LESSONS FROM PRACTICE: INSIGHTS FROM PROTIVITI PROFESSIONALS

May 2019

Internal Audit, Risk, Business & Technology Consulting

TODAY’S PRESENTERS

DANIEL STONE is a Senior Manager within the Internal Audit and Financial Advisory (IAFA) practice focused on Technology Audit. Daniel has 6 years of experience in leading and performing IT general and application controls assessments for SOX compliance. Daniel also has significant experience with Cybersecurity Risk Assessments, primarily using the NIST Cybersecurity Framework, and audits of technical security controls including hardware and network device configuration management, encryption, vulnerability management, and identity management.

ANUP VASISTH is a Manager with Protiviti’s Security and Privacy practice based out of Atlanta. He specializes in Application Security and has built Secure Development Lifecycle Programs, led GDPR, NIST and HIPAA Risk Assessments and PCI remediation activities for his clients. Prior to that, he was a software engineer at Noble Systems Corporation and worked with several cross-functional teams to deliver custom tools and applications in Python and C/C++.

Setting the Stage

> VIRTUALLY ALL ECONOMIC ACTIVITIES NOW TAKE PLACE THROUGH DIGITAL TECHNOLOGY AND ELECTRONIC COMMUNICATION, LEAVING BUSINESS TRANSACTIONS AND ASSETS SUSCEPTIBLE TO A VARIETY OF CYBER-RELATED THREATS.

- SEC Cyber Threat Report, October 16 2018

AUDIT’S ROLE IN CYBERSECURITY

“Limited, But Important”

ICFR EFFECTIVENESS
RISK ASSESSMENT
CYBER DISCLOSURE

ICFR EFFECTIVENESS

Highlights from SEC Cyber-Related Frauds Report

- 9 issuers lost at least $1 million, 2 of which lost over $30 million
- Report categorized findings based on:
  - Emails from fake executives
  - Emails from fake vendors
- 1 issuer made 14 wire payments over several weeks at the request of a fake executive, losing over $45 million
  - Critically, the fraud was uncovered by a foreign bank – not the company's own controls
- Were these cybersecurity or business control failures?

"…did not follow the company's dual-authorization requirement for wire payments…"

"…the accounting employee misinterpreted the company's authorization Matrix…"

"In two instances the targeted recipients were themselves executive-level employees—
chief accounting officer…"

Source: SEC Release No. 84429, October 16 2018

SEC INTERPRETIVE GUIDANCE ON CYBERSECURITY DISCLOSURES

Guidance published on February 21, 2018 is designed to reinforce the guidance on Cybersecurity disclosures published in October 2011 and further expand on it.

DISCLOSURE OF CYBERSECURITY RISKS AND INCIDENTS

- Periodic reports (10-Q, 10-K)
- Current reports (Form 8-K)
- Registration statements (Form S-1)
- Securities Act and Exchange Act obligations – consider adequacy of disclosures
- Disclosures must be updated if additional material information becomes available or previous disclosure becomes materially inaccurate
- Cybersecurity Risk Factors, including those arising from any acquisition
  - Prior incidents, adequacy of controls, costs of cybersecurity protections, reputational harm, laws and regulations, litigations and investigations

Source: Commission Statement and Guidance on Public Company Cybersecurity Disclosures, February 21 2018

SEC INTERPRETIVE GUIDANCE ON CYBERSECURITY DISCLOSURES (CONTD.)

IMPORTANCE OF CYBERSECURITY POLICIES AND PROCEDURES

- Sufficiency of disclosure controls and procedures related to cybersecurity disclosure
- Prohibit insiders from trading on nonpublic information about cybersecurity incidents
- Preventing selective disclosure

PROHIBITION OF INSIDER TRADING IN CYBERSECURITY CONTEXT

- It is illegal to trade securities on the basis of material nonpublic information
- Recommended to restrict insider training while cybersecurity incidents are investigated

BOARD RISK OVERSIGHT

- Disclosure of the extent of its board of director’s role in risk oversight
- Board’s role in overseeing the management cybersecurity risks
- How the board of directors engages with management on cybersecurity issues

Source: Commission Statement and Guidance on Public Company Cybersecurity Disclosures, February 21 2018

EXAMPLE DISCLOSURE – SLACK S-1

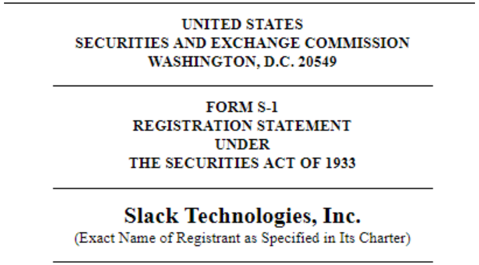
(presented partially, emphasis ours)

*“If there are interruptions or performance problems associated with the technology or infrastructure used to provide Slack, **organizations on Slack may experience service outages**, other organizations may be reluctant to adopt Slack, and our **reputation could be harmed**.”*

“A security incident may allow unauthorized access to our systems, networks, or data or the data of organizations on Slack, harm our reputation, create additional liability, and harm our financial results.

*…For instance, for a period of approximately four days in March 2015, **a security incident occurred** in which unauthorized third parties had access to information maintained by us … We are **not aware of any material impact** on any organizations that resulted from the incident. …”*

*“Interruptions or delays in the services provided by third-party data centers or Internet service providers **could impair Slack** and our business could suffer.”*



UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

FORM S-1
REGISTRATION STATEMENT
UNDER
THE SECURITIES ACT OF 1933

Slack Technologies, Inc.
(Exact Name of Registrant as Specified in Its Charter)

SLACK TECHNOLOGIES, INC.

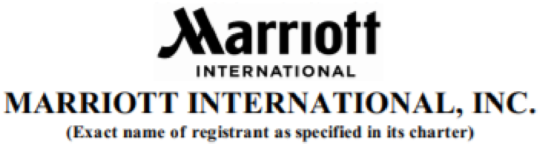
slack

Shares of Class A Common Stock

Source: Slack S-1 Filing, April 26 2019

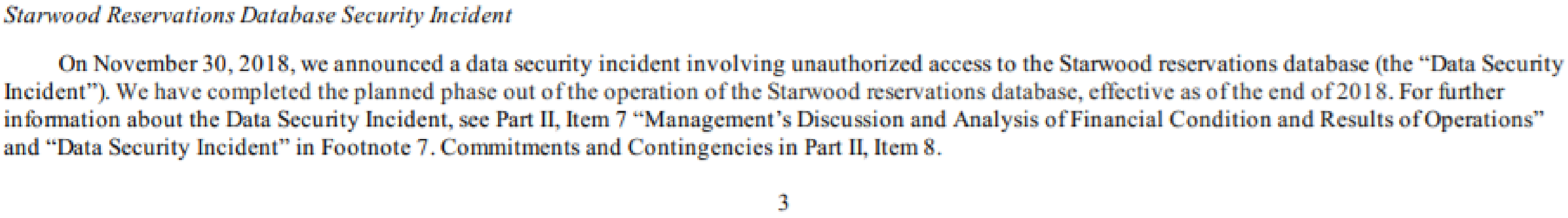
EXAMPLE DISCLOSURE – MARRIOTT 10-K

(presented partially)



MARRIOTT INTERNATIONAL, INC.

