My web site has been breached and my customer's data have been published online, what I can do next ?

Marco Morana
Global Industry Committee
OWASP Foundation

OWASP

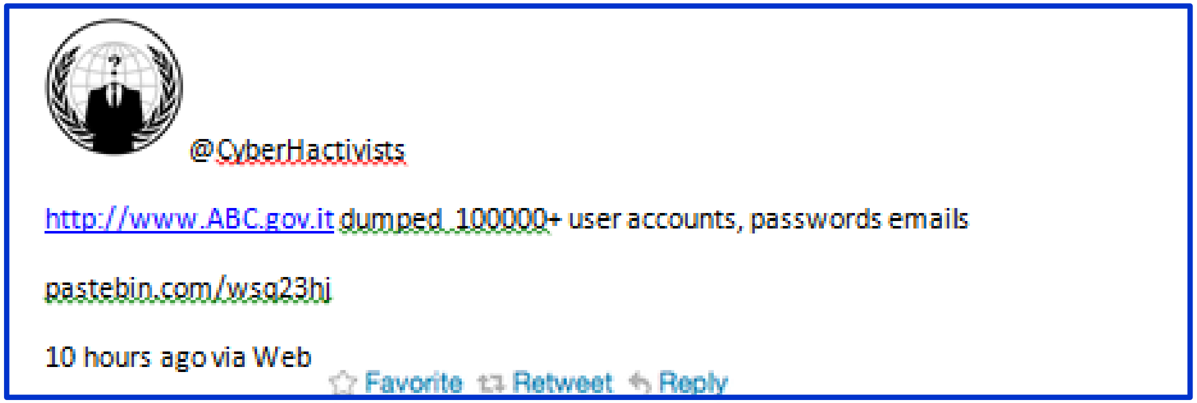
OWASP Day 2, Rome, Italy, November 23rd 2012

Bad news of a security incident are out !!

Your company is on the headlines of a major newspaper today..

Hackers hit
"What's been taken is bits of data that the
... put together into an identity."

