through online websites such as in the case of e-commerce and financial websites, need to consider the threat of denial of service from DDoS attacks as top priority for risk mitigation and consider investing in security measures to mitigate the risk of such attacks.

Today DDoS attacks are very widespread. The reason why such attacks are so widespread is due to the availability of DDoS tools and of botnets rented to conduct DDoS attacks at a relatively low cost for the attacker. According to “Modeling the Economic Incentives of DDoS Attacks: Femtocell Case Study, Vicente

Segura and Javier Lahuer ta, Department of Network and Services Security of Telefonica" for example, the cost of renting a botnet for DDoS attacks is about $ 100 per day for 1 Gbps bandwidth.

CISOs also need to be aware of the escalating DDoS threat since the severity and sophistication of DDoS attacks are also increasing. According to "2011 Arbor Networks, Sixth Annual Worldwide Infrastructure Security Report", considering with DDoS of six years ago, the power of DDoS attacks increased ten times reaching bandwidths of 100 Gbps. This escalation of DDoS power cannot be explained by the sophistication of the DDoS tools alone but with new DDoS attack techniques seeking to amplify the bandwidth of the attacks. These new DDoS attack techniques consist of Distributed Reflector Denial of Service Attacks (DRDoS). DRDoS attacks spoof the victim's source IP address with DNS queries sent towards open DNS resolvers, since open DNS resolvers that receive the DNS queries respond to the victim's system with large packets, they can be used to amplify the bandwidth further such as when thousands of bots are querying thousands of DNS servers.

Traditional network layer countermeasures for protecting from DDoS attacks include setting routers to examine and drop packets, filter IP addresses, configure rate limits and apply ingress and egress network filtering. Unfortunately today, most of these countermeasures are not enough to protect from DDoS and DDRoS attacks of the intensity of 100 Gbps bandwidth. In order to protect from high power DDoS and DRDoS attacks, CISOs whose organizations high availability websites are under the threat of high bandwidth DDoS and DDRoS attacks, need to consider investments in network segmentation, hosting part of the website static content on CDN (Content Delivery Networks) and use third party cloud-based DDoS protection services with service level agreements to increase traffic bandwidth in case it is consumed during a DDoS attack. Refer to (Attacks FS-ISAC_Threat_Viewpoint_DDoS_June_2012.pdf).

II-6 Mitigating the Inherent Risks of New Application Technologies

The goal of this chapter is to guide the CISO on the consideration of the security risks posed to the organization by the adoption of new technologies. The term "technologies" is used herein to include recent examples of technologies that impact applications such as mobile technologies, web 2.0 technologies, and cloud computing Software as a Service (SaaS). As technologies evolve, it is important for the CISO to understand the security risks introduced by the adoption of these new technologies since these might represent new opportunities for attackers to attack both applications and the data. The increased risk to applications due to the adoption of new technologies includes the increased exposure/attack surface such as in the case of extending applications to mobile devices, the introduction of a new class of client and server side vulnerabilities such as in the case of Web 2.0 and the increased risk of loss of data and transaction integrity due to the use of cloud computing. In order to target the mitigation of the risks due to the adoption of these technologies, CISO needs to have a clear picture of the risks that are introduced and decide to invest in a new type of application security assessments, tools and security measures to mitigate the risks.

Managing the risks of mobile applications

Mobile application security is a particular concern for most organizations today: this is mostly due to the exponential growth in the adoption of mobile smartphones and tablets by users both for personal and business use. From the application security perspective, access of business applications from mobile devices increases the opportunity for threat agents to attack the mobile device and the applications and the data that can be stored in the mobile devices. Mobile phones that are compromised with malware for example, expose both the client application installed on the device as well as the server application that can be assessed through the mobile device. Different mobile communication channels can be also attacked including web channels to access Wi-Fi networks, MMS, SMS messaging and GSM 2G, 3G, 4G wireless networks. Businesses whose applications can be accessed through mobile devices should consider the exposure to attacks increased by the adoption of mobile applications. One important security measure is to require a specific vulnerability assessment for testing the security of mobile applications and of the protection of sensitive data that is stored on the mobile device. The requirement to encrypt any confidential and authentication data that is stored on the device, for example, might be required by compliance with internal mobile security standards and policies. Exposure of web services that can be accessed through a mobile application needs also to be tested for vulnerabilities. Often the organization might decide to avoid the risk of mobile applications accessing financial risk transactions such as money transfers and payment when authentication on the device is considered not as strong as the one available for the internet PC based applications. In some cases, device security controls might be considered not secure enough, such as when using device based encryption (e.g. iOS keychain) because this can be brute forced when the user is no longer in possession of the mobile device. These are important risk considerations and can be enforced by requiring the development organization to follow security standards for designing mobile applications.

Besides device compromise because of a device being lost or stolen another risk to consider is the compromise of the mobile device by malware designed to install keyloggers to collect user's credentials and to redirect these stolen credentials to the fraudster's server. Today mobile applications represent an opportunity to attack applications installed on the mobile devices through different communication channels such as emails, social media, video-audio streaming, instant messaging and web. Examples of opportunities for an attacker to compromise mobile devices with malware, for example, include social engineering mobile users to click on malicious links in emails and messages that carry malware payloads to install spyware and remote access tools. The sophistication of the mobile malware today is such that some mobile malware is specifically designed to attack the time tokens sent to the user's phone to authenticate online banking web sites. This type of mobile banking malware has the capability to perform (MiTMO) Man in the Mobile attacks and redirect the one time authentication tokens to the fraudster's mobile phone so they can be used to authenticate to the online banking site along with username and passwords. Another avenue of attacks to mobile applications is to upload malicious applications on the mobile application provisioning stores (e.g. Market place and Apple Store) and lure mobile users to download rogue applications from these stores. Since applications for

Android and iOS together compose nearly 90 % of the worldwide smartphone type of applications, attacking application provisioning stores represent the best opportunity for an attacker to spread mobile malware to a large numbers of mobile application users. Typically the security checks that are performed by these mobile application stores especially in the case of the Apple Store mitigate these risks but downloading mobile type of applications from sites whose origin cannot always be validated by the mobile users (possible for Android mobile type of applications) should be considered a risk.

Nevertheless, a lot of security can be gained by just having mobile users follow basic security measures. In some cases the lack of enforcement of basic simple default security measures such as use of PINs to prevent unauthorized access and allowing the installation of applications that require to "jail break" the phone represent an increased risk both for the data and the mobile applications residing on these devices. A good preventive measure is to keep informing users of the threats targeting mobile devices and recommend them to follow basic security measures. Good resource of security awareness for mobile phones and protection from threats targeting mobile devices is US CERT Cyber Threats to Mobile Phones.

For CISOs whose responsibility is to manage the security of mobile applications it is important to consider the adoption of specific security processes and standards for the security of mobile applications. These measures might include the adoption and documentation of mobile technology security standards, the adoption of vulnerability assessments to specifically security test for mobile application type of vulnerabilities and standards for secure provisioning of these mobile applications and application data on the personal owned consumer devices. From the perspective of adoption of specific security testing process for vulnerabilities in mobile type of applications, the OWASP mobile security project has a number of resources such as documentation on mobile security risks, free vulnerability assessment tools, cheat-sheets and guidelines for the secure design of mobile applications.

An important aspect that mobile security and of particular CISO concern is to secure organization-issued mobile devices as well as user personal devices brought into the organization (e.g., Bring Your Own Device, BYOD). As the practice to bring personal devices into the enterprise environment becomes prevalent, CISOs will need to access the potential risks and determine how much access to grant to potentially unsafe employee-owned devices. Today some organizations might allow employee owned devices to directly access the organization's network only through secure connectivity such as VPN, secure virtualization, terminal servers or remote access utilities like virtual network computing (VNC). In all these cases, it is important that CISOs have rolled out specific policies for remote access from employee owned devices that are strictly enforced through a secured and centrally managed controlled access technologies and services. A good resource that can help CISOs to set guidelines for BYOD and for centrally managed and secure mobile devices, such as smart phones and tablets is the NIST SP 800-124, Guidelines for Managing and Securing Mobile Devices in the Enterprise (Draft) and Guidelines on Cell Phone and PDA Security.

Managing the risks of Web 2.0 technologies

New technologies introduce new risks and new measures need to be put in place by the organization to mitigate these risks. One possible way to prepare for the impact of new technologies it to plan in advance the adoption of security measures and processes to mitigate the risks by knowing when such technologies will become "mainstream" that it will be widely adopted by the business. According to some analysts like Gartner, the adoption of new technologies by the market follow a cycle also referred as "hype" that comprises five phases that are (1) "Technology Trigger", (2) "Peak of Inflated Expectations", (3) "Trough of Disillusionment", (4) "Slope of Enlightenment" and (5)"Plateau of Productivity". In the hype cycle that Gartner published in 2009 covering emerging technologies, Web 2.0 was shown as two or less than two years for mainstream adoption. This prediction is validated today (2012) by considering that several applications today have adopted and integrated Web 2.0 technologies in their web applications. Since typically senior management and executives' pay specific attention on the market and security technology research of analysts (e.g. Gartner and Forrester) it is important for CISO to look at this research as well from the perspective of

deciding whether to adopt a certain type of technology as well as for preparing for the security impacts of such technology. First of all it is important to understand the terminology used. Web 2.0 technologies can be defined as "Web applications that facilitate interactive information sharing and collaboration, interoperability, and user-centered design on the World Wide Web". The main characteristics of Web 2.0 technologies are:

- Encourage user's participation and collaboration through a virtual community of social networks/sites. Users can and add and update their own content, examples include Twitter and social networks such as Facebook, Myspace, LinkedIn, YouTube
- Transcend from the technology/frameworks used. Examples include AJAX, Adobe AIR, Flash, Flex, Dojo, Google Gears and others
- Combine and aggregate data and functionality from different applications and systems, example include "mashups" as aggregators of client functionality provided by different in-house developed and/or third party services (e.g. web services, SaaS)

One important aspect that CISOs need to be aware of regarding of Web 2.0 technologies is how these technologies affect the threat landscape. First of all, Web 1.0 threats are amplified by the intrinsic nature of Web 2.0 due to the expanded volume of user's interaction: consider for example the hundredths of millions of users of social networks and the increased attack surface to the web application offering links to corporate Facebook and twitter accounts now provided to a threat agent for attacking the user with phishing, malware as well as for exploit of traditional Web 1.0 vulnerabilities such as injection flaws, XSS and CSRF. Social networks specifically facilitate customer's sharing of confidential and private information since boundaries between private and personal information are often crossed by voluntarily sharing of such information with the company even if is not being explicitly requested.

Another element of increased risks is represented by the increased complexity of the functionality due to the integration of different Web 2.0 technologies and services both as front-end-client as well as back-end-server. Business rich client interfaces such as widgets for example increase the likelihood of business logic attacks while exposure of new web services increases the exposure of attacks to back end servers.

Web 2.0 vulnerabilities exploited by attackers

Because of the increased risks to web applications due the introduction of Web 2.0 technologies, it is important that CISOs make sure that web applications are specifically designed, implemented and tested to mitigate the risks. From a vulnerability and threat analysis perspective, Web 2.0 application vulnerabilities can be analyzed using the OWASP Top 10 and the WASC Top 50 threats. OWASP Top 10 vulnerabilities that Web 2.0 applications need to be tested for include A1-Injection, A2-XSS, A3-Broken Authentication and Session Management and A5-CSRF. Examples of Web 2.0 injection vulnerabilities include XML injections such as when an attacker will provide user-supplied input that is inserted into XML without sufficient validation affecting the structure of the XML record and the tags (and not just content). A particular type of XML injection vulnerability is XPATH injection. This is an attack aimed to alter an XML query to achieve the attacker's goals such as to perform un-authorized queries to retrieve confidential data. Another Web 2.0 specific injection vulnerabilities includes JSON injections to run un-authorized code, potentially malicious by injecting malicious JavaScript code into the JSON (JavaScript Object Notation structure) on the client.

Among Web 2.0 injection vulnerabilities, RSS feed injections can be used to consume un-trusted sources from RSS feeds such as malicious links to download malware on the victim's computer. Web 2.0 exploits of XSS are facilitated by the fact that a lot of Web 2.0 based sites that allow adding HTML to normal text content such as when posting blogs and feedbacks to the company products-services. When HTML data is unfiltered from malicious input it might allow the attacker to enter unsafe HTML tags that can be abused for XSS to attack victims reading the blog postings or comments to select malicious links. An additional attack vector for Web 2.0 XSS is also represented by XSS DOM since WEB 2.0 APIs use DOM in Rich Internet Applications (RIA) written in FLASH, Silverlight such as Mashups and Widgets. The use of AJAX

(Asynchronous JavaScript) on the client also increases the possible entry points for attacking several HTTP requests to the web site with XSS attacks. An example of a Web 2.0 attack exploiting injection vulnerabilities is included in the Web Hacking Incident Database WHID 2008-32: Yahoo HotJobs XSS that allowed the threat agents to exploit an XSS vulnerability on Yahoo HotJobs to steal session cookies of the victims and gain control of every service accessible to the victim within Yahoo, including Yahoo! Mail.

