



OWASP - CISO Guide and CISO report 2013 for managers

(with special thanks to Marco Morana)

Tobias Gondrom

*Board member of OWASP London
Project Lead of the OWASP CISO Survey & Report
Managing Director, CISO of Thames Stanley*

tobias.gondrom@owasp.org

Tobias Gondrom

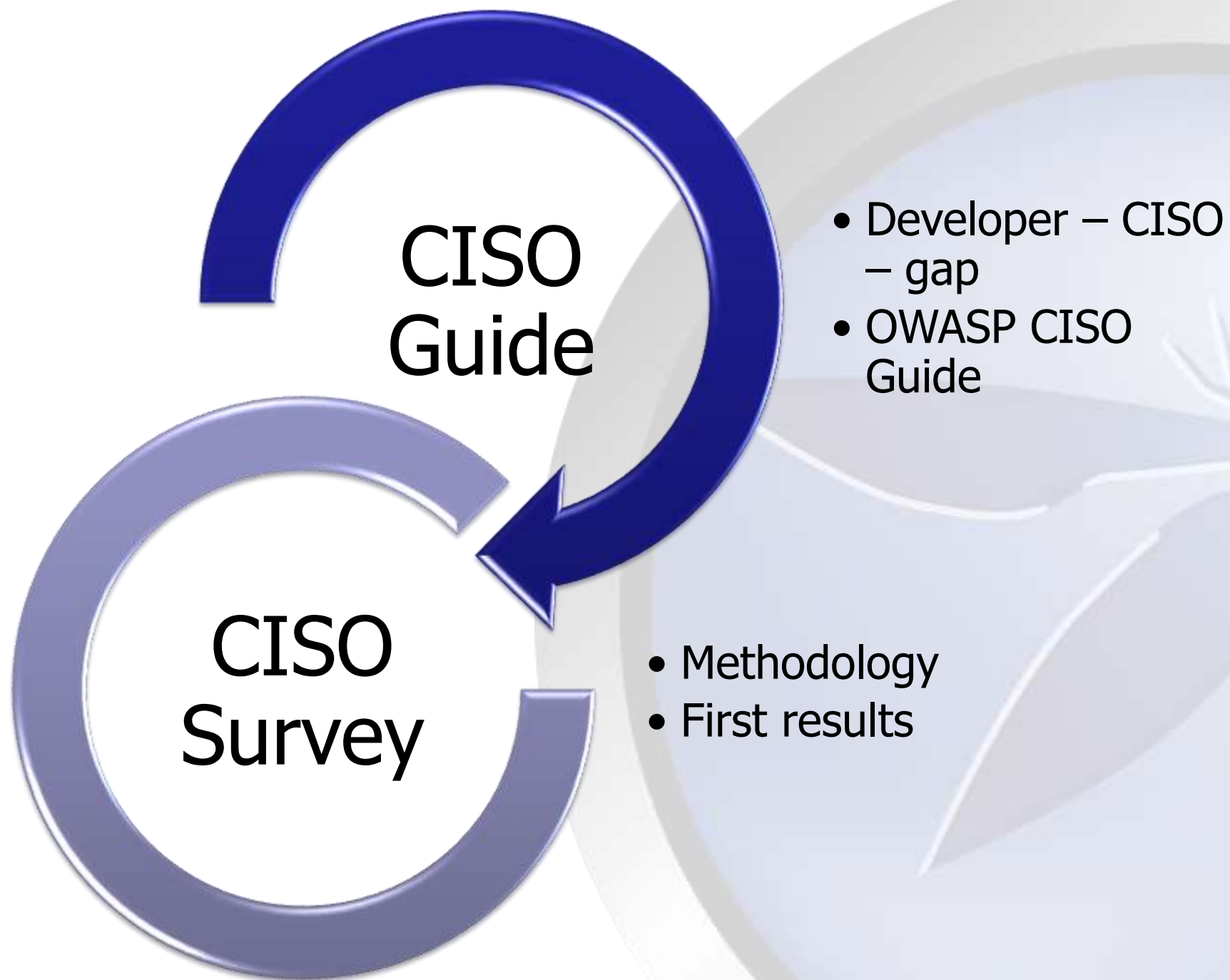


- 15 years information security experience
(Global Head of Security, CISO, CTO)
CISSP, CSSLP, CCISO
- 12 years management of application development
- Sloan Fellow M.Sc. London Business School
- Thames Stanley: Managing Director,
CISO Advisory, Information Security & Risk Management,
Research and Advisory
- Author of Internet Standards on Secure Archiving, CISO
training and co-author of the OWASP CISO guide
- Chair of IETF Web Security Working Group
<http://datatracker.ietf.org/wg/websec/charter/>
Member of the IETF Security Directorate
Cloud Security Alliance, Hong Kong chapter board
- London OWASP chapter board member
OWASP Project Leader for the CISO Survey & Report

Agenda

- Application Security Guide For CISOs
 - Developer – CISO – gap
 - [OWASP CISO Guide](#)
- CISO Survey & Report 2013
 - Methodology
 - First results

Agenda



Application Security: What Software Developer Say ?



What Can Security Professionals Learn
From Web Application Developers ?



Developers largely say applications are not secure, while security professionals are much more optimistic:

Developers say application security lacking

By Brandon Butler | Network World US | 20 March 12

- **70% of developers say security of applications is not addressed vs. 50 % of security officers**
- **80% of developers say there is no build security in process S-SDLC vs. 64% security professionals**
- **68% of developers and 47% of officers say their applications had a security breach in the past 2 yrs**
- **50% of developers and officers say they did not receive software and application security training**
- **15% of developers and 12% of security officials say their applications meet security regulations**

Source: <http://www.pcadvisor.co.uk/news/network-wire/3345773/developers-say-application-security-lacking/#ixzz2Vj0QCALy>

Application Security: What The CISOs Say ?