How today’s data breaches are communicated and posted online



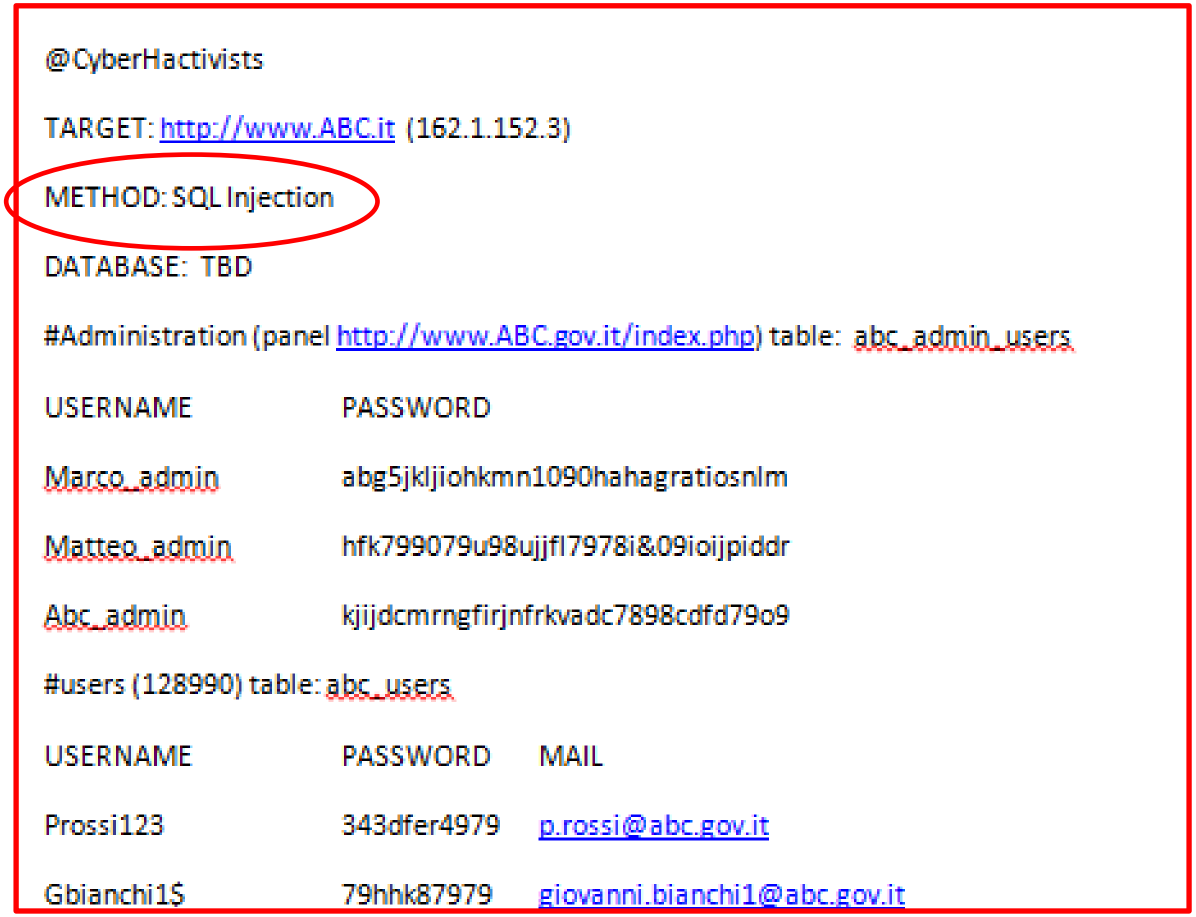
@CyberHactivists

http://www.ABC.gov.it dumped 100000+ user accounts, passwords emails

pastebin.com/wsq23hj

10 hours ago via Web

Twitter Notice



```
@CyberHactivists

TARGET: http://www.ABC.it (162.1.152.3)

METHOD: SQL Injection

DATABASE:  TBD

#Administration (panel http://www.ABC.gov.it/index.php) table:  abc_admin_users

USERNAME            PASSWORD

Marco_admin         abg5jkljiohkmn1090hahagratiosnlm

Matteo_admin        hfk799079u98ujjfl7978i&09ioijpiddr

Abc_admin           kjijdcmrngfirjnfrkvadc7898cdfd79o9

#users (128990) table: abc_users

USERNAME            PASSWORD      MAIL

Prossi123           343dfer4979   p.rossi@abc.gov.it

Gbianchi1$          79hhk87979    giovanni.bianchi1@abc.gov.it
```

