The changing cybersecurity landscape for employee benefit plans

June 7th 2016

James Fox
Partner (Principal)
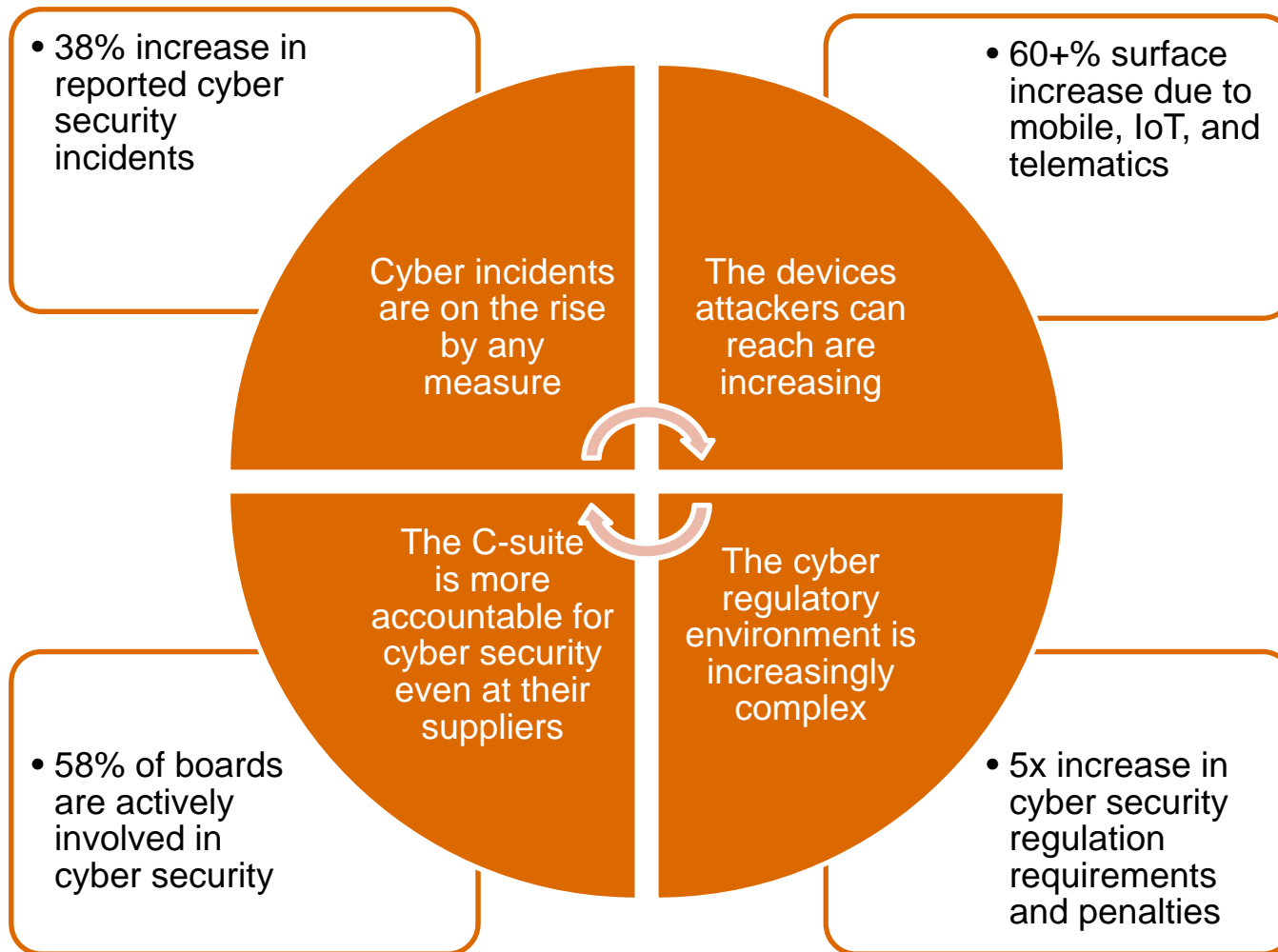PricewaterhouseCoopers

