OWASP Application Security Guide for Chief Information Security Officers (CISOs)

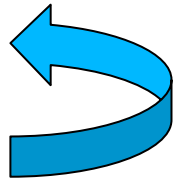
Marco Morana
Global Industry Committee
OWASP Foundation

OWASP

Chapter Meeting
November 15th 2012
NYC U.S.A.

About myself and the life journey that brought me here..

citi



OWASP
The Open Web Application Security Project
http://www.owasp.org

COMPUCREDIT

Bridgefex

VISA

CERBTECH LLC

McAfee

EWA
Electronic Warfare Associates, Inc.

INTERNET SECURITY SYSTEMS

Alenia

UNIVERSITY OF CALIFORNIA BERKELEY

NORTHWESTERN POLYTECHNIC UNIVERSITY

NASA

STERLING SOFTWARE

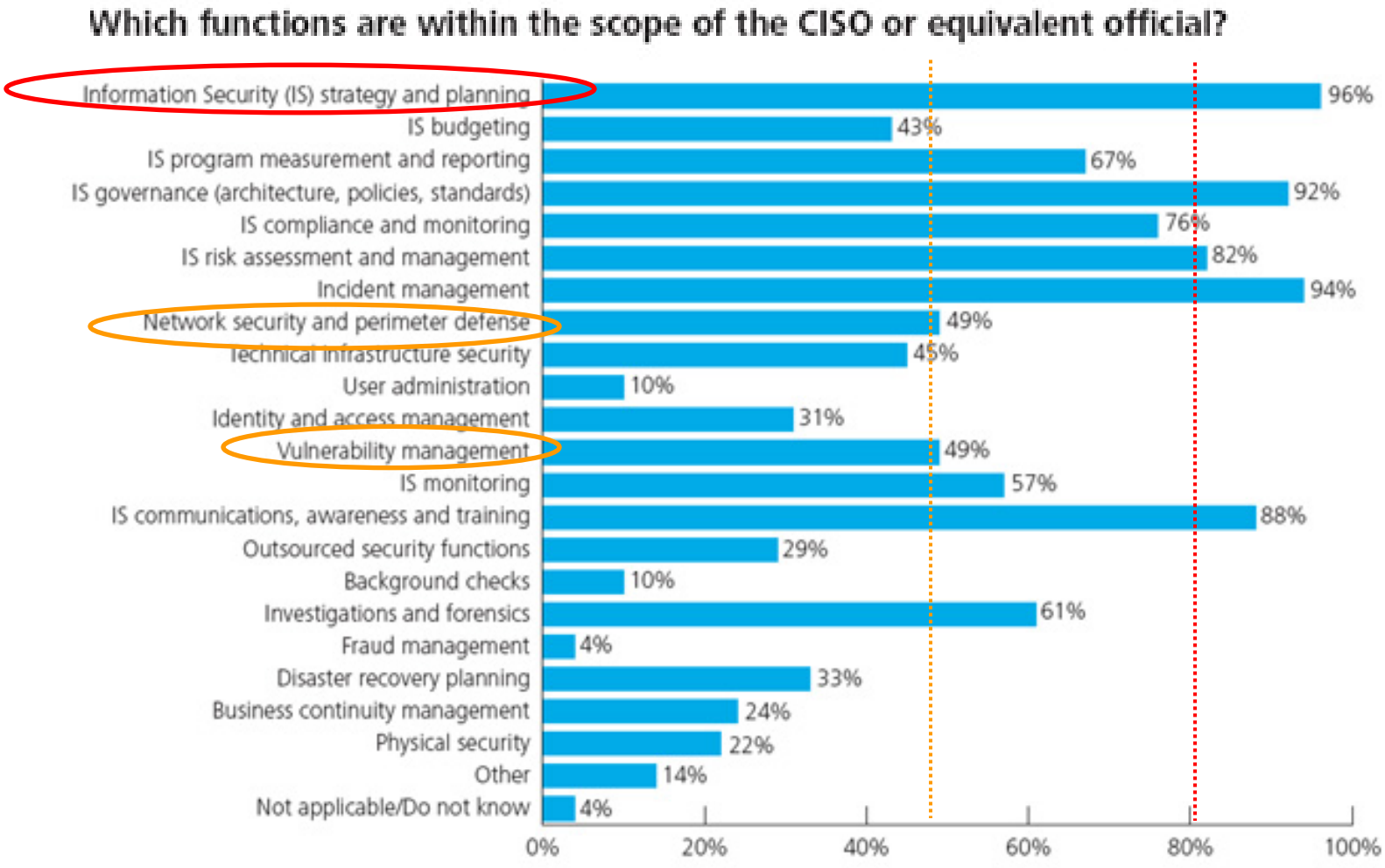
LOCKHEED MARTIN

Why an OWASP Guide For CISOs?

Today's CISOs are like four star generals

What CISO care for today?

