

# **Application Security Guide for CISO and Survey Reboot Project Summit Session(s)**

**Marco M. Morana, CISO Guide Project Lead**



**September 19 - 20 Training Days and September 21 - 22 Conference Days | Orlando, FL**

# Agenda

## **2013 OWASP CISO GUIDE**

- Why we developed version 1**
- Roadmap for version 1**
- Main Themes**

## **2013 OWASP CISO SURVEY**

- What matters to CISO**
- OWASP CISO Survey 2013-2014**

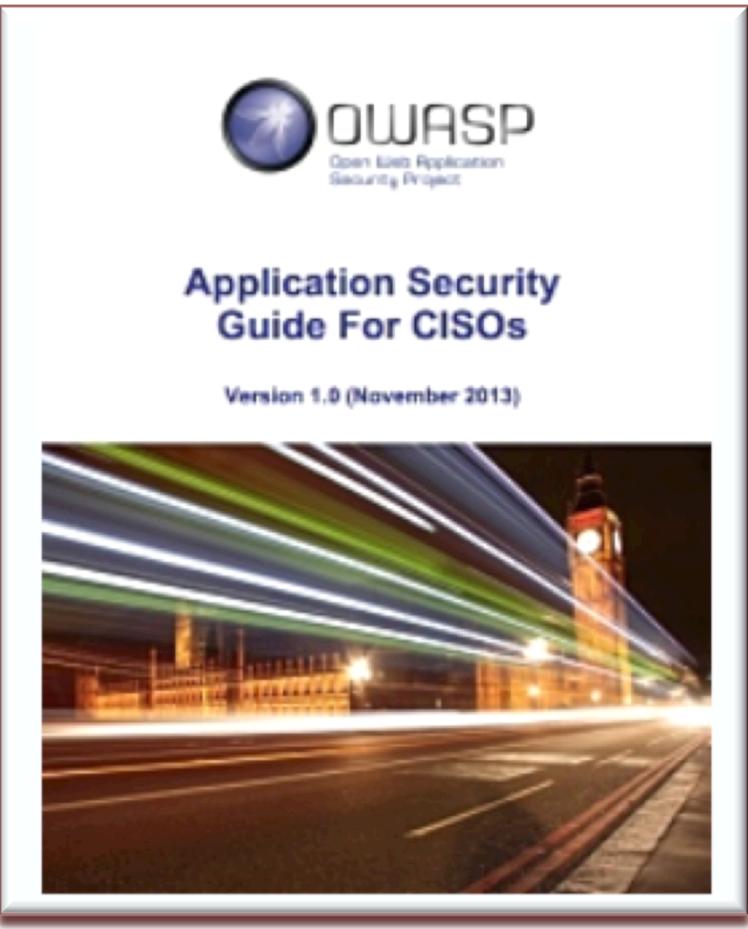
## **2018 OWASP CISO GUIDE VERSION 2**

- Discussions at OWASP Summit in London**
- Outcomes of Discussion**
- Roadmap for development of vs 2 of GUIDE + survey**

# CISO Guide Version 1 (2013)

## OWASP CISO Guide authors, contributors and reviewers:

- Tobias Gondrom
- Eoin Keary
- Any Lewis
- Marco Morana
- Stephanie Tan
- Colin Watson



- **OWASP CISO Guide:**  
<https://www.owasp.org/images/d/d6/Owasp-ciso-guide.pdf>
- **OWASP CISO Survey:**  
<https://www.surveymonkey.com/s/CISO2013Survey>