pwc

Todays Discussion

Cybersecurity in a perfect storm

The potential cost of ineffective cybersecurity

Three steps to improve cybersecurity posture

# *The cybersecurity perfect storm*

- 38% increase in reported cyber security incidents

- 60+% surface increase due to mobile, IoT, and telematics

Cyber incidents are on the rise by any measure

The devices attackers can reach are increasing

The C-suite is more accountable for cyber security even at their suppliers

The cyber regulatory environment is increasingly complex

- 58% of boards are actively involved in cyber security

- 5x increase in cyber security regulation requirements and penalties

Source PwC 2016 Global cyber Security Survey

PwC

3

Benefit plans' network business model can increase cyber exposure

Benefit Plan Operational Ecosystem
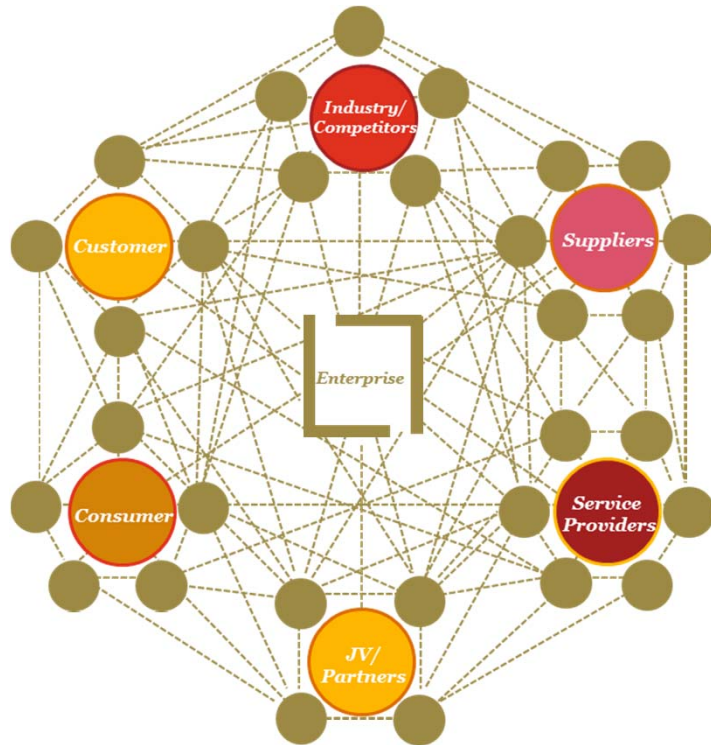
Plan Sponsors typically service benefit plans internally and through the use of third party service providers. Although this increases efficiency, the cyber risks need to be understood and managed.

Plans may use a network of different service providers

The ecosystem is **built around a model of open collaboration and trust.**

Smaller plans may be more dependent upon 3rd parties and infrastructure they do not own