What Can Security Professionals Learn
From Web Application Developers ?

Which Security Functions Matter The Most to CISOs?



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 Can Security Professionals Learn
From Web Application Developers ?

How We Bridge The Software-Developer CISOs Gap?



What Can Security Professionals Learn
From Web Application Developers ?

Application Security Guide & Survey For CISOs



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

Organization Supporters of OWASP's mission





Application Security Guide For CISOs

1. Make Application Security More Visible to CISOs
2. Provide Guidance For Instituting and Managing Application Security Processes
3. Assure Compliance of Web Applications With Security Regulations For Privacy, Data Protection and Information Security
4. Prioritize Fixing Vulnerabilities Based Upon Risk to the Business
5. Analyze Cyber-Threats & Attacks Targeting Web Applications And Identify Countermeasures
6. Institute Training for Application Developers
7. Measure Risk Reduction and Process Management



CISO Guide – Part I: Reasons for Investing in Application Security

Information Security Standards, Policies and Compliance

- Identifying Standards and Policies in Scope for Compliance
- Capturing Application Security Requirements: PCI-DSS, FFIEC, GLBA, Privacy Laws

Risk Management

- Proactive vs. Reactive Risk Management
- Asset Centric Risk Management
- Technical vs. Business Risk Management
- Risk Management Strategies
- Threat Analysis and Awareness of Emerging Threats

CISO Guide – Part II: Criteria for Managing Application Security Risks

Estimating the Risks of Vulnerability Exploits

- Estimating the Probability & Business Impact of Vulnerability Exploits

Mitigating the Risks of Attacks Targeting Web Applications

- Threat Agents their Motivations and Historical Impacts
- Threat Agents and Type of Attacks
- Mitigating the Inherent Risks of New Application Technologies
 - Managing the Risk of Mobile Applications
 - Managing the Risks of Web 2.0 Technologies
 - Web 2.0 Vulnerabilities Exploited by Attackers
 - Security Measures To Mitigate Risks
 - Managing the Risk of Cloud Computing Services

CISO Guide: Part III: Selection of Application Security Processes

Addressing CISO's Application Security Functions

- Application Security Governance, Risk and Compliance, Security Metrics

Targeting Software Security Activities and S-SDLC Processes

How to Choose the Right OWASP Projects and Tools For Your Organization

CISO Guide: Part IV: Selection of Metrics For Managing Risks & Application Security Investments