# Why We Developed the CISO Guide Version 1 (2013)

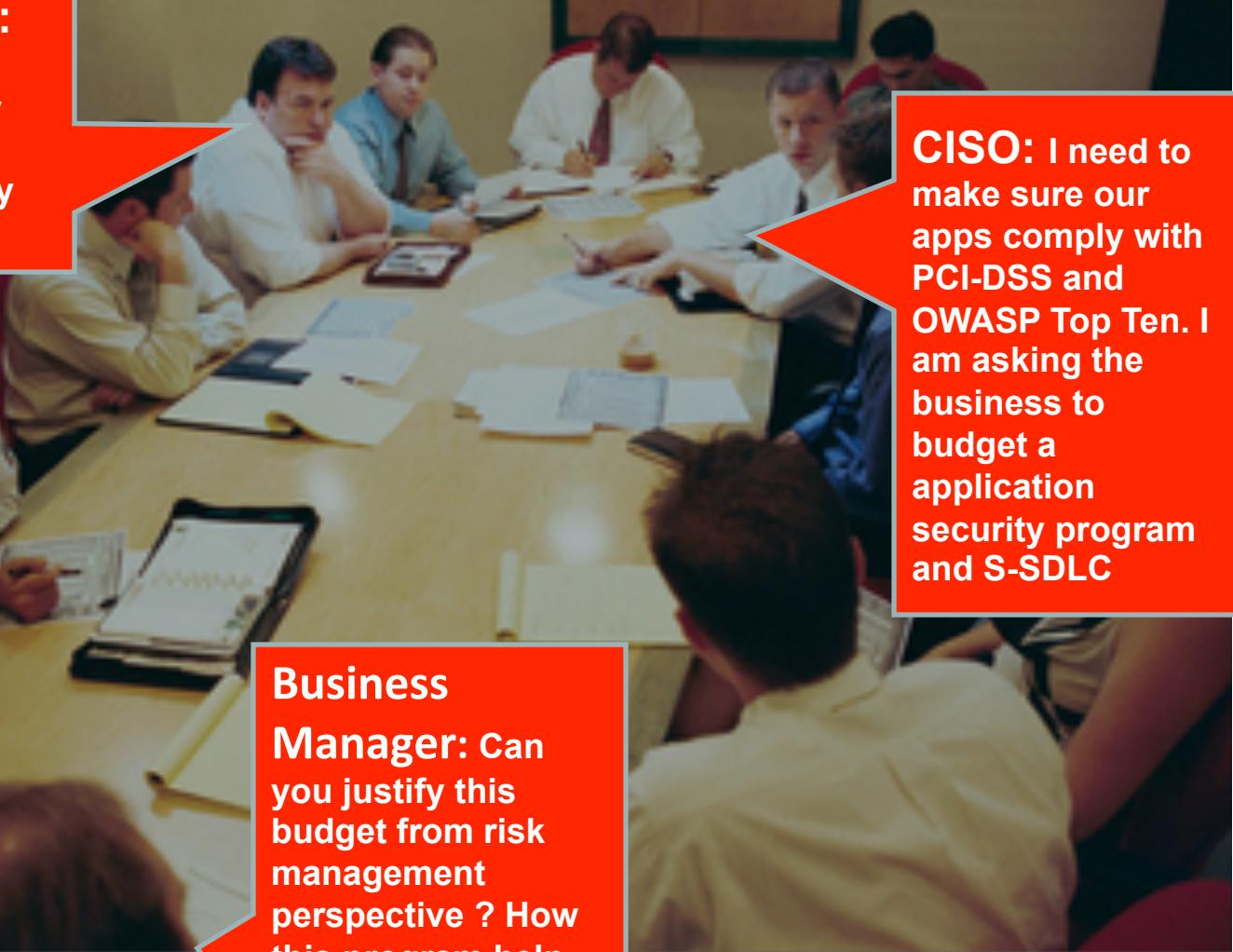
**Pen-Testing Team Manager:** Can we include budget for security testing tools and training for security testers ?



**Engineering Manager:** can we budget for secure coding training and security tools for S/W developers as well?

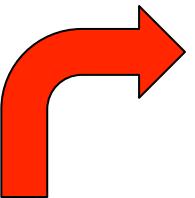


**Business Manager:** Can you justify this budget from risk management perspective ? How this program help reduce risks of security breaches we had in the past?



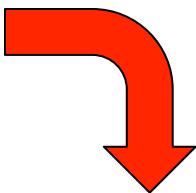
**CISO:** I need to make sure our apps comply with PCI-DSS and OWASP Top Ten. I am asking the business to budget a application security program and S-SDLC

# Application Security Guide For CISO and Survey Roadmap for Version 1 (2013)

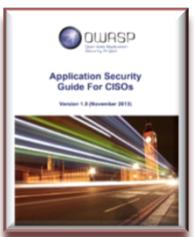


STEP 1: Discuss OWASP Application Security Guide Goals & Questions for Survey

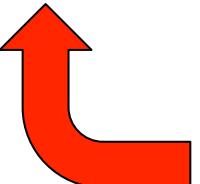
STEP 2: Enroll CISOs to participate to a CISO survey



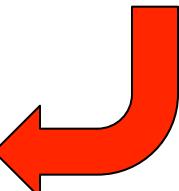
STEP 3: Gather the Answers and analyze the survey