(Exact name of registrant as specified in its charter)



Starwood Reservations Database Security Incident

On November 30, 2018, we announced a data security incident involving unauthorized access to the Starwood reservations database (the "Data Security Incident"). We have completed the planned phase out of the operation of the Starwood reservations database, effective as of the end of 2018. For further information about the Data Security Incident, see Part II, Item 7 "Management's Discussion and Analysis of Financial Condition and Results of Operations" and "Data Security Incident" in Footnote 7. Commitments and Contingencies in Part II, Item 8.

3

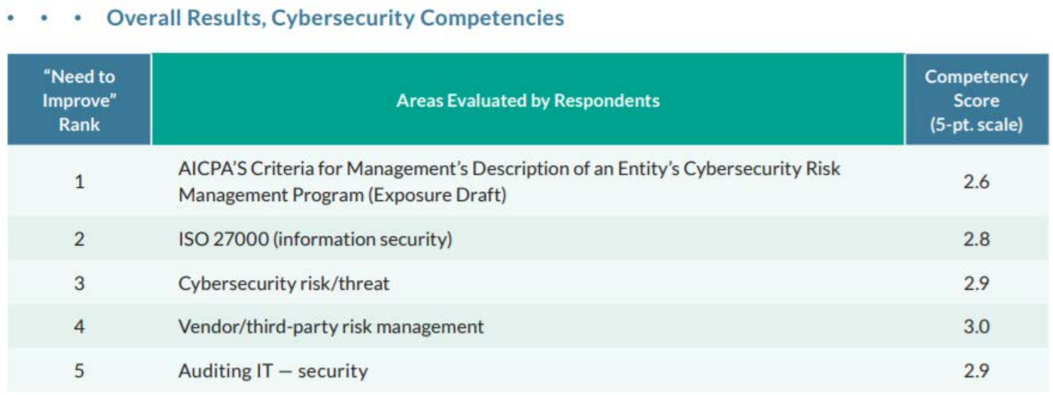
"In 2018, we recorded $28 million of expenses related to the Data Security Incident, partially offset by $25 million of accrued insurance recoveries…"

"While we believe it is reasonably possible that we may incur losses associated with the above described proceedings and investigations, it is not possible to estimate the amount of loss or range of loss, if any, that might result from adverse judgments, settlements, fines, penalties or other resolution of these proceedings and investigations based on the early stage of these proceedings…"

Source: Marriott 10-K Filing, March 1 2019

Cybersecurity Environment

TOP CYBER AREAS FOR AUDITORS – KNOWLEDGE



• • • Overall Results, Cybersecurity Competencies

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency Score (5-pt. scale)
1	AICPA'S Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program (Exposure Draft)	2.6
2	ISO 27000 (information security)	2.8
3	Cybersecurity risk/threat	2.9
4	Vendor/third-party risk management	3.0
5	Auditing IT — security	2.9

Key Findings

01 Vendor / third-party risk management has risen to a key area of "Need to Improve" year over year

02 There is continued interest in SOC for cybersecurity risk management, and impact on both the Service Organization and User Entity

03 Cybersecurity is a "staple" of audit plans, and no longer a question of "if" it will be covered but "how" and to what extent

Source: *Protiviti's 2019 Internal Audit Capabilities and Needs Survey*

INTRODUCTION: THE CYBERSECURITY IMPERATIVE

ESI Thought Lab joined with WSJ Pro Cybersecurity to launch **The Cybersecurity Imperative.**

The Cybersecurity Imperative, a thought leadership program conducted by ESI Thought Lab in partnership with a group of prominent organizations, including Protiviti, dissects results from a rigorous mixed-methods research program, consisting of four elements:

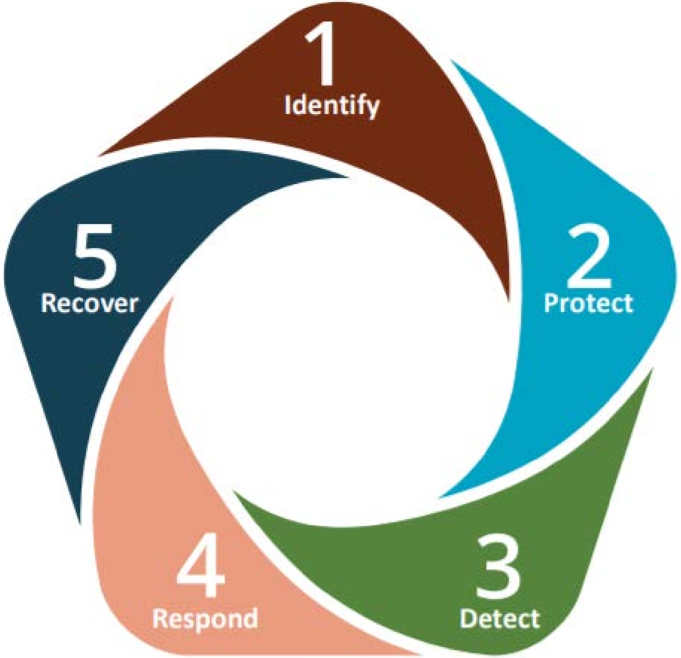
1. A diagnostic survey of 1,300 firms across industries and regions
2. In-depth interviews with 18 chief information security officers (CISOs) and cybersecurity experts
3. Insights from an advisory board of executives representing a variety of perspectives
4. Cost-benefit analysis and modeling to gauge the impact of information security practices on performance

ESI THOUGHTLAB
Tailoring thought leadership
Finding the best ways to engage an executive audience
WSJ PRO
CYBERSECURITY

By 2021, cybercrime is likely to cost the world **$6 trillion** annually. As companies embrace the latest technologies and respond to rising regulations, cybersecurity has become a top management priority across industries and markets.

THE NIST CYBERSECURITY FRAMEWORK

- Used elements of the NIST framework to support the diagnostic survey tool.
- Asked executives to rate their company’s progress across five key cybersecurity pillars: identify, protect, detect, respond, and recover.
- In addition, grouped companies into three categories based on the progress they have achieved against the five cybersecurity pillars:
  - cybersecurity beginners
  - intermediates
  - leaders



