How Organizations are Managing Cyber Risk in a Fast-Changing Business Environment: Marsh Microsoft 2019 Cyber Survey Results

Monday, October 7th @ 11 AM Eastern

MARSH

Advisen
Transforming • Insurance℠

Today's Moderator

Erin Ayers
Editor
Cyber Front Page News
Advisen

Contact at eayers@advisen.com

Today's Panelists

Joram Borenstein
General Manager
Cyber Security Solutions Group
Microsoft

Tom Reagan
US Cyber Practice Leader
Marsh

Kevin Richards
Global Head
Marsh Cyber Risk Consulting

Sarah Stephens
UK Cyber Practice Leader
Marsh

MARSH | Microsoft

2019 GLOBAL CYBER RISK PERCEPTION SURVEY

OCTOBER 7, 2019

MARSH & McLENNAN COMPANIES

Survey Findings Confirm What We’re Hearing from Clients

- Current cyber risk landscape:
  - Rising **frequency & severity** of cyber incidents.
  - Rising **economic impact.**

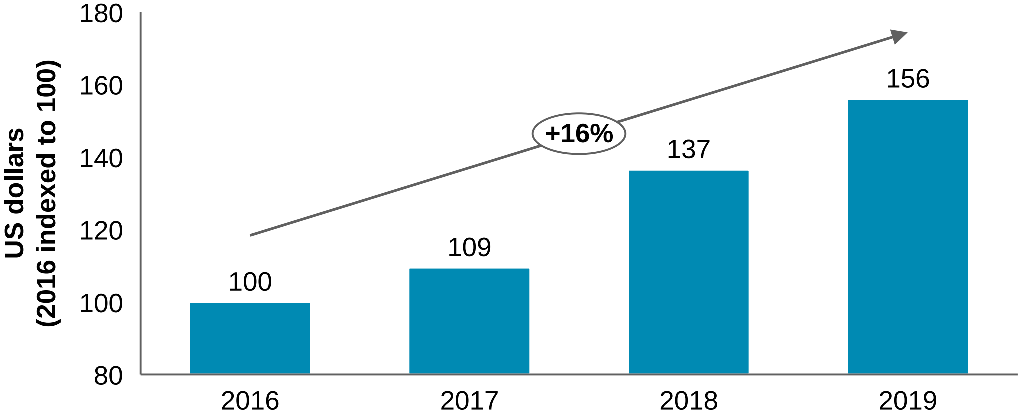
- Many organizations **are challenged** to identify the right strategies, right actions, right solutions.
  - Awareness is high, but confidence about the best approach is not.

- Spending is rising – are we getting **maximal utility** of that investment?
  - Increased cybersecurity investment not yielding expected performance improvements.
  - Need to optimize balance of spending on technology vs. risk transfer.

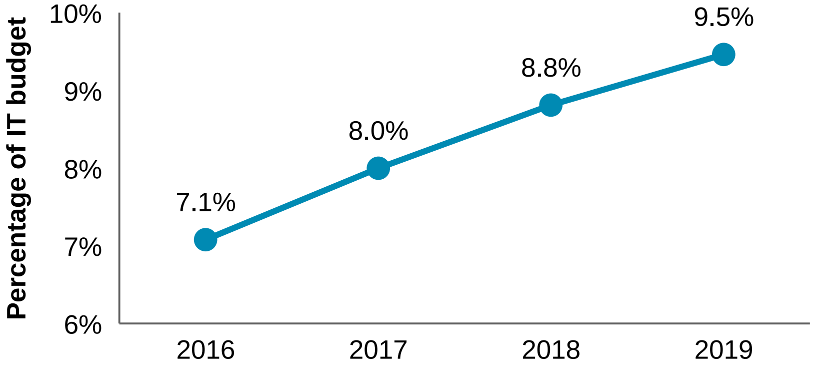
Cyber Defense Spending is Soaring – Where Will It Top Out?

Growth of CISO budgets

US dollars indexed to 100, 2016-2019

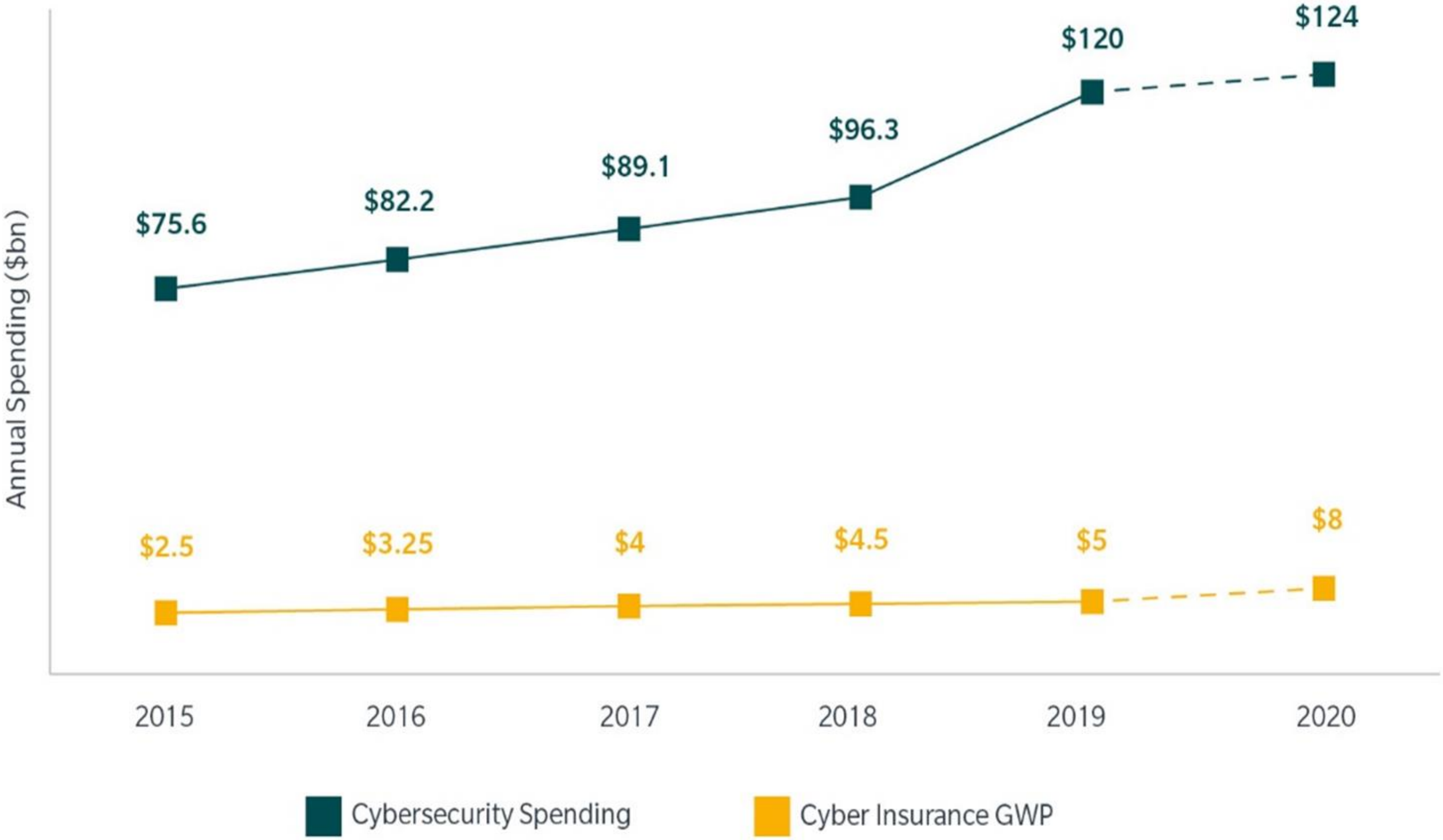


As a percentage of overall IT budget, 2016-2019



- In the past few years, **cyber related spending has grown rapidly**
- **Factors fueling growth**, include:
  - New regulation and laws (e.g., **GDPR**, **California Consumer Privacy Act** and CCPA-like laws across many states)
  - **Media coverage** of high-profile cyber breaches…and associated **fines**
  - Shareholder scrutiny (e.g., new ratings methodologies)
- CISO cyber budgets grew faster than IT budgets and therefore **increased as a share of total IT spend**
  - 20% of IT budget dedicated to the CISO strategy represented the high watermark

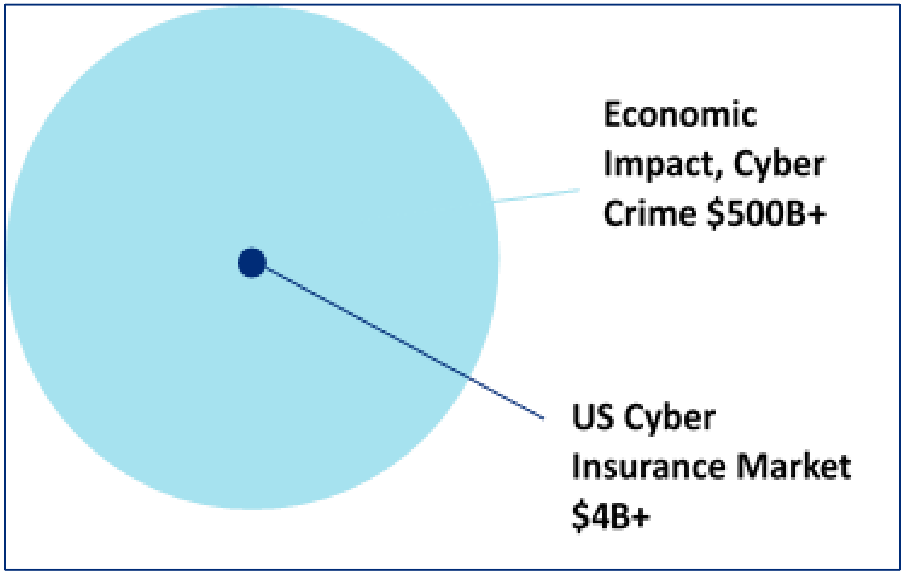
Cybersecurity Budgets Far Outpace Cyber Insurance Spending



