DEVSECOPS UNPLUGGED

Why a Focus on Development and Operations Leaves a Massive Gap for Security

SecurityCompass

OUTLINE

1 Confluence of Events

2 Antipatterns

3 Industry Challenges

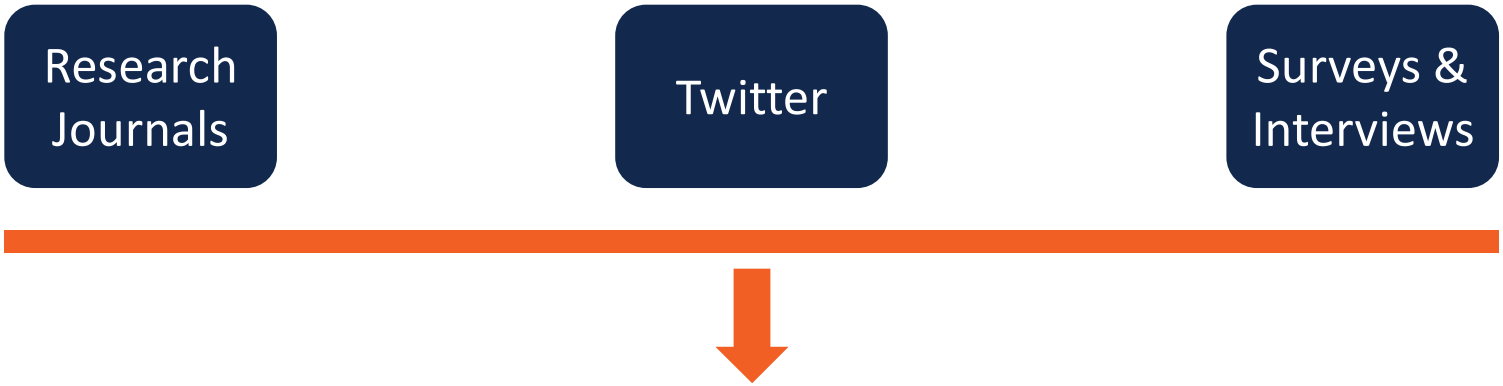
4 Role Challenges

5 Best Practices

6 Addressing the Collaboration Gap

7 Future Research

RESEARCH METHODOLOGY

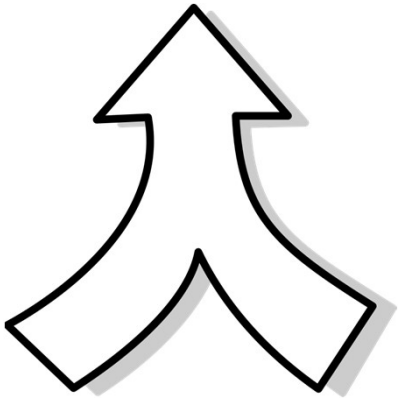


Research Questions

1. What do we know about current best practices in DevSecOps?
2. What do we know about antipatterns in DevSecOps?
3. What do we know is missing in the DevSecOps discussion?

CONFLUENCE OF EVENTS

1. The strict controls used previously haven't all migrated into the DevOps workflow.
   - Traditionally, we have used DevOps in failure tolerant systems.
   - DevOps is now being adopted in operating systems, routers, government communications, and critical infrastructure.
2. Traditional security is getting in the way of DevOps
   - Developers don't have access to production or SecOps data.
   - Security testing is too slow.
   - Pressure to release quickly leads to missed security reviews.



ANTIPATTERNS

- Use of immature automated deployment tools
- Incorrect metrics
- Lack of controlled collaboration
- Disregard for quality
- Lack of centralized coordination
- Poor communication
- Emphasis on speed of feature releases
- Lack of audit and control points
- Lack of security throughout the process
- Vulnerabilities in the deployment pipeline
- Lack of sufficient third party library testing

LEADERSHIP PRESSURE TO TRANSFORM

> “50% of the CIOs that have not transformed their capabilities will be displaced from the digital leadership team.”