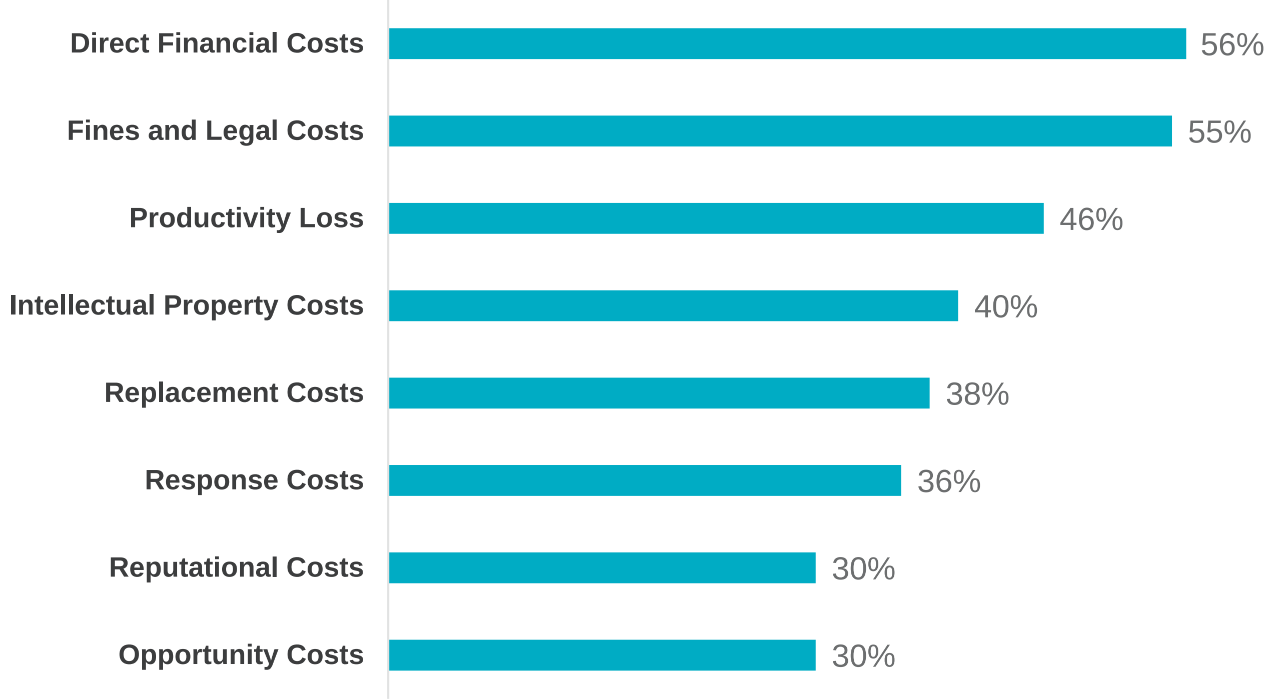
KEY FINDINGS

Important insights for executives striving to take their cybersecurity approach to a higher level:

- The costs for cybersecurity beginners are higher, but also more difficult to measure
- Companies tend to spend more on detection and protection rather than on response and recovery
- Digital transformation creates a business paradox for companies
- The greatest cyber threat for companies now come from within
- The cybersecurity of companies varies by country
- Companies are reorganizing to improve cybersecurity
- To win the cybersecurity arms race, companies are tapping a growing arsenal of cybersecurity technologies
- For advanced firms, cybersecurity is no longer just a risk activity, it is a business enabler

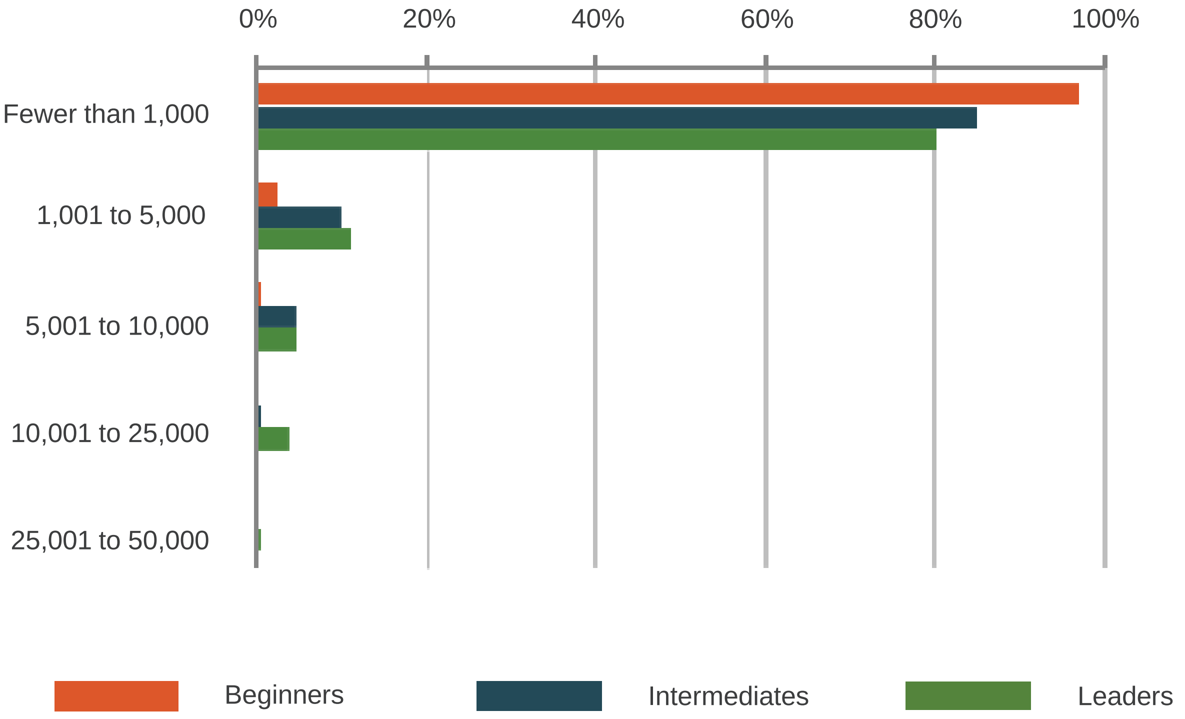
CYBER ATTACK COSTS

Self-Assessment Question: How did each of the following types of cyber incident losses impact your business over the last fiscal year?



