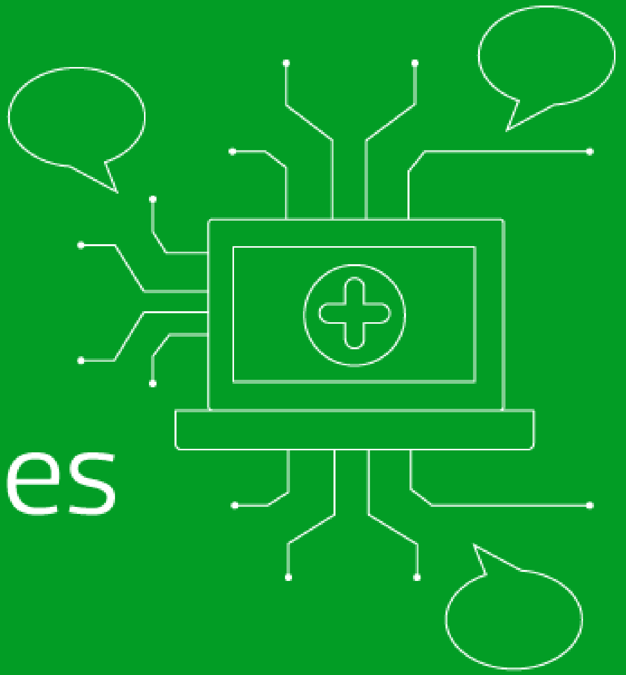
HEALTH CARE WEBCAST SERIES

SPRING 2021

MAY 20, 2021

RSM | HEALTH CARE WEBCAST SERIES

Uncovering hidden IT and security risks: Lessons from the trenches



Thurs., May 20 | 1:00 P.M. – 2:30 P.M. EST

RSM

Agenda

Topic	Minutes
Introductions, Objectives & About RSM	08 Minutes
Pandemic Impacts	15 Minutes
Risks with Cloud Providers and Your Managed Service Provider	15 Minutes
Integrating Security Risk Management With Enterprise Risk Management	15 Minutes
Effective Governance Committee	15 Minutes
Evaluating Adequacy of IT Spend	10 Minutes
Questions & Answers	10 Minutes

RSM Introductions

TODAY'S FACILITATOR

Jessika Garis

Director | Tampa, Florida
Risk Advisory Services and
Health Care Senior Analyst
jessika.garis@rsmus.com
+1 813 316 2247

12+ years of experience

Served as interim Chief Compliance Officer. Recognized by *Consulting Magazine* as a Women Leader in Consulting - Future Leader category

Certified in Healthcare Compliance (CHC),
HCCA Member
Institute of Internal Auditors Member

PRESENTER

Greg Vetter

Principal | New York City, New York
National HIPAA and HITRUST Leader
Security Privacy & Risk Consulting
greg.vetter@rsmus.com
+1 212 372 1624

20+ years of experience

Completed HIPAA/HITECH compliance assessments for payers and health systems ranging from single hospitals to greater-than-20-hospital systems with over 400 medical practices

HITRUST Certified CSF
Practitioner (CCSFP)

PRESENTER

Paul Fountain, MBA

Director | Dallas, Texas
National ePHI Leader
Security Privacy & Risk Consulting
paul.fountain@rsmus.com
+1 817 312 9733

24+ years of experience

Specializes in: HITRUST, HIPAA and NIST 800-171 and 53 series and CSF

HITRUST Certified CSF
Practitioner (CCSFP)
Certified Information Systems Security
Professional (CISSP)

PRESENTER

Ron Ritenour, MBA

Manager | Dallas, Texas
National HIPAA Methodology Leader
Security Privacy & Risk Consulting
ron.ritenour@rsmus.com
+1 469 391 9096

18+ years of experience

Specializes in: Cybersecurity, HIPAA regulatory compliance, NIST CSF, 800-171 and 53 series, and CIS CSC

Healthcare Information Security and
Privacy Practitioner (HCISPP)
Certified Information Systems Auditor
(CISA)

RSM

Objectives

After attending this webcast, you will be able to:

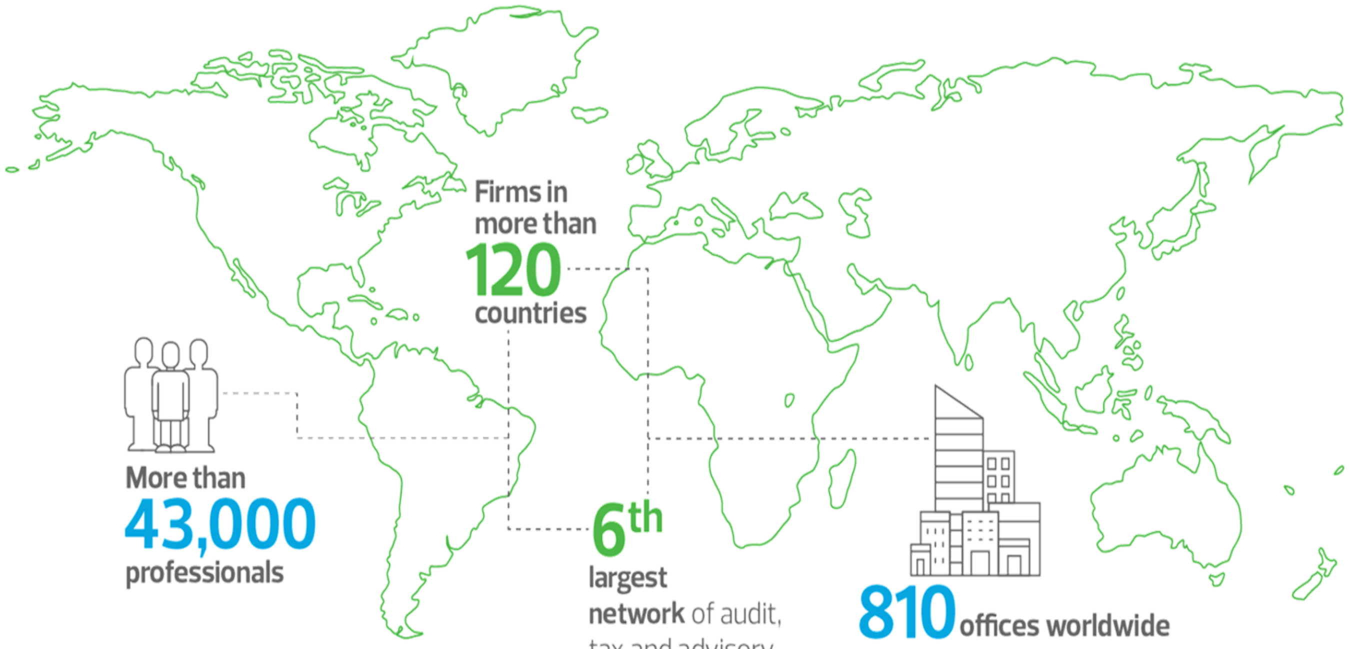
- Uncover risks through sharing insights
- Identify and understand new risks in your ever-changing environment
- Summarize effective strategies for managing risk

If you are looking to **streamline risk compliance efforts** you are in good company.

More and more organizations are adopting **multiple security and privacy frameworks**, as well as **regulatory requirements**, under ONE information security program.

About RSM

RSM International is a **global network** of independent audit, tax and advisory firms.