Example of exploits of Web 2.0 OWASP-A3: Broken Authentication and Session Management vulnerabilities include use of weak passwords, passwords stored in AJAX Widgets/Mashup that are sent and stored in clear outside the control of the host, passwords that are stored on the client as "autologon feature" or in the cloud to SSO from the desktop and password recovery controls that are not protected from brute force attacks since do not lock the accounts when several failed tries to guess the passwords are attempted. An example of this vulnerability type exploit is also part of the WHID catalogue as 2008-47: The Federal Suppliers Guide validates login credential in JavaScript.

A type of vulnerability that is facilitated by Web 2.0 is CSRF such as when clients use AJAX to make XHR calls that enable invisible queries of a web application and the user cannot visually validate for forgery. CSRF is also facilitated by insufficient browser enforcement of the Single Origin Policy for desktop widgets and weak session management when session expiration times are set to be quite high, increasing the risk of session base attacks such as CSRF. Persistent session cookies that are shared by widgets also increase the opportunities for CSRF attacks. A known Web 2.0 security incident that is in the WHID catalogue as 2009-4:"Twitter Personal info CSRF" allowed an attacker to exploit a CSRF bug in Twitter to get twitter profiles of the visitors.

A type of vulnerability that is also exploited and used against Web 2.0 applications but also more in general against web sites is due to the lack of anti-automation defenses. This vulnerability is not tracked by OWASP Top 10 but by the Web Application Secure Consortium (WASC) as Top 21 within the TOP 50 issues tracked by WASC. Automation attacks against Web 2.0 applications that are allowed to post information such as feedback forms, blogs and wiki pages for example seek to spam these pages with commercial information and potentially by attackers to post links to malicious sites to spread malware via drive by download or by phishing.

Example: Insufficient Anti-automation for Facebook

In 2007, Facebook was accessed through automation in an attempt to harvest user information. See WHID 2007-65:" Botnet to manipulate Facebook"

Security measures to mitigate risks

Critical to the vulnerability analysis of Web 2.0 applications is the determination of the root causes of the vulnerabilities. Only through the identification of the vulnerabilities root causes, can vulnerabilities be eradicated. For example if these vulnerabilities originate from lack of security requirements for Web 2.0 that software developers need to follow, these need to be documented. In case the issues are caused by errors in design, these needs to be prevented by making sure the design of web 2.0 applications is reviewed by a security architect that has subject matter expertise in Web 2.0 technology. For Web 2.0 vulnerabilities that are introduced by software developers as coding errors or because of integration with software and third party libraries that are exposed to Web 2.0 vulnerabilities it is important that software developers are trained in defensive coding Web 2.0 applications and that security testers know how to identify and test Web 2.0 vulnerabilities.

A prescriptive set of Web 2.0 security measures that CISOs can undertake to mitigate the risks include:

- Documentation of security standards for Web 2.0 technologies such as security requirements for design, coding and testing specific Web 2.0 technologies such as AJAX, FLASH and enforcement of them at the beginning of the SDLC
- Institute a security activity during design to review threats against Web 2.0 applications and identify countermeasures such as application threat modeling. Part of this activity also includes the security review of the application architecture and the security controls that are exploited by attacks against Web 2.0 applications such as input validation, authentication, session management and anti-automation controls such as CAPTCHA.
- Require Web 2.0 based applications to undergo a secure code review to assure source code adherence to security coding standards and static source code analysis to identify Web 2.0 coding issues in both client source code used by Widgets, RIA, AJAX components as well as server side code that is used in web services and Service Oriented Architectures (SOA). Specific secure code requirements can be documented for AJAX, these can be socialized with architects and software developers and validated during design and source code reviews.
- Require security tests to include specific test cases for testing Web 2.0 component vulnerabilities and for Web Services. Refer to OWASP test guide test cases for testing AJAX and Web Services as example.
- Make sure Web 2.0 technical risks are managed such as the business risks that Web 2.0 design flaws and bugs might pose to the business. The OWASP risk methodology can be used to manage Web 2.0 security risks. An example of OWASP risk framework applied to Web 2.0 technologies is included in the table below.

Table 1 THE OWASP RISK FRAMEWORK APPLIED TO WEB 2.0 TECHNOLOGIES

Threat Agents	Misuses and Attack Vectors	Security Weaknesses	Security Controls / Countermeasures	Technical Impacts	Business Impacts
Web 2.0, Users	User shares private/confidential information, agents post confidential information	Inherent weaknesses in controlling user contributed content in social network, blogs, IMs, private emails	Web 2.0 social networking security policies, compliance monitoring, filtering, archiving, approval workflow for social site posts	Less of sensitive / confidential data	Reputation damage, compliance failure fines
Malicious users, fraudsters	Victim is targeted by phishing, download of malicious widgets, clicking on malicious posts	Social engineering, web 2.0 vulnerabilities: XSS	User education, data filtering, escaping/encoding untrusted data	Execute JavaScript on client, install malware	Fraud, financial losses, defacements, reputation damage
Malicious users, fraudsters	Attacker sends malicious data to the application's interfaces	Web 2.0 vulnerabilities: XPATH injection, XML injection, JSON injection	Filtering, parameterized APIs, ESAPI filtering methods, white list validation	Loss of data, data alteration, denial of service/access	Public disclosure, reputation damage
Malicious users, fraudsters	Attackers use leaks or flaws in the authentication or session management functions	Web 2.0 broken authentication and session management vulnerabilities	Security requirements for secure password policies, account lockout, disable auto-logins	Unauthorized access to data, functions	Loss of CIA, legal and financial implications
Fraudsters	Attackers create forged HTTP requests and tricks victims into submitting them	Web 2.0 cross site request forgery vulnerabilities	Include the unique token in a hidden field	Can change data and undertake functions on behalf of the user	Loss of CIA, fraud, denial of access

Threat Agents	Misuses and Attack Vectors	Security Weaknesses	Security Controls / Countermeasures	Technical Impacts	Business Impacts
Automated Scripts / Spam Bots	Application post links, create accounts, game the application, scrape data	Insufficient anti-automation	Behavior monitoring, AppSensor attack detection, include CAPTCHA, ESAPI intrusion APIs	Can overflow process with spam, enumerations	Business disruption/loss, reputation damage

Managing the risks of cloud computing services

The concept of cloud computing is not new. Many organizations used to outsource their data centers to third party owned data centers, a concept that in cloud computing is considered a deployment of Infrastructure As A Service (IaaS) cloud service. The term cloud computing encompasses outsourced infrastructure such as in the case of Infrastructure as a Service (IaaS), outsourced platforms such as in the case of Platform As A service (PaaS) and through outsourced software a term that is also referred to as Software As A Service (SaaS).

CISOs today face the challenge to assess and assert the security of cloud computing deployments within their network (e.g. on-premises or private cloud) or outside the organization (e.g. outside premise or public cloud). Information and application security is a primary concern for organizations that outsource either their infrastructure component and platforms or software and data to a third party vendor cloud provider. CISOs need to consider the potential risks and assess them prior to deciding to outsource their services to third parties. CISOs should consider for example the potential risk of the company data that is hosted on a third party cloud computing provider can be compromised because of a security incident occurring at the cloud provider. CISOs should also consider for example the risk that an organization might face when the data service that is provided to their customers is outsourced to a third party software and become unavailable because such cloud service provider has been targeted by a denial of service attack.

It is therefore important that CISOs consider the whole spectrum of information security risks before the organization decides to move either their services or their data to the cloud computing service providers. At high level these risks can be assessed by conducting a due diligence third party information security assessment on the cloud computing provider service vendor. These type of assessments seek to assert the security posture of the cloud provider against the company's information security policies and standards as well as with audit of industry relevant IT security standards such as SAS 70, SOC, FISMA, PCI DSS, ISO, FIPS-140, ISO/IEC 27001-2005 etc. and others as these are relevant to the organization's regulated security business operations such as HIPPA, FFIEC, MPAA etc. etc.

In the case of cloud computing assessment, security risks and compliance-audit are actually some of the domains that need to be assessed along with others such as cloud architecture, governance, legal and law enforcement, privacy, business continuity and disaster recovery, incident response, application security, encryption and key management, identity, entitlements and access management, virtualization and security as a service.

A comprehensive guidance on how to conduct oversight on all these domains of cloud computing is the Cloud Security Alliance. CSA provides top level security guidance for critical areas in cloud computing. CSA also provides a set of tools that can be used by organizations to assess security risks of cloud computing services in these domains including a cloud control matrix spreadsheet to assess SaaS, PaaS and IaaS controls for information security, legal, organizational-policies, risk management, resilience and security architecture, against standards such as COBIT 4.1, ISO 27001, NIST SP 800-53, PCI-DSS vs. 2.0 and others. The CSA Consensus Assessments Initiative Questionnaire v1.1 allows CISOs to assert the third party cloud computing service providers with respect to information security as well as compliance, data governance, facility security, human resource security, legal, operations management, risk management, release management, resilience and

security architecture. In 2013 CSA also published a white paper with guidance on adopting controls in the cloud to mitigate the risk of the top threats to cloud computing.

Top Nine Threats to Cloud Computing

https://cloudsecurityalliance.org/

1. **Data breaches**
2. **Data loss**
3. **Account hijacking**
4. **Insecure APIs**
5. **Denial of service**
6. **Malicious insiders**
7. **Abuse of cloud services**
8. **Insufficient due diligence**
9. **Shared technology issues**

OWASP recommends that CISOs leverage CSA documentation guidance; questionnaires and threat analysis referred herein and use these to construct an ad-hoc cloud computing security assessment process that can be used by the organization's information security team to conduct due diligence information security, risk and compliance-audit assessment on cloud computing providers. Such ad-hoc cloud computing security assessment might consider the organization information security policies, standards and regulations are the starting point to assert the security of cloud providers since these are the same that are applicable and more relevant to the organization requirements to protect confidentiality, integrity and availability of the data. An ad-hoc cloud computing security assessment should at minimum include a standard process that can be followed including a set if questionnaires that can be used to capture and assert the security, compliance and risk management posture of the cloud computing security provider prior to making a business decision to whether outsource services such as infrastructure, networks, platform and software-data to a third party cloud computing service provider.

The main goal of such an assessment is to identify control gaps and potential areas of risk for the organization. Examples of application security risks that can be identified with these assessments might include the identification of the lack of end to end encryption of the data granting full control and assurance to the business of the confidentiality of the data either in transit or in storage to the third party cloud provider, the lack of segregation of data from other businesses in a virtualized cloud computing environment and the lack of audit and logging for specific security events and incidents. Examples of mitigating security controls for these risks might include the requirement of use of end to end encryption for confidential data in transit and storage at the cloud provider, the use of virtual firewall and secure hypervisor architecture for securing tenants in SaaS cloud virtualized environments and the adoption of specific audit and logging facilities that can be used to alert both the cloud provider and the organization outsourcing the service in the case of a security incident as few examples.

Once these control gaps have been identified it is important to assign the level of severity-risk and determine if compensating controls might be implemented prior to the deployment of the cloud computing solution. An important aspect for managing these risks is also to make sure a SLA (Service Level Agreement) captures these risks and provides binding contractual agreements with the cloud service provider and liability clauses and indemnities for the organization in case these agreements are breached.

Part III : Application Security Program

III-1 Executive Summary

From the risk management strategic point of view, the mitigation of application security risks is not a one time exercise; rather it is an ongoing activity that requires paying close attention to emerging threats and planning ahead for the deployment of new security measures to mitigate these new threats.

This includes the planning for the adoption of new application security activities, processes, controls and training. When planning for new application security processes and controls, it is important for CISOs to know on which application security domains to invest in order for the business to deliver on its missions.

To build and grow an application security program, CISOs must:

- Map business priorities to security priorities
- Assess the current state using a security program maturity model
- Establish the target state using a security program maturity model

Map business priorities to security priorities

All security priorities must be able to be mapped to business priorities. This is the first step towards establishing the relevance of every security initiative and shows business management how security supports the mission. It also demonstrates to security staff how the staff supports the mission.

Assess the current state using a security program maturity model

Accessing process maturity is a prerequisite for adoption of application security and software security processes. One criteria that is often adopted by organizations is to consider the organization's capabilities in application security domains and the maturity of the organization in operating in these domains. Examples of these application security domains include application security governance, vulnerability risk management, regulatory compliance and application security engineering such as to design and implement secure applications. Specifically in the case of application security engineering, adopting software security assurance is often necessary when there is not direct control on implementing the security of such software since it is produced by a third party vendor. A factor to consider in this case is to measure the software security assurance using a maturity model. A pre-requisite for measuring software security assurance is the adoption of a Secure Software Development Lifecycle (S-SDLC). At high level, S-SDLC consists of embedding "build security in" security activities, training and tools within the SDLC. Examples of these activities might include software security processes/tools such as architectural risk analysis/threat modeling, secure code reviews/static source code analysis, application security testing/application vulnerability scanning and secure coding for software developers. A reference to OWASP software assurance maturity model as well as to the several OWASP projects dedicated to software security and S-SDLC are provided in this guide as well.

