OWASP Application Security Guide for CISOs

Part I: Business cases and risk-cost criteria for application security spending

In the digital era, banks and financial institutions serve an increasing number of customers through web online and mobile banking applications. These are feature rich applications: online banking applications for example, allow banking customers opening of accounts, paying bills, applying for loans, transferring money between accounts and between financial institutions, viewing account balances and recent transactions, downloading bank statements and viewing check images of paid checks. The online banking experience is convenient for customers: it allow them to perform the same bank transactions as being at the branch but with convenience to be remote from their home PC or their mobile phone. At the same time, this convenience comes at a price for banks since online banking sites become the target of increased number of attacks from hacking and malware. The goal of these attacks is the unauthorized acquisition of sensitive data that includes online banking passwords, bank account data, credit and ATM cards data and least but not last, alteration of on-line financial transactions such as transfers and transfers of money to commit fraud. By recent statistical data of security incidents such as the Verizon's 2011 data breach investigations report [1] for example, hacking and malware are the most prominent type of attacks and stolen passwords and credentials pose the major threat to financial institutions.

To cope with this increase in hacking and malware attacks, Chief Information Security Officers (CISOs) are called to roll out security measures to mitigate the risks and investments in application security an even larger portion of the overall information security and information technology budgets. Nevertheless, making the business case for increasing the budget on application security today still represents some challenges especially when competing with the same budget allocated for application development of new features for online banking sites that could retain and attract new customers as well as expand the profitability of the bank.

Moreover, in today's recession economy and in a scenario of slow growth in business investments including the company's built-in software (Ref [2]), it is increasingly important for CISOs to articulate the "case" for investment in application and software security. Typically, application security budget allocation include the development of new countermeasures at the application layer for mitigating risks of hacking and malware and limit the occurrence of future data breach incidents. This increased spending in risk mitigation measures add on to other security costs such as cost for governance to comply with new security guidelines such as, in the case of the banking sector, the new Federal Financial Institutions Examination Council ("FFIEC") guidelines for online authentication (Ref [3]).

CISOs can build a business case for application security budget today for different reasons, some directly tailored to the specific company risk culture or appetite for risk others, including using application security surveys (refer to OWASP CISO survey here TBD).

Specifically, (based by the OWASP CISO survey) the most popular business cases for budget increase in application security spending today need to satisfy, at minimum, the following company needs:

1. **Mitigation of new hacking and malware threats and if being hacked to prevents other similar data breaches/incidents to occur**
2. **Meeting of new compliance requirements (e.g. new 2011 FFIEC authentication in the banking environment guideline's addendum)**

Nevertheless, assuming the business case is made with the points 1 and 2 herein, CISOs today still have the difficult task to justify "how much" money should the company spend for application security and "where" to spend it. .Regarding the how much is boils down to how much is needed to mitigate the risks or to reduce the residual risks to an acceptable value for the business.

Both for real risks (e.g. incidents) and for compliance risks (e.g. unlawful non-compliance), the question for CISO is also what is the most efficient way to spend the application security budget today or which application security process, activity tools yields the company "more bang for the money". Regarding the "where" it comes down to budget properly different application security and risk domains, to name the most important ones: governance, risk management, identity management and access control, network security and infrastructure, detection and incident management and last but not least the security of applications and software development projects. Since as 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.

From the perspective of "governance" for example, allocation of application security budget might represent an opportunity to move on from compliance to risk mitigation. Sites that carry out payment transactions with credit cards at the level of "merchant" for example, are subject to compliance with the PCI-DSS (Ref [4]). PCI-DSS has provisions for the development and maintenance of secure systems and applications (requirement # 6), for testing security systems and processes (requirement # 11) and for the test of web application for common vulnerabilities (requirement 11.3.2) such as the OWASP Top Ten (Ref [5]).

The need of compliance with the PCI-DSS requirements can be a reason to justify an additional investment in technology and services for security testing: examples include source code security reviews with SAST (Static Analysis Security Tests) assessment/tools and application security reviews with DAST (Dynamic Analysis Security Tests) assessments/tools.