The importance of CISOs Surveys

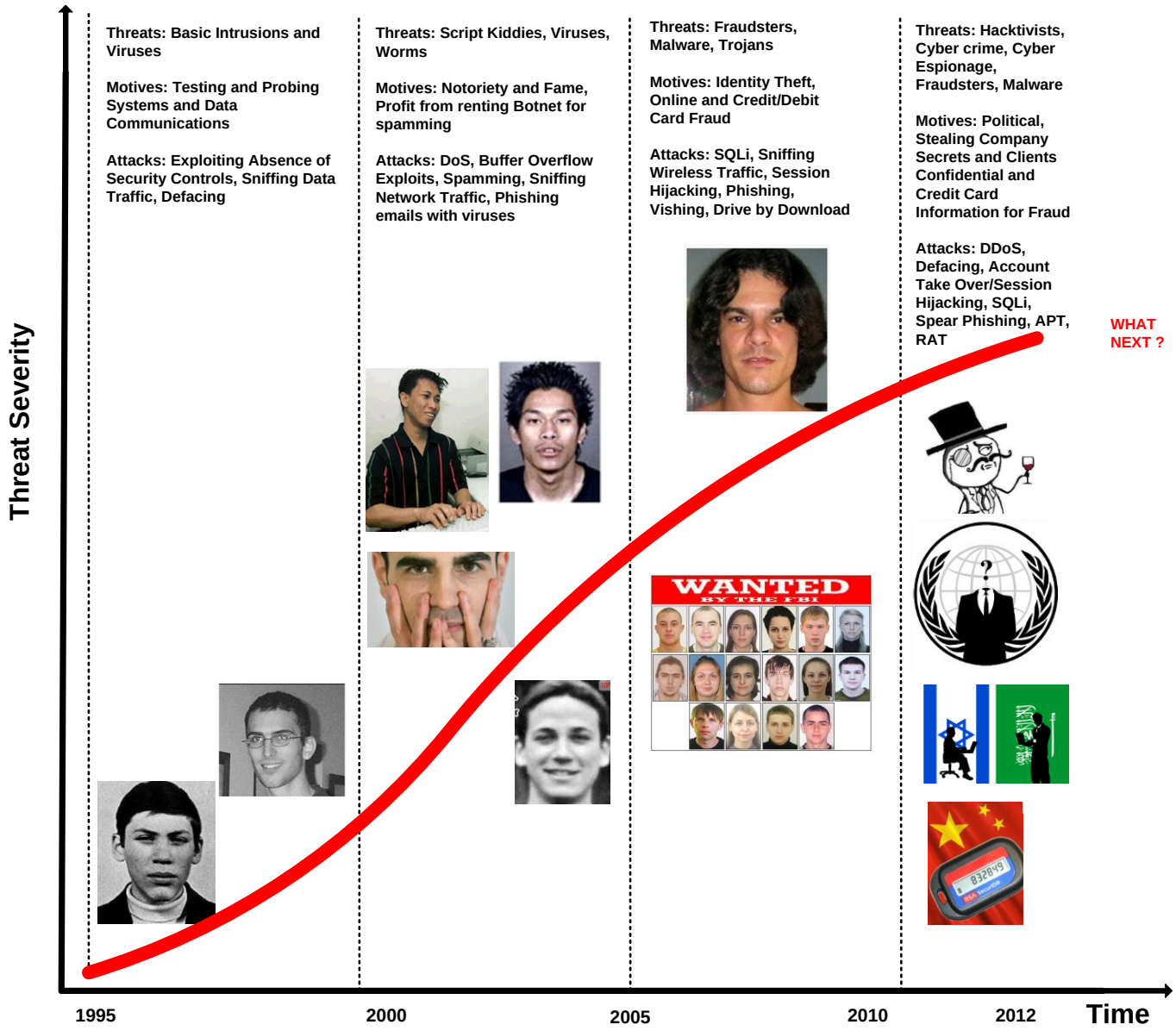


Sources:
Deloitte and the National Association of State CIOs (NASCIO) are sharing the results of a joint Cyber Security Survey, finding that State Chief Information Security Officers (CISOs) in 2010

What CISOs will care of in the future?


Do you pay attention to the threats coming toward you ?

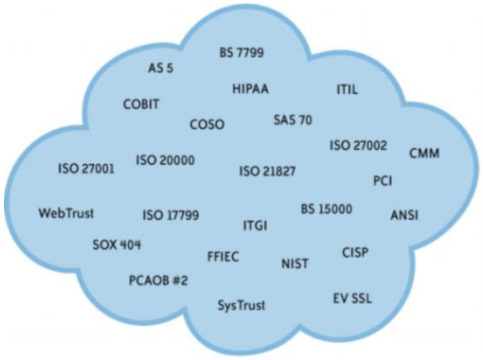
The Escalation of Cyber Threats



How a CISO Guide Can Help?

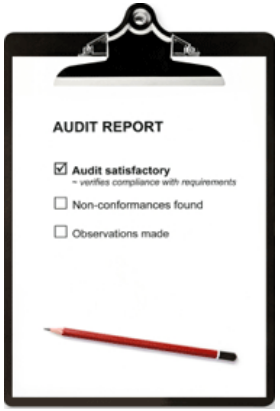
OWASP Appsec CISO GUIDE PART I: Guidance Criteria for Application Security Investments