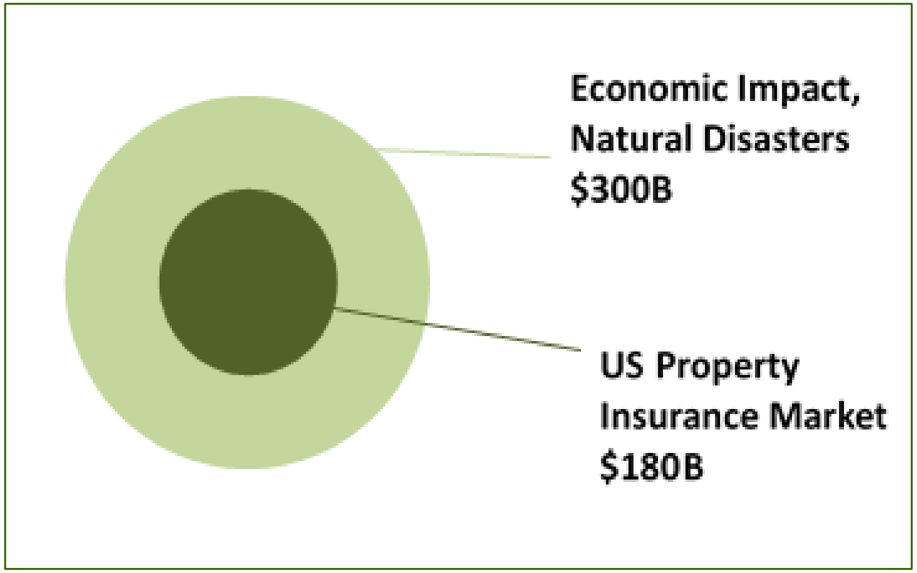
Source: Gartner, Munich Re

Insurance Investment, Property vs. Cyber Risk

Cyber Risk



Property Risk



Marsh and MMC Estimates 2018

** Marsh US clients, $1 billion+ revenues, 2018*

MARSH | Microsoft

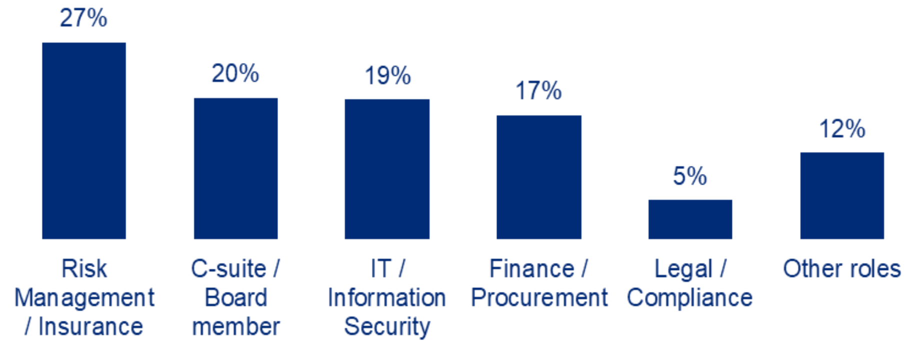
2019 GLOBAL CYBER RISK PERCEPTION SURVEY
KEY FINDINGS

More than 1500 Respondents Across Industries, Roles, and Regions
Conducted In-Market February/March 2019

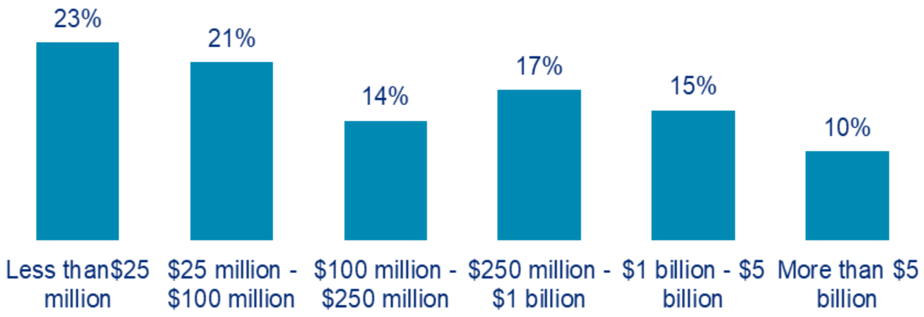
Industries

Manufacturing & Automotive	**16%**	Real Estate	**4%**
Retail & Wholesale	**11%**	Chemical	**4%**
Financial Institutions	**9%**	Construction	**4%**
Energy & Power	**8%**	Education	**4%**
HealthCare & Life Sciences	**7%**	Public Entity/ Not for Profit	**4%**
Transportation, Rail & Marine	**6%**	Mining, Metals & Minerals	**2%**
Communications, Media & Technology	**5%**	Aviation & Aerospace	**1%**
Professional Services	**5%**	Others	**12%**

