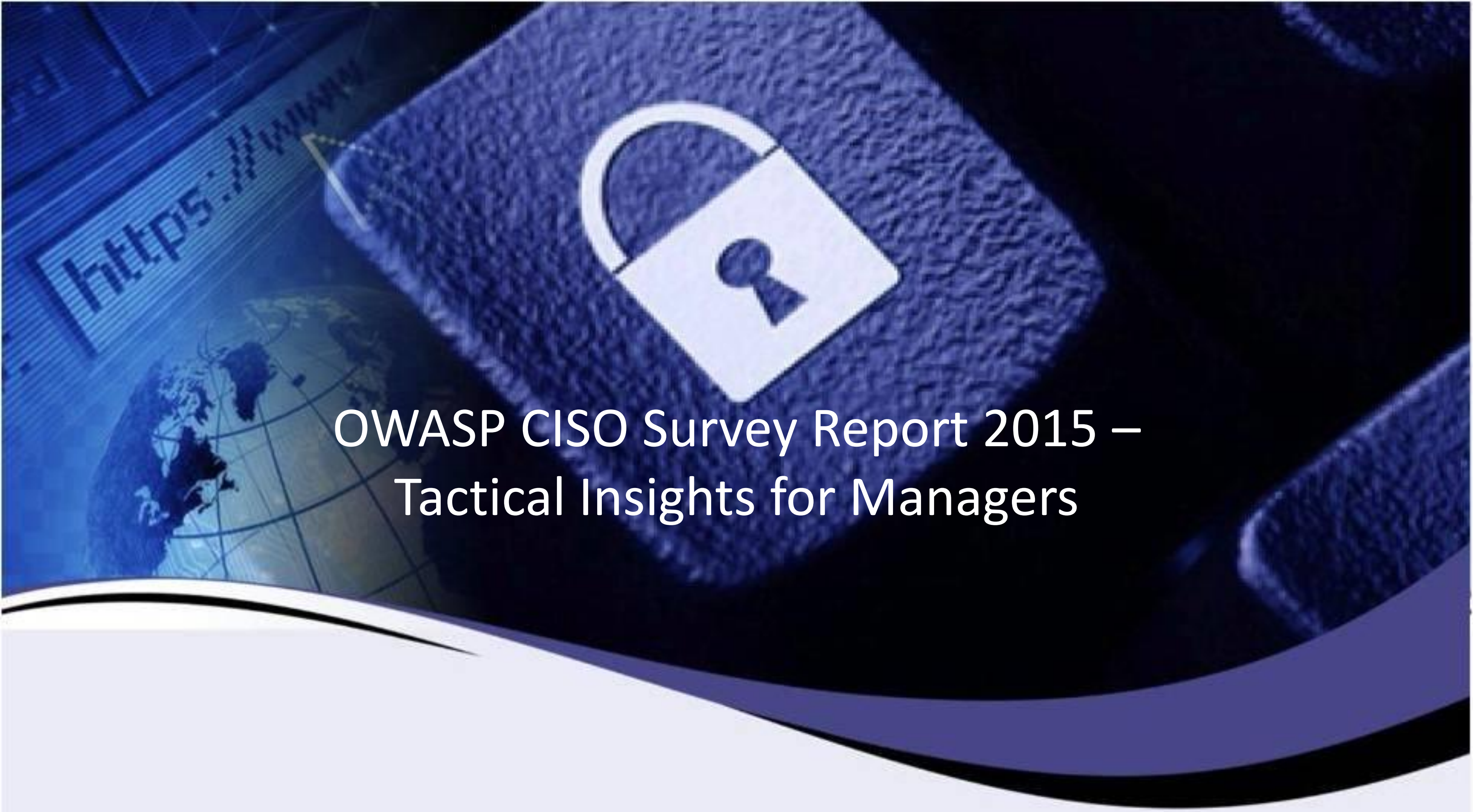


OWASP CISO Survey Report 2015 – Tactical Insights for Managers

OWASP 中国

The Open Web Application Security Project

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

OWASP 中国
The Open Web Application Security Project

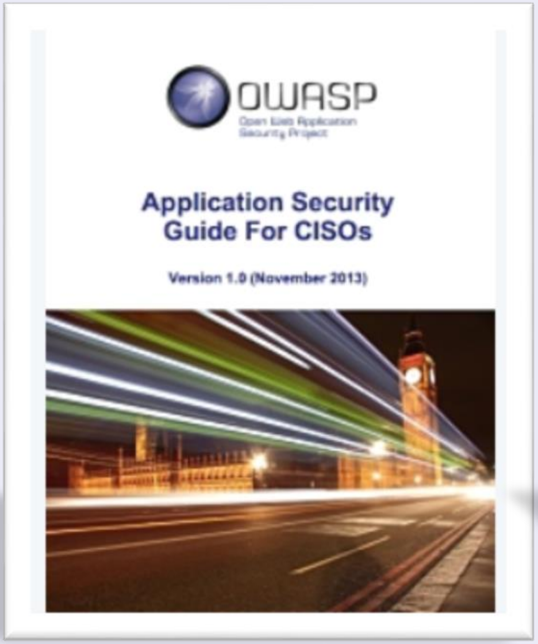
OWASP
Open Web & Application Security Project, www.owasp.org
global non-profit open source security community

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 IAOC (IETF Admininistrative Ovesight Committee), Chair of IETF Security WGs, Member of the IETF Security Directorate, Cloud Security Alliance HK chapter board member

HUAWEI

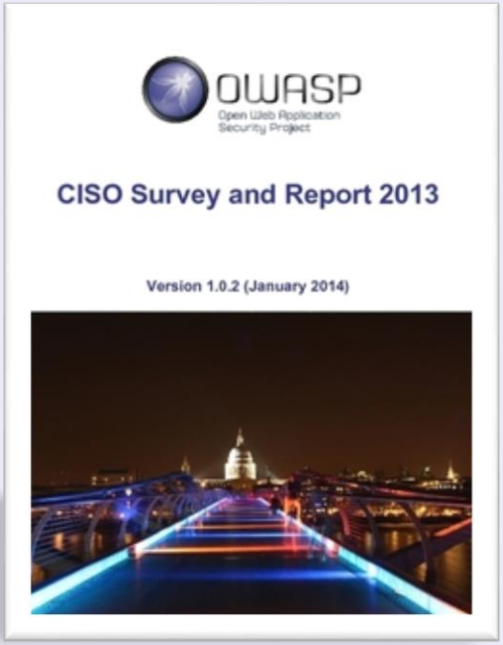
Based on findings of the OWASP CISO Survey Report & CISO Guide



OWASP
Open Web Application Security Project

Application Security Guide For CISOs

Version 1.0 (November 2013)



OWASP
Open Web Application Security Project

CISO Survey and Report 2013

Version 1.0.2 (January 2014)

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

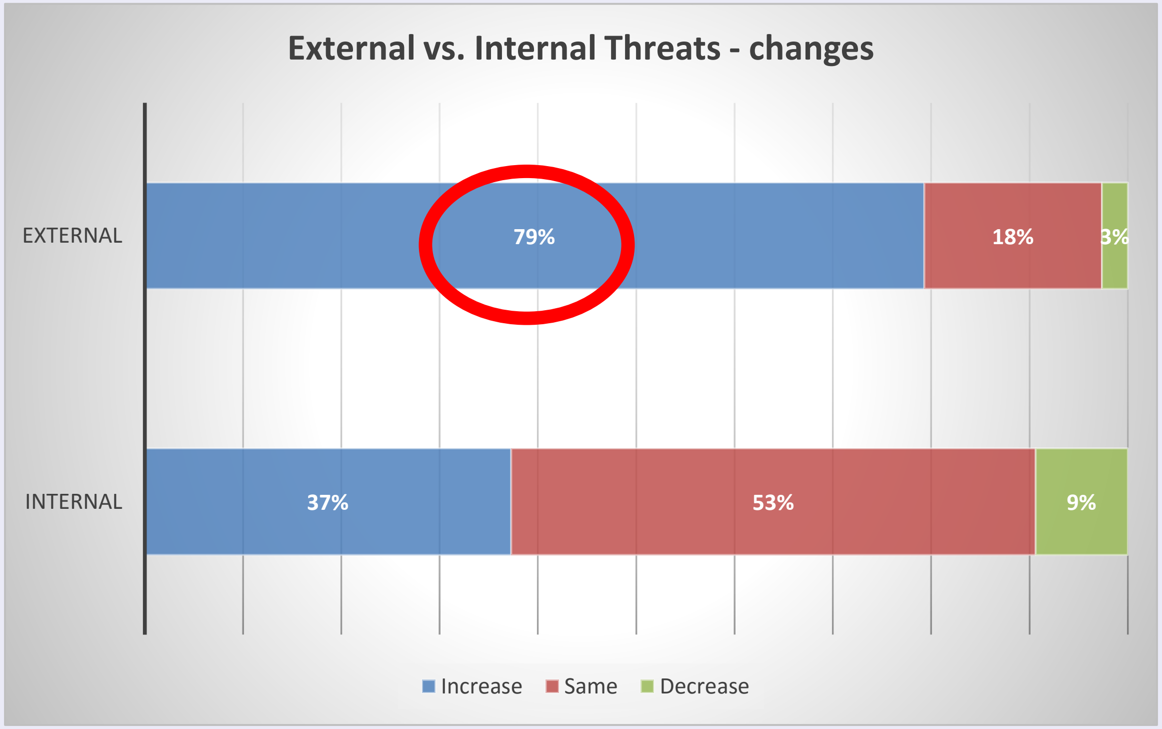
OWASP CISO Survey:
https://www.owasp.org/index.php/OWASP_CISO_Survey

- 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 June 2016*

CYBER
ATTACKS
AHEAD

CISO Survey: External Threats are on the Rise!

OWASP 中国
The Open Web Application Security Project

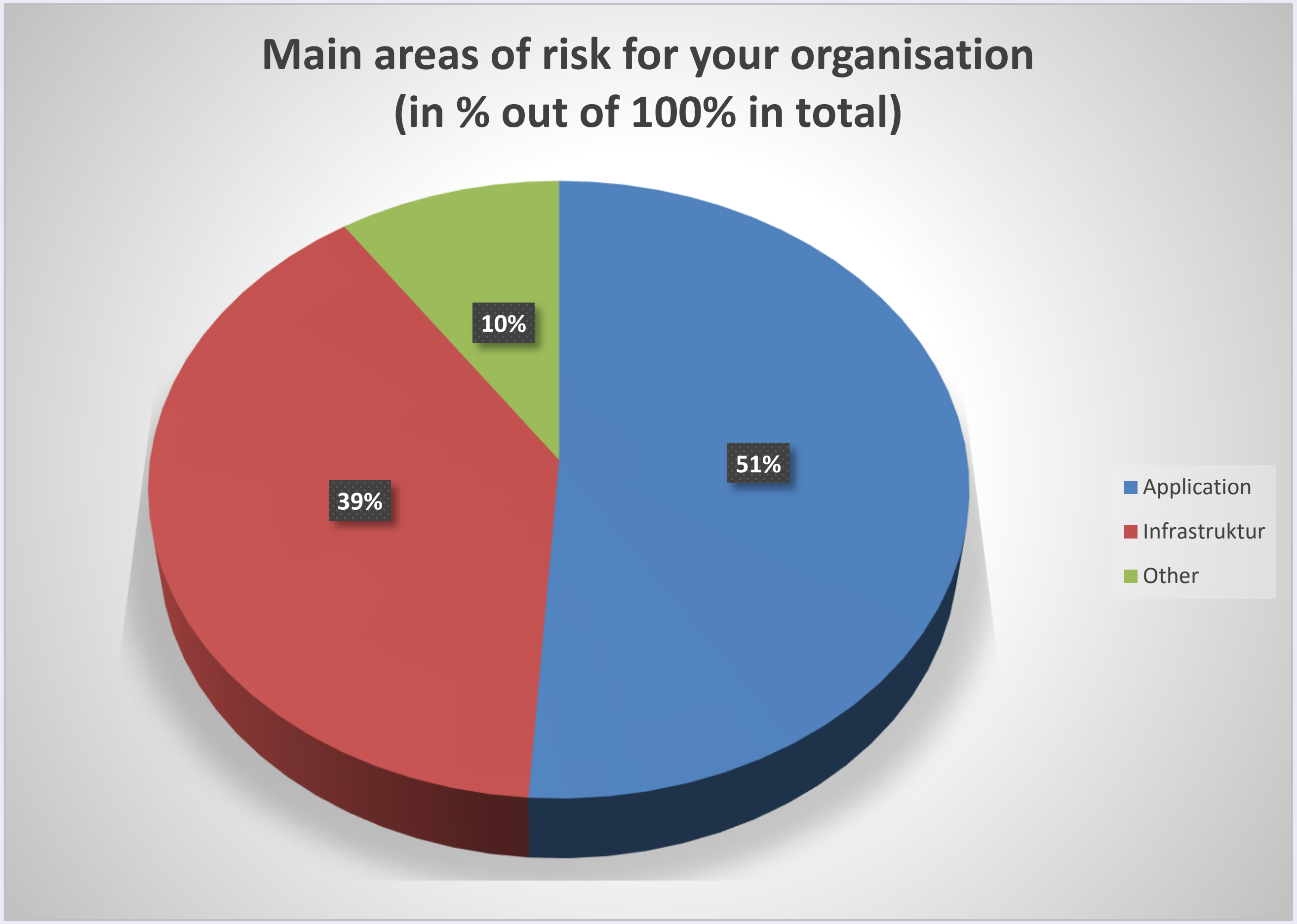


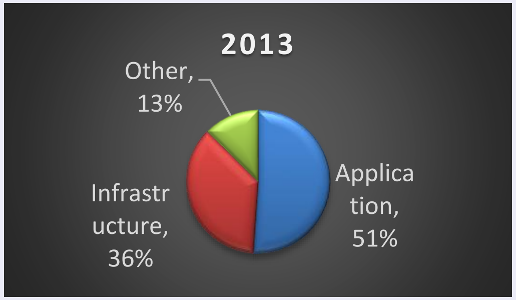
» External attacks or fraud (e.g., phishing, website attacks)