Source: Gartner, 2016. “Gartner Predicts”, https://www.gartner.com/binaries/content/assets/events/keywords/infrastructure-operations-management/iome5/gartner-predicts-for-it-infrastructure-and-operations.pdf

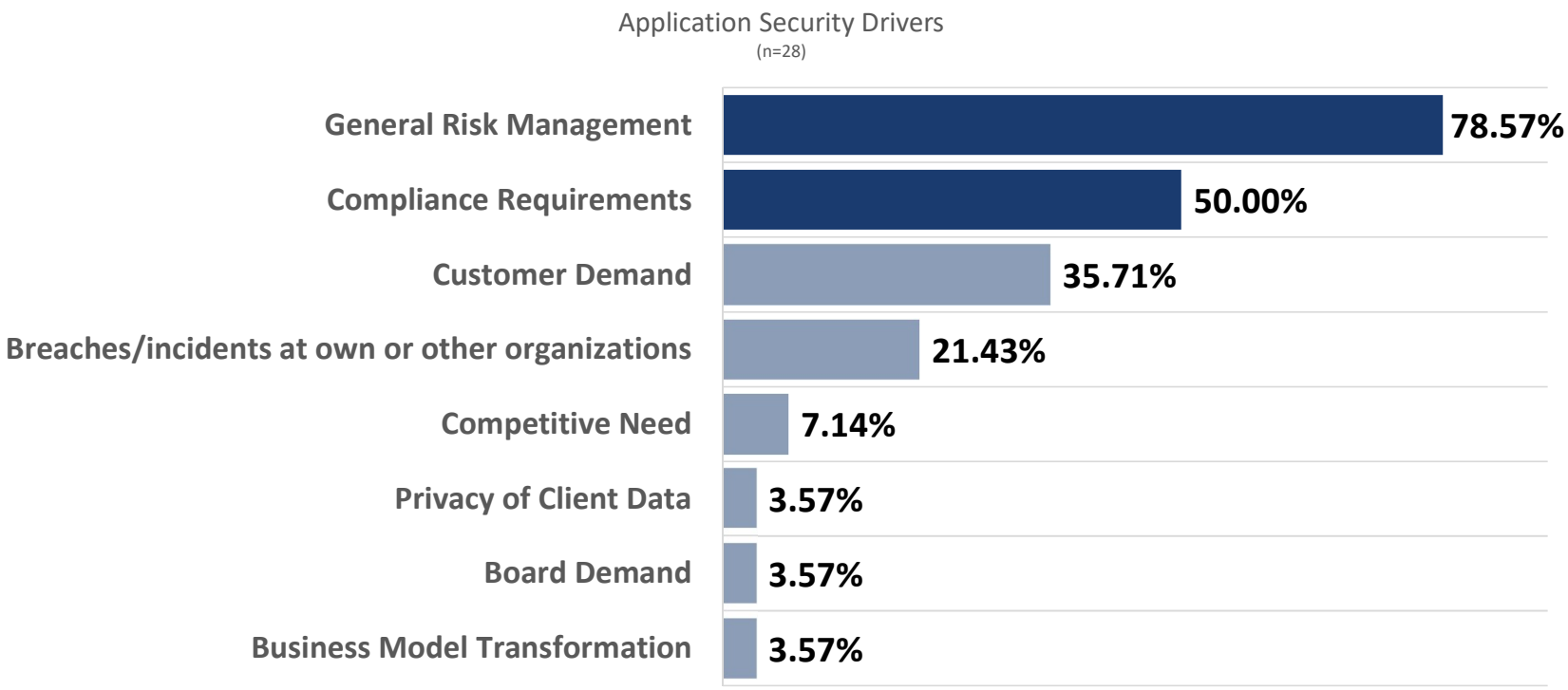
WHEN SOFTWARE IS EVERYWHERE…

- Telecommunications
  - Distributed Denial of Service
- Financial
  - Flash Crash
- Medical
  - Electrical Medical Record distribution
- Transportation
  - Logistics security
- Software
  - Malware

ROLE CHALLENGES (NO LONGER JUST A DEV AND OPS ISSUE)

- Business
  - Technical masquerading
- Project Manager
  - Justifying technical debt for poor practices
- Quality Assurance
  - Lack of proof for bug free software
- Customer
  - Don’t know what to ask for around security
- Developer
  - Best practices are insufficient

