Application Security Guide for CISO & Survey
Version 2, 2018 Edition
Project Updates

Marco M. Morana, OWASP CISO Guide Project Lead

ORLANDO
2017
APPSEC USA 2017
September 19 - 20 Training Days and September 21 - 22 Conference Days | Orlando, FL

Agenda

2013 OWASP CISO GUIDE VERSION 1

- **Why we developed**
- **Main Themes**
- **Lesson learned from OWASP CISO Survey 2013-2014**

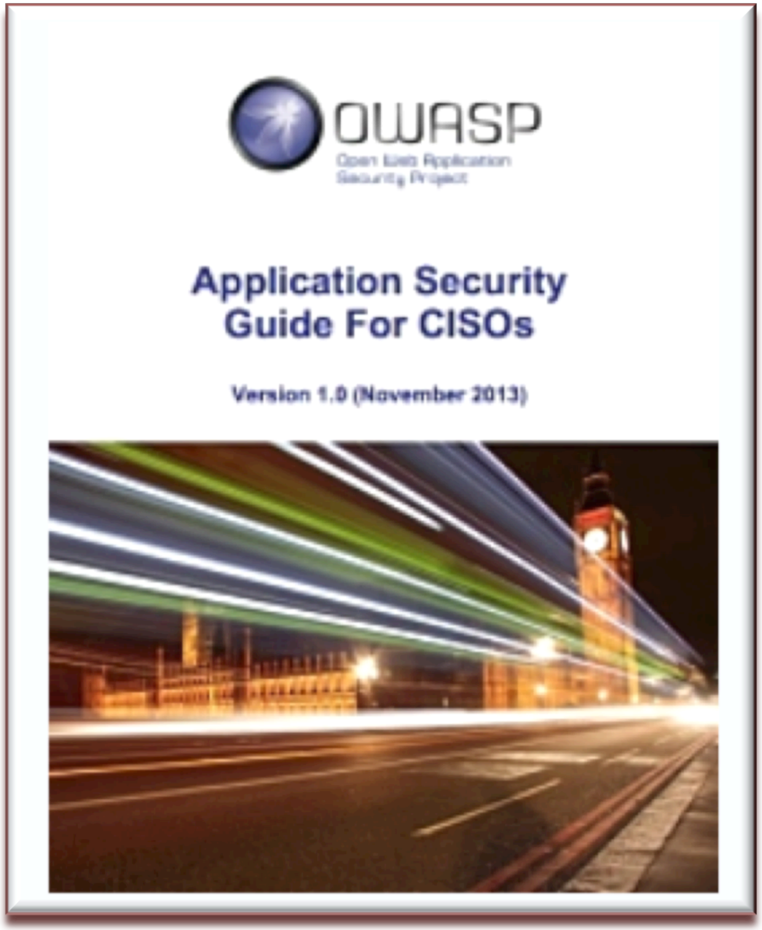
Planned 2018 OWASP CISO GUIDE VERSION 2

- **CISO discussions at 2017 OWASP Summit in London**
- **Outcomes of CISO track discussions**
- **Roadmap for updated to vs. 2 + (mini CISO 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
Open Web Application Security Project

Application Security Guide For CISOs

Version 1.0 (November 2013)