STEP 4: Present releases



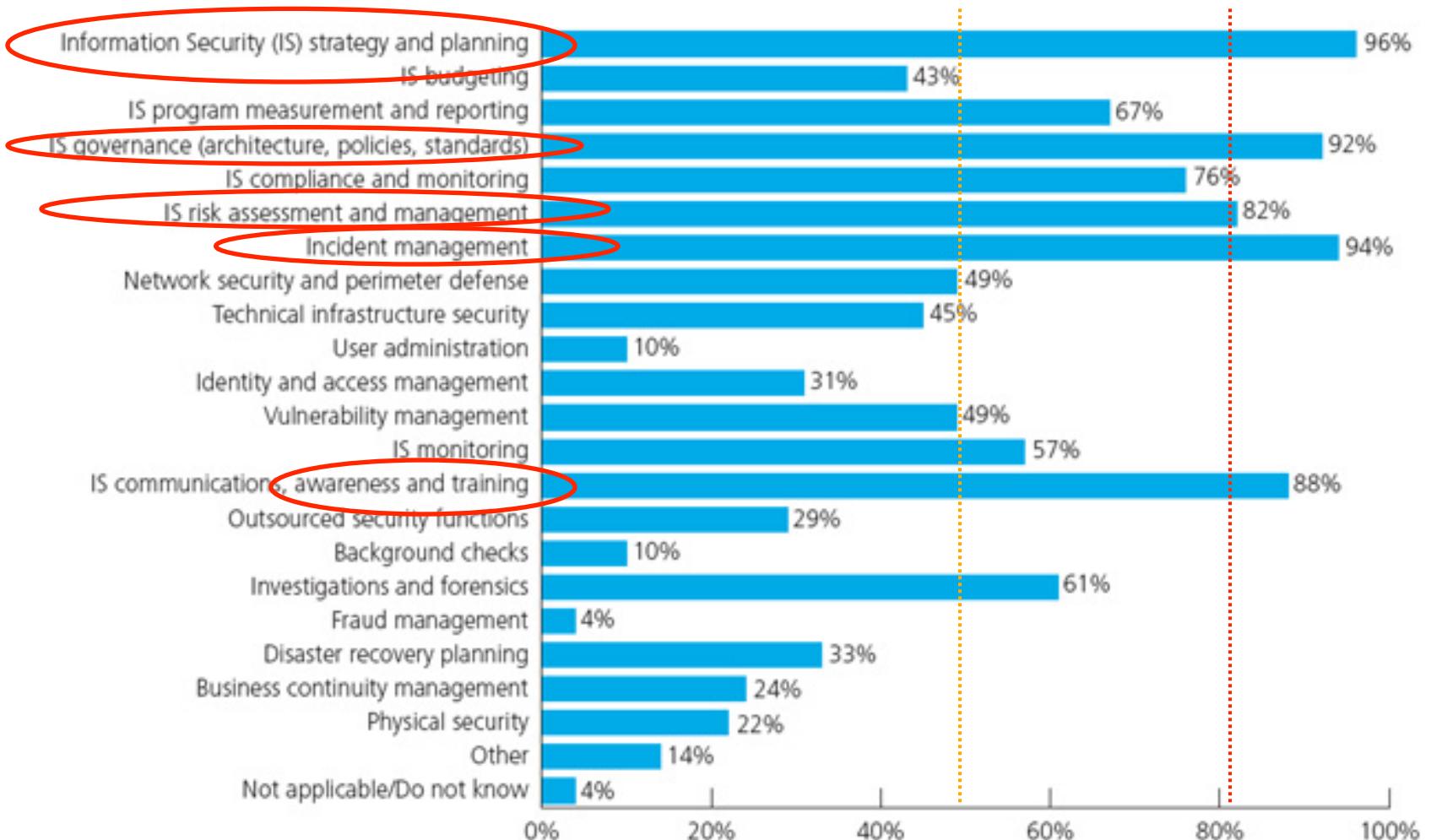
The screenshot shows the OWASP Application Security Guide For CISOs page. The header includes the OWASP logo and the title 'Application Security Guide For CISOs'. The page content starts with an 'Introduction' section, which states: 'The goal of this guide is aligned to OWASP mission goals that are "to get application security risks". Specifically, the intent of this guide is to help CISOs (Chief Information Security Officers) manage application security risks. CISOs today are responsible for directing and managing application security programs. Specifically to managing of application security risks, one of the roles and responsibilities: implementing security policies, standards and guidelines, work with audit and legal counsils, an ongoing application security program which will identify the critical web application as measures. Specifically for the recommendation of application security measures, it is important to decide in which application security measures to invest. This aim of this guide is to...'.