Corporate Role

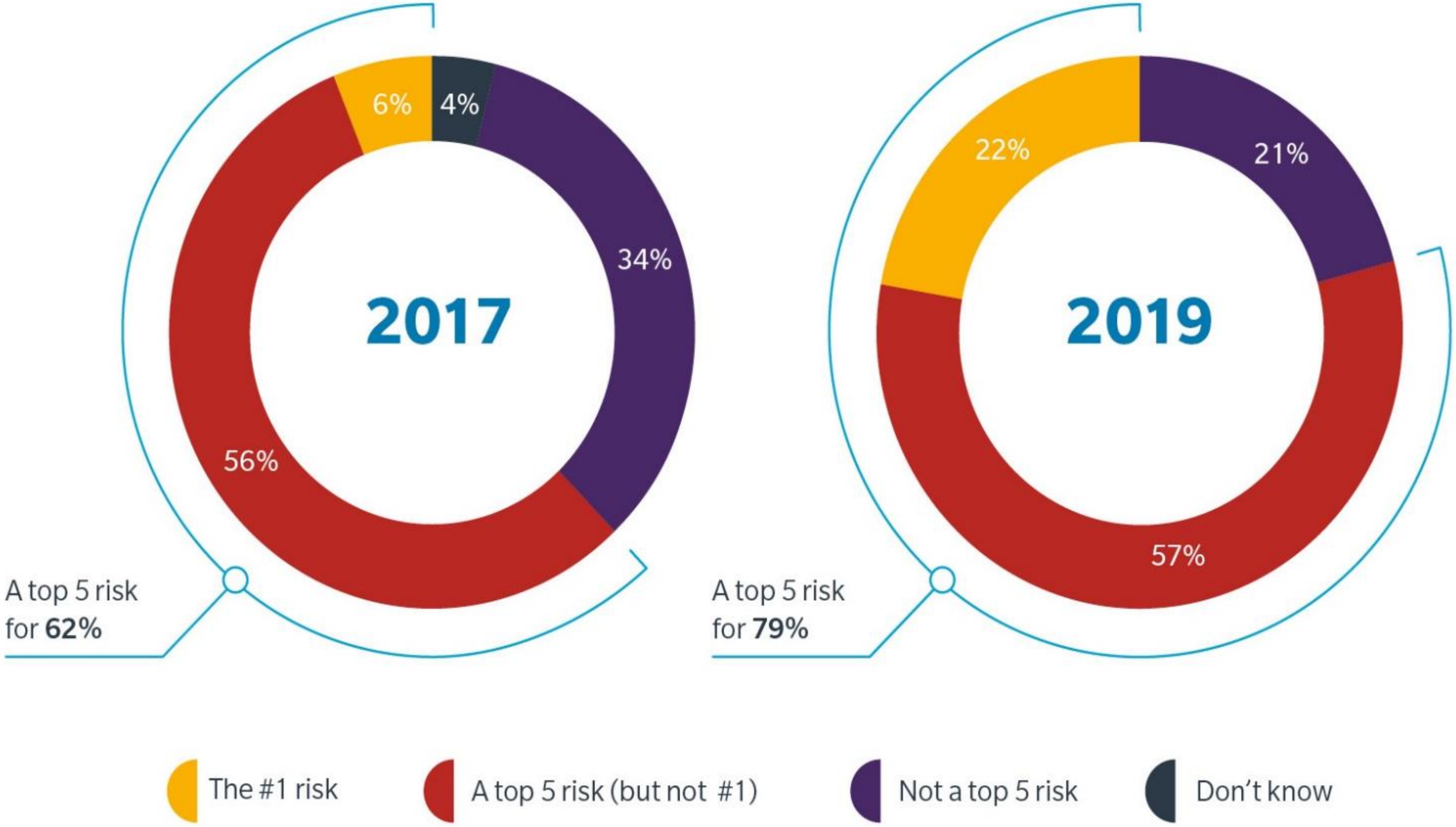


Annual Revenue

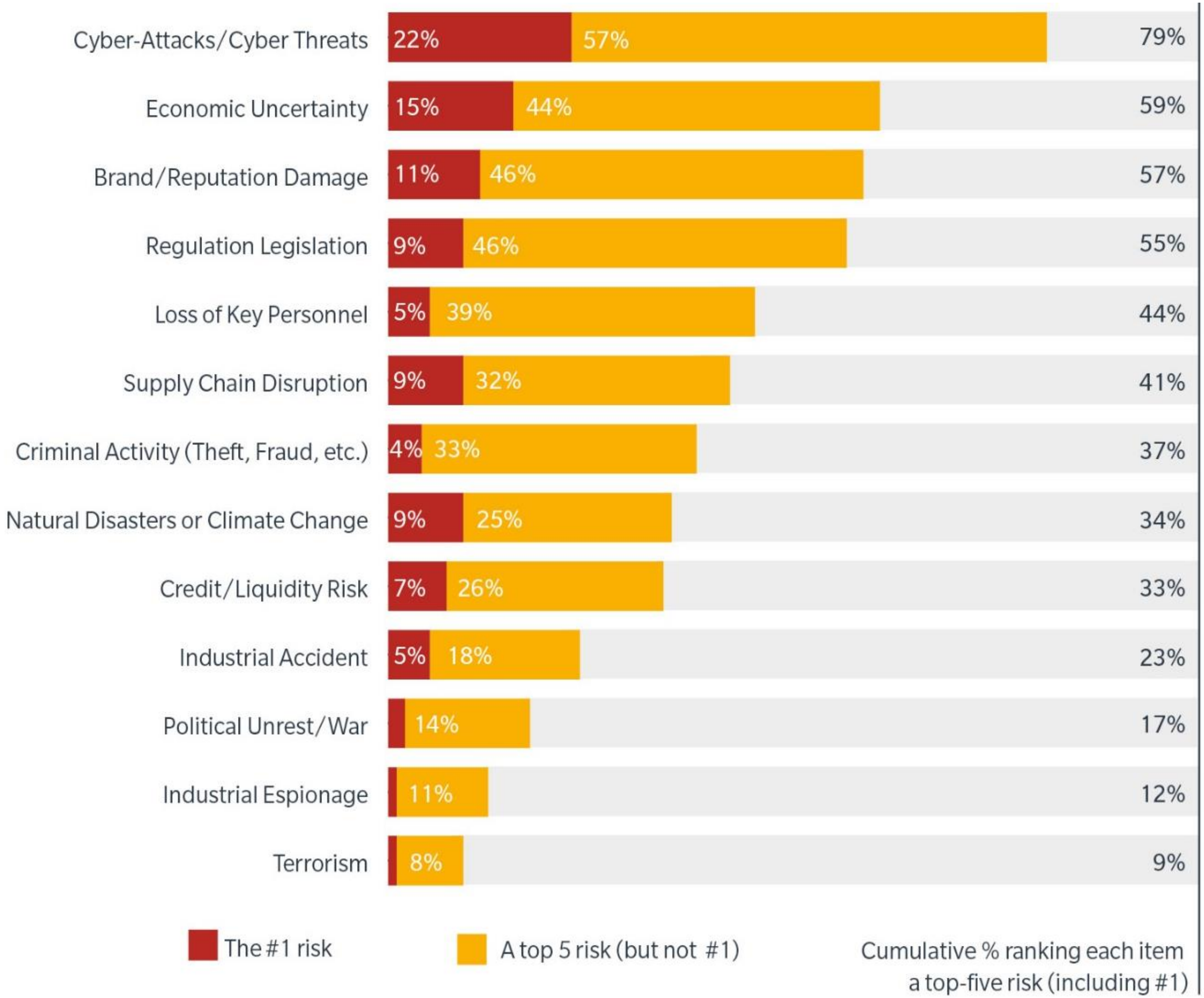


Concern About Cyber Risk is Peaking

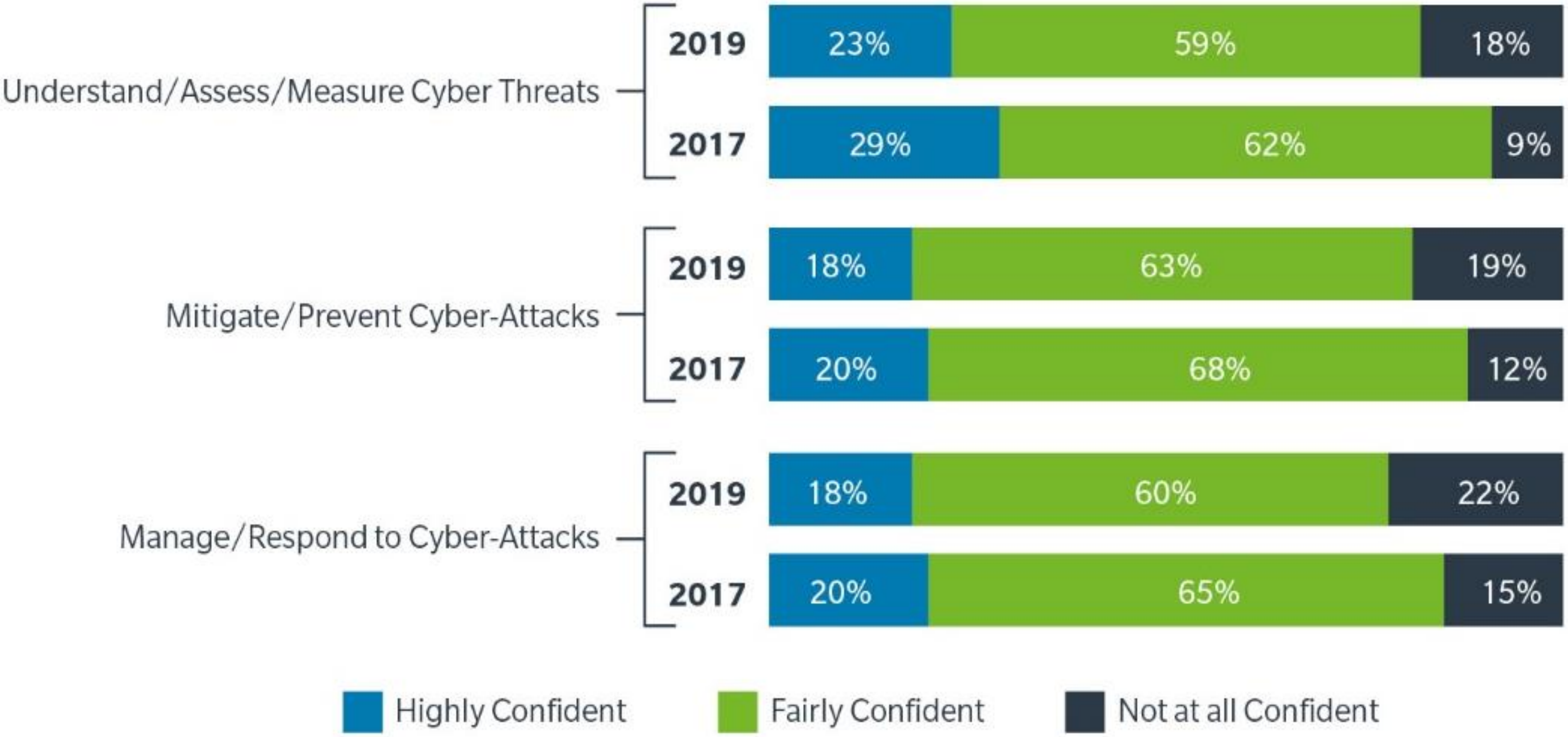
#1: Concern/Confidence Gap



Cyber Risk Surpasses Other Risk Concerns
#1: Concern/Confidence Gap

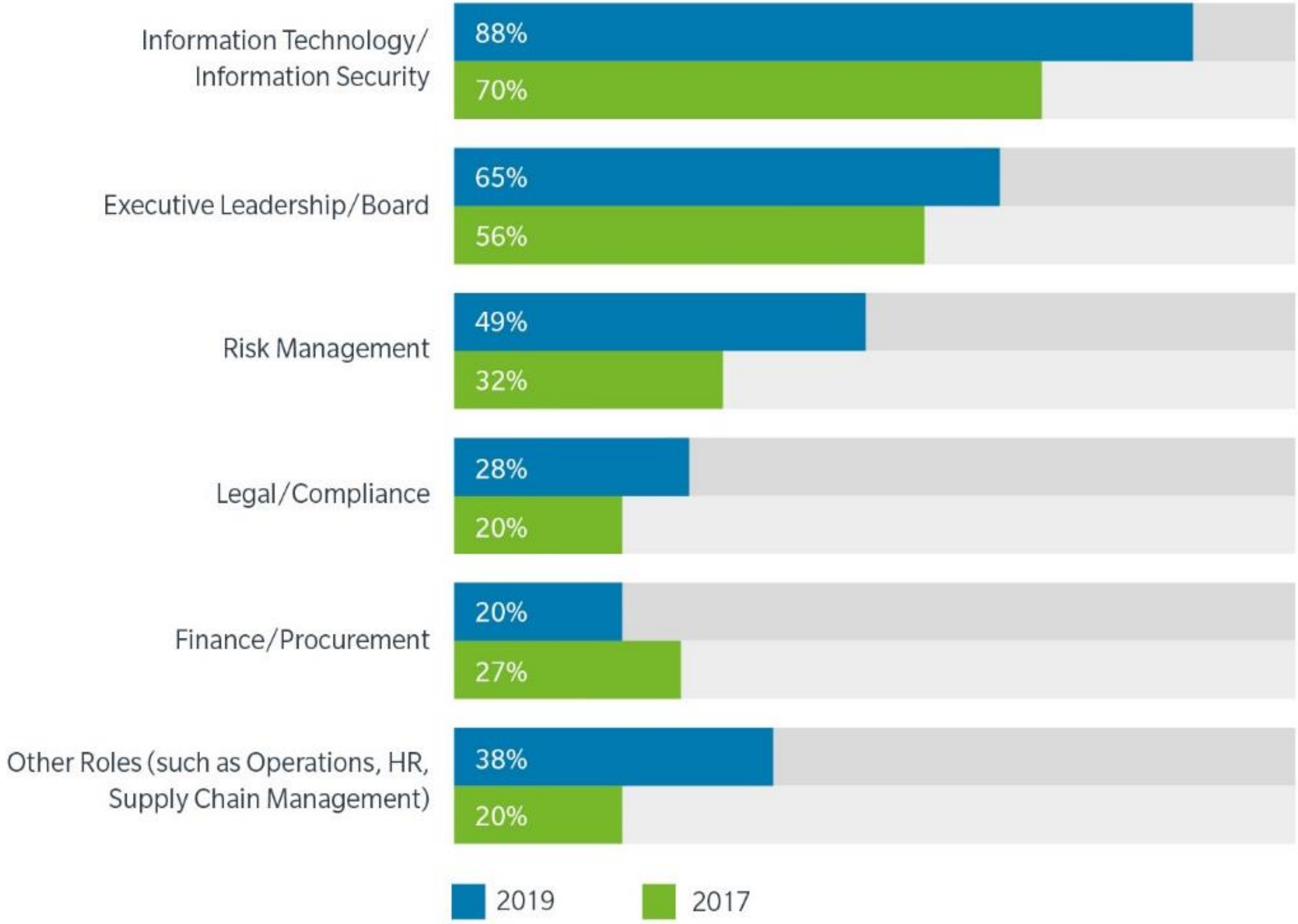