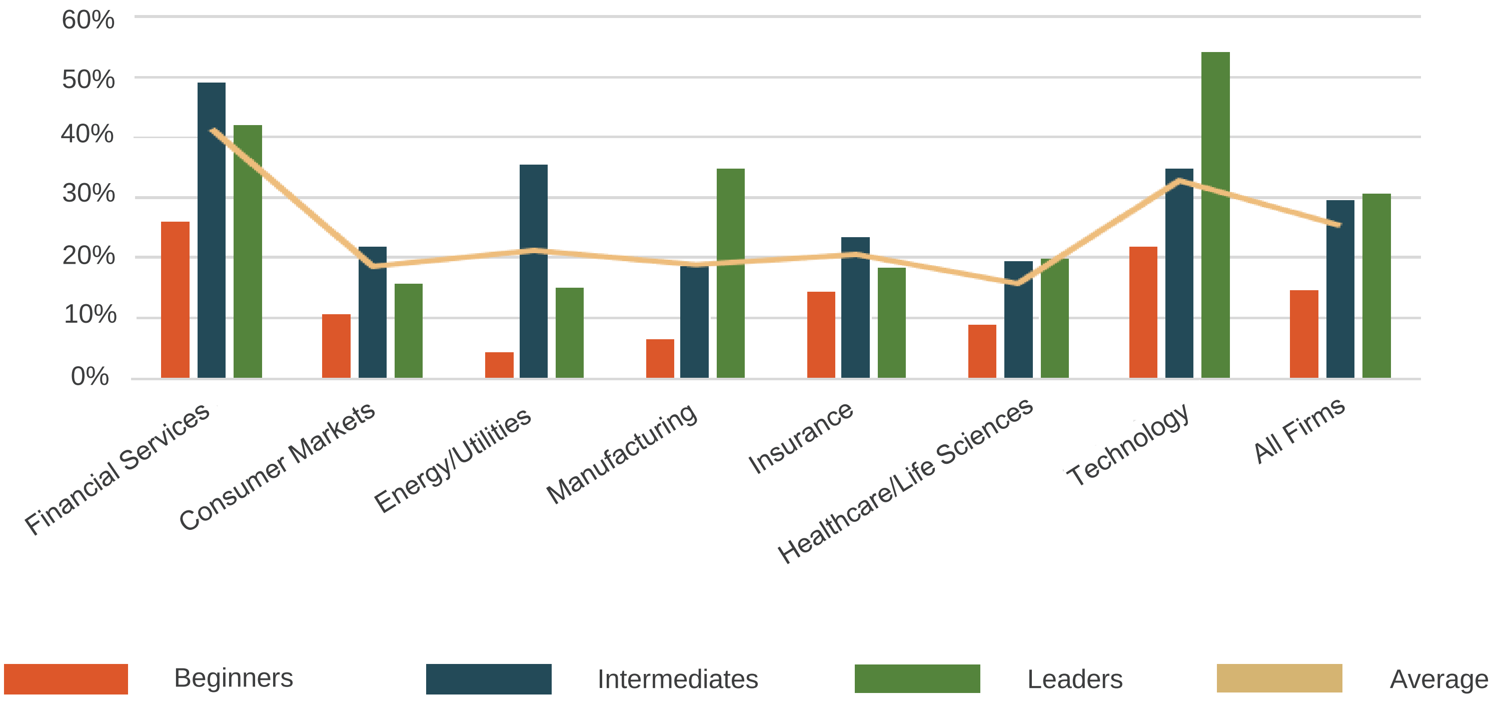
SUCCESSFUL ATTACKS BY MATURITY

Self-Assessment Question: Do we have sufficient detection capability? Are we factoring in the speed of digital transformation?



INCIDENTS BY SECURITY / MATURITY

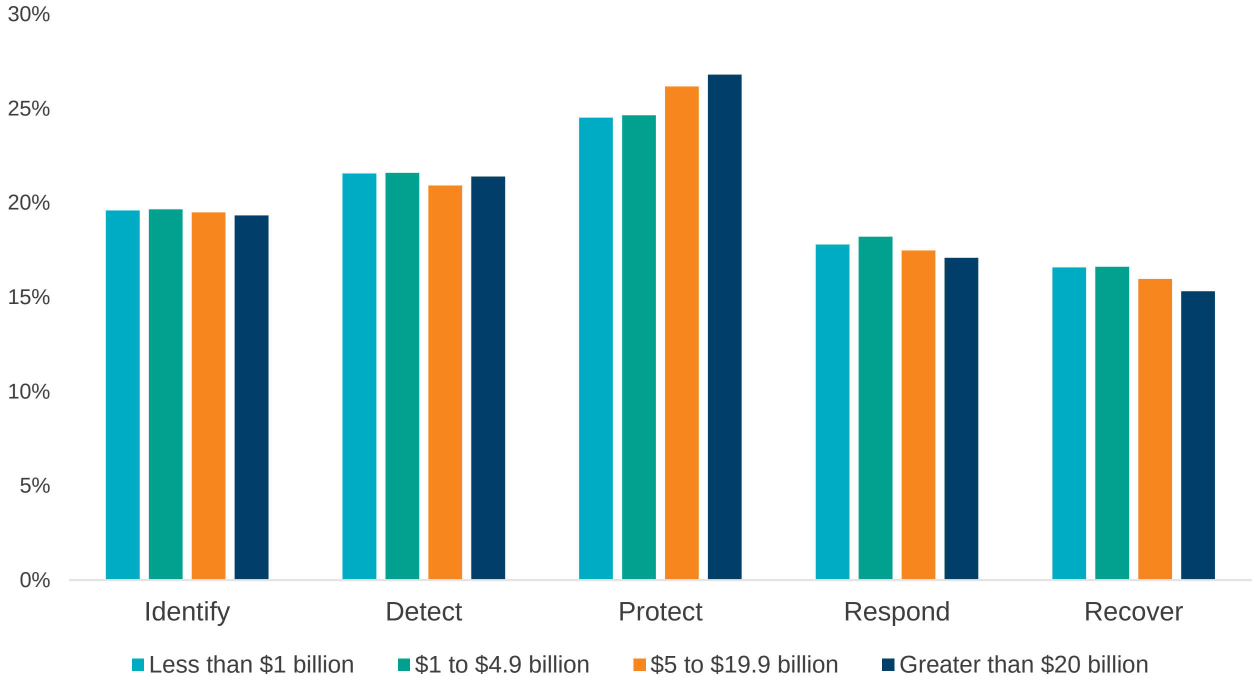
Self-Assessment Question: Do we have sufficient detection capability? Are we factoring in the speed of digital transformation?



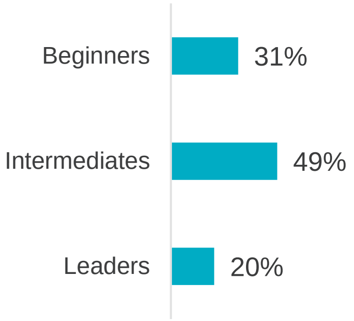
CYBERSECURITY: A WORK IN PROGRESS

Self-Assessment Question: Are our security program and corresponding investments balanced across the areas of identify, detect, protect, respond and recover?