Application Security Process Metrics

- Metrics and Measurements Goals

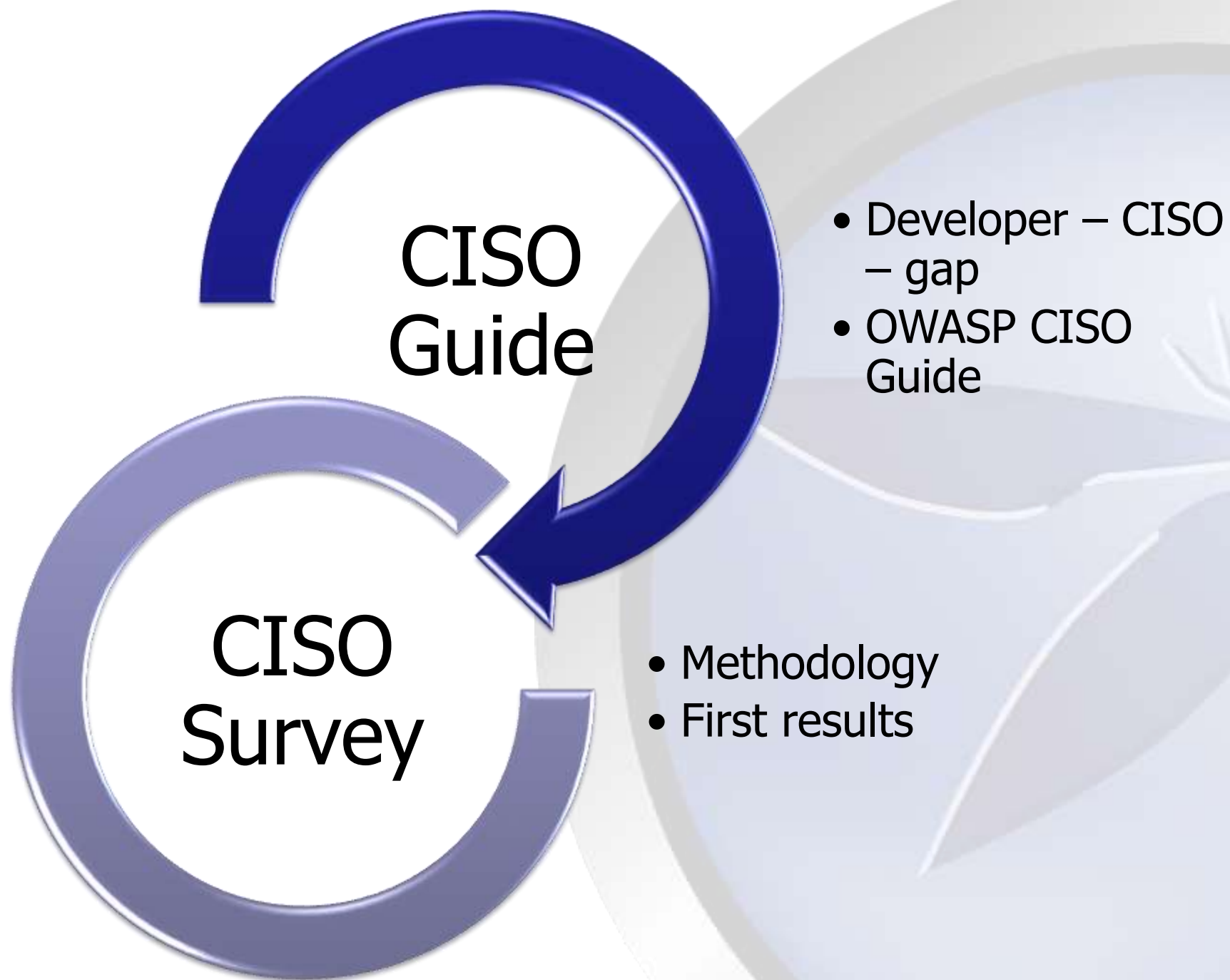
Application Security Risk Metrics

- Vulnerability Risk Management Metrics
- Security Incident Metrics
- Threat Intelligence Reporting and Attack Monitoring Metrics

Security in SDLC Management Metrics

- Metrics for Risk Mitigation Decisions
- Metrics for Vulnerability Root Causes Identification
- Metrics for Software Security Investments