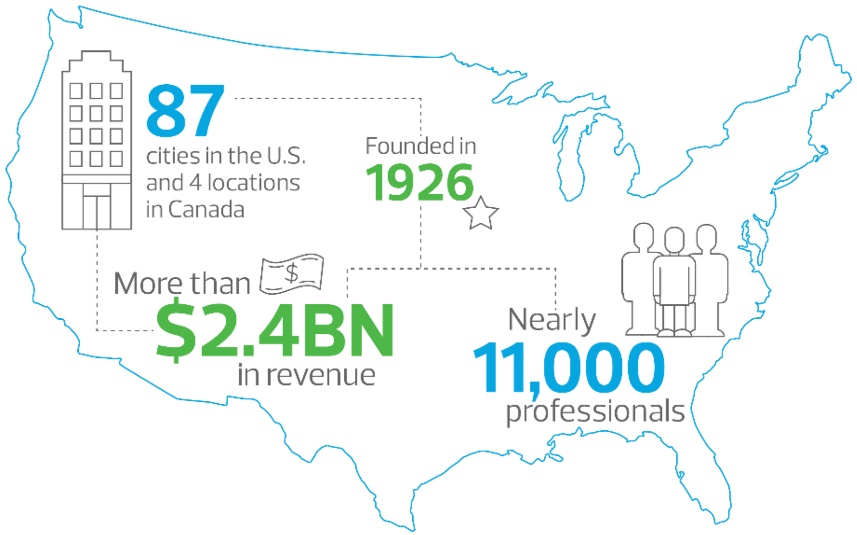


Firms in more than **120** countries

More than **43,000** professionals

6th largest network of audit, tax and advisory firms globally

810 offices worldwide



87 cities in the U.S. and 4 locations in Canada

Founded in **1926**

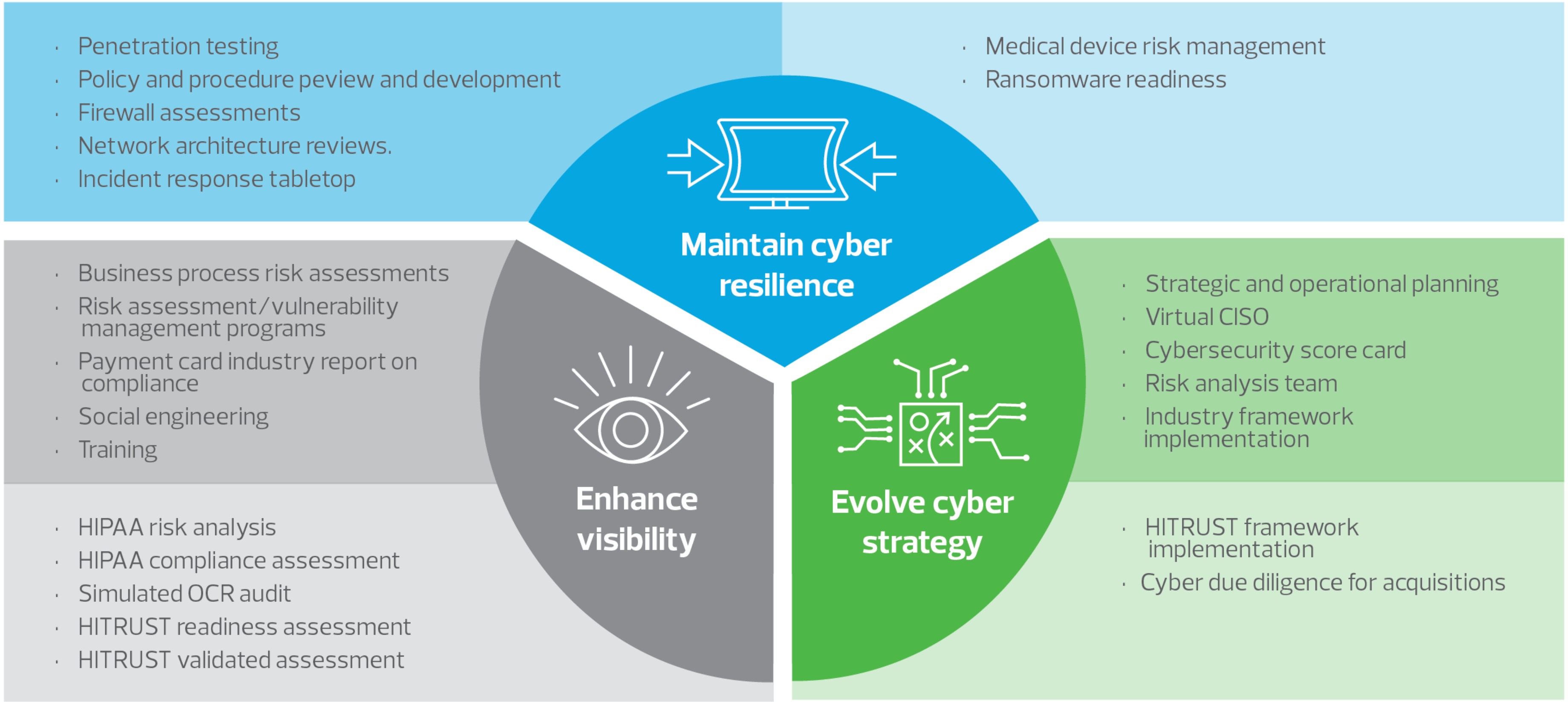
More than **$2.4BN** in revenue

Nearly **11,000** professionals

RSM US LLP is the **leading provider** of audit, tax and consulting services focused on the **middle market.**

About RSM

Security, privacy and risk services for health care



Maintain cyber resilience

- Penetration testing
- Policy and procedure peview and development
- Firewall assessments
- Network architecture reviews.
- Incident response tabletop

- Medical device risk management
- Ransomware readiness

Enhance visibility

- Business process risk assessments
- Risk assessment/vulnerability management programs
- Payment card industry report on compliance
- Social engineering
- Training

- HIPAA risk analysis
- HIPAA compliance assessment
- Simulated OCR audit
- HITRUST readiness assessment
- HITRUST validated assessment

Evolve cyber strategy

- Strategic and operational planning
- Virtual CISO
- Cybersecurity score card
- Risk analysis team
- Industry framework implementation

- HITRUST framework implementation
- Cyber due diligence for acquisitions

RSM Webcast Perspective

RSM US MIDDLE MARKET BUSINESS INDEX

CYBERSECURITY

SPECIAL REPORT

2021

- 700 middle market executives recruited by The Harris Poll and surveyed in Q1 of 2021
- Middle market economic index developed by RSM in Collaboration with Moody's Analytics representing companies with a revenue of $10 million to $1 billion.
- Co-sponsored by the U.S. Chamber of Commerce