# Main Themes For Version 1



# What Matter to CISOs?.. CISO Survey(s)

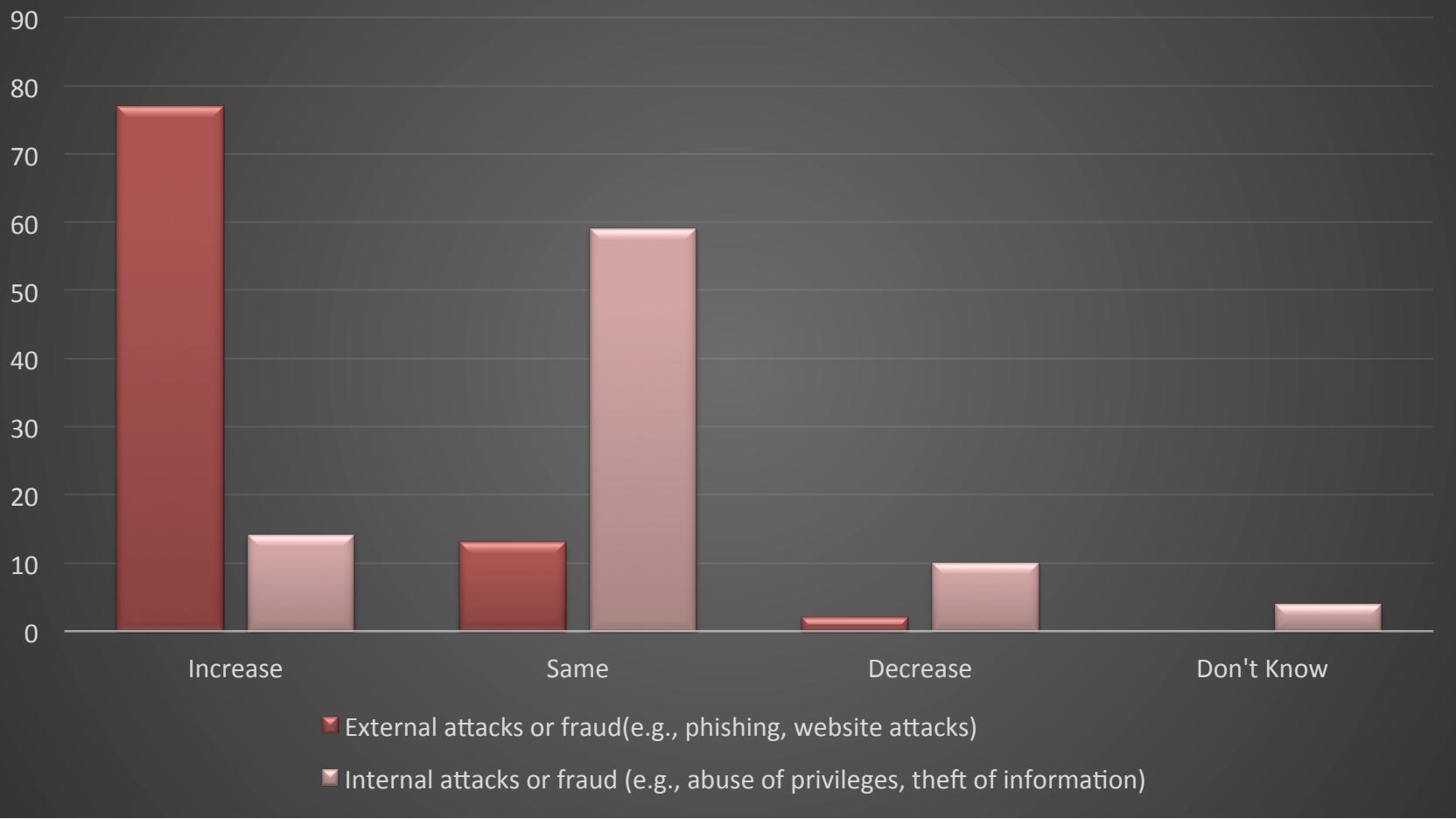


Sources:

[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

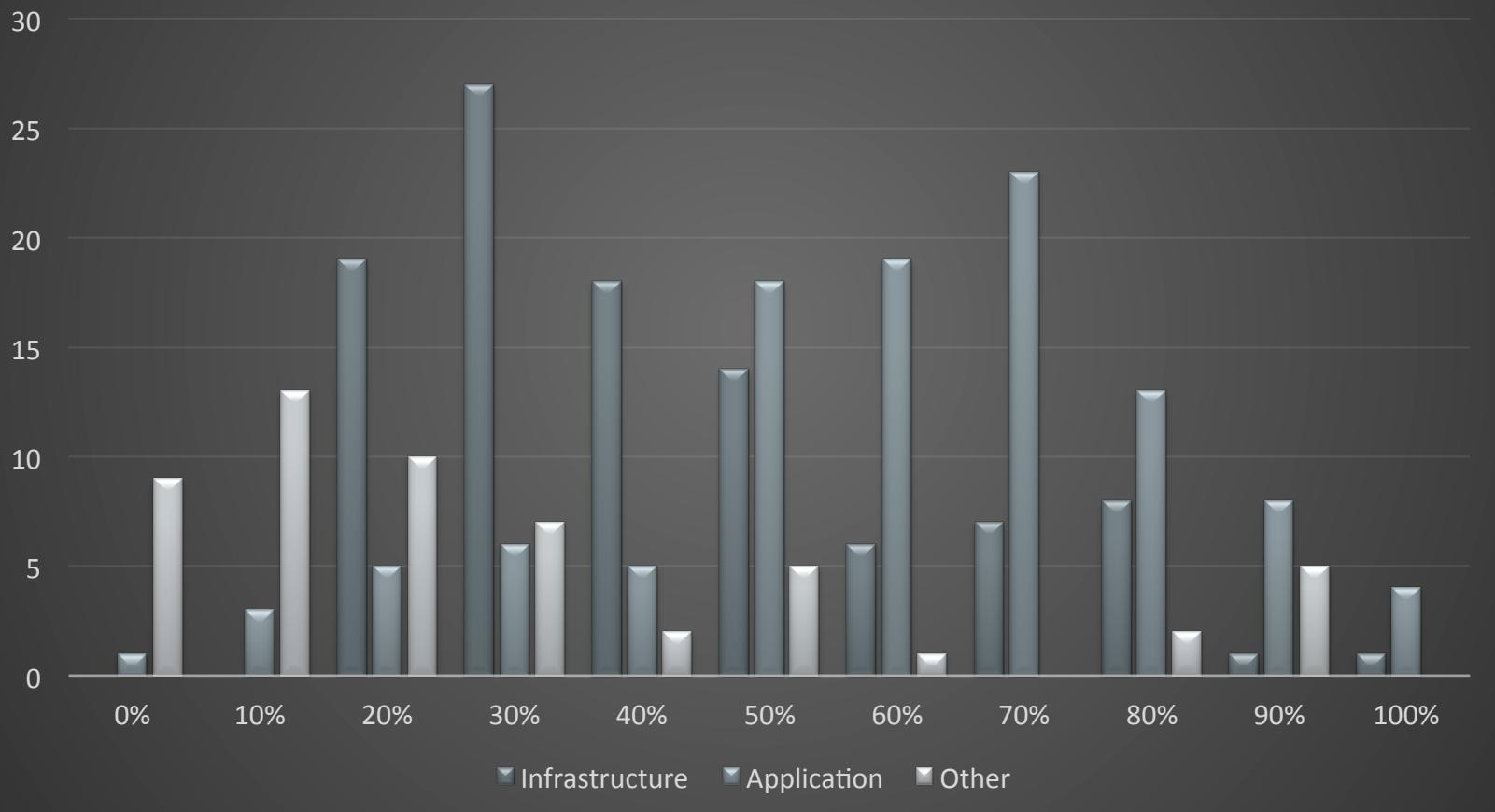
# OWASP 2013 CISO Survey 1/7

## Change in the threats facing your organization

