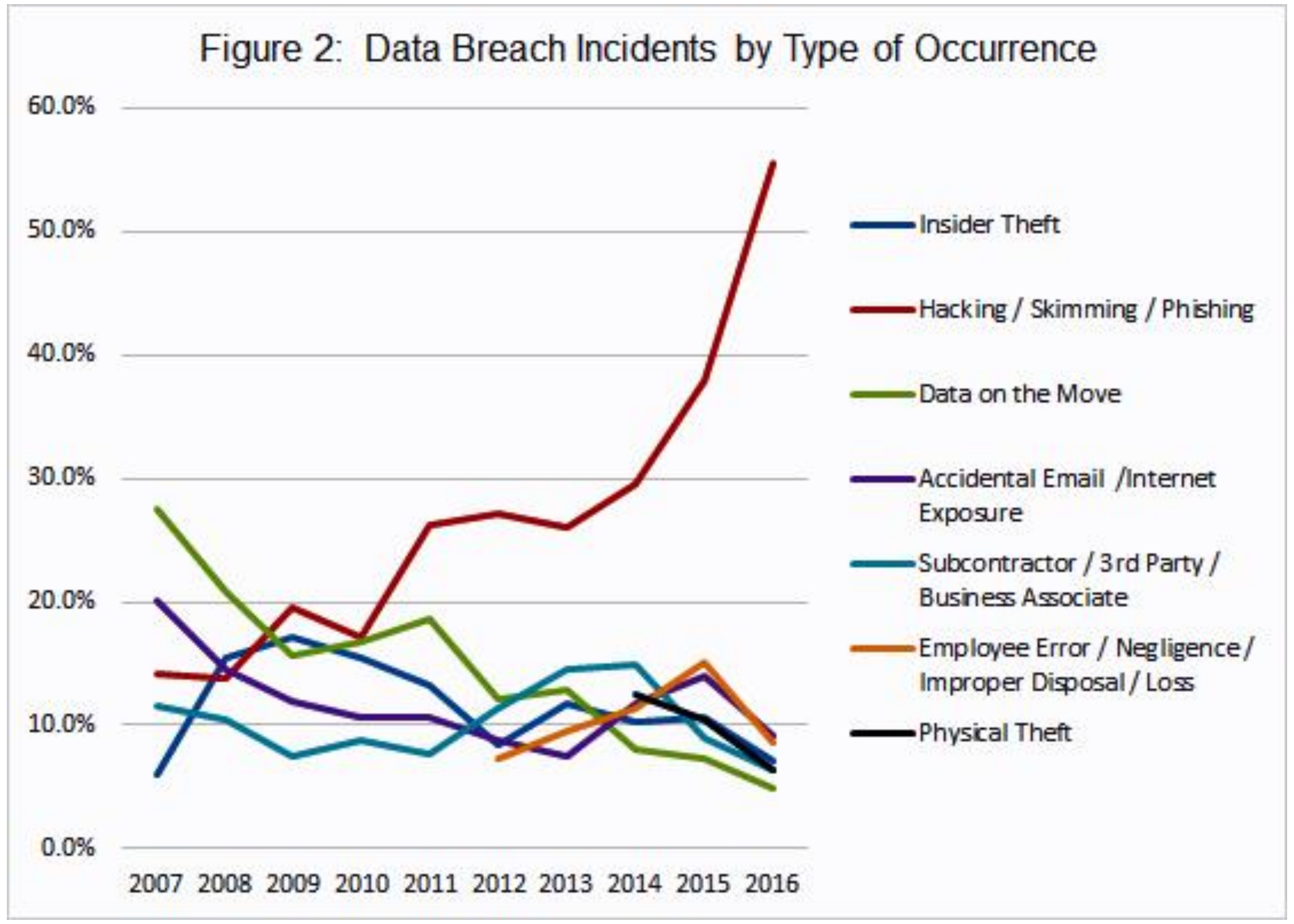
Metrics for Justifying SOC Investment to the CEO and Board