Cyber Confidence Has Declined in All Areas Since 2017
#1: Concern/Confidence Gap



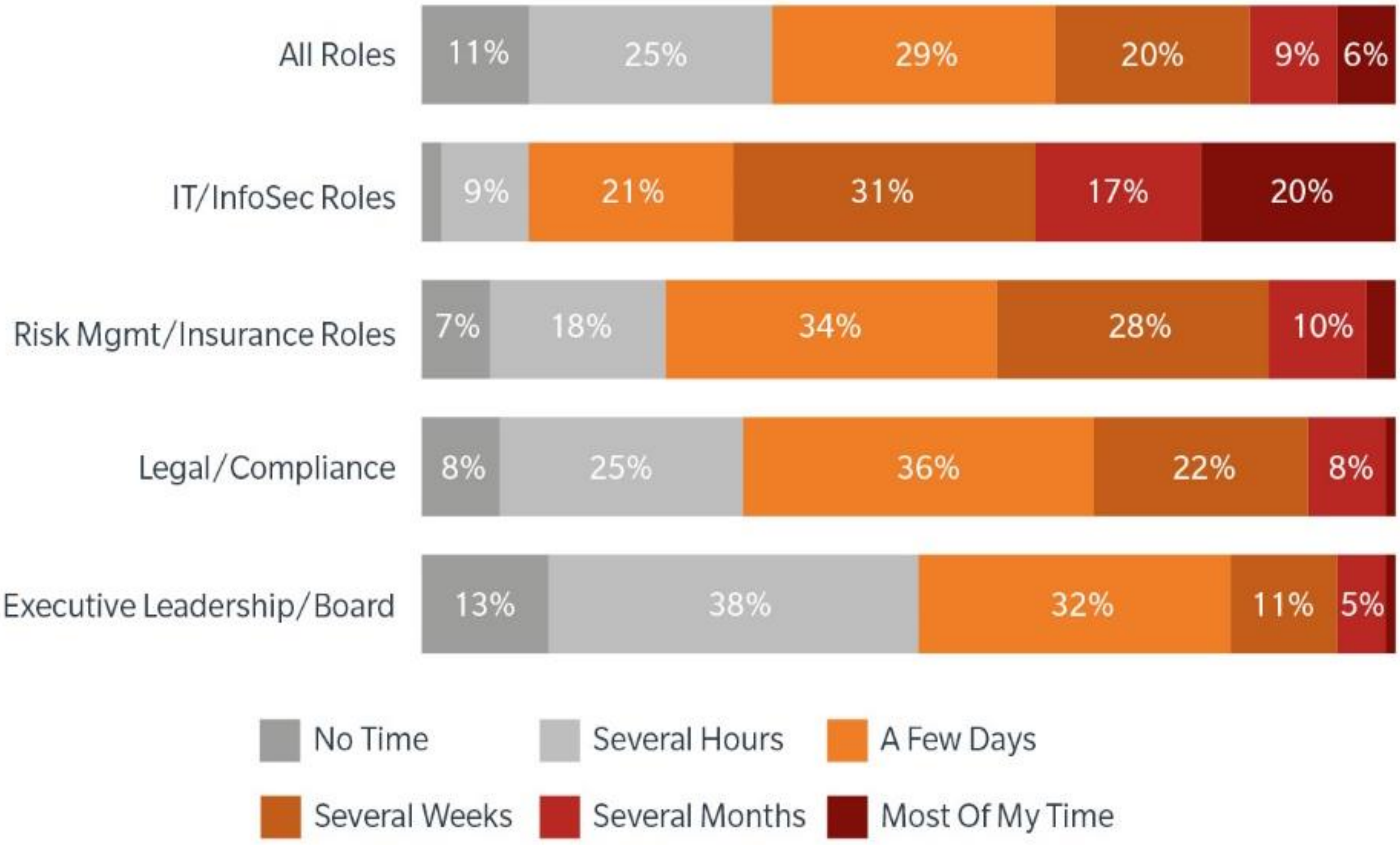
Base: All answering, excluding "don't know" responses; n=1312 (2017); n=1457 (2019)

IT/InfoSec Continue to be Seen as Owners of Cyber Risk
#2: Dissonance – Strategic Risk, Managed Tactically