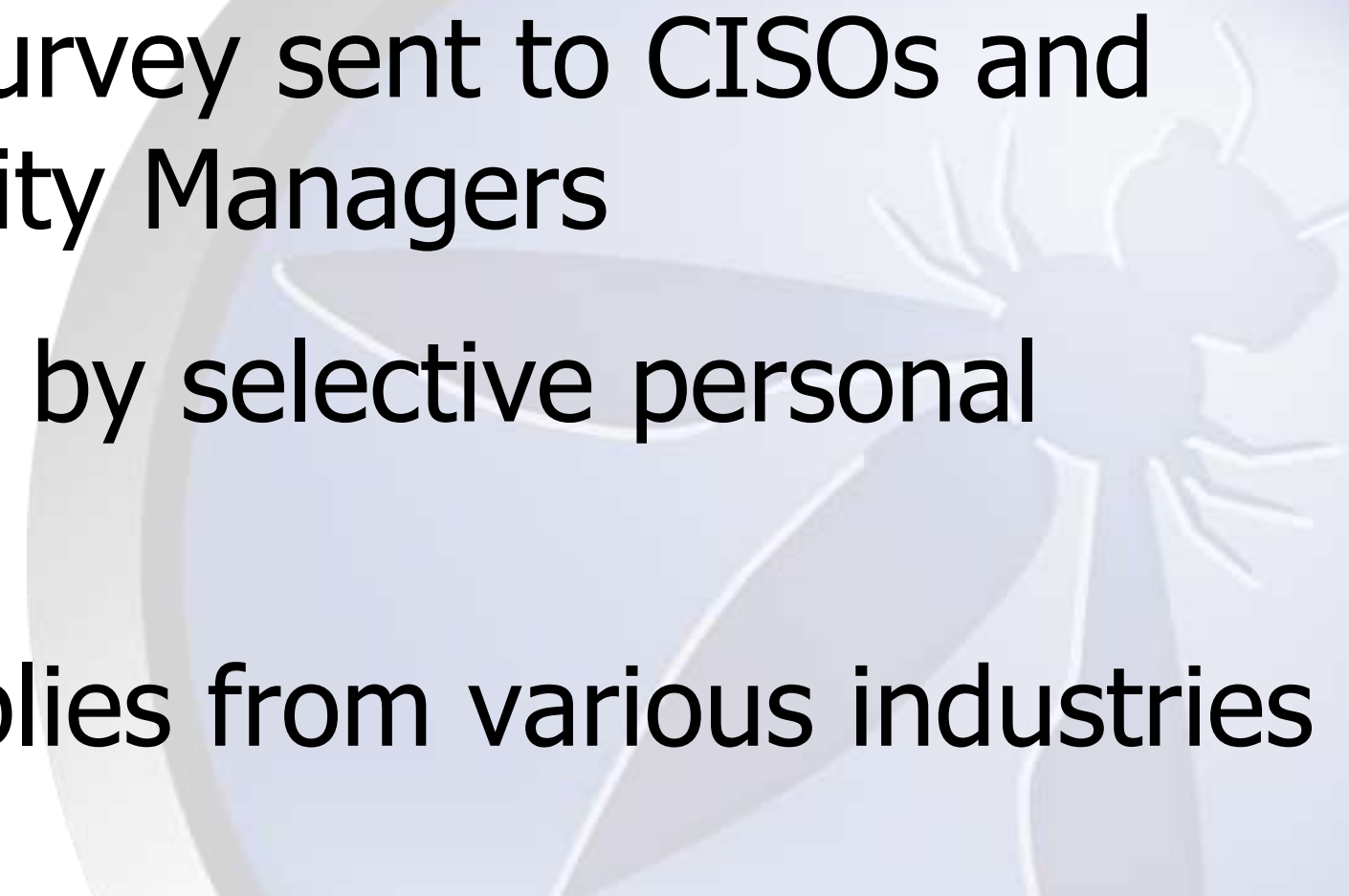
Agenda





CISO Survey

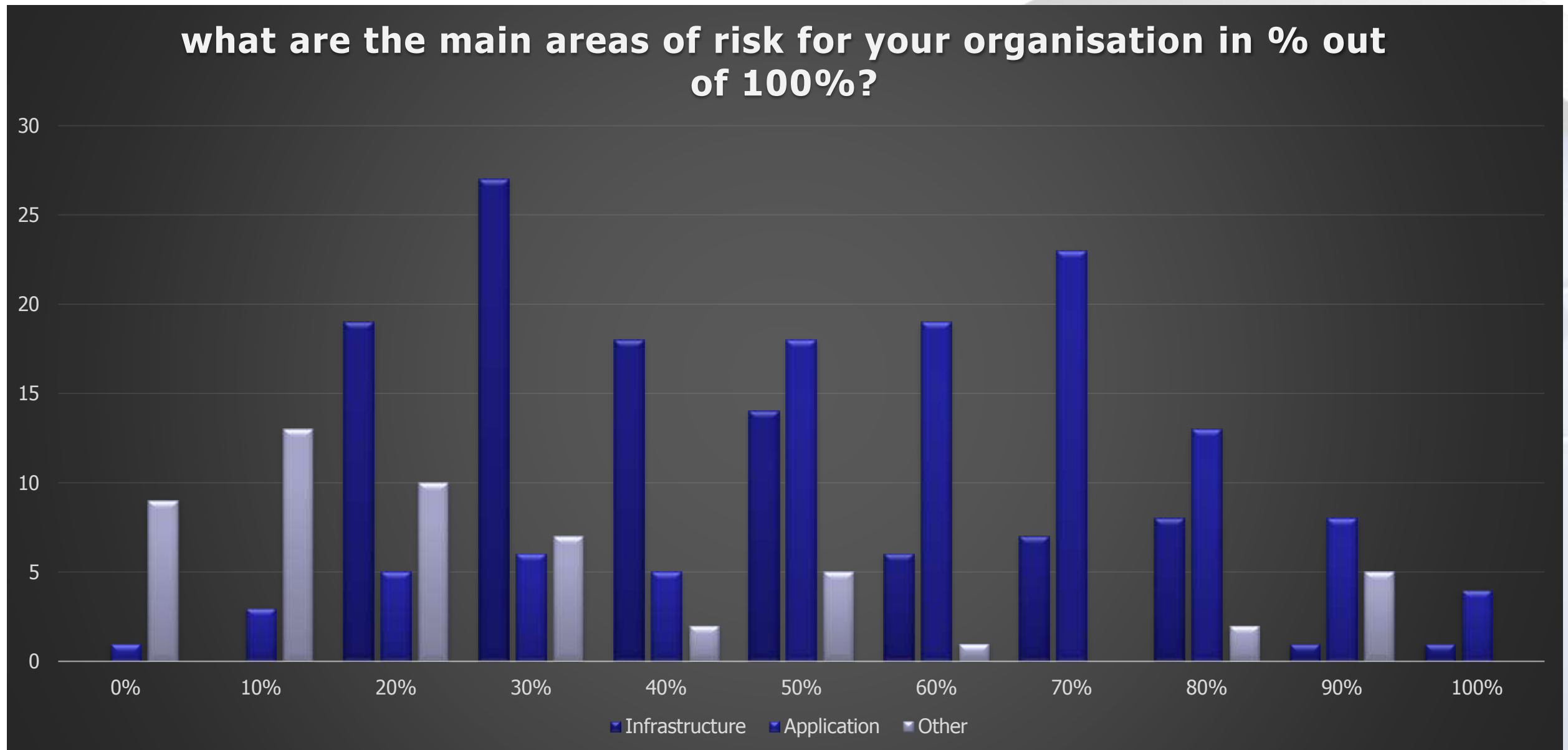
Methodology

- Phase 1: Online Survey sent to CISOs and Information Security Managers
 - Phase 2: Followed by selective personal interviews
 - More than 100 replies from various industries and counting...
- 

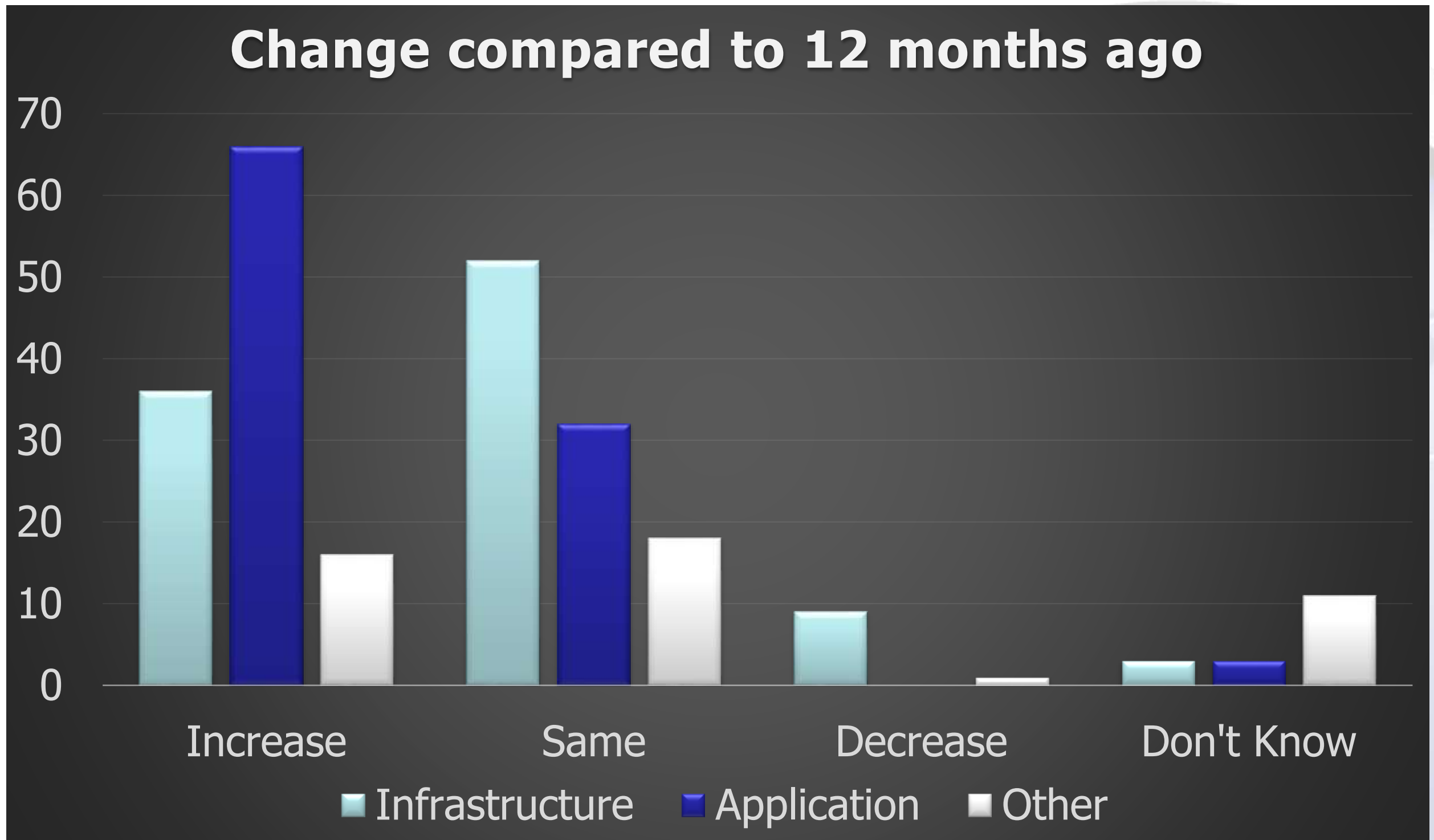
CISO Survey: Change in the threats facing your organization



