OWASP CISO Survey Report 2015 – Tactical Insights for Managers

Tobias Gondrom
OWASP Global Board, CISO Survey Project Lead
CTO IP Security, Huawei
twitter: @tgondrom

Disclaimer

- *The views and opinions expressed in this presentation are those of the author and not of any organisation.*

- *“Everything I say is my own personal opinion. Especially the wrong ones….”*

About Me

HUAWEI

ROMA MMXVI

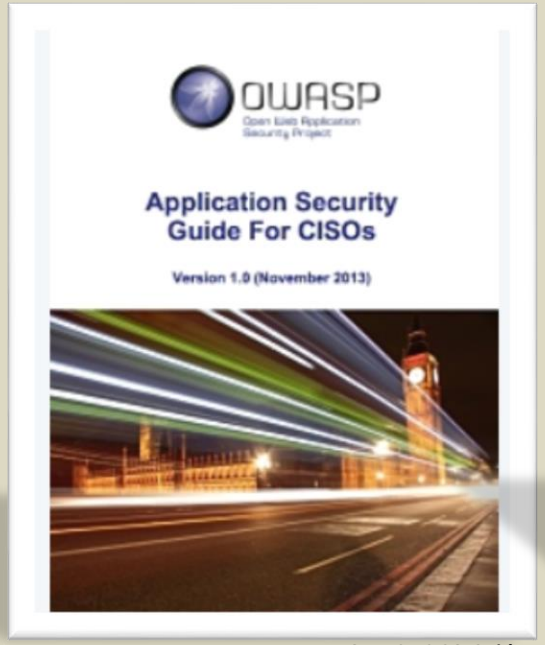
APPSEC EUROPE

OWASP
Open Web & Application Security Project, www.owasp.org
global non-profit open source security community

Tobias Gondrom
Global Board, OWASP
CTO Security, Huawei

- 20 years information security and development experience (Global Head of Security, CISO, CTO), CISSP, CSSLP, CCISO
- Project Leader OWASP CISO Survey Report
- Author of Internet Standards on Secure Archiving, CISO training and co-author of the OWASP CISO survey report and CISO guide
- Sloan Fellow M.Sc. London Business School
- Chair of IETF Trust, Member of IAOC (IETF Admininistrative Ovesight Committee), Chair of IETF Security WGs, Member of the IETF Security Directorate, Cloud Security Alliance HK chapter board member

Based on findings of the OWASP CISO Survey Report & CISO Guide



OWASP CISO Guide:
https://www.owasp.org/images/d/d6/Owasp-ciso-guide.pdf

OWASP CISO Survey:
https://www.owasp.org/index.php/OWASP_CISO_Survey

ROMA MMXVI

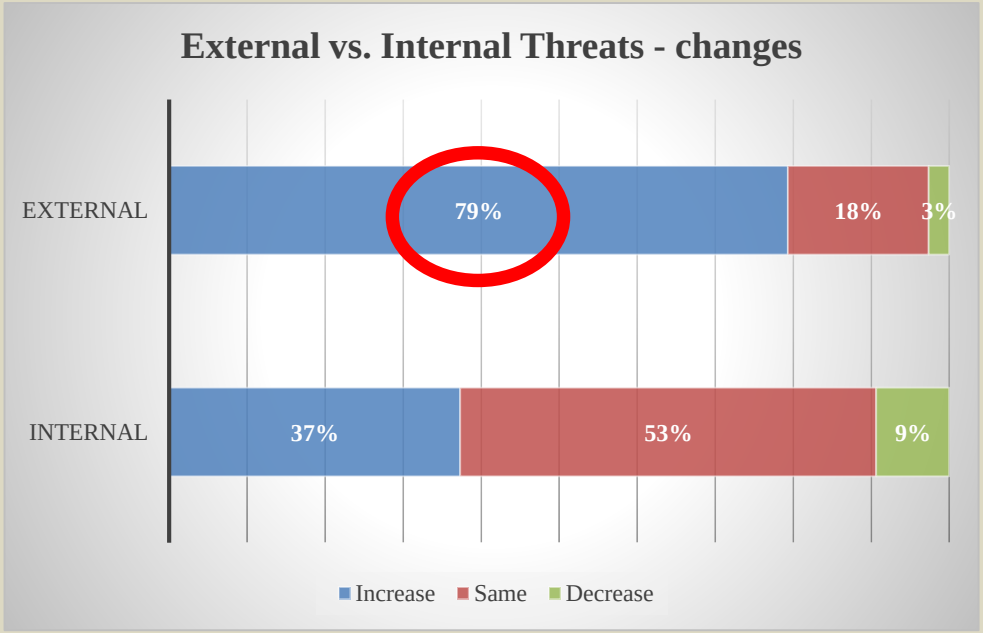
APPSEC EUROPE

CISO Survey

- Methodology
  - Phase 1: Online Survey sent to 1000s of CISOs and Information Security Managers, with comprehensive question sets
    - Dataset received of about 500 replies from various industries…
  - Phase 2: Followed by selective personal interviews
  - *Release of 2015 version in July 2016*


CYBER
ATTACKS
AHEAD

CISO Survey: External Threats are on the Rise!



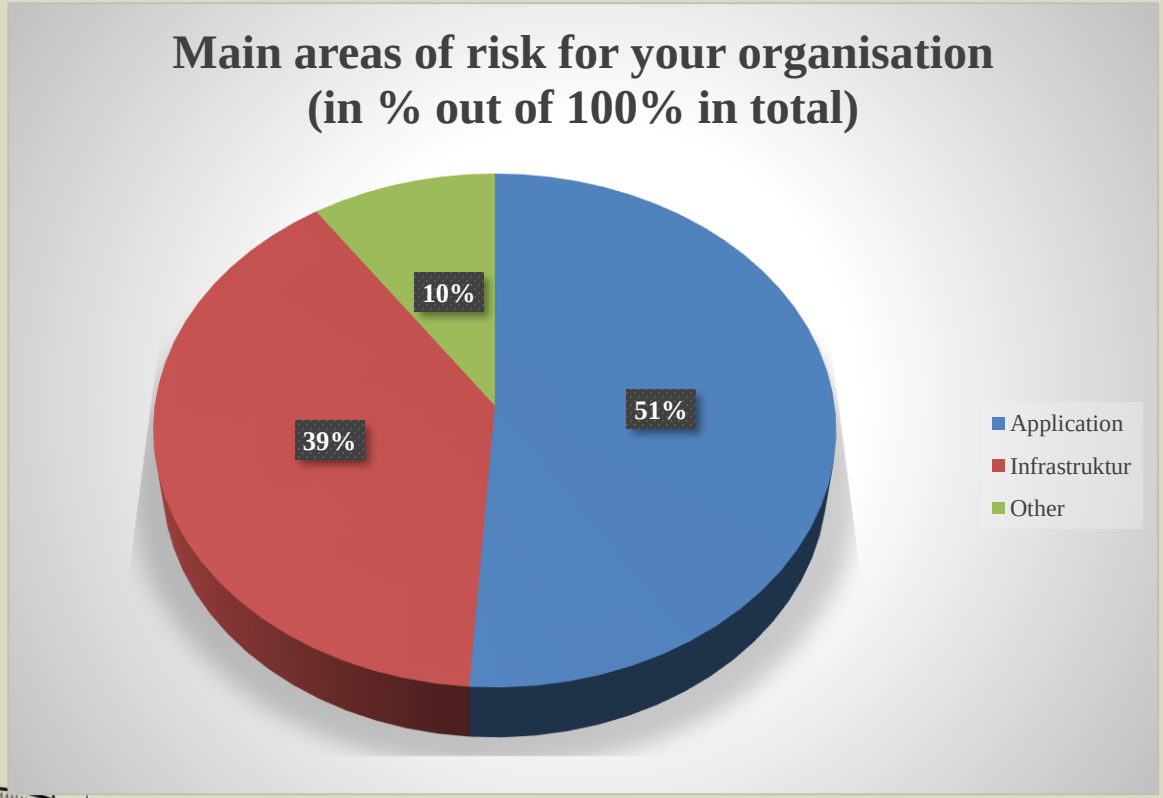
»External attacks or fraud (e.g., phishing, website attacks)

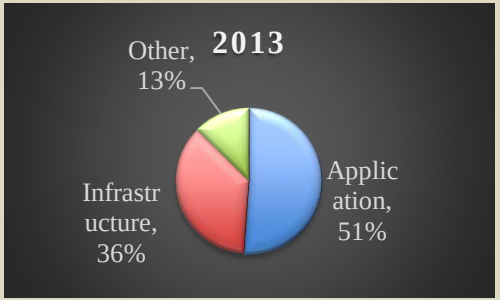
»Internal attacks or fraud (e.g., abuse of privileges, theft of information)

