MARSH

INSIGHTS | DECEMBER 2019

Staying on Top of the Changing Cyber Insurance Market Is a Necessity for Boards

Cyber threats are a strategic enterprise risk that requires significant focus and time by boards and C-suite members, as well as other key stakeholders. And yet many organizations have worryingly low board and executive-level engagement around cyber risk, according to the *Marsh Microsoft Global Cyber Risk Perception Survey*. Moreover, the practices employed by many firms that lack sufficient senior management engagement to counteract these risks significantly lag in effectiveness relative to the critical nature of cyber risk.

Recent shifts in the way insurers are covering cyber risk may necessitate changes in many organizations' approaches to insuring this risk. And it's imperative that board members become more knowledgeable on how insurance market changes can affect their organization's coverage of those risks.

Insurers Move to Affirm or Exclude Cyber Risk

The cyber insurance market has evolved significantly since the first network security policies were offered in 1999. This evolution has mainly been driven by the dynamic, volatile nature of cyber risks and shifting buyer demographics from privacy-driven entities to companies in all industries, most notably the manufacturing sector. This has also fueled the purchase of standalone cyber insurance: 47% of respondents to