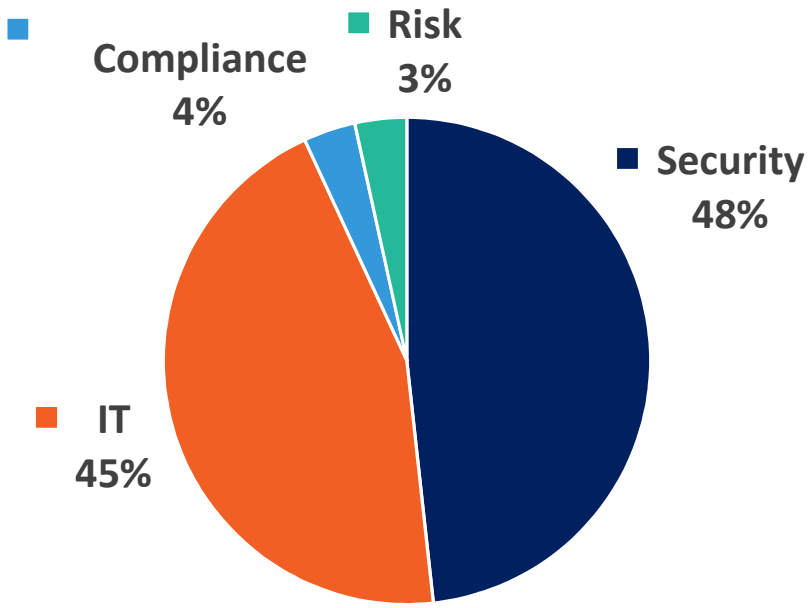
RISK AND COMPLIANCE



Source: “Managing Application Security”, Security Compass, 2017.

THE RISK AND COMPLIANCE GAP

Who is responsible for triggering the discussion on functional and non-functional requirements around software security?



n=29

Source: Security Compass, 2018. Attendee survey at SecureCISO conference.

BEST PRACTICES (YES, GAPS EXIST!)

	AUTOMATION	SECURITY	COMPLIANCE	RISK
REQUIREMENTS		• Security requirements analysis • Defining security policies		• Risk analysis • Continuous planning
DESIGN		• Data flow analysis • Untrusted boundaries		• Design review • Threat modeling • Supply chain
DEVELOP	• Automated code review • Input validation • Isolation of untrusted inputs • Code scanning • Continuous integration	• Developer training		
TEST	• Functional testing	• Penetration testing		• Compliance testing
DEPLOY	• Automated deployment • Software defined firewall • Automated performance monitoring • Continuous deployment • Continuous delivery • Integrated change management • Infrastructure as code	• Configuring security		
MAINTAIN	• Automated monitoring • Continuous monitoring • Rapidly fixing errors in production	• Short lived access • Explicit authorization		

WHERE IS RISK & COMPLIANCE IN THE DEVOPS DISCUSSION?

Source: Twitter search using #DevOps over a 7 day period ending 2018-02-22 11:06 AM.