ROMA MMXVI

APPSEC EUROPE

CISO Survey: Threats towards your organization

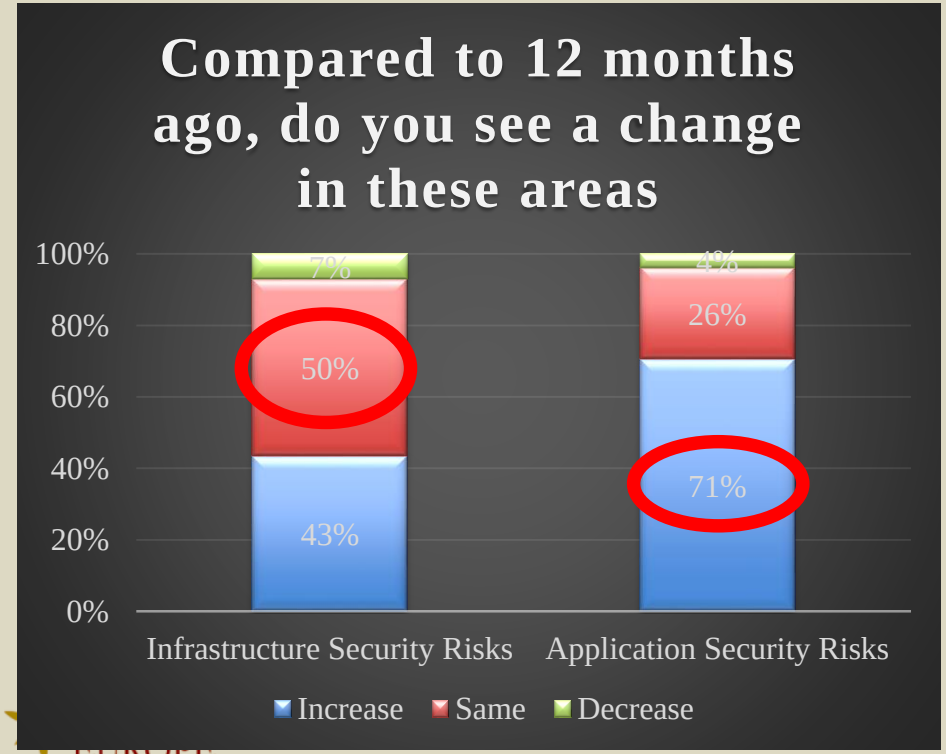




ROMA MMXVI

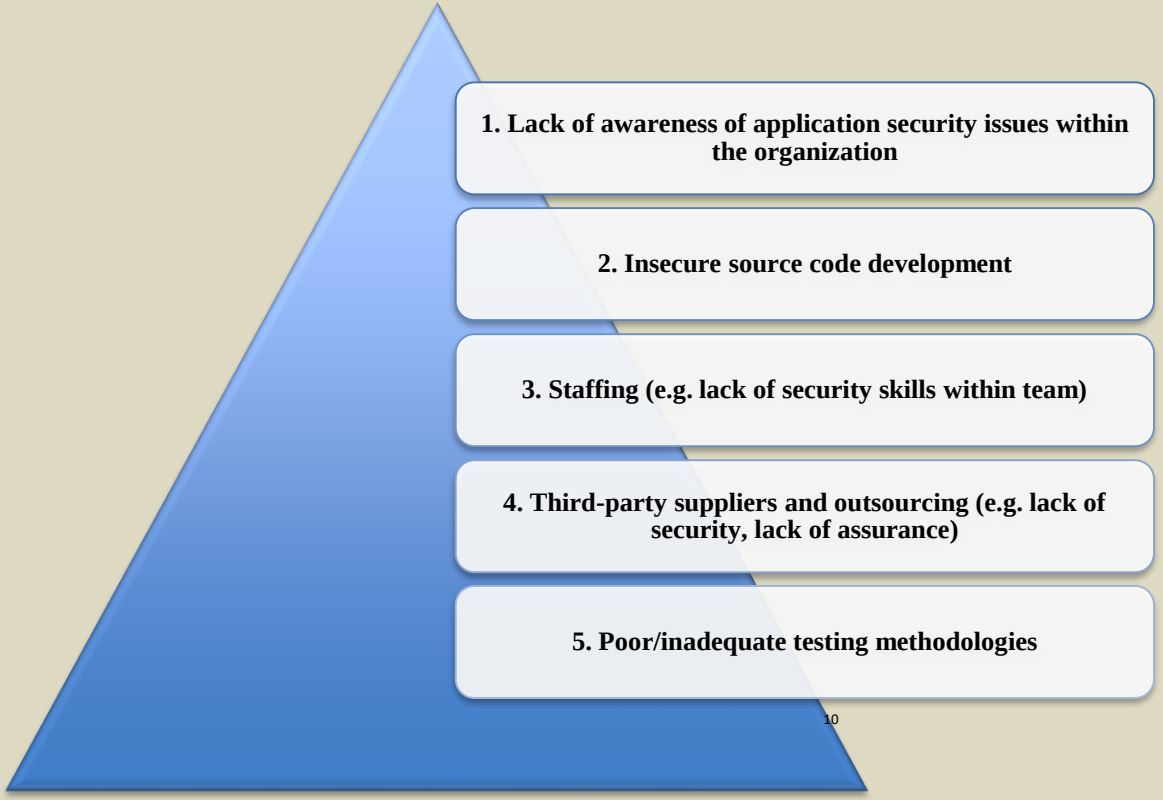
APPSEC EUROPE

CISO Survey : Threat Trends

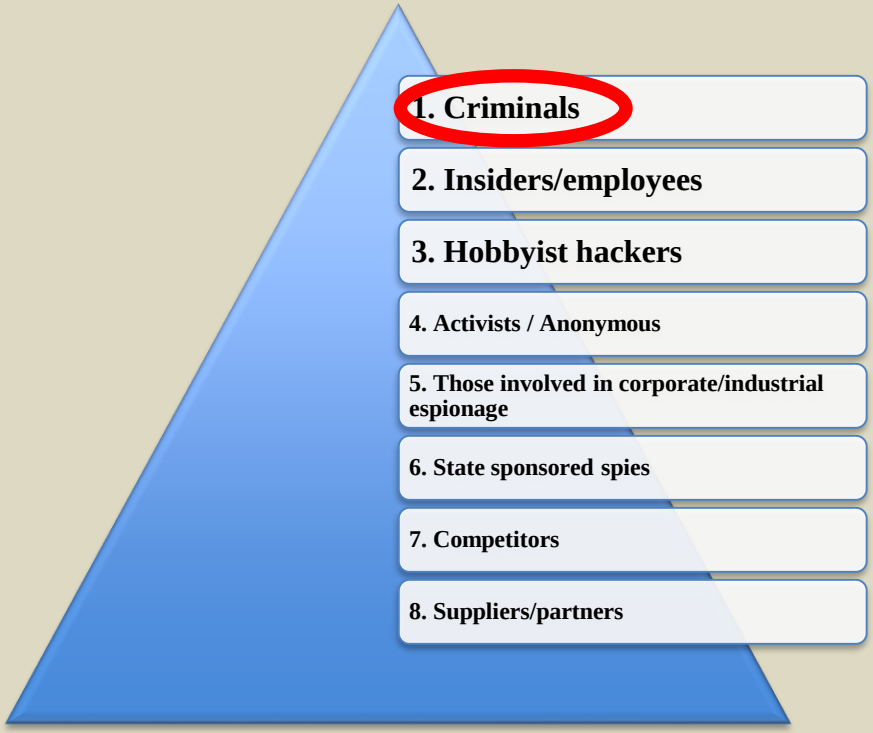


ROMA MMXVI

Top-5 Sources of application security risk

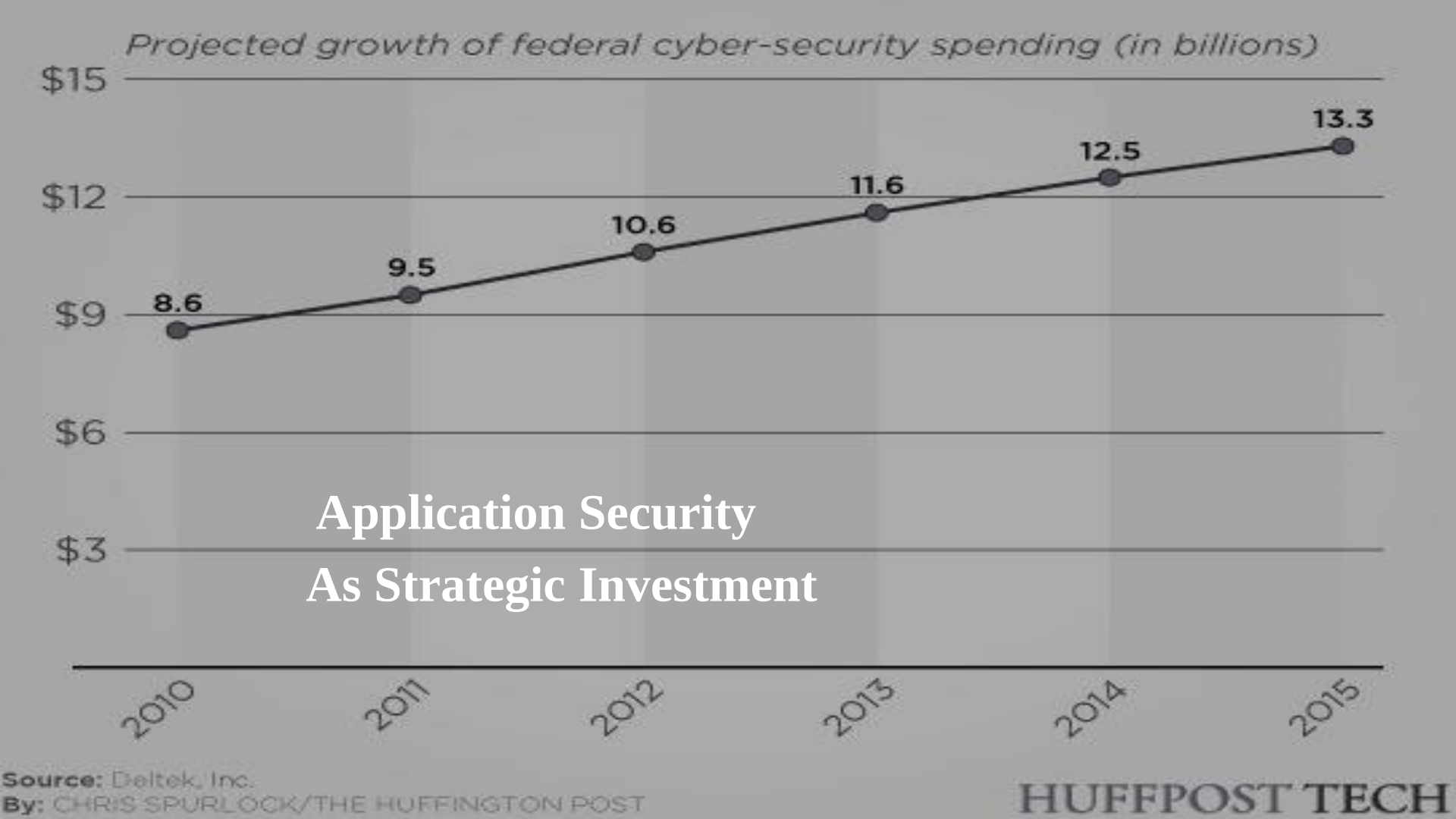


Which kind of attackers do you think are the most likely to target your company in the next 12 months



Learning from application security incidents…
…things are easier than you think

- Reviewing the incidents of the past year(s), many could be traced back to:
  1. Lack of proper basic application security controls during the development phase
  2. Lack of awareness
  3. Did not require a “very high” level of skill from the attacker to exploit (though they may require time and patience to find)


Projected growth of federal cyber-security spending (in billions)
$15
$12
$9
$6
$3
8.6
9.5
10.6
11.6
12.5
13.3
2010
2011
2012
2013
2014
2015
Application Security
As Strategic Investment
Source: Deltek, Inc.
By: CHRIS SPURLOCK/THE HUFFINGTON POST
HUFFPOST TECH

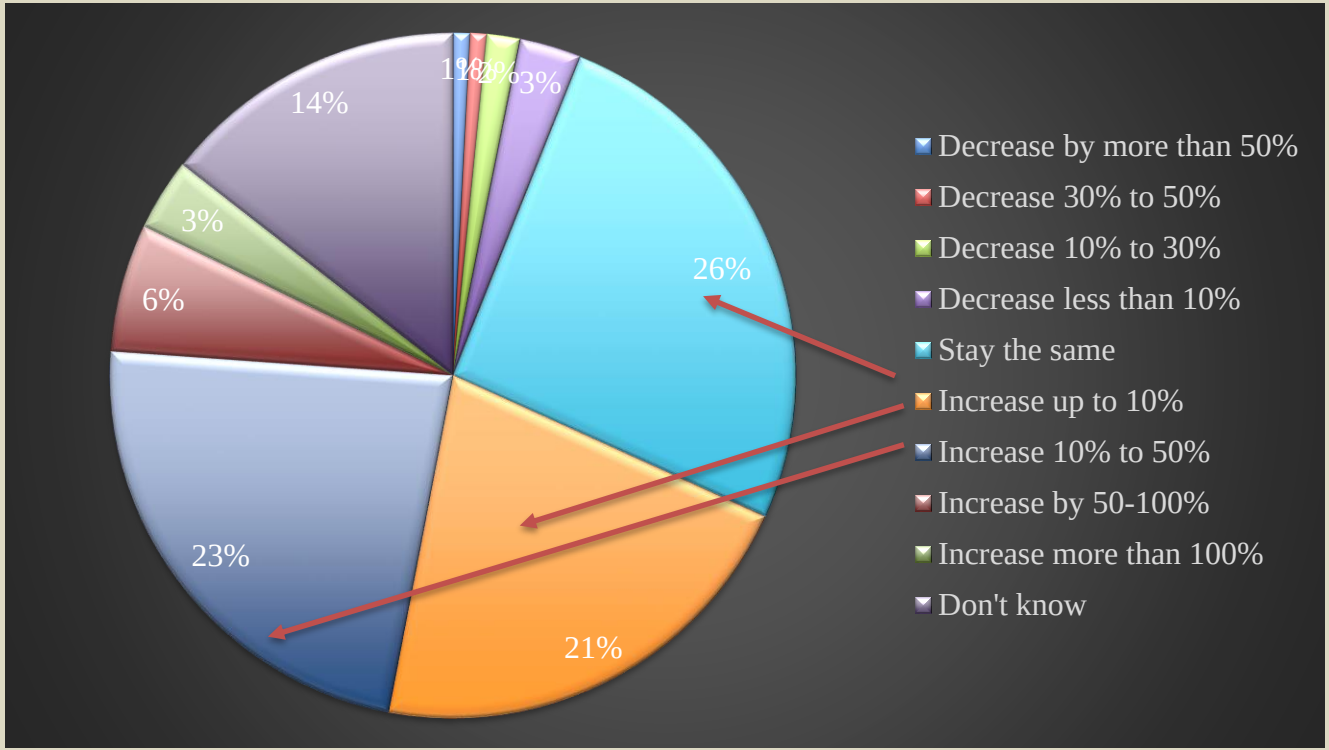
CISO Survey & Report: Investments in Security - % of IT budget for Security