As a Result

Adversaries are actively targeting critical assets throughout the ecosystem—significantly increasing the exposure and impact to businesses.
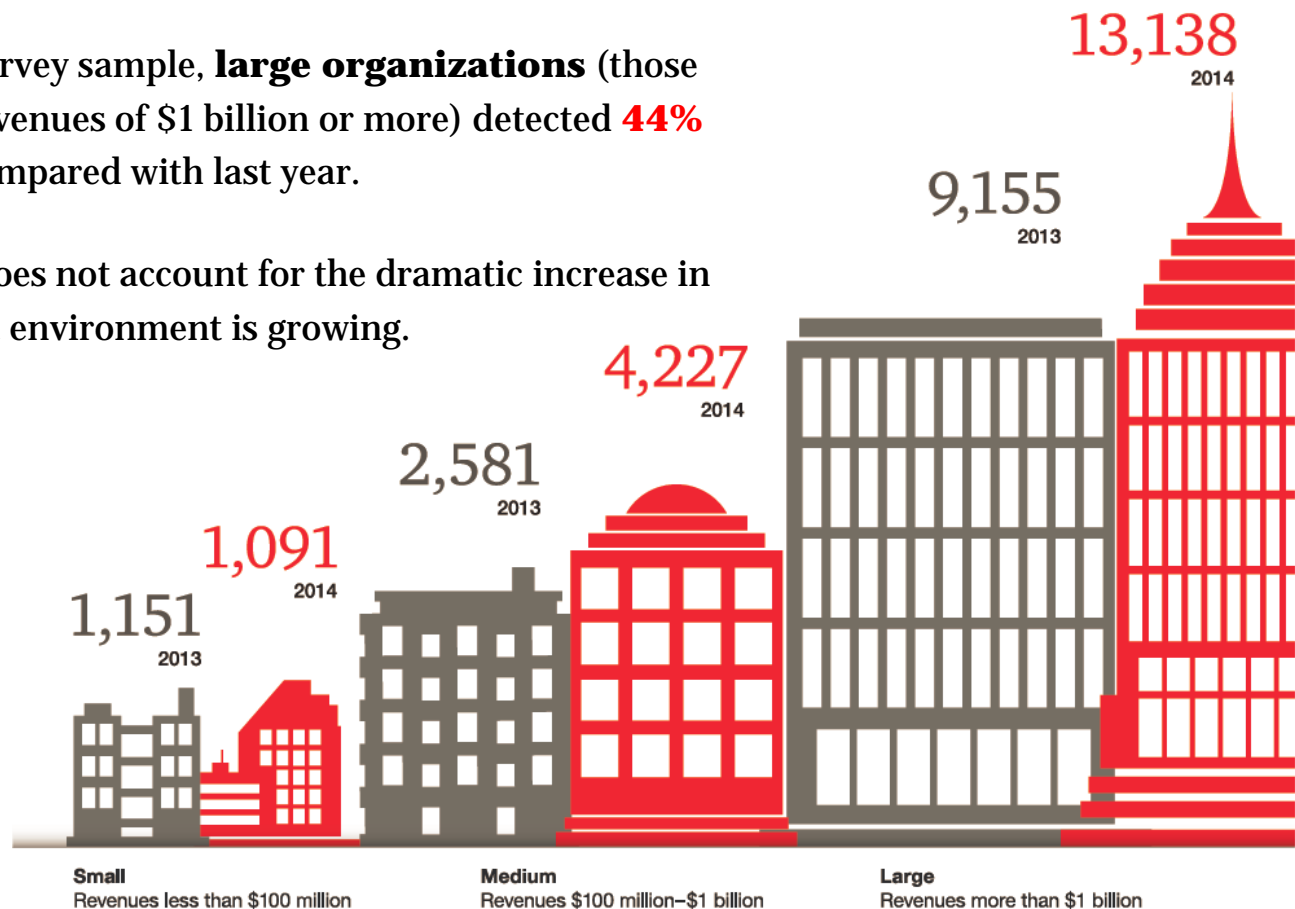
The number of incidents is on the rise...

Organizations reported a dramatic increase in the number of reported incidents Year on Year.

Among our global survey sample, **large organizations** (those with gross annual revenues of $1 billion or more) detected **44% more incidents** compared with last year.

Measurement bias does not account for the dramatic increase in incidents. The threat environment is growing.
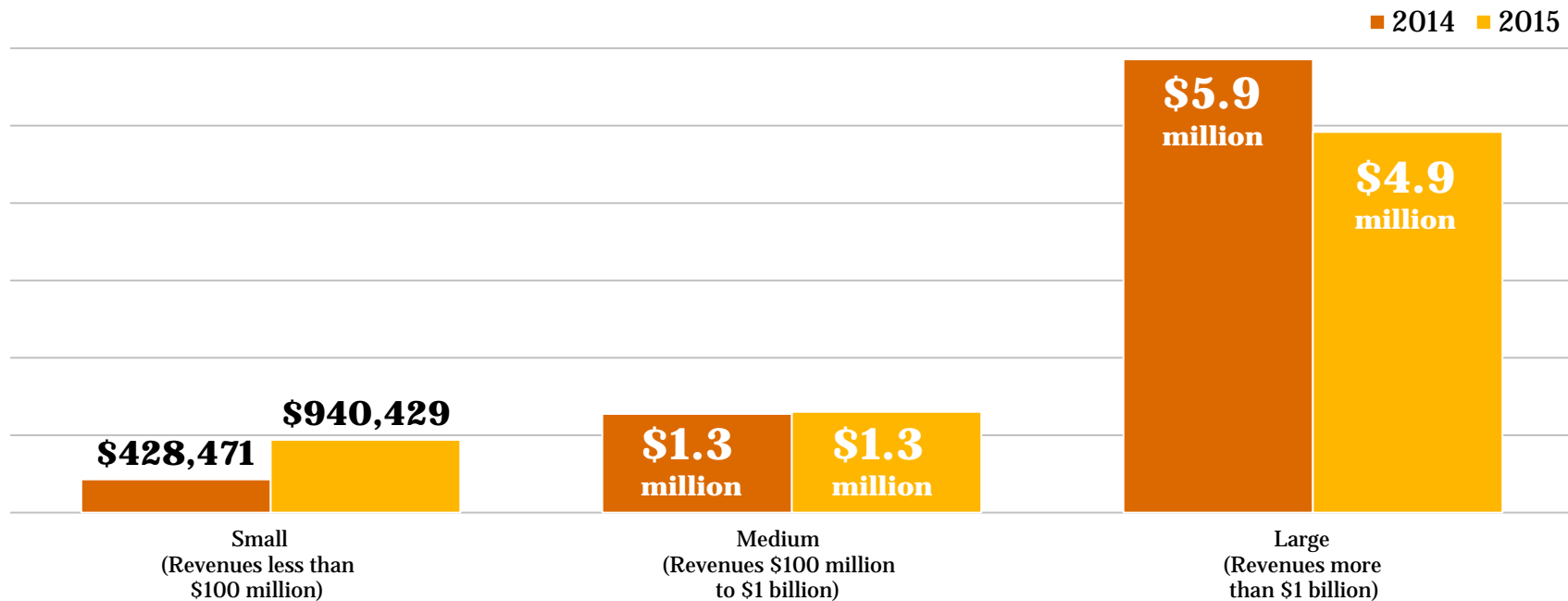