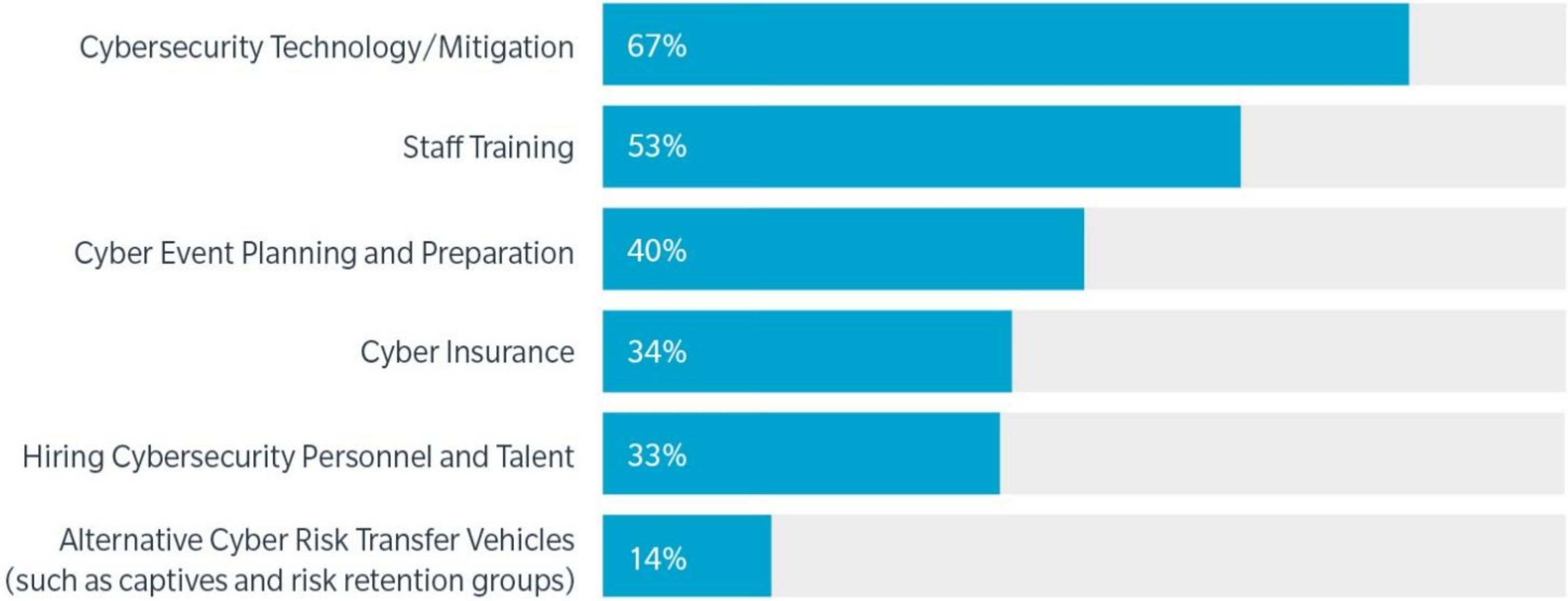


83% of Executives Spend Less Than a Few Days Per Year on Cyber Risk

#2: Dissonance – Strategic Risk, Managed Tactically

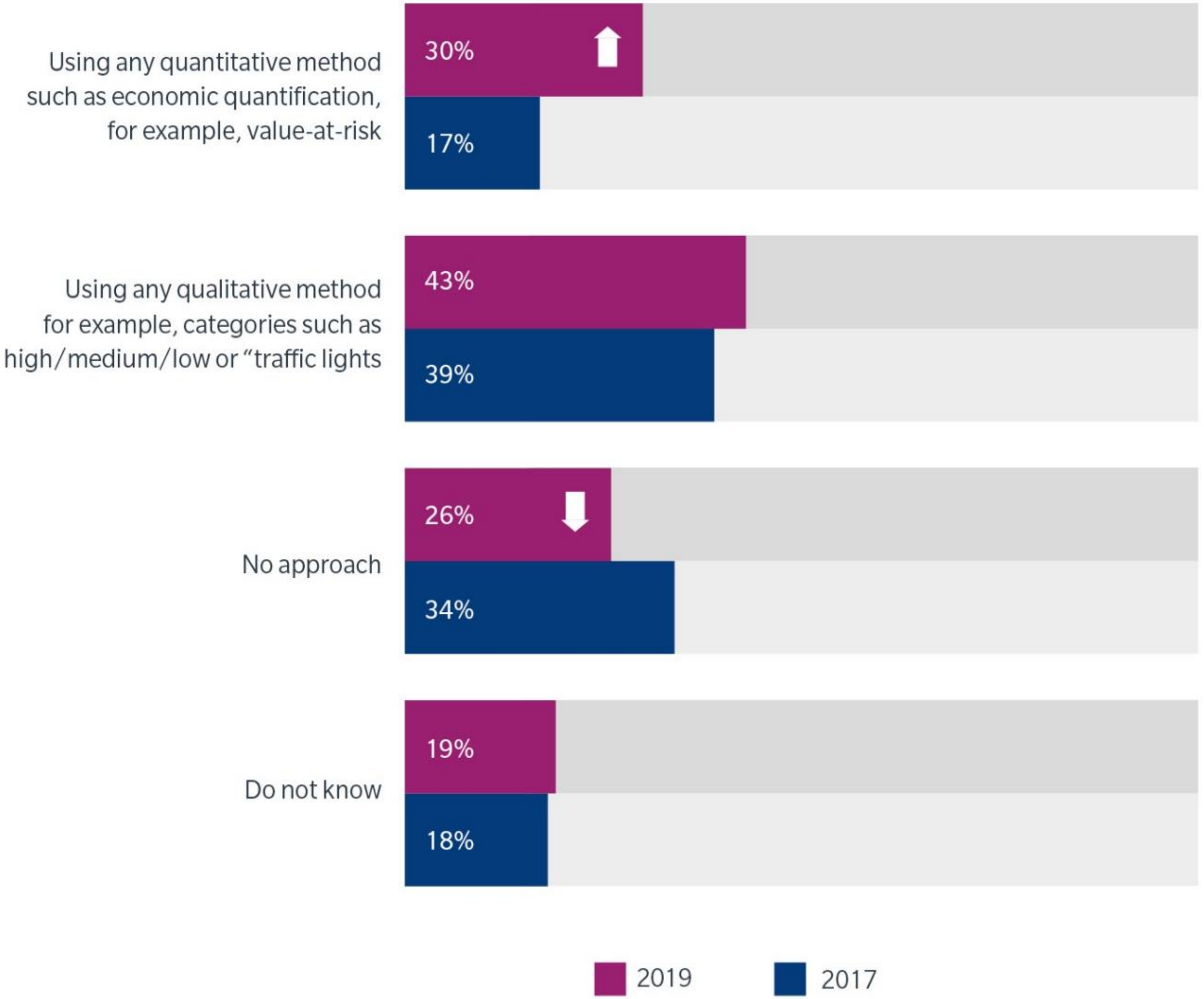


Organizations’ Future Capital Allocation Plans Emphasize Technology
#2: Dissonance – Strategic Threat, Managed Tactically



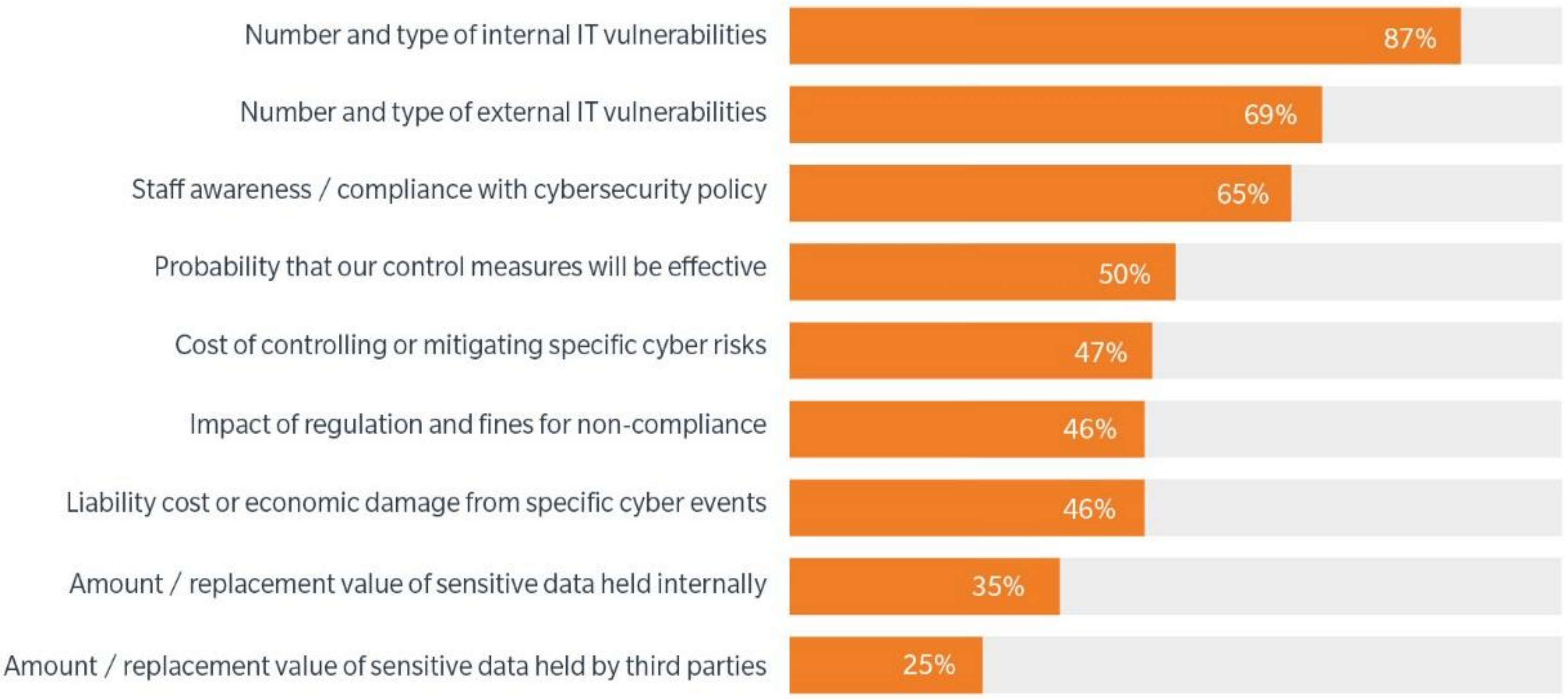
30% of Organizations Now Quantify Cyber Risk - Double that of 2017