John Pescatore
Director, SANS Institute
jpescatore@sans.org

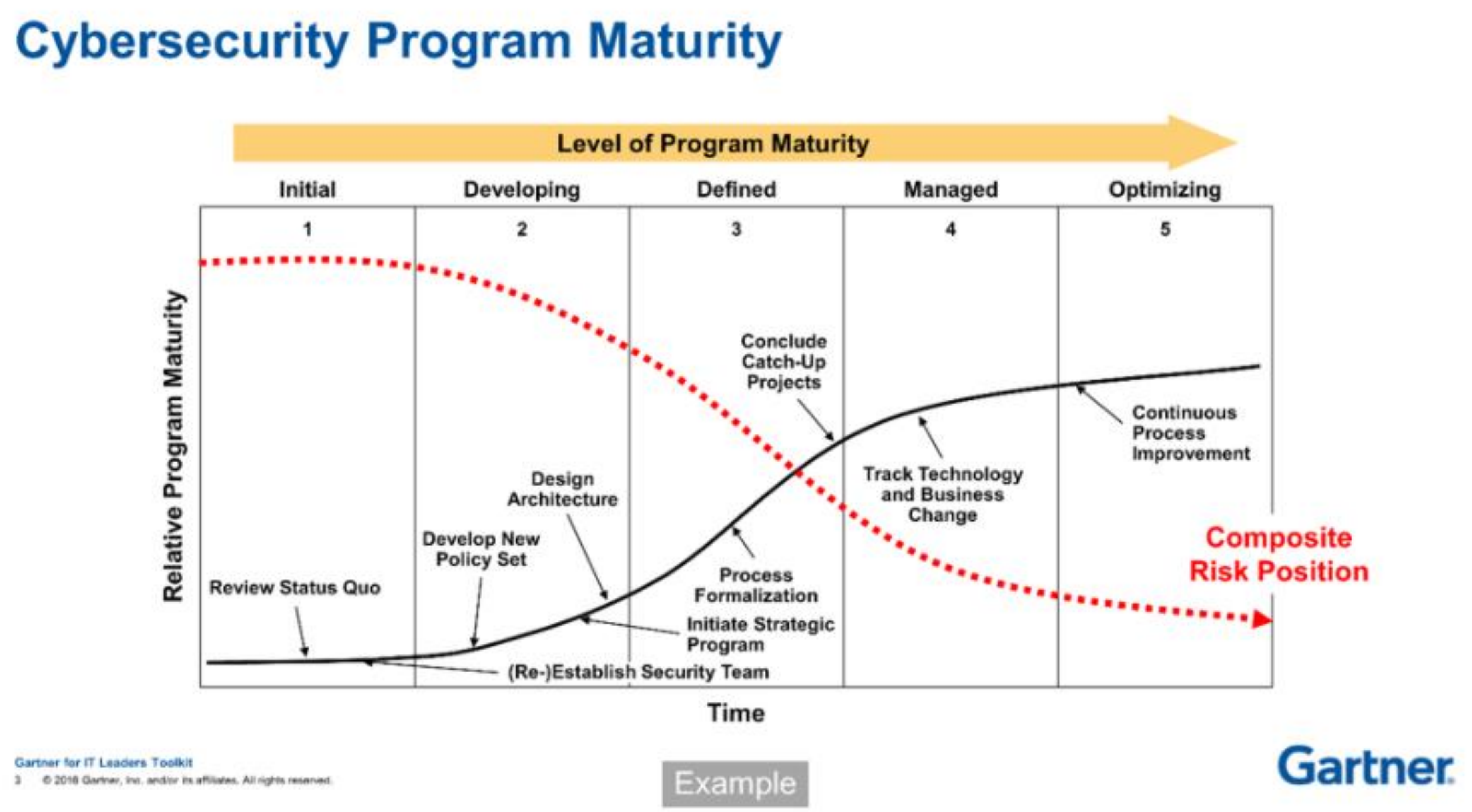
Why Do Some Do Better Than Others?

- 980 breaches in 2016
  - What did the other 9,020 of the F10000 do differently?
  - (781 in 2015)
- On average, 36K records exposed per breach
  - What did those who limited breach size do differently?
  - (Average = 215K in 2015)
- **Almost invariably, the organizations with the least cyber incident impact have the strongest security teams and processes.**