Data Leaked Online

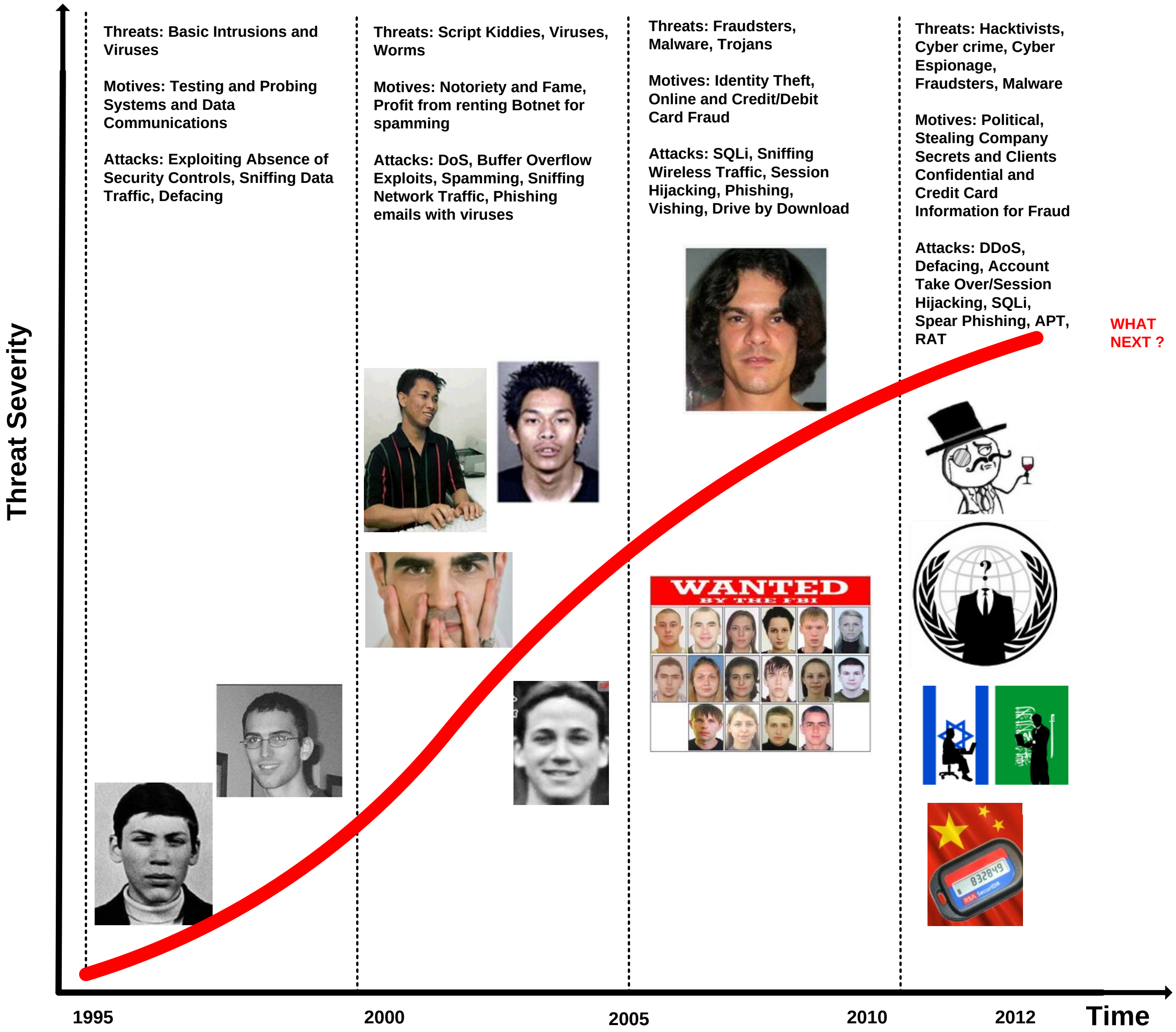
How to respond to data breach security incidents?

Computer Security Incident Response Team
We are open 24/7

What to do next (e.g. which post incident activities) ?

Did you pay attention to the elephant in the room?

Threat Agents Motives and Attacks



Threats: Basic Intrusions and Viruses

Motives: Testing and Probing Systems and Data Communications

Attacks: Exploiting Absence of Security Controls, Sniffing Data Traffic, Defacing

Threats: Script Kiddies, Viruses, Worms

Motives: Notoriety and Fame, Profit from renting Botnet for spamming

Attacks: DoS, Buffer Overflow Exploits, Spamming, Sniffing Network Traffic, Phishing emails with viruses

Threats: Fraudsters, Malware, Trojans

Motives: Identity Theft, Online and Credit/Debit Card Fraud

Attacks: SQLi, Sniffing Wireless Traffic, Session Hijacking, Phishing, Vishing, Drive by Download