13,138
2014

9,155
2013

4,227
2014

2,581
2013

1,091
2014

1,151
2013

Small
Revenues less than $100 million

Medium
Revenues $100 million–$1 billion

Large
Revenues more than $1 billion

Threats come from a myriad of backgrounds and capabilities

Adversary	Motives	Targets	Impact
Nation State	• Economic, political and /or military advantage	• Trade secrets • Sensitive business information • Emerging technologies • Critical infrastructure	• Loss of competitive advantage • Disruption to critical infrastructure • Monetary loss
Organized Crime	• Illicit profit • Fraud • Identity theft	• Financial / Payment Systems • Data breaches and intellectual property theft • Third-party service providers	• Costly regulatory inquiries and penalties • Consumer and shareholder lawsuits • Loss of consumer confidence
Hacktivists	• Influence political and /or social change • Pressure business to change their practices	• Corporate secrets • Sensitive business information • Information related to employees, customers & business partners	• Disruption of business activities • Brand and reputation • Loss of consumer confidence
Insiders	• Personal advantage, monetary gain • Professional revenge • Patriotism	• Sales, deals, market strategies • Corporate secrets, IP, R&D • Business operations • Personnel information	• Trade secret disclosure • Operational disruption • Brand and reputation • National security impact

... and the financial costs of incidents can be significant

*Average **initial financial losses** due to security incidents – does not account for ongoing remediation and longer term financial expenditures*

Legend: ■ 2014 ■ 2015

- Small (Revenues less than $100 million): $428,471 (2014); $940,429 (2015)
- Medium (Revenues $100 million to $1 billion): $1.3 million (2014); $1.3 million (2015)
- Large (Revenues more than $1 billion): $5.9 million (2014); $4.9 million (2015)