Another important factor for the "where" is to adopt the "executive perspective" in IT investment for technology. Today, company executives at CIO and CISO level seldom follow the recommendations of the trusted analyst sources such as Gartner and Forrester when making investments in application security technology. Gartner (Ref[6]) for example, few years ago predicted that investment in firewalls, IDS, VPN and access controls were no longer sufficient to protect applications and that these required separate and specific security measures in particular security testing for vulnerabilities and the integration of security processes with the software development lifecycle (SDLC). This prompted several organizations including banks today to invest in SAST and DAST processes and tools (cite OWASP survey question on which activities are being rolled out)

From the perspective of the "how much need to be spent in application security", CISOs today might need to know how much, of the overall security budget should be spent to make sure a security breach that hit the company won't happen again. For example, assume the online banking site become a victim of an exploit of a SQL injection vulnerability the question is, specifically how much money should be spent in SQL injection countermeasures to prevent this incident to happen again.

To answer these questions, some application security investments criteria needs to be adopted, so that for example, budget allocated for application security can effectively mitigate malware and banking threats and prevent similar incidents and application vulnerability exploits such as SQL injection to occur. Application security investment criteria can only be useful if are based upon objective and not subjective considerations such as using quantitative evaluations of the security incident response costs that the organization incurred because of security breaches exploiting web application vulnerabilities. These criteria must be able to work out the security costs in terms of potential losses due to accidents and attacks and compare it with the cost of the investment in the security of web and mobile applications.

Typically, an increase in application security spending can be triggered by the fact of the organization being victimized because of a security incident (use survey again), this shifts executive management perception of risk. The problem is that when CISOs need to decide how much money to spend in application security the approach mostly followed is to apply common sense based upon perception of risk. In the case of a possible loss for data breach incident, let's say of $ 10 million for example, spending for application security to cover 100% of the costs of the data breach is not always justifiable. The question therefore is still how much should be spent, if not 100% it is the 50%, 25% or 10% or my possible monetary losses? In addition, if allocating a budget of 25% of the estimated potential losses due to data breaches is justifiable, how much of this 25% should be allocated in secure software development/engineering or application security testing for vulnerabilities? We can try to answer these questions by adopting the following criteria for application security budget allocation:

1. Estimate of the impact of the costs incurred in the event of an security incident
2. Quantitative risk calculation of the annual cost for losses due to a security incident
3. Optimization of the security costs in relation to cost of incidents and cost of security measures
4. The Return of Security Investment (ROSI)

To obtain an estimate of the impact of the costs incurred in the event of a security incident, the key factor is the ability of ascertain the costs incurred due to the security incident such as the costs of the loss of company data due to an hacking and malware attack.

In the case of a security incident that caused a loss of sensitive customer data such as personal identifiable information, debit and credit card data, the costs incurred by the bank include several operational costs. 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 withdraw of money from ATMs.

Often times, the determination of such "failure" costs is not directly quantifiable by an organization, such as when this is not a case of a possible monetary loss because of a data breach. In this case, it is possible for the CISO to rely on statistical data. By using statistical data from the Federal Trade Commission (FTC) for example, it is possible to estimate the costs incurred by companies to repair the damage caused by security incidents that resulted in losses of customer sensitive data. For example, the cost incurred by a bank for loss of customer's bank account data and personal identifiable information due to a security incident of large scale (e.g. 1 million users) for example is approximately $ 655 dollars per customer per incident year (Ref [7]). Based upon the same FTC data assuming a 4.6% probability that a customer becomes a victim of a similar security incident, the impact or the bank liability is $ 30.11 per customer per incident per year.

Other statistical data about hacking and incidents can be used for real case estimates of likelihood of incidents: for an online banking site that serves 1 million customers for example, the odds that a security incident due to the exploitation of an application type of vulnerability such as SQL injection might occur is for example 2.5%. This value is estimated based on the percentage of incident caused by attacks to web interface (13% of security incident) (Ref [8]) and the percentage that these attacks exploit application vulnerabilities such as SQL injection (19% of all incidents) (Ref [9]). With these estimated values, the impact of security incident to a bank for an attack that exploits SQL injection is of $ 16 per customer per year. For an online banking website that serves one million customers, the estimation of the impact of a security incident affecting a large customer base (1 million registered users) per year is thus about $ 16,000,000.