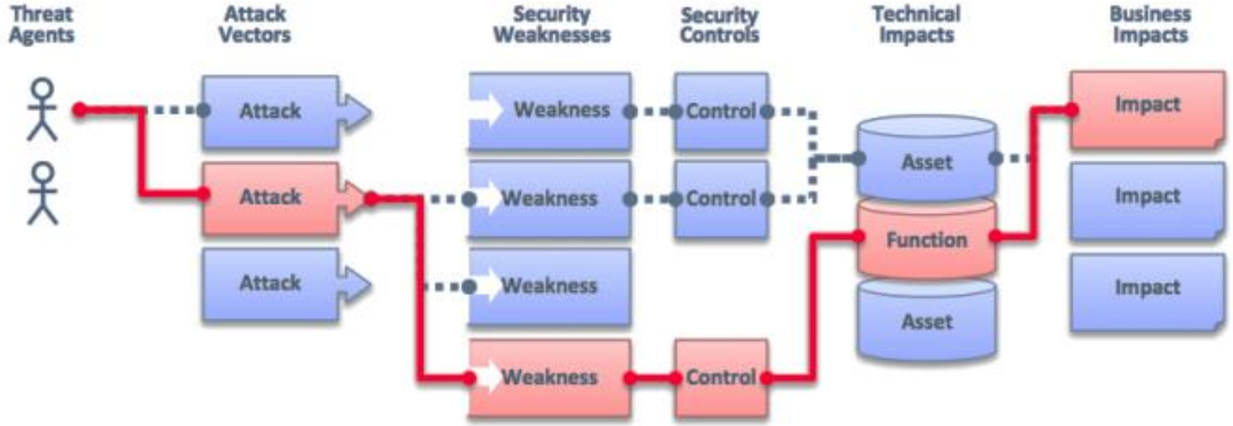
Threats: Hacktivists, Cyber crime, Cyber Espionage, Fraudsters, Malware

Motives: Political, Stealing Company Secrets and Clients Confidential and Credit Card Information for Fraud

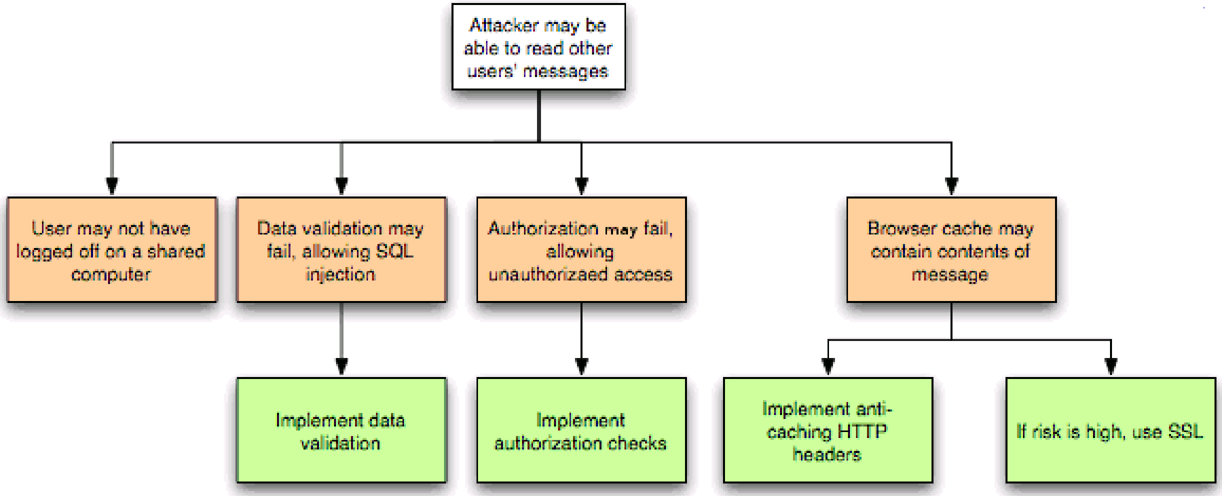
Attacks: DDoS, Defacing, Account Take Over/Session Hijacking, SQLi, Spear Phishing, APT, RAT