ROMA MMXVI

APPSEC EUROPE

CISO Survey & Report: Investments in Security

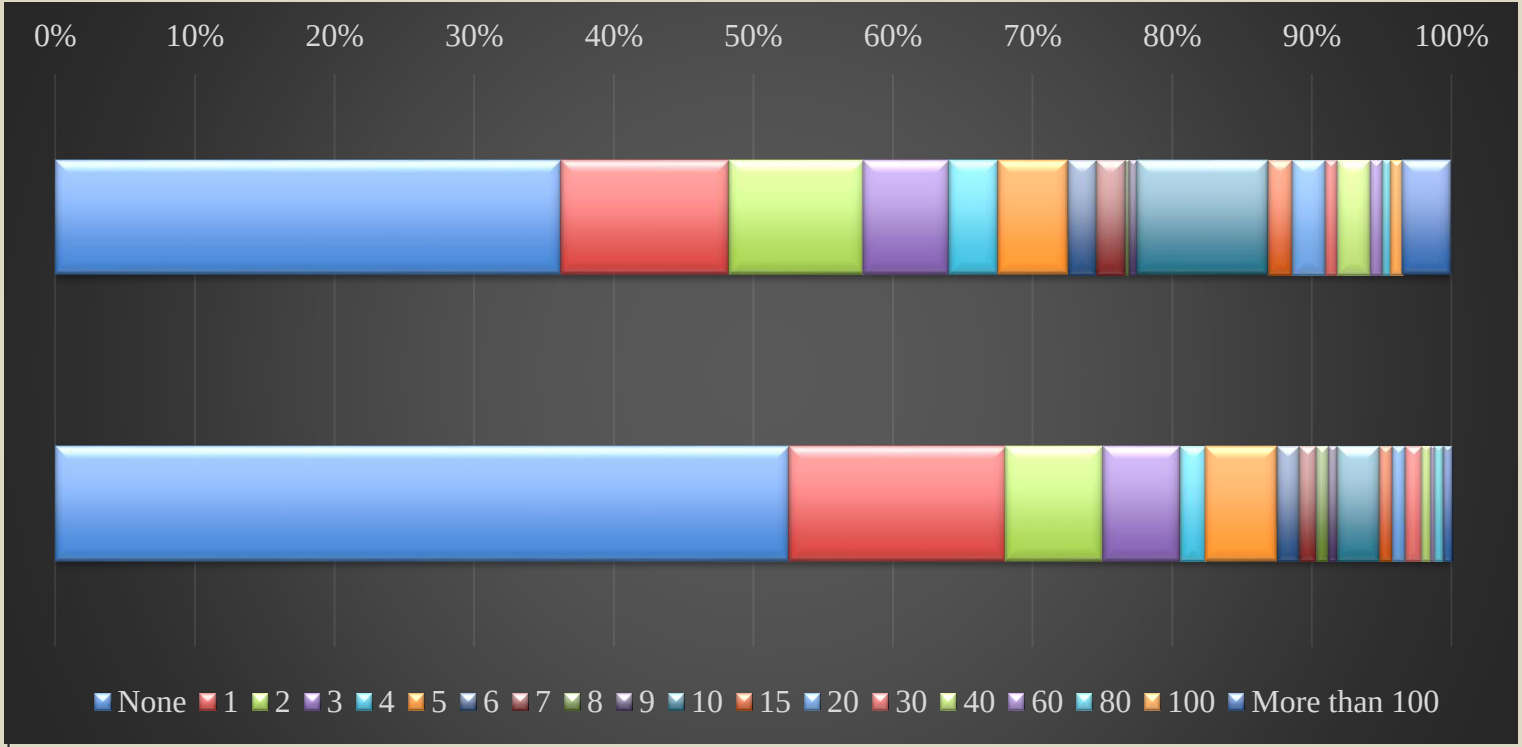
Your total cyber security spending over the next 12 months will…



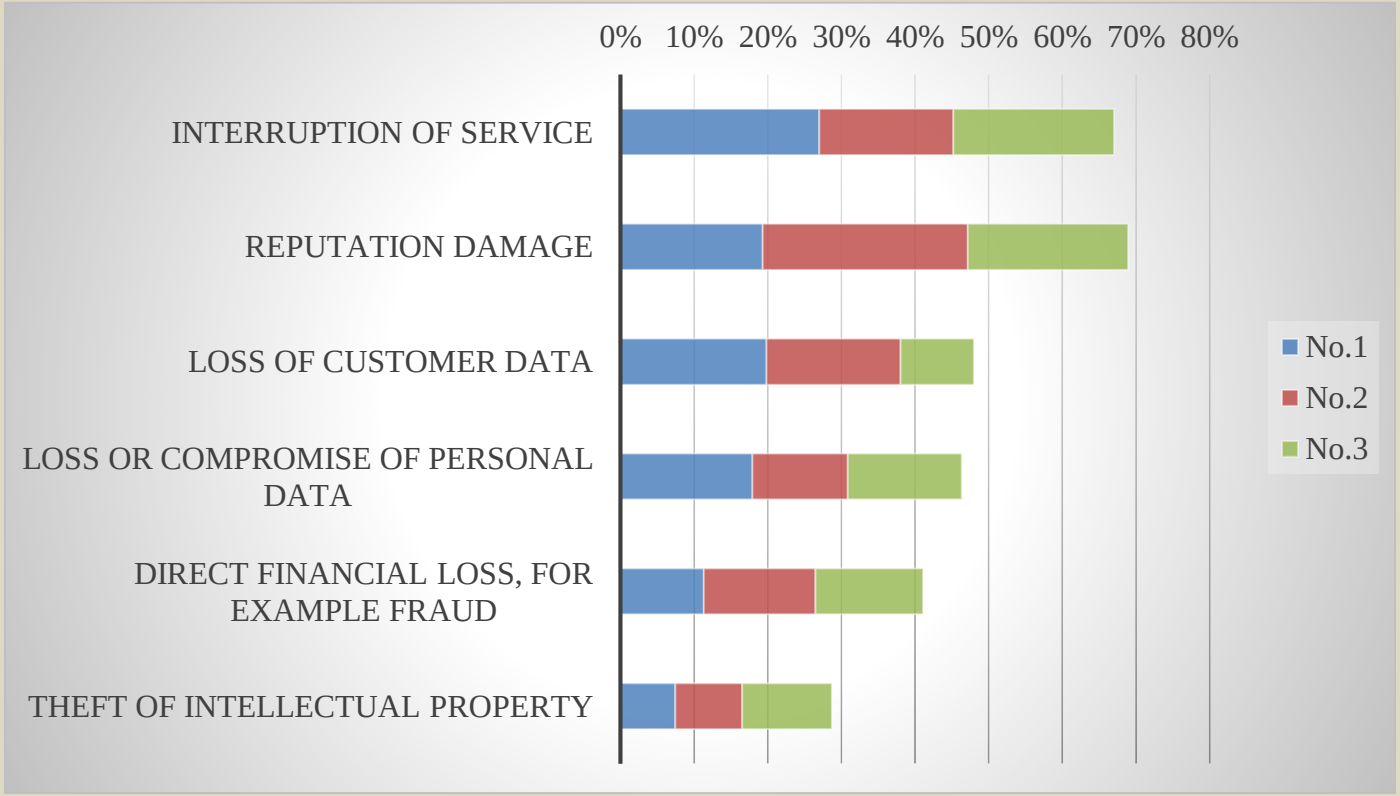
ROMA MMXVI

APPSEC EUROPE

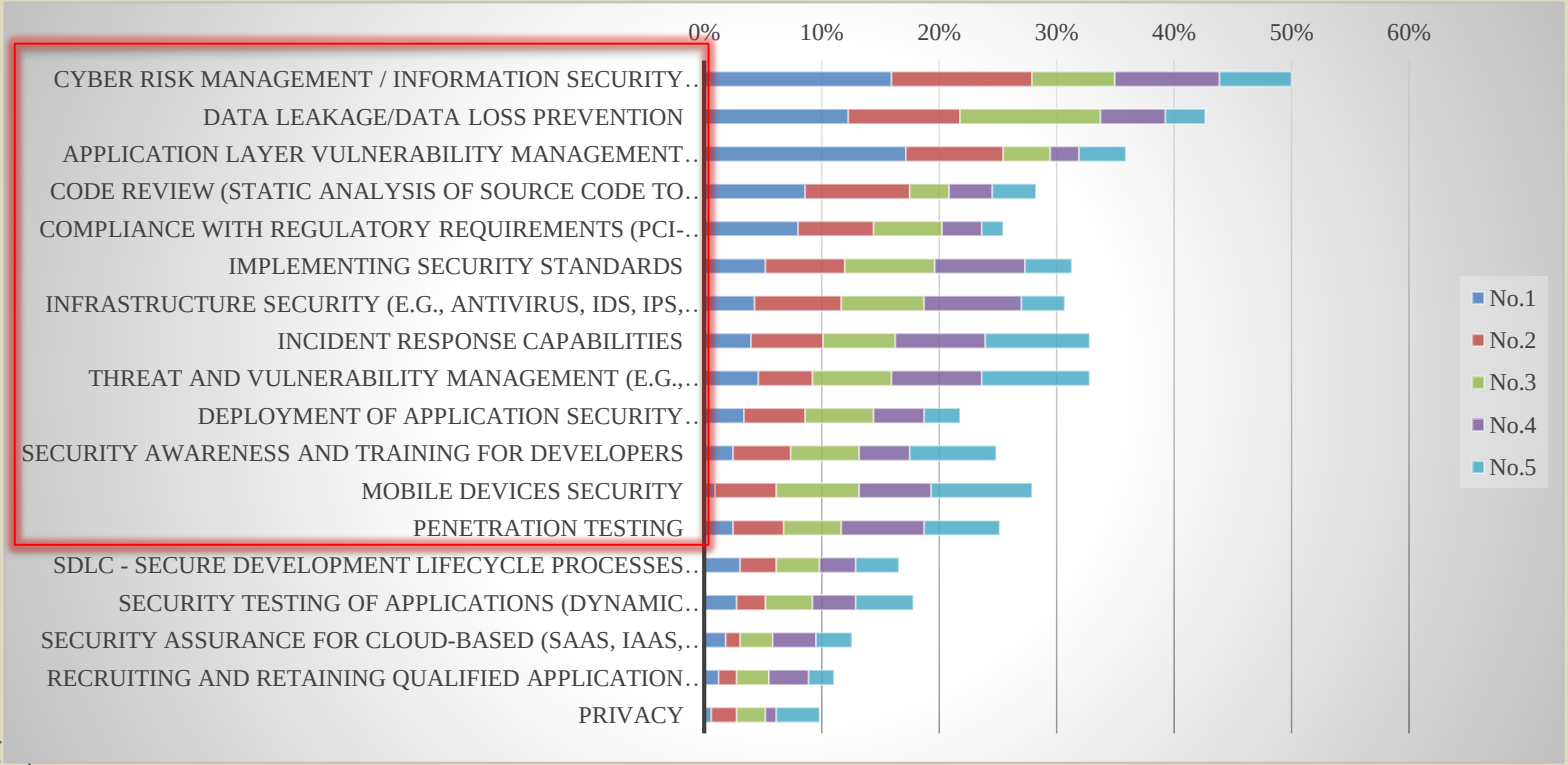
How many security breaches did your company experience in the last 12 months? (Cyber security and Application Security breaches)



Main damage types caused by cyber attacks



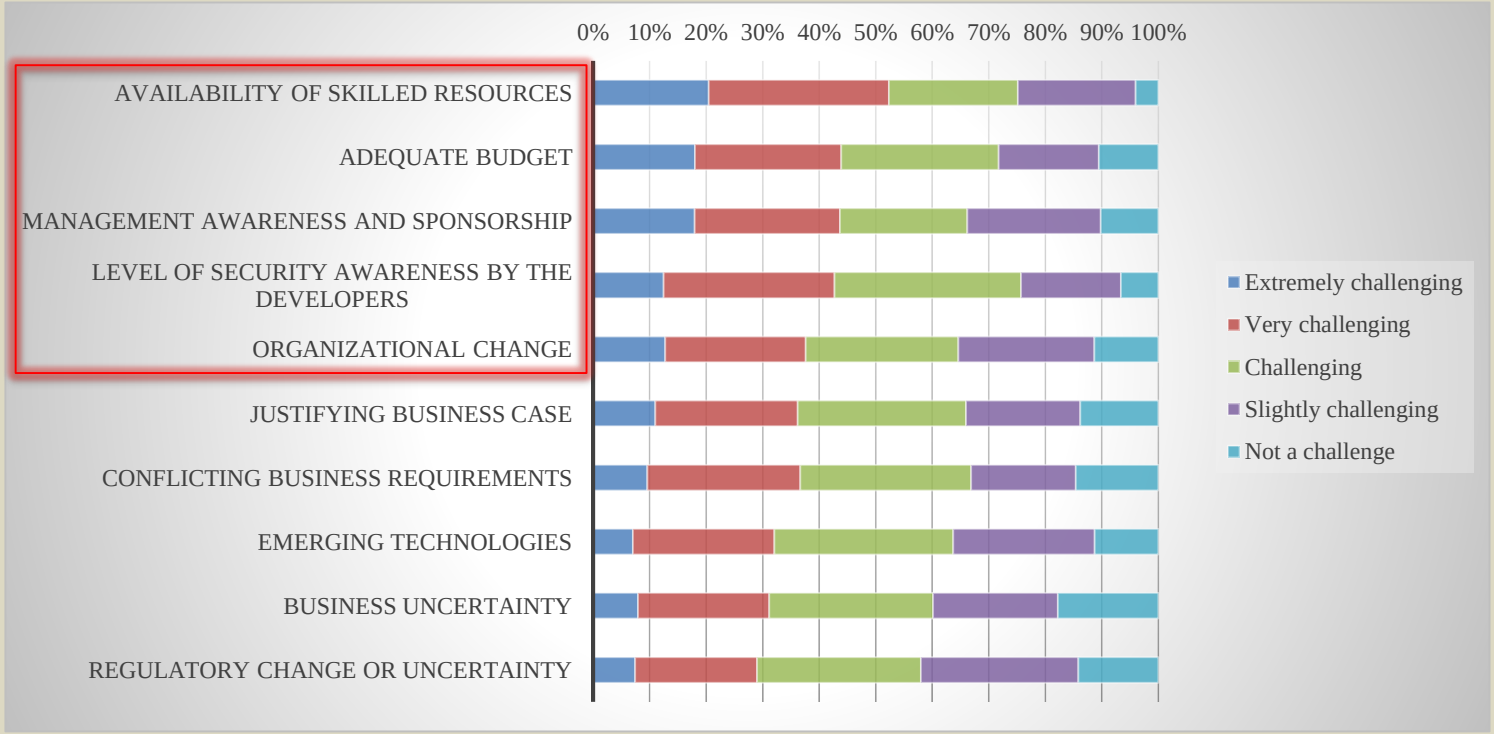
Investments in Security: Top security priorities for the coming 12 months