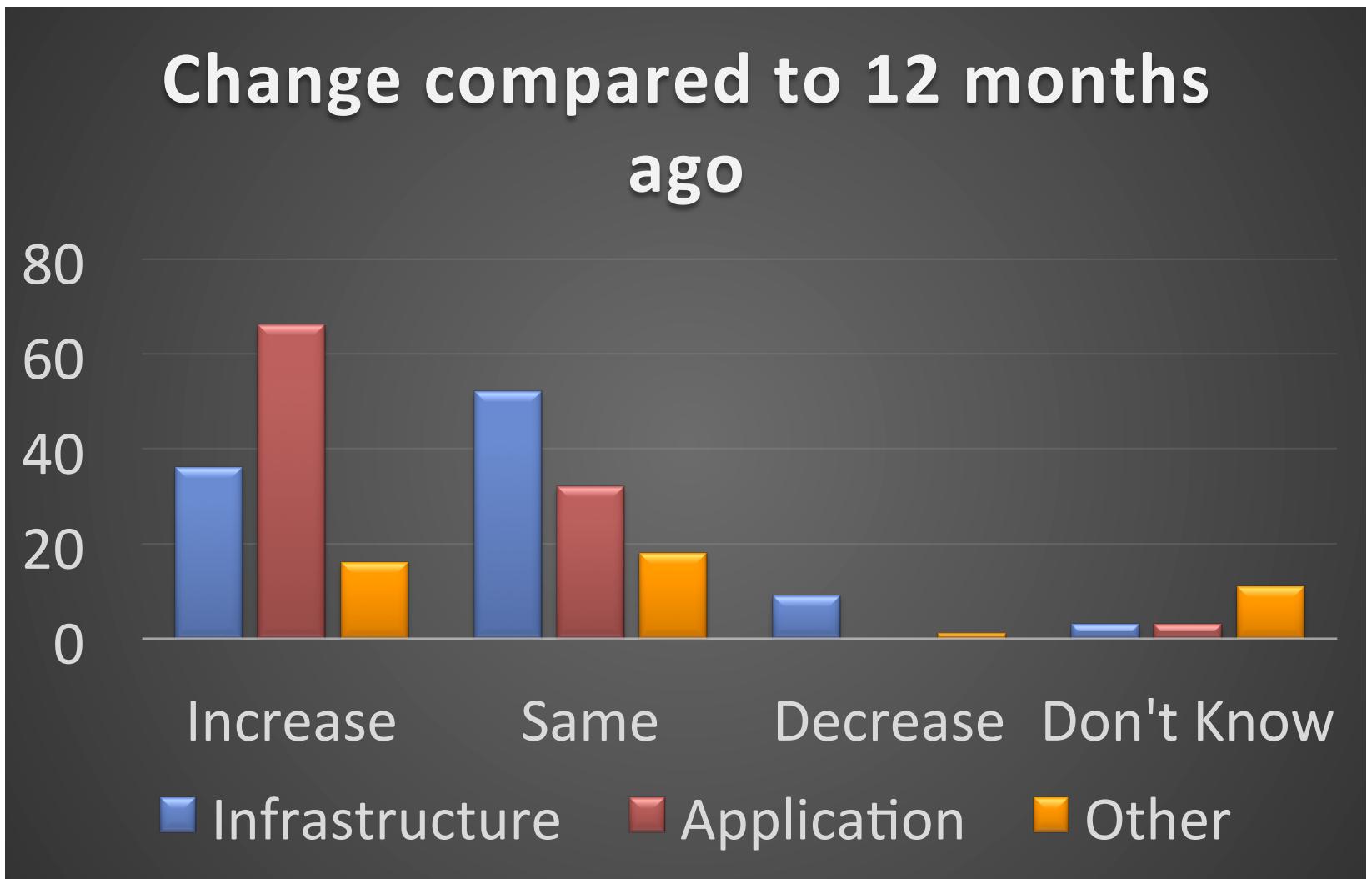


# 2013 OWASP CISO Survey 2/7

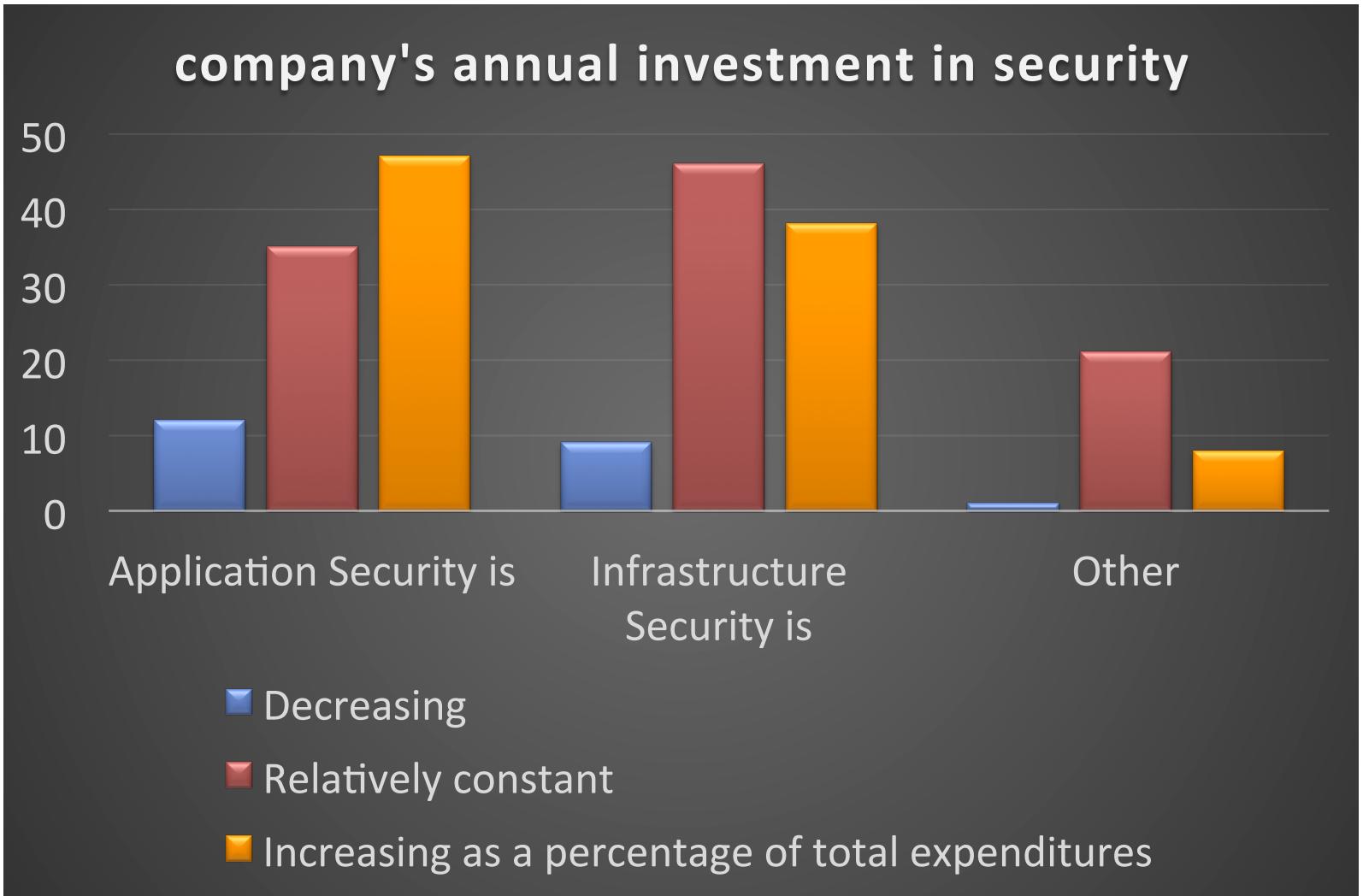
what are the main areas of risk for your organisation in % out of 100%?



