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

Monday, October 7th @ 11 AM Eastern
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
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?

- 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

Economic Impact, Cyber Crime $500B+

US Cyber Insurance Market $4B+

Property Risk

Economic Impact, Natural Disasters $300B

US Property Insurance Market $180B

Marsh and MMC Estimates 2018

* Marsh US clients, $1 billion+ revenues, 2018
2019 GLOBAL CYBER RISK PERCEPTION SURVEY
KEY FINDINGS
More than 1500 Respondents Across Industries, Roles, and Regions Conducted In-Market February/March 2019

### Industries

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturing &amp; Automotive</td>
<td>16%</td>
</tr>
<tr>
<td>Real Estate</td>
<td>4%</td>
</tr>
<tr>
<td>Retail &amp; Wholesale</td>
<td>11%</td>
</tr>
<tr>
<td>Chemical</td>
<td>4%</td>
</tr>
<tr>
<td>Financial Institutions</td>
<td>9%</td>
</tr>
<tr>
<td>Construction</td>
<td>4%</td>
</tr>
<tr>
<td>Energy &amp; Power</td>
<td>8%</td>
</tr>
<tr>
<td>Education</td>
<td>4%</td>
</tr>
<tr>
<td>HealthCare &amp; Life Sciences</td>
<td>7%</td>
</tr>
<tr>
<td>Public Entity/Not for Profit</td>
<td>4%</td>
</tr>
<tr>
<td>Transportation, Rail &amp; Marine</td>
<td>6%</td>
</tr>
<tr>
<td>Mining, Metals &amp; Minerals</td>
<td>2%</td>
</tr>
<tr>
<td>Communications, Media &amp; Technology</td>
<td>5%</td>
</tr>
<tr>
<td>Aviation &amp; Aerospace</td>
<td>1%</td>
</tr>
<tr>
<td>Professional Services</td>
<td>5%</td>
</tr>
<tr>
<td>Others</td>
<td>12%</td>
</tr>
</tbody>
</table>

### Corporate Role

<table>
<thead>
<tr>
<th>Role</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Management / Insurance</td>
<td>27%</td>
</tr>
<tr>
<td>C-suite / Board member</td>
<td>20%</td>
</tr>
<tr>
<td>IT / Information Security</td>
<td>19%</td>
</tr>
<tr>
<td>Finance / Procurement</td>
<td>17%</td>
</tr>
<tr>
<td>Legal / Compliance</td>
<td>5%</td>
</tr>
<tr>
<td>Other roles</td>
<td>12%</td>
</tr>
</tbody>
</table>

### Annual Revenue

<table>
<thead>
<tr>
<th>Revenue Range</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than $25 million</td>
<td>23%</td>
</tr>
<tr>
<td>$25 million - $100 million</td>
<td>21%</td>
</tr>
<tr>
<td>$100 million - $250 million</td>
<td>14%</td>
</tr>
<tr>
<td>$250 million - $1 billion</td>
<td>17%</td>
</tr>
<tr>
<td>$1 billion - $5 billion</td>
<td>15%</td>
</tr>
<tr>
<td>More than $5 billion</td>
<td>10%</td>
</tr>
</tbody>
</table>
Concern About Cyber Risk is Peaking
#1: Concern/Confidence Gap

2017:
- The #1 risk: 56%
- A top 5 risk: 34%
- Not a top 5 risk: 6%
- Don’t know: 4%

2019:
- The #1 risk: 57%
- A top 5 risk: 22%
- Not a top 5 risk: 21%
- Don’t know: 6%
# Cyber Risk Surpasses Other Risk Concerns

## #1: Concern/Confidence Gap

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Concern</th>
<th>Confidence</th>
<th>Top 5 Risk (including #1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber-Attacks/Cyber Threats</td>
<td>22%</td>
<td>57%</td>
<td>79%</td>
</tr>
<tr>
<td>Economic Uncertainty</td>
<td>15%</td>
<td>44%</td>
<td>59%</td>
</tr>
<tr>
<td>Brand/Reputation Damage</td>
<td>11%</td>
<td>46%</td>
<td>57%</td>
</tr>
<tr>
<td>Regulation Legislation</td>
<td>9%</td>
<td>46%</td>
<td>55%</td>
</tr>
<tr>
<td>Loss of Key Personnel</td>
<td>5%</td>
<td>39%</td>
<td>44%</td>
</tr>
<tr>
<td>Supply Chain Disruption</td>
<td>9%</td>
<td>32%</td>
<td>41%</td>
</tr>
<tr>
<td>Criminal Activity (Theft, Fraud, etc.)</td>
<td>4%</td>
<td>33%</td>
<td>37%</td>
</tr>
<tr>
<td>Natural Disasters or Climate Change</td>
<td>9%</td>
<td>25%</td>
<td>34%</td>
</tr>
<tr>
<td>Credit/Liquidity Risk</td>
<td>7%</td>
<td>26%</td>
<td>33%</td>
</tr>
<tr>
<td>Industrial Accident</td>
<td>5%</td>
<td>18%</td>
<td>23%</td>
</tr>
<tr>
<td>Political Unrest/War</td>
<td>14%</td>
<td></td>
<td>17%</td>
</tr>
<tr>
<td>Industrial Espionage</td>
<td>11%</td>
<td></td>
<td>12%</td>
</tr>
<tr>
<td>Terrorism</td>
<td>8%</td>
<td></td>
<td>9%</td>
</tr>
</tbody>
</table>