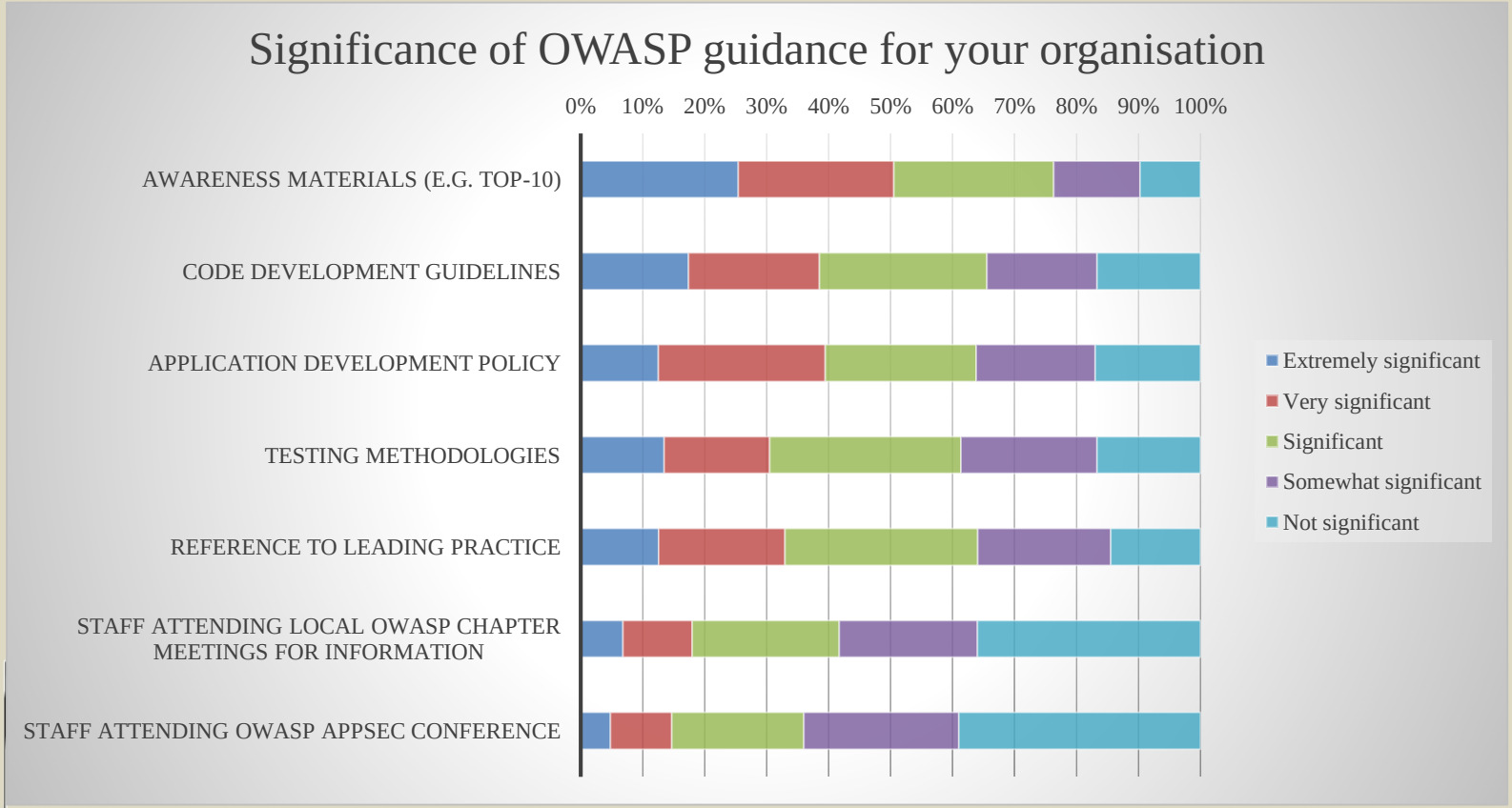
ROMA MMXVI

APPSEC EUROPE

Biggest challenges delivering your organization's application security initiatives

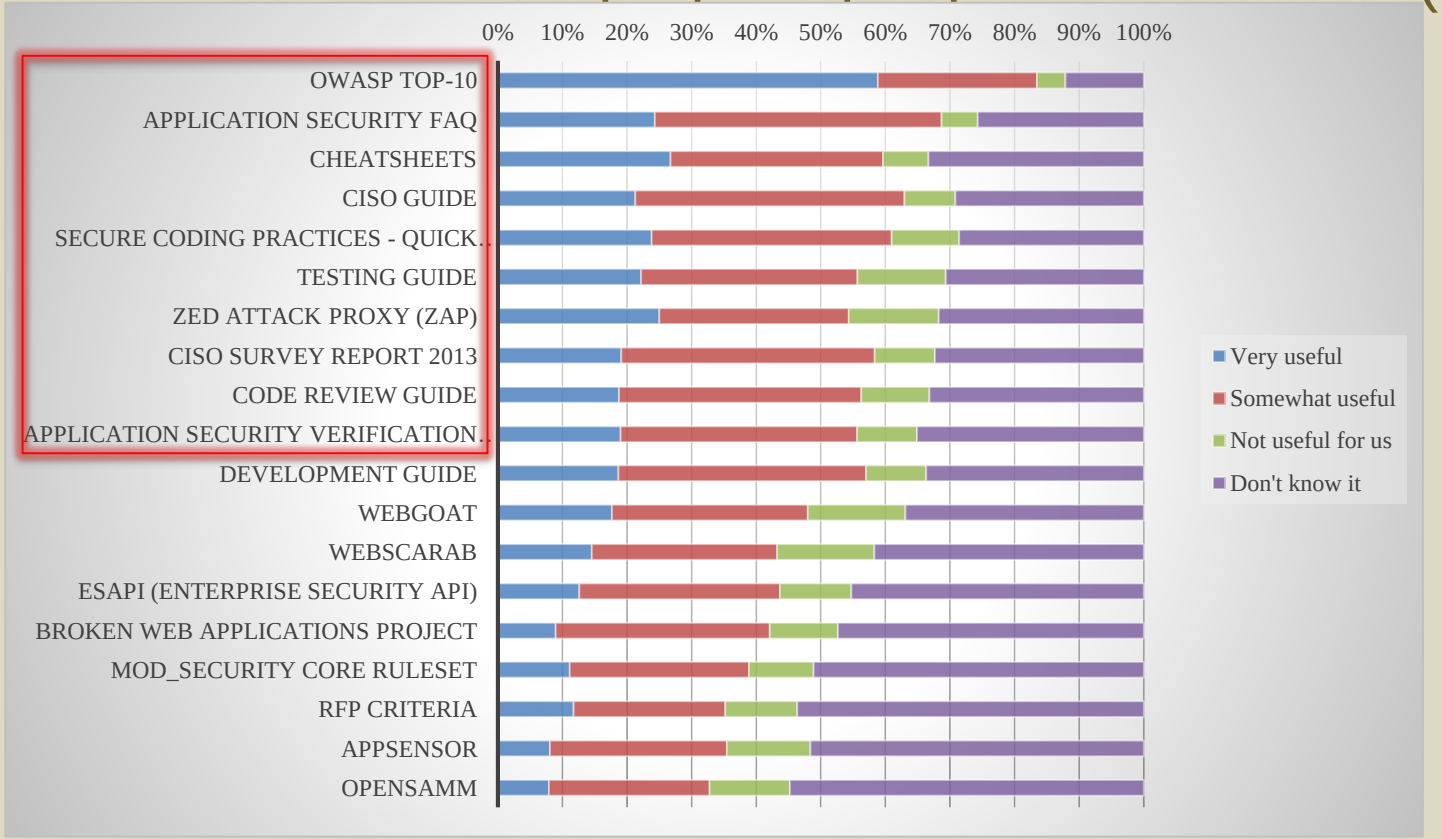


Where you see OWASP can help you…



ROMA
MMXVI

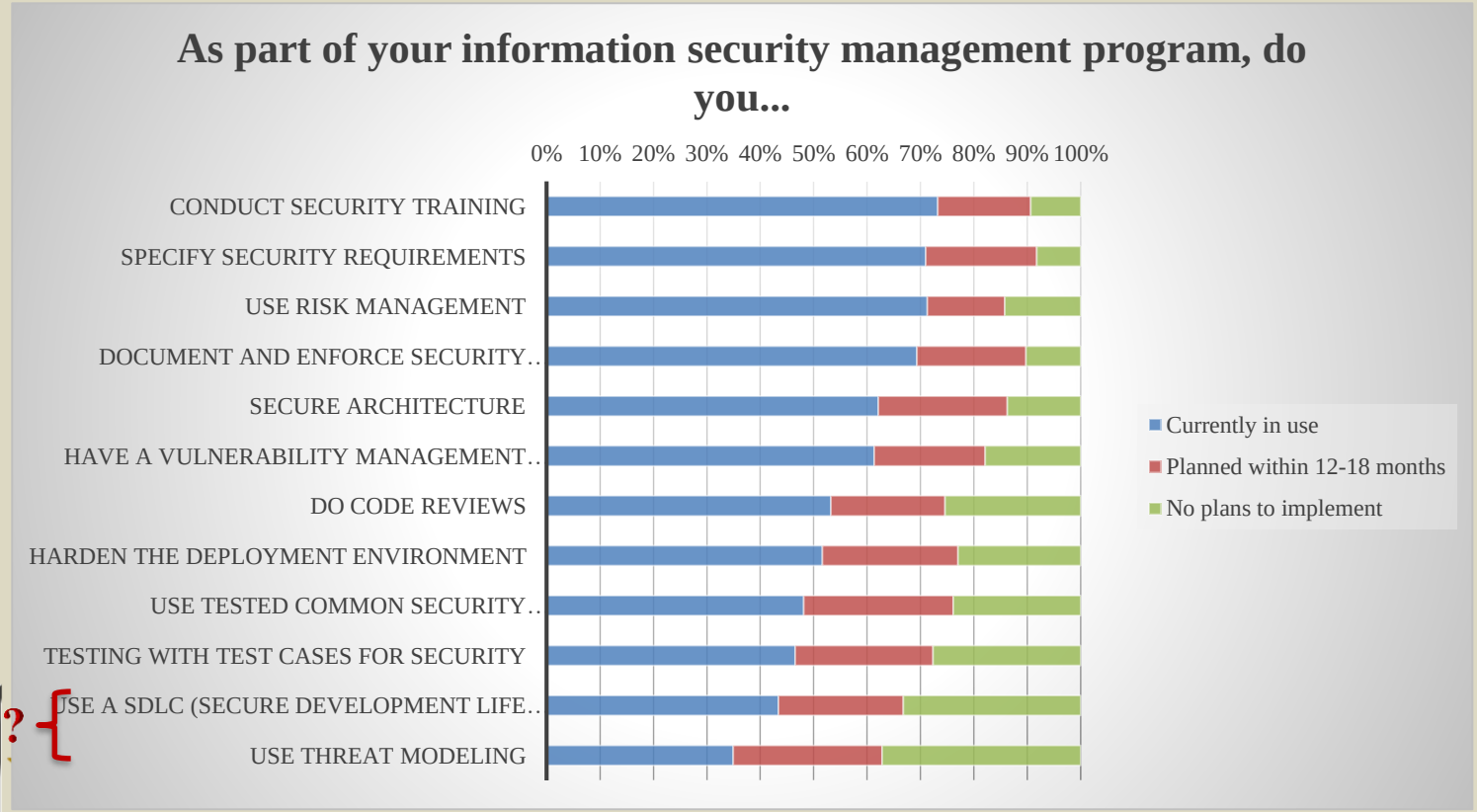
Which OWASP projects people found useful (Top-10)