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

CISO Survey: Threats towards your organization

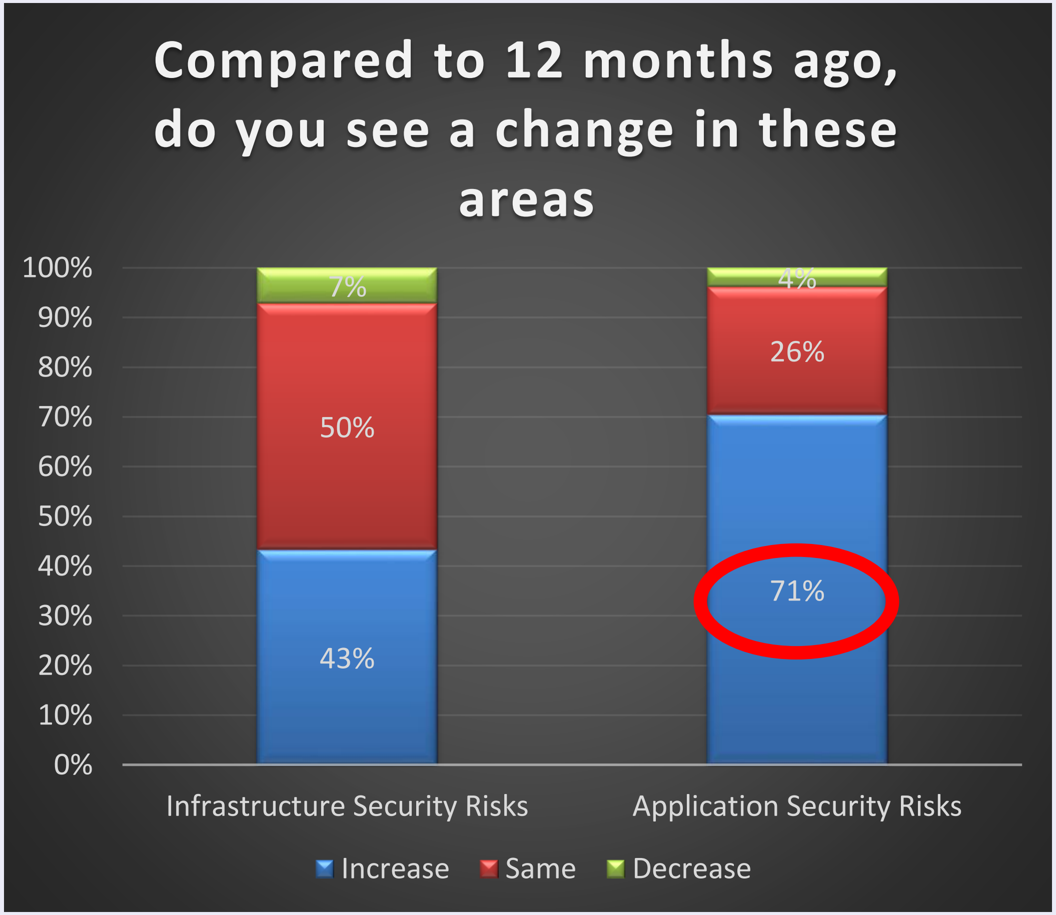
OWASP 中国
The Open Web Application Security Project

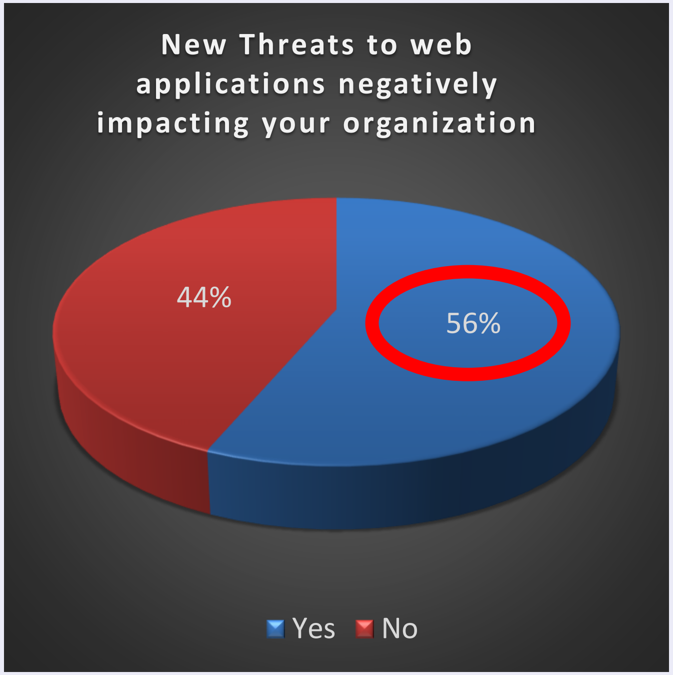




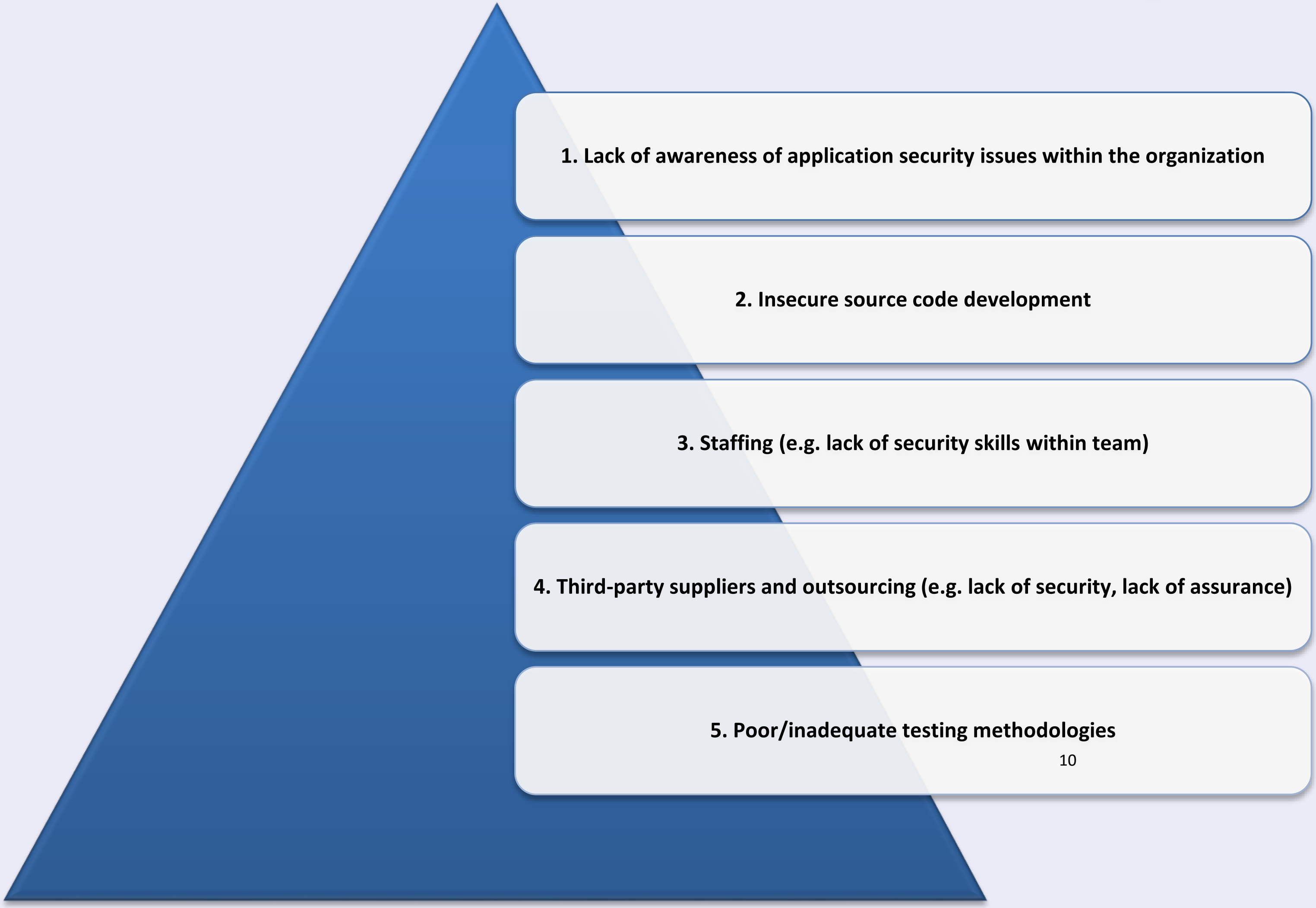
CISO Survey : Threat Trends

OWASP 中国
The Open Web Application Security Project





Top-5 Sources of application security risk



1. Lack of awareness of application security issues within the organization

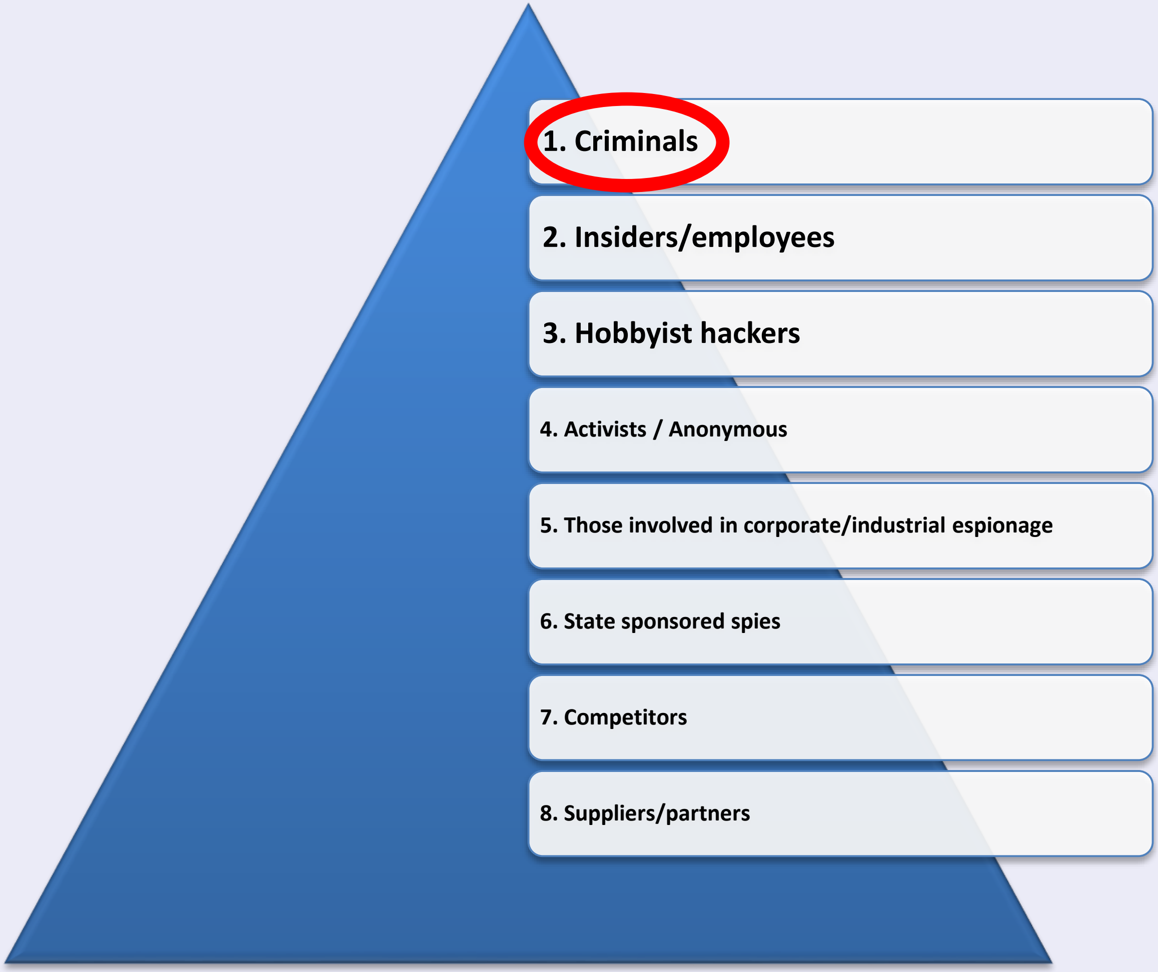
2. Insecure source code development

3. Staffing (e.g. lack of security skills within team)

4. Third-party suppliers and outsourcing (e.g. lack of security, lack of assurance)

5. Poor/inadequate testing methodologies

you think are the most likely to target your company in the next 12 months



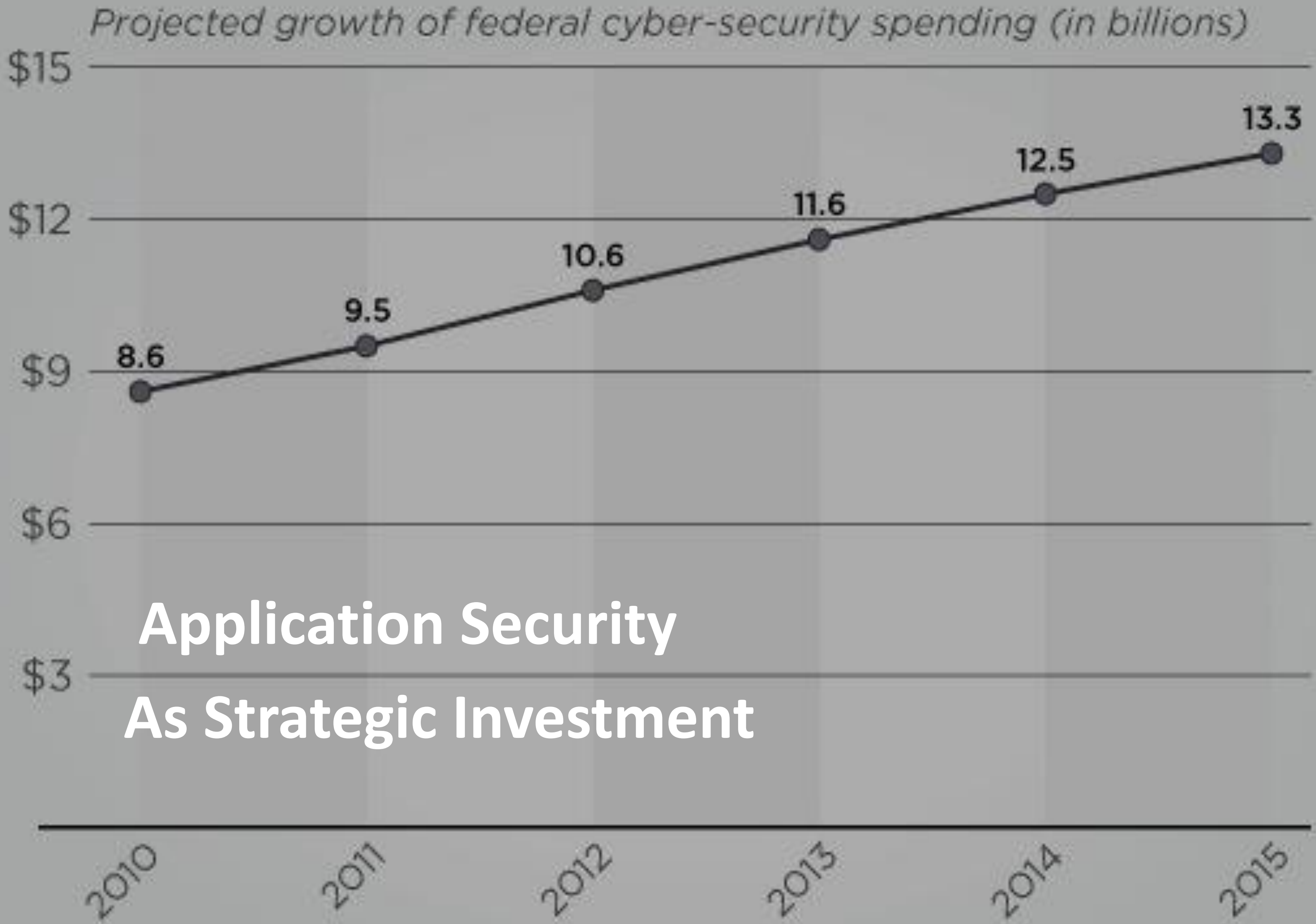
1. Criminals
2. Insiders/employees
3. Hobbyist hackers
4. Activists / Anonymous
5. Those involved in corporate/industrial espionage
6. State sponsored spies
7. Competitors
8. Suppliers/partners