Compliance-Legal

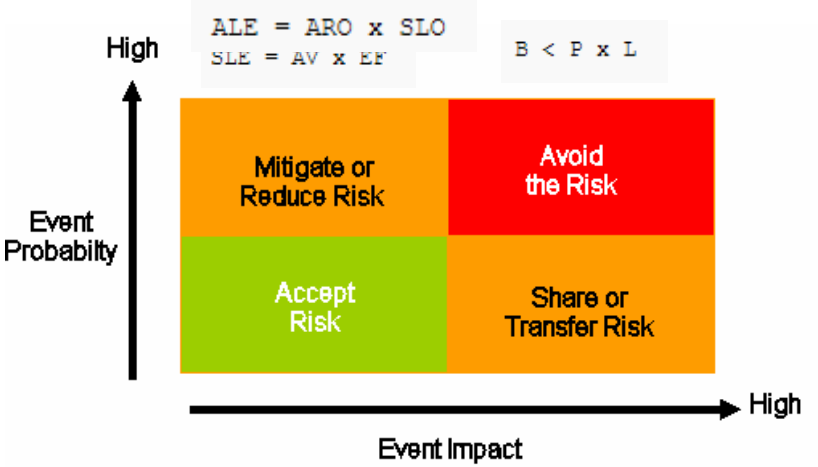


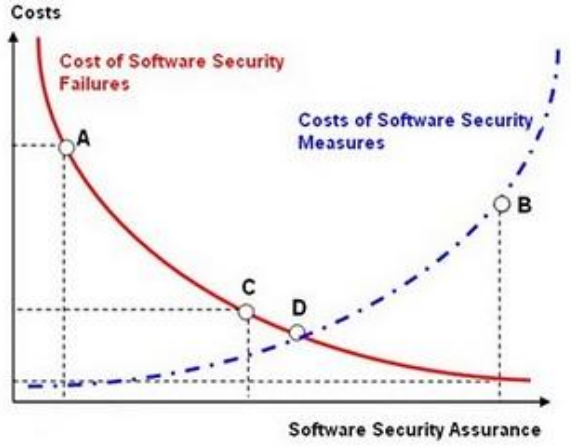
Governance

Audits



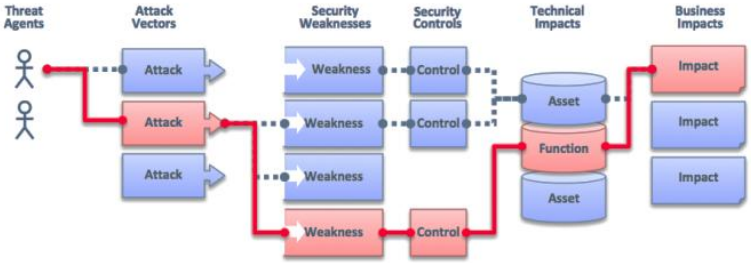
Risk Quantification, Costs vs. Benefits of Measures, ROSI