This is the maximum amount estimated for expenses in security measures to thwart SQL injection attacks. These include expenses to acquire technology for secure software development, documentation, standards and processes, tools as well costs for the recruitment of personnel and training. Normally this dollar figure can be considered a maximum value since it affects a loss of all the customer data assets handled by the application.

Quantitative risk formulas help estimating the spending for application security measures 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. Assuming the SLE for an SQL injection attack of $ 16,000,000 (as previously calculated) and assuming a frequency of 4 attacks every ten years (40%) for the ARO, the estimated annual loss or Annual Loss Expectancy (ALE) can be calculated using the formula ALE = ARO x SLO that is $ 6,400,000.

By using quantitative risk analysis, CISOs can estimate the amount that a given organization managing a web application should spend on application security measures to mitigate the risk of a data loss due to the exploitation of an application vulnerability such as SQL injection.

The question is if using quantitative risk analysis leads to an estimate to the optimal investment for application security measures. The honest answer is, not necessarily. The correct answer is, need to use cost vs. benefit analysis. Only by comparing the costs of security incidents against the cost of security

measures it is possible to determine when these maximize the benefit, that is, the overall security of the application. In case of software security costs for example, the cost due to software security failures including security incidents decrease as the company spends more money in security measures (FIG 1).

The optimal investment in the security measures is the one that maximizes the security of the application and minimizes both the cost of security measures and of the cost incurred because of security incidents.

According to an analytical study of costs vs. benefits of security (Ref [10]) the optimal investment is when the cost of security measures is approximately 37% of the estimated losses. For our example, assuming the total estimated losses of $ 16,000,000 due to a SQL injection attack, the optimal expense for application security measures, using this empirical value from the study, is $ 5,920,000.

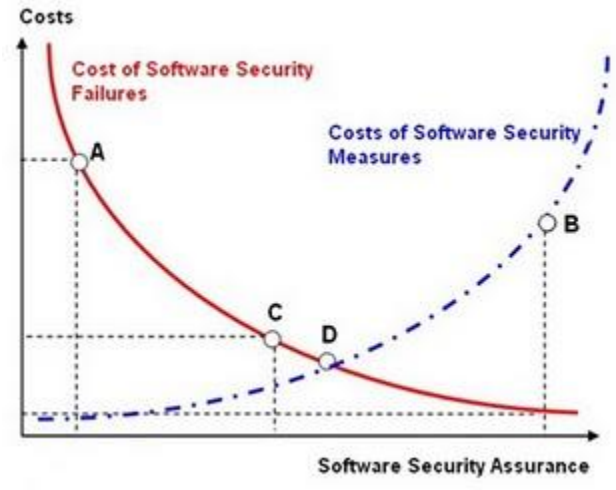

Figure 1: Cost of Investment in software security measures against failure costs due to incidents that exploit software vulnerabilities. At the point (A) to the costs due to software security failures exceed of several order of magnitude the expenditure in countermeasures and the assurance on the security 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.

Finally, it is important to determine the most efficient way to spend the application security budget from a 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 the investment in security.

The factor to calculate the savings in terms of investment in security is the Return of Security Investment (ROSI). The ROSI can also help to determine if the investment in countermeasures to thwart hacking and malware attacks is justifiable: 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 of the savings for the data losses avoided over the total cost of the countermeasures.

Assuming the Total Cost of Ownership (TCO) (Ref [11]) of the countermeasure of $ 5.9 million (previously calculated as optimal value of expense in countermeasures for SQL injection) that include development costs of acquisition of the new technologies, processes, tools as well as operating and maintenance costs it is possible to calculate the savings. Using the following ROSI formula: ROSI= ALE (Annual Loss Expectancy) x percentage of effective risk mitigation costs subtracted by the cost of countermeasures (Ref [12]).