Threat- Risk Assessments for Web Applications

Analyze the risk of web application vulnerabilities



Identify countermeasures that can mitigate the risks



Attacker may be able to read other users' messages

User may not have logged off on a shared computer

Data validation may fail, allowing SQL injection

Authorization may fail, allowing unauthorizaed access

Browser cache may contain contents of message

Implement data validation

Implement authorization checks

Implement anti-caching HTTP headers

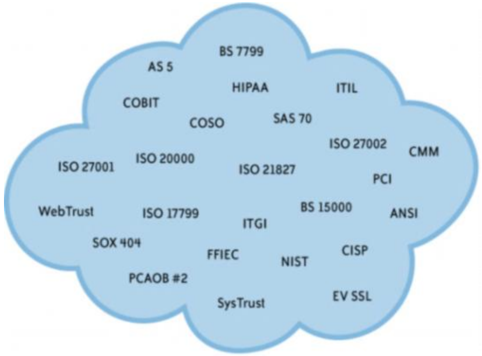
If risk is high, use SSL

Making the Business Cases for Application Security Investments

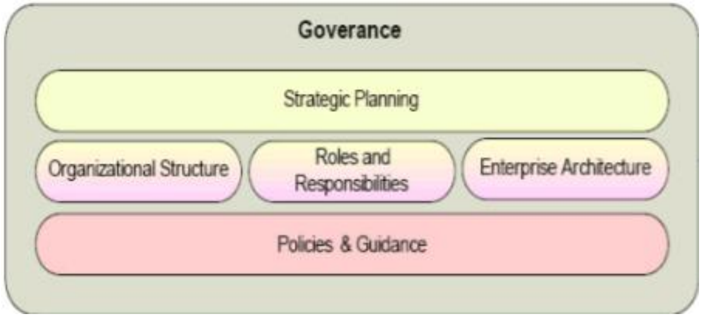
Legal-Compliance

Governance

Audits



BS 7799
AS 5
HIPAA
ITIL
COBIT
COSO
SAS 70
ISO 27002
CMM
ISO 27001
ISO 20000
ISO 21827
PCI
WebTrust
ISO 17799
BS 15000
ANSI
ITGI
SOX 404
FFIEC
NIST
CISP
PCAOB #2
SysTrust
EV SSL