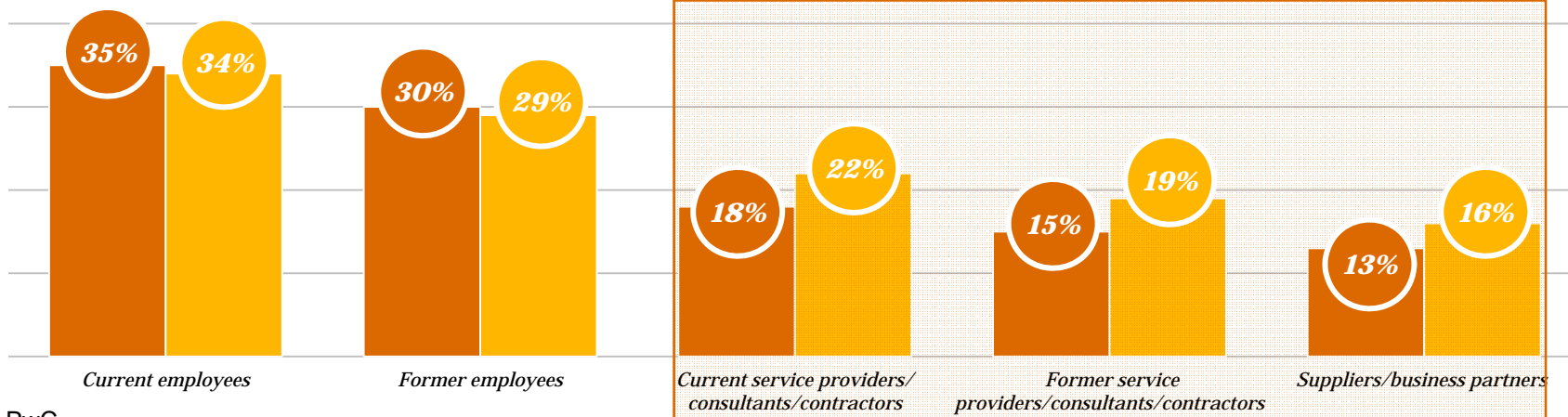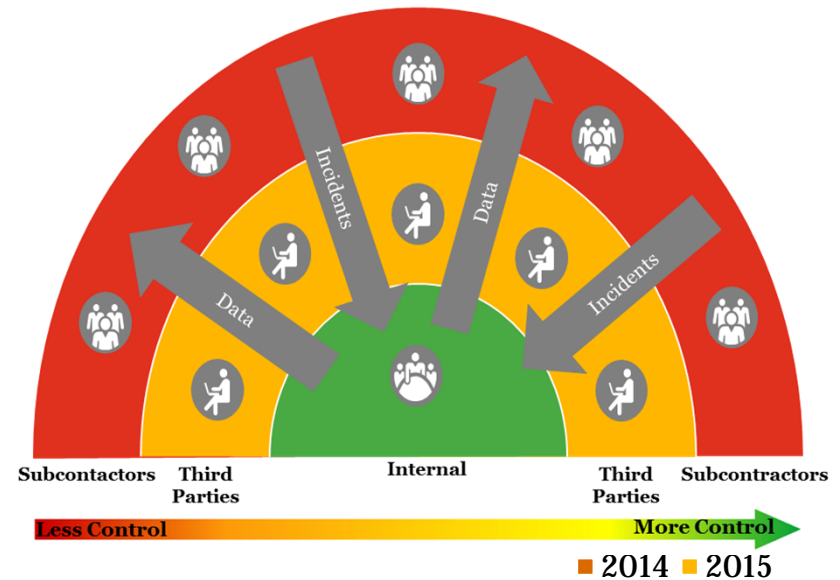Source : PwC – 2016 – Global State of Information Security Survey

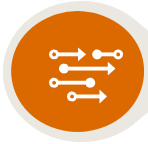# *Third parties are often the weakest cybersecurity link*