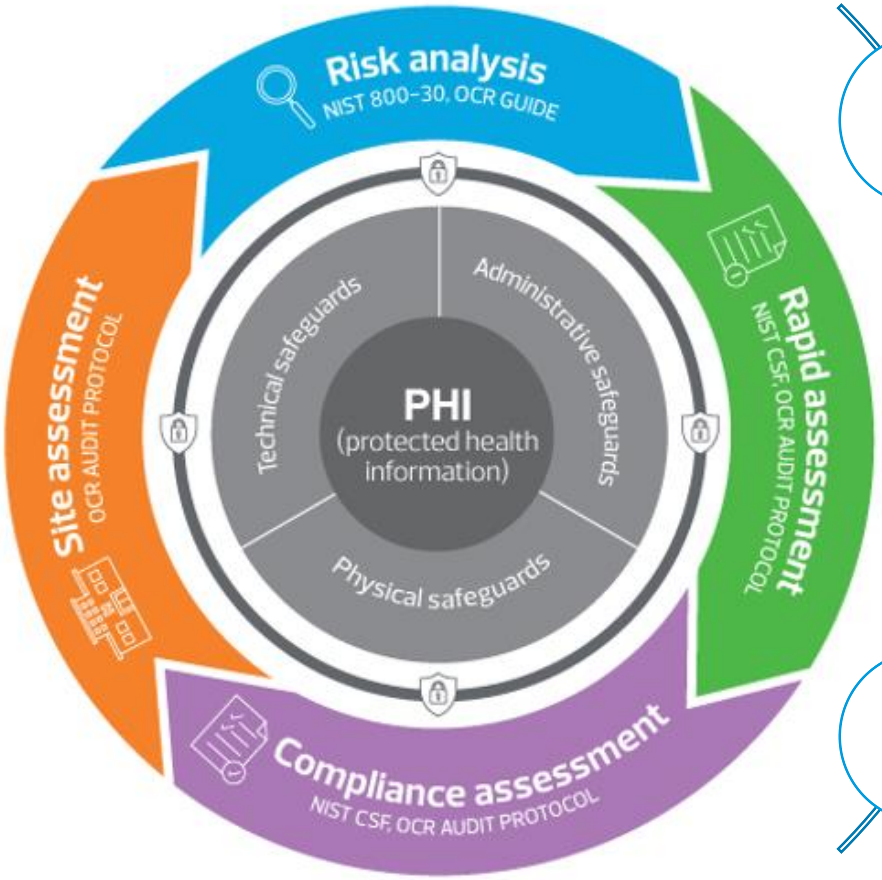
To download a copy, please visit: https://rsmus.com/economics/rsm-middle-market-business-index-mmbi.html

RSM Webcast Perspective

- 2020/2021 changes have been impactful for all businesses
- *Information protection and security* are not exempt
- These challenges have highlighted the need for better security practices
- RSM's Security and Privacy group works across all industries, and is deeply experienced with healthcare
- RSM teams have been side by side with our clients managing the challenges of the past year
- This Webcast allows us to provide risk management insights in the context of recent events

About RSM

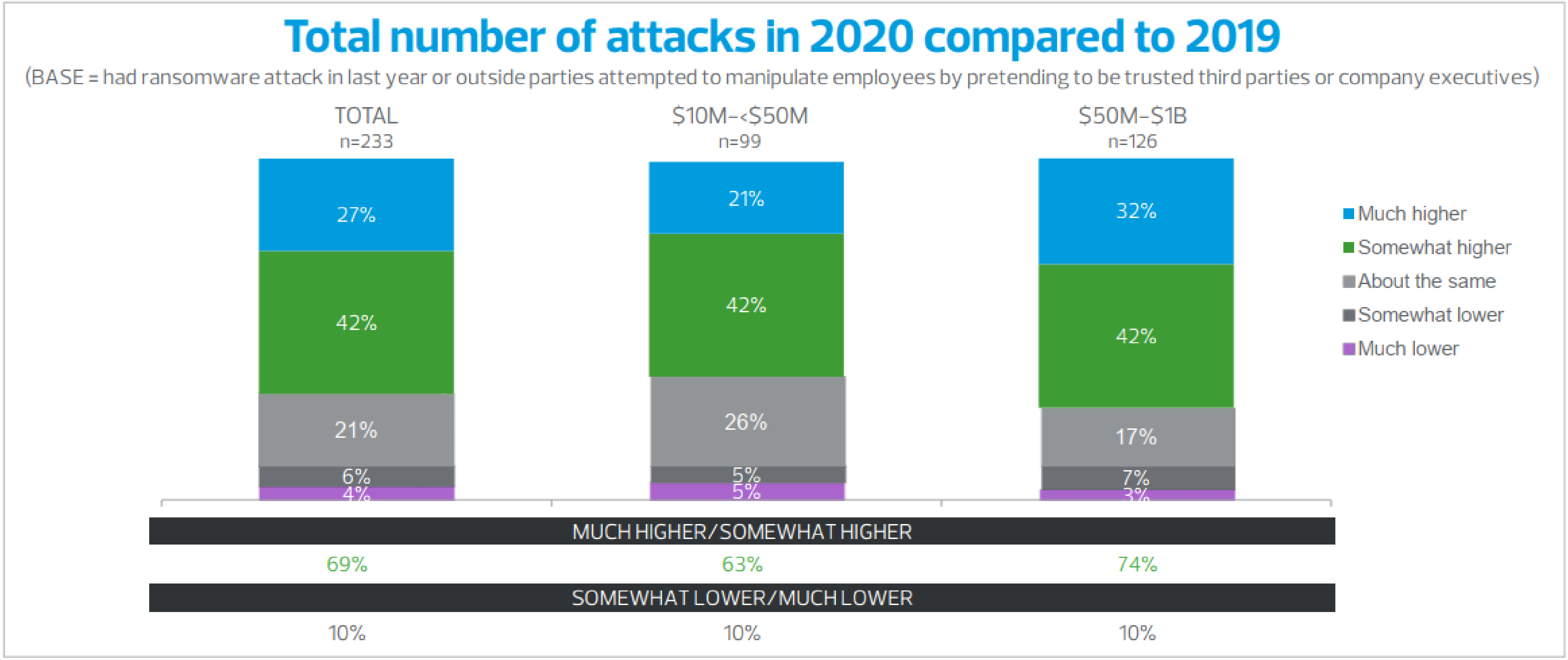
RSM HIPAA compliance methodology



- Information security risk analysis
- Evaluating policy and program design
- Evaluate control design & effectiveness
- Security safeguards operationalized across the entity

PANDEMIC IMPACTS

Pandemic Impacts



Total number of attacks in 2020 compared to 2019

(BASE = had ransomware attack in last year or outside parties attempted to manipulate employees by pretending to be trusted third parties or company executives)

MUCH HIGHER/SOMEWHAT HIGHER		
69%	63%	74%

SOMEWHAT LOWER/MUCH LOWER		
10%	10%	10%

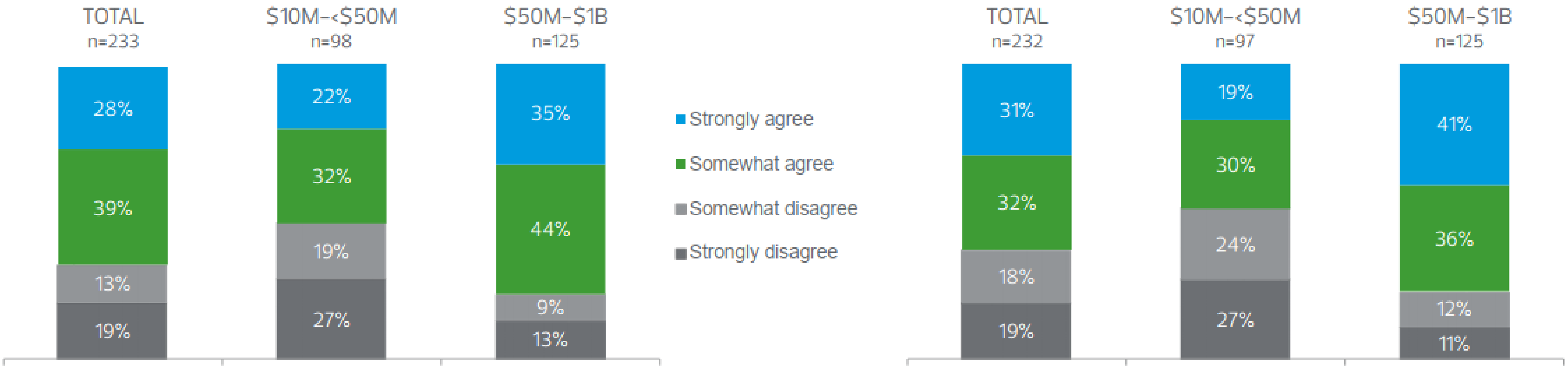
Pandemic Impacts

Level of agreement attacks result of Covid-19 pandemic

(BASE = had ransomware attack in last year or outside parties attempted to manipulate employees by pretending to be trusted third parties or company executives)