#2: Dissonance – Strategic Threat, Managed Tactically



Risk Assessment Focuses on Technical Aspects Over Economic Cost

#2: Dissonance – Strategic Threat, Managed Tactically

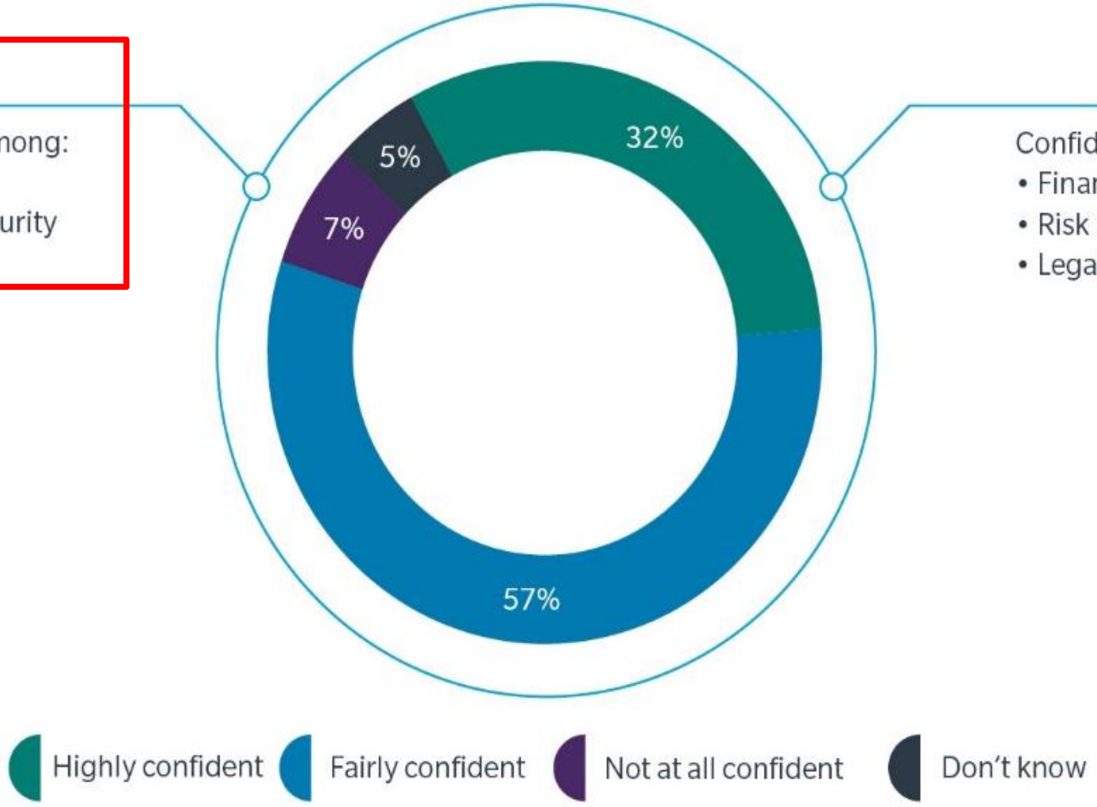


4 of 5 Say Insurance Would Cover Cyber Losses

#2: Dissonance – Strategic Threat, Managed Tactically

Confidence **lowest** among:

- C-Suite / Board
- IT / Information Security



Confidence **highest** among:

- Finance
- Risk Management
- Legal / Compliance

Recommended Actions

Build a strong cybersecurity culture.

Treat cyber risk as a strategic threat, not a technical issue. Involve all key stakeholders, not just IT/InfoSec.

C-suite engagement, ownership and attention is critical. Make cyber risk a continual board agenda item.

Apply a rigorous risk management strategy. Devote appropriate governance, prioritization, resources, and resilience-building measures.

Frame cyber risk in economic terms.

Talk dollars, not technical jargon, to express cyber risk in lingua franca of business.

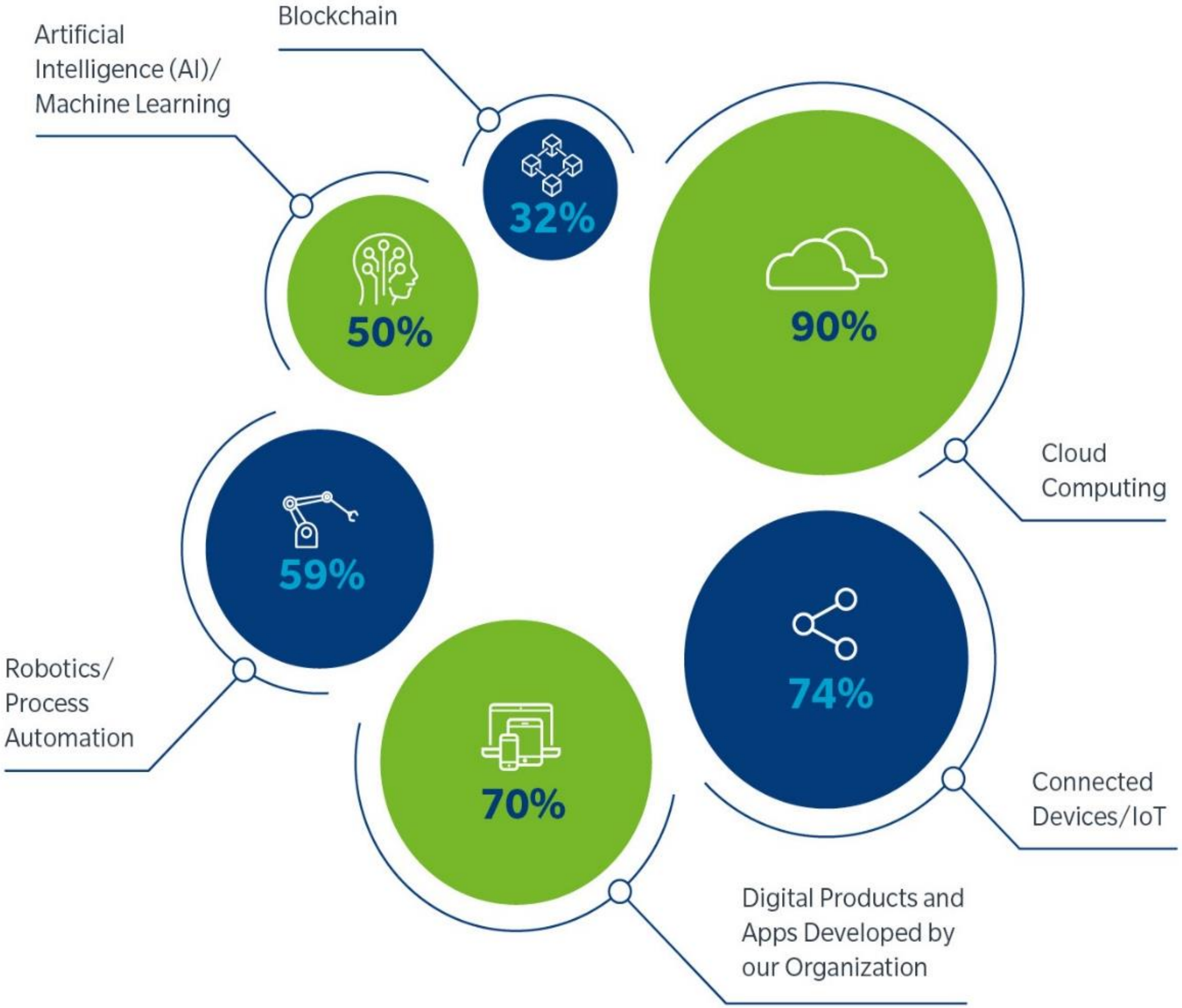
Maximize utility of every cyber dollar. Target investment to largest exposures and optimize balance of technology vs. risk transfer.

Build resilience, not just prevention.

Look beyond technology and controls – engage in planning, training, response rehearsal, and engage outside resources to build cyber resilience.

Use insurance to protect against cyber-related losses.

Most Organizations are Embracing a Range of New Technologies
#3: New Technology Risks Only Partially Understood or Evaluated



Artificial Intelligence (AI)/ Machine Learning 50%

Blockchain 32%

Cloud Computing 90%

Robotics/ Process Automation 59%

Connected Devices/IoT 74%

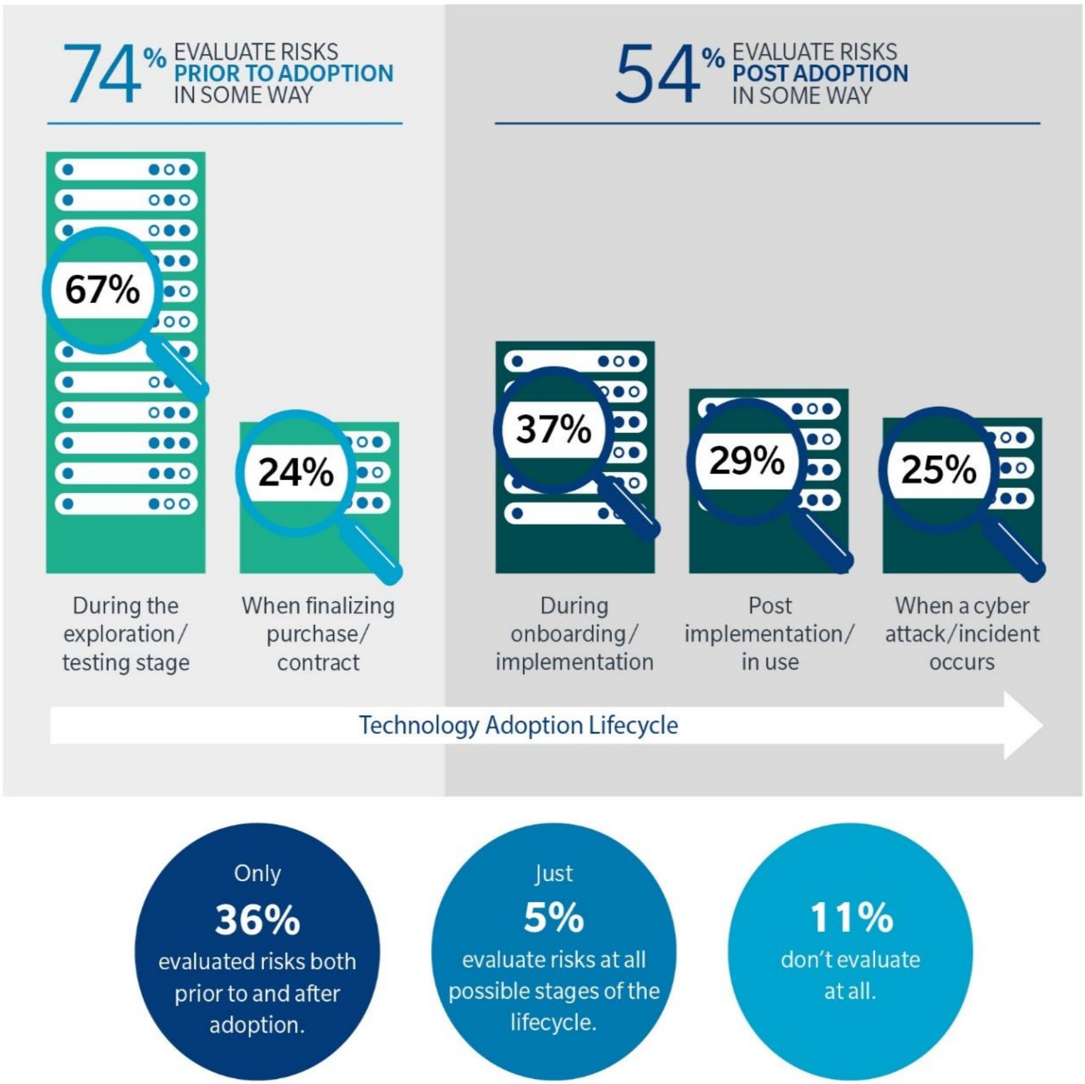
Digital Products and Apps Developed by our Organization 70%