Establish the target state using a security program maturity model

Not all organizations need to be at the highest maturity. The maturity should be at a level that it can manage the security risk that affects the business. Obviously, this varies among organizations and is driven by the business and what it accepts as risk as part of continuous collaboration and transparency from the security organization.

Once a target state is identified, CISOs should build a roadmap that identifies its strategy for addressing known issues as well as detecting and mitigating new risks.

OWASP provides several projects and guidance for CISOs to help develop and implement an application security program. Besides reading this section of the guide, see the Appendix B: Quick Reference to OWASP Guides & Projects for more information on the type of security engineering domain activities that can be incorporated within an application security program.

III-2 Introduction

Mitigating the risk of attacks that seek to exploit application vulnerabilities as well as potential gaps in protective and detective controls is one of the CISOs main concerns. In the case when vulnerabilities are only found after a security incident, the next step is to fix the identified vulnerabilities and limit further impact. Typically, this involves reproducing the vulnerabilities and re-testing the vulnerabilities after fixes are implemented to ensure vulnerabilities can no longer be exploited. If the incident is due to a gap of a security control such as a failure to filter malicious input or to detect the attack event, the next step is to implement countermeasures to mitigate the risk. Countermeasures may be a combination of deterrent, preventative, detective, corrective, and compensating security controls. To make such decisions, the CISO needs to consider both the risks of vulnerabilities as well as the weaknesses of security control measures to make a decision on how to mitigate the risks. Typically fixing a vulnerability involves a vulnerability management cycle that includes identifying the vulnerability, fixing it and then re-testing it to determine that it is no longer present.

For countermeasures, the test that the countermeasure is effective in preventing and detecting an attack vector can also be tested with a functional security test after a countermeasure is deployed. The decision as to which countermeasure to deploy might depend on different factors such as the cost of the countermeasure vs. the business impact of the incident as well as on how risk mitigation effective is the countermeasure by comparing with others. The next step for the CISO after the security incident is under control is to make sure any vulnerabilities are fixed and countermeasures are deployed to mitigate the risk. In this section of the guide we focus on application security measures that are most cost effective to target the issues identified in Part 2. For example how to divide budgets across software security activities such as secure code training, secure code reviews, security verification and testing and issue and risk management.

In the 2013 CISO Survey, CISOs identified their top priorities and also the risks facing their programs. In this guide, you will find guidance for tools and processes to not only execute on these priorities, but also to manage the risks that may impact your priorities.

2013 CISO Survey: Top 5 CISO Priorities

1. **Security awareness and training for developers**
2. **Secure development lifecycle processes (e.g., secure coding, QA process)**
3. **Security testing of applications (dynamic analysis, runtime observation)**
4. **Application layer vulnerability management technologies and processes**
5. **Code review (static analysis of source code to find security defects)**

These priorities can be inhibited by the top program risks identified by CISOs in the same 2013 CISO Survey, as shown on the next page.

2013 CISO Survey: Top 5 CISO Risks

1. **Lack of awareness of application security issues within the organization**
2. **Insecure source code development**
3. **Poor/inadequate testing methodologies**
4. **Lack of budget to support application security initiatives**
5. **Staffing (e.g., lack of security skills within team)**

III-3 Addressing CISO's Application Security Functions

Application security governance, risk and compliance

Governance is the process that introduces policies, standards, processes and sets the strategy, goals and organizational structure to support them. At an operational level, governance, compliance and risk management are interrelated. As part of governance responsibilities, CISOs influence the application security goals and work with executive management to set the application security standards, processes and organizational structure to support these goals. As part of compliance responsibilities, CISOs work with auditors and the legal counsel to derive information security policies and establish requirements to comply, measure and monitor these requirements including application security requirements. As part of risk management responsibilities, CISOs identify, quantify and make risk evaluations to determine how to mitigate application security risks that include introducing new application security standards and processes (governance), new application security requirements (compliance) and new application security measures (risks and controls). From a governance perspective, the adoption of application and software security processes, the establishment of application security teams and application security standards within any given organization varies greatly depending on the type of organization's industry, the size of the organization and the different roles and responsibility that the CISO has in that organization. OWASP provides several projects and guidance for CISOs to help develop, implement and manage application security governance. See the Appendix B: Quick Reference to OWASP Guides & Projects for more information on OWASP projects and guides in the governance domain.

Typically the source of application security investments also varies depending on the size and the type of the organization. For CISOs reporting to the organization's head of operational information security and risk management, typically the budget for application security is part of the overall budget allocated by information security and operational risk departments. For these CISOs, one the main reasons for the adoption of new application security activities, guides and tools such as the ones that OWASP provides, is first and foremost to satisfy compliance and to reduce risks to the organization's assets such as applications and software. Compliance varies greatly depending on the type of industry and clients served by the organization. For example, organizations that produce software that implements cryptography for use by governments such as the department and agencies of the United States Federal government need to comply with Federal Information Processing Standards (FIPS) 140. Organizations that produce software and applications that handle cardholder data such credit and debit card data for payments need to comply with the Payment Card Industry Data Security Standard (PCI DSS). CISOs that report to the organization's head of information technology, typically have responsibility on both security and information technology functions that might also include the compliance of applications and software with technology security standards such as FIPS 140 and PCI-DSS. Compliance with security technology standards represent an opportunity for promoting secure development and testing within the organization such as by using OWASP security testing guides for achieving security certifications for applications and software products. Compliance with PCI-DSS requirements, for example, might already require the organization to test applications for a minimum set of common vulnerabilities such as the OWASP Top 10. The budget allocated by the IT department for achieving certifications with technology security standards such as FIPS-140 and PCI-DSS can also be used for promoting secure coding guides such as the OWASP secure coding guide and invest in static code analysis tools. For example, in the case of compliance with PCI-DSS, CISOs might opt for static code analysis to satisfy the requirement 6.6 of PCI-DSS. OWASP provides several projects and guidance for CISOs to help develop and implement policies, standards and guidelines for application security as well as to help define application security requirements that can be verified and audited. See the Appendix B: Quick Reference to OWASP Guides & Projects for information on OWASP projects in the standards and policies and audit & compliance domains.

CISOs of small organizations can also use vulnerability management metrics to make the business case in which phases of the SDLC to invest in security and improve both software quality as well as security. For

example, since most of the quality and security bugs are due to coding errors, it is important for CISOs to emphasize to the IT department the need for secure coding processes, standards and training for developers since focusing on these software security activities also leads to cost savings for the organization. A study from NIST about the cost of fixing security issues for example has shown that the cost of fixing a coding issue in production is six times more expensive than fixing it during coding. To achieve these money saving and efficiency goals, CISOs can work together with the engineering department managers to promote application and secure software initiatives. Part IV of the CISO guide provides guidance regarding setting metrics for managing application security risks and for deciding on application security investments.

Among CISO responsibilities the Continuity of Business (CoB) is of primary importance specifically for web applications that provide critical business functions to customers. CISOs are responsible to roll out CoB plans to ensure that the business could continue to operate despite adverse circumstances or events. A CoB plan includes procedures to restore services that are lost because of a negative event such as a power outage of the data center where a web application is hosted. A critical item of CoB planning is the identification of web applications that are deemed business critical and assign a level of criticality and specific requirements for CoB testing such as the maximum time to recover from a loss of service. Similarly to CoB, having a disaster recovery plan is also one of the CISO responsibilities: this includes process, policies and procedures for recovery or continuation of technology infrastructure in the case of natural or human provoked disaster.

One of the main CISOs responsibilities is to increase application security awareness among the application security stakeholders. A 2012 Survey by the Ponemon Institute and Security Innovation that included more than 800 IT executives found that "gaps in perceptions between security practitioners and developers about application security maturity, readiness and accountability indicate why many organizations' critical applications are at risk." Almost 80% of developers and 64% of security managers that participated to this survey, responded that their organization has no process for building security controls into their applications, and more than 50% of both developers and security officers reported that they did not receive software and application security training, only 15% of developers and 12% of security officers reported that applications met security regulations and 68% of developers versus 47% of officers reported to be aware of any security breaches affecting applications occurring in the past 2 years. It is clear that there is opportunity for efficiency gain by building security into the SDLC through security training. OWASP has several training and awareness resources that can be used for the training on application and software security for development, operational and information security teams. Please consult theAppendix B: Quick Reference to OWASP Guides & Projects for more information on OWASP guides and projects in the security training domain.

For CISOs whose main focus is information security and risk management, one of the main requirements besides compliance is to introduce efficiencies and save the money spent for existing security processes, including application security. Since the information security department allocates budgeting, any request for budget of application security needs to be justified by improving security and by reducing risks. Security and risk reduction goals are aligned by improving security test processes with use of better tools and training for developers. For CISOs of large organizations, promoting a software security initiative is also justified by cost-avoidance revenue from the decreased cost fixing vulnerabilities as a result of secure coding standards, secure code reviews and security testing in earlier phases of the SDLC when bug fixes are less costly. See Appendix B: Quick Reference to OWASP Guides & Projects for information on OWASP guides and projects that help CISOs in implementing an application security program including software security development and security testing processes.

Often CISOs need to justify the budget for application security by taking into consideration the different needs of security and business departments. For CISOs that serve in financial organizations for example, security is often a compromise with security and business goals. In this case, it is important for CISOs to be able to align application security programs with the business goals and when these goals not align, to focus on the ones that do. For example, by focusing on improving both software quality and security and by reaching a compromise in the case security impacts negatively the customer experience so different security options

need to be considered. In the case the business is sponsoring a new application development project, CISOs can use this as an opportunity to promote new application security features for the application and work together with project managers by achieving compliance with security standards, improving security by design and by coding and yet achieving overall cost savings for the overall project.

The importance of security metrics

For CISOs whose responsibility is manage application vulnerability risks, security metrics such as application vulnerability metrics constitutes an important factor in making business cases for investing in application security measures to control and reduce risks. Security metrics such as measurements of vulnerabilities found on the same applications during the roll out of application security activities aimed to reduce the number and the risk of vulnerabilities for example, can demonstrate to senior managers and company executives that the adoption of application security processes, training and tools ultimately helps the organization to deliver applications and software products that have a fewer number of vulnerabilities and pose less risk to the organization and the customers.

III-4 Targeting Software Security Activities and S-SDLC Processes

OWASP provides several projects and guidance for CISOs to help in the development and implementation of software security activities and Security in the Software Life Cycle (S-SDLC). To know more, besides reading this section of the guide, please consult the Appendix B: Quick Reference to OWASP Guides & Projects for more information

Recognizing the importance and criticality of secure software

Since insecure coding causes a large number of vulnerabilities in applications, it is important that the CISO recognizes the importance that secure software has in improving the security of the application. The causes of insecure software might depends by different factors such as coding errors, not following secure coding standards and security requirements, integration with vulnerable software libraries, missing secure code review processes and security testing and formal secure code training and awareness for software developers. From CISO perspective, it is important to understand that software security is a complex discipline and requires a special focus in security processes, tools as well as people skills. It is also important to recognize that investing in software security helps the organization to save money spent in application vulnerability remediation costs in the future. By investing in software security initiatives, organizations can focus on fixing vulnerabilities as early as during coding phase of the Software Development Life-Cycle (SDLC) where is cheaper to identify, test and fix them than during the validation phase.

Today, also thanks to OWASP, software security has matured and evolved as a discipline. For example, several organizations already adopt software security best practices within their software development processes such as the documentation of security requirements, following of secure coding standards and use of software security testing tools such as static source code analysis tools to identify vulnerabilities in source code before releasing source code to be build and integrated for final integrated and user acceptance tests. By integrating software security activities in the SDLC, organizations can produce software and applications with a fewer number of vulnerabilities and lower risks than software and applications that don't.

Integrating Risk Management as part of The SDLC

CISOs determine how software security activities can be integrated as part of the SDLC. According to the National Institute of Standards and Technology's Special Publication 800-30, "Effective risk management must be totally integrated into the SDLC ... [which] has five phases: initiation, development or acquisition, implementation, operation or maintenance and disposal." The integration of security in the SDLC process begins by identifying the information assets that the software will be processing and by specifying requirements for confidentiality, integrity and availability. The next steps consist of information assets value determination, identification of the potential threats and identification of the necessary application security countermeasures such as authentication, authorization and encryption.

A comprehensive set of security requirements need to also include requirements to implement secure software by following certain security and technology standards, security approved technologies and platforms as well as security checks prior of software integration with other vendors software components/libraries.