Goverance

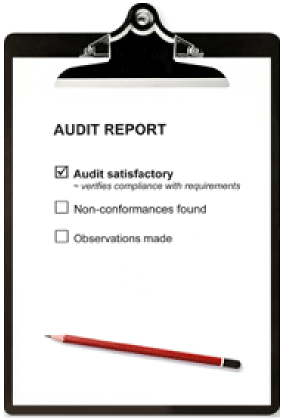
Strategic Planning

Organizational Structure

Roles and Responsibilities

Enterprise Architecture

Policies & Guidance



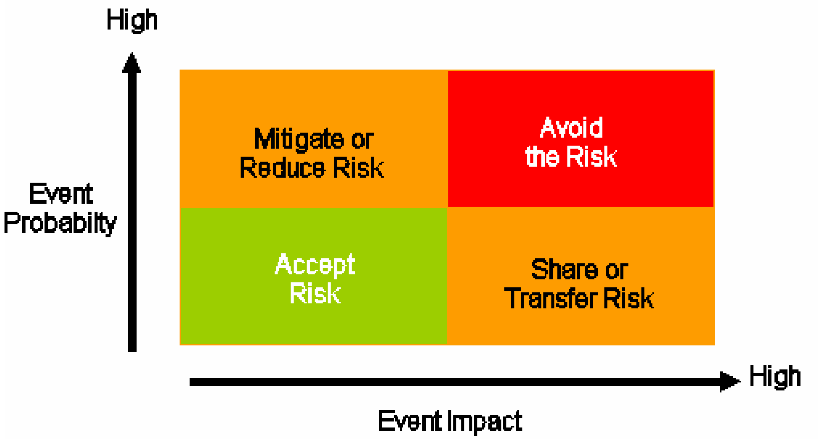
AUDIT REPORT

☑ Audit satisfactory
~ verifies compliance with requirements

☐ Non-conformances found

☐ Observations made

Proactive Risk Mitigation, Cost Savings, Efficiencies

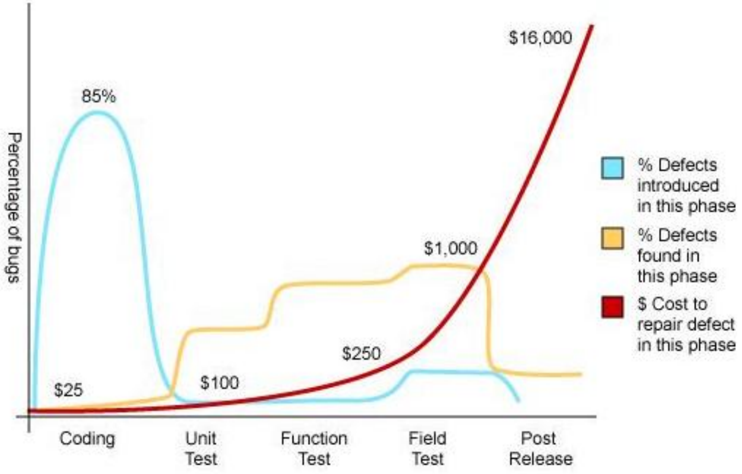


Mitigate or Reduce Risk

Avoid the Risk

Accept Risk

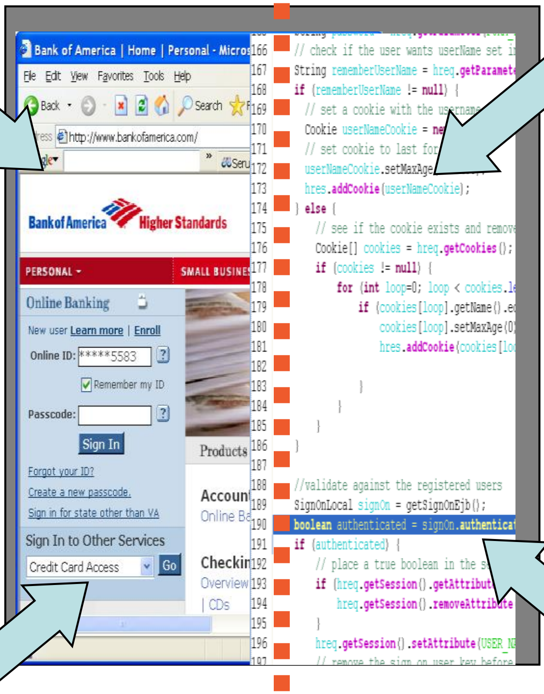
Share or Transfer Risk



Security Testing Applications for Vulnerabilities

Manual Penetration Testing

Manual Code Review


Bank of America | Home | Personal - Micros
File Edit View Favorites Tools Help
Back
Search
http://www.bankofamerica.com/
Bank of America Higher Standards
PERSONAL
SMALL BUSINES
Online Banking
New user Learn more | Enroll
Remember my ID
Passcode:
Sign In
Forgot your ID?
Create a new passcode.
Sign in for state other than VA
Sign In to Other Services
Go
Products
Account
Online Ba
Checkin
Overview
| CDs

Online ID: *****5583

☑ Remember my ID

Credit Card Access

```
// check if the user wants userName set i
String rememberUserName = hreq.getParamete
if (rememberUserName != null) {
  // set a cookie with the username
  Cookie userNameCookie = ne
  // set cookie to last for
  userNameCookie.setMaxAge
  hres.addCookie(userNameCookie);
} else {
   // see if the cookie exists and remove
   Cookie[] cookies = hreq.getCookies();
   if (cookies != null) {
       for (int loop=0; loop < cookies.le
           if (cookies[loop].getName().ec
               cookies[loop].setMaxAge(0)
               hres.addCookie(cookies[loo


           }
       }
   }
}

//validate against the registered users
SignOnLocal signOn = getSignOnEjb();
boolean authenticated = signOn.authenticat
if (authenticated) {
   // place a true boolean in the se
   if (hreq.getSession().getAttribute
       hreq.getSession().removeAttribute
   }
   hreq.getSession().setAttribute(USER_NA
   // remove the sign on user key before
```