With this ROSI empirical formula, assuming the ALE for SQL injection is $ 6.4 million and the effectiveness of the mitigation is 95% (assume for example, a SQL injection mitigation at different levels that includes use of prepared statements/store procedures in source code as well as filtering of malicious SQL characters at the web server and application server), the money that the company will save every year because of fixing SQL injection vulnerabilities before waiting of a security incident to exploit the same, is of $ 160,000 per year.

Finally, it is important to note that ROSI can be used by CISOs to determine where in the SDLC the investment in software security is more efficient or yields the organization the higher savings and returns on the investment. According to research of Soo Hoo (IBM) (Ref [13]) on ROSI of the various activities of software security in software development cycle, the maximum return of investment (21%) or a savings of $ 210,000 on an investment of $ 1 million is obtained when the investment is in activities that aim to identify and remedy security defects during the design phase. The return of investment is 15% when the defects are identified and remedied during implementation (code) and of only 12% when these are identified and remedied during the testing-validation phase.

The best investment in application security is therefore in activities that aim to identify defects in the design phase using threat modeling and secure architecture risk analysis, in essence, the more CISOs think about application security proactively that is by applying security practices as early as possible during the SDLC, the more they'll save on the costs of implementing and fixing security issues later in SDLC such when applying fixes for vulnerabilities identified during validation phase of a project or when the application is in already in production as reactive response to security incidents.

References

Ref [1]: Verizon 2011 Data Breach Investigation Report
http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

Ref [2]: 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

Ref [3]: Supplement to Authentication in an Internet banking Environment
www.fdic.gov/news/news/press/2011/pr11111a.pdf

Ref [4] PCI-DSS: https://www.pcisecuritystandards.org/security_standards/index.php

Ref [5] OWASP Top Ten: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Ref [6] Gartner teleconference on application security, Joseph Feiman, VP and Gartner Fellow http://www.gartner.com/it/content/760400/760421/ks_sd_oct.pdf

Ref [7] Dan E Geer Economics and Strategies of Data Security http://www.verdasys.com/thoughtleadership/

Ref [8] Data Loss Database http://datalossdb.org/

Ref [9] WHID, Web Hacking Incident Database http://projects.webappsec.org/w/page/13246995/Web-Hacking-Incident-Database

Ref [10] 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.

Ref [11] Total Cost of Ownership http://en.wikipedia.org/wiki/Total_cost_of_ownership

Ref [12] Wes SonnenReich, Return of Security Investment, Practical Quantitative Model http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf

Ref [13] Tangible ROI through Secure Software Engineering http://www.mudynamics.com/assets/files/Tangible%20ROI%20Secure%20SW%20Engineering.pdf

Author Bio:

Marco Morana serves the OWASP (Open Web Application Security Project) as chapter leader of Cincinnati, Ohio, USA. As OWASP chapter leader, Marco's main goal is to promote awareness of application and software security within the local community that includes representatives of different sectors such as academic institutions, financial-banking, software development and consulting. As OWASP project contributor, Marco has also authored and helped to review OWASP projects such as the secure coding guide and the testing guide and published several articles on application and software security topics on behalf of OWASP on Secure Magazine and on behalf of other companies on Secure Enterprise, Network Computing, ISSA Journal, and C/C++ User Journal. In the past, Marco presented on the topic of software security at major security conferences such as CSI and BlackHat. In his current position, Marco works as Sr. Technology Information Security Officer and Security Architect for Citigroup Global Consumer North America where his primary responsibility is managing application and software security programs for web applications including on-line banking. Prior to Citigroup, Marco worked for several years at different companies as software security consultant, secure coding instructor, application architect and software engineer designing and developing secure applications and security assessment tools. Marco academic credentials include a Masters Degree in Computer Systems Engineering from Northwestern Polytechnic University and an Engineering Doctorate Degree (Dr. Ing.) in Mechanical Engineering from University of Padova, Italy. Marco is also a Certified Software Security Lifecycle Professional (CSSLP).