Assess risks before procurement of third party components/services

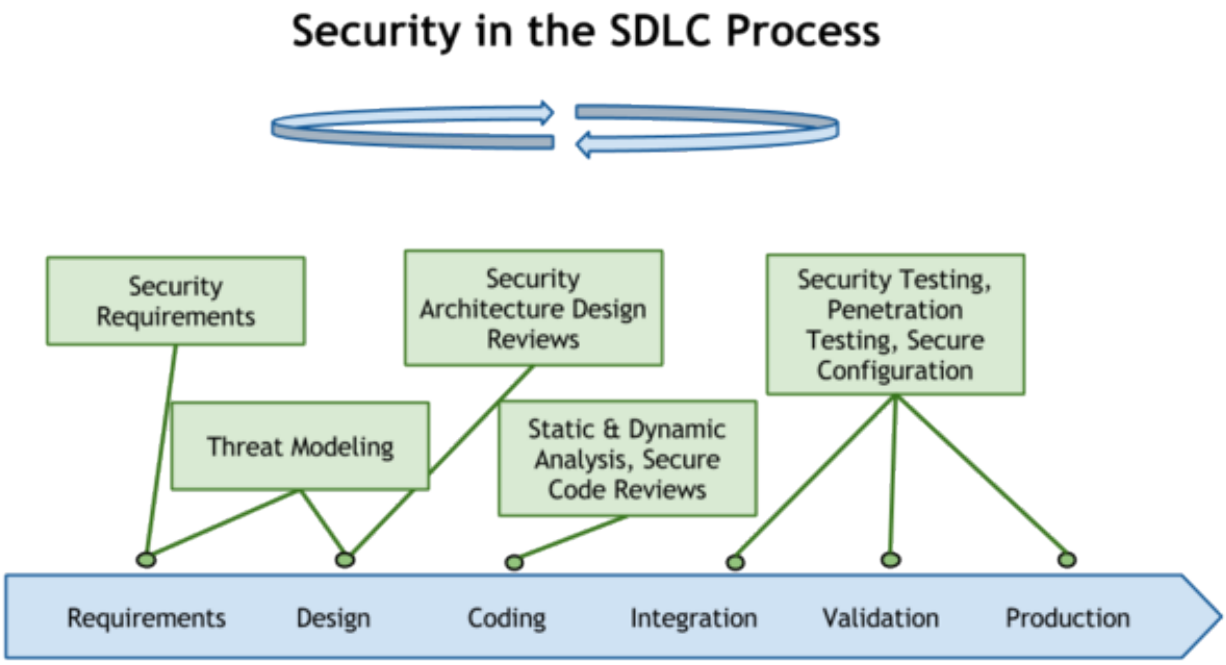
When software is acquired as either part of the commercial off-the-shelf (COTS) or as free open source (FOSS) for example, it is important for CISO to have a process in place to validate this type of software libraries against specific security requirements prior to acquiring them. This could provide the CISO of the organization a certain level of assurance that the acquired software is secure and can be integrated with the application. In that regard, OWASP had developed a legal project and a contract annex of a sample contract that included security requirements for the life cycle so that COTS products would be more secure. Please

refer to the Appendix B Quick Reference to OWASP Guides & Projects for more information on OWASP projects that can help CISOs to assess procurement of new application processes, services, technologies and security tools.

Security in the SDLC (S-SDLC) methodologies

In cases when the CISO of the organization has also responsibility over promoting a software security process within the organization, it is important not to take this goal lightly since usually requires careful planning of resources and development of new processes and activities. Fortunately today, several "Security in the SDLC" (S-SDLC) methodologies can be adopted by CISOs to incorporate security in the SDLC. The most popular S-SDLC methodologies used today are Cigital's Touch Points, Microsoft SDL, OWASP CLASP and the BITS Software Assurance Framework. At high level, these S-SDLC methodologies are very similar and consist on integrating security activities such as security requirements, secure architecture review, architecture risk analysis/threat modeling, static analysis/review of source code, security/penetration testing activities within the existing SDLCs used by the organization. The challenge for the integration of security in the SDLC from CISO perspective is to make sure that these software security activities are aligned with the software engineering processes used by the organization. This means for example to integrate with different types of S-SDLC s such as Agile, RUP, Waterfall as these might be already followed by different software development teams within the organization. An example on how these can be integrated within a waterfall SDLC as well as iterated within different iterations of a SDLC process is shown below.

Figure 7 EXAMPLE SECURITY PROCESSES BUILT INTO A WATERFALL SDLC



Adopting a holistic approach toward application and software security leads to better results since can align with information security and risk management already adopted by the organization. From information security perspective, the holistic approach toward application security should include for example security training for software developers as well as security officers and managers, integration with information

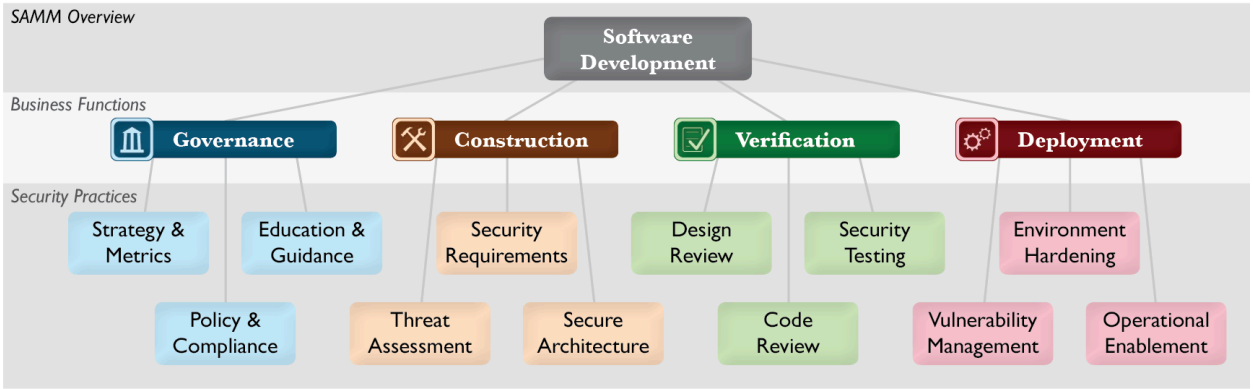
security and risk management, alignment with information security policies and technology standards and leveraging of information security tools and technologies used by the organization.

Software assurance maturity models

Besides of following a holistic approach toward application security that considers other domains it is also important for the CISO to consider what the organization capabilities are from day one in building software security and plan on how to integrate new activities in the future. Measuring the organizations capabilities in software security is possible today with software security maturity models such as the Build Security In Maturity Model (BSIMM) and the Open Software Assurance Maturity Model (SAMM). These models can also help the CISO in the assessment, planning and implementation of a software security initiative for the organization. These maturity models are explicitly designed for software security assurance. These models, even if are based upon empirical measurements, are feed from real data (e.g. software security surveys) hence allow to measure organizations against peers that already had implemented software security initiatives. By allowing their organization's secure software development software practices to be measured using these models, CISOs can compare their organization secure software development capabilities against other software development organizations to determine in which software security activities the organization either leads or lags.

For the software security activities for which the organization is lagging, BSIMM and SAMM measurements allow the CISO to construct a plan for software security activities to close these gaps in the future. It is important to notice that these models are not prescriptive that is, are not telling organizations what to do but rather to measure security activities in comparison with similar organizations in the field. The models are organized along similar domains, governance, intelligence, SSDL touch points, deployment for BSIMM and governance, construction, verification, deployment for SAMM. SAMM measurements are done in three best practices and three levels of maturity for each business function.

Figure 8 BUSINESS FUNCTIONS AND RELATED SECURITY PRACTICES WITHIN OPEN SOFTWARE ASSURANCE MATURITY MODEL (OWASP OPEN SAMM V1.0)



BSIMM measurements cover 12 best practices and 110 software security activities. The maturity levels help the CISO to plan for the organizational improvements in software security processes. Software security improvements can be measured by assigning goals and objectives to reach for each activity. For CISOs that either have already started to deploy a software security initiative such as S-SDLC within their organization or that just plan it in the future, the measurements that a model such as BSIMM and SAMM provide are important measurement yard sticks to determine in which application security activities to focus spending. If not already familiar with BSIMM and SAMM, CISOs can also refer to the Capability Maturity Model (CMM) and the various maturity levels to plan for the organization secure software development process capabilities.

Like BSIMM and SAMM, CMM is also an empirical model whose goal is improve the predictability, effectiveness, and control of an organization's software processes. In CMM for example, these are five levels that can be used to measure how the organization moves up to different levels of maturity of software engineering process: initial, repeatable, defined, managed, optimizing. In the first level (initial), the software engineering process is ad-hoc and used by the organization in uncontrolled and reactive manner. As the software development organization reaches level 2, the software development processes are repeatable and is possible to provide consistent results. When an organization reaches level 3, it means that it has adopted a set of defined and documented standard software development processes and these are followed consistently across the organization. At a level 4, that is managed, a software development organization has adopted metrics and measurements so that software development can be managed and controlled. When a software development organization is at level 5, optimized, the focus is on continually improving process performance through both incremental and innovative technological change and improvements in software development.

In reference to software security processes, at CMM Level 1 (Initial) CISOs have an ad-hoc process to "catch" and "patch" application vulnerabilities. At this level, the organization maturity in software security practice consists on running web application vulnerability scanning tool in reaction of events such as to validate the applications for compliance with PCI-DSS and OWASP Top 10. At CMM Level 2, the organization has already adopted standard processes for security testing applications for vulnerabilities including secure code reviews of the existing software libraries and components. At this level, the secure testing process can be repeated to produce consistent results (e.g. get same security issues if executed by different testers) but is not adopted across all software development groups within the same organization. At CMM Level 2, the application security processes are also reactive, that is, are not executed as required by the security testing standards. At CMM Level 3, application security processes are executed by following defined process standards and these are followed by all security teams within the same organization. At this level, application security processes are also proactive that means are executed to security test applications as part of governance, risk and compliance requirements prior to release into production. At level CMM 4 (managed) application security risks are identified and managed at different phases of the SDLC. At this level, the focus of security is the reduction of risks for all applications before these are released in production. At level CMM 5 (optimized), the application security processes are optimized for increased application coverage and for the highest return of investments in application security activities.

Security strategy

Strategy

"Strategy (Greek "στρατηγία"—stratēgia, "art of general, command, generalship") is a high level plan to achieve one or more goals under conditions of uncertainty. The art and science of planning and marshalling resources for their most efficient and effective use. Strategy is important because the resources available to achieve these goals are usually limited. Strategy is also about attaining and maintaining a position of advantage over adversaries through the successive exploitation of known or emergent possibilities rather than committing to any specific fixed plan designed at the outset."

Like with a general IT strategy most organizations should have a security strategy. It enables an organization to look beyond short-term tactical choices and develop strategic and long term planning. Because of the evolving cyber threat landscape it is important for CISOs to protect the information security assets for the threat of tomorrow. This strategy can guide operational decisions, plans and set priorities for the appropriate level of investment of resources to achieve your organization's goals.

Have a plan and be ready to change it

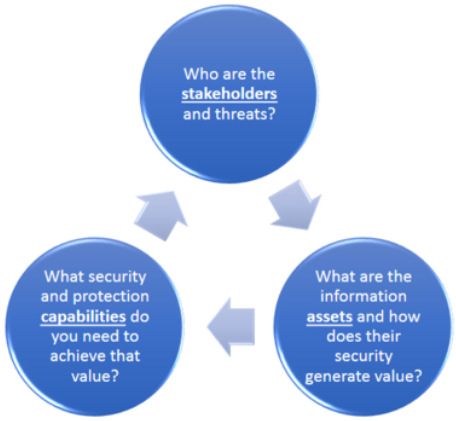
A security strategy will not cover all eventualities, but rather provide you with a good strategic framework. Furthermore, with time your environment or underlying assumptions will change and your strategy will need to constantly evolve and be adapted accordingly. It is better to define a strategy and revise it frequently,

adapting it to new circumstances, than to hold back developing your security strategy indefinitely, waiting for all information to become available.

To define the fundamentals of you security strategy, you should consider the following three general questions:

1. Stakeholders: Who are your key stakeholders and potential threat agents?
2. Assets: What are your information assets and how do they (and their protection) generate value for your clients inside and outside the organization?
3. Capabilities: What are the essential security and protection capabilities that the organization and its stakeholders need to deliver that value proposition?

Figure 9 THREE KEY QUESTIONS FOR THE SECURITY STRATEGY



How to define your organization's security strategy

As with all strategy documents you will analyze the impact of underlying assumptions and goals and derive your security strategy on how to achieve these goals.

Collecting input for developing your security strategy

In general the following inputs are useful in the process of defining your security strategy. Often organizations may not have all of them, or these inputs maybe in informal less accessible form (e.g. in the mind of some of your key employees in the organization). Or they might be outdated or not exactly matching what you are expecting. Devising a security strategy based on limited clarity of the overall strategy of an organization or missing pieces of information may be challenging. However, it is still better to develop some strategy and evolve it over time as more and more related information becomes available.