Source: Identity Theft Resource Center

Basic Security Hygiene and a Strong SOC as Foundation

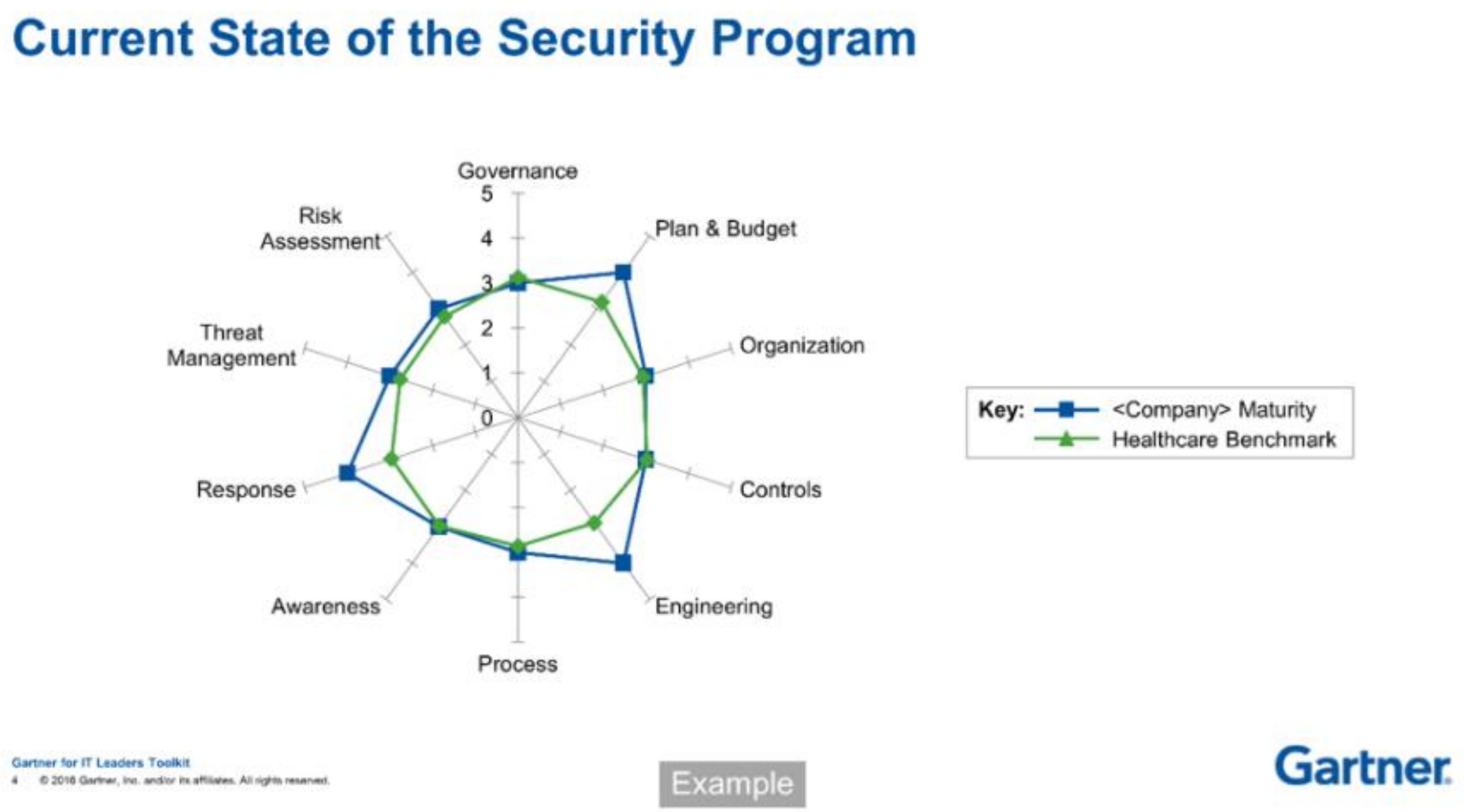


Cybersecurity Program Maturity

Gartner for IT Leaders Toolkit
3 © 2016 Gartner, Inc. and/or its affiliates. All rights reserved.

Example

Gartner.



Current State of the Security Program

Gartner for IT Leaders Toolkit
4 © 2016 Gartner, Inc. and/or its affiliates. All rights reserved.

Example

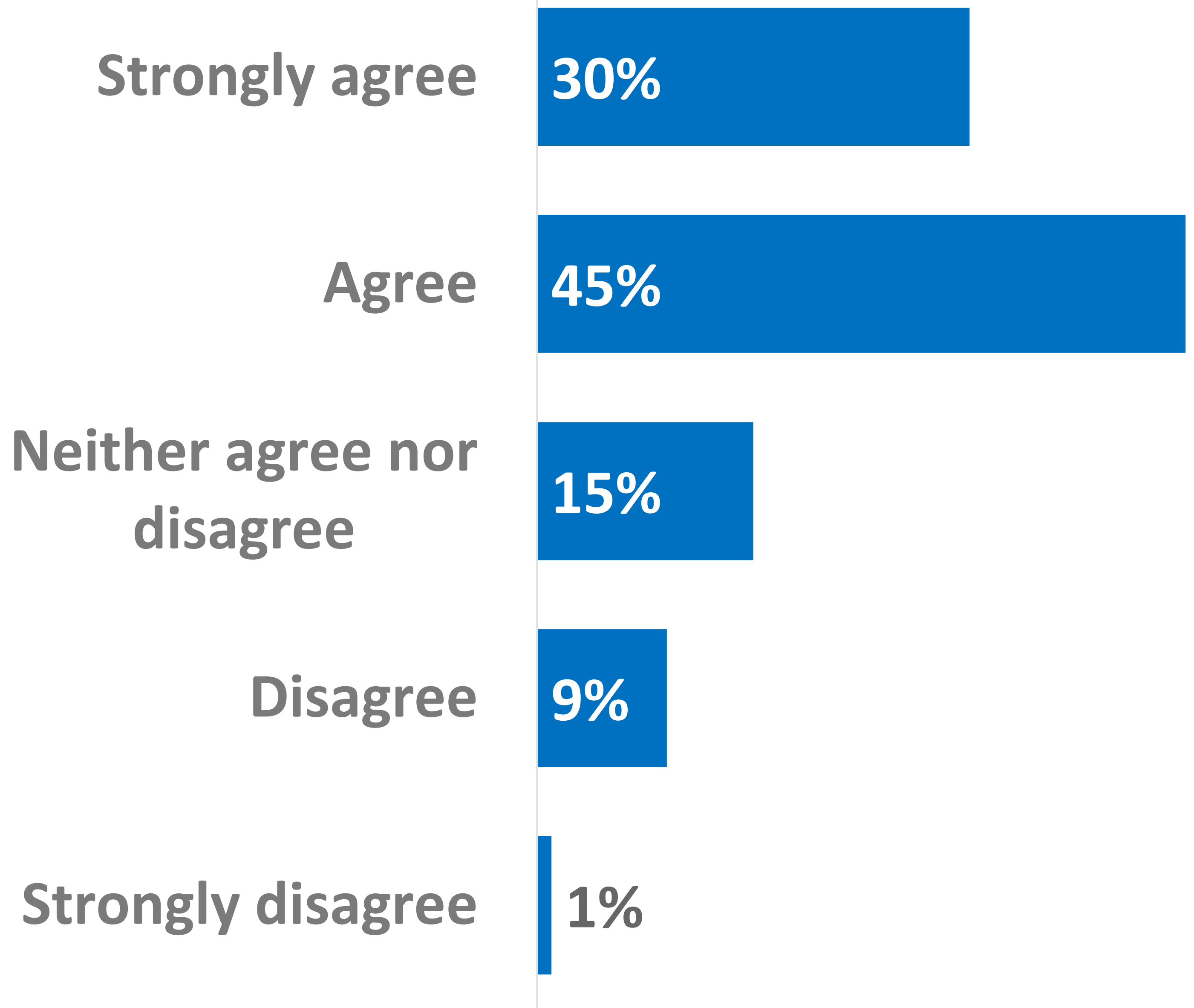
Gartner.

- Mature = Effective and efficient
- Key indicators:
  - **Basic security hygiene**
  - **Security Operations Center processes and tools**
  - “Business Security Analysts”
  - Integration into procurement, M&A, supply chain decisions
  - Cross-industry participation

Communicating to the C-Suite and Board of Directors

- We mostly know **what** to do in security, and we can learn **how** to do **our** part.
- The biggest obstacle to success is getting **others** to do **their** part.
- Support from **above** is the most powerful force to break through.
- **Goal: Learn how to inform CEOs and Boards and convince them to back SOC strategies to *drive change and provide measurable improvements in cybersecurity.***

Would you say your company's Board of Directors has taken an active interest in cybersecurity issues?