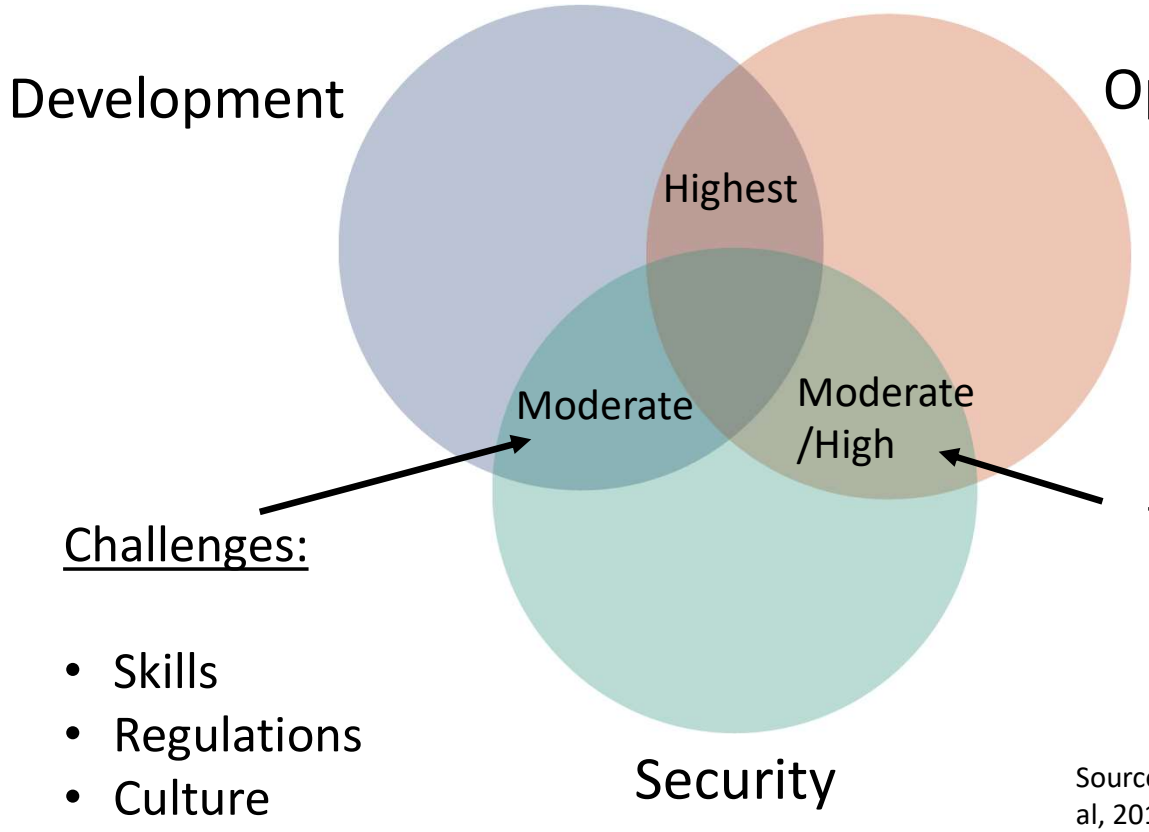
WHERE IS RISK & COMPLIANCE IN THE DEVSECOPS DISCUSSION?

Source: Twitter search using #DevSecOps over a 7 day period ending 2018-02-19 11:24 AM.

WHERE IS DEVSECOPS IN THE RISK & COMPLIANCE DISCUSSION?

Source: Twitter search using #GRC over a 7 day period ending 2018-02-22 1:45 PM.

COLLABORATION



Challenges:

- Skills
- Regulations
- Culture

Challenges:

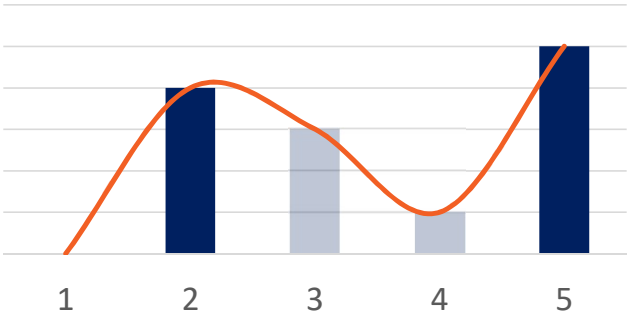
- Data volume
- Analytics

Source: Adopted in part from Akond Ashfaque Ur Rahman et al, 2016. “Security Practices in DevOps”.

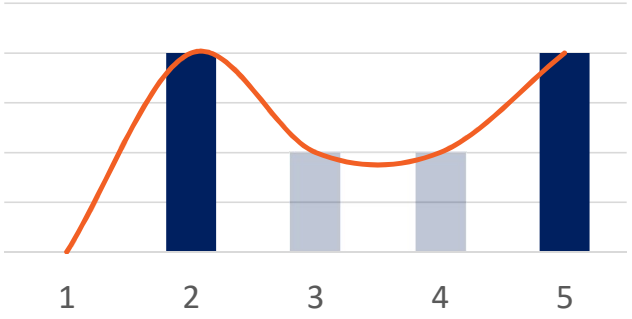
THE MYTH THAT ALL DEVELOPERS KNOW ABOUT SECURITY

How broad is the adoption of developer security awareness training at your organization?