Figure 10 INPUTS FOR DEVELOPING THE SECURITY STRATEGY

1. Business strategy

CISOs should look first at the organization's business strategy such as the mission statement, the business goals as well as the other strategy components (see the following points) in support of these goals. For example, which parts of your operation are critically reliant on the confidentiality, availability and integrity of the information provided by the IT functions? What would be the impact on your Sales and Marketing in case of system failures or loss of prizing information, how dependent is the supply chain on the functioning IT backbone, can deliveries be made in case of failure, would fraud be spotted in case of security problems? Which parts of the value chain are susceptible to potential attacks? Which opportunities can certain security postures offer as a competitive advantage for the business (e.g. can a more robust security environment enable more e-commerce, higher dependency on IT processes and more efficiency)? Can procurement processes be dramatically changed, e.g. when allowing a BYOD (bring your own device) strategy? Are there new and potentially disruptive business cases possible due to secure and reliable application? How far can you allow some of your data to leave the immediate control of your organization (e.g. in case of cloud based applications)? How can you minimize the risks, by legal and technical controls? Are the resulting risk levels acceptable for the business?

2. Corporate strategy

How does your corporate strategy align with your IT and security strategy? Does your corporation aim for a decentralized or centralized organizational structure? How does this affect your ability to enforce central and local security policies? Are frequent corporate acquisitions and their integration an important part of your corporate strategy and how do you integrate new entities effectively and manage the security of these newly acquired corporate entities across the whole organization?

3. IT strategy & Review of the IT architecture

One important aspect of the security strategy is the alignment with the IT strategy for example depending on whether systems are decentralized or centralized, it will determine how and to which extend the organization can enforce central and local security policies. Further aspects are system architecture overview, trust boundaries, data flows, data in motion, and data at rest. How did your business strategy drive your IT strategy. What kind of IT assets and capabilities does your organization have and plan to develop going forward?

4. Compliance and legal requirements

5. Analyze your threats and risks

You need to understand how these risks affect your business operation and could possibly affect your business and business strategy. (See also part II of this guide)

6. Review of your current security status

Another important factor to consider before setting the security strategy is the maturity of the organization and the capabilities in the various security domains and specifically the application security domain. A maturity model such as OWASP openSAMM and the various activities in the Strategy and Metrics (SM) can also be used by CISOs to review the current security status and set goals. Specifically, by following the openSAMM model CISOs can start with level 1 (basic) SAMM activities such as "estimate the overall business risk profile" and "build and maintain assurance program roadmap"'. As the maturity of the organization grows, CISO can incorporate level 2 openSAMM activities such as "classify data and applications based on business risk", and "establish and measure per-classification security goals". Understanding the current security status of your organization will allow to develop a clear roadmap as one of the key components of a good security strategy going forward.

Components of your security strategy

A security strategy should contain or enable the following components:

1. General guiding principles & priorities

What security investments will the organization make over the next x months. In general most companies use a time period of 12 – 24 months for their strategy definitions. It would be advisable to have a main security strategy defined for 12 months, with a second longer term planning component for between 2 and 5 years, depending on the type of organization, that outlines security investment plans for the longer term. Of course in today's fast changing security arena, threats and risks can change very quickly and the plan should be adapted whenever underlying assumption change and be reviewed at least on a yearly basis.

2. Risk Management, risk acceptance levels

(see Part II)

3. Security Roadmap

To define your security roadmap, a good way is to look at the general company and IT roadmaps and combine this with a security roadmap derived from risk based assessments using maturity models like for example openSAMM.

4. Security architecture & Processes

What security properties does the overall system architecture present? What and where are the trust boundaries and underlying trust assumptions for your organization? Which are core security systems like authentication and authorization? How deep is the reliance on individual central and legacy systems, e.g. if you deploy single-sign-on or equivalents, how reliable is the central system managing all authorization controls?

Furthermore the security architecture needs to consider the attack surface and the exposure to cyber threats, specifically which parts of the application architecture and the functionality are susceptible to potential cyber attacks. And building on that is resiliency, hence the question is which security architecture is the most resilient in case of attacks, like for example DdoS, etc.

The procurement of security technology and services is a critical component of the security strategy, too. Questions to ask here are whether the procurement process addresses security risks introduced by the adoption of third part technology and what the organization can do to improve the security of third party processes and applications.

And in today's cloud based systems, data can often leave the security perimeter and flow through other networks (e.g. in the cloud) and systems. And the organization may have no or only very limited control on how this data is protected in such cloud applications.

5. Continuity of Business & Incidence Response

It is important that CISOs also develop a Continuity of Business (CoB) plan as part of the security strategy that takes into account possible system failures and the dependencies of the supply chain on the functioning IT infrastructure.

A security strategy should consider worst case scenarios and plan for security measures in advance. A proactive risk strategy is to answer questions about managing business impact before an incident actually occurs. For a service delivery business for example the question might be whether the application can still operate to guarantee delivery and fail securely.

Figure 11 ELEMENTS OF THE SECURITY STRATEGY

Conclusion

The overall goal for the security strategy is to minimize the risks and maximize the business benefits for the organization. The key question that the strategy must answer is whether security controls are sufficient and efficient enough to reduce the risk for the organization and the residual risks after security measures are applied are acceptable for the business.

Figure 12 ANALYSIS OF APPLICATION SECURITY ROADMAP DURATIONS (OWASP CISO SURVEY 2013)

Duration	%
1 year	35.59%
2 years	28.81%
3 months	10.17%
3 years	10.17%
5 years+	6.78%
6 months	8.47%
Grand Total	**100.00%**

Generally, most roadmaps have a duration of 1-2 years. The 2013 OWASP CISO Survey found that 64% of roadmaps projected for 1-2 years.

III-5 How to Choose the Right OWASP Projects For Your Organization

Depending on the overall security level and risk profile of the organization unit different tools and standards can be particularly useful for the CISO in advancing his or her security strategy.

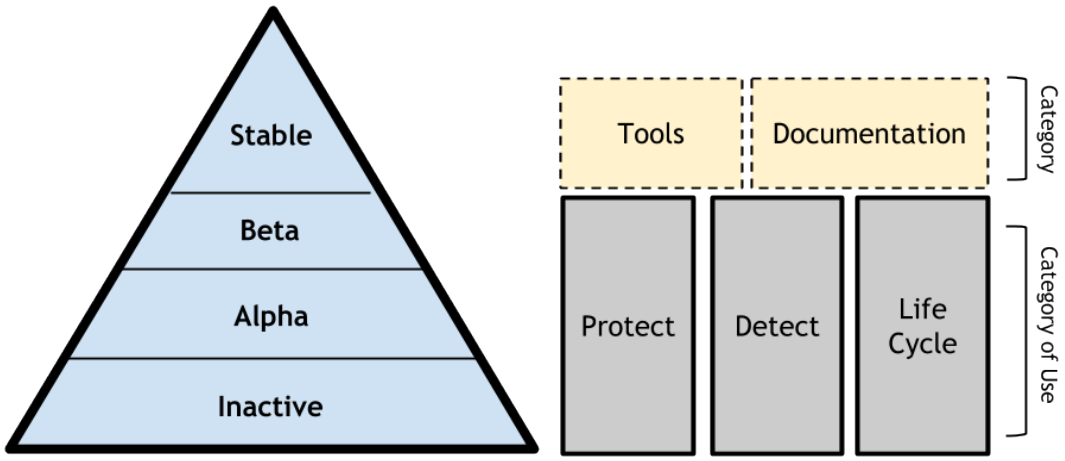
Note, following the risk discussions in the previous chapter, depending on the risk profile of different business units, the security strategy can actually be different based on their different individual risk scenarios and different regulatory requirements. For example a financial department may require a substantially stronger security posture, while an internal web page announcing the lunch menus of the cantine may be sufficiently protected with basic security measures (though to the authors knowledge in military settings, even the lunch menu can be considered as confidential information as further information about supply logistics etc. could be derived from that).

Based on these different risk profiles different tools and standards may be more relevant for the project and organizational unit in question.

Also note that OWASP provides several projects and guidance for CISOs to help in the development and implementation of software security development and security testing processes. Please refer to Appendix B for a quick reference to OWASP guides & projects.

In general tools can be classified in various categories (and so are also the OWASP projects).

Figure 13 AN ILLUSTRATION OF OWASP'S PROJECT CATEGORIES



Project's maturity

- Stable (a project or tool that is mature and constantly maintained to a good quality)
- Beta (relatively proven, though not to optimal quality)
- Alpha (this usually reflects a good first prototype, but still a lot of functionality may be missing or not up to standard)
- Inactive (former projects that have been retired or deprecated or that at some point have been abandoned).

Obviously for a CISO, the most interesting projects and tools would be stable and reliable ones. He can rely on a certain proven quality, and on them being available and maintained to a certain degree in the future days

to come. Beta projects can also be very valuable, as they may represent projects that have not finished their full review cycle yet but are already available for early adopters and can help to build good foundations for your security programs and tools going forward.

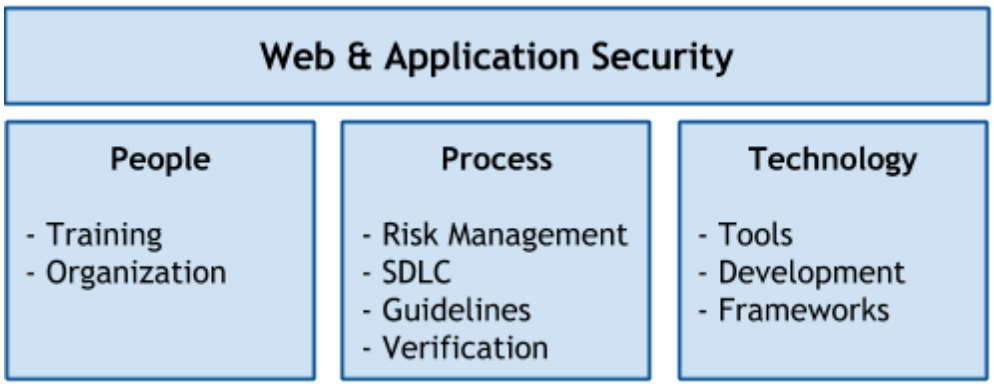
Project's categories

Usually OWASP projects are divided in either Tools or Documentation. And by the category of use: Builders, Breakers and Defenders. These categories can help the manager to quickly navigate the large portfolio of OWASP tools available and more easily find the right project for his current needs.

People, processes and technology

The CISO can also choose to achieve his security goals through three main ways. People, Processes and Technology. Managing the organization it is usually important to shape all three pillars to achieve the best impact throughout your organization. Focusing on only one or two of them can leave the organization vulnerable.

Figure 14 PEOPLE, PROCESSES AND TECHNOLOGY CONTROLS SUPPORT APPLICATION SECURITY



People

This will address the training and motivation of staff, suppliers, clients and partners. If they are well educated and motivated, the chances of malicious behavior or accidental mistakes can dramatically be reduced and many basic security threats can be avoided.

Processes

If an organization becomes more mature, the processes will be well defined and in fact channel and enable the work force to do things the "right way". Processes can ensure that the actions of the organization became reliable and repeatable. For example with well-defined standard operating procedures, the incident response process will be reliable and not rely on ad hoc decisions that would before have varied with the individual decision maker. In highly mature organizations, the business and IT processes will be constantly evaluated and improved. If a failure happens, improved processes can allow an organization as a whole to learn from past mistakes and improve its operation to more efficient and secure ways.

Technology

Technology can guide and support people by providing good training and knowledge, by being engaging and motivating to work with. Technology can facilitate an organization to follow sound security practices by providing good tools, while making difficult to deviate from the right path without detection. For example, good technology would automate access controls and authentication and make them very simple for the authorized user, while denying access or privileges to an unauthorized attacker. Finally, a number of automated tools can in the background help and support the people and organization in their work to defend against risks more effectively and more efficiently. Many of the security standards and tools (in OWASP and other bodies) can also be seen as focusing on parts of this framework. For example, staff training will enable the people to build their security understanding and do the right thing, while the various SDLC models can help an organization establish the right level of processes for its development and incident response mechanisms.

Part IV : Metrics For Managing Risks & Application Security Investments

IV-1 Executive Summary

CISOs need metrics to report to Senior Management the effectiveness of the application security program investment and its impact on business risk. CISOs also need metrics to manage and monitor the people, processes, and technologies that make up the application security program.

These metrics are made up of three categories. CISOs should be able to answer these questions based on the metrics and push her team to provide these in a near real-time basis through automated means. Critical questions include:

- Application security process metrics - How well is the organization meeting security policies, technical standards, and industry practices? How consistently are we executing security SLAs? By application? By division? By channel?
- Application security risk metrics
    - Vulnerability risk management metrics - What is the Mean Time to Repair on an annual basis? On a monthly basis? By application? By division? What are the known security issues in production?
    - Security incident metrics - What security issues have been exploited? Were they known issues that were released in production? What was the cost to the business?
    - Threat intelligence reporting and attack monitoring metrics - Which applications are receiving more attacks than others? Which applications have upcoming expected peak usage?
- Security in the SDLC metrics
    - Metrics for risk mitigation decisions - What is the Mean Time to Repair by an application's risk category? Does it meet expectations? What is the risk heat map by application? By division? By channel?
    - Metrics for vulnerability root causes identification - What are the root causes of vulnerabilities for each application? Is there a systemic issue? Which security practices have been best adopted by each development team? Which development teams need more attention?
    - Metrics for software security investments - Which SDLC phase have identified the most security issues? What is the maturity of the corresponding security practices in each SDLC phase? What is the urgency for more security people, process, and technologies in each SDLC phase?