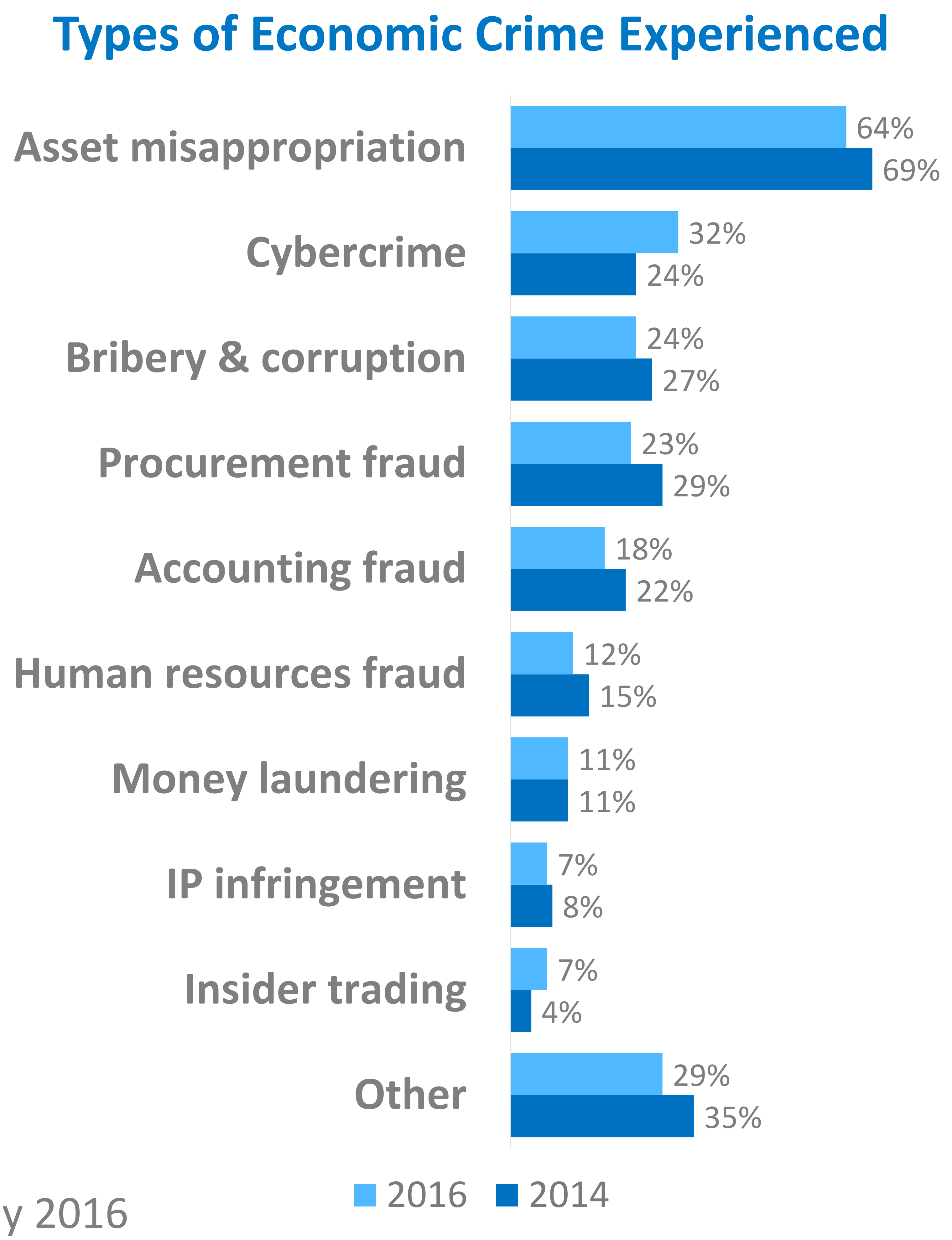
Source: PaloAlto Networks

The Messages Back from Directors

- “**Security people don’t speak our language**. In fact, at each briefing they seem to speak a different language.”
- “The CISO is great at talking about ‘blood in the streets’ but **very weak on strategy to avoid disasters.**”
- “We know bad things will happen – the CEO and CFO and VPs inform us of business problems frequently. **We want to have confidence that basic competence and strategies are in place to reduce bottom line impact**.”
- “The Board is not an ATM – **we are not here to give you resources**.”
- “A big part of **being believable and building our trust** is showing us how we compare to competitors, other industries, some kind of standards or benchmarks.”