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)

Application Security

As Strategic Investment

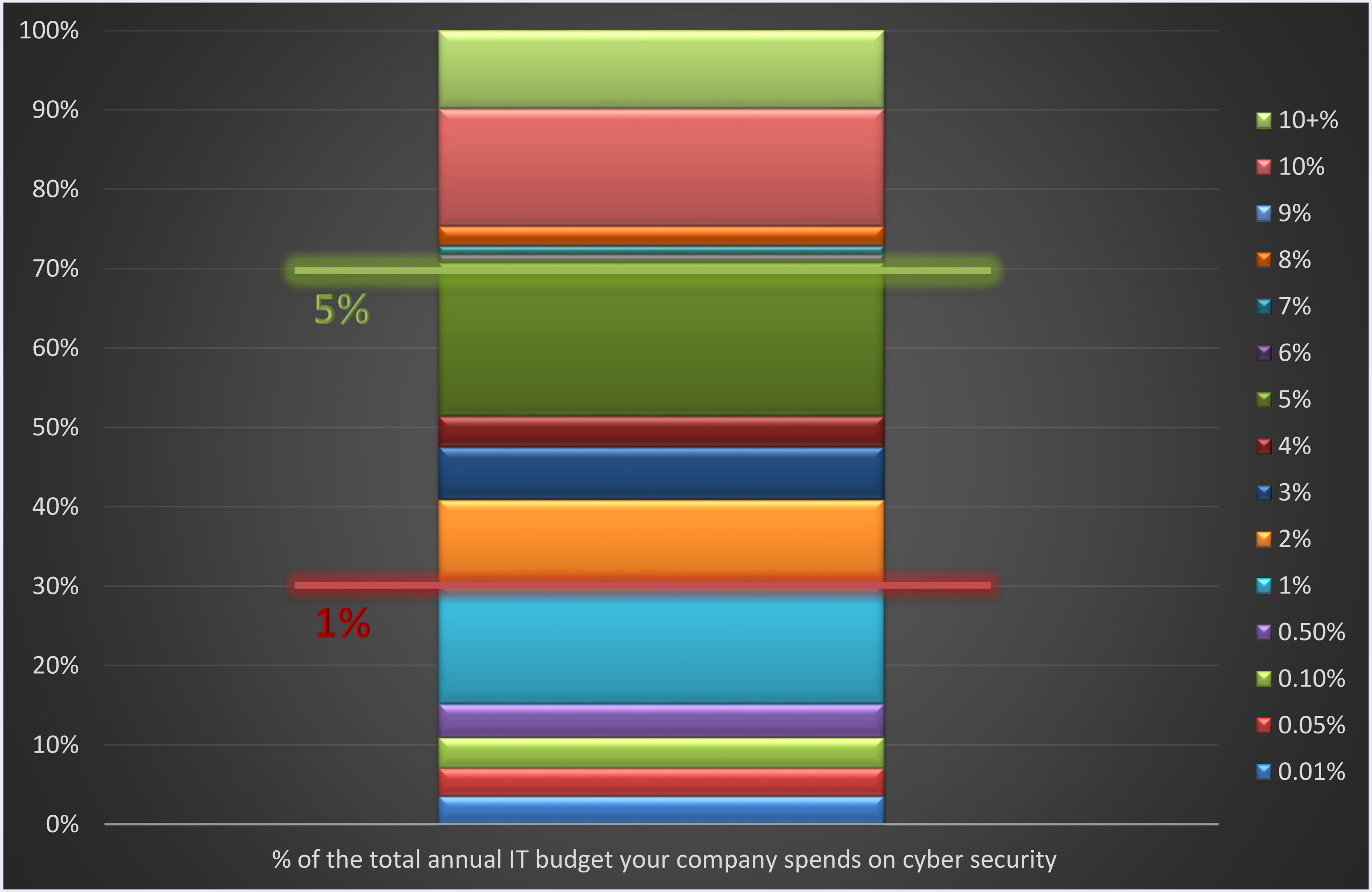


Source: Deltek, Inc.
By: CHRIS SPURLOCK/THE HUFFINGTON POST

HUFFPOST TECH

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

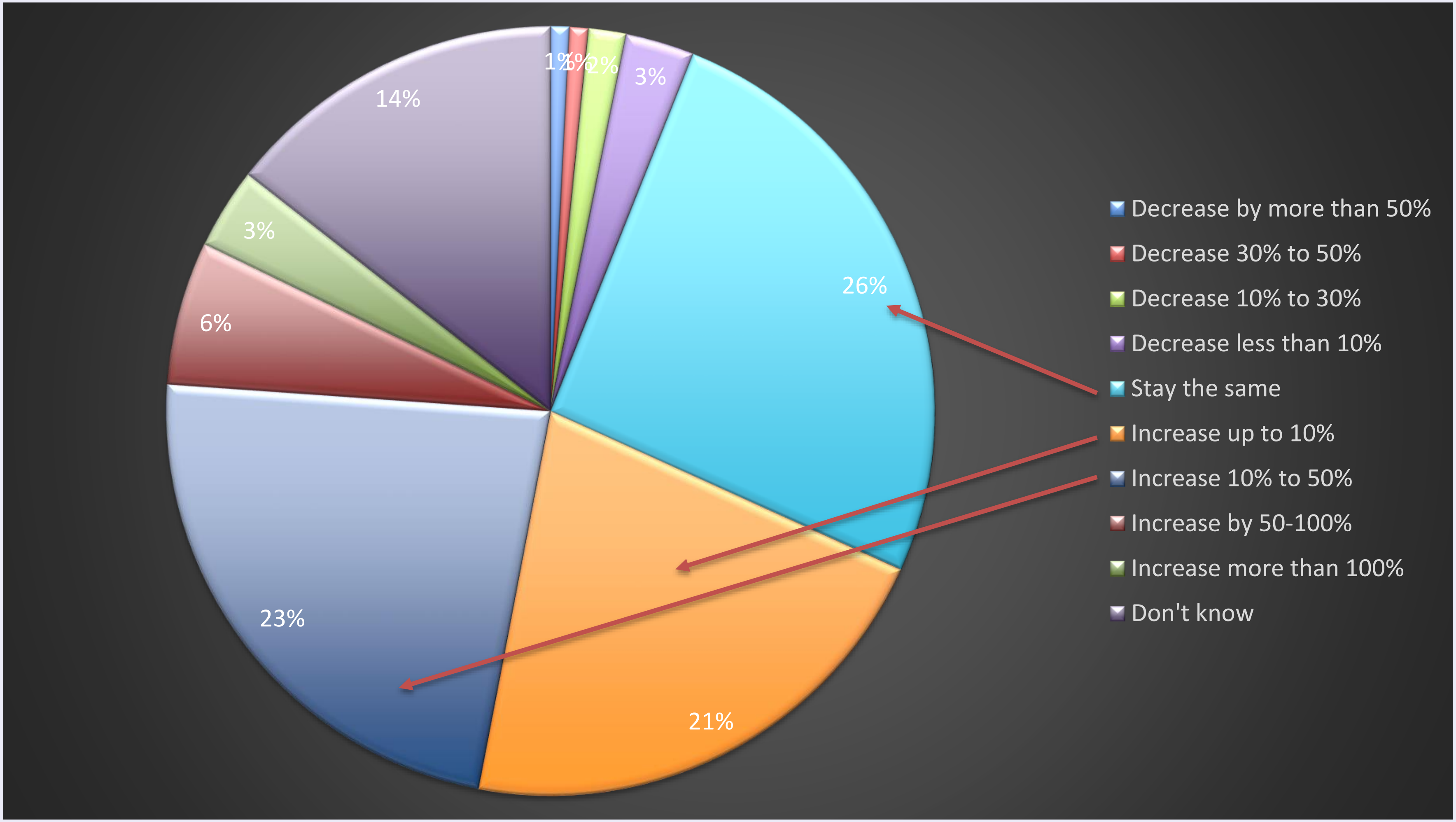
OWASP 中国
The Open Web Application Security Project



CISO Survey & Report: Investments in Security

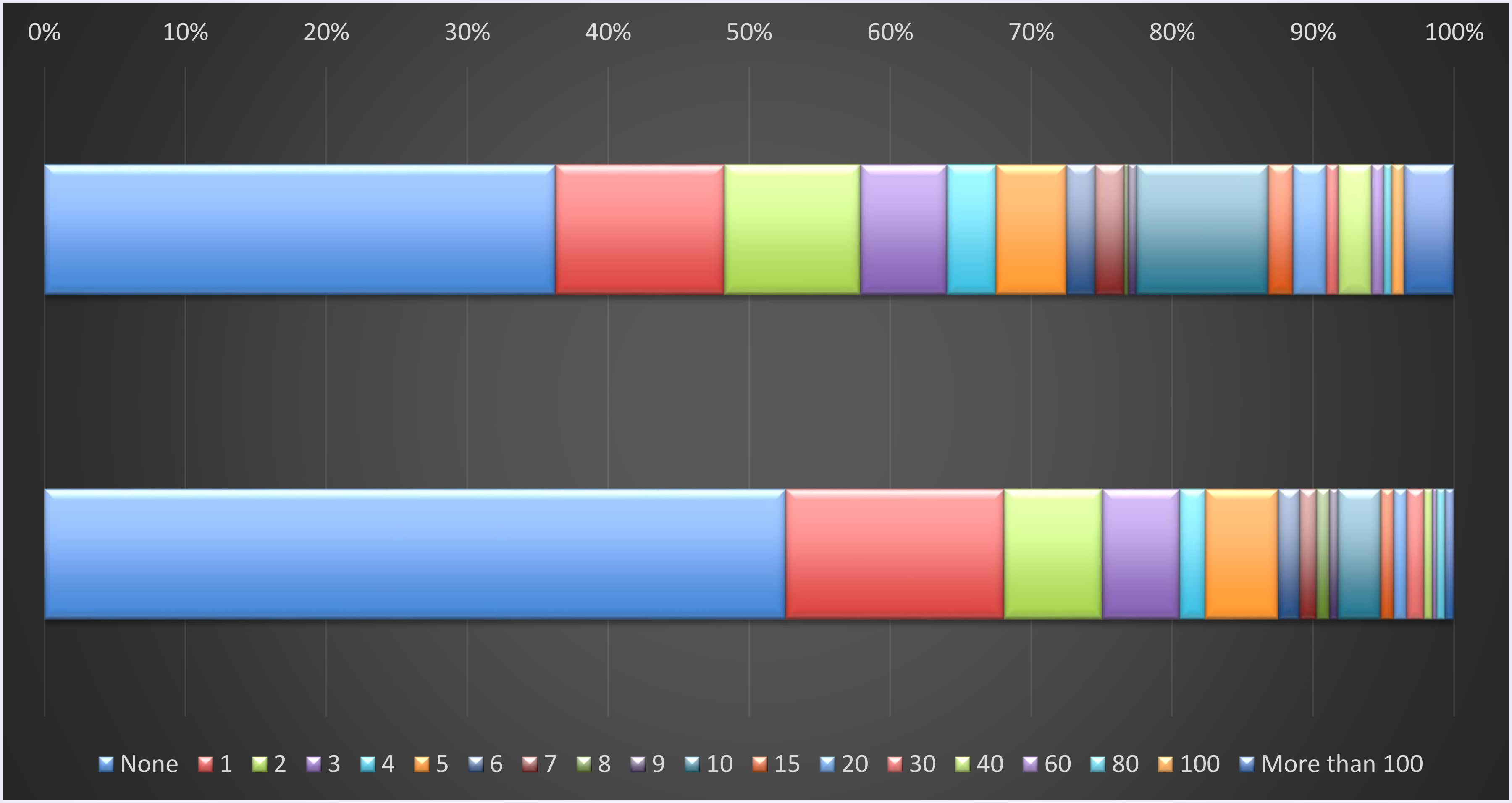
Your total cyber security spending over the next 12 months will…

OWASP 中国
The Open Web Application Security Project



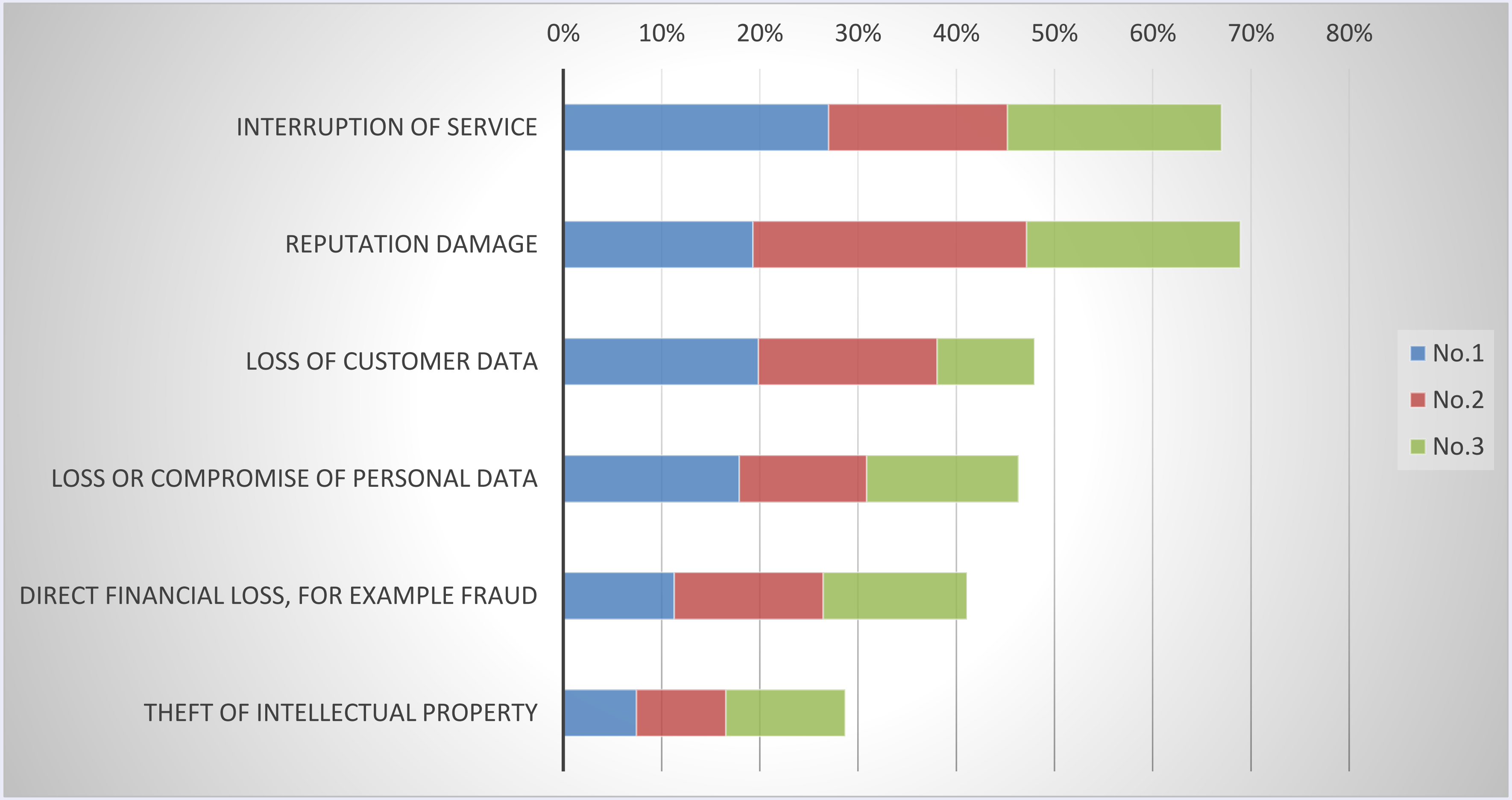
How many security breaches did your company experience in the last 12 months? (Cyber security and Application Security breaches)