- **The #1 risk**
- **A top 5 risk (but not #1)**
- **Cumulative % ranking each item a top-five risk (including #1)**
Cyber Confidence Has Declined in All Areas Since 2017

#1: Concern/Confidence Gap

- **Understand/Assess/Measure Cyber Threats**
  - 2019: 23% Highly Confident, 59% Fairly Confident, 18% Not at all Confident
  - 2017: 29% Highly Confident, 62% Fairly Confident, 9% Not at all Confident

- **Mitigate/Prevent Cyber-Attacks**
  - 2019: 18% Highly Confident, 63% Fairly Confident, 19% Not at all Confident
  - 2017: 20% Highly Confident, 68% Fairly Confident, 12% Not at all Confident

- **Manage/Respond to Cyber-Attacks**
  - 2019: 18% Highly Confident, 60% Fairly Confident, 22% Not at all Confident
  - 2017: 20% Highly Confident, 65% Fairly Confident, 15% Not at all Confident

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

- Executive Leadership/Board: 65% (2019), 56% (2017)
- Risk Management: 49% (2019), 32% (2017)
- Legal/Compliance: 28% (2019), 20% (2017)
- Finance/Procurement: 20% (2019), 27% (2017)
- Other Roles (such as Operations, HR, Supply Chain Management): 38% (2019), 20% (2017)
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

- Cybersecurity Technology/Mitigation: 67%
- Staff Training: 53%
- Cyber Event Planning and Preparation: 40%
- Cyber Insurance: 34%
- Hiring Cybersecurity Personnel and Talent: 33%
- Alternative Cyber Risk Transfer Vehicles (such as captives and risk retention groups): 14%
30% of Organizations Now Quantify Cyber Risk - Double that of 2017

#2: Dissonance – Strategic Threat, Managed Tactically

- Using any quantitative method such as economic quantification, for example, value-at-risk
  - 2019: 30%
  - 2017: 17%

- Using any qualitative method for example, categories such as high/medium/low or “traffic lights
  - 2019: 43%
  - 2017: 39%

- No approach
  - 2019: 26%
  - 2017: 34%

- Do not know
  - 2019: 19%
  - 2017: 18%
### Risk Assessment Focuses on Technical Aspects Over Economic Cost

**#2: Dissonance – Strategic Threat, Managed Tactically**

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number and type of internal IT vulnerabilities</td>
<td>87%</td>
</tr>
<tr>
<td>Number and type of external IT vulnerabilities</td>
<td>69%</td>
</tr>
<tr>
<td>Staff awareness / compliance with cybersecurity policy</td>
<td>65%</td>
</tr>
<tr>
<td>Probability that our control measures will be effective</td>
<td>50%</td>
</tr>
<tr>
<td>Cost of controlling or mitigating specific cyber risks</td>
<td>47%</td>
</tr>
<tr>
<td>Impact of regulation and fines for non-compliance</td>
<td>46%</td>
</tr>
<tr>
<td>Liability cost or economic damage from specific cyber events</td>
<td>46%</td>
</tr>
<tr>
<td>Amount / replacement value of sensitive data held internally</td>
<td>35%</td>
</tr>
<tr>
<td>Amount / replacement value of sensitive data held by third parties</td>
<td>25%</td>
</tr>
</tbody>
</table>
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

Highly confident  Fairly confident  Not at all confident  Don’t know
## 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

- 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

- 74% evaluate risks prior to adoption in some way
  - 67% during the exploration/testing stage
  - 24% when finalizing purchase/contract

- 54% evaluate risks post adoption in some way
  - 37% during onboarding/implementation
  - 29% post implementation/in use
  - 25% when a cyber attack/incident occurs

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

- Level of cyber risk posed to our organisation by our supply chain
- Level of cyber risk posed by our organisation to our supply chain
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 3\textsuperscript{rd} party risk.**

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

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

Require vendors and 3\textsuperscript{rd} 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

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?

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