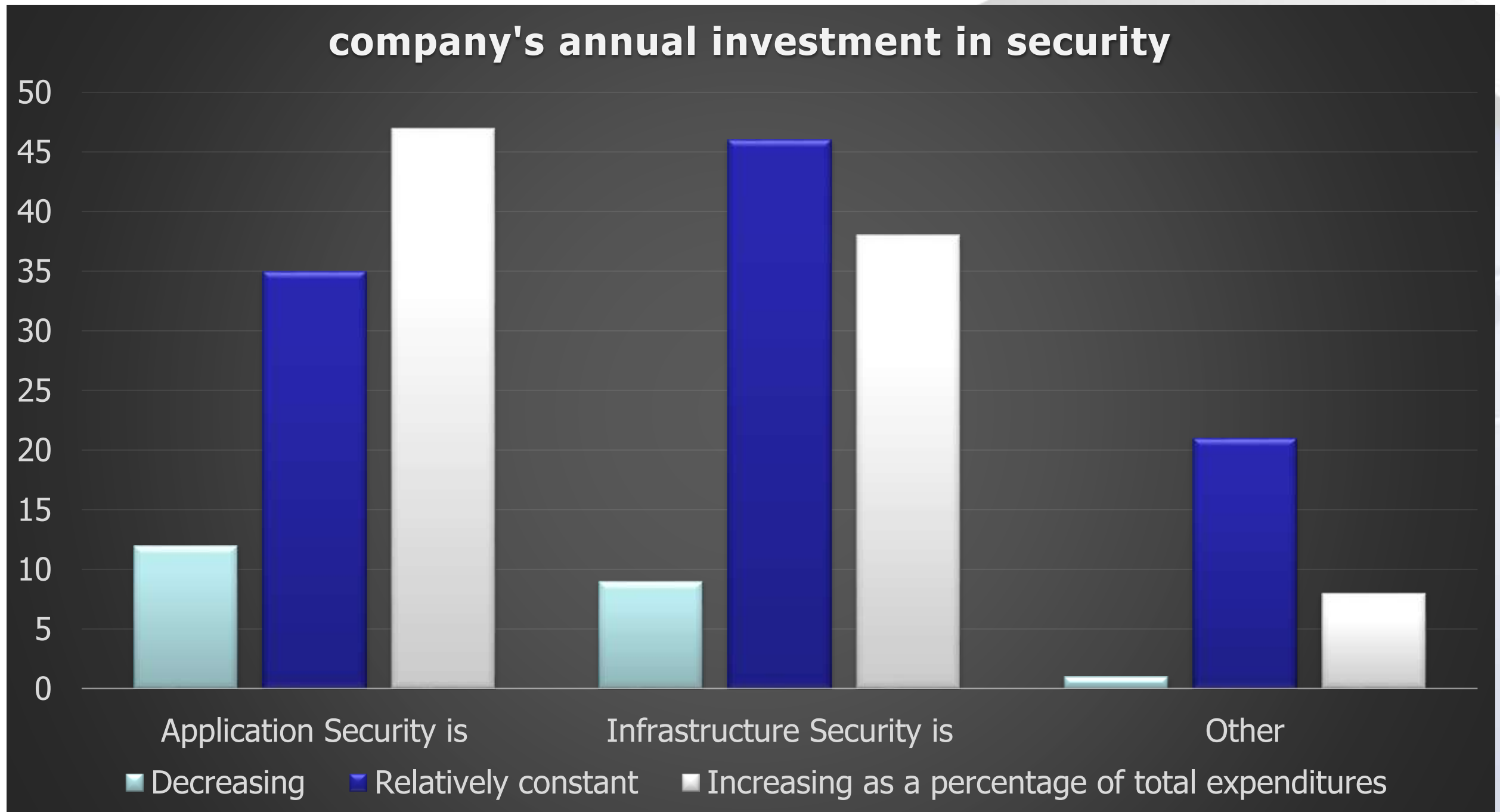
CISO Survey: Change in the threats facing your organization