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

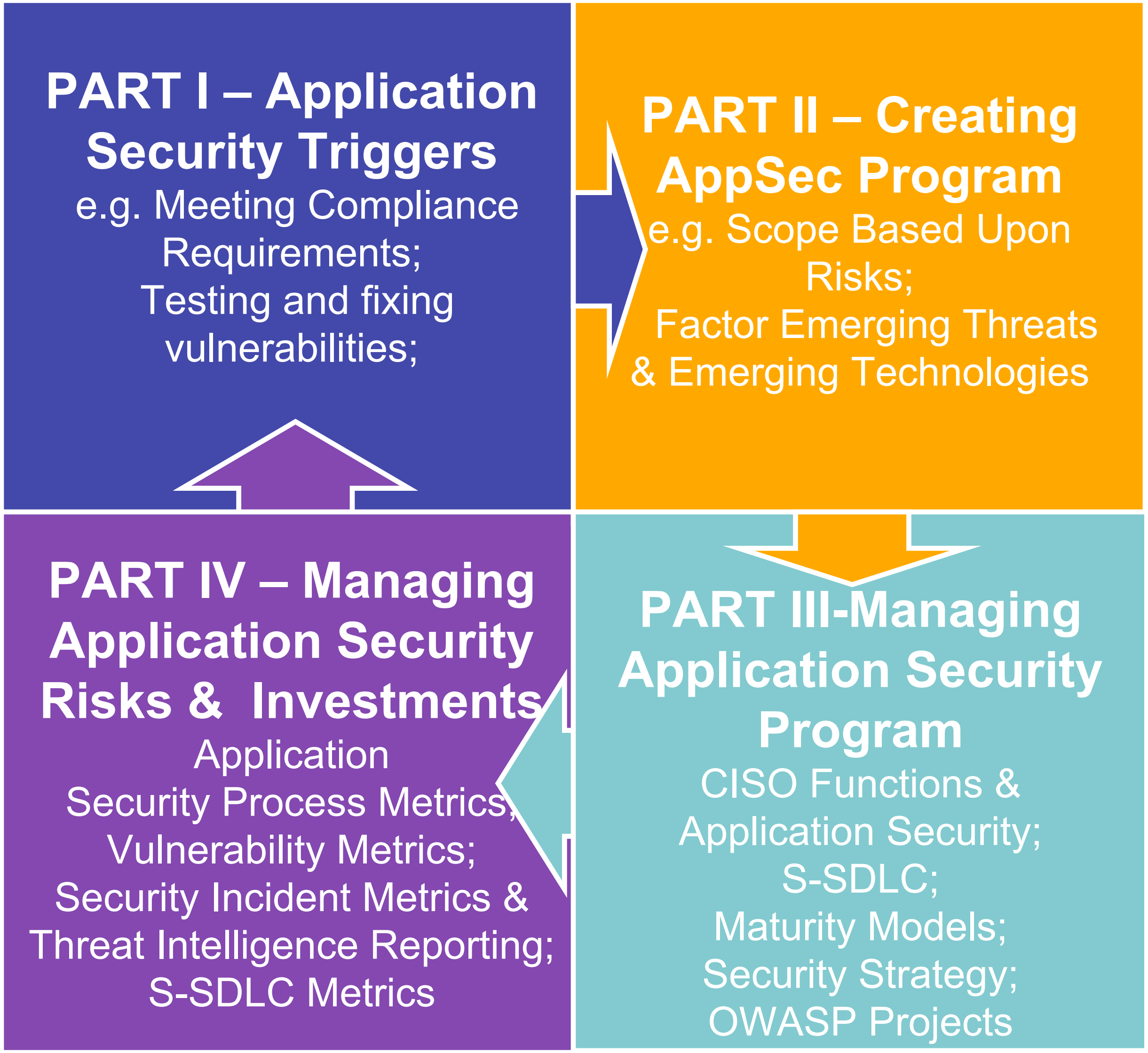
Why We Developed the CISO Guide Version 1 (2013)

DevOps Manager: can we include secure coding training for S/W developers ?

Business-Product Manager: Can we align this with our project cycle? What will be the impact on releases?

CISOs: I need to make sure our apps comply with PCI-DSS and OWASP Top Ten. I need to initiate a Security in SDLC program and activities such as threat modeling and secure code reviews