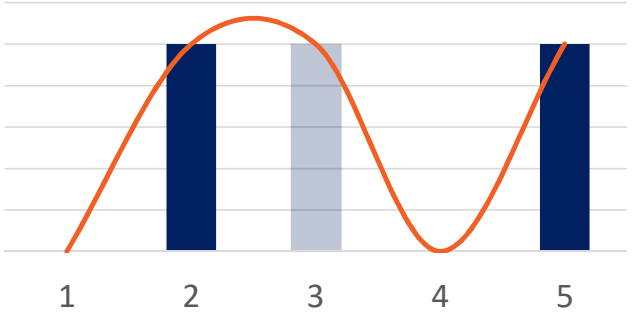
Finance
(n=13)



ISV
(n=6)



Energy/Utility
(n=3)

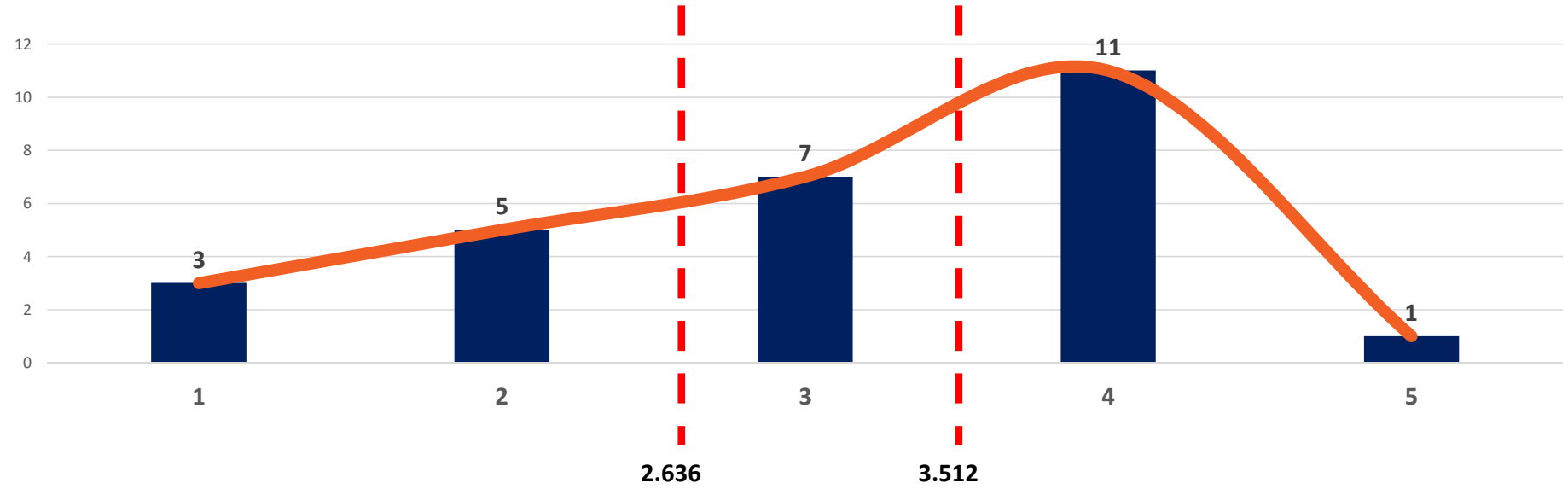


RESPONSE RANGE: 1 = NO TRAINING TO 5 = ALL DEVELOPERS ARE TRAINED

Source: “Managing Application Security”, Security Compass, 2017.

CYBERSECURITY RISK

On a scale from 1 to 5 how confident are you in measuring your cyber-security risk across your business environment

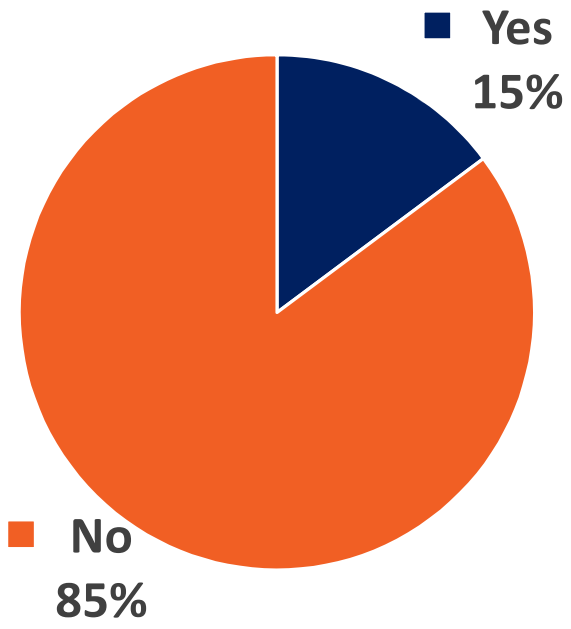


n=27

Source: Security Compass, 2018. Attendee survey at SecureCISO conference.