Data Vs. More Horror Stories

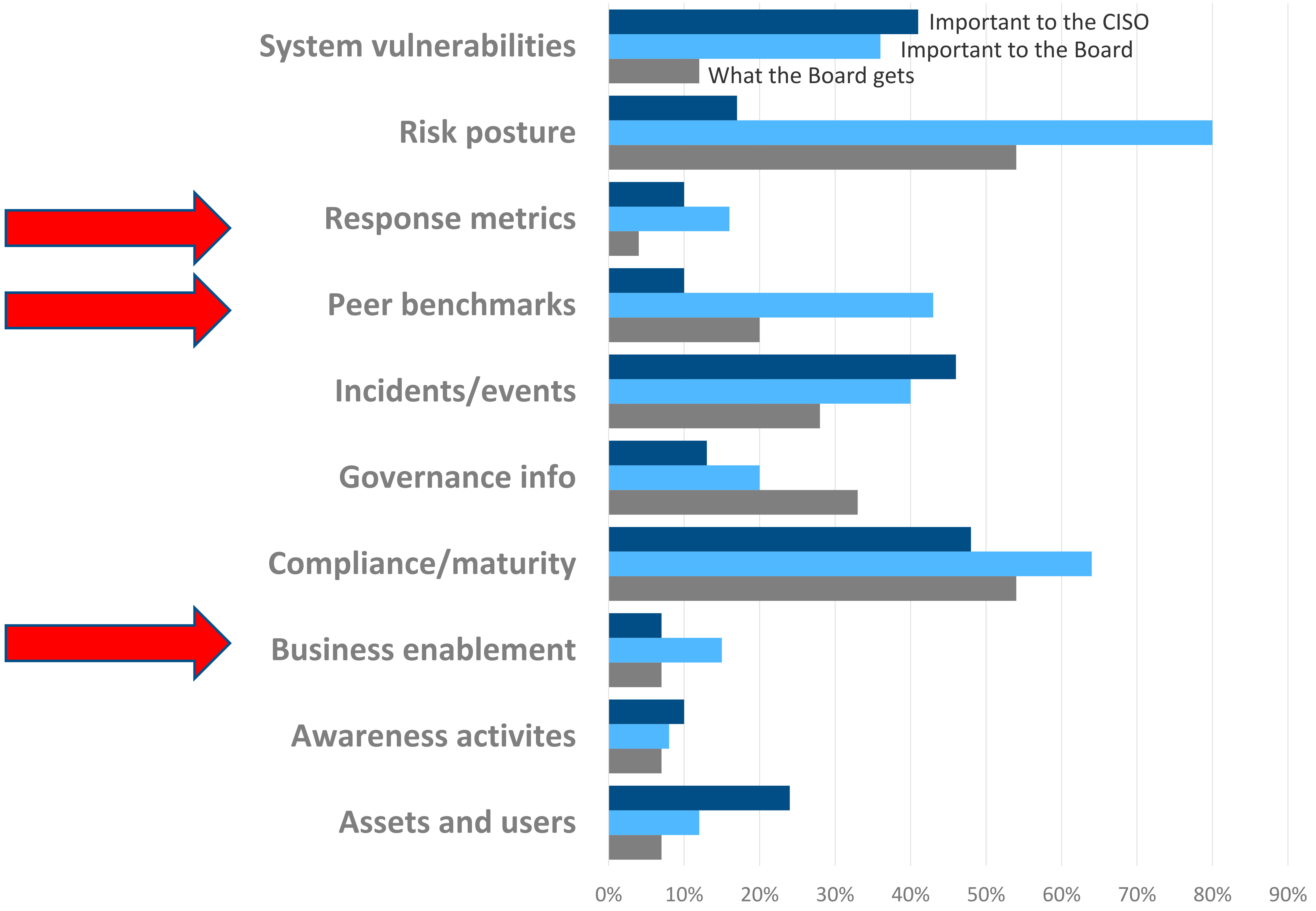
- Cybercrime impact is growing faster than most other forms of crime and fraud:
  - Identity theft for new account fraud
  - “Ransomware” – hold information hostage
  - Denial of service – hold Internet connection hostage
  - Industrial espionage
- The vast majority of asset misappropriation (insider threats) are enabled by IT vulnerabilities.
- Cybercrime attack techniques are often adopted by nation states.



Source: PWC Global Economic Crime Survey 2016

SOC Data to Close the Gap

What metrics do CISOs rely on most? What’s reported to the Board? Which do Board members value most?



Source: Focal Point 2017

Delivering Security Efficiency and Effectiveness

Efficiency

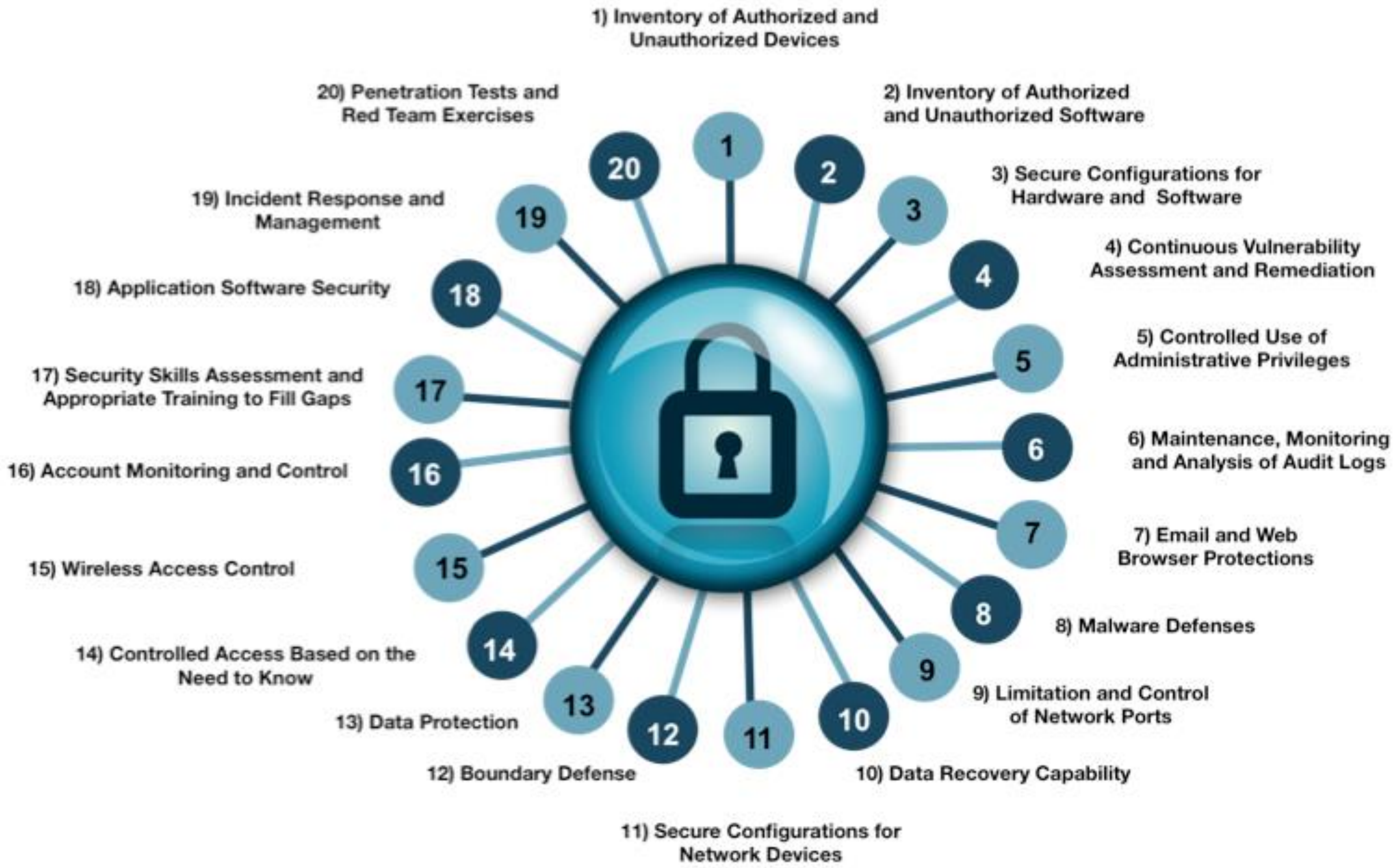
- Decrease the cost of dealing with known threats
- Decrease the impact of residual risks
- Decrease the cost of demonstrating compliance
- Reduce business damage due to security failures
- Maintaining level of protection with less EBITDA impact