Main Themes For CISO Guide Version 1



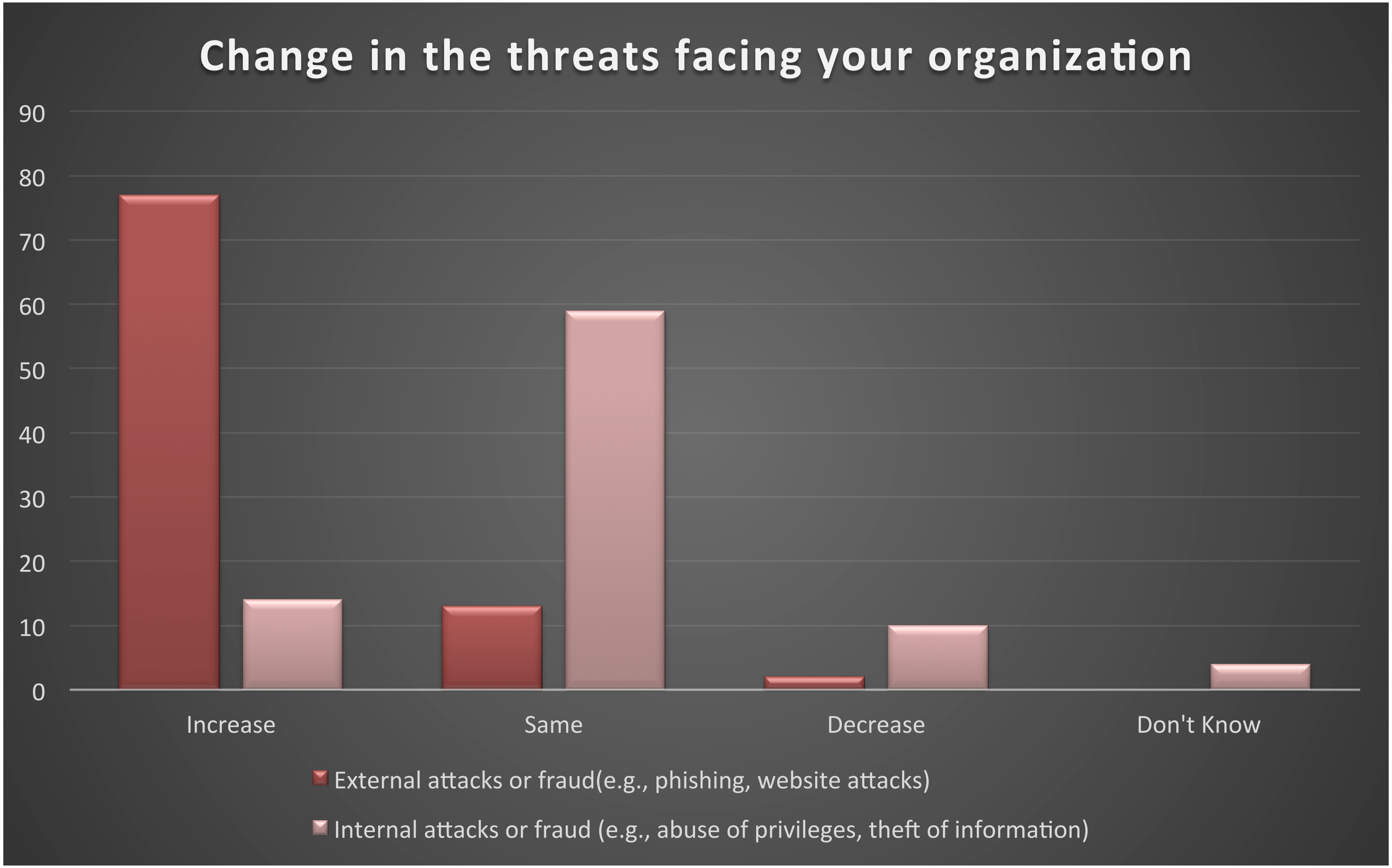
PART I – Application Security Triggers
e.g. Meeting Compliance Requirements;
Testing and fixing vulnerabilities;

PART II – Creating AppSec Program
e.g. Scope Based Upon Risks;
Factor Emerging Threats & Emerging Technologies