Note OWASP provides several projects and guidance for CISOs to help measuring and monitor security and risks of application assets within the organization develop and implement an application security program. Besides reading this section of the guide, please consult the Appendix B: Quick Reference to OWASP Guides & Projects for more information on OWASP projects within the application risk management metrics & monitoring domain.

IV-2 Introduction

The aim of this part of the guide is to help CISOs manage the many aspects of an application security program – specifically risk and compliance, as well as application security resources such as processes, people and tools. One of the goals of application security metrics is to measure application security risks as well as compliance with application security requirements mandated by information security legislation, regulation and standards. Among critical application security processes that CISOs need to report on and manage are development processes and operational aspects such as application vulnerability management. It is often CISOs' responsibility to report the status of application security activities to senior management such as, for example, the status of application security testing and software security activities in the SDLC.

From a risk management perspective, it is important that application security metrics include reports on technical risks such as un-mitigated vulnerabilities for applications that are developed and managed by the organization. Another important aspect of the these metrics is to measure coverage, such as the percentage of the application portfolio regularly assessed in the application security verification program, the percentage of internal apps vs. external apps covered, the inherent risk of these applications and the type of security assessments performed, and when in the SDLC they are performed. These types of metric help CISOs in reporting on application security process compliance and application security risks to the head of the information security as well as to the application business owners.

Since one of CISOs' responsibilities is to manage both information security and application security risks and to make decisions on how to mitigate them, it is important for these metrics to be able to measure these risks in terms of risk exposure to the organization’s assets that include application data and functions.

IV-3 Application Security Process Metrics

Metrics and measurements goals

The goal of the application security process metrics is to determine how well the organization's application security processes meet the security requirements defined by application security policies and technical standards. For example, an application vulnerability process might include requirements to execute vulnerability assessments on internet facing applications every six or twelve months depending on the inherent risk rating of the application. Another vulnerability process requirement would be to execute security in multiple SDLC processes such as architecture risk analysis/threat modeling, static source code analysis/secure code reviews and risk based security testing on applications that store individuals' confidential information and whose business functionality is a critical service to citizens, clients, customers, employees, etc.

From the perspective of process coverage, one of the goals of these metrics might be to report on the coverage of application security process such as to measure how applications fall in scope for application security assessments to identify potential vulnerability assessment gaps based upon application type and the application security requirements. These help CISOs provide visibility on process coverage as well as the status of the operational execution of the application security programs. For example the metrics might show (e.g. in red status) that some of the application security processes in the SDLC such as secure code reviews are being not executed for a number of high risk rated applications and flag this as an out of compliance issue with the security testing requirements. This type of metric allows the CISO to prioritize resources by allocating them on where is most needed to comply with the standard process requirements.

Another important measurement for application security verification is to measure the time when the application security processes are scheduled versus when they are actually executed, to identify potential delays in security code review, static source code analysis, ethical hacking and application penetration testing processes.

IV-4 Application Security Risk Metrics

Vulnerability risk management metrics

CISOs' responsibilities include the management of application security risks. From a technical risk perspective, application security risks might be due to vulnerabilities in the applications that expose the application assets such as data and critical functions to potential attacks that seek to compromise these. Typically, technical risk management comprises mitigating the risks posed by vulnerabilities by applying fixes and countermeasures. The mitigation of the risk of these vulnerabilities is typically prioritized based upon the qualitative measurement of risks. For example, for each application that is developed and managed by the organization there would be a certain number of vulnerabilities identified at ranked by severity (e.g. high, medium and low). The greater the number of high and medium risk vulnerabilities, the higher is the risk to the application. The higher the value of the data assets protected by the application and the criticality of the functions supported, the higher the impact of these vulnerabilities on the application assets.

One important data point in vulnerability metrics is the number of vulnerabilities that remain unfixed. A given number of application vulnerabilities might still be "open", that is not yet fixed in the production environment, and these represent a risk to the organization and require the CISO to prioritize the risk mitigating actions such as "closing" the vulnerability within the compliance timeframes that is deemed acceptable by the application vulnerability management standards.

Security incident metrics

Another important metrics for CISOs managing information security risks is the reporting of security incidents relating to applications that are developed and/or managed by the organization. The CISO might gather this data reported from SIRT (Security Incident Response Team Incidents) that affect a given application due to the exploitation of a vulnerability. The correlation of the security incidents reported for a given application with the vulnerabilities reported by security testing allows the CISO to prioritize the risk mitigation effort on mitigating vulnerabilities that might cause the most impact to the organization. Obviously, waiting for a security incident to occur to decide which vulnerabilities to mitigate is symptomatic of a reactive rather than proactive approach toward risk management, but feedback is important.

Threat intelligence reporting and attack monitoring metrics

Risk proactive organizations do not wait for security incidents to occur but instead learn from other attacks, published vulnerabilities and threat intelligence, using the information to adjust severity and risk assessments, take proactive risk mitigation measures such as to develop and implement countermeasures, or prioritizing the mitigation of known higher risk known vulnerabilities that might potentially be exploited in an incident to cause the most impact to the organization. The CISO can use threat intelligence reports as well as metrics from monitored application layer security events such as from SIEM (Security Incident Event Management) systems and honeypot applications to assess the level of risk. Unfortunately today, most of security incidents are discovered and reported only months after the initial intrusion or data compromise. Security metrics that are actionable and targeted towards preventing risks of attacks is of critical importance for CISOs since it might facilitate deciding which applications to put under stricter monitoring and alerting in able to be able act more quickly in the case of an attack, reducing the impact of an event. For example,:

- A threat alert of a possible distributed denial of service against online banking applications might allow the CISO to put the organization on alert and prepare to roll out prepared countermeasures to prevent a subsequent outage
- A reported threat of malware targeting e-commerce applications to steal user credentials and conduct un-authorized purchases allows the CISO to issue monitoring alerts for the incident event monitoring management team.

- A published vulnerability in a software framework or library may alter the CISO's scheduling of patch testing, deployment and verification.

IV-5 Security in SDLC Management Metrics

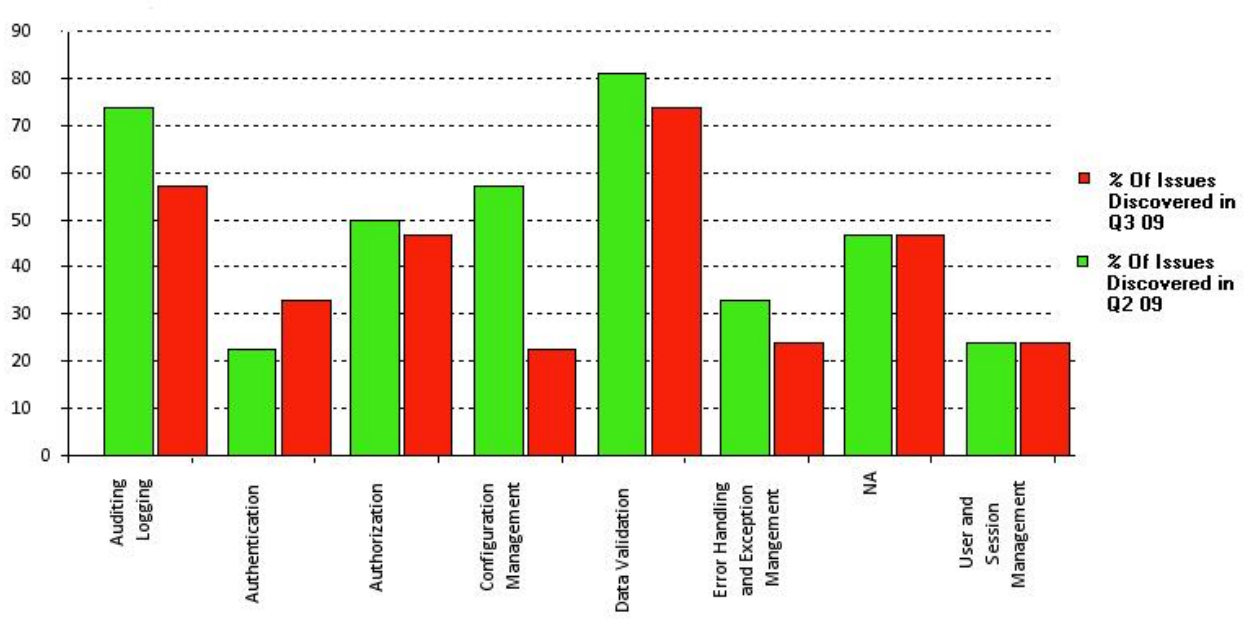
Metrics for risk mitigation decisions

Once vulnerabilities are identified at any stage of development and operation, the next step is to decide which should be fixed, when and how. The first question can be answered by the vulnerability assessment process compliance requirements that might state for example that high risk vulnerabilities are remediated in shorter time frames than medium and low risk vulnerabilities. The requirement might also vary depending on the type of application, being for example a totally newly developed application versus a new release of an existing application. As new applications have not been security tested previously, they represent a higher risk than existing applications and therefore this might require that high risk vulnerabilities to be mitigated prior to release of the application into the production. Once the issues are identified and prioritized for mitigation based upon the risk severity of the vulnerability, the next step is to determine how to fix the vulnerability. This depends on factors such as the type of the vulnerability, the security controls/measures that are affected by the vulnerability, and where the vulnerability is most likely being introduced. This type of metric allows the CISO to identify the root causes of vulnerabilities and present the case for remediation to the application development teams.

Metrics for vulnerability root causes identification

When the vulnerability metrics are reported as a trend, it allows CISOs to assess improvement. For example, in the case of a single issue measured over time for the same type of application, it is possible for the CISO to point to potential root causes. With trend vulnerability metrics and categorization of the type of vulnerabilities, it is possible for CISOs to make the business case for investing in certain types of security activities such as process improvements, adoption of testing tools as well as training and awareness. For example, the metrics showed in figure 1 shows positive trends of certain type of vulnerabilities by comparing two quarterly releases of the same applications. Application security improvements measured as a reduced number of vulnerabilities identified from one quarterly release to another is observed for most vulnerability types except for authentication and user/session management issues.

Figure 15 EXAMPLE VULNERABILITY CATEGORIZATION TREND CHART



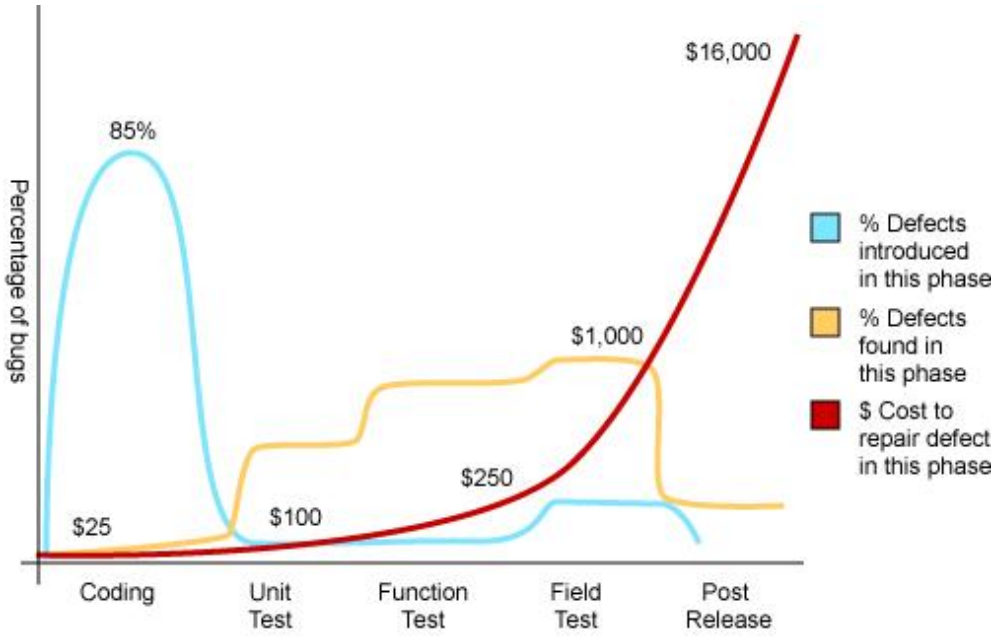
CISOs might use these metrics to discuss with CIOs and development directors on whether the organization is getting better or worse over time in releasing more secure application software, and to direct the application security resources (e.g. process, people and tools) to where they are most needed for reducing risks. With the metrics shown in Figure 1 for example, assuming the application changes introduced between releases do not differ much in term of type and complexity, as well as the number and the type of software developers in the development team, and the tools used, a case can be made on focusing on the type of vulnerabilities that the organization is having trouble fixing such as better design and implementation of authentication and user/session management controls. The CISO might then coordinate with the CIO and the development directors to schedule a targeted training on these types of vulnerabilities, document development guides for authentication and session management and adopt specific security test cases. Ultimately this coordinated effort will empower software developers in designing, implementing and testing more secure authentication and session management controls and show these as improvements in the vulnerability metrics.