CISO Survey & Report 2013



CISO Survey & Report 2013



CISO Survey & Report 2013

Top application security priorities for the coming 12 months



Secure development lifecycle processes (e.g., secure coding, QA process)

Security awareness and training for developers

Security testing of applications (penetration testing)

CISO Survey & Report 2013

level of significance of OWASP guidance, books and white papers within your organization

- Awareness material (e.g. Top-10)
- Code development guidelines
- Reference to leading practice
- Application development policy
- Testing methodologies
- Staff attending local OWASP chapter meetings for information
- Staff attending OWASP AppSec conferences

CISO Survey & Report 2013

Which of the following OWASP projects has your organization found useful? (note: we did not have a full list of 168 active projects)

☐ **OWASP Top-10**

☐ **Development Guide**

☐ **Secure Coding Practices Quick Reference**

☐ **Cheatsheets**

☐ **Application Security FAQ**

CISO Survey & Report 2013

Biggest challenge related to effectively delivering your organization's application security initiatives



Availability of skilled resources

Level of security awareness by the developers

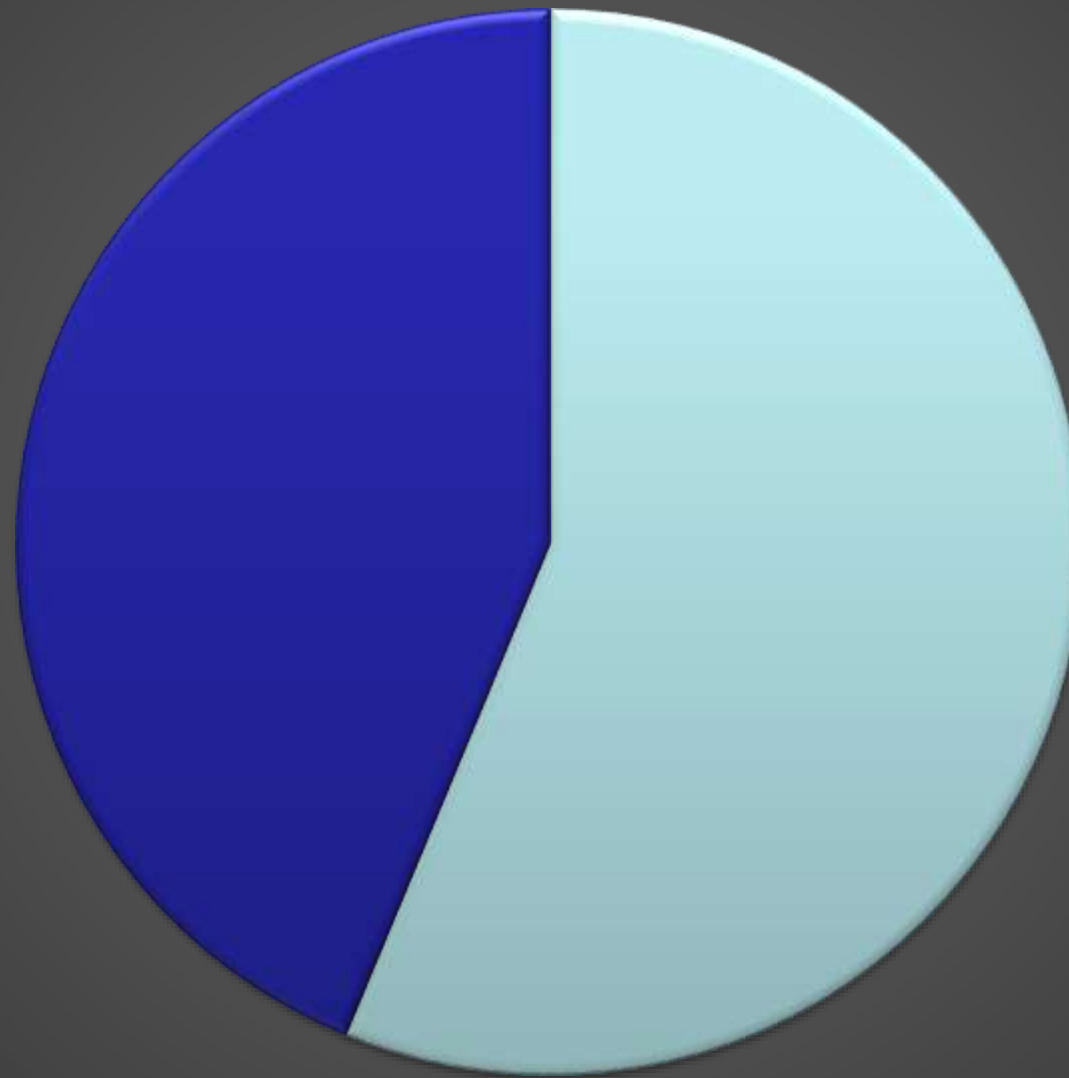
Management awareness and sponsorship

Organizational change

Adequate budget

CISO Survey & Report 2013

Does your organization have a documented application security strategy?