77% have already adopted at least one of these technologies

76% are piloting or considering adopting at least one of these

Few Organizations Evaluate New Technology Risk After Adoption

#3: New Technology Risks Only Partially Understood or Evaluated



Only **36%** evaluated risks both prior to and after adoption.

Just **5%** evaluate risks at all possible stages of the lifecycle.

11% don't evaluate at all.

Recommended Actions

Continual risk assessment of new technologies.

Evaluate the risk impact of new technologies and devices before, during and after implementation – throughout the technology lifecycle.

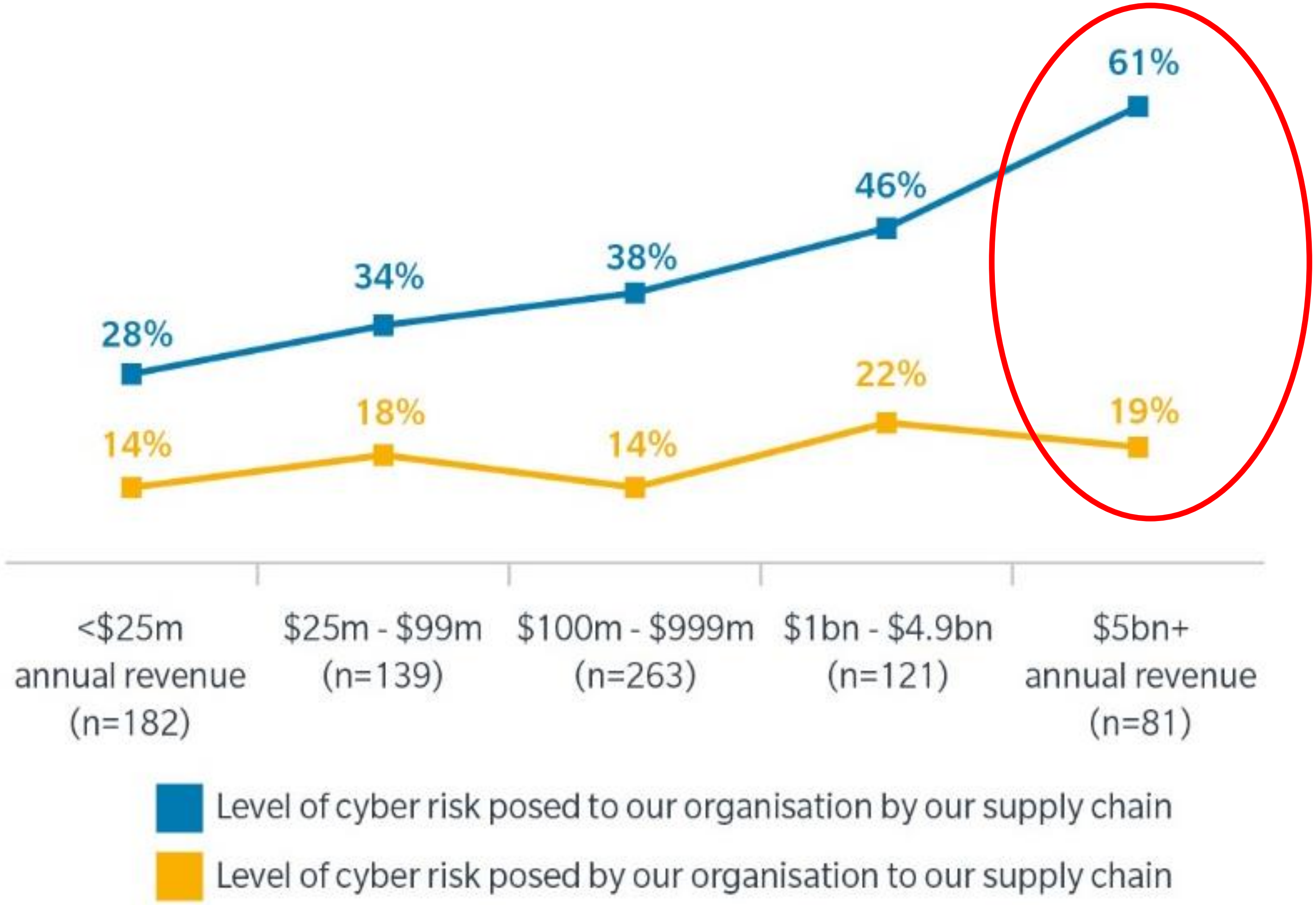
Involve key stakeholders for a holistic view.

Assessment of new technology risk – including the decision to adopt – should include risk management, IT/InfoSec, legal/compliance, and privacy/data officers, not just business/product development.

Trust but verify.

Evaluate the baked-in security of 3rd party vendor devices and technologies against your own organization’s technology footprint, cyber exposures, and business model – especially when the technology is inherent to your core operations.

Large Enterprises More Likely to Perceive Risks to Themselves
#4: Supply Chain Risk Viewed Unequally



Recommended Actions

Technological Social Responsibility.

In interconnected supply chains, risk can come from anywhere. Recognize your own organization's responsibility for supply chain integrity and security and embrace your technological social responsibility.

Engage supply chain partners and vendors in dialogue about bilateral supply chain risk and shared responsibility.

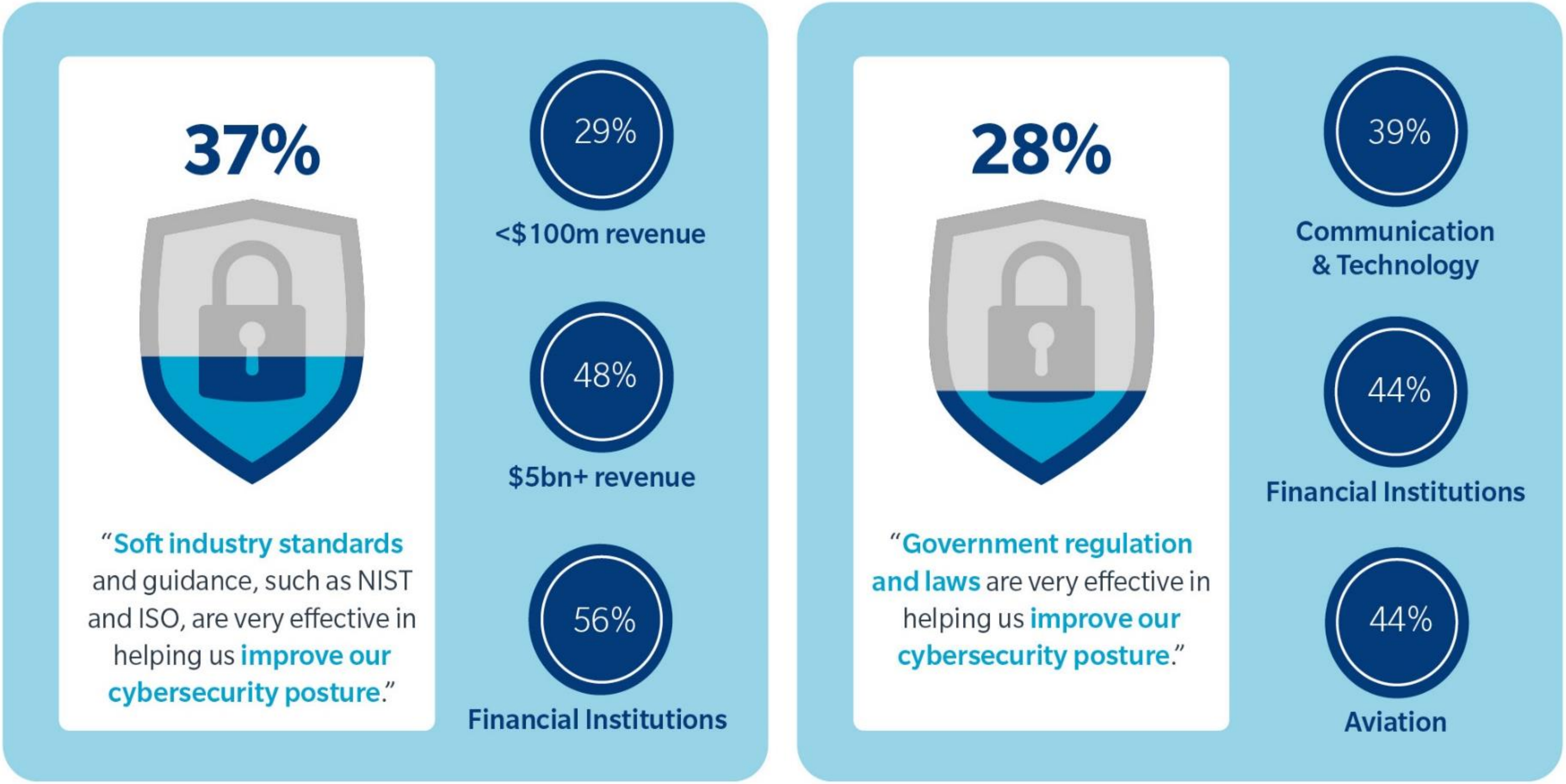
Continual assessment of 3rd party risk.