OWASP 中国
The Open Web Application Security Project



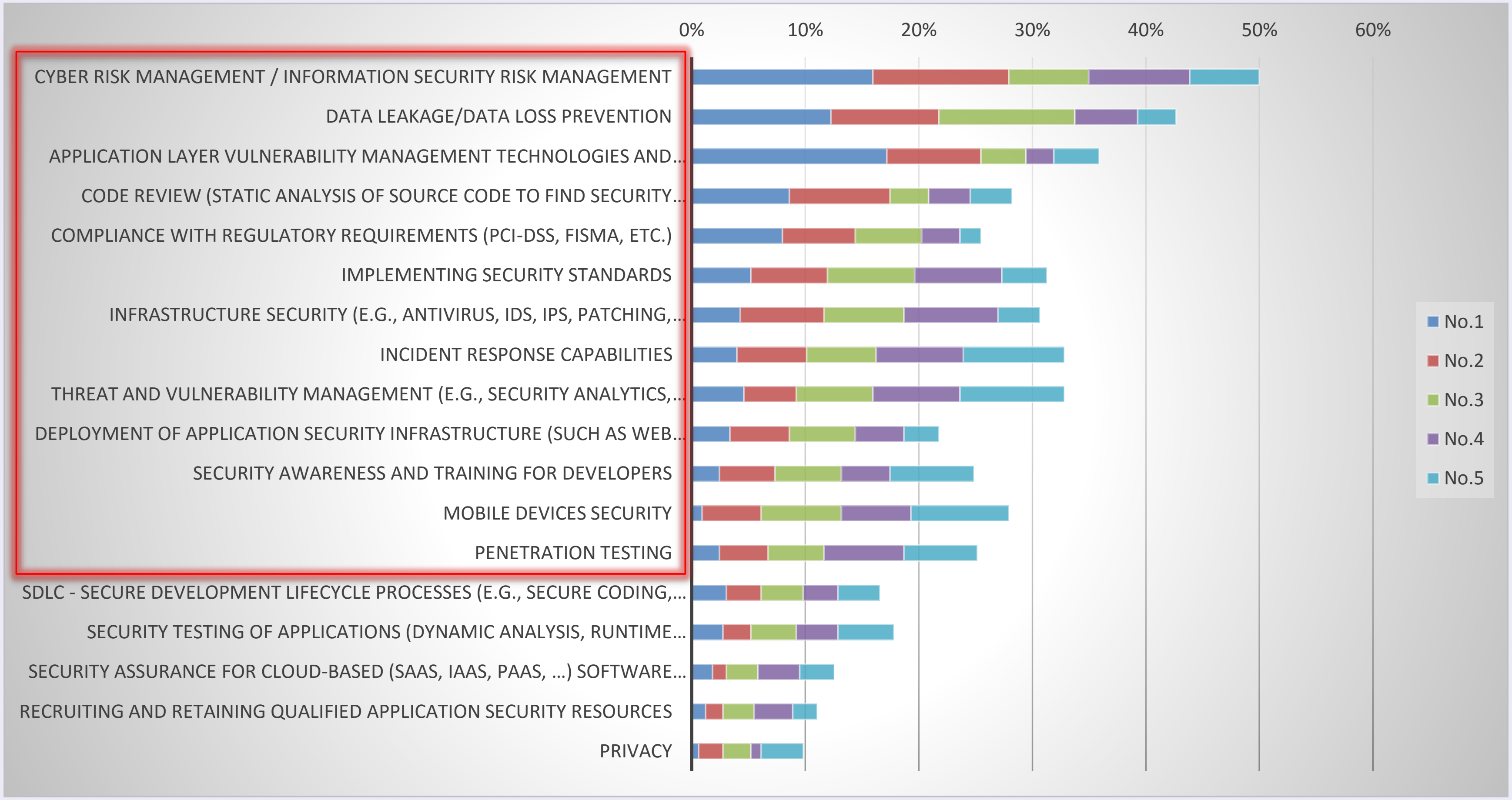
Main damage types caused by cyber attacks

OWASP 中国
The Open Web Application Security Project



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

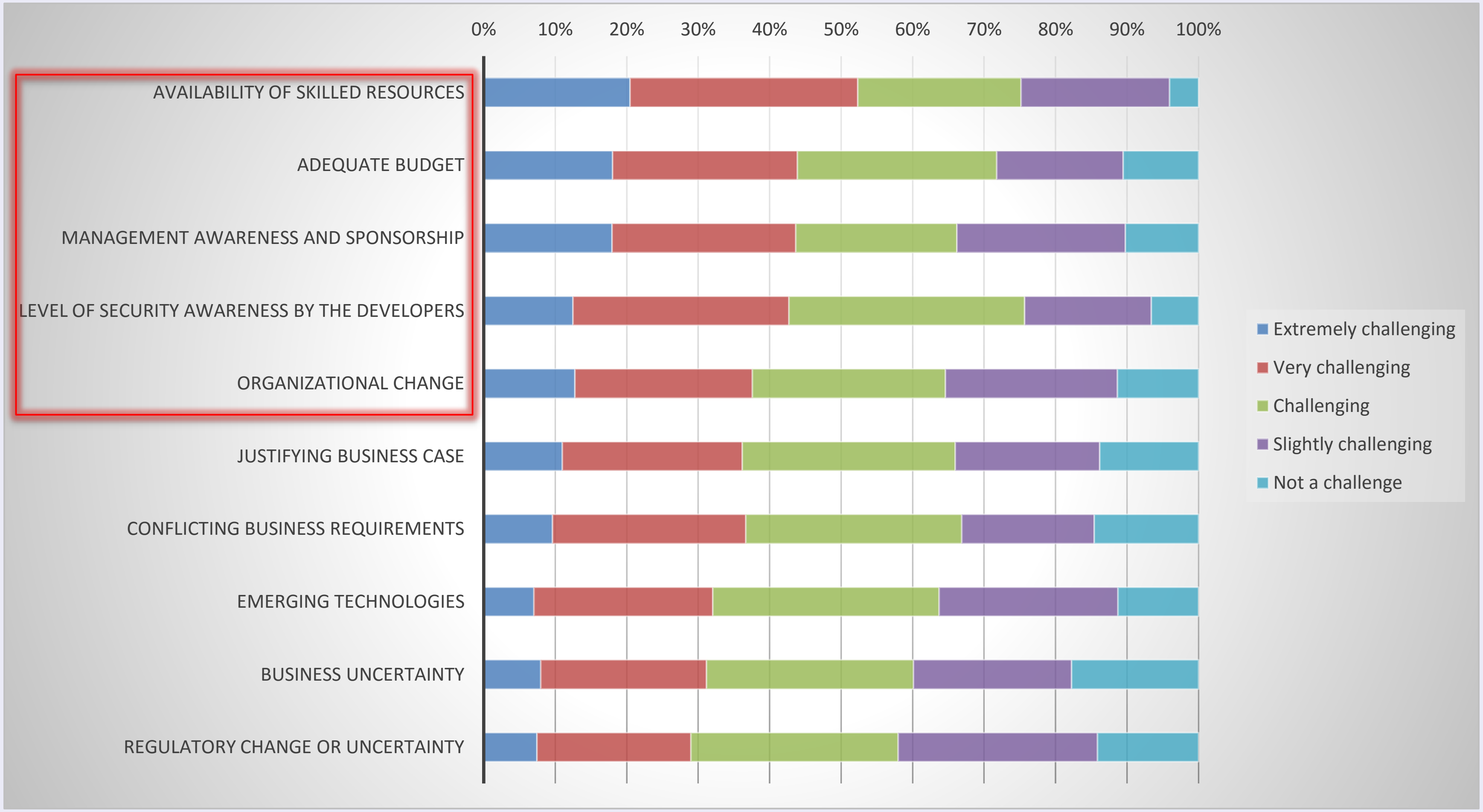
OWASP 中国
The Open Web Application Security Project



Biggest challenges delivering your organization's application security initiatives

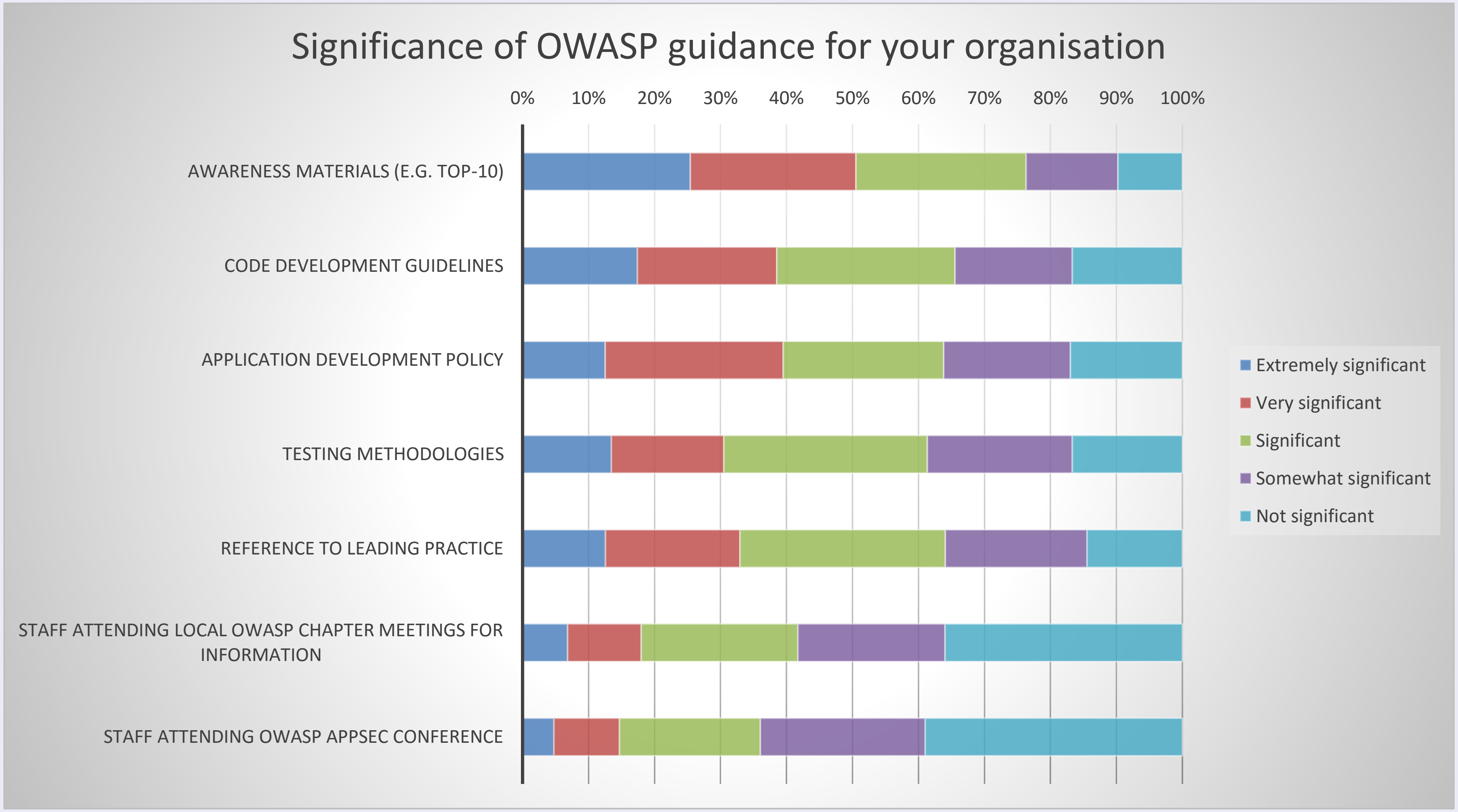
OWASP 中国

The Open Web Application Security Project



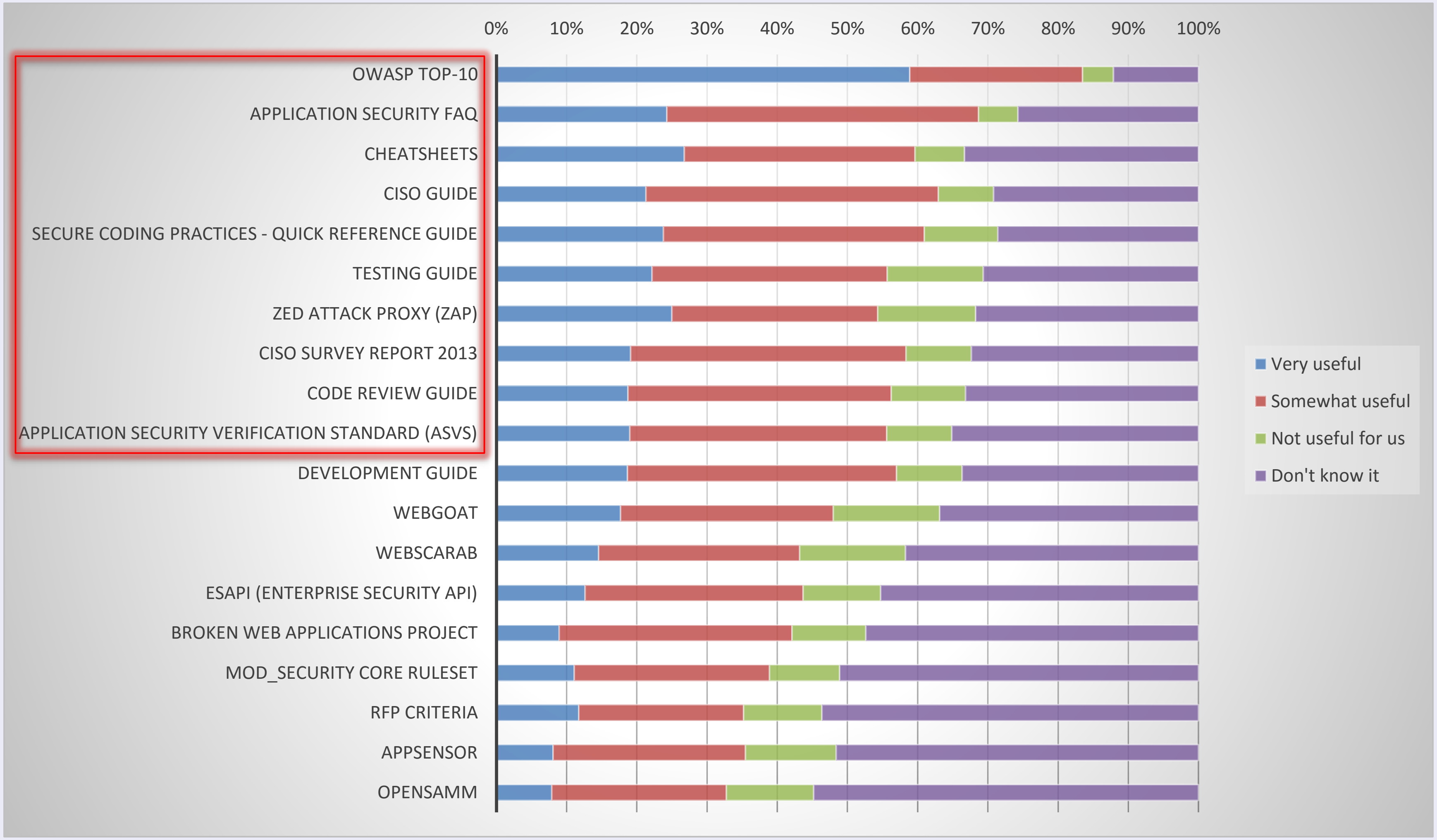
Where you see OWASP can help you

OWASP 中国
The Open Web Application Security Project



Which OWASP projects people found useful (Top-10)