My business experienced attacks as an indirect result of the COVID-19 pandemic (e.g., attempts to exploit vulnerabilities due to more employees working remotely)

My business experienced attacks as a direct result of the COVID-19 pandemic (e.g., social engineering or phishing emails using COVID-related pretenses to gain access to your systems or data)



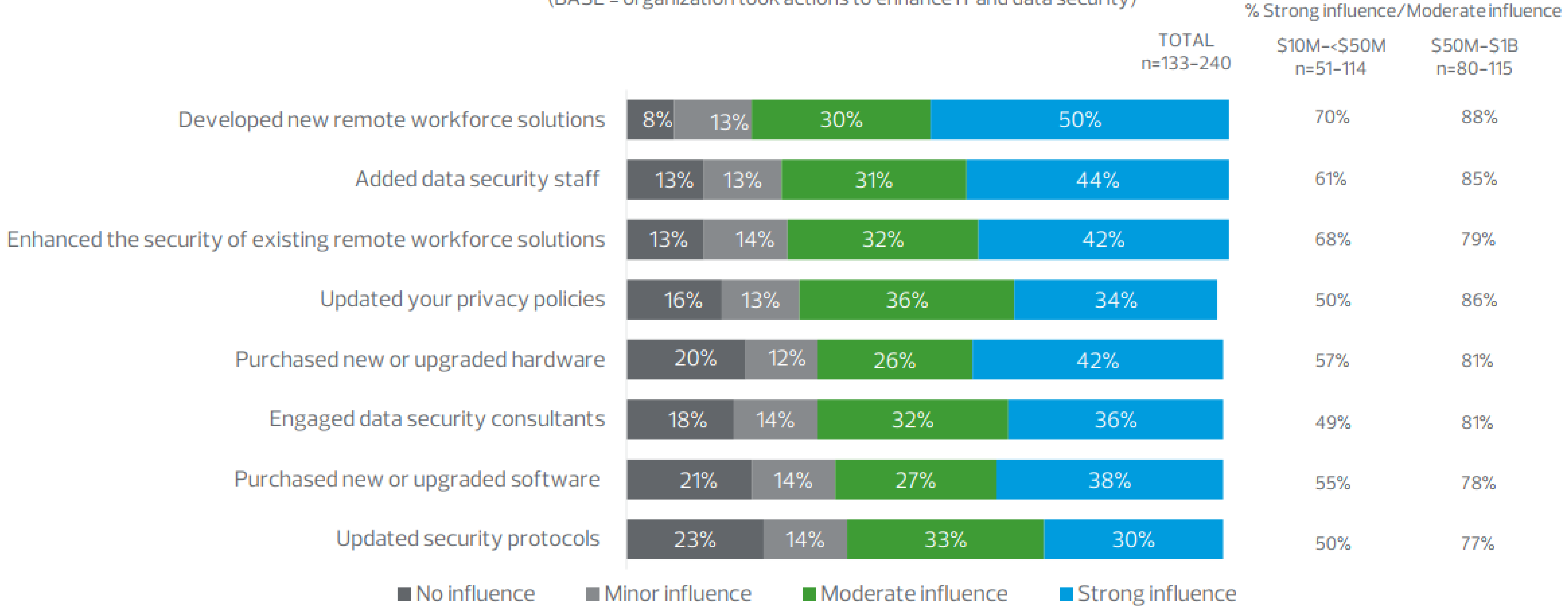
STRONGLY AGREE/SOMEWHAT AGREE		
67%	54%	79%
SOMEWHAT DISAGREE/STRONGLY DISAGREE		
32%	46%	22%

STRONGLY AGREE/SOMEWHAT AGREE		
63%	49%	77%
SOMEWHAT DISAGREE/STRONGLY DISAGREE		
37%	51%	23%

Pandemic Impacts

Level of influence that security concerns with Covid-19 had on actions to enhance IT and data security

(BASE = organization took actions to enhance IT and data security)



Pandemic Impacts

Many middle market companies responded to the challenges of the pandemic environment by making adjustments to their security posture. For instance, among companies in the survey that took actions to enhance their own IT and data security in response to well-publicized breaches, security concerns with COVID-19 were either a moderate or strong influence on 80% of companies that developed new workforce solutions. Comparatively, the pandemic had an influence on 75% of companies that added data security staff and 74% of organizations that enhanced the security of existing remote workforce solutions.

Security concerns with COVID-19 were either a moderate or strong influence on

80%

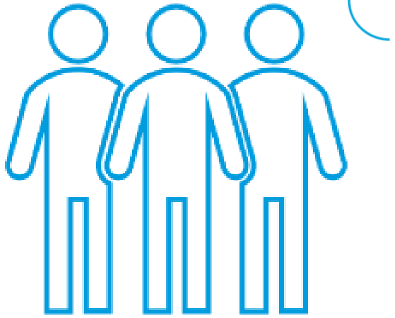
of companies that developed new workforce solutions

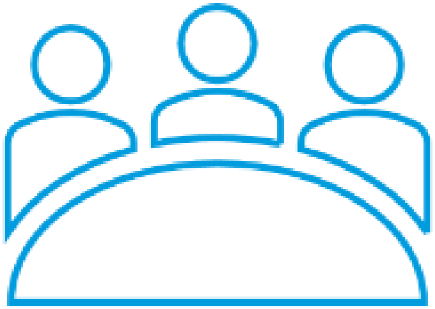
RISKS WITH CLOUD PROVIDERS AND YOUR MANAGED SERVICE PROVIDER

Risks with cloud providers and your managed service provider

- Companies are increasingly using cloud services to support business requirements
  - SaaS, PaaS, IaaS
  - Predominately virtual private clouds
  - Policies and procedures don’t keep apace with organizational strategies
- Companies are increasingly supplementing their IT and security competencies with a MSP/MSSP
  - Critical IT and security processes such as threat detection and incident response
  - Roles and responsibilities don’t keep apace with growing need to supplement capabilities
- Outsource the process but not the risks
  - Security due diligence
  - Enterprise risk management process
  - Third-party risk management process