AREAS OF GREATEST PROGRESS BY CATEGORY



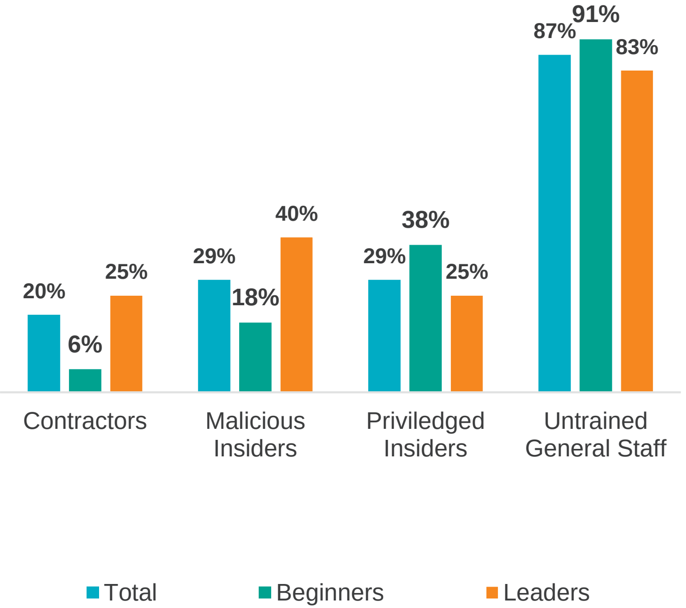
% OF FIRMS BY CYBERSECURITY STAGE



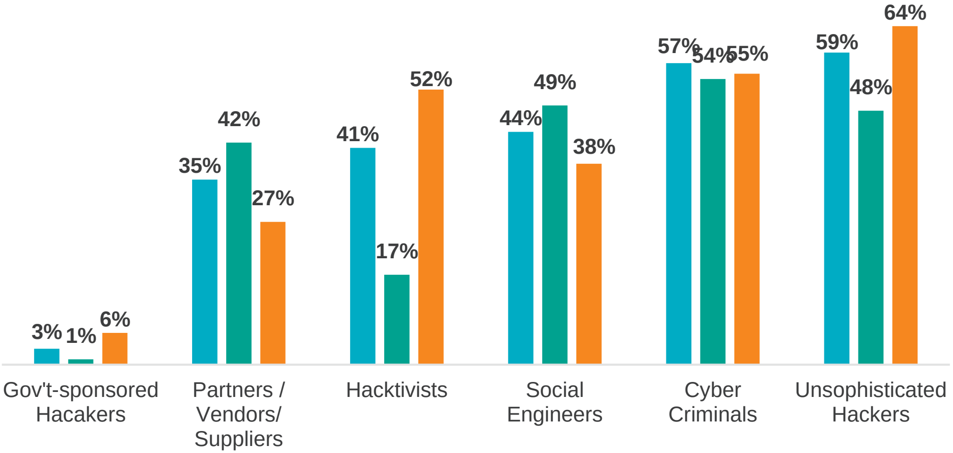
THREAT PERSPECTIVES

Self-Assessment Question: Do we understand our internal and external threats and are we able to detect them?

LARGEST RISKS FROM INTERNAL THREAT ACTORS

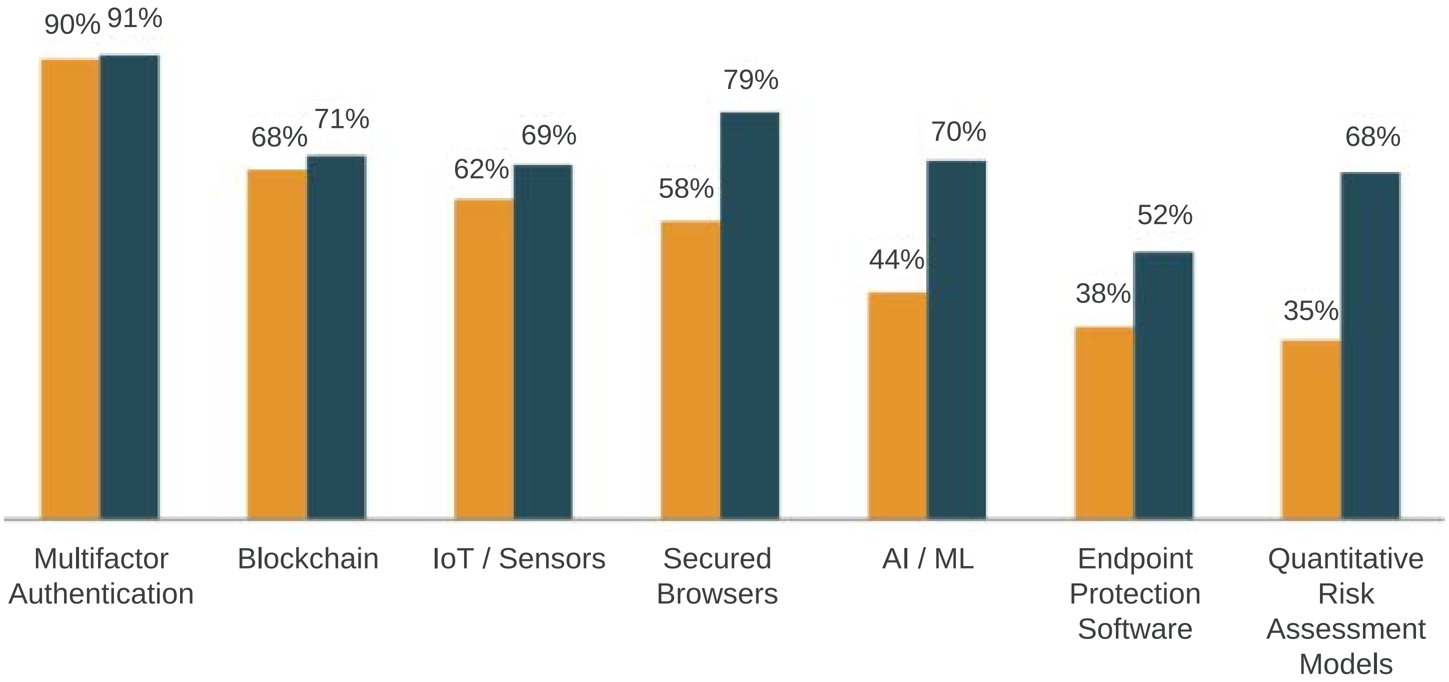


LARGEST RISKS FROM EXTERNAL THREAT ACTORS



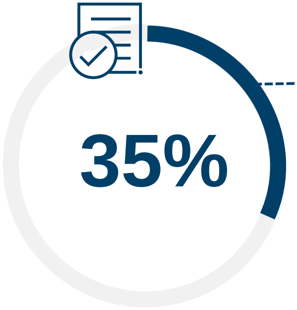
TOOLS OF THE TRADE

Self-Assessment Question: Which of the following is your company using now and which is your company planning to start using over the next two years?

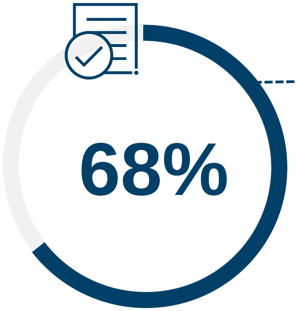


USE OF CYBER RISK QUANTIFICATION

Across industries, companies are **increasing the use of quantitative risk assessment models**



35% of institutions **use quantitative models** for assessing cybersecurity risk **today**