ROMA MMXVI

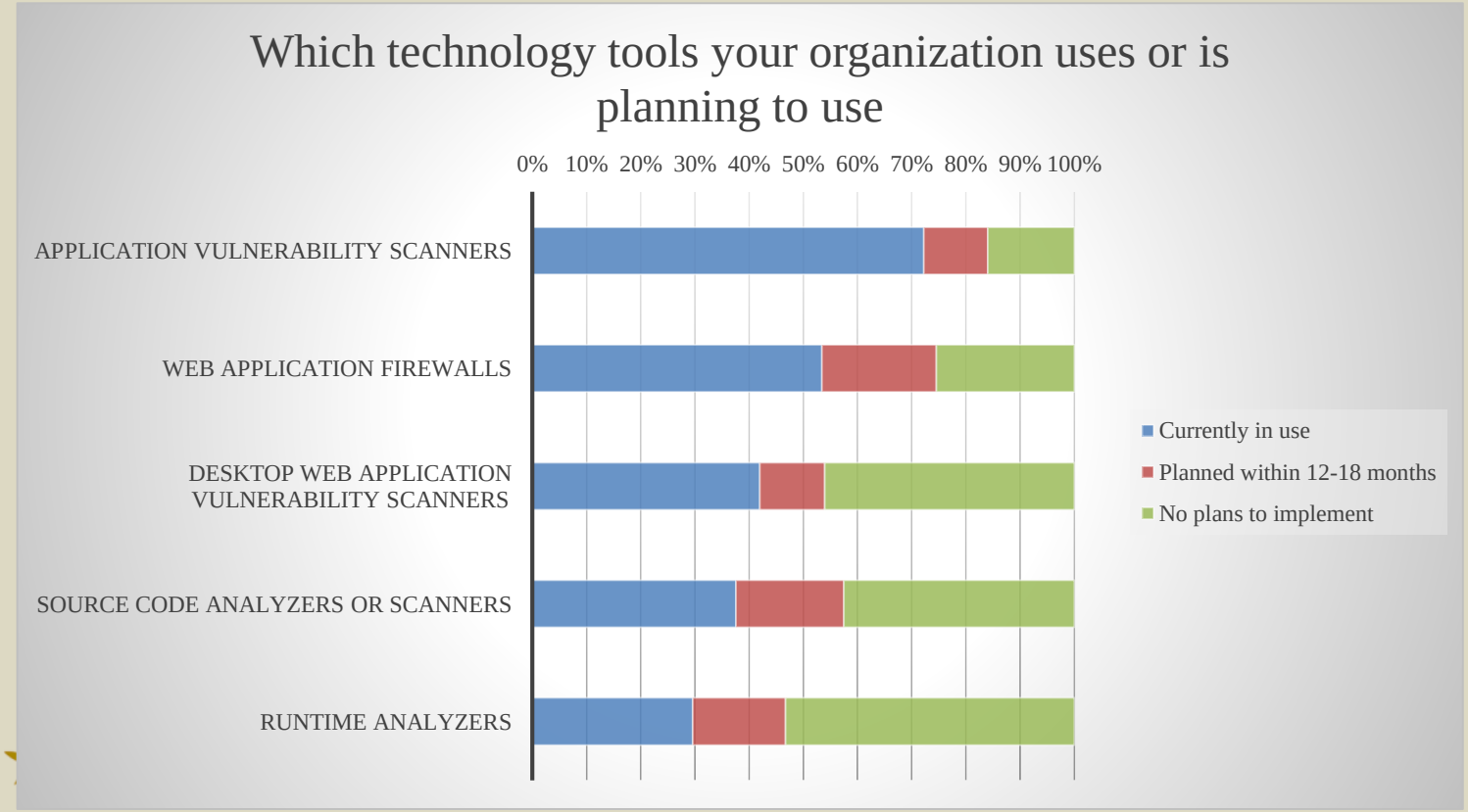
APPSEC EUROPE

As part of your information security management program, do you…



ROMA MMXVI

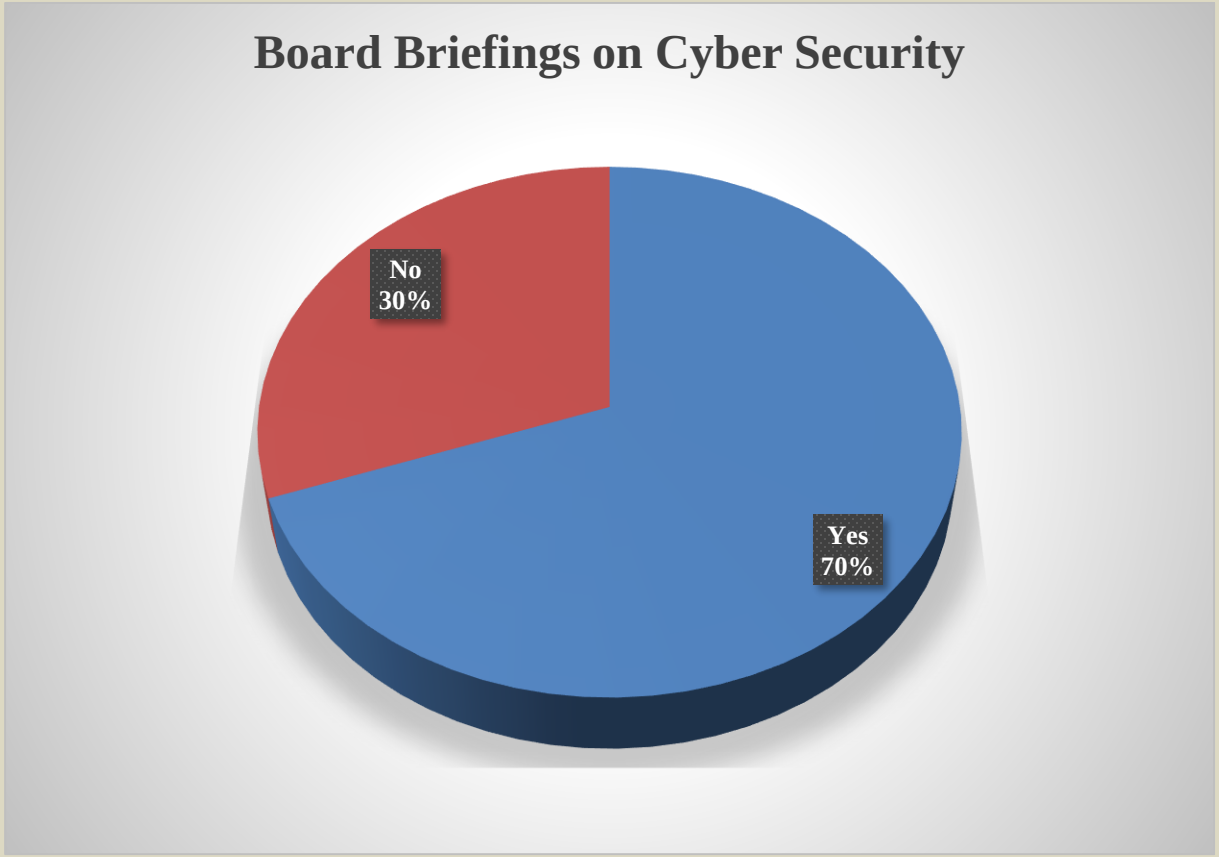
Which technology tools organizations use or are planning to use…



ROMA
MMXVI


Build Security In,
Security Strategy &
Maturity Models

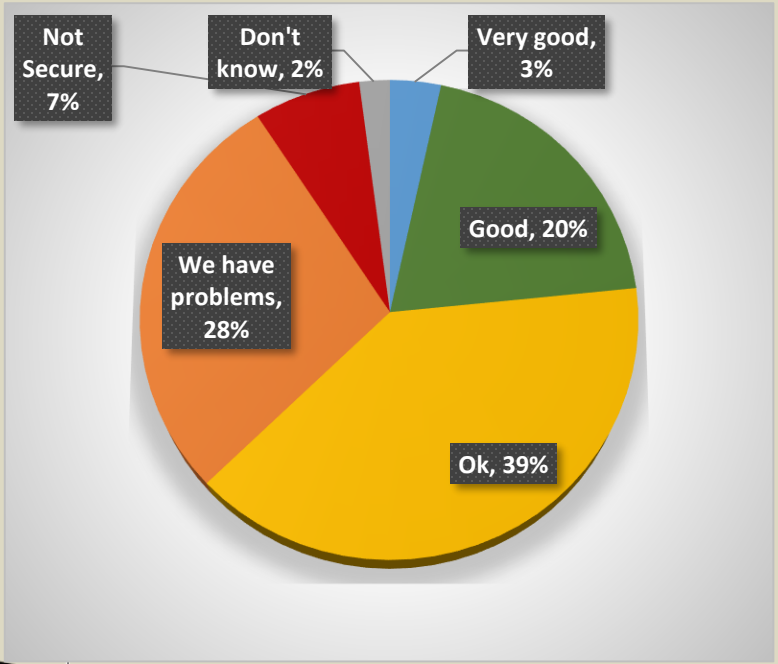
Strategy & Planning: board awareness…



ROMA MMXVI

APPSEC EUROPE

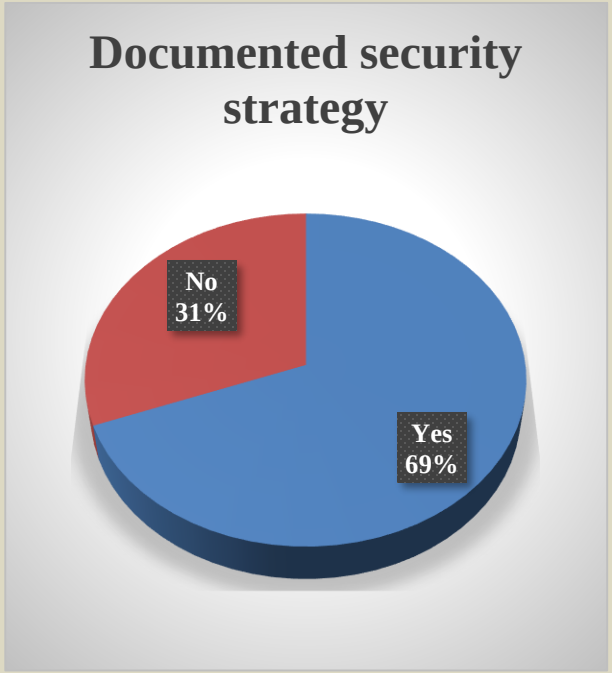
How confident are you that your organization is protected from cyber security risk?