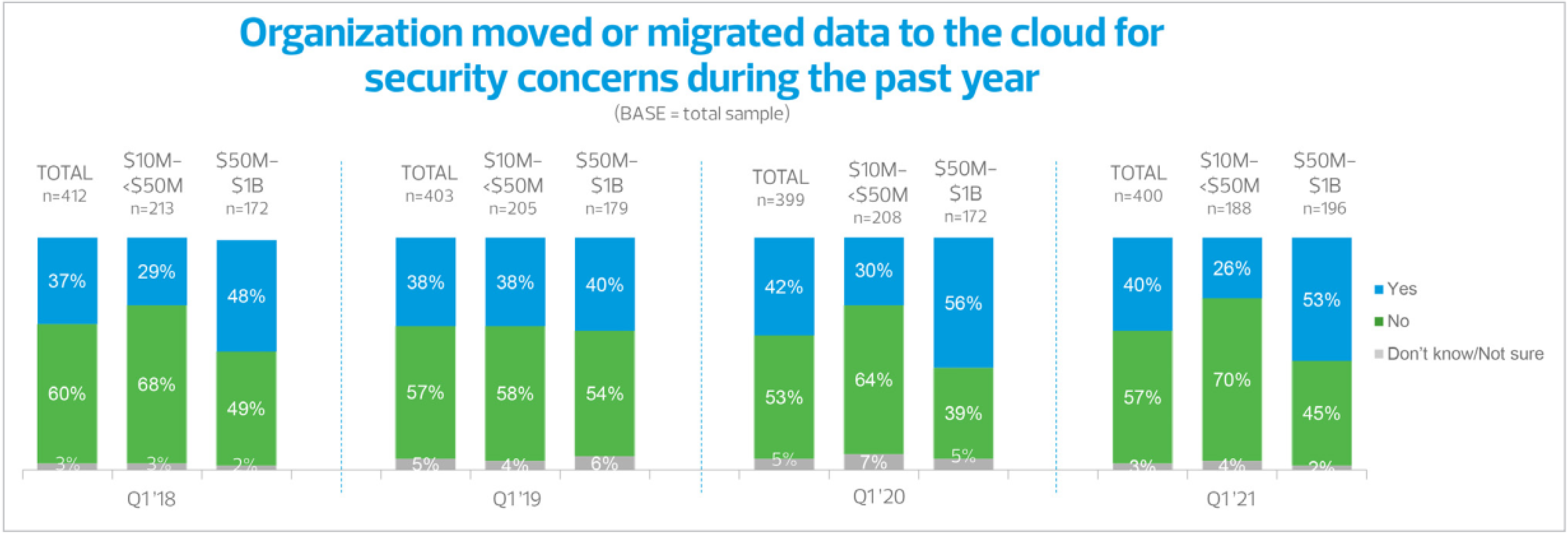
54% of executives who depend on the cloud believe the **data migrated to the cloud is much more secure**





RSM

Risks with cloud providers and your managed service provider



Organization moved or migrated data to the cloud for security concerns during the past year

(BASE = total sample)

Risks with cloud providers and your managed service provider

Cloud shared responsibilities matrix

	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Security, Governance, Risk, and Compliance (GRC)	⬜	⬜	⬜
Data Security	⬜	⬜	⬜
Application Security	⬜	⬜	🟩
Platform Security	⬜	🟩	🟦
Infrastructure Security	🟩	🟦	🟦
Physical Security	🟦	🟦	🟦

⬜ Consumer Responsibility 🟩 Shared Responsibility 🟦 CSP Responsibility

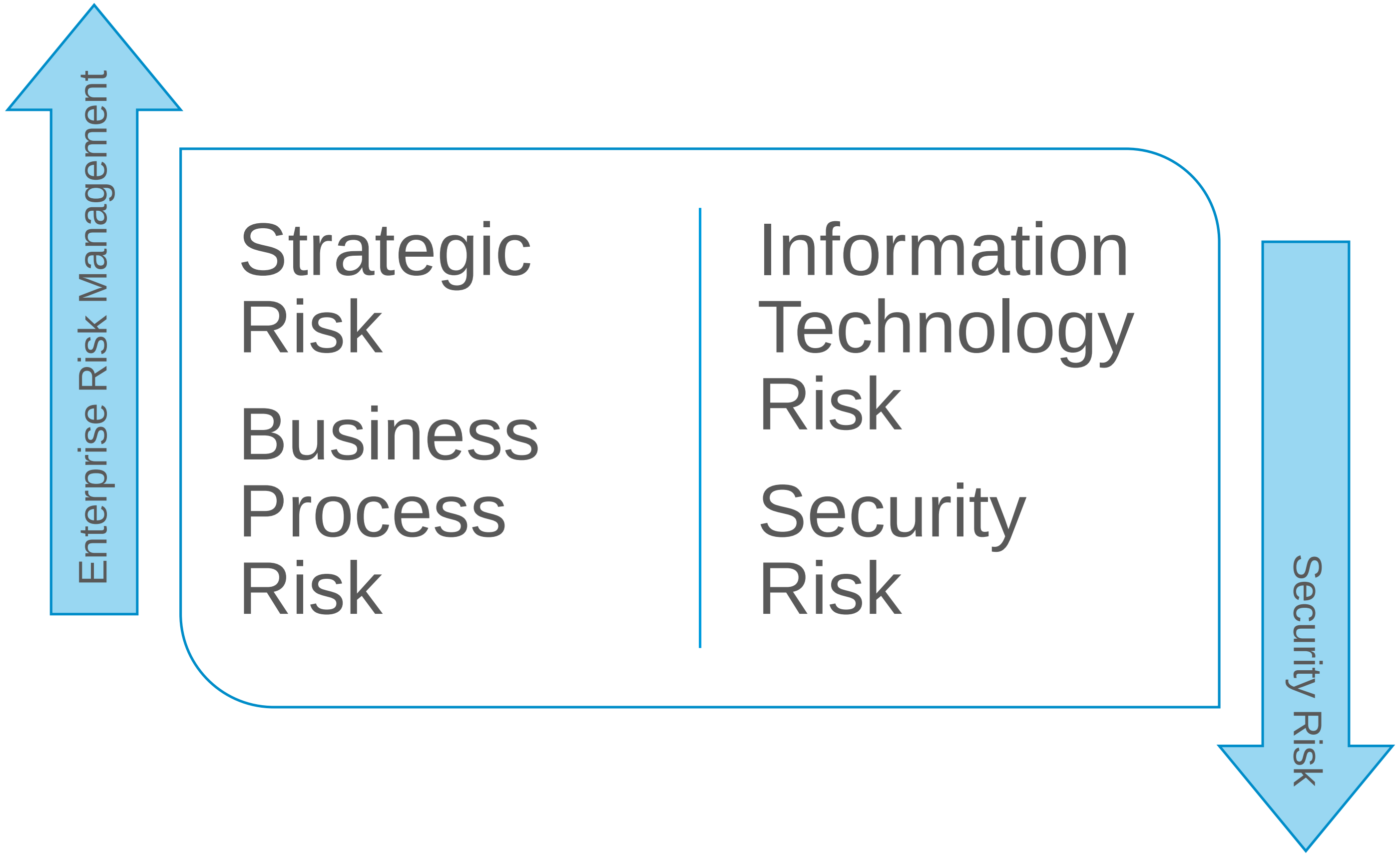
Risks with cloud providers and your managed service provider

- Updating contracts and establishing service level agreements
  - Ensure contracts are updated to include current services with a third party partner
  - Ensure adequate SLAs are defined based on business requirements
  - Ensure sanctions are appropriate for ensure SLA adherence
- Know what you are paying for
- Cloud services agreement
  - Security and data privacy
    - Cloud service provider's responsibilities
    - Data privacy
    - Cloud consumer's responsibilities
      - Your content
      - Your security and backups
      - Login credentials and account keys
      - End users