Effectiveness

- Increase the speed of dealing with a new threat or technology
- Decrease the time required to secure a new business application, partner, supplier
- Reducing incident cost
- Less down time
- Fewer customer defections
- Security as a competitive business factor

Cybersecurity Frameworks

Center for Internet Security Critical Security Controls



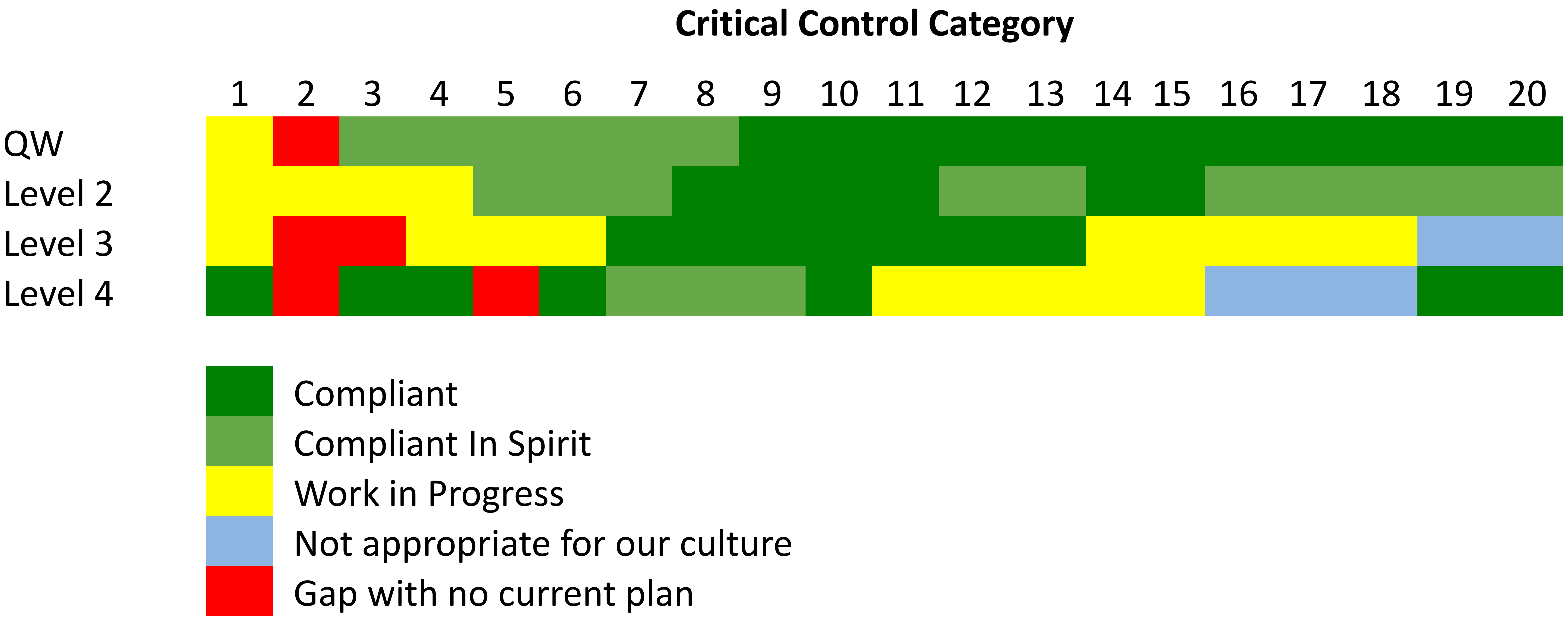
1) Inventory of Authorized and Unauthorized Devices
2) Inventory of Authorized and Unauthorized Software
3) Secure Configurations for Hardware and Software
4) Continuous Vulnerability Assessment and Remediation
5) Controlled Use of Administrative Privileges
6) Maintenance, Monitoring and Analysis of Audit Logs
7) Email and Web Browser Protections
8) Malware Defenses
9) Limitation and Control of Network Ports
10) Data Recovery Capability
11) Secure Configurations for Network Devices
12) Boundary Defense
13) Data Protection
14) Controlled Access Based on the Need to Know
15) Wireless Access Control
16) Account Monitoring and Control
17) Security Skills Assessment and Appropriate Training to Fill Gaps
18) Application Software Security
19) Incident Response and Management
20) Penetration Tests and Red Team Exercises