# 2013 OWASP CISO Survey 3/7



# 2013 OWASP CISO Survey 4/7



# 2013 OWASP CISO Survey 5/7

## Application Security Management System (ASMS) or Maturity Model (e.g., OWASP SAMM)



# 2013 OWASP CISO Survey 6/7

## Security Strategy:

- Only 27% believe their current application security strategy adequately addresses the risks associated with the increased use of social networking, personal devices, or cloud
- Most organisations define the strategy for 1 or 2 years:

Time Horizon	Percent
3 months	9.3%
6 months	9.3%
1 year	37.0%
2 years	27.8%
3 years	11.1%
5 years+	5.6%

# 2017 OWASP Summit London UK

## THE SUMMIT

The OWASP Summit 2017 is a 5-day participant driven event, dedicated to the collaboration of Development and Security professionals, with a strong focus on DevSecOps.

**Join us in interactive working sessions to tackle some of the hardest security problems we are facing in 2017 and create actionable solutions.**



### WHY

As Developers and Security professionals we know that the best work often happens when we take a collaborative approach.

But in our day-to-day (work) lives it can be hard to find support and space to pursue bold ideas with energy and commitment.

[+ Find out more about the summit](#)

### WHAT

The OWASP Summit 2017 will be a meeting of like-minded professionals focused on solving hard security problems.

Participants will join forces in thoroughly prepared working sessions and create actionable solutions to application security challenges.

[+ Take a look at the working sessions](#)

### WHERE / WHEN

Taking place from 12th to 16th June 2017 in Woburn Forest Center Parcs near London, all summit participants will be accommodated in lodges and villas, an ideal environment for maximum geek-time, synergy and collaboration.

[+ Discover the summit venue](#)

## TRACKS

Here are the current Tracks (with multiple Working Sessions)

AGILE APPSEC	CISO	DEVSECOPS	EDUCATION	JUICE SHOP	MOBILE SECURITY
OWASP	OWASP PROJECTS	OWASP TESTING GUIDE V5	OWASP TOP 10 2017	OWASPSAMM	RESEARCH
SECURITY CROWDSOURCING	SECURITY PLAYBOOKS	SUMMIT TEAM	THREAT MODEL		

# Vs. 2 Guide Contents: What Was Discussed

It was..

1. Make OWASP Resources More Visible to CISOs
2. Practices for Built-In Software Security into Processes, Testing Tools and Training
3. How to derive security requirements for compliance with Standards and Policies
4. How to Prioritize Vulnerability Management Based Upon Risks of Threats, Vulnerabilities and Attacks/Exploits
5. Guidance on How to Align Application Security Strategy with IT Strategy
6. How to factor emerging technology risks
7. How to Communicate Risks to Business Including Threats, Vulnerabilities (OWASP T10) and Impacts

Could be:

1. Incorporate reference to outcomes of 2017 Summit CISO track
2. Expand to include new tools/technologies such as RASP
3. Expand to include compliance with GDPR
4. Expand on new emerging technology risks and provide risk Mitigation Guidance (e.g. APIs and Micro-services, Biometrics)
5. Expand on Risk Mgmt. Strategies For Vendors, Provisioning, Supply-Chain Risks
6. Expand on new evolving threats facing web Applications (e.g. 0-day exploits)
7. Add reference to handbooks and playbooks for CISO's managed process

# Vs. 2 Survey Contents: What Was Discussed

It was..

1. **Do you worry more of External Threats** (e.g., phishing, website attacks) **or Internal Threats** (e.g., abuse of privileges, theft of information) ?
2. **What are your the main areas of risk** for your organisation in % out of 100 %?
3. **Compared to 12 months ago, do you see a change** in application security vs I/F threats?
4. **Do you have a cyber-security strategy?** If YES how many years does this strategy cover?
5. **Have you implemented a Maturity Model** (e.g., OWASP SAMM) ?

It could be (as suggestions):

1. **Which among the organization IT assets, networks or applications are considered more at risk of cyber-attacks ?**
2. **Does your organization have a cyber-threat intelligence program** and attack monitoring/alert process ?
3. **Does your organization has adopted S-SDLC?** If yes which one. Does it include threat modeling ?
4. **Is application security seen as an investment** or as a cost by your organization ?
5. **Does your planning of application security follow a long term strategy** (at least two years) ?