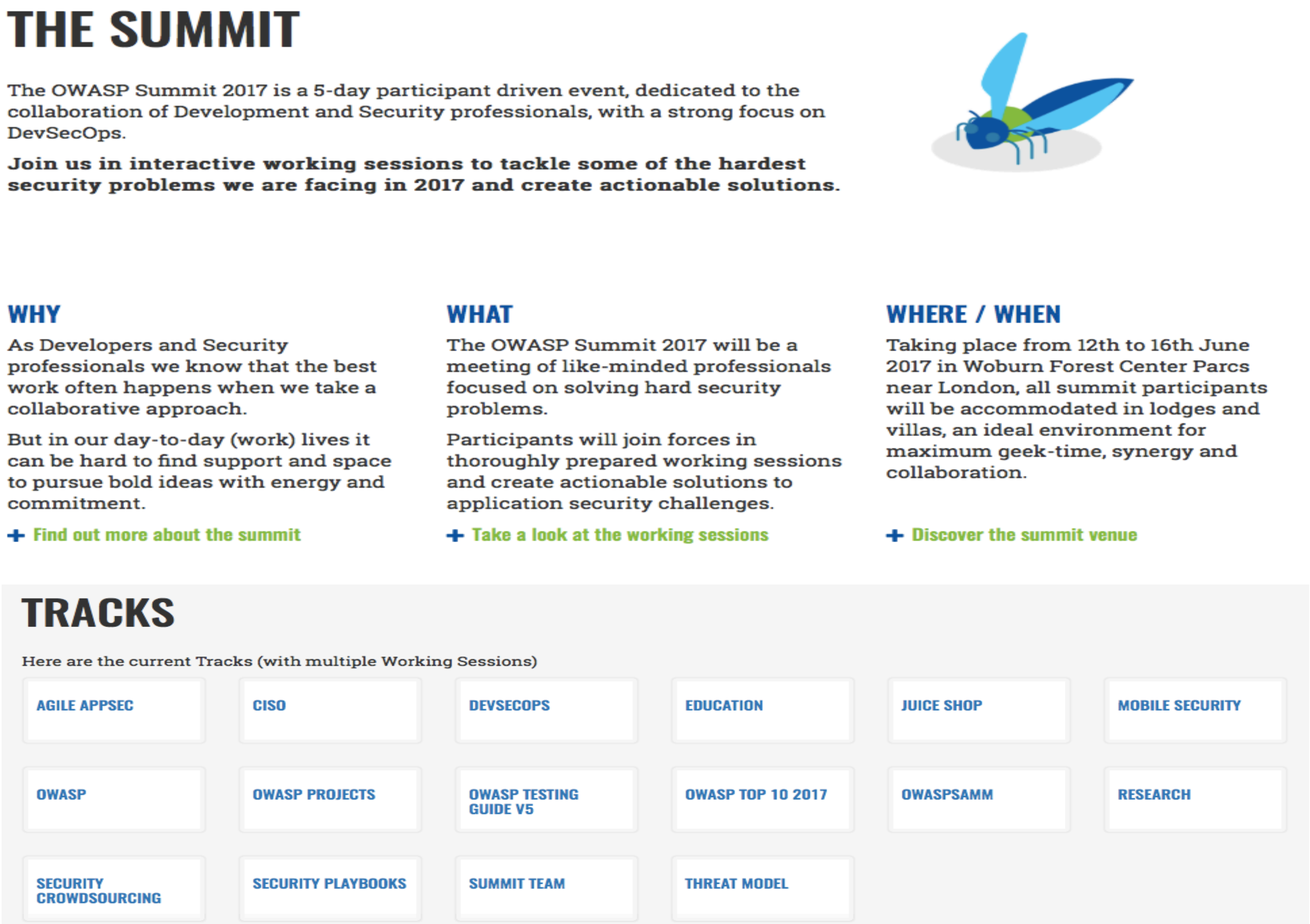
PART III-Managing Application Security Program
CISO Functions & Application Security;
S-SDLC;
Maturity Models;
Security Strategy;
OWASP Projects

PART IV – Managing Application Security Risks & Investments
Application Security Process Metrics;
Vulnerability Metrics;
Security Incident Metrics & Threat Intelligence Reporting;
S-SDLC Metrics