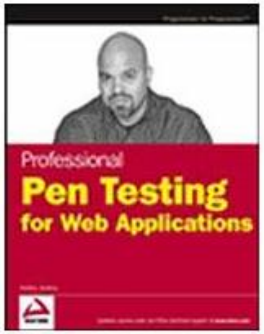
Automated Vulnerability Scanning

Automated Static Code Analysis

Devising a Strategic Plan for Application Security

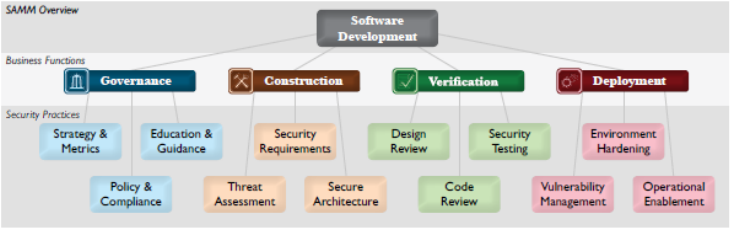
Moving From Tactical-Reactive App Security

Incident Response, Pen testing, Vulnerability Catch and Patch



To Strategic-Proactive App Security

Maturity models, Security In The SDLC, Vuln. Metrics



SAMM Overview

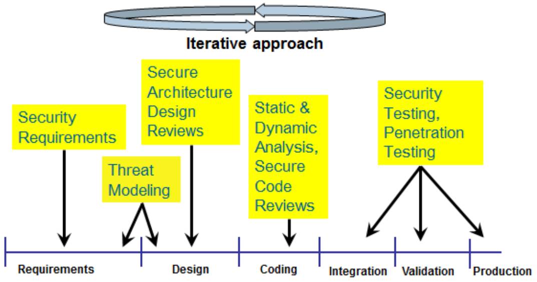
Software Development

Business Functions

Governance
Construction
Verification
Deployment

Security Practices

Strategy & Metrics
Education & Guidance
Policy & Compliance
Security Requirements
Threat Assessment
Secure Architecture
Design Review
Security Testing
Code Review
Environment Hardening
Vulnerability Management
Operational Enablement



Iterative approach

Security Requirements

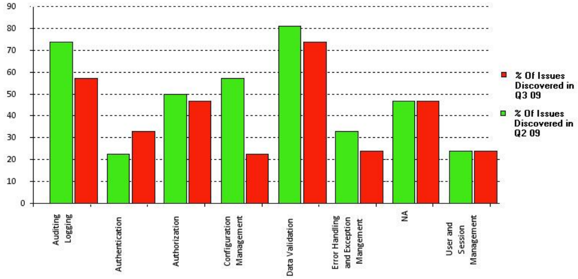
Secure Architecture Design Reviews

Threat Modeling

Static & Dynamic Analysis, Secure Code Reviews

Security Testing, Penetration Testing

Requirements
Design
Coding
Integration
Validation
Production



How the OWASP Appsec Guide for CISOs can Help?

OWASP Appsec Guide for CISOs

1. **Criteria for Application Security Investments**
    1. Legal and Compliance Criteria
    2. Risk Management Criteria
2. **Selection of Application Security Measures**
    1. Vulnerabilities with the Most Business Impact
    2. Target Threats with Countermeasures
    3. Mitigate the Risks of New Technologies
3. **Selection of Application Security Processes**
    1. Addressing CISO Role & Responsibilities
    2. Targeting Software Security Activities and S-SDLC Processes
    3. How to choose the right projects and tools from OWASP
4. **Metrics for managing application security governance, compliance and risks**
    1. Application Security Process Metrics
    2. Application Security Risk Metrics
    3. Security in SDLC Issue Management Metrics

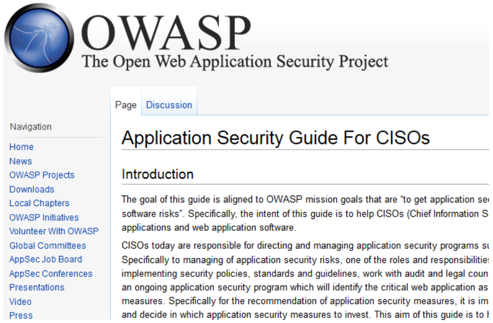
The OWASP Application Security Guide For CISOs Four Step Project Plan

STEP 1: Present OWASP Application Security GUIDE Draft to IS Community

STEP 2: Enroll CISOs to participate to a CISO survey

STEP 3: Gather and analyze the survey

STEP 4: Tailor the guide to the results of the survey and final release status



OWASP
The Open Web Application Security Project

Page Discussion

Navigation

- Home
- News
- OWASP Projects
- Downloads
- Local Chapters
- OWASP Initiatives
- Volunteer With OWASP
- Global Committees
- AppSec Job Board
- AppSec Conferences
- Presentations
- Video
- Press

Application Security Guide For CISOs

Introduction

The goal of this guide is aligned to OWASP mission goals that are "to get application se software risks". Specifically, the intent of this guide is to help CISOs (Chief Information S applications and web application software.