Metrics for software security investments

Another important aspect of the S-SDLC security metrics is to decide where in the SDLC to invest in security testing and remediation. To know this, it is important to measure in which phase of the SDLC the most of vulnerabilities (higher percentage of issues) originate, when these vulnerabilities are tested and how much it cost the organization to fix them in each phase of the SDLC. A sample metric that measure this is shown in the figure below based upon a case study on the costs of testing and managing software bugs (Ref Capers Jones Study).

These metrics can also be used to assist the proper allocation of security investment between application and infrastructure.

Figure 16 CHART ILLUSTRATING HOW THE COST OF TESTING AND MANAGING SOFTWARE BUGS VARY WITH STAGE OF SDLC



Source: Applied Software Measurement, Capers Jones, 1996

A similar type of security defect management metrics can be used by CISOs for managing security issues effectively by reducing overall security costs. Assuming the CISO has rolled out security throughout all SDLC

process and has budget allocated for investment in security in the SDLC activities such as secure coding training and secure code review process and static code analysis tools, these metrics allows the CISO to make that case for investing in testing and fixing security issues in the early phases of the SDLC. This is based upon the following measurements from this case study:

- Most of the vulnerabilities are introduced by software developers during coding,
- The majority of these vulnerabilities are tested during field tests prior to production, and
- Testing and fixing vulnerabilities late in the SDLC is the most inefficient way to do it since is approx. ten times more expensive to fix issues during pre-production tests than during unit tests.

CISOs can use vulnerability case studies like these or use their own metrics to make the case for investing in secure software development activities since these will save the organization time and money.

Supporting Information

References

Metrics and Benchmarking

In order of report release date.

2013

- Verizon 2013 Data Breach Investigation Report: http://www.verizonenterprise.com/DBIR/2013/
- Security Innovation and the Ponemon Institute: The Current(2013) State of Application Security report:https://www.securityinnovation.com/security-lab/our-research/current-state-of-application-security.html

2012

- Security Innovation and Ponemon Institute's 2012 Application Security Gap Study: A Survey of IT Security & Developers: https://www.securityinnovation.com/uploads/Application%20Security%20Gap%20Report.pdf

2011

- Verizon 2011 Data Breach Investigation Report: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf
- US Q2 2011 GDP Report Is Bad News for the US Tech Sector, But With Some Silver Linings: http://blogs.forrester.com/andrew_bartels/11-07-29-us_q2_2011_gdp_report_is_bad_news_for_the_us_tech_sector_but_with_some_silver_linings
- Imperva's July 2011 Web Application Attack Report: http://www.imperva.com/docs/HII_Web_Application_Attack_Report_Ed1.pdf

2010

- First Annual Cost of Cyber Crime Study Benchmark Study of U.S. Companies, Sponsored by ArcSight Independently conducted by Ponemon Institute LLC, July 2010: http://www.arcsight.com/collateral/whitepapers/Ponemon_Cost_of_Cyber_Crime_study_2010.pdf
- 2010 Annual Study: U.S. Cost of a Data Breach: http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach

2009 and prior

- OWASP Security Spending Benchmarks Project Report: https://www.owasp.org/images/b/b2/OWASP_SSB_Project_Report_March_2009.pdf
- Identity Theft Survey Report, Federal Trade Commission,September, 2003: http://www.ftc.gov/os/2003/09/synovatereport.pdf

Standards

- PCI DSS: https://www.pcisecuritystandards.org/security_standards/index.php
- OWASP Application Security Verification Standard https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

Guidelines and Best Practices

- OWASP Top Ten: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Supplement to Authentication in an Internet Banking Environment: http://www.fdic.gov/news/news/press/2011/pr11111a.pdf
- Feiman, Joseph. Teleconference on Application Security. 9 Oct. 2008. Gartner. 30 Sept. 2013 http://www.gartner.com/it/content/760400/760421/ks_sd_oct.pdf

Security Incidents and Data Breaches

- Data Loss Database: http://datalossdb.org/
- WHID, Web Hacking Incident Database: http://projects.webappsec.org/w/page/13246995/Web-Hacking-Incident-Database
- Sony data breach could be most expensive ever: http://www.csmonitor.com/Business/2011/0503/Sony-data-breach-could-be-most-expensive-ever
- Dmitri Alperovitch, Vice President, Threat Research, McAfee, Revealed: Operation Shady RAT: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf
- Health Net discloses loss of data to 1.9 million customers: http://www.computerworld.com/s/article/9214600/Health_Net_discloses_loss_of_data_to_1.9_million_customers
- Albert Gonzalez data breach indictment: http://www.wired.com/images_blogs/threatlevel/2009/08/gonzalez.pdf
- Share prices and data breaches: http://www.securityninja.co.uk/data-loss/share-prices-and-data-breaches/
- EMC spends $66 million to clean up RSA SecureID mess: http://www.infosecurity-us.com/view/19826/emc-spends-66-million-to-clean-up-rsa-secureid-mess/

Security Investments and Budgets

- Gordon, L.A. and Loeb, M.P. "The economics of information security investment", ACM Transactions on Information and Systems Security, Vol.5, No.4, pp.438-457, 2002.
- Total Cost of Ownership: http://en.wikipedia.org/wiki/Total_cost_of_ownership
- Wes SonnenReich, Return of Security Investment, Practical Quantitative Model: http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf
- Tangible ROI through Secure Software Engineering: http://www.mudynamics.com/assets/files/Tangible%20ROI%20Secure%20SW%20Engineering.pdf
- The Privacy Dividend: the business case for investing in proactive privacy protection, Information Commissioner's Office, UK, 2009: http://www.ico.gov.uk/news/current_topics/privacy_dividend.aspx
- A commissioned study conducted by Forrester Consulting on behalf of VeriSign: DDoS: A Threat You Can't Afford To Ignore: http://www.verisigninc.com/assets/whitepaper-ddos-threat-forrester.pdf

- The Security Threat/Budget Paradox: http://www.verizonbusiness.com/Thinkforward/blog/?postid=164
- Security and the Software Development Lifecycle: Secure at the Source, Aberdeen Group, 2011 http://www.aberdeen.com/Aberdeen-Library/6983/RA-software-development-lifecycle.aspx
- State of Application Security - Immature Practices Fuel Inefficiencies, But Positive ROI Is Attainable, Forrester Consulting, 2011 http://www.microsoft.com/downloads/en/details.aspx?FamilyID=813810f9-2a8e-4cbf-bd8f-1b0aca7af61d&displaylang=en
- Dan E Geer Economics and Strategies of Data Security: http://www.amazon.com/Economics-Strategies-Data-Security-DANIEL/dp/B001LZM1BY

About OWASP

Description

OWASP is a global open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted. OWASP builds documents, tools, teaching environments, guidelines, checklists, and other materials to help organizations improve their capability to produce secure code. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security.

OWASP was formed in 2001, in an entirely organic fashion, when a group of security professionals came to realize how terribly insecure the way we develop our web applications was. The initial goal was deemed to be modest: write a guide for developers, which would document secure software development practices. While the initial effort was meant to last a few weeks, it came out to several hundred pages. When released, the OWASP Guide to Building Secure Web Applications was an instant success. The OWASP Guide Series now encompasses six documents.

OWASP is a place where good people gather to help increase the awareness of the security problems in applications. It is a grass-roots effort, with the driving force being the people who are dealing with these problems every day, and wanting to lend a hand to change the situation for the better. The OWASP Foundation is a not-for-profit entity that ensures the project's long-term success.

The OWASP Foundation is a US 501(c)(3) not-for-profit organization. OWASP Europe VZW is a non-profit organization registered in Belgium.

Participation

Everyone is welcome to participate in our forums, projects, chapters, and conferences. OWASP is a fantastic place to learn about application security, to network, and even to build your reputation as an expert. All OWASP's documents, tools and other resources are published using open source licenses, and are available free of charge.

Local Chapters

OWASP has almost 200 local chapters around the world. Chapter meetings are always free to attend, are vendor neutral and the presentations are made available free-of-charge on each chapter's web page. The meetings help foster local discussion of application security around the world.

To find your nearest local chapter, information on how to start a new one, and how to run a chapter see https://www.owasp.org/index.php/OWASP_Chapter and https://www.owasp.org/index.php/Chapter_Leader_Handbook

AppSec Conferences

For the last ten years, OWASP AppSec conferences bring together industry, government, security researchers, and practitioners to discuss the state of the art in application security. Global AppSec conferences are held annually in North America, Latin America, Europe, and Asia Pacific. Additionally, regional events are held in locations such as Brazil, China, India, Ireland, Israel, and Washington D.C. Presentation slides and video recordings are available free of charge on the OWASP website after each conference.

For upcoming global and regional events see
https://www.owasp.org/index.php/Category:OWASP_AppSec_Conference

Citations

To find almost 80 national and international Legislation, standards, guidelines, committees and industry codes of practice that refer to OWASP see https://www.owasp.org/index.php/Industry:Citations

Helping to Support OWASP's Mission

Many organizations have been corporate or education supporters. many more have encourage their employees to contribute time and resources to OWASP Projects.

OWASP has also produced six guidance documents for other groups, suggesting how they could best support OWASP's mission. These are known as the OWASP Application Security Codes of Conduct, for government bodies, educational institutions, standards groups, trade organizations, certifying bodies, and development organizations. The Codes of Conduct can be downloaded from the project page
https://www.owasp.org/index.php/OWASP_Codes_of_Conduct

Contact

Our global address for general correspondence is:

FAO Kate Hartmann

OWASP Foundation

1200-C Agora Drive, #232

Bel Air, MD 21014

United States

The European correspondence address is below:

OWASP Europe VZW

Leinstraat 104A

B-9660 Opbrakel

Belgium

Or phone Kate Hartmann at +1 301-275-9403 or use the contact form at http://sl.owasp.org/contactus

CISO Guide Appendixes

Appendix A: Value of Data & Cost of an Incident

Introduction

This is quick reference for providing guidance on how to assign monetary value to information assets to determine the monetary impact for the organization in the case of such assets will be lost because of a security incident. Included in this appendix are also a simple formula to determine the potential liability risk in case of data loss incidents and a data breach calculation tool to estimate the cost of a data breach based upon statistical data.

Value of Information

The selection of security measures must consider the value of asset being protected. Like personal data, all types of data can have value determined from a number of different perspectives. While it may be most common the look at the value of data by its value as an asset to the organization or the cost of an incident, these are neither always the most appropriate nor greatest valuations to consider. For example, a report looking at the value of personal data (personally identifiable information) suggests four perspectives from which personal information draws its privacy value. These are:

- Its value as an asset used within the organization's operations
- Its value to the individual to whom it relates
- Its value to other parties who might want to use the information, whether for legitimate or improper purposes
- Its societal value as interpreted by regulators and other groups.

The value to the subject of the data, to other parties or to society may be more appropriate for some organizations than others. The report also examines the wider consequences of not protecting (personal) data and the benefits of protection. It describes how incidents involving personal data that lead to financial fraud can have much larger impacts on individuals, but that financial effects are not the only impact. The report provides methods of calculation, and provides examples where the value of an individual's personal data record could be in the £500-£1,100 (approximately $800-$1,800) in 2008.

Data Breaches and Monetary Losses

Regarding the monetary loss per victim, exact figures vary depending on the factors that are considered to calculate them depending by the type of industry and the type of attack causing the data loss incident. According to a July 2010 study conducted by Ponemon Institute on 45 organizations of different industry sectors about the costs of cyber attacks, the costs of web-based attacks is 17% of the annualized cyber-attack costs. This cost varies across different industry sectors with the higher costs for defense, energy and financial services ($16.31 million, $15.63 million and $12.37 million respectively) than organization in retails, services and education.

Also according to the 2011 Ponemon Institute annual survey of data loss costs for U.S. companies, the average cost per compromised record in 2010 was $214 up 5% from 2009. According to this survey, the communication sector bear the highest cost of $380 per customer record with financial services the second highest cost of $353 followed by healthcare with $345, media, at $131, education at $112 and the public sector at $81.

The security company Symantec, which sponsored the report, developed with Ponemon Institute a data breach risk calculator that can be used to calculate the likelihood of data breach in the next 12 months, as well as to calculate the the average cost per breach and average cost per lost record.

The Ponemon institute direct costs estimates, are also used for estimating the direct cost of data breach incidents collected by OSF DataLossDB. 2009 direct cost figures of $60.00/record are multiplied by the number of records reported by each incident to obtain the monetary loss estimate. It is assumed that direct costs are suffered by the breached organizations while this is not always true such as in the case of credit card number breaches where the direct costs can often be suffered by banks and card issuers. Furthermore, estimate costs does not include indirect costs (e.g. time, effort and other organizational resources spent) as well as opportunity costs (e.g. the cost resulting from lost business opportunities because of reputation damage).