Lesson Learned From OWASP 2013 CISO Survey 1/7



CISO Guide Reboot @ 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

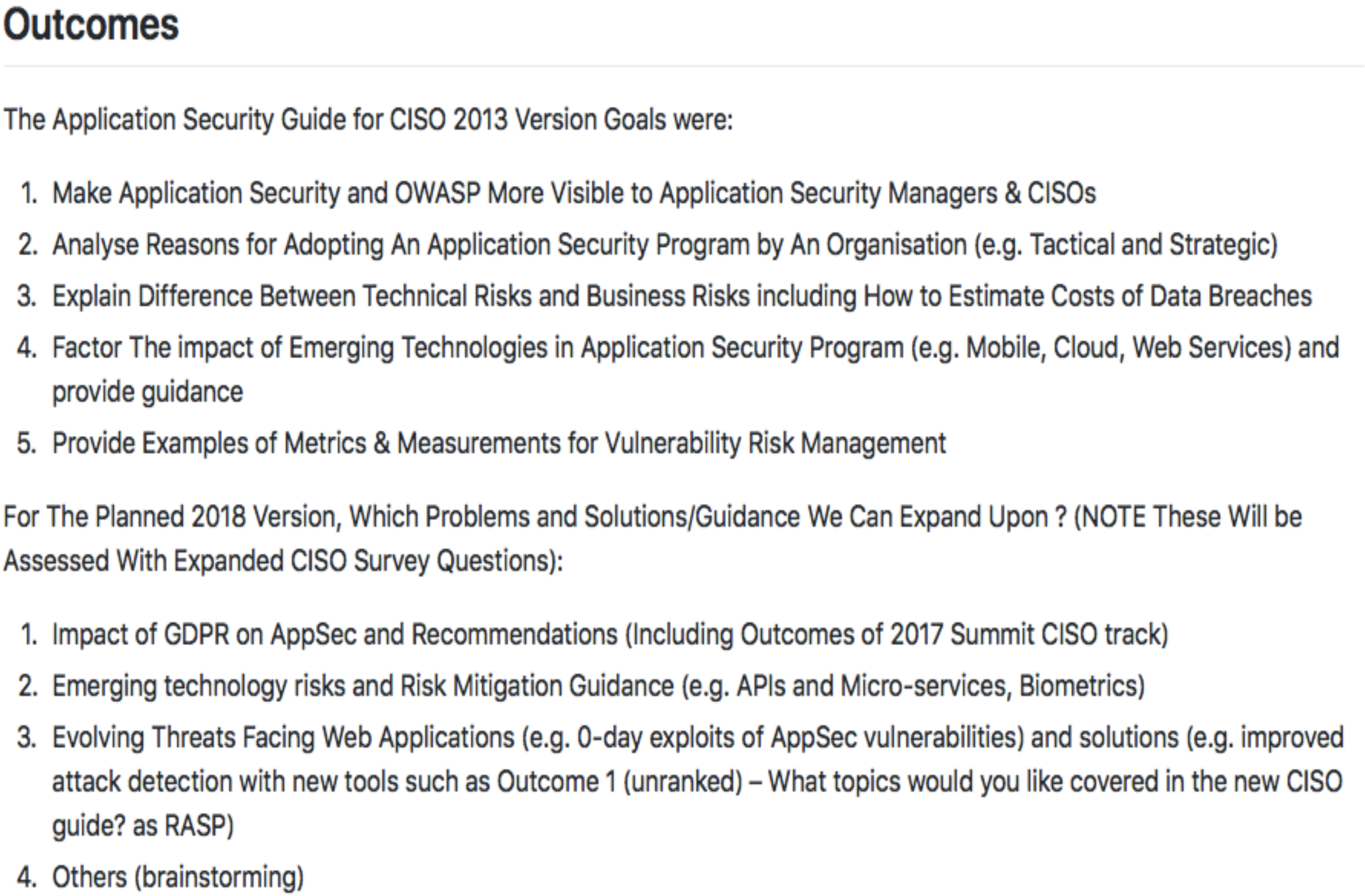
It was..