THE RISK GAP

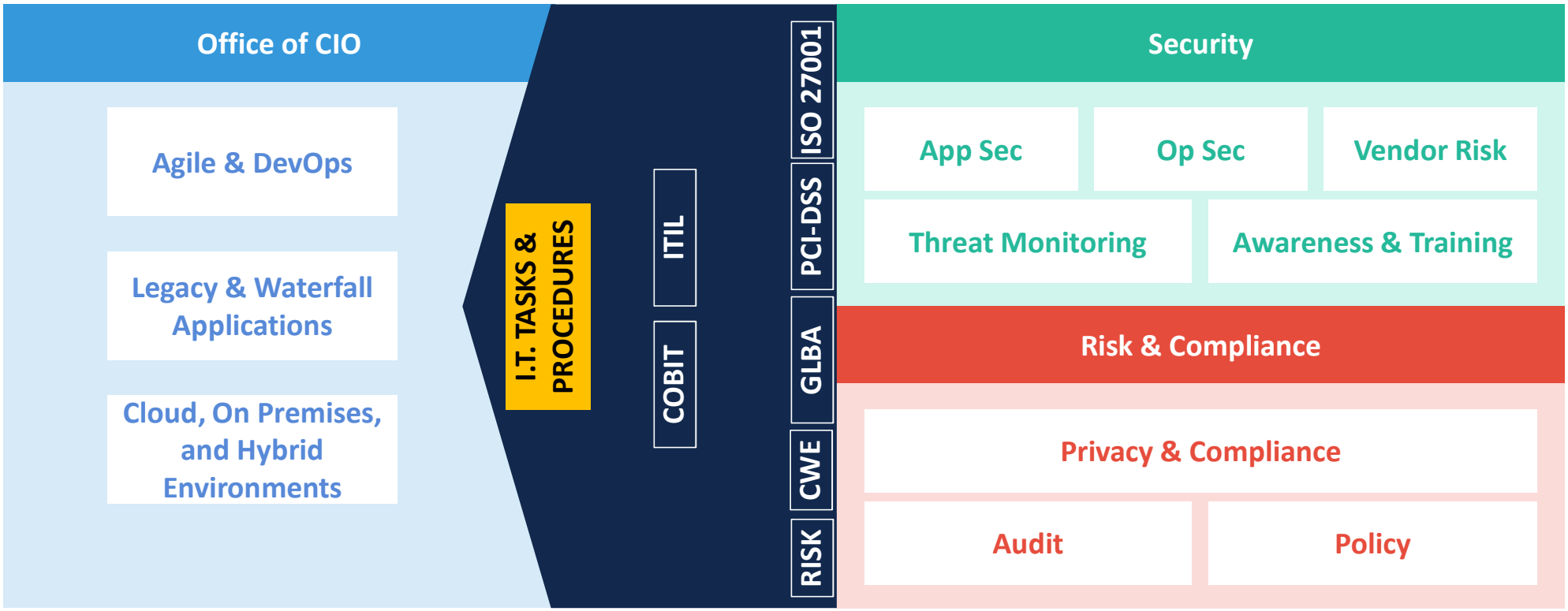
Are you 100% confident in your current cybersecurity posture?



n=27

Source: Security Compass, 2018. Attendee survey at SecureCISO conference.