**PLEASE WRITE DOWN YOURS**

# 2017 OWASP Summit: CISO Guide Outcomes

## Outcomes

---

The Application Security Guide for CISO 2013 Version Goals were:

1. Make Application Security and OWASP More Visible to Application Security Managers & CISOs
2. Analyse Reasons for Adopting An Application Security Program by An Organisation (e.g. Tactical and Strategic)
3. Explain Difference Between Technical Risks and Business Risks including How to Estimate Costs of Data Breaches
4. Factor The impact of Emerging Technologies in Application Security Program (e.g. Mobile, Cloud, Web Services) and provide guidance
5. Provide Examples of Metrics & Measurements for Vulnerability Risk Management

For The Planned 2018 Version, Which Problems and Solutions/Guidance We Can Expand Upon ? (NOTE These Will be Assessed With Expanded CISO Survey Questions):

1. Impact of GDPR on AppSec and Recommendations (Including Outcomes of 2017 Summit CISO track)
2. Emerging technology risks and Risk Mitigation Guidance (e.g. APIs and Micro-services, Biometrics)
3. Evolving Threats Facing Web Applications (e.g. 0-day exploits of AppSec vulnerabilities) and solutions (e.g. improved attack detection with new tools such as Outcome 1 (unranked) – What topics would you like covered in the new CISO guide? as RASP)
4. Others (brainstorming)

# 2017 OWASP Summit: CISO Guide Outcomes

## Synopsis and Takeaways

### Outcome 1 – What topics would you like covered in the new CISO guide? (unranked)

- Incorporate reference to outcomes of 2017 Summit CISO track
- Expand to include new tools/technologies
- Expand to include compliance with GDPR
- Expand on new emerging technology risks and provide risk Mitigation Guidance (e.g. APIs, proliferation, and Micro-services/interoperability, Biometrics, Cloud (internal and external), strategies for managing risk in Cloud environments)
- Expand on Risk Management Strategies for Vendors, Provisioning, Supply-Chain Risks
- Expand on new evolving threats facing web Applications (e.g. 0-day exploits)
- Add reference to handbooks and playbooks for CISO's managed process
- Where to provide guidance or where to put a focus, e.g., 5,000 applications in different countries, where to allocate security resources in such a situation
- How to get visibility across the organisation – who is doing what. As CISO you need to know what changes are being made, and where
- Corporate culture: how can a CISO be an agent of change and overcome cultural challenges? Knowing the corporate culture to enable CISO to function properly; trust is crucial to success
- Success stories as examples of how to win – people can refer to these as a value-add – how can the CISO provide value to the business
- Knowing the right questions to ask triggers the appropriate response and action
- A proactive, strategic CISO is better than a reactive one: knowing to shift focus from fighting fires to ensuring the fires do not get out of control
- After an incident, think about how to promote change; train people to think holistically not just about the incident, but about the impact of the incident
- Involvement CISO should be involved in road mapping for future deployment and included in business development meeting so CISO can plan ahead
- Format: It was agreed that a handbook would have more value than a playbook given threat variables between company requirements

# 2017 OWASP Summit: CISO Survey Outcomes

## Outcome 2 – What type of question would you like included in the new CISO guide? (unranked)

- Which among the organization IT assets, networks or applications are considered more at risk of cyber-attacks ?
- Does your organization have a cyber-threat intelligence program and attack monitoring/alert process ?
- Does your organization has adopted S-SDLC? If yes which one. Does it include threat modeling ?
- Is application security seen as an investment or as a cost by your organization ?
- Does your planning of application security follow a long term strategy (at least two years) ?
- Need to ask questions about how to map the scope, application, and business process perspectives
- How to manage risk from third parties, private vs. public premise
- How do you manage the risk for developing technologies, such as the Cloud?

## Who

---

The target audience for this Working Session is:

- Information security professionals who are responsible for managing and delivering application security programs, including security in the SDLC (S-SDLC)
- Information security officers in senior management roles, including technology managers/directors responsible for managing software and application security

# 2018 OWASP CISO Guide & Survey: Next Steps

Roadmap, Status and Goals/Objectives:

1. Reboot the project (at AppSec USA 2017 Project Summit)
2. Reactivate OWASP CISO mailing list (done)
3. Create new version 2, wiki, GitHub repository (in progress)
4. Develop the contents in Q4 as being discussed at OWASP Summit in London back in June (in progress)
5. In sync, create a 2018 CISO survey in Q4 to be used in 2018 Q1 to gather answers from CISOs at chapter meetings, CISO summits using Survey Monkey lists (not started yet)
6. **Main goal is to develop the first draft of version 1 by Q1 2018 and a reviewed version by Q2 2018**