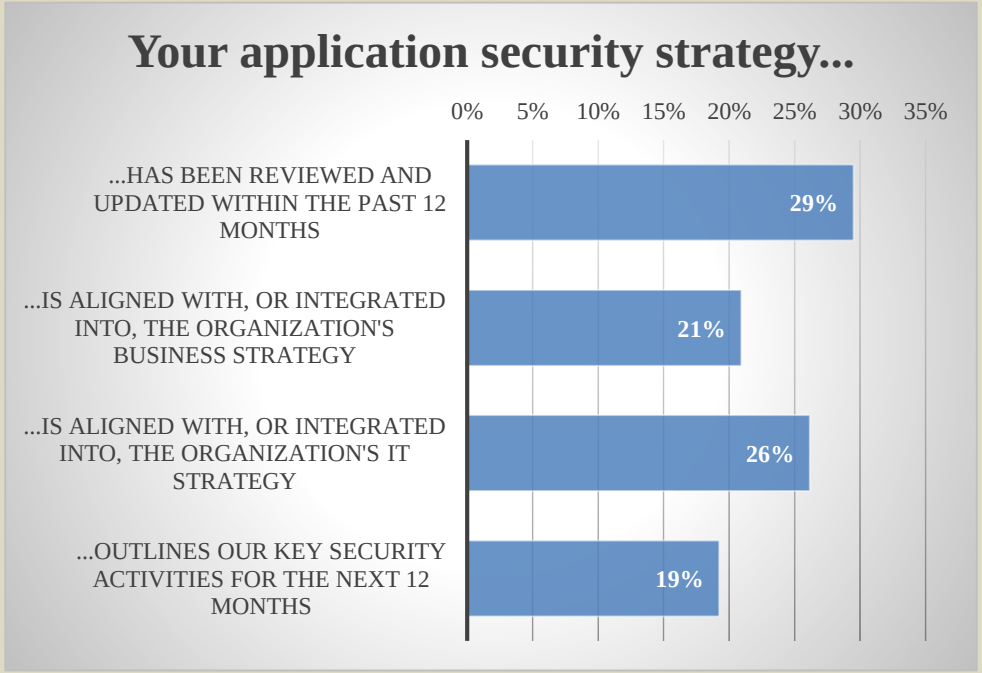


ROMA MMXVI

APPSEC EUROPE

Strategy & Planning



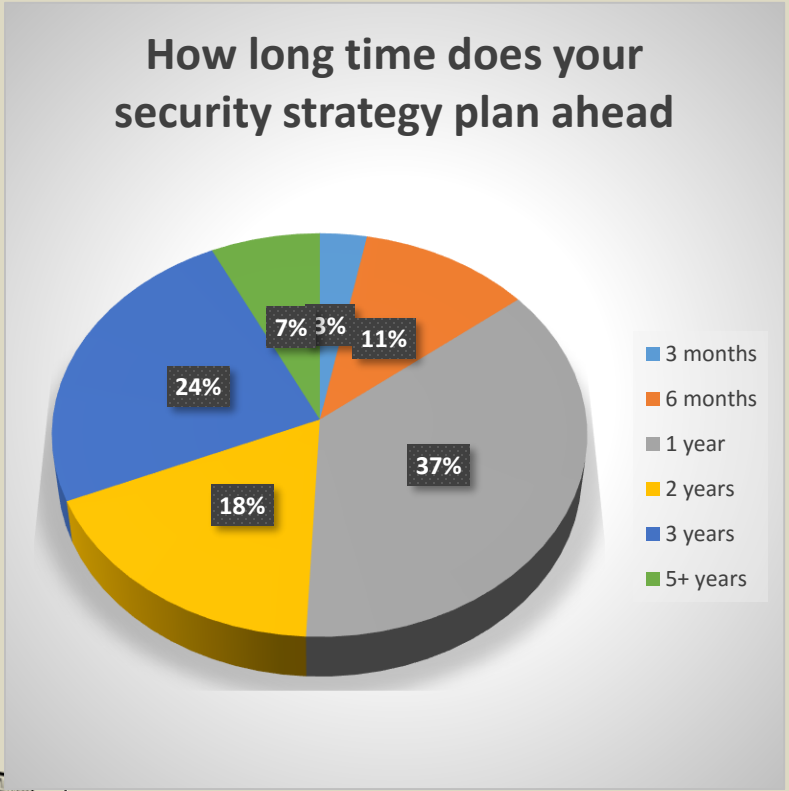


ROMA MMXVI

APPSEC EUROPE

In case you wonder:
We found a medium positive correlation between board briefings and whether you have a security strategy: 0.43

Strategy & Planning

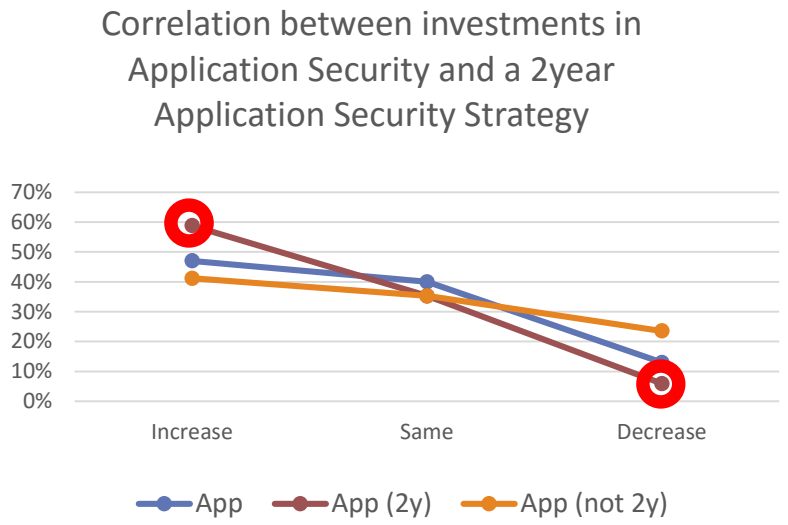


Trends of security strategy planning 2013 -> 2015: longer time horizons

Time Horizon	2013	2015
3 months	9.3%	3%
6 months	9.3%	11%
1 year	**37.0%**	**37%**
2 years	**27.8%**	18%
3 years	11.1%	**24%**
5 years+	5.6%	7%

Security Strategy (findings from 2013): advantages of a 2-year security strategy

»Benefits of a security strategy for application security investments:



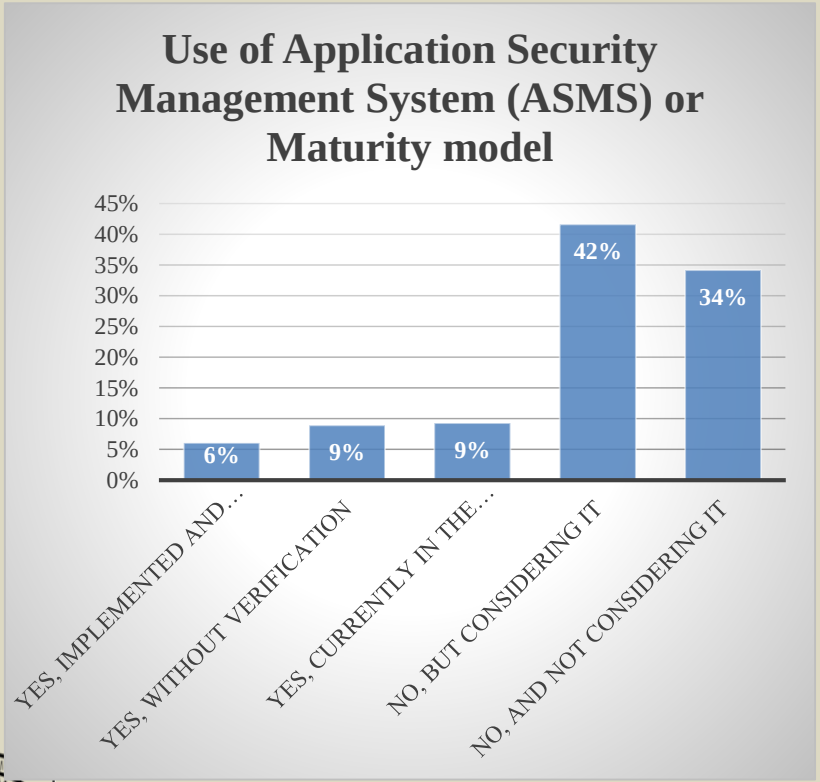
Analysis for correlations with:

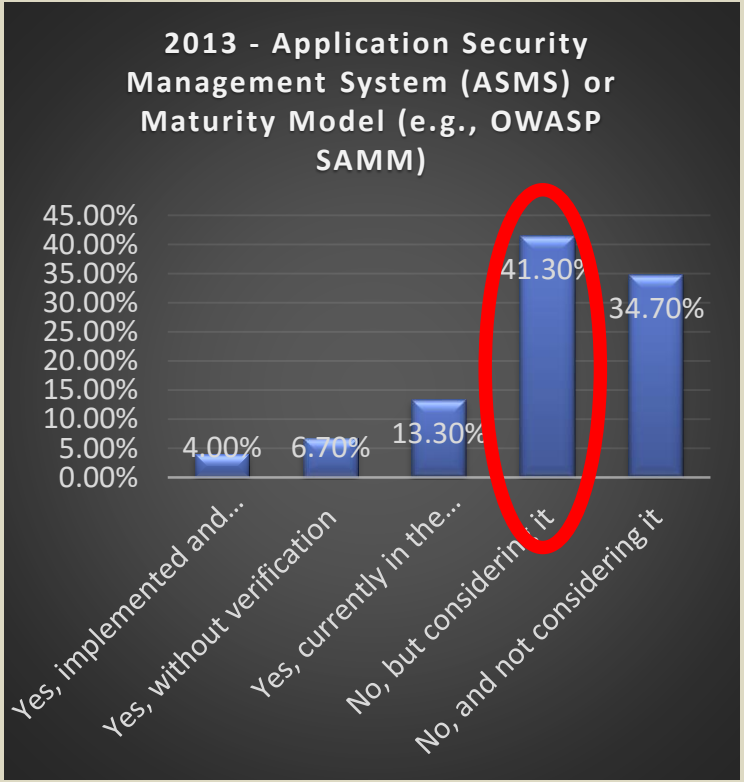
- Recent security breach
- Has a ASMS
- Company size
- Role (i.e. CISO)
- Has a Security Strategy
- **Time horizon of security strategy (2 years)**

ROMA MMXVI

APPSEC EUROPE

Strategy & Planning: Usage trends for ASMS and Maturity Models (2015 vs. 2013)