Frameworks:

- **Critical Security Controls**
- NIST Cybersecurity Framework
- ISO 27001
- Industry-specific
  - HIPAA
  - Retail
  - NERC

Power Utility Example

Continuous gap analysis vs. the Critical Security Controls



Critical Control Category

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
QW	🟨	🟥	▨	▨	▨	▨	▨	▨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Level 2	🟨	🟨	🟨	🟨	▨	▨	▨	🟩	🟩	🟩	🟩	▨	▨	🟩	🟩	▨	▨	▨	▨	▨
Level 3	🟨	🟥	🟥	🟨	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟦	🟦
Level 4	🟩	🟥	🟩	🟩	🟥	🟩	▨	▨	▨	🟩	🟨	🟨	🟨	🟨	🟨	🟦	🟦	🟦	🟩	🟩

🟩 Compliant

▨ Compliant In Spirit

🟨 Work in Progress

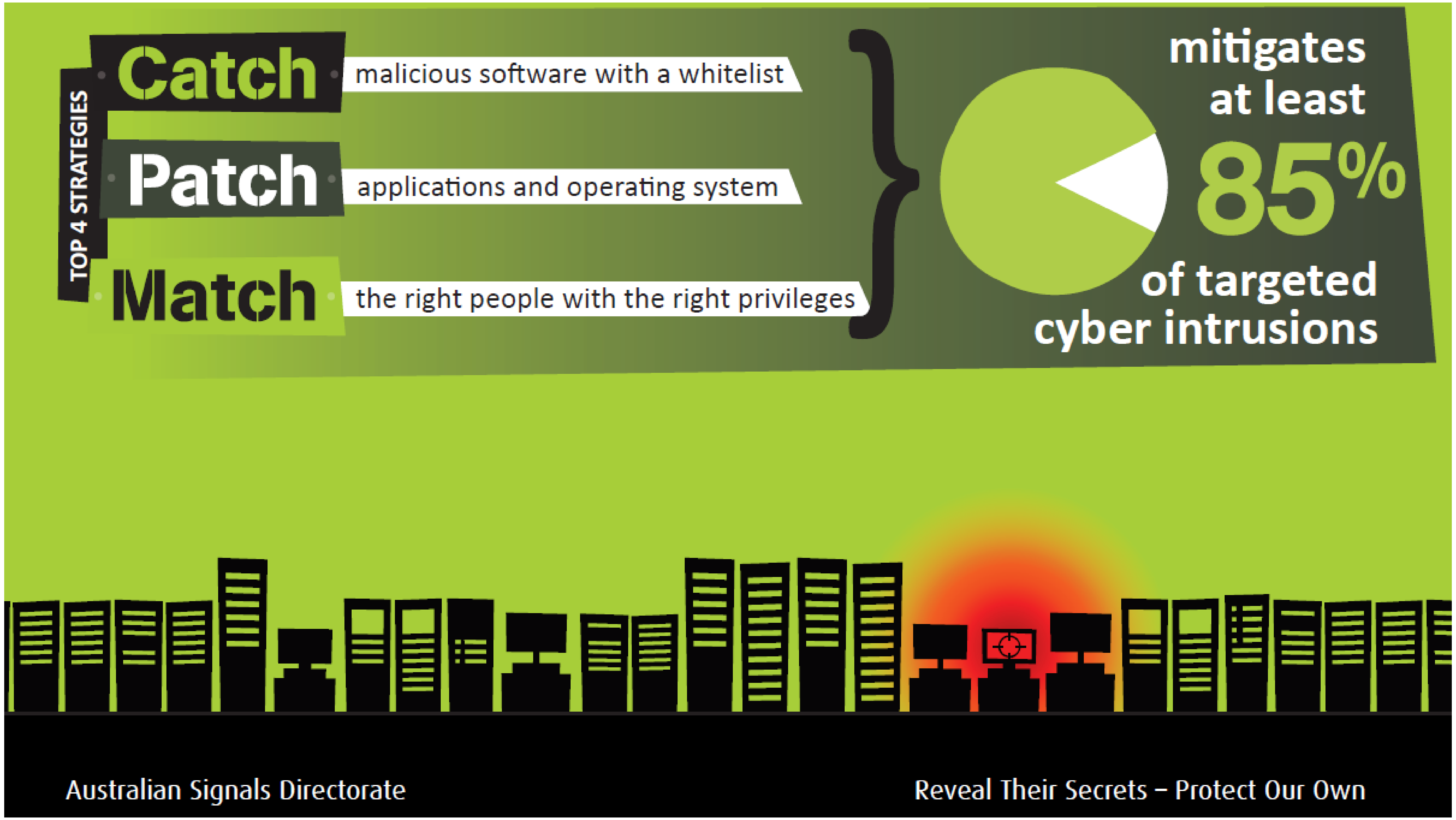
🟦 Not appropriate for our culture

🟥 Gap with no current plan

Plus: Continuous:

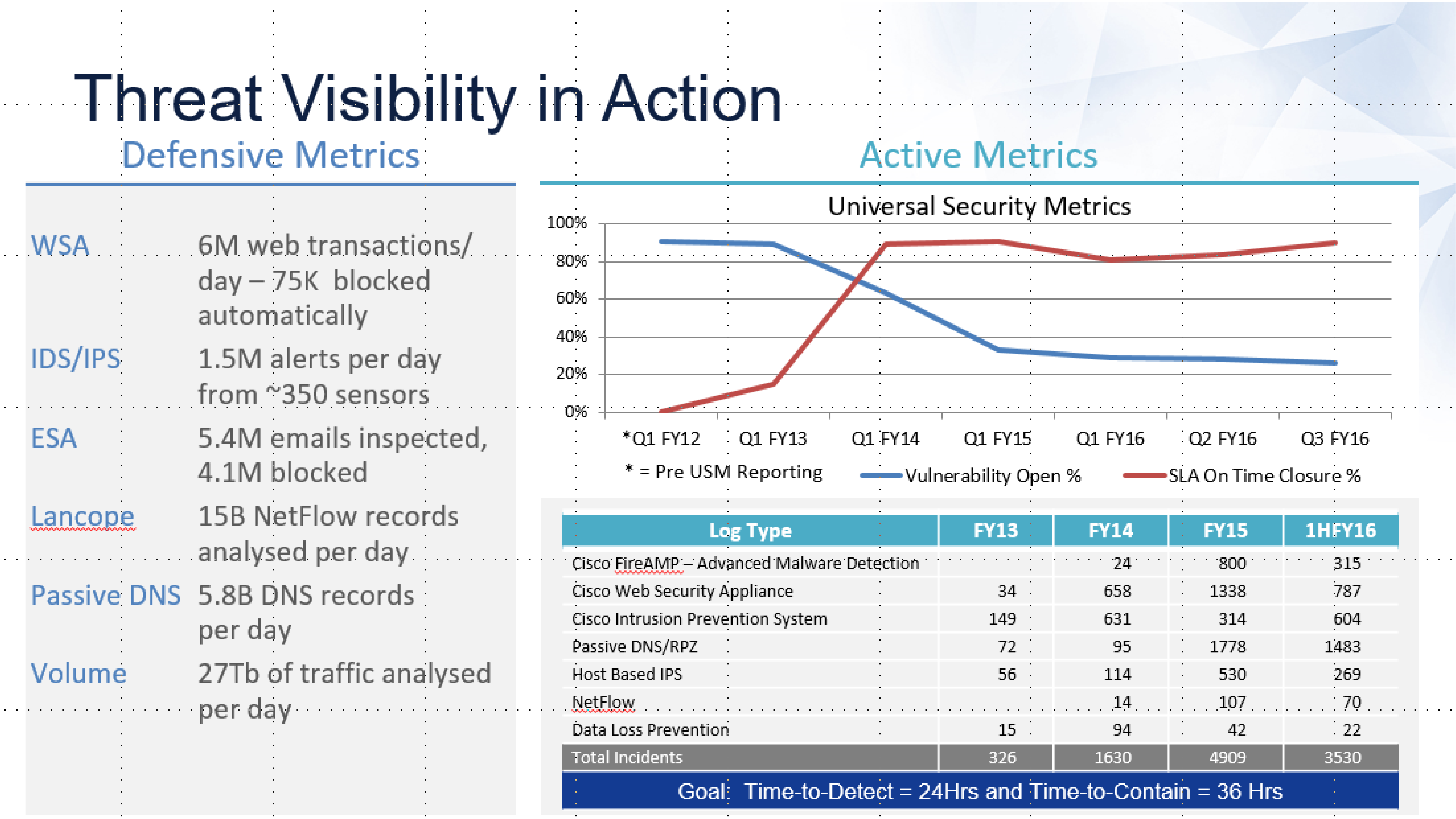
1) "Mean time to Detect Incidents" and "Mean time to Contain Incidents"
2) 4 key automated vulnerability metrics

Basic Security Hygiene ROI Example



TOP 4 STRATEGIES
Catch malicious software with a whitelist
Patch applications and operating system
Match the right people with the right privileges
mitigates at least 85% of targeted cyber intrusions
Australian Signals Directorate
Reveal Their Secrets – Protect Our Own

Steve Martino, VP InfoSec, Cisco



Threat Visibility in Action

Defensive Metrics

WSA	6M web transactions/ day – 75K blocked automatically
IDS/IPS	1.5M alerts per day from ~350 sensors
ESA	5.4M emails inspected, 4.1M blocked
Lancope	15B NetFlow records analysed per day
Passive DNS	5.8B DNS records per day
Volume	27Tb of traffic analysed per day

Active Metrics

Universal Security Metrics

* = Pre USM Reporting

Log Type	FY13	FY14	FY15	1HFY16
Cisco FireAMP – Advanced Malware Detection		24	800	315
Cisco Web Security Appliance	34	658	1338	787
Cisco Intrusion Prevention System	149	631	314	604
Passive DNS/RPZ	72	95	1778	1483
Host Based IPS	56	114	530	269
NetFlow		14	107	70
Data Loss Prevention	15	94	42	22
Total Incidents	326	1630	4909	3530

Goal: Time-to-Detect = 24Hrs and Time-to-Contain = 36 Hrs

Summary

- Mature SOC processes are critical to control risk, **limit business damage and customer impact** – need to **demonstrate**
- Response and recovery effectiveness and efficiency metrics are key to monitor and show improvement – **against business critical functions**.
- Board of Directors can play a role in assessing if cybersecurity in overcoming strategic obstacles – but **you need to get to basic security hygiene first**.
- The C-suite is where the first 80% of the battle will be won – **find a friend**.
- Show how investments in the SOC act as **force multipliers.**
- Be realistically about out-sourcing vs. all DIY>