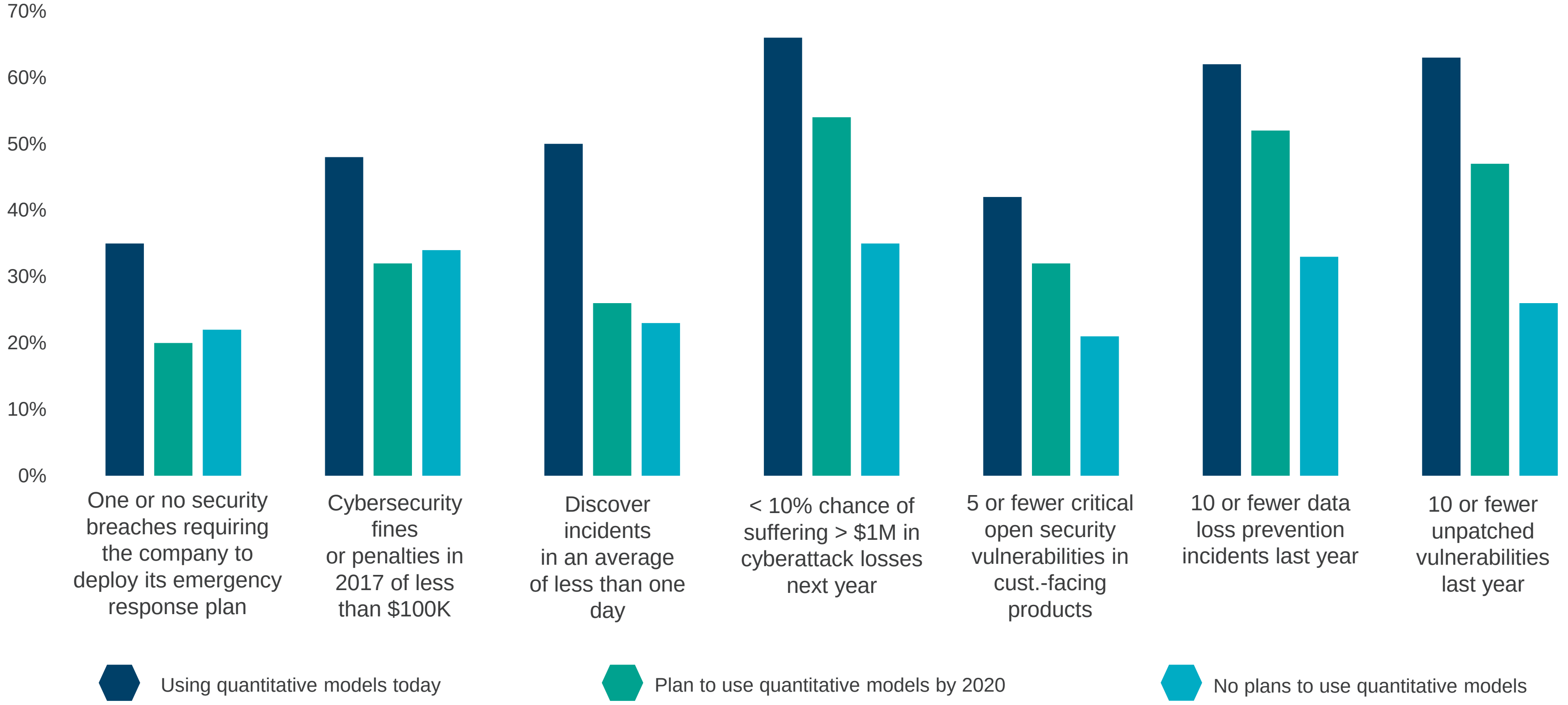


68% of institutions **plan to use quantitative methods** for assessing cybersecurity risk by **2020**

71% of institutions **using quantitative methods today** are planning to **increase use by 2020**

USE OF CYBER RISK QUANTIFICATION

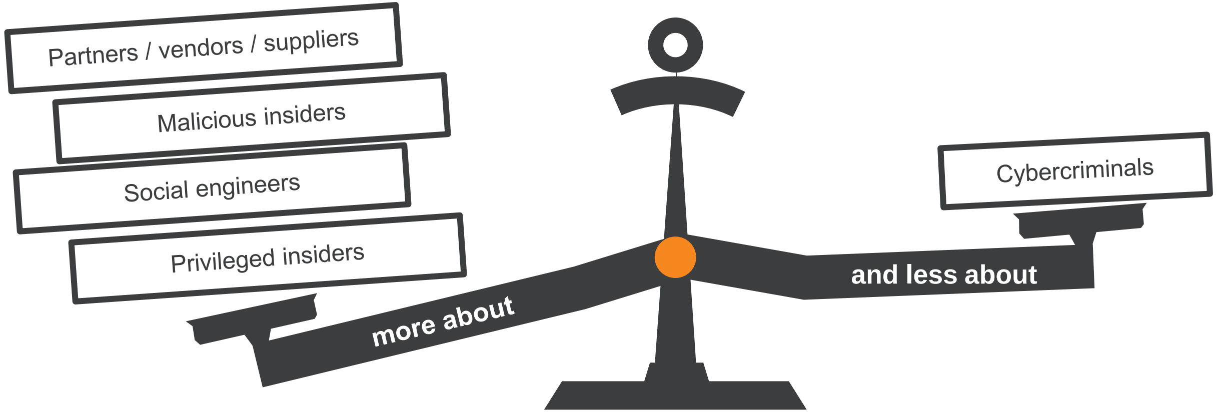
Self-Assessment Question: Do we perform quantitative risk analysis to understand our risks and balance our investment?



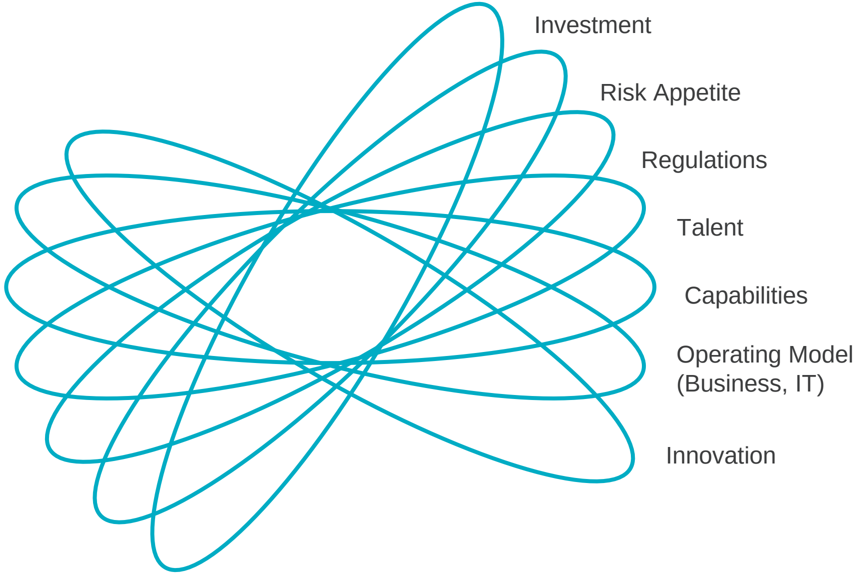
THREAT PERSPECTIVES

Companies that are engaged with quantitative risk assessment models are **more likely** to have a **holistic view of cybersecurity and its threats and attack vectors**