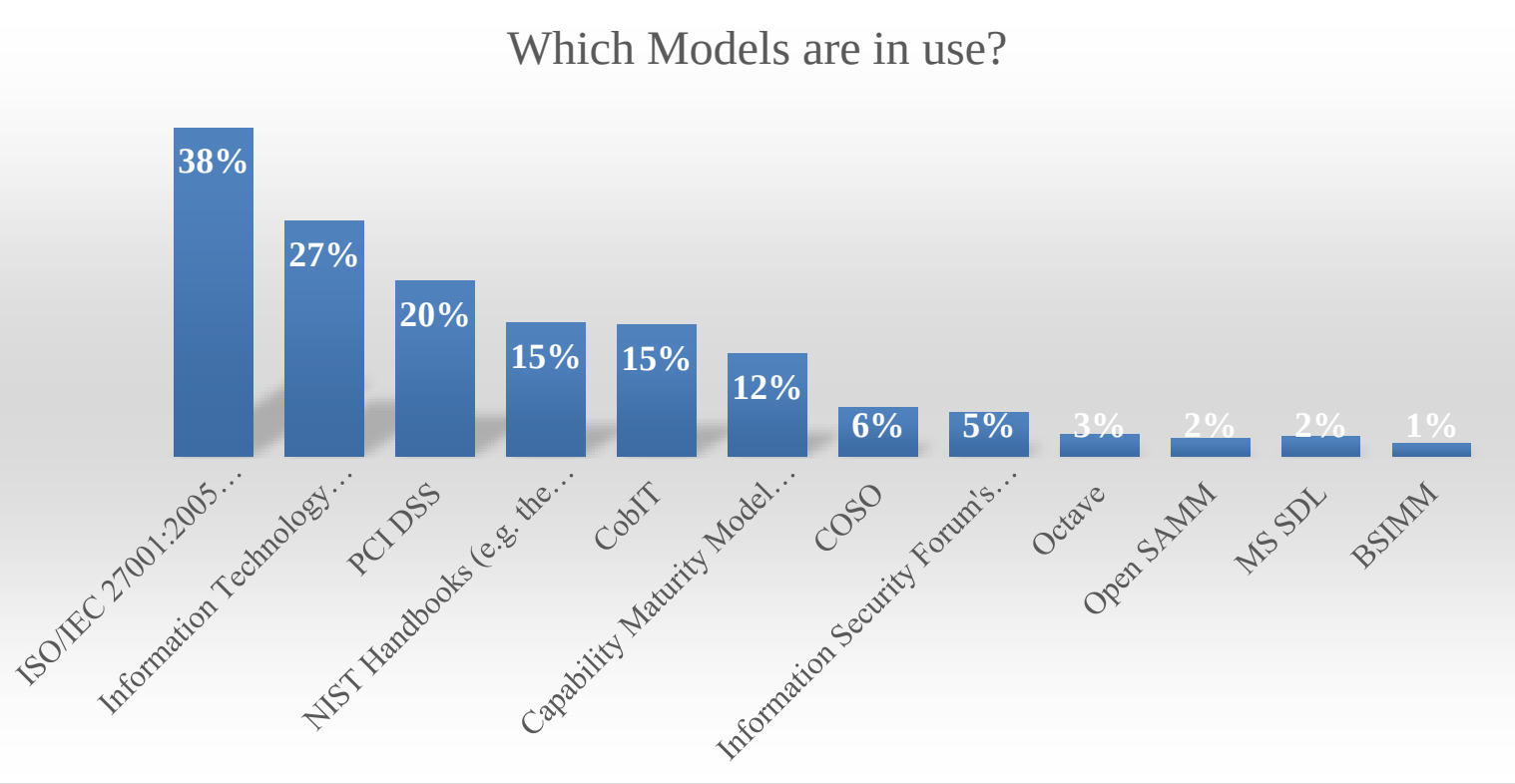




ROMA MMXVI

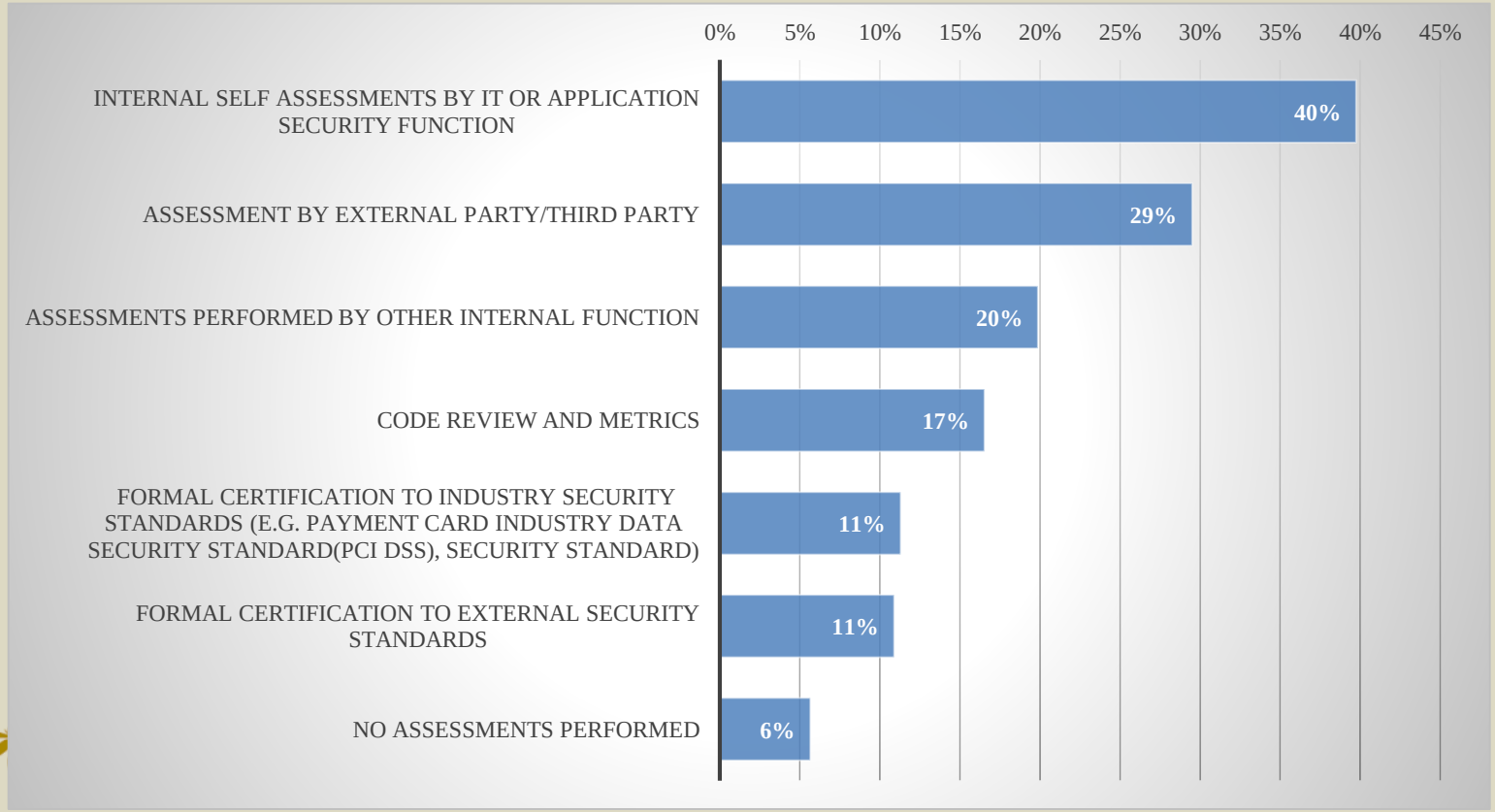
APPSEC EUROPE

Strategy & Planning: Maturity Models



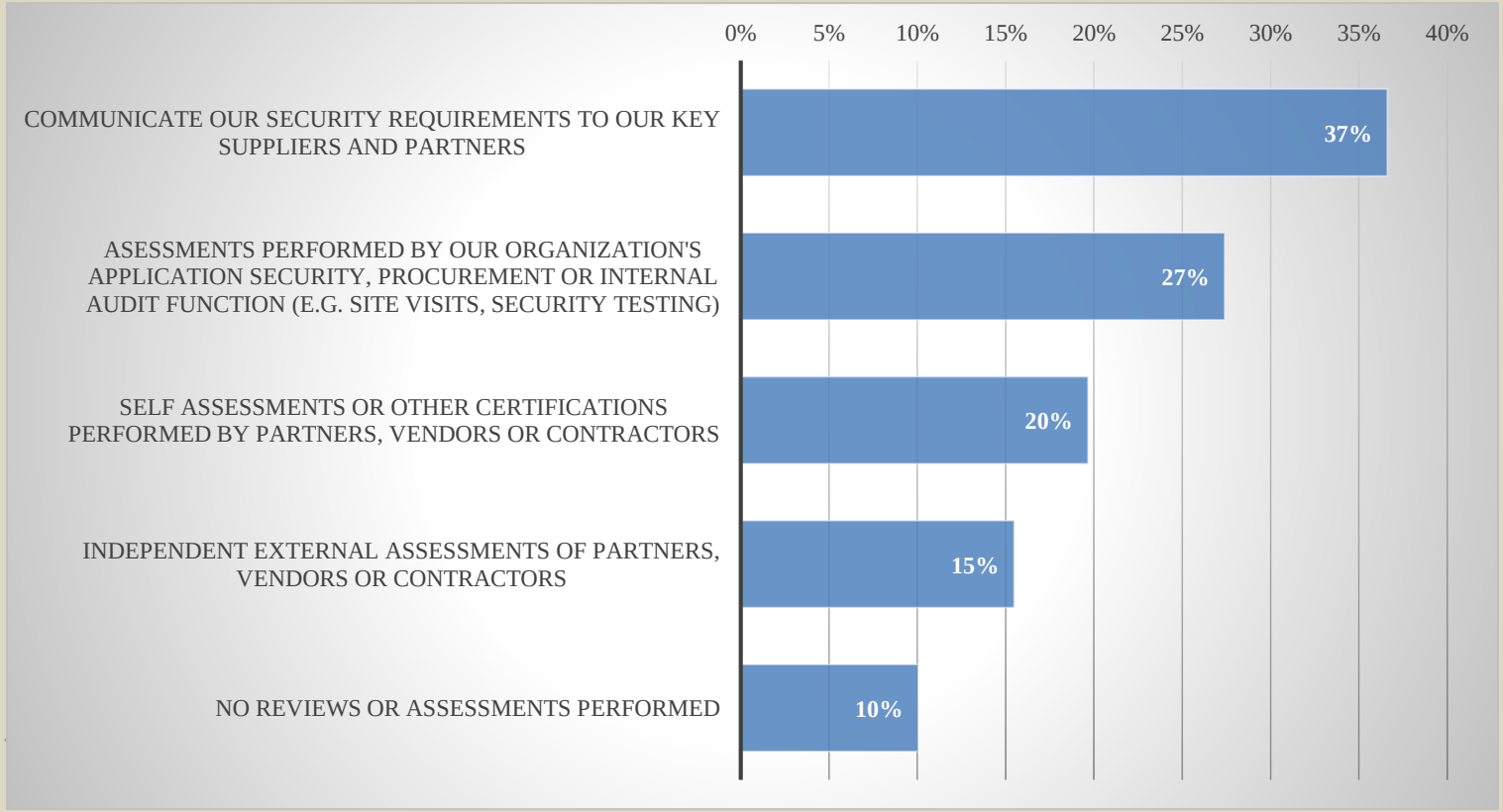
ROMA
MMXVI

How does your organization assess the quality and effectiveness of application security?



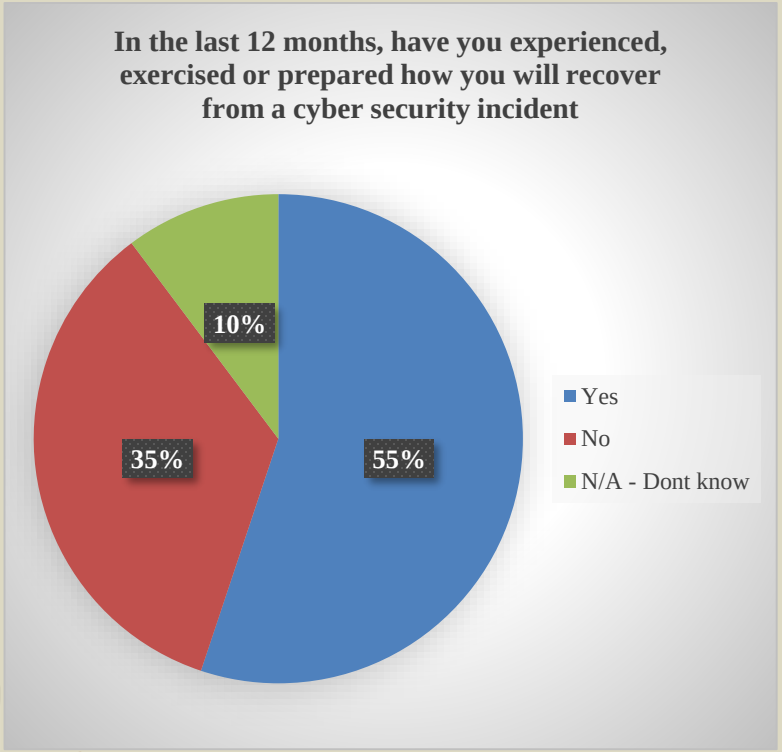
ROMA
MMXVI

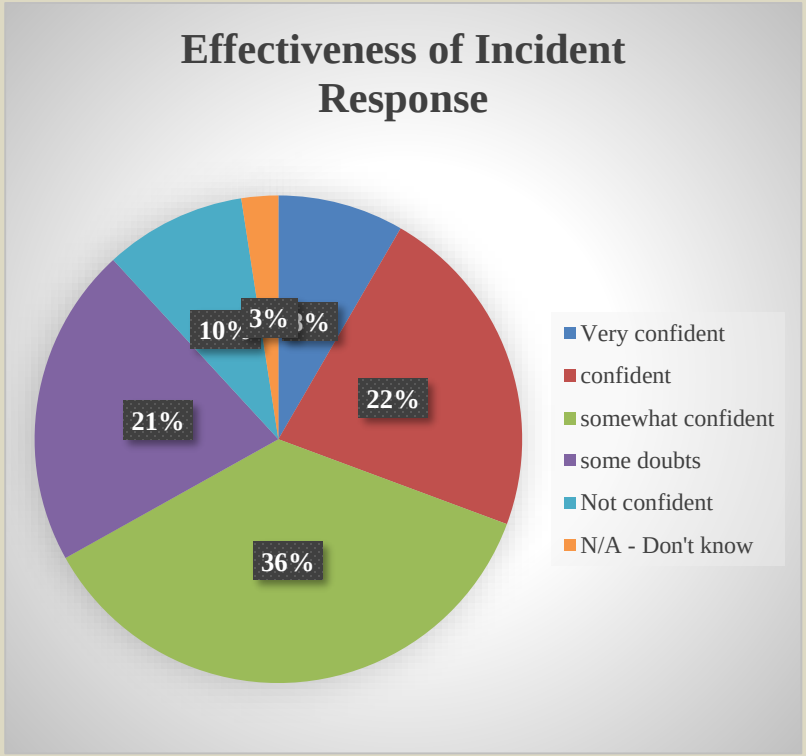
Suppliers & External Partners: How do you verify your external partners…