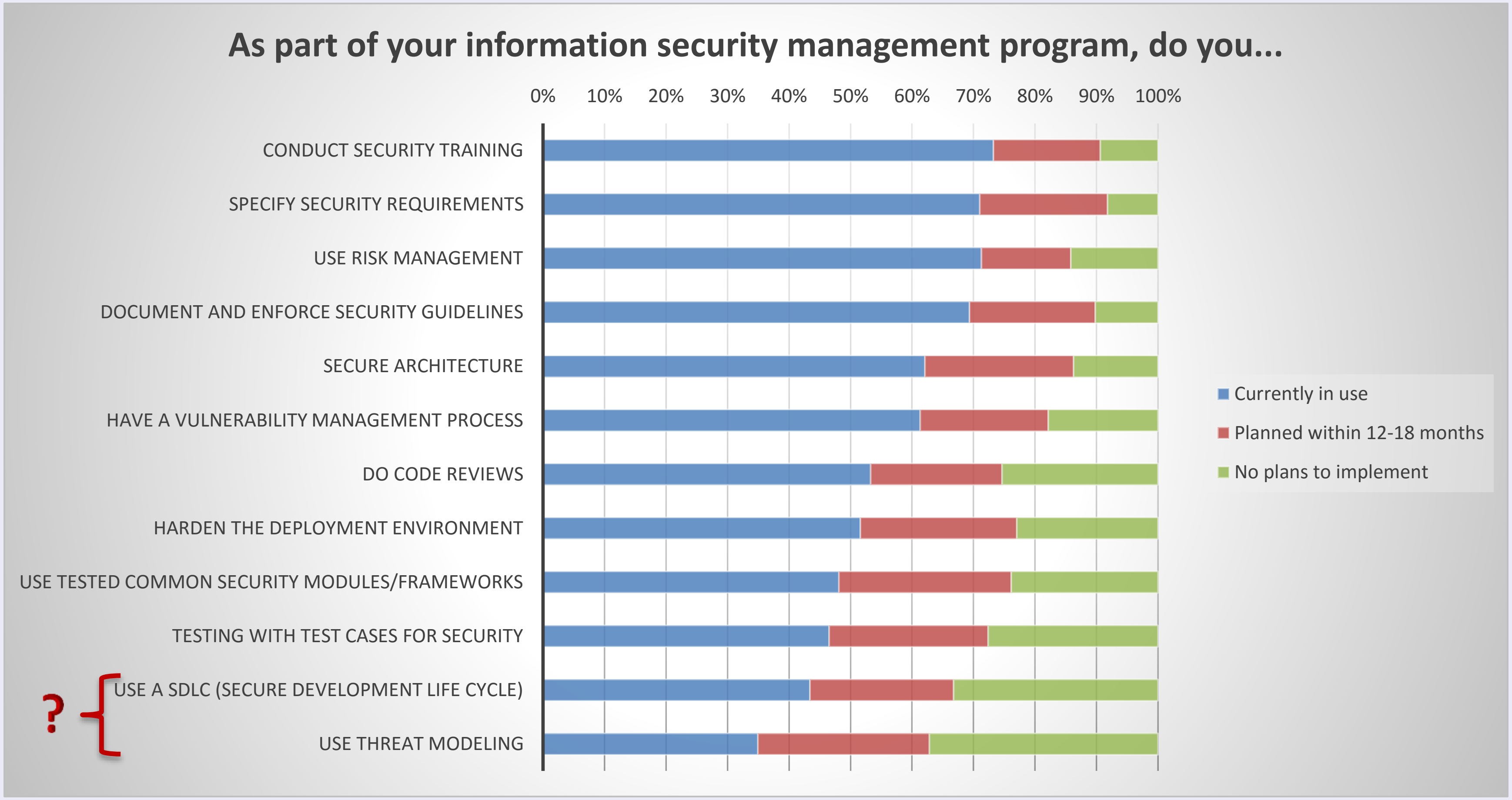
OWASP 中国
The Open Web Application Security Project



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

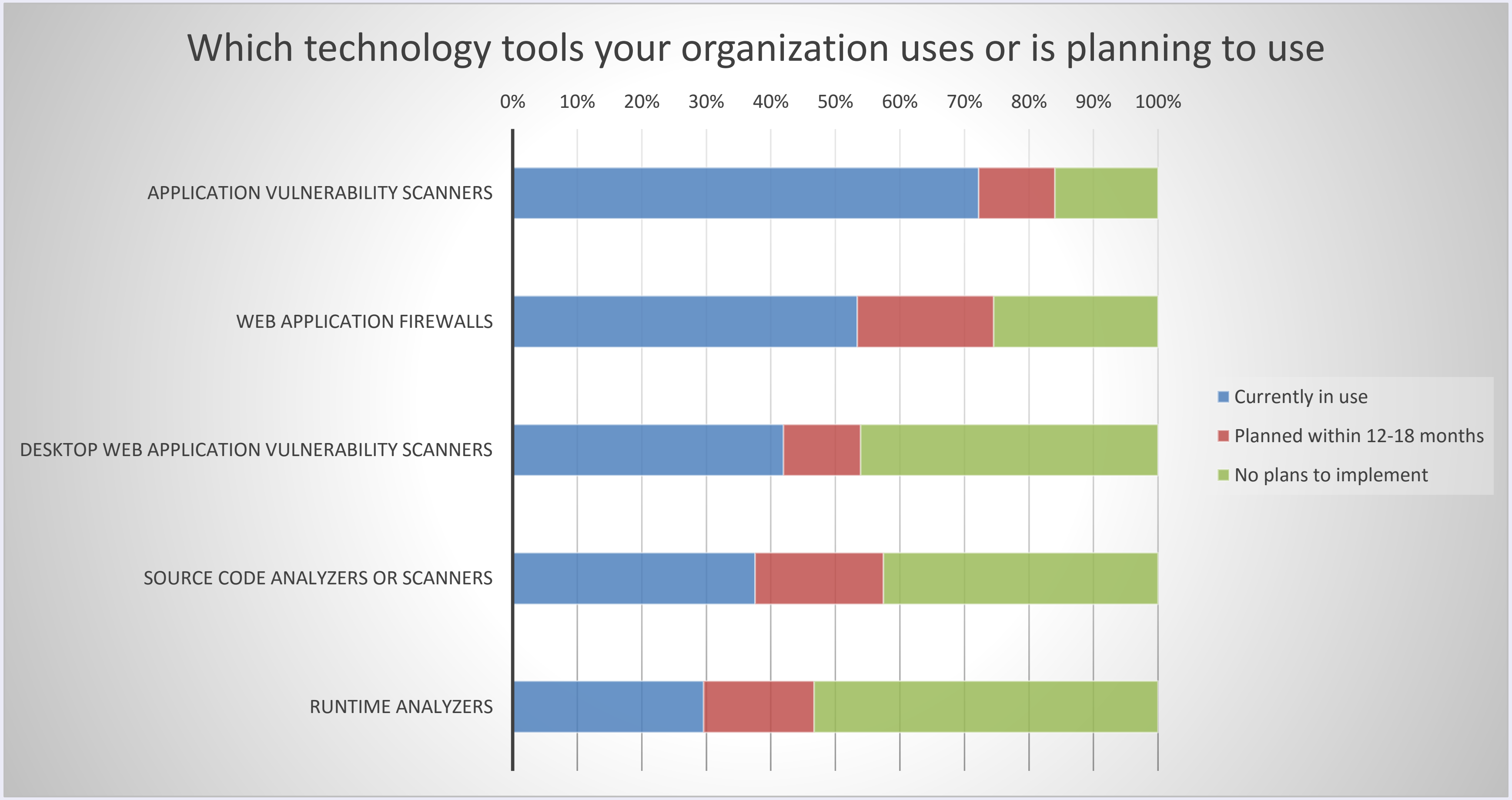
OWASP 中国

The Open Web Application Security Project



Which technology tools organizations use or are planning to use…

OWASP 中国
The Open Web Application Security Project

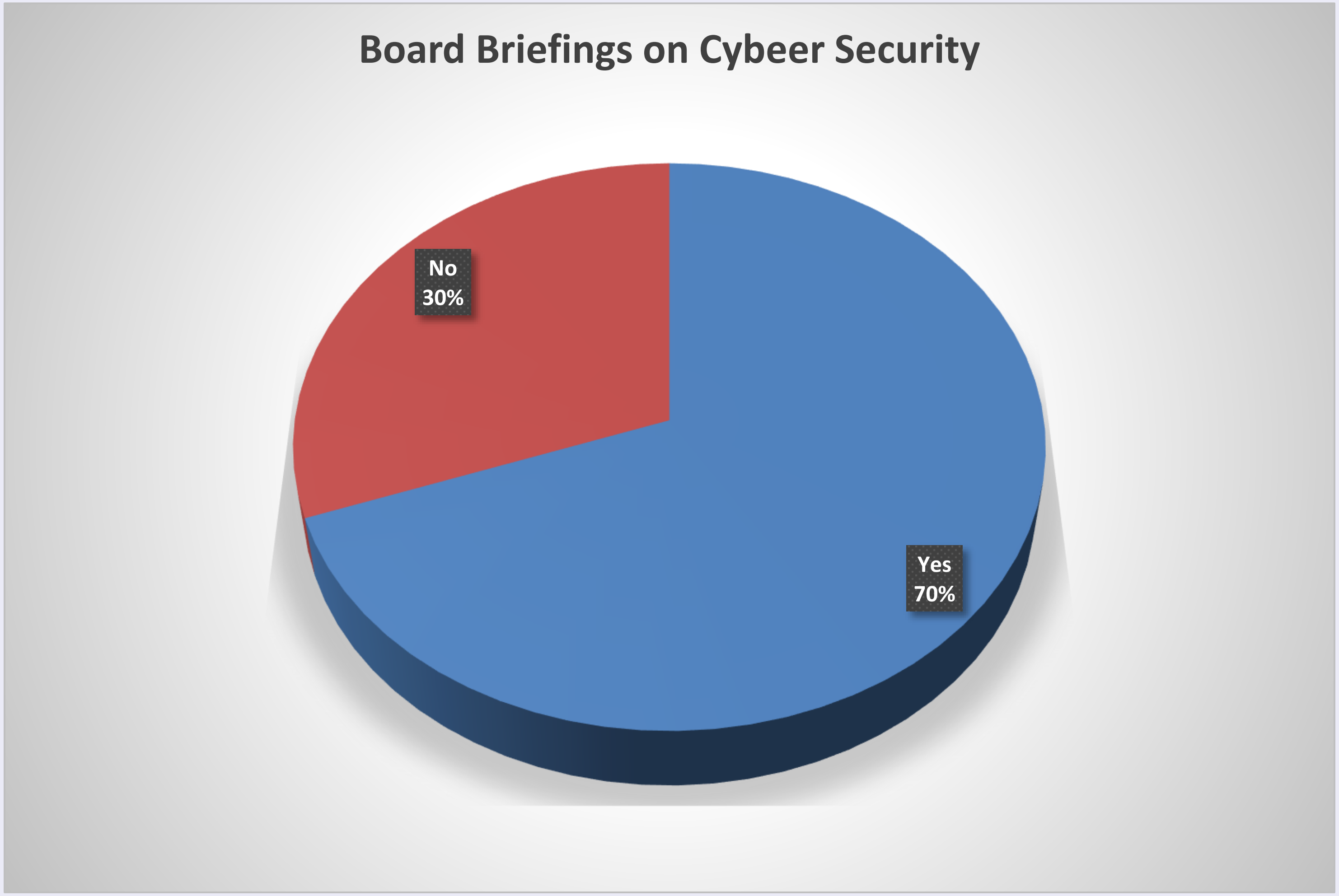


Build Security In, Security Strategy & Maturity Models

Strategy & Planning: board awareness…

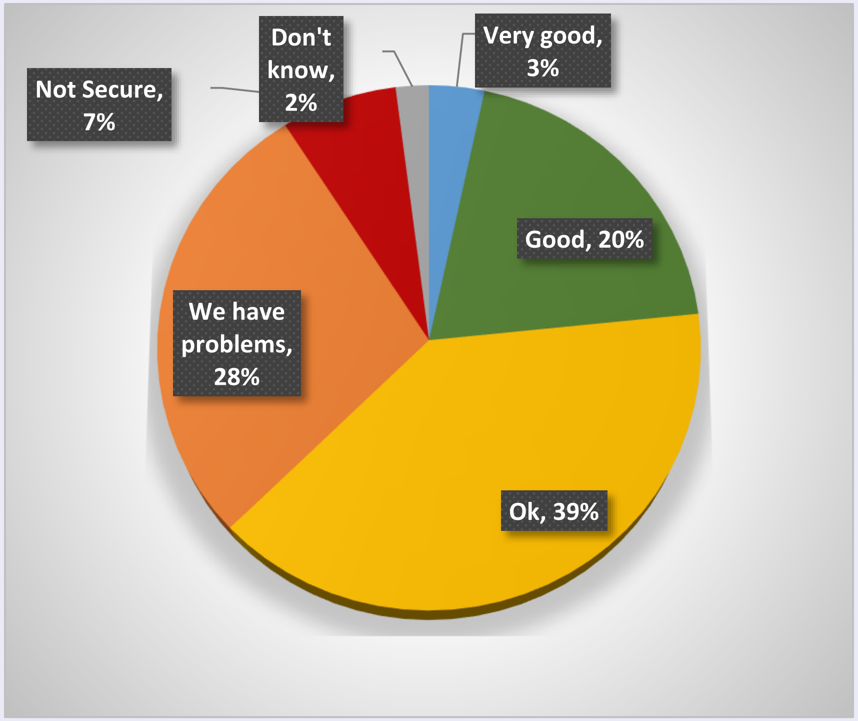
OWASP 中国

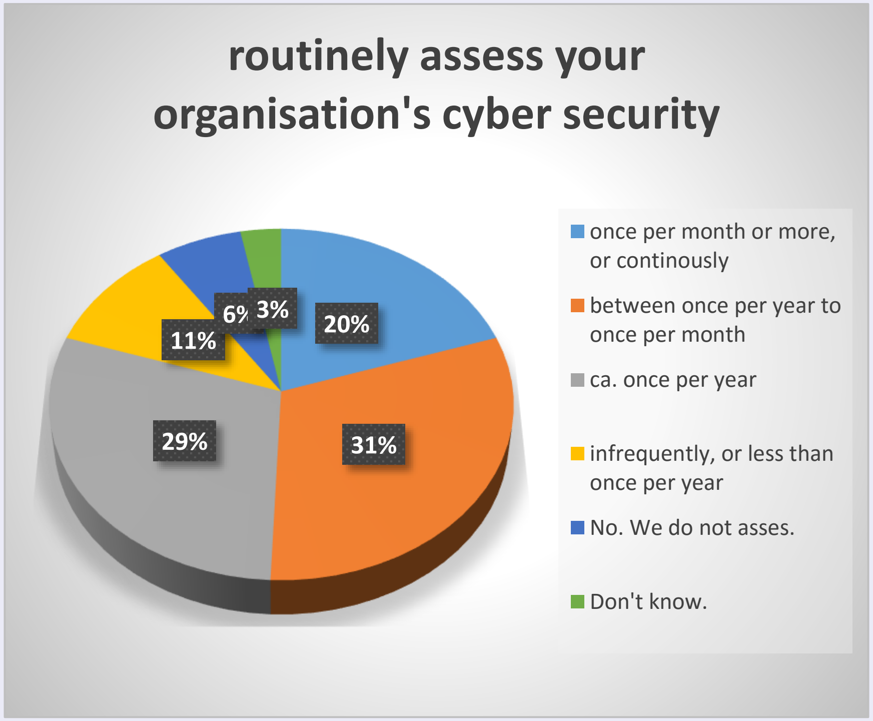
The Open Web Application Security Project