CISOs today are responsible for directing and managing application security programs su Specifically to managing of application security risks, one of the roles and responsibilitie implementing security policies, standards and guidelines, work with audit and legal coun an ongoing application security program which will identify the critical web application as measures. Specifically for the recommendation of application security measures, it is im and decide in which application security measures to invest. This aim of this guide is to I

STEP 4: Present final release

Thank you for listening

QUESTIONS
ANSWERS

Appendix: Business Cases Cheat Sheet-Data Breach Incidents 2011-2012 Statistics

1. **Threats Agents**: Majority are hacking and malware
2. **Targets**: 54% of incidents target web applications
3. **Likelihood**: 90% of organizations had at least one data breach over the period of 12 months
4. **Attacks-Vulnerabilities:** SQL injection reigning as the top attack technique, 51% of all vulnerabilities are XSS
5. **Data Breach Impact**: Majority are data lost are user's credentials, emails and personal identifiable information
6. **Business Breach Impact**: The average cost of a data record breached is estimated as $ 222 per record
7. **Incident Response**: Majority of incidents is discovered after weeks/months from the time of initial data compromise

Sources: OSF, DataLossDb.org
Ponemon Institute and Symantec, Research March 2012
Verizon's Investigative data Breach Report 2012
IBM X-Force 2012 Mid Year Trend & Risk Report

Appendix: Mapping CISO's Responsibilities

CISO RESPONABILITY	DOMAIN	CURRENT OWASP PROJECTS	OWASP CISO GUIDE
Develop and implement policies, standards and guidelines for application security	Standards & Policies	Development Guide - Policy Frameworks CLASP - Identify Global Security Policy SAMM - Policy & Compliance, Code Review- Code Reviews and Compliance, Cloud-10 Regulatory Compliance	✖
Develop implement and manage application security governance processes	Governance	SAMM - Governance	✖
Develop and implement software security development and security testing processes	Security Engineering Processes	Development Guide -All Code Review Guide- All, Secure Code Practices Guide-All, Testing Guide-All, CLASP-All, SAMM-All, Security Tools for Developers-All Application Security Standards-All	✖
Develop, articulate and implement risk management strategy for applications	Risk Strategy	SAMM - Strategy & Metrics	✖
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	Application Security Verification Standard-All, CLASP-Document Security-Relevant Requirements, SAMM-Security requirements, Testing Guide-Security Requirements Test Derivation, Legal-Secure Software Contract Annex	✖
Measure and monitor security and risks of web application assets within the organziation	Risk Metrics & Monitoring	Application Security Metrics Project, CLASP-Define and monitor metrics	✖
Define, identify and assess the inherent security of critical web application assets, assess the threats, vulnerabilities, business impacts and recommend countermeasures/corrective actions	Risk Analysis & Management	OWASP Top Ten Risks, Testing Guide-Threat Risk Modeling Development Guide-Threat Risk Modeling, Code Review Guide-Application Threat Modeling Testing Guide-Threat Risk Modeling	✖
Assess procurement of new web application processes, services, technologies and testing tools	Procurement	Legal project Tools project Contract Annex	✖
Oversees the training on application securty for information security and web application development teams	Security Training	Education Project Training Modules/Conference Videos Application Security FAQ CLASP-Institute security awareness program	✖
Develop, articulate and implement continuity planning/disaster recovery	Business Continuity/ Disaster Recovery	Cloud- Business Continuity and Resiliency	✖
Investigate and analyze suspected security breaches and recommend corrective actions	Incident Response	.NET Incident Response, CLASP-Manage Security Issue Disclosure Process	✖