ADDRESSING THE COLLABORATION GAP



ADDRESSING THE COLLABORATION GAP

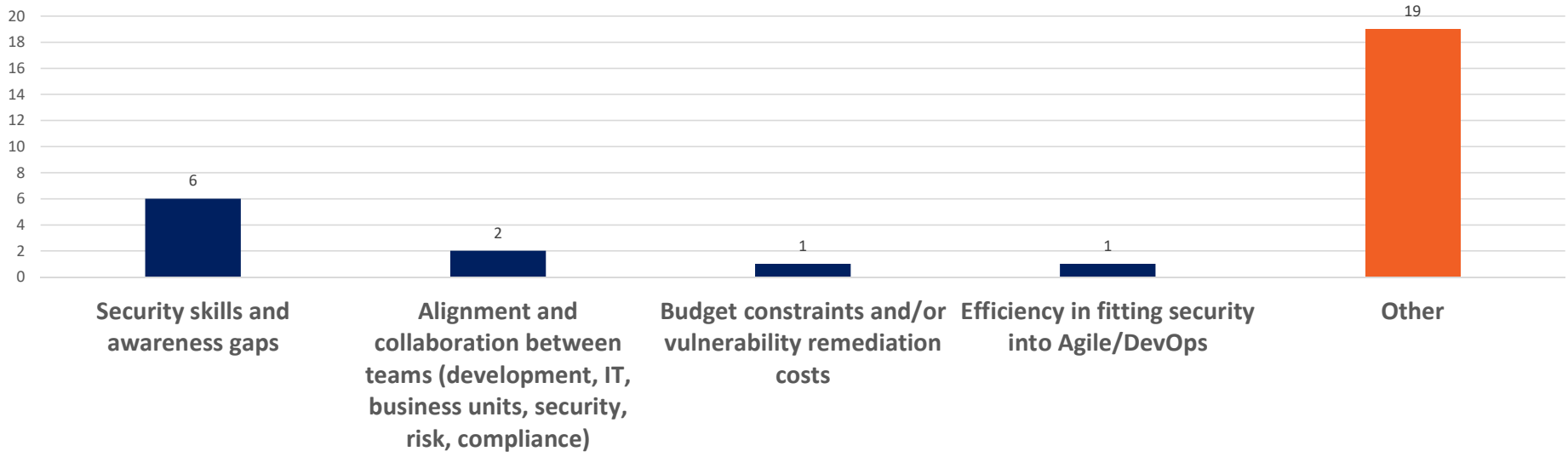
CASE STUDY: PAYPAL

Source: https://www.youtube.com/watch?v=_rFVui0dWnI

- Agile transformation to over 400 scrum teams across the world
- Seamless plugin to quarterly release plan
- Less than 15 minutes for product developer to complete survey
- Usage of dynamic / in-context security requirements (security stories) along with other controls in the continuous integration pipeline
- Wide adoption across product development organization
- Automated dashboard makes metrics transparent to product development leadership

FUTURE RESEARCH

- What are the top challenges that you face with your application security program?



n=29

Source: Security Compass, 2018. Attendee survey at SecureCISO conference.

- How are organizations addressing the Policy to Procedure gap?

SOURCES

- Akond Ashfaque Ur Rahman et al, 2016. “Software Security in DevOps: Synthesizing Practitioner Perceptions and Practices”.
- Akond Ashfaque Ur Rahman et al, 2016. “Security Practices in DevOps”.
- Don O’Neill, 2017. “In Search of a Modern Software Life Cycle – Secure DevOps Foundations for Large-Scale Software Systems”.
- Gartner, 2016. “Gartner Predicts”, https://www.gartner.com/binaries/content/assets/events/keywords/infrastructure-operations-management/iome5/gartner-predicts-for-it-infrastructure-and-operations.pdf
- John Michener et al, 2016. “Mitigating an Oxymoron: Compliance in a DevOps environment”.
- Len Bass, 2018. “The Software Architect and DevOps”.
- Nicole Forsgren et al, 2017. “DevOps Metrics”.
- Ramtin Jabbari et al, 2016. “What is DevOps? A Systematic Mapping Study on Definitions and Practices”.
- Security Compass, 2017. “Managing Application Security Survey”.
- Security Compass, 2018. Attendee survey at SecureCISO conference.
- Theo Schlossnagle, 2017. “Monitoring in a DevOps World”.
- Twitter, 2018. Various #DevOps, #DevSecOps, #GRC.
- Vishnavi Mohan et al, 2016. “SecDevOps: Is It a Marketing Buzzword?”.

THANK YOU

EMAIL US AT:
info@securitycompass.com

SIGN UP TO TAKE OUR FREE COURSE ON SECURITY WITH AGILITY:
https://www.securitycompass.com/devsecops

JOIN THE DEVSECOPS DISCUSSION:
https://www.linkedin.com/groups/13551214

Security Compass