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

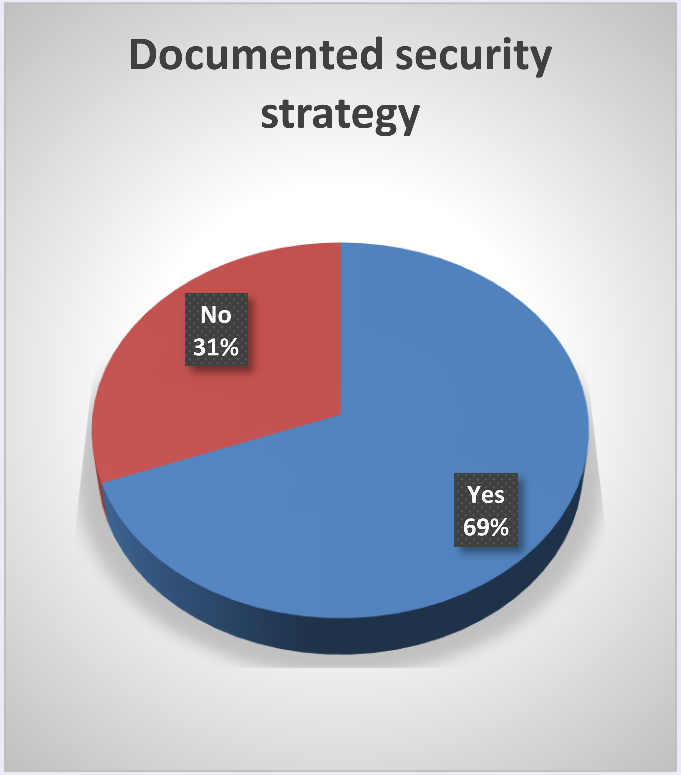
OWASP 中国
The Open Web Application Security Project

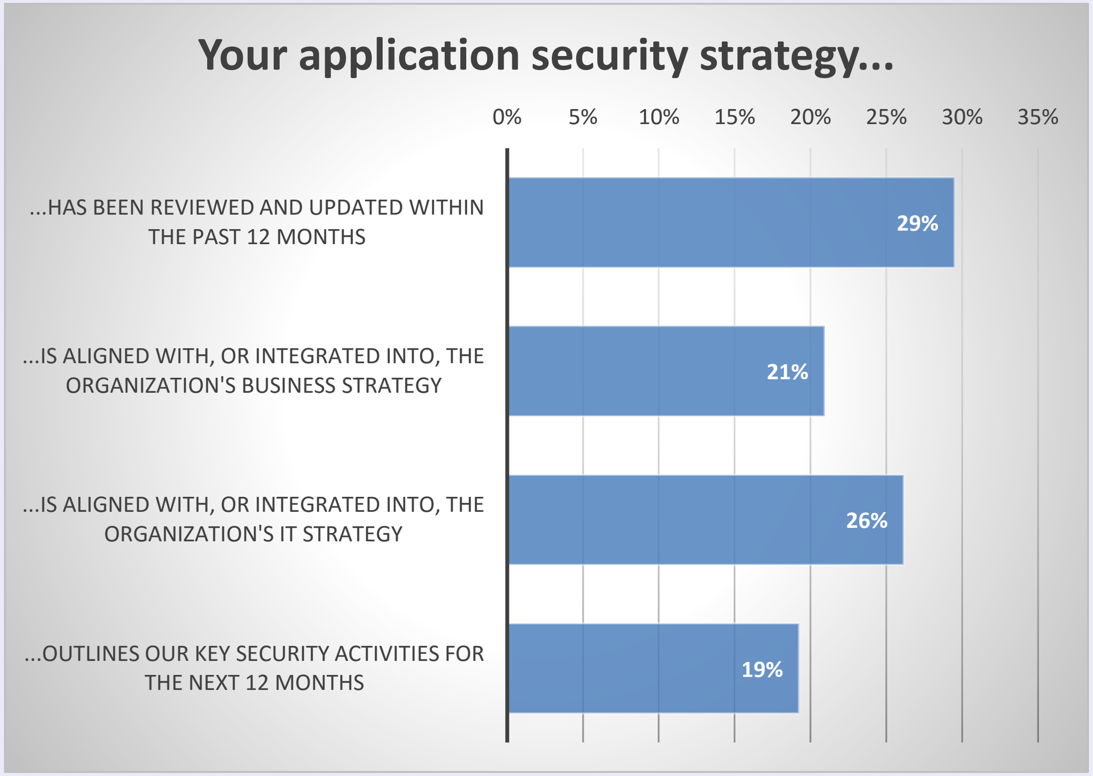




Strategy & Planning

OWASP 中国
The Open Web Application Security Project

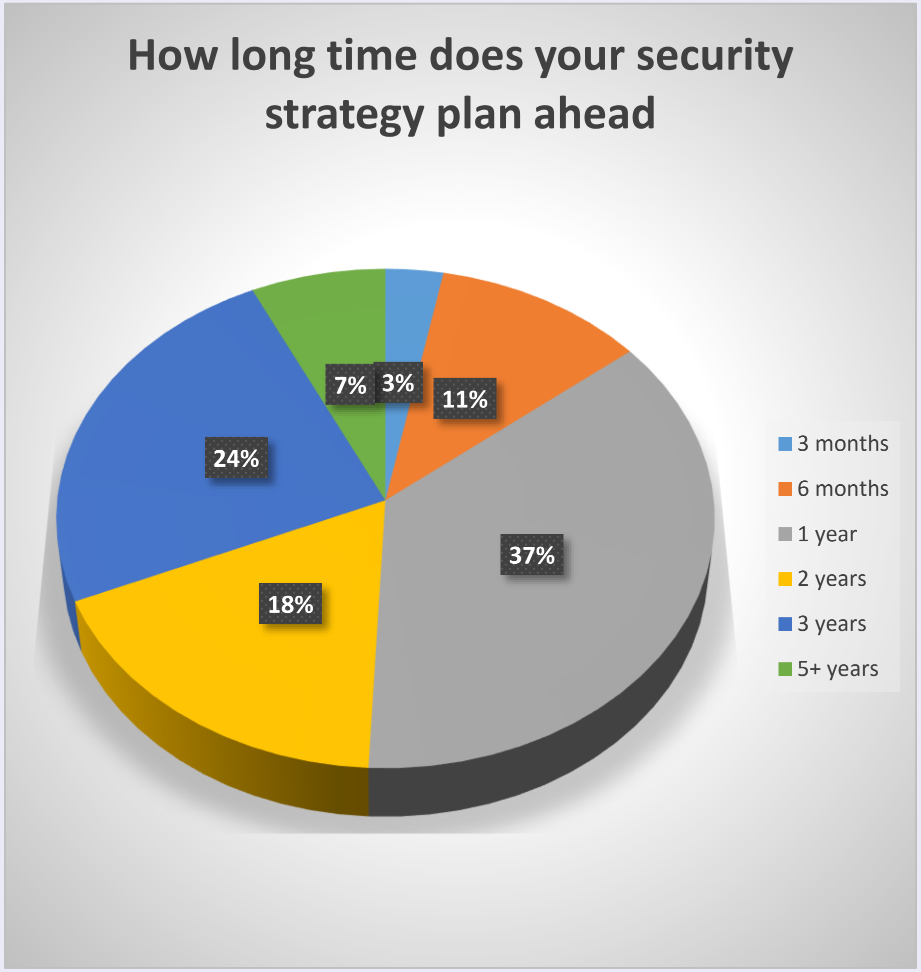




In case you wonder:
We found a medium positive correlation between board briefings and whether you have a security strategy: 0.43

Strategy & Planning

OWASP 中国
The Open Web Application Security Project



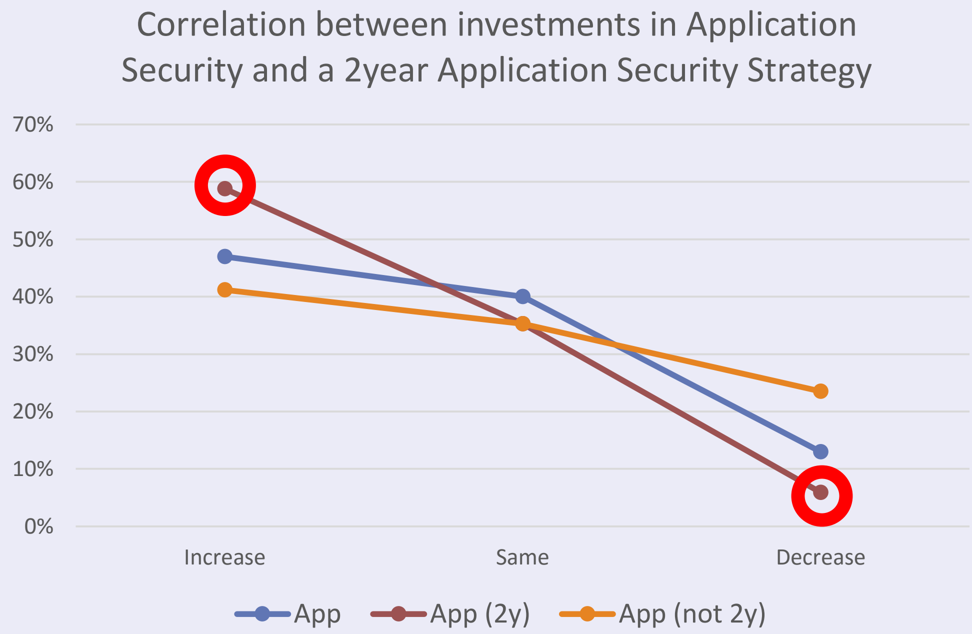
Trends of security strategy planning 2013 -> 2015: longer time horizons

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

OWASP 中国
The Open Web Application Security Project

»Benefits of a security strategy for application security investments:

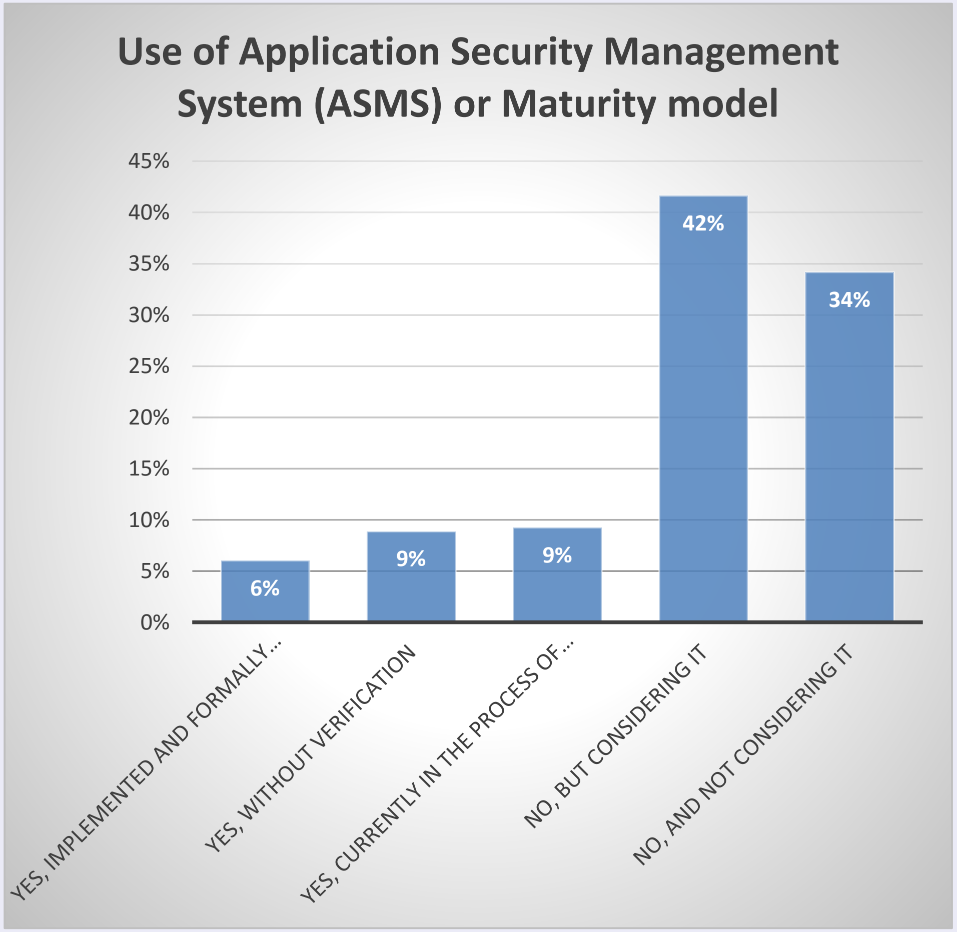


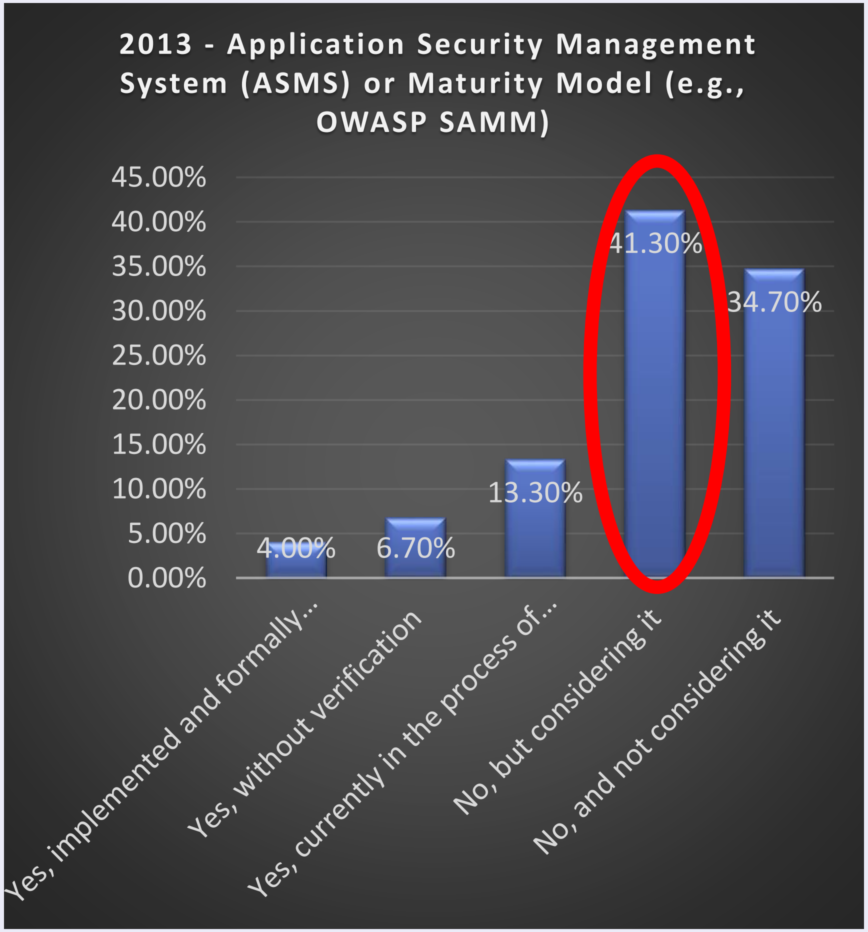
Analysis for correlations with:

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

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

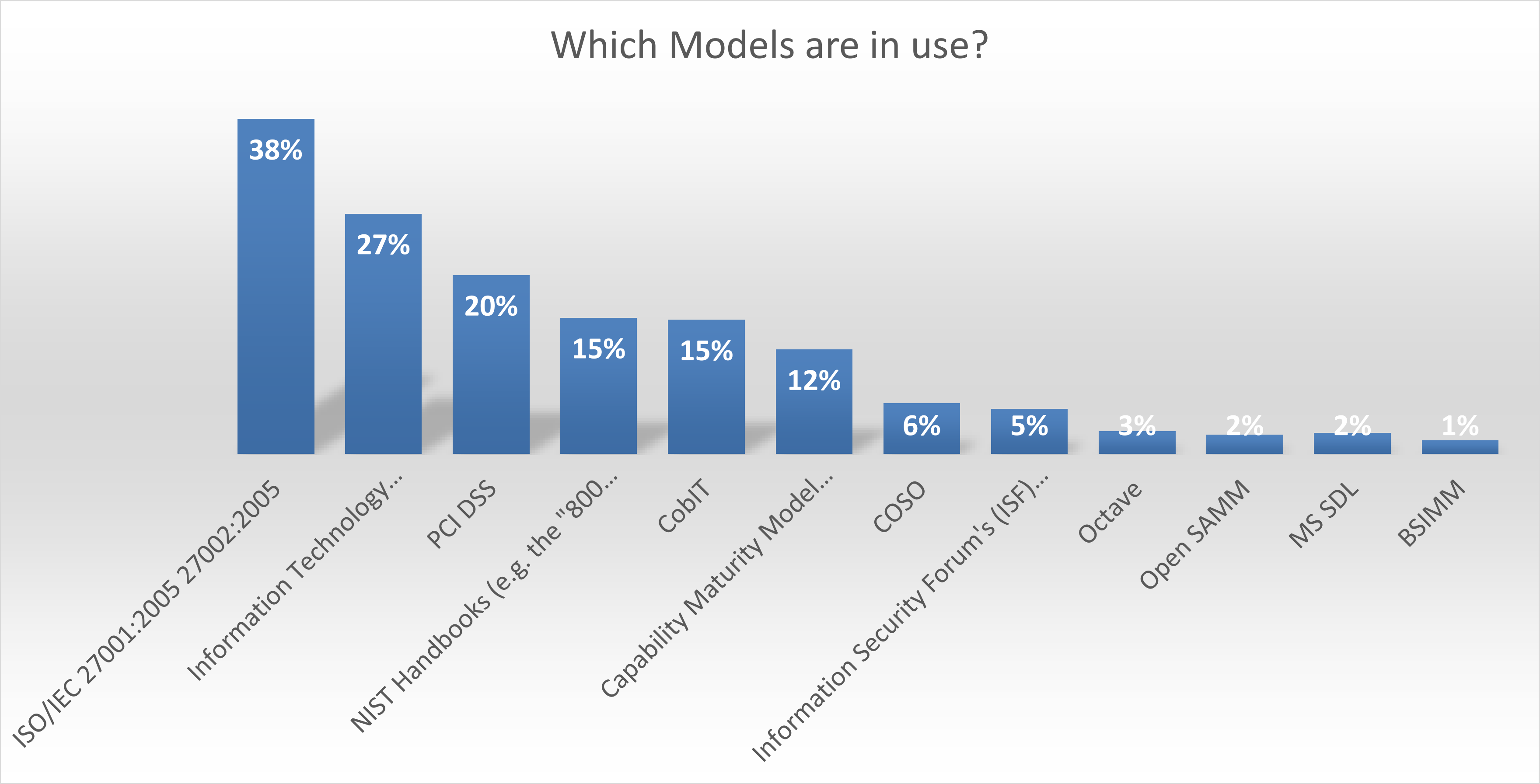
OWASP 中国
The Open Web Application Security Project





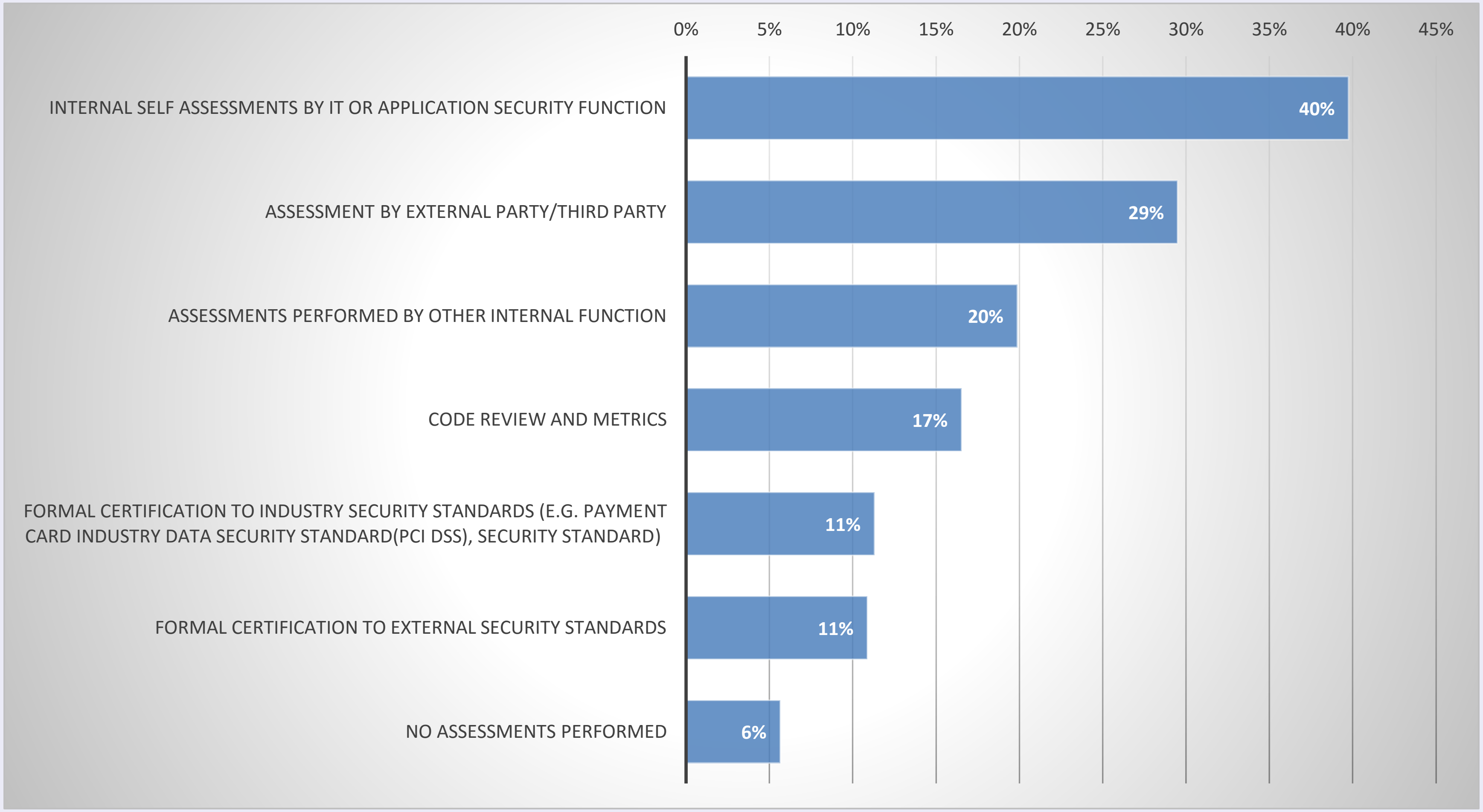
Strategy & Planning: Maturity Model trends compare with 2013

OWASP 中国
The Open Web Application Security Project



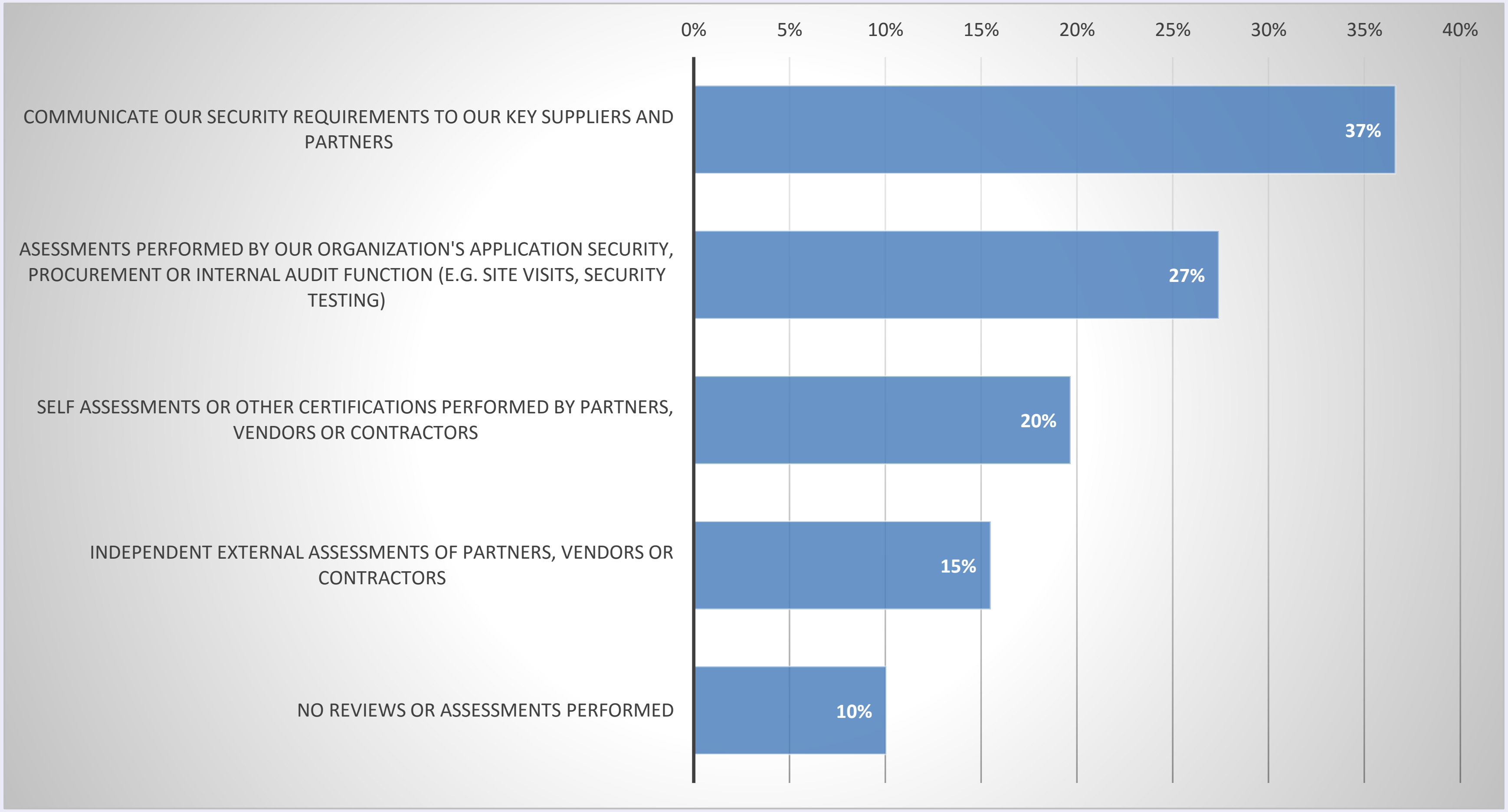
How does your organization assess the quality and effectiveness of application security?