Third Parties will be overtaking internal vectors

Employees are still the most cited source of compromise, **but incidents attributed to business partners continues to rise**.
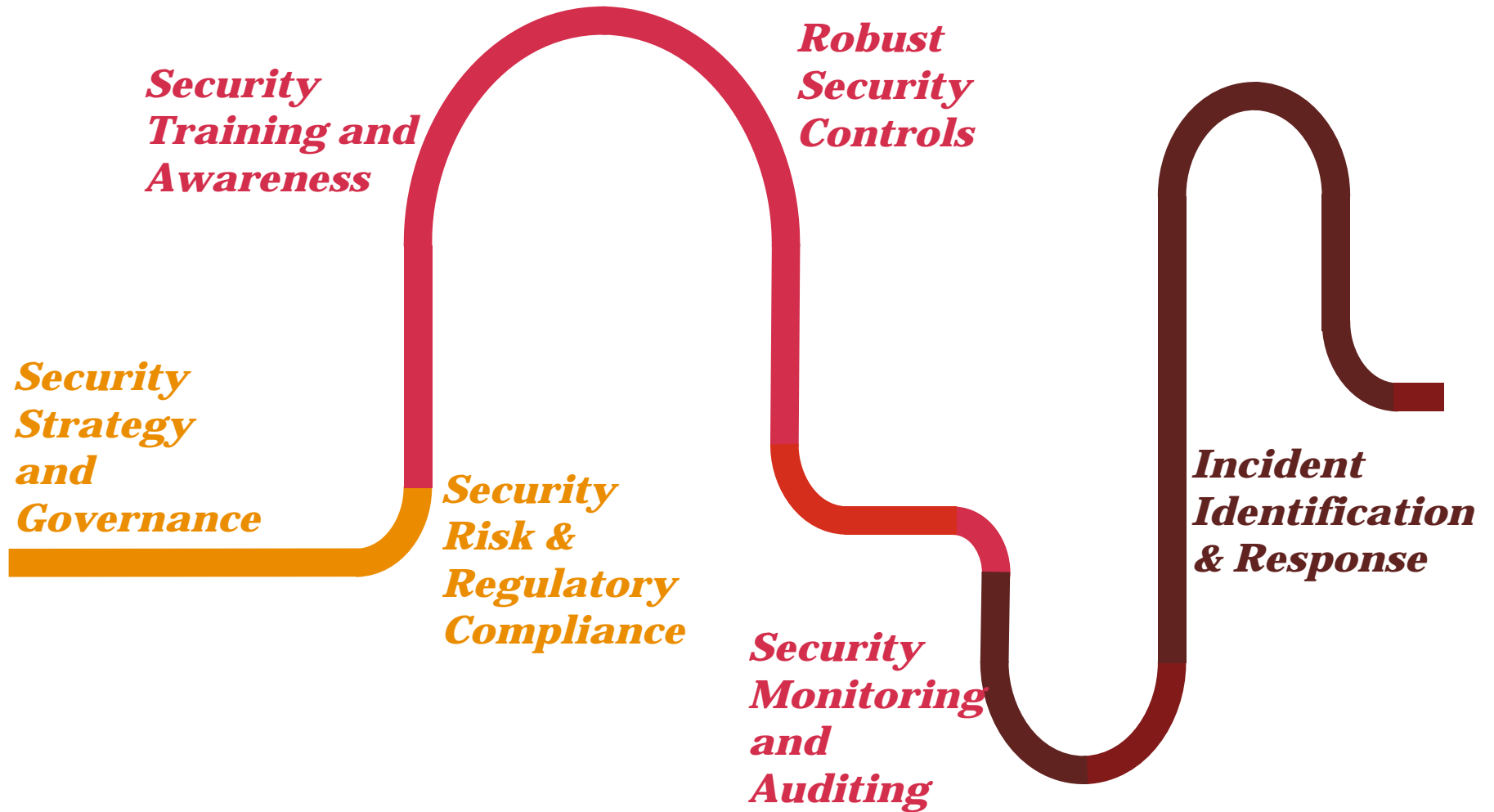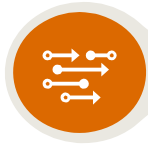
The so-what:

Organizations continue to experience an increased number of third party related breaches. As benefit plans outsource more of their processes and share data with service providers, they need a **means to monitor, measure and manage third party cybersecurity risk.**

Subcontactors   Third Parties   Internal   Third Parties   Subcontractors

Less Control   More Control

■ 2014 ■ 2015

35% **34%** **30%** **29%** Current employees   Former employees

18% **22%** **15%** **19%** **13%** **16%**

Current service providers/ consultants/contractors   Former service providers/consultants/contractors   Suppliers/business partners

PwC

Key cybersecurity program components

Security Training and Awareness

Robust Security Controls

Security Strategy and Governance

Security Risk & Regulatory Compliance

Security Monitoring and Auditing

Incident Identification & Response

Three steps to an improved cybersecurity program

Develop a Risk-driven Cybersecurity Program

Step 1
ID Threats and risks to key business drivers/assets

Step 2
Cybersecurity program assessment

Step 3
Define initiatives and a consolidated roadmap

Understand your critical systems ("Crown Jewels"), the potential impact of a compromise and relevant threats and risks against them.

Understand your current Cybersecurity program maturity, and the adequacy of your program's capabilities using a threat and risk informed target-state. Identify any gaps to target.

Develop findings and a prioritized set of initiatives and program roadmap to address the gaps.

Thank you

James F. Fox

Partner (Principal)
james.fox@pwc.com

PwC