COMPANIES USING QUANTITATIVE RISK ASSESSMENT METHODS CARE…



CYBERSECURITY MARKET DRIVERS



Investment

Risk Appetite

Regulations

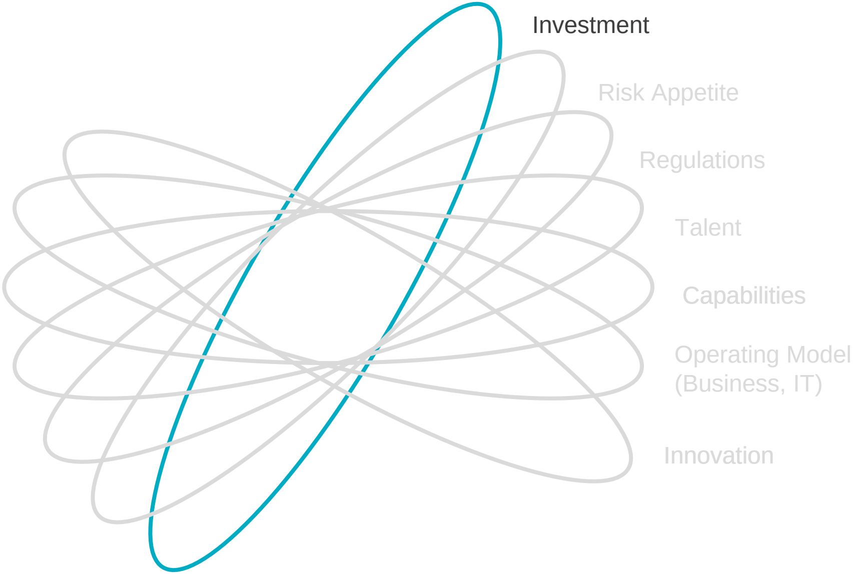
Talent

Capabilities

Operating Model
(Business, IT)

Innovation

CYBERSECURITY MARKET DRIVERS

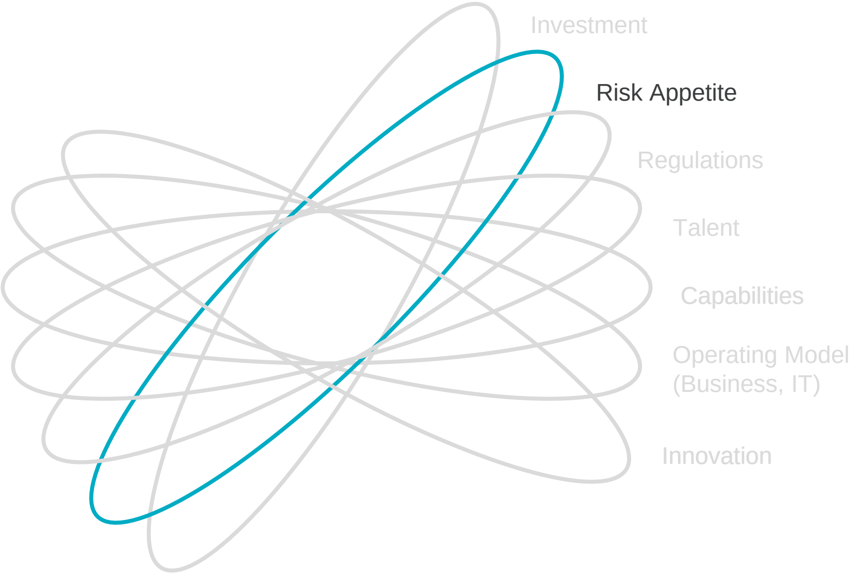


Most companies have under-invested in managing their security risks historically.

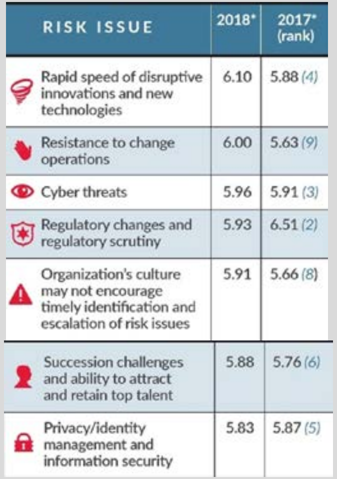
$1 Trillion

Predicted cybersecurity spending from 2017 to 2021

CYBERSECURITY MARKET DRIVERS

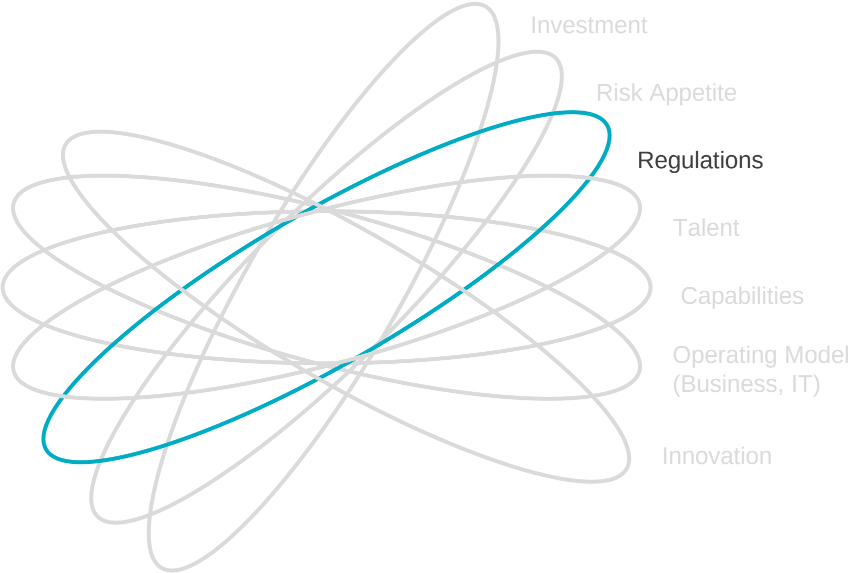


Executive Perspectives on Top Risks



RISK ISSUE	2018*	2017* (rank)
Rapid speed of disruptive innovations and new technologies	6.10	5.88 (4)
Resistance to change operations	6.00	5.63 (9)
Cyber threats	5.96	5.91 (3)
Regulatory changes and regulatory scrutiny	5.93	6.51 (2)
Organization's culture may not encourage timely identification and escalation of risk issues	5.91	5.66 (8)
Succession challenges and ability to attract and retain top talent	5.88	5.76 (6)
Privacy/identity management and information security	5.83	5.87 (5)

CYBERSECURITY MARKET DRIVERS



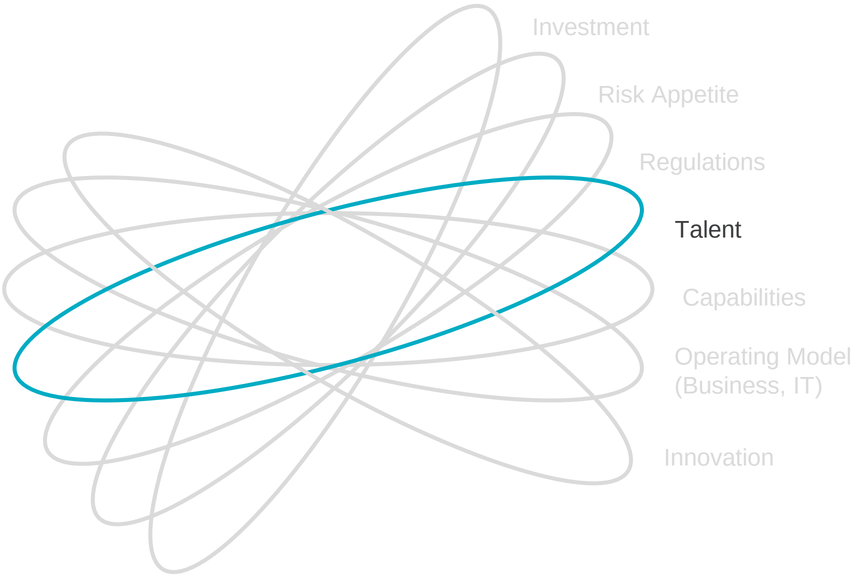
NYDFS, GDPR, and on and on...