INTEGRATING SECURITY RISK MANAGEMENT WITH ENTERPRISE RISK MANAGEMENT

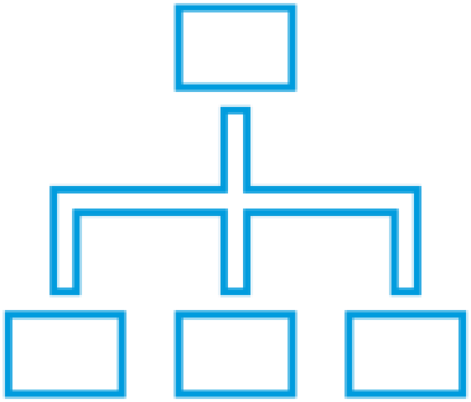
Integrating security risk management with enterprise risk management

- IT decisions made within the technology environment
- Security decisions made with the security environment
- Risk management decisions need to be viewed holistically
- Risk treatment strategies need to be made by executive management, especially when significant risk is accepted



Integrating security risk management with enterprise risk management

- Aligning risk acceptance processes
  - Integrated with security governance processes
  - Policies and procedures
  - Risk acceptance forms
  - Risk acceptance process (set acceptance frequencies)
  - Risk acceptance review process (periodically)
- Reduce shadow IT risks
  - Reduce opportunities to circumvent polices and procedures
  - ARBs don’t see everything
  - Leverage deployed security technology

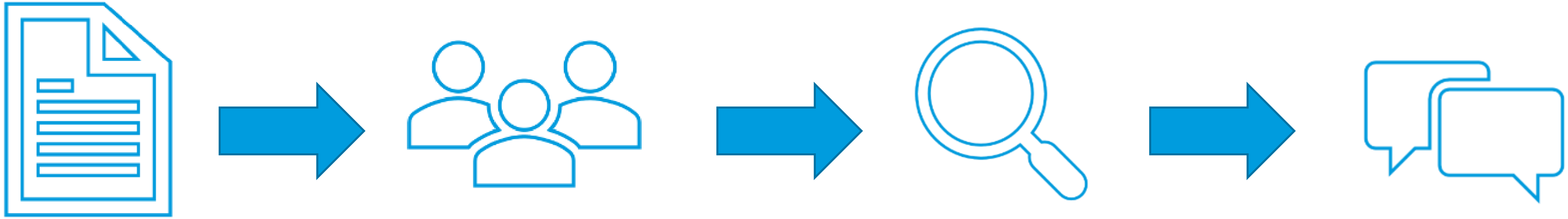


EFFECTIVE GOVERNANCE COMMITTEE

Effective Governance Committee

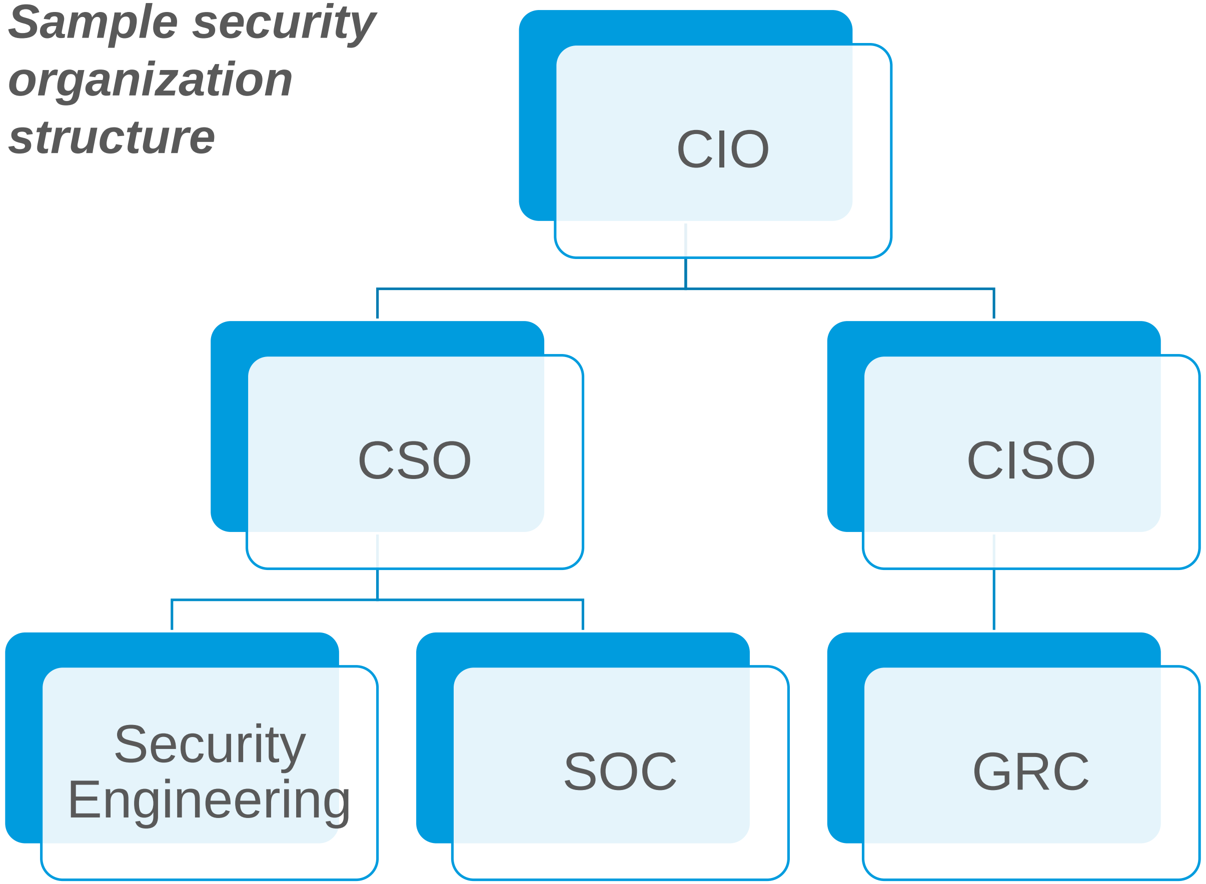
Implementing effective governance:

- Establish an effective committee charter
- Ensure affective committee composition
- Governance of policy oversight
- Mid-management risk review
- Document accountability
- Act on roles and responsibilities



Effective Governance Committee

Sample security organization structure



Effective Reporting Structures

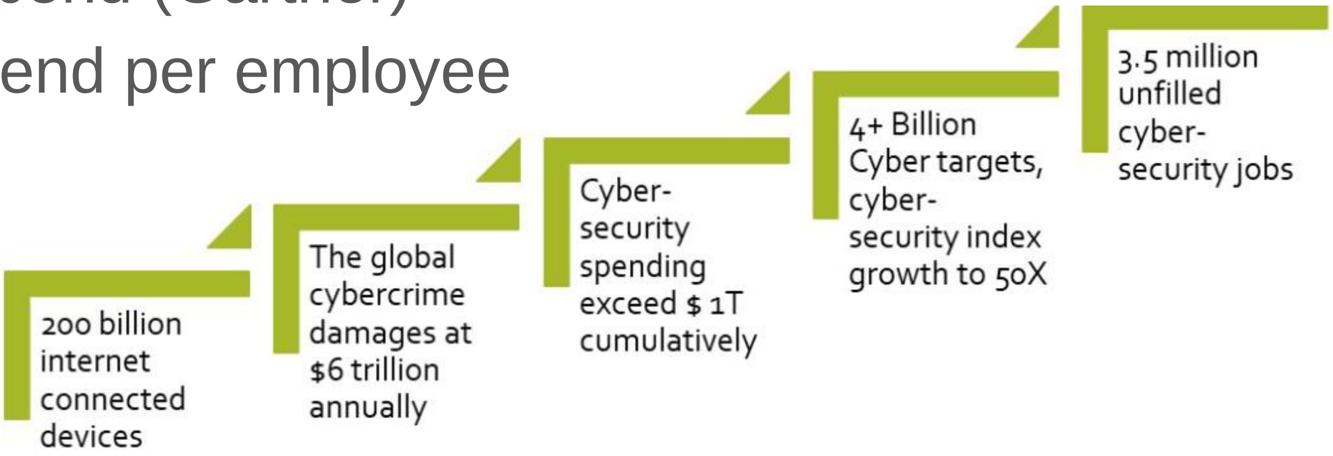
- Implement:
  - Executive sponsorship
  - Direct lines of communication with C-Suite
  - Sufficient budget strategy
  - Collaboration among teams
  - Ensuring the correct roles are assigned
- Avoid:
  - Appearance of conflicts of interests
  - Duplication of effort
  - Ineffective communication channels