ROMA
MMXVI

Incident Response

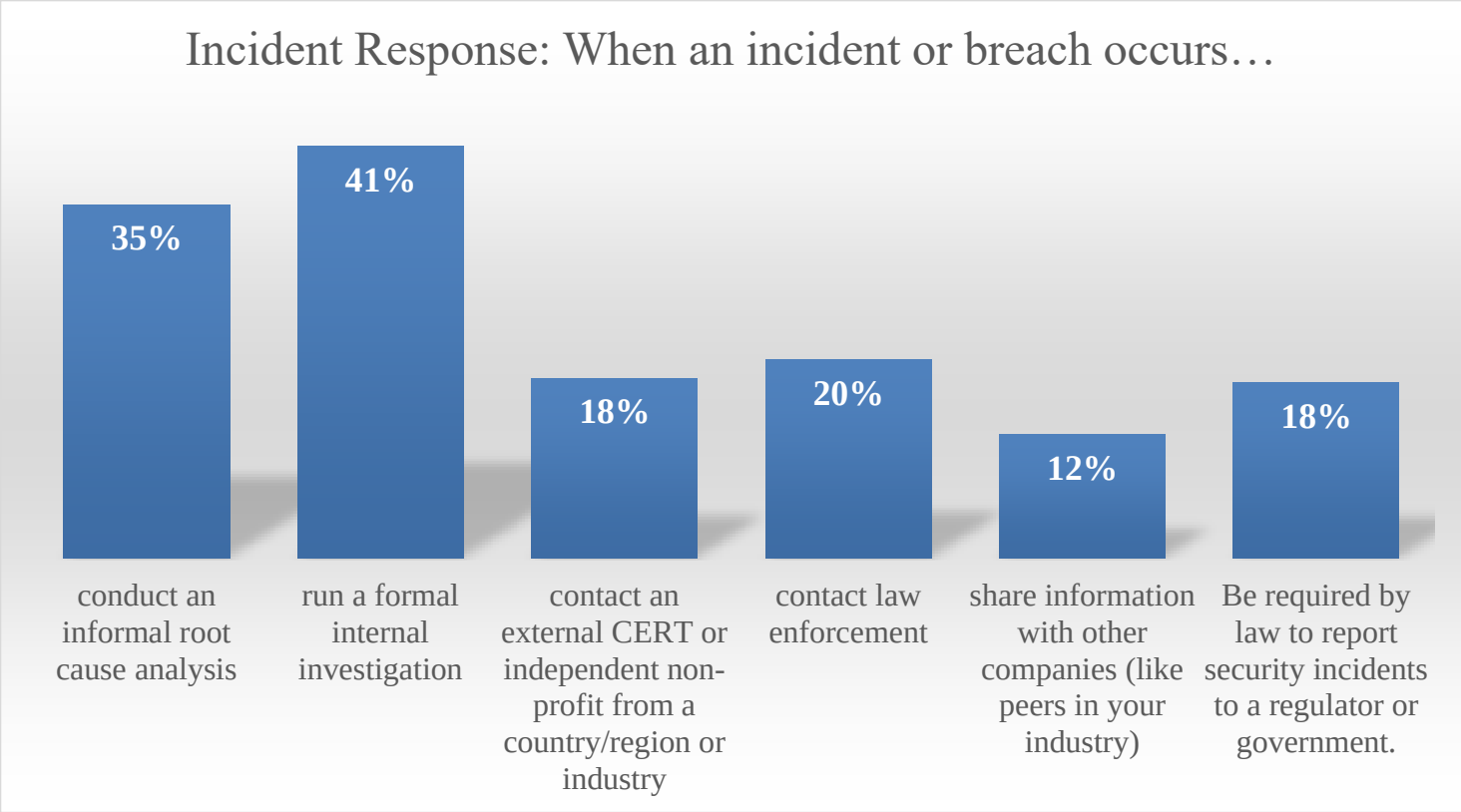




ROMA MMXVI

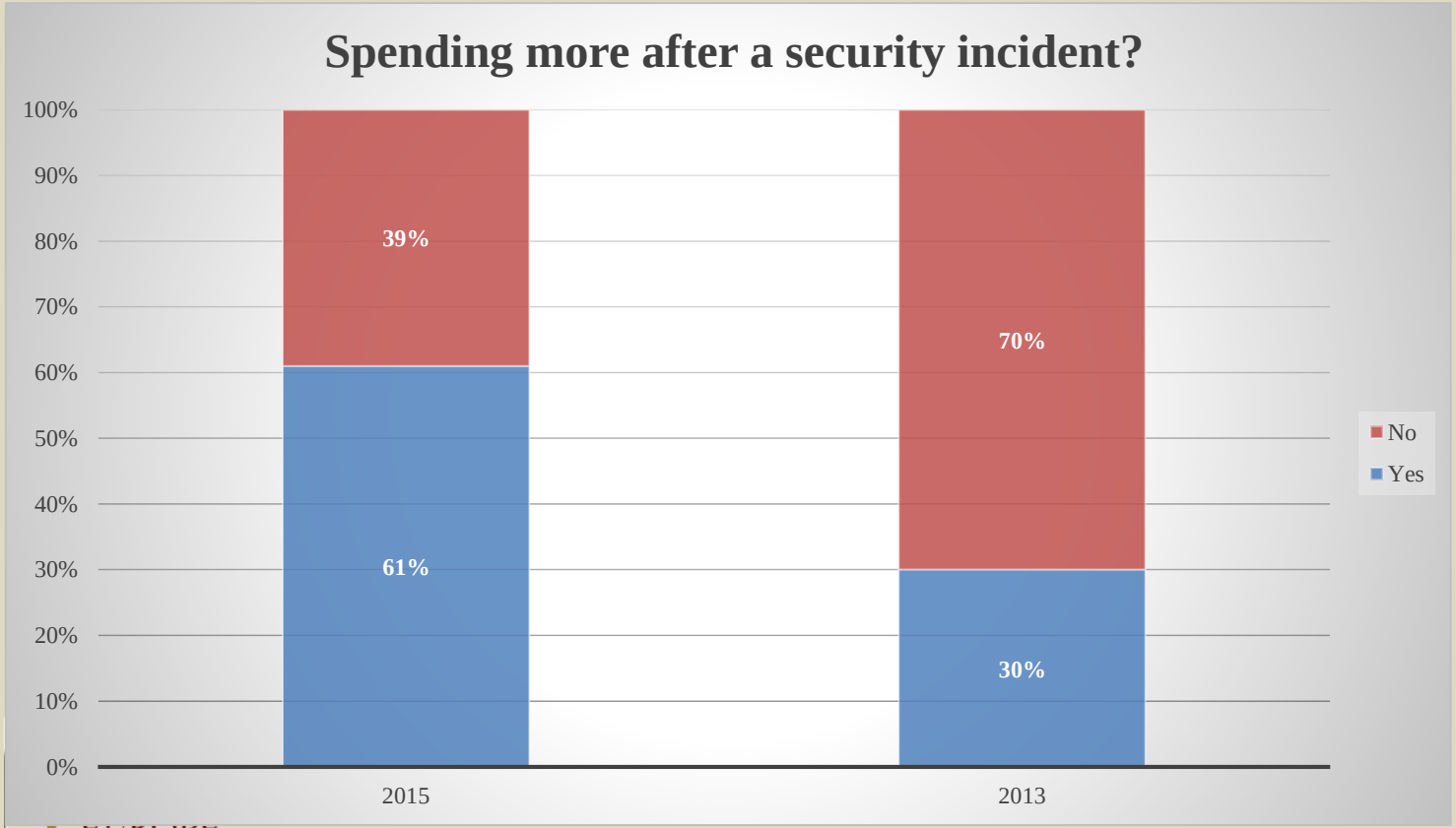
APPSEC EUROPE

Incident Response (2)



ROMA
MMXVI

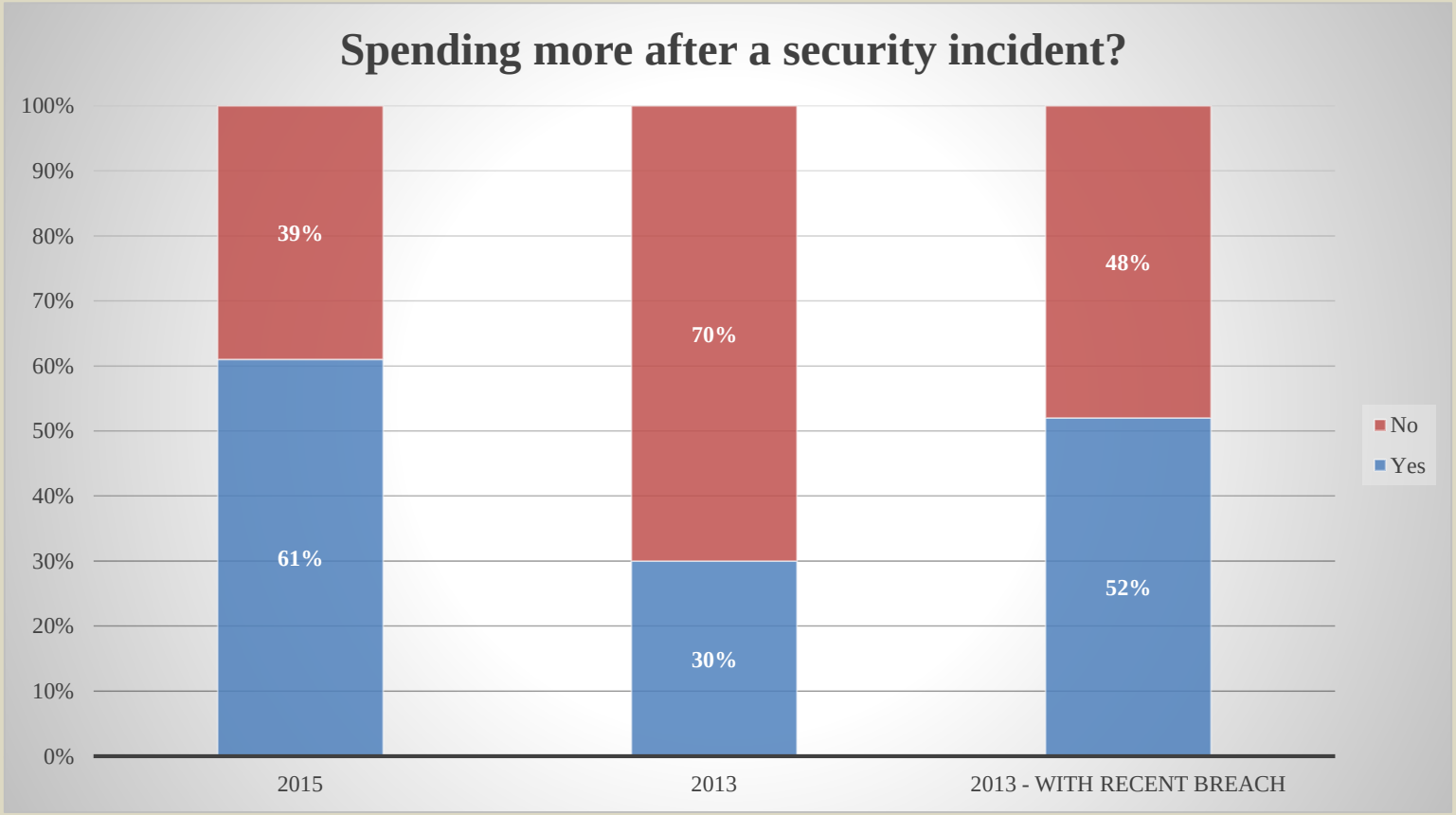
Incident Response: Increase spending after incident?



EUROPE

ROMA
MMXVI

Incident Response: Increase spending after incident?



ROMA
MMXVI

Thank you - Q&A

» *If you like to be notified when the new OWASP CISO Survey Report will be released, leave your card or send an email.*

ROMA MMXVI

APPSEC EUROPE

Thank you

If you like to be notified when the OWASP CISO Survey Report will be released, leave your card or send an email.

Email: tobias.gondrom@owasp.org

Twitter: @tgondrom