Another possible way to make a risk management decision on whether to mitigate a potential loss is to determine if the company will be legally liable for that data loss. By using the definition of legal liability from a U.S. liability case law, given as Probability (P) of the loss, (L) the amount of the Loss, then there is liability whenever the cost of adequate precautions or the Burden (B) to the company is:

B < P x L

By applying this formula to 2003 data from the Federal Trade Commission (FTC) for example, the probability of the loss is 4.6% as the amount of the population that suffered identity fraud while the amount of the loss x victim can be calculated by factoring how much money was spent to recover from the loss considering the time spent was 300 million hours at the hourly wages of $ 5.25/hr plus out of pocket expenses of $ 5 billion:

L = [Time Spent x Recover From Loss x Hourly Wage + Out Of Pocket Expenses] / Number of Victims

With this formula for calculating the amount of loss due to an identity fraud incident, based upon 2003 FTC data, the loss per customer/victim is approximately $ 655 dollars and the burden imposed to the company is $ 30.11 per customer/victim per incident.

The risk management decision is then to decide to whether it is possible to protect a customer for $ 30.11 per customer per annum. If it is, then liability is found and there is liability risk for the company. This calculation can be useful to determine the potential liability risk in case of data loss incidents, for example by applying the FTC figures to the TJX Inc. incident of 2007 where it was initially announced the exposure of confidential information of 45,700,000 customers, the exposure to the incident for the victims involved could be calculated as:

Cost exposure to the incident = Number of victims exposed by the incident x loss per victim

With this formula using TJX Inc data or number of victims affected and by applying the loss per victim using FTC data, the cost of the incident that represents the loss potential is $ 30 Billion. By factoring this with the probability of the incident occurring, then it is possible to determine how much money should be spend in security measures. In the case of TJX Inc incident for example, assuming a 1 in 1000 chance of occurrence a $ 30 Million security program for TJX Inc would have been justifiable.

Data Breach Calculation Tools

A calculator for estimating the cost incurred by organizations, across industry sectors, after experiencing a data breach is provided by Symantec based upon data surveys of the Ponemon Institute:

https://databreachcalculator.com/

Estimating the Probability of Vulnerability Exploits

To estimate the probability of a specific web application vulnerability exploit, we can refer to data reports from the Web Hacking Incident Database (WHID). The WHID is a Web Application Security Consortium (WASC) project to provide statistical analysis information of web application security incidents collected from public sources. in 2010 WHID categorized 222 incidents and observed that 33% of the incidents aimed to take down web sites (e.g. with Denial of Service), 15% aimed to deface web sites and 13% to steal information. Among the overall type of attacks the ones that sought to exploit application vulnerabilities such as SQL injection were 21%.

By using 2010 WHID data of reported incident and analysis, the overall probability of an attack aimed to steal information by exploiting of a SQL injection vulnerability is therefore 13 % x 21 % = 2.7%. Since SQL injection was also reported to be used for defacement, this ought to be considered as rough estimate.

In another survey of malicious web attack traffic observed over a period of six months, December 2010 through May 2011 from the security company Imperva, SQL injection was identified in 23% of the attacks as third most prevalent after cross site scripting, the second most prevalent in 36% of the attacks and directory traversal as the most prevalent in 37% of all the attacks.

Estimating the Business Impact of Vulnerability Exploits

By comparing WHID and Imperva web attack surveys, an order of magnitude of 21-23% for attacks exploiting SQL injection vulnerability seems an acceptable rough estimate. By assuming the cost of data loss of security incident for a financial organization of $355/record (Ponemon Institute 2010 data), and that the probability that such incident exploits a SQL injection vulnerability is 2.7% (WHID 2010 data), the 2010 liability for a company's web site such as online banking for a data loss of 1 million records is thus $ 9,585,000. With this figures a 2010 budget of $9 Million spent by a financial organization for application security measures specifically focused to prevent risks of data losses due to SQL injection attacks would have been justifiable.

Assuming that you will spend as much in security measures, this is the maximum amount estimated for expenses in security measures to thwart SQL injection attacks that includes acquisition of technology for secure software development, documentation, standards, processes, tools as well costs for the recruitment of qualified personnel and secure coding training especially for web developers. Normally this dollar figure ought to be considered a maximum value since assumes for example a total loss of the user data.

It is important to notice that injection vulnerabilities are considered by OWASP (2013 A1-Injection) the most critical application security risks for opportunistic vulnerability exploits. OWASP rates the risk of data injection, including SQL injection vulnerability, as severe since "can result in data loss or corruption, lack of accountability, or denial of access and sometimes lead to complete host takeover". The business impact that we calculated as liability for a medium size financial services company (1 million registered online banking users) assumes that the value of the data assets can be stolen by a threat agent to cause tangible harm to the company.

Historically, SQL injection attacks have been of high impact and in the United States, have been associated with the largest data breach incidents ever committed and prosecuted. In the August 2009 U.S. indictment case against Albert Gonzalez (also indicted in May 2009 in Massachusetts for the TJX Inc breach) and other two Russian hackers, SQL injection attacks were used to break into 7-Eleven network in August 2007 resulting in the theft of credit card data. Allegedly, the same kind of attack was also used to infiltrate Hannaford Brothers in November 2007 which resulted in 4.2 million debit and credit card numbers being stolen and to steal 130 million credit card numbers from Heartland Payment Systems on December 2007. In 2010, Albert Gonzalez was found guilty and sentenced to serve 20 years in federal prison while Heartland paid about $ 140 million in fines and settlements because of the security breach.

Summary

We can see that there are different ways to determine the value of information and that some of these are purely based on the costs relating to data breaches. But overall, the references suggest that typically individual's data can be valued in the range $500 to $2,000 per record.

Appendix B: Quick Reference to OWASP Guides & Projects

This quick reference maps typical CISO's functions and information security domains to different sections of the OWASP' CISO Guide and relevant OWASP projects.

Table 2 CISO FUNCTIONS MAPPED TO OWASP GUIDES AND OTHER PROJECTS

CISO Function	Security Domain	OWASP CISO Guide	OWASP Projects
Develop and implement policies, standards and guidelines for application security	Standards and Policies	I-3 "Information Security Standards, Policies and Compliance"	• Development Guide - Policy Frameworks • Project CLASP - Identify Global Security Policy • Project SAMM - Policy & Compliance • Code Review Guide - Code Reviews and Compliance
Develop, implement and manage application security governance	Governance	III-3 "Application Security Governance, Risk and Compliance"	• Project SAMM - Governance • Project ASVS - How to Write Job Requisitions
Develop and implement software security development and security testing processes	Security Engineering Processes	III-4 "Targeting Software Security Activities and S-SDLC Processes" III-5 "How to Choose the Right OWASP Projects and Tools For Your Organization"	• Development Guide • Code Review Guide • Secure Coding Practices • Testing Guide • Comprehensive Lightweight Application Security Process (CLASP) Introduction • CLASP Concepts • Software Assurance Maturity Model (SAMM) • Testing Guide - Tools • Project Application Security Verification Standard Project (ASVS)
Develop, articulate and implement a risk management strategy for applications	Risk Strategy	I-4 "Risk Management Strategies" II "Criteria for Managing Application Security Risks" III-4 "Security Strategy"	• SAMM - Strategy & Metrics • Application Threat Modeling - Risk Mitigation Strategies
Work with executive management, business managers and internal audit and legal counsel to define application security requirements that can be verified and audited	Audit & Compliance	I-3 "Capturing Application Security Requirements" III-3 "Addressing CISO's Application Security Functions"	• Application Security Verification Standard • CLASP - Capture Security Requirements • SAMM - Security Requirements • Testing Guide - Security Requirements Test Derivation • Project OWASP Cornucopia • Project Secure Software Contract Annex
Measure and monitor security and risks of application assets within the organization	Risk Metrics & Monitoring	IV "Metrics for Managing Risks & Application Security Investments"	• CLASP - Define and Monitor Metrics • SAMM - Strategy & Metrics • Types of Application Security Metrics
Define, identify and assess the inherent security of critical application assets, assess the threats, vulnerabilities, business impacts and recommend countermeasures/corrective actions	Risk Analysis & Management	I-4 "Risk Management" II "Criteria for Managing Application Security Risks"	• Project Top Ten Web Application Risks • Project Top Ten Mobile Application Risks • Project Top Ten Cloud Risks • ASVS - Implementation of NIST Risk Management Verification Activities • Risk Rating Methodology • Threat Risk Modelling • Application Threat Modelling
Assess procurement of new application processes, services, technologies and security tools	Procurement	III-4 "Assess Risks before Procurement of Third Party Components/Services"	• Project Secure Software Contract Annex • ASVS - Verification of Contract Requirements

CISO Function	Security Domain	OWASP CISO Guide	OWASP Projects
Oversee the training on application security for development, operational and information security teams	Security Training	III-5 "People, Processes and Technology"	• Project CLASP - Institute Awareness Programs • Education Projects • Appsec Training Videos • Conference Videos • Application Security FAQs • CLASP - Institute Security Awareness Program
Develop, articulate and implement continuity planning/disaster recovery	Business Continuity / Disaster Recovery	III-3 "Addressing CISO's Application Security Functions"	• Cloud Business Continuity and Resiliency
Investigate and analyse suspected and actual application security incidents and recommend corrective actions	Vulnerability Management & Incident Response	I-4 "Addressing the Business Concerns after a Security Incident"	• SAMM Vulnerability Management • CLASP - Manage Security Issue Disclosure Process • .NET Incident Response

Guides

- Development Guide
  https://www.owasp.org/index.php/Category:OWASP_Guide_Project
  - Policy Frameworks
    https://www.owasp.org/index.php/Policy_Frameworks
- Code Review Guide
  https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project
- Standards Guide
  - Application Security Verification Standard (ASVS)
    https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
    - Implementation of NIST Risk Management Verification Activities
      https://www.owasp.org/index.php/How_to_bootstrap_the_NIST_risk_management_framework_with_verification_activities
    - Verification of contract requirements
      https://www.owasp.org/index.php/How_to_specify_verification_requirements_in_contracts
- Testing Guide
  https://www.owasp.org/index.php/OWASP_Testing_Project
  - Code reviews and compliance
    https://www.owasp.org/index.php/Code_Reviews_and_Compliance
  - Security requirements test derivation
    https://www.owasp.org/index.php/Testing_Guide_Introduction#Security_Requirements_Test_Derivation
  - Tools
    https://www.owasp.org/index.php/Appendix_A:_Testing_Tools
  -

Other projects

- Application Security FAQs
  https://www.owasp.org/index.php/OWASP_Application_Security_FAQ

- Application Threat Modeling
  https://www.owasp.org/index.php/Application_Threat_Modeling
  - Mitigation strategies
    https://www.owasp.org/index.php/Application_Threat_Modeling#Mitigation_Strategies
- AppSec Training Videos
  https://www.owasp.org/index.php/OWASP_Appsec_Tutorial_Series
- CLASP
  - Capture Security Requirements
    https://www.owasp.org/index.php/Category:BP3_Capture_security_requirements
  - Concepts
    https://www.owasp.org/index.php/CLASP_Concepts
  - Define and monitor metrics
    https://www.owasp.org/index.php/Category:BP6_Define_and_monitor_metrics
  - Identify global security policy
    https://www.owasp.org/index.php/Identify_global_security_policy
  - Institute Awareness Programs
    https://www.owasp.org/index.php/Category:BP1_Institute_awareness_programs
  - Introduction
    https://buildsecurityin.us-cert.gov/articles/best-practices/requirements-engineering/introduction-to-the-clasp-process
  - Manage Security Issue Disclosure Process
    https://www.owasp.org/index.php/Manage_security_issue_disclosure_process
- Cloud Business Continuity and Resiliency
  https://www.owasp.org/index.php/Cloud-10_Business_Continuity_and_Resiliency
- Conference videos
  https://www.owasp.org/index.php/Category:OWASP_Video
- Cornucopia
  https://www.owasp.org/index.php/OWASP_Cornucopia
- Education projects
  https://www.owasp.org/index.php/Category:OWASP_Education_Project
- .NET Incident Response
  https://www.owasp.org/index.php/.NET_Incident_Response
- Risk rating methodology
  https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
- SAMM
  http://www.opensamm.org/
  - Governance
    https://www.owasp.org/index.php/SAMM_-_Governance
  - Policy & Compliance
    https://www.owasp.org/index.php/SAMM_-_Policy_&_Compliance_-_1
  - Security Requirements
    https://www.owasp.org/index.php/SAMM_-_Security_Requirements_-_1
  - Strategy & Metrics
    https://www.owasp.org/index.php/SAMM_-_Strategy_&_Metrics_-_1
  - Vulnerability Management
    https://www.owasp.org/index.php/SAMM_-_Vulnerability_Management_-_1
- Secure Coding Practices
  https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
- Secure Software Contract Annex
  https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

- Threat risk modeling
  https://www.owasp.org/index.php/Threat_Risk_Modeling
- Top Ten Cloud Risks
  https://www.owasp.org/index.php/OWASP_Cloud_%E2%80%90_10/Initial_Pre-Alpha_List_of_OWASP_Cloud_Top_10_Security_Risks
- Top Ten Mobile Application Risks
  https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks
- Top Ten Web Application Risks
  https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Projec
- Types of Application Security Metrics
  https://www.owasp.org/index.php/Types_of_application_security_metrics