OWASP 中国
The Open Web Application Security Project



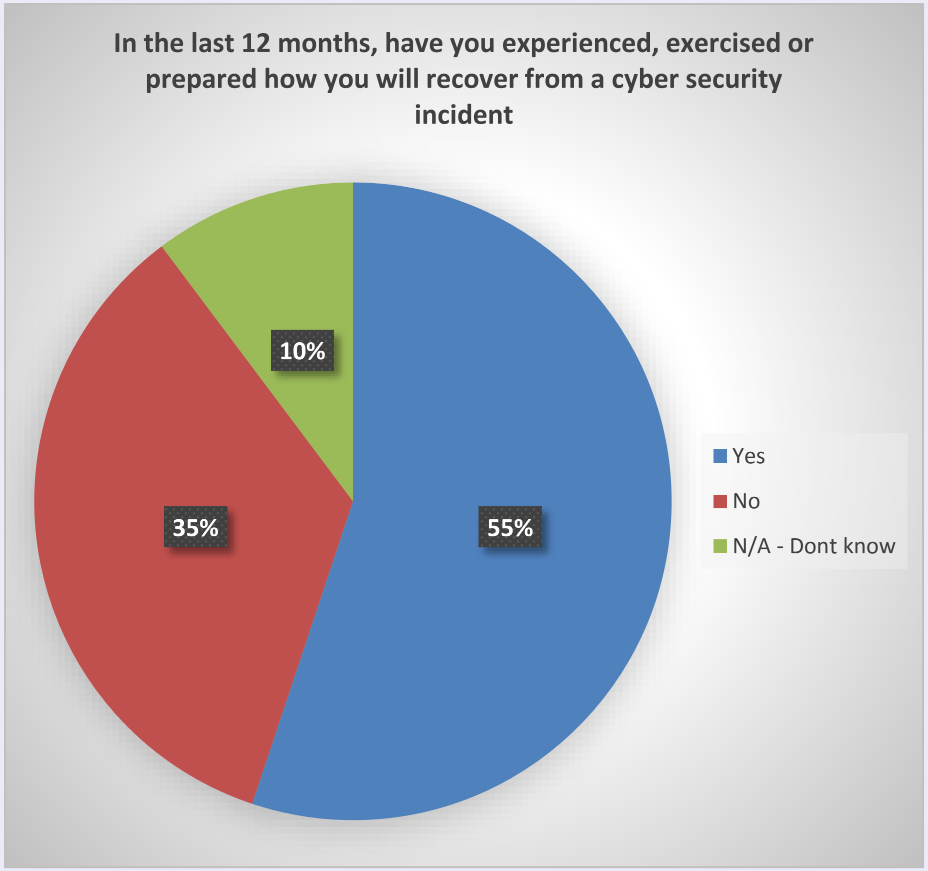
Suppliers & External Partners: How do you verify your external partners…

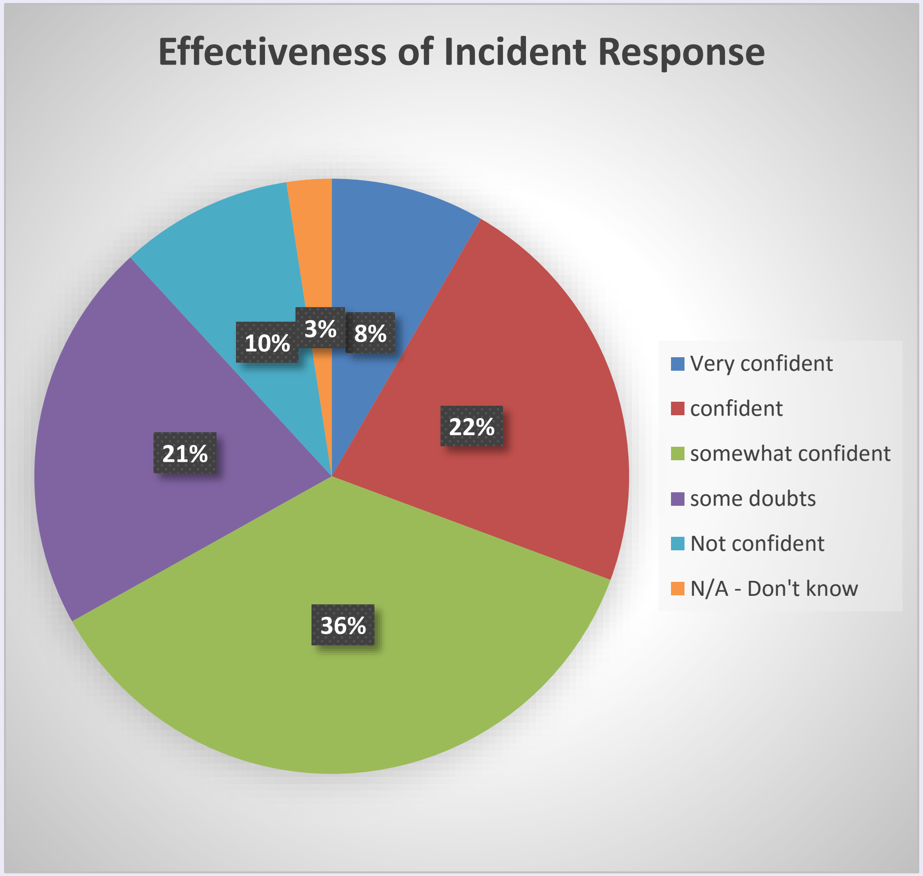
OWASP 中国
The Open Web Application Security Project



Incident Response

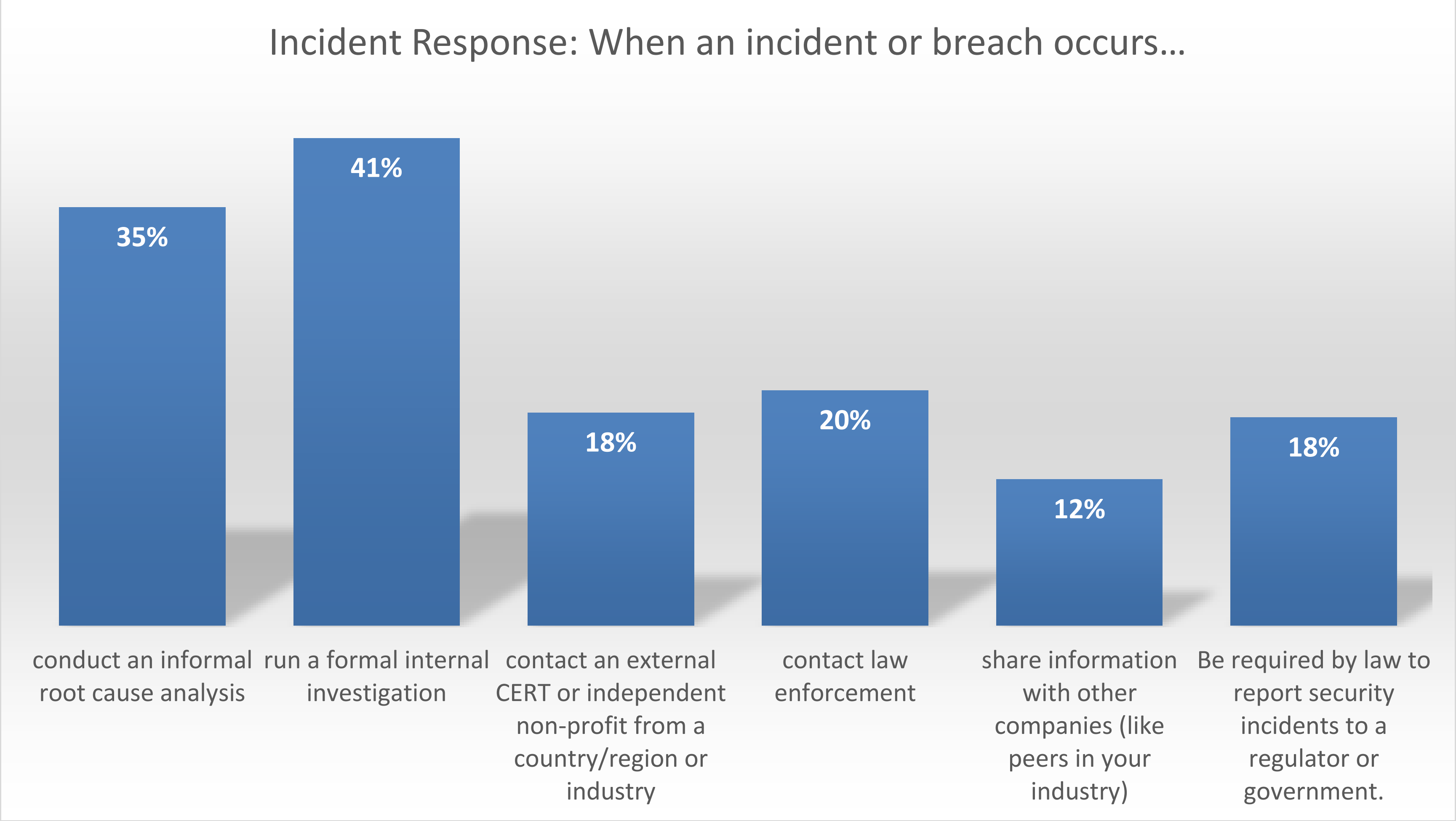
OWASP 中国
The Open Web Application Security Project





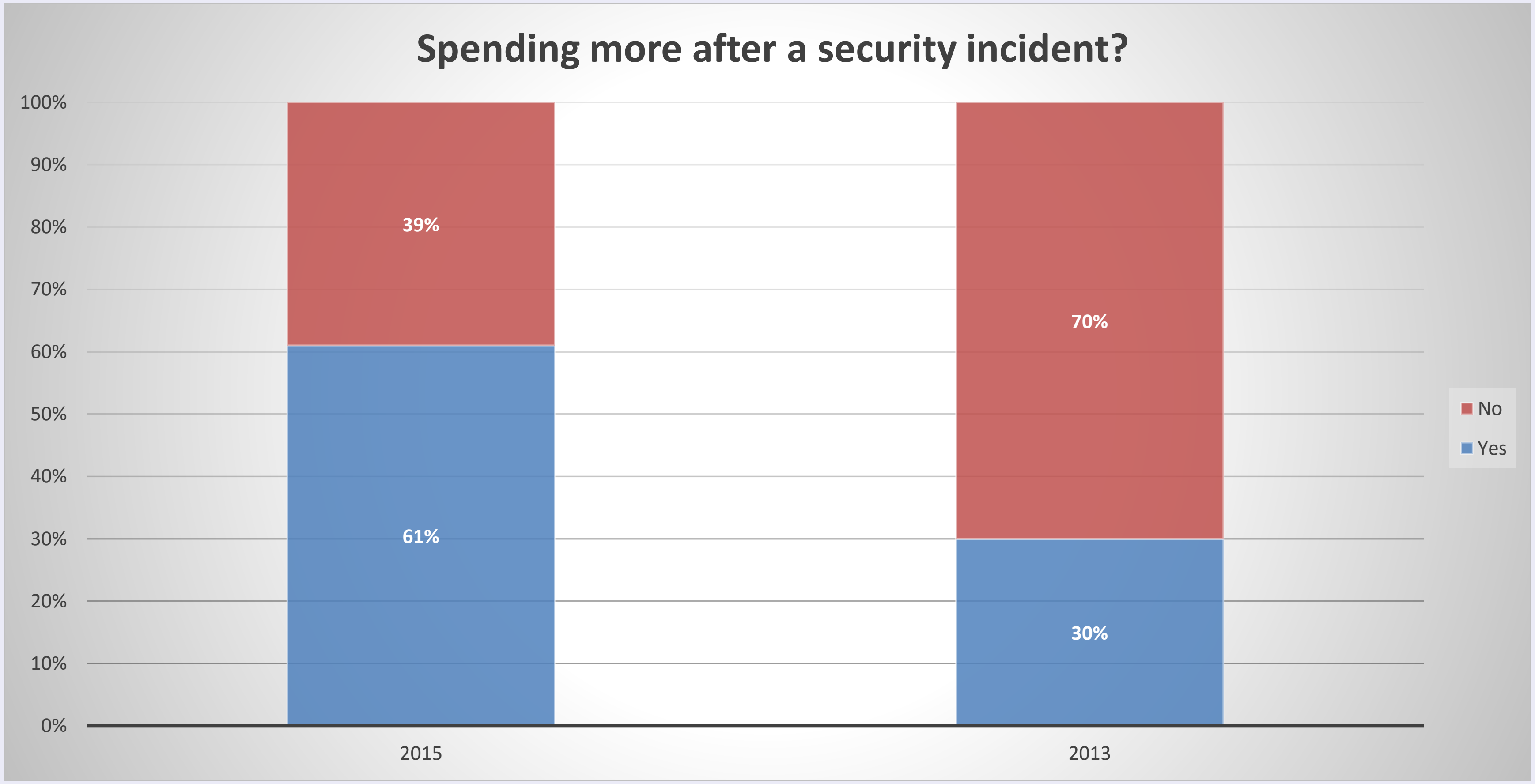
Incident Response (2)

OWASP 中国
The Open Web Application Security Project



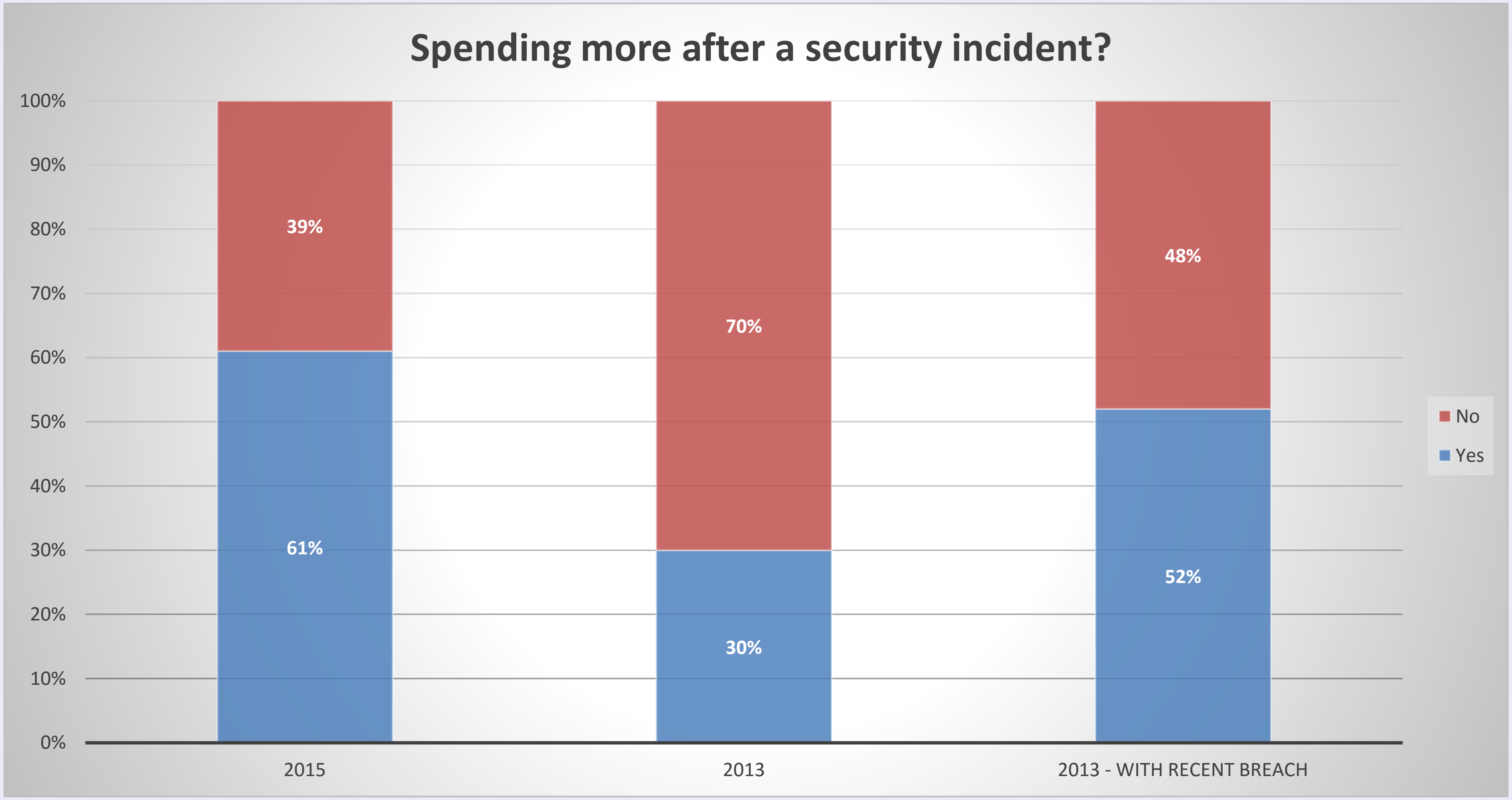
Incident Response: Increase spending after incident?

OWASP 中国
The Open Web Application Security Project



Incident Response: Increase spending after incident?

OWASP 中国
The Open Web Application Security Project



Thank you - Q&A

OWASP 中国
The Open Web Application Security Project

Questions & Answers

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

Thank you