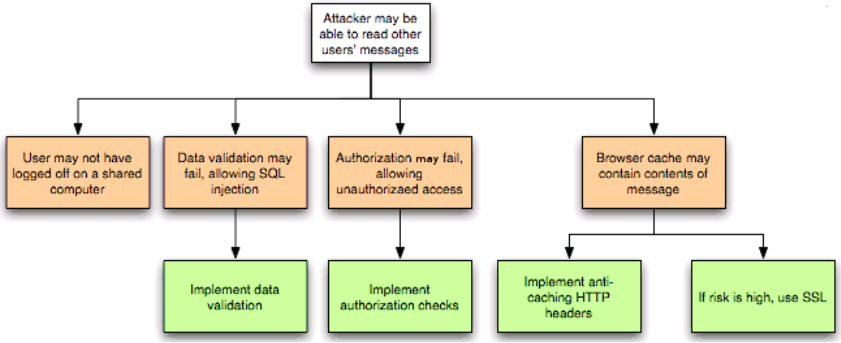


OWASP Appsec CISO GUIDE PART II: Selection of Application Security Measures

Prioritization of Vulnerabilities by Business Impacts



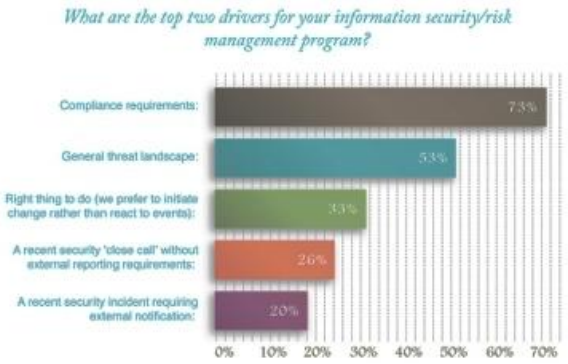
Threat Agent Specific Countermeasures



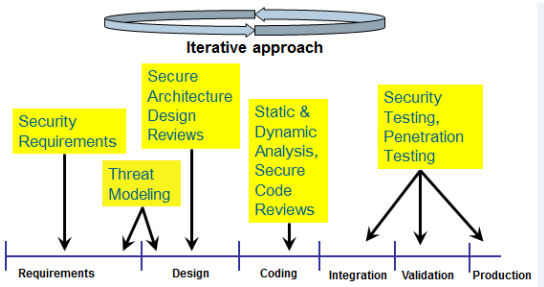
Measures for Securing New Technologies

PART III: Strategic Guidance for the Selection of Application Security Processes

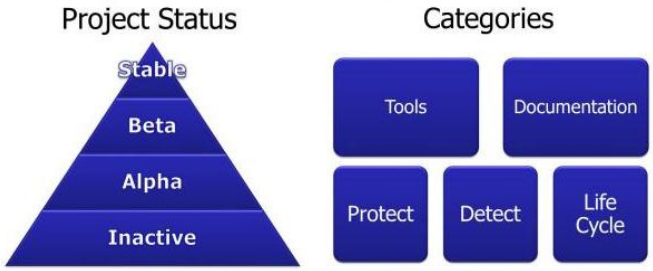
Alignment with CISO Role & Functions



Maturity Models and S-SDLC Processes