EVALUATING ADEQUACY OF IT SPEND

RSM

Evaluating adequacy of IT spend

- Evaluating IT spend
  - Industry average 5% security team size against IT employee group (Gartner)
  - Industry Average IT spend 3.49% of revenue (Deloitte/WSJ)
  - Security spend 4.9% of IT Spend (Gartner)
  - Industry average security spend per employee spend $388 (Gartner)



200 billion internet connected devices

The global cybercrime damages at $6 trillion annually

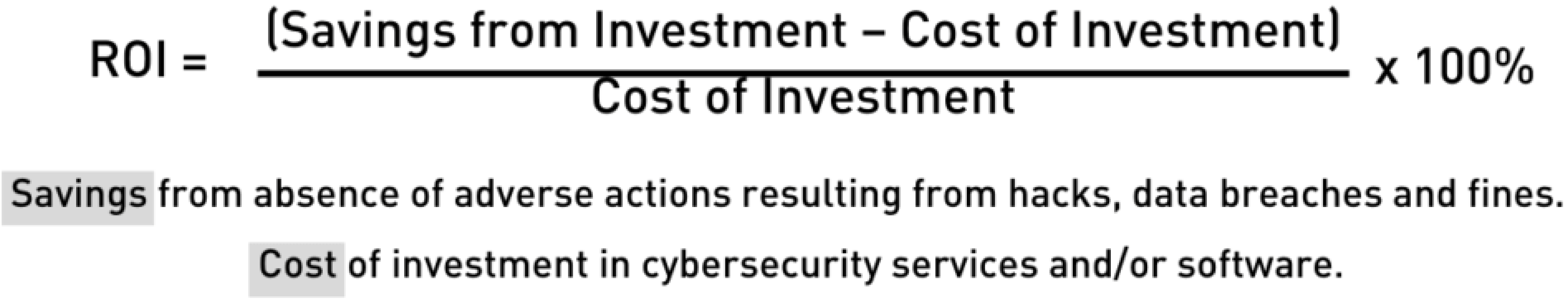
Cyber-security spending exceed $ 1T cumulatively

4+ Billion Cyber targets, cyber-security index growth to 50X

3.5 million unfilled cyber-security jobs

Evaluating adequacy of IT spend – ROI and KPI’s

- Measuring return on security investment and benchmarking
- Most cybersecurity ROI predictions rely on risk evaluations and applying probability of a data breach to projected cost of a data breach. As organizations look to reduce costs to maintain financially viable, a “what if” approach may not be as appealing.
- Cybersecurity initiatives focus on leveraging resources effectively so that they can ensure the most streamlined process possible while maintaining a robust security program. Aligning purchase KPIs with specific reduced operational costs can help gain buy-in for the solution.



$$\text{ROI} = \frac{(\text{Savings from Investment} - \text{Cost of Investment})}{\text{Cost of Investment}} \times 100\%$$

Savings from absence of adverse actions resulting from hacks, data breaches and fines.

Cost of investment in cybersecurity services and/or software.

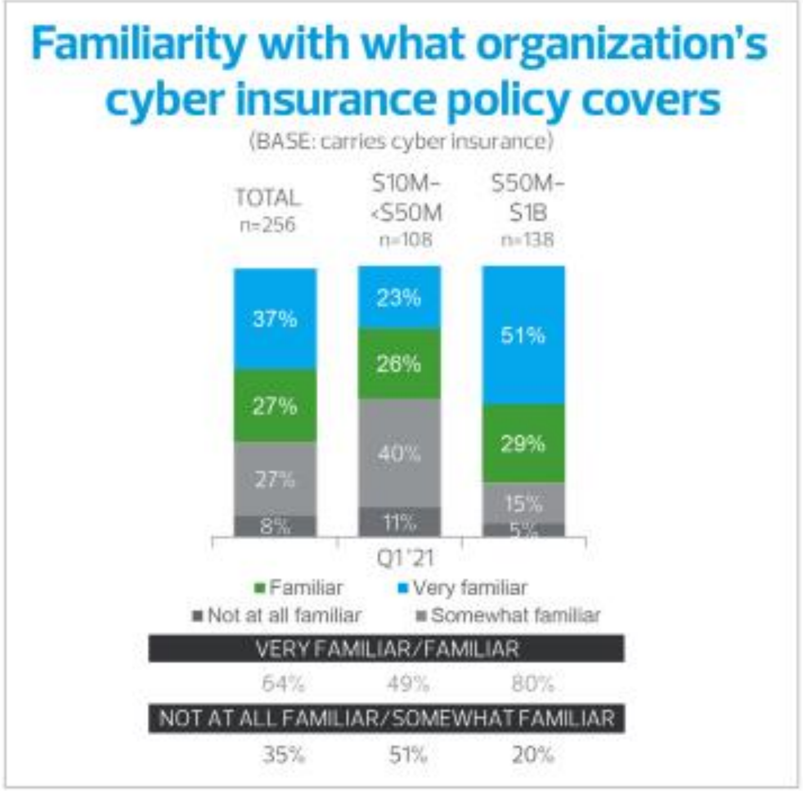
Evaluating adequacy of IT spend – Cyber Insurance

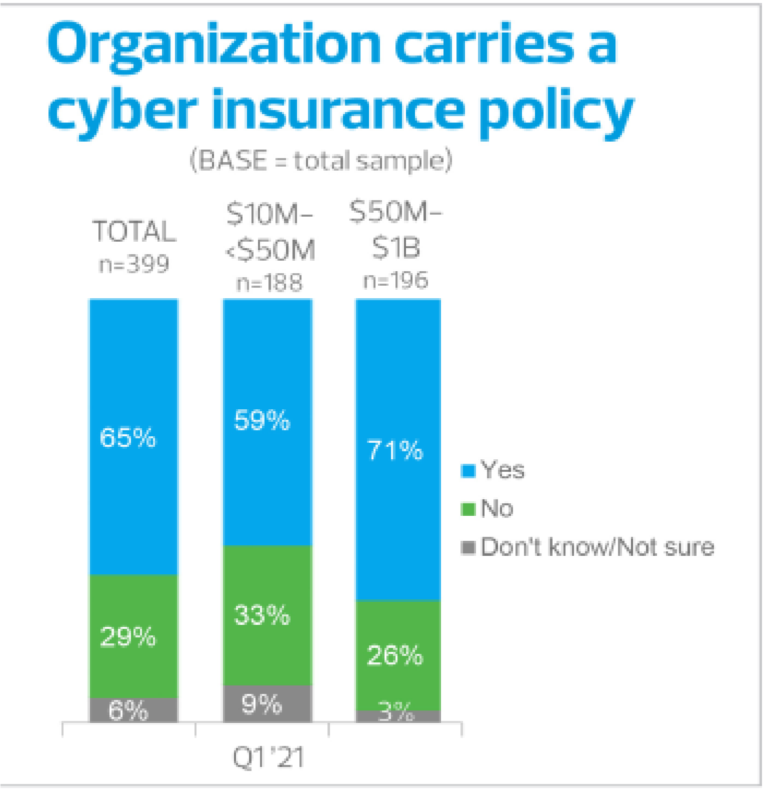
Info

- The average cost of a data breach is about $250 per record lost. A business with a few thousand customers could face hundreds of thousands of dollars in costs.
- Average Cyber liability coverage is around $1-5 million per policy.
- Many small businesses (39%) pay less than $1,500 per year for cyber liability insurance, and 41% pay between $1,500 and $3,000 per year.