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

2017 OWASP Summit: CISO Discussion Outcomes (1/2)



Outcomes

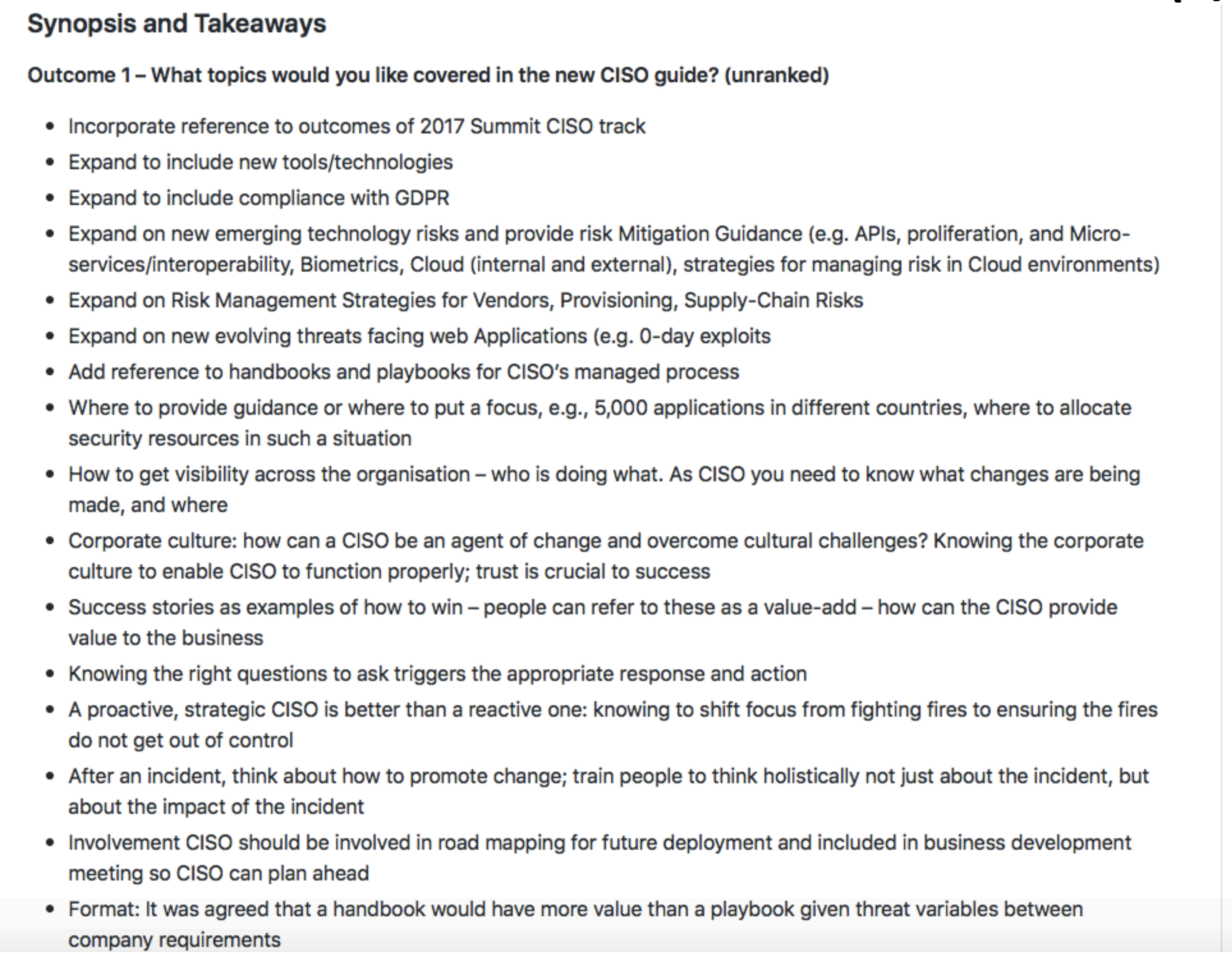
The Application Security Guide for CISO 2013 Version Goals were:

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 Discussion Outcomes (2/2)