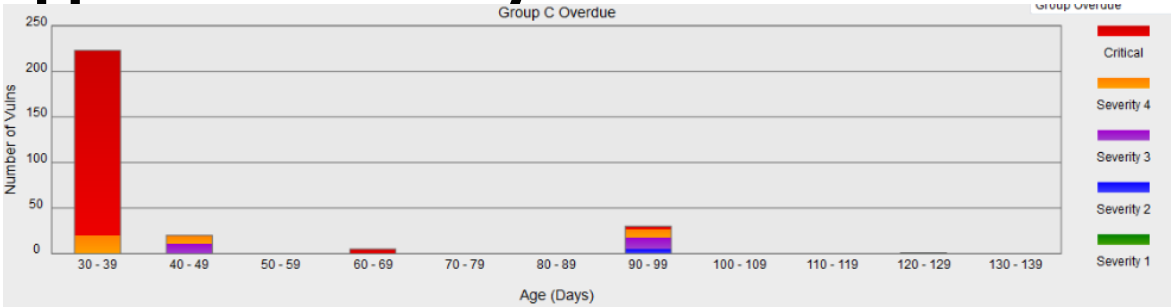


Guidance for choosing OWASP Projects

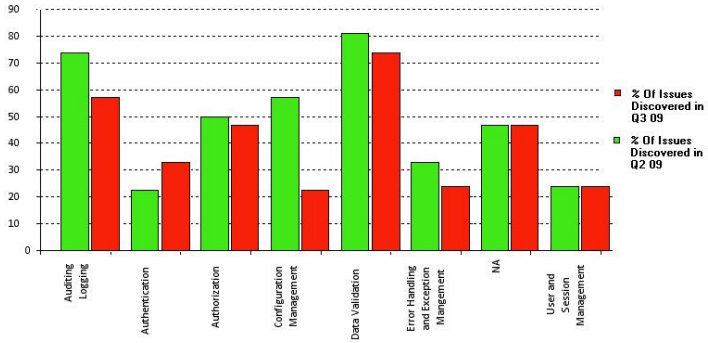


PART IV: Guidance on metrics for managing application security programs

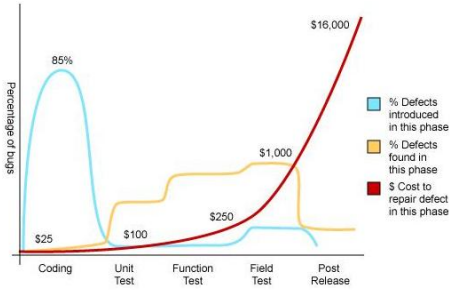
Application Security Processes Metrics



Application Security Issues Risk Metrics



Security in SDLC Issue Management Metrics



How we are creating the guide

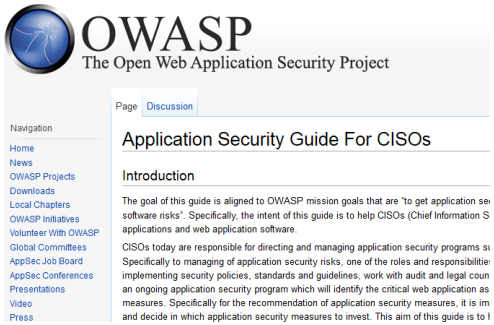
The OWASP Application Security Guide For CISOs Four Step Project Plan