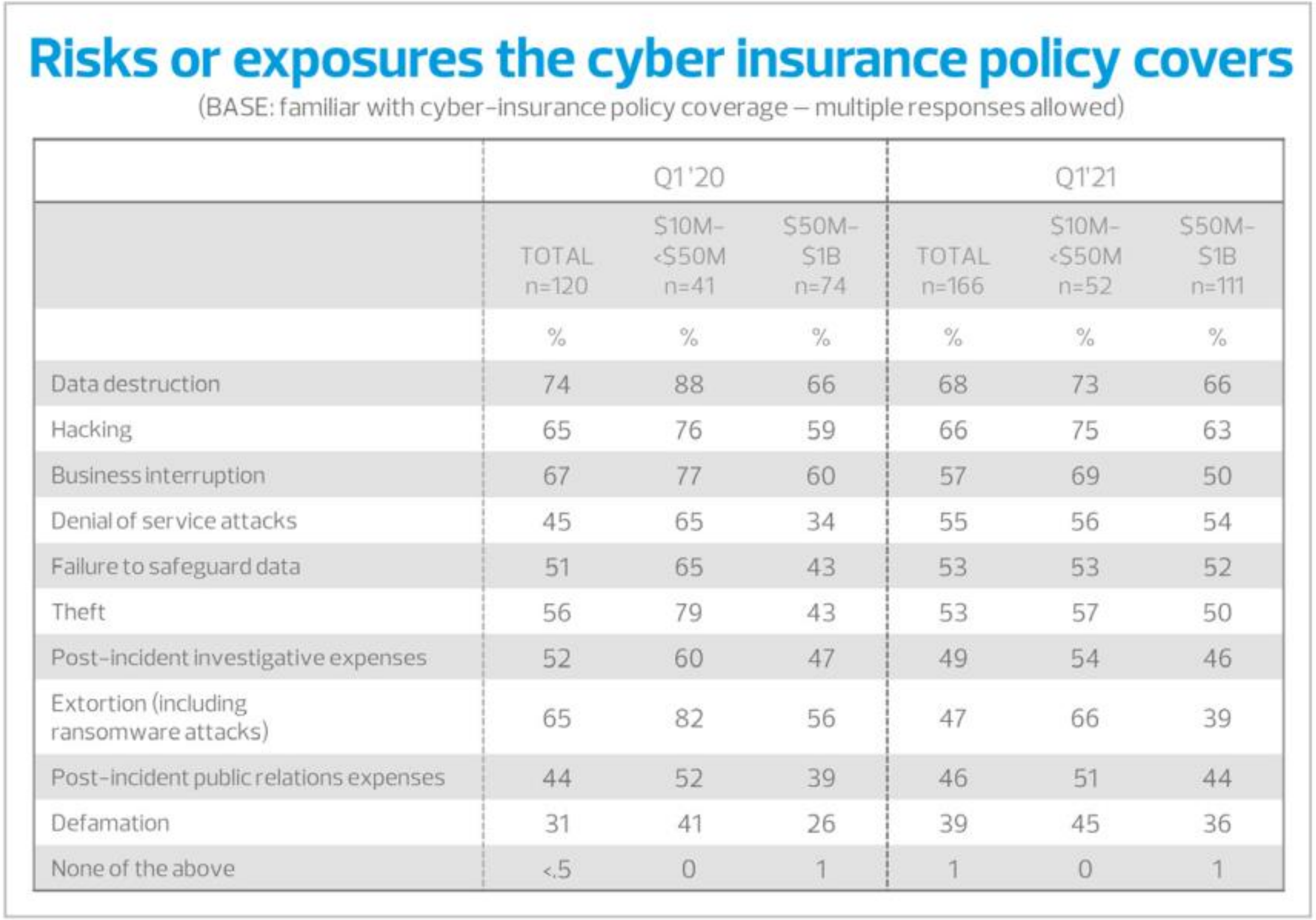
Coverages

- At the time of the breach –Response, fees, types
- After a breach – Notifications, rental, staffing, additional
- Cyber liability insurance doesn’t cover:
  - Professional negligence
  - Breach of contract





Evaluating adequacy of IT spend – Cyber Insurance cont.



Risks or exposures the cyber insurance policy covers

(BASE: familiar with cyber-insurance policy coverage – multiple responses allowed)

	Q1'20			Q1'21		
	TOTAL n=120	$10M-<$50M n=41	$50M-$1B n=74	TOTAL n=166	$10M-<$50M n=52	$50M-$1B n=111
	%	%	%	%	%	%
Data destruction	74	88	66	68	73	66
Hacking	65	76	59	66	75	63
Business interruption	67	77	60	57	69	50
Denial of service attacks	45	65	34	55	56	54
Failure to safeguard data	51	65	43	53	53	52
Theft	56	79	43	53	57	50
Post-incident investigative expenses	52	60	47	49	54	46
Extortion (including ransomware attacks)	65	82	56	47	66	39
Post-incident public relations expenses	44	52	39	46	51	44
Defamation	31	41	26	39	45	36
None of the above	<.5	0	1	1	0	1

64%

of respondents whose firms carry cyber insurance say they are **familiar with what their policy covers**

Cyber liability insurance covers the costs of a data breach or cyberattack, including legal representation and crisis management. It helps tech companies recover quickly and notify affected clients.

Being diligent with information security during this time of change

Where to start:

GENERAL RISK ASSESMENT	REMOTE WORKFORCE ASSESSMENT	FRAMEWORK ADOPTION	CLOUD SECURITY ASSESSMENT
A Risk Assessment measures data storage, access protocols, security policies, governance, antivirus protection, incidence response planning, liability insurance and more.	A Remote Workforce Assessment focuses on employee tools, solutions, controls, shared data processes, virtual private networks, regulatory considerations and more. We can help you determine your best path forward.	Aligning to a security framework; like HITRUST, that fits your organizational requirements can be an effective way to mitigate cyber risks. We can help you adopt a framework and drive your strategy and roadmap.	Utilizing the cloud can be cost effective and reach larger audiences. The effort requires due diligence before implementation and after it is in place. Let us show you how to securely implement controls and configurations to protect your valuable data.

Contact us today to discuss your next steps.

QUESTIONS AND ANSWERS

THANK YOU FOR YOUR TIME AND ATTENTION

RSM

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM, the RSM logo and *the power of being understood* are registered trademarks of RSM International Association.

RSM