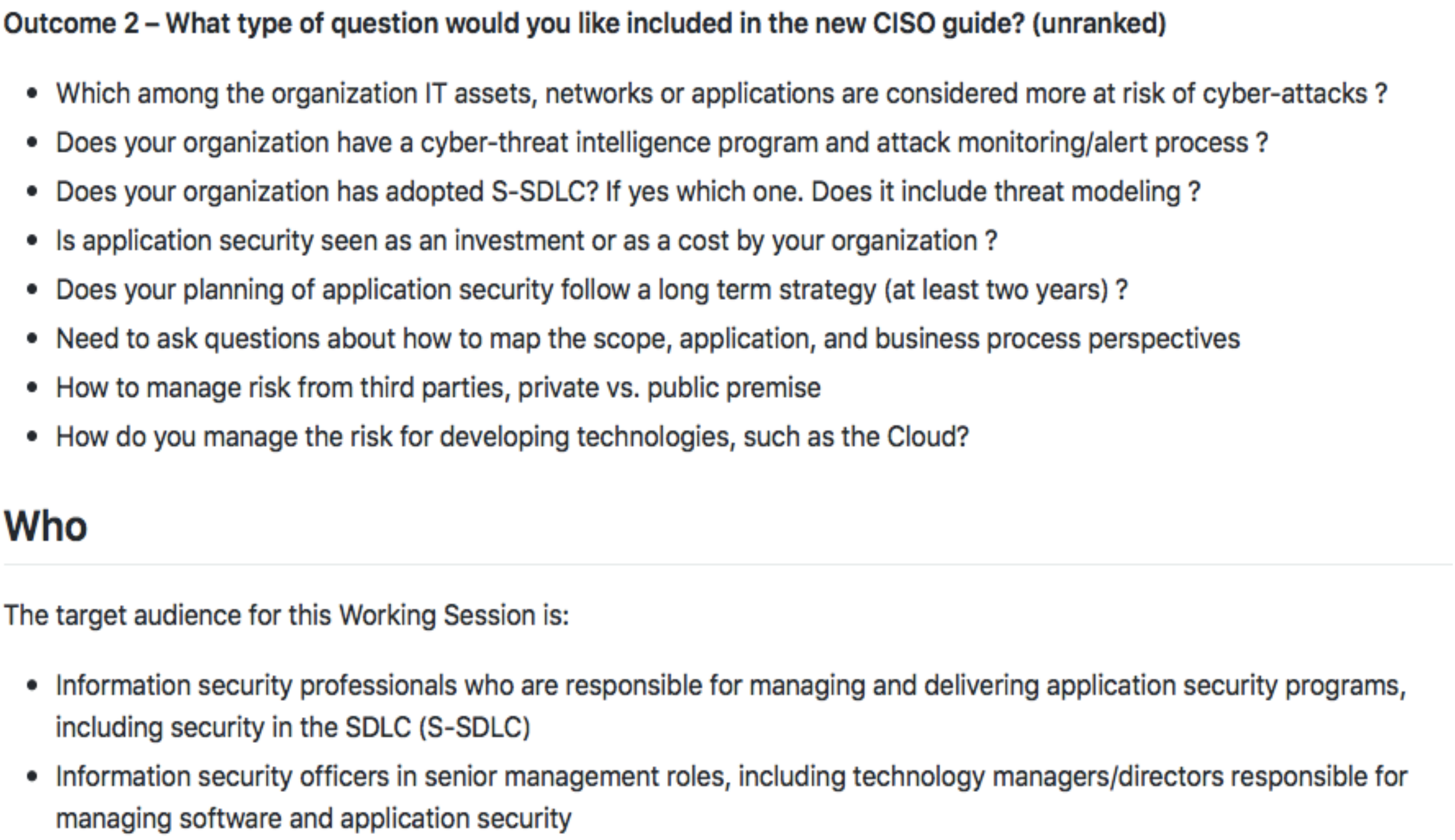


Synopsis and Takeaways

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

OWASP CISO Guide Vs2 2018 Edition Plan

Roadmap and (Status) :

1. **Reboot the project** (at AppSec USA 2017 Project Summit) create new version 2, wiki, GitHub repository (done)
2. **Reactivate OWASP CISO mailing list** (done)
3. **Call for contributions, sponsors and revisions** (in progress)
4. **Develop the contents:** (in progress) as being discussed at OWASP Summit in London back in June (in progress)
5. **Create a mini 2018 CISO:** to socialize with CISOs at CISO summits using Survey Monkey lists (not started)
6. **Create contents for the first draft of version 2**: (in progress)

Goal is produce a draft by 30/3/2018 and a reviewed version by end of June 2018