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

STEP 2: Enroll CISOs to participate to a CISO survey

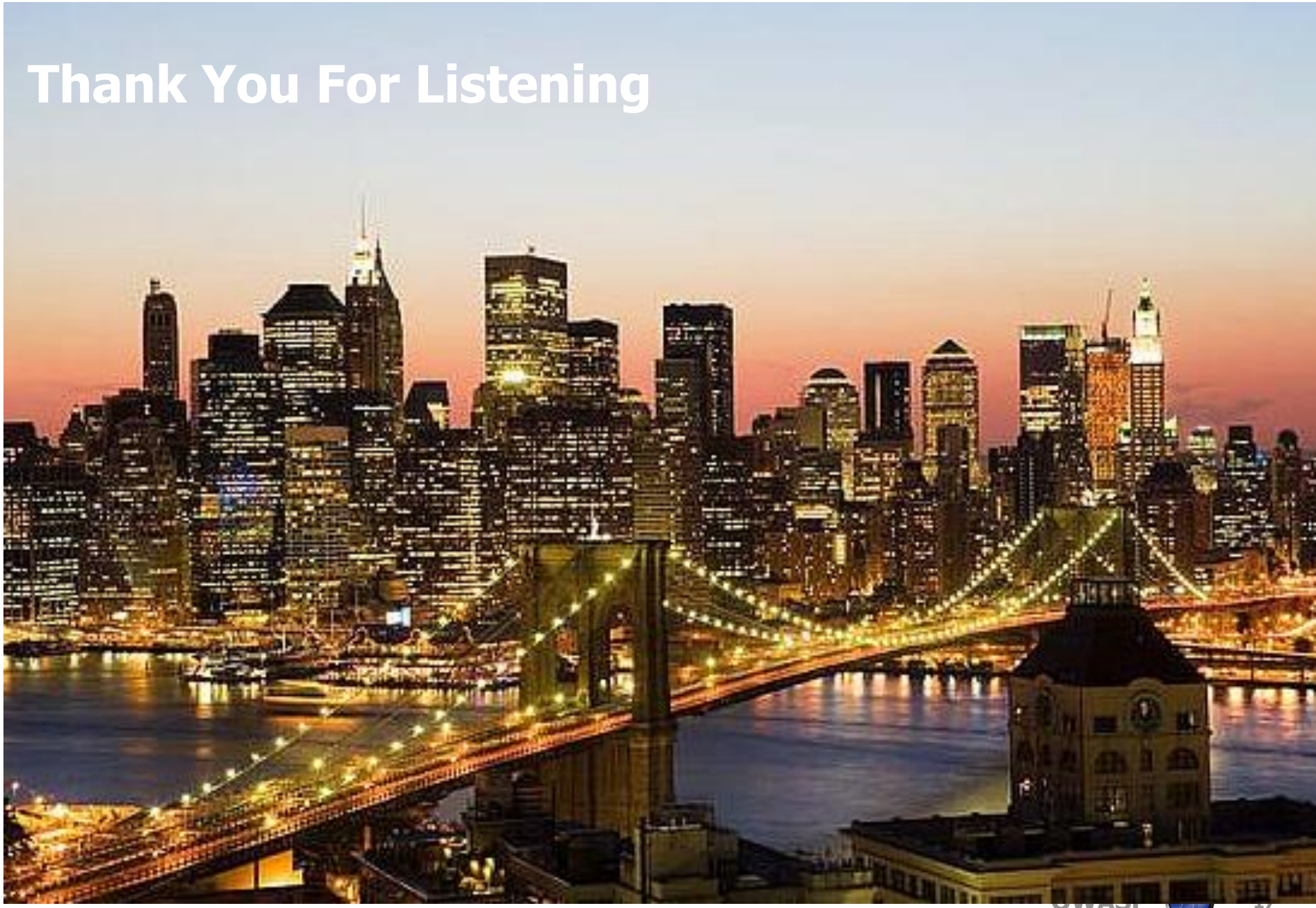
STEP 3: Gather and analyze the survey

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



STEP 4: Present final release

Thank You For Listening



QUESTIONS ANSWERS

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 securuty 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	✖

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