‘Large US Banks Scramble to meet US Privacy Laws’

‘Across all industries, new regulations will impact how organizations will prepare for and respond to insider threats. ‘

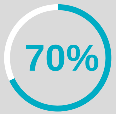
‘Enforcement is not going away, and as the federal agencies create a vacuum, the states will be more active’

CYBERSECURITY MARKET DRIVERS



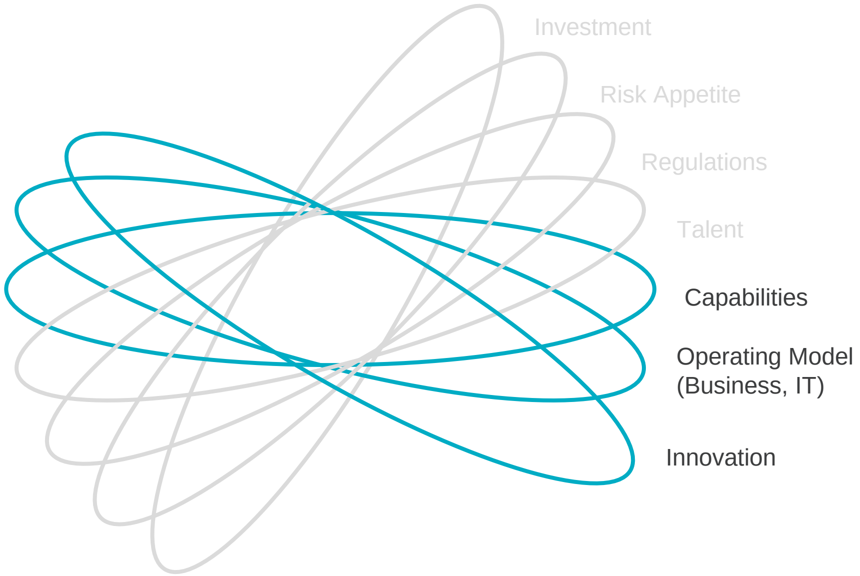
1.5 Million

roles will be unfilled in the Cyber Security Field by 2020



of hiring managers will increase their workforce this year: 30% wish to expand by 20% or more.

CYBERSECURITY MARKET DRIVERS



New Technologies, Evolving Business Needs

- Cloud
- Big Data
- Machine Learning
- Artificial Intelligence
- Expanding Partner Ecosystems

Cybersecurity Briefings

CYBERSECURITY TRENDS AND STATISTICS FOR 2018

90%

of remote code execution attacks are associated with crypto-mining.

92%

of malware is delivered by email.

56%

of IT decision makers say targeted phishing is their top security threat.

77%

of compromised attacks in 2017 were fileless.

69%

of companies see compliance mandates driving spending.

88%

companies spent more than $1 million on preparing for the GDPR.

25%

of organizations have a standalone security department.

54%

of companies experienced an industrial control system security incident.

Sources: CSOOnline

CYBERSECURITY PREDICTIONS FOR 2019

01

Hackers will game end-user face recognition software, and organizations will respond with behavior based systems.

02

Attackers will disrupt Industrial Internet of Things (IIoT) devices using vulnerabilities in cloud infrastructure and hardware.

03

Industry-wide “security trust ratings” will emerge as organizations seek trust assurances for partners and supply chains.

04

There is no real AI in cybersecurity, nor any likelihood for it to develop in 2019.

05

It is probable that a major cloud provider will go down as a result of a breach in 2019. The “it’s not if, but when" doctrine of detection and response will hold true.

06

Isolationist trade policies will incentivize nation states and corporate entities to steal trade secrets and use cyber tactics to disrupt government, critical infrastructure, and vital industries.

07

It is probable that a much stricter internet will evolve, with geographic blocking at the public level as a rule.

08

Tech-savvy businesses and consumers alike will see through the hype, and remain cautious when evaluating solutions whose differentiator is AI or ML.

09

It is probable that a court case will arise in which, after a data breach, an employee claims innocence and an employer claims deliberate action.

10

Consumer concern about breaches will cause companies to embrace edge computing in order to enhance privacy. Designers will struggle with adoption due to low user trust.

Sources: Forcepoint report, Intelligonetworks

WHERE TO START?

EASIER QUESTIONS

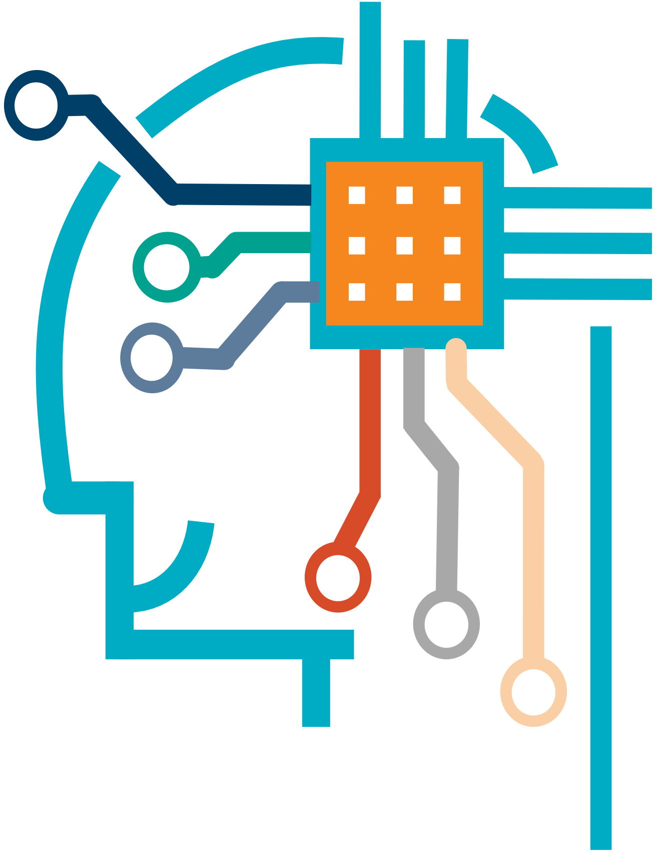
- What does our network look like (systems, network, users)?
- Where is our sensitive data?
- What are our weaknesses?

HARDER QUESTIONS

- What programs should be running on our systems?
- What type of traffic is "normal" for us?
- What user activity is normal?

WHAT'S THE RISK?

- Not knowing what you have makes it hard to know what to protect.
- Not knowing your weaknesses makes it hard to know where you will be hit.
- Not knowing what is normal makes it hard to know what is abnormal.



Q&A

Face the Future with Confidence

protiviti®