■ Yes ■ No

CISO Survey & Report 2013

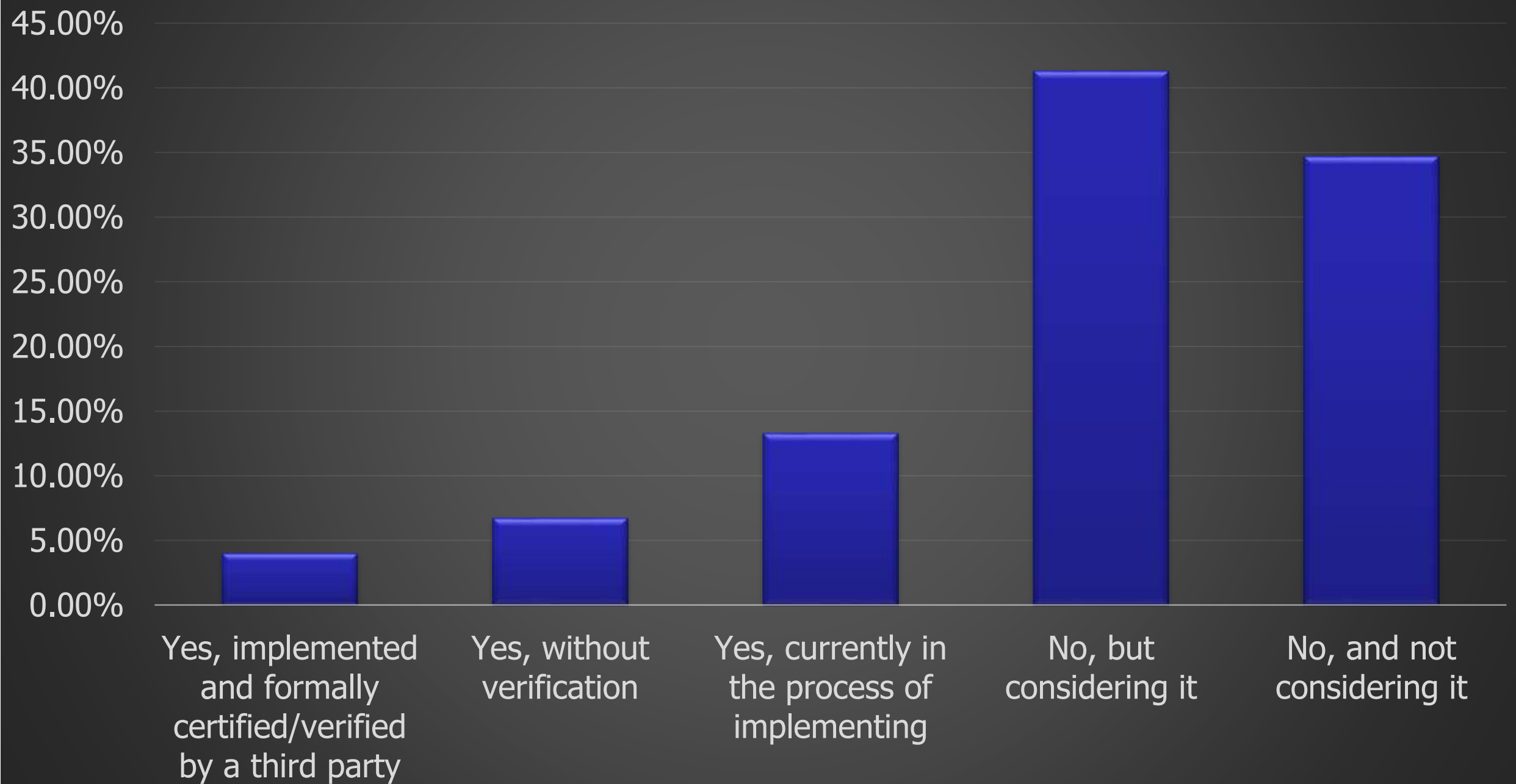
Security Strategy:

- 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%

CISO Survey & Report 2013

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

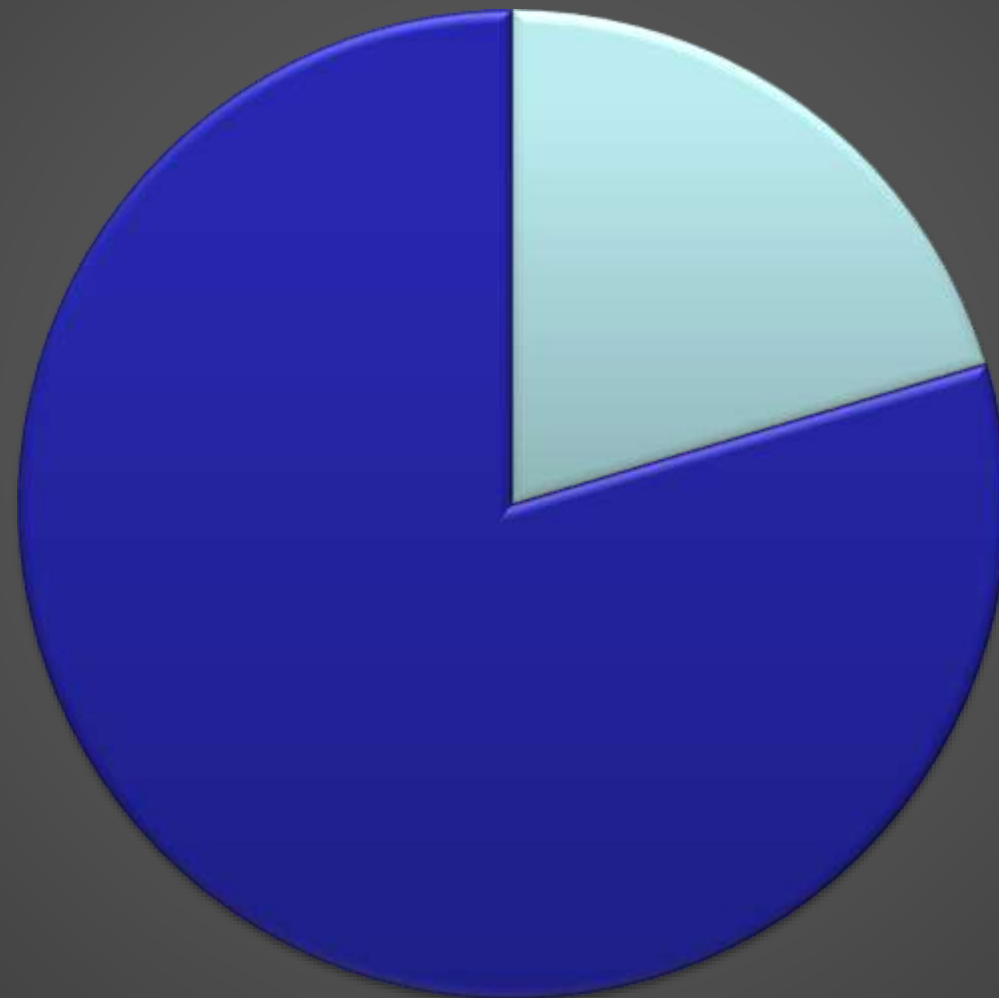


CISO Survey & Report 2013



CISO Survey & Report 2013

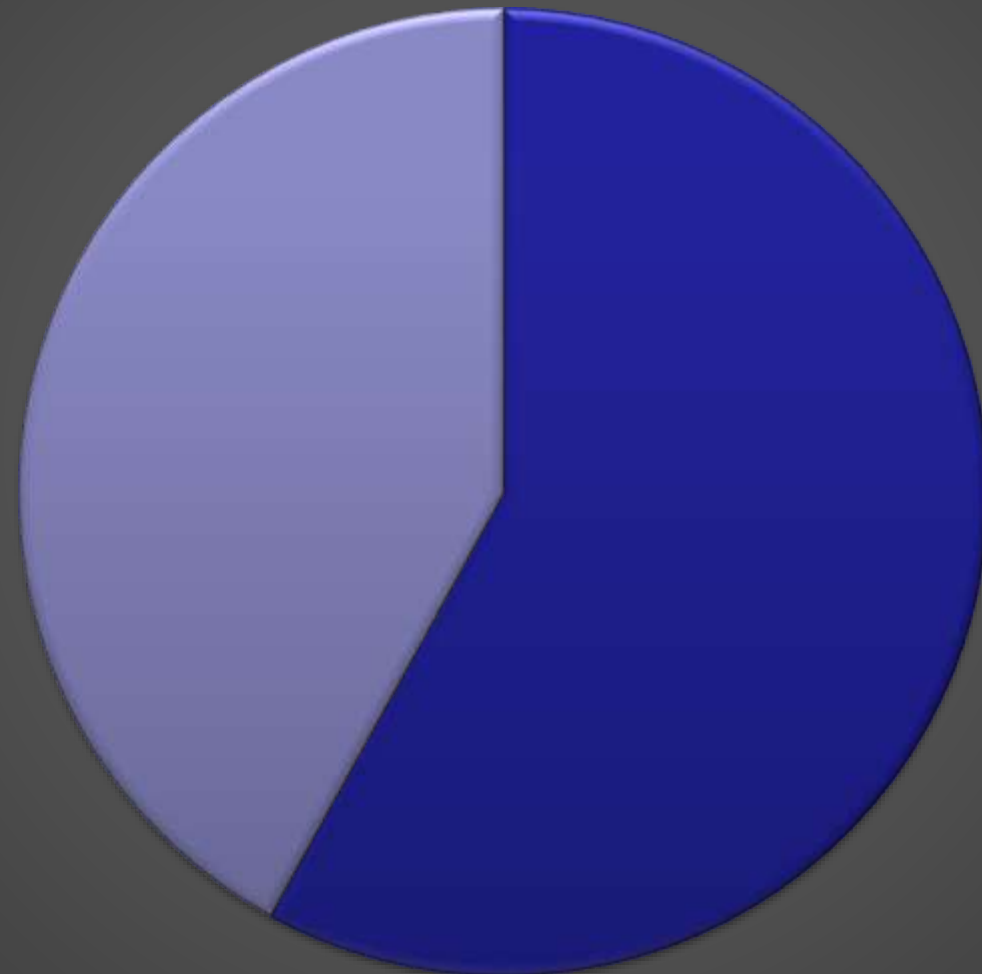
Did your company experience a data breach because of a web application security incident in the last 12 months?



■ Yes ■ No

CISO Survey & Report 2013

Do you see new threats to web applications negatively impacting your organisation?



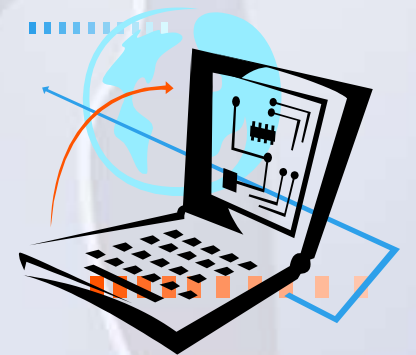
■ Yes ■ No

CISO Survey & Report 2013

What's next?

- Extended open survey time
- Conducting interviews
- Number Crunching...

... processing
... stay tuned ...





Further Resources:

- OWASP CISO Guide:

https://www.owasp.org/index.php/Application_Security_Guide_For_CISOs

- OWASP CISO Survey

<https://www.surveymonkey.com/s/CISO2013Survey>

- Email me: tobias.gondrom@owasp.org



Thank you