Inventory and evaluate vulnerabilities, exposures, and risks presented by your supply chain partners, vendors, and 3rd parties.

Set cybersecurity standards for your supply chain partners as rigorous as those you set for your own organization.

Require vendors and 3rd parties to have adequate insurance coverage for cyber liabilities and events they may present to your organization.

Cyber Regulation or Industry Standards Not Viewed as Very Effective
#5: Limited Appreciation for Government Involvement



37%

"**Soft industry standards** and guidance, such as NIST and ISO, are very effective in helping us **improve our cybersecurity posture**."

29%
<$100m revenue

48%
$5bn+ revenue

56%
Financial Institutions

28%

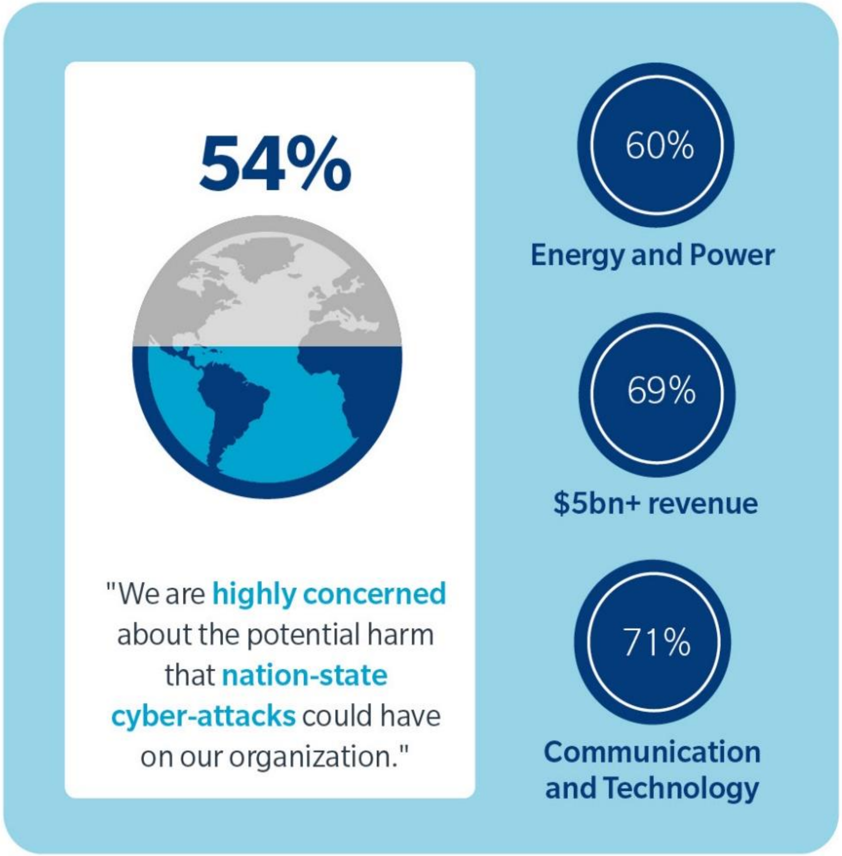
"**Government regulation and laws** are very effective in helping us **improve our cybersecurity posture**."

39%
Communication & Technology

44%
Financial Institutions

44%
Aviation

…With the Exception of Support Against Nation-State Attacks
#5: Limited Appreciation for Government Involvement



54%

"We are **highly concerned** about the potential harm that **nation-state cyber-attacks** could have on our organization."

60%

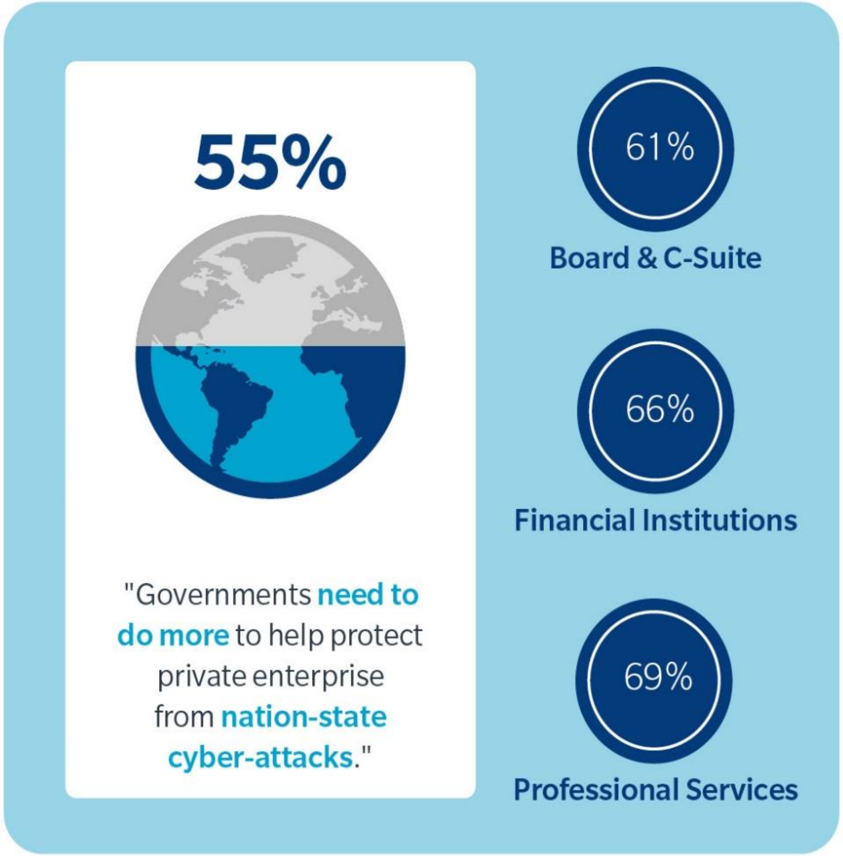
Energy and Power

69%

$5bn+ revenue

71%

Communication and Technology



55%

"Governments **need to do more** to help protect private enterprise from **nation-state cyber-attacks**."

61%

Board & C-Suite

66%

Financial Institutions

69%

Professional Services

Recommended Actions

Cyber regulation is here to stay, and the stakes are rising.

Global regulatory momentum is creating broad and rigorous new requirements for data and privacy protections, and creating new expectations for regulatory disclosure, management awareness, and public reporting.

Stay aware of new and evolving regulation, such as CCPA, and review your data practices and controls, and your insurance policies, to ensure regulatory compliance and coverage sufficiency.

Ensure c-suite and board members fully understand expectations and requirements of new regulations as SEC Public Company Cybersecurity Disclosure, and ensure adequate D&O coverages are in place.

Nation-State Attacks May Require Public/Private Partnerships

The interconnected nature of technology, infrastructure, and commerce means that no organization is an island against cyber threats – the security perimeter now extends to the broader economic ecosystem. Engage with government and industry bodies to help improve cybersecurity for all, especially in the face of existential threats that affect every company.

2019 GLOBAL CYBER RISK PERCEPTION SURVEY

SUMMARY

In Conclusion…What Should Organizations Do Now? Do Better?

Considerable dissonance between high cyber concerns and non-strategic cyber risk management.	Organizations need to build a **strong cybersecurity culture** with appropriate governance, prioritization, resources, ownership, and resilience-building actions.
Cyber risk quantification is essential to drive well-informed capital allocation decision.	**Economic expression of cyber risk** helps target spending to largest exposures and optimize investment balance in technology vs. risk transfer.
New technologies are transforming business models but can bring unexpected risks.	**Ongoing, regular risk assessment** should occur throughout the technology lifecycle.
Supply chain risk is collective with interconnected supply chains.	Businesses need to recognize a **shared technological social responsibility** that includes 3rd parties.
Nation-state threats are critical risks that can't be managed by enterprise alone.	Stay abreast of evolving cyber regulations, and look for **opportunity for risk management partnerships** between government and private enterprise.
Cyber insurance is an effective, essential risk management tool.	Organizations should use insurance to **protect against cyber-related losses**.

Thank you, panelists!

cyber.risk@marsh.com

Joram Borenstein
General Manager
Cyber Security Solutions Group
Microsoft

Tom Reagan
US Cyber Practice Leader
Marsh

Kevin Richards
Global Head
Marsh Cyber Risk Consulting

Sarah Stephens
UK Cyber Practice Leader
Marsh

How Organizations are Managing Cyber Risk in a Fast-Changing Business Environment:

Marsh Microsoft 2019 Cyber Survey Results

Visit www.advisenltd.com at the end of this webinar to download:

- Copy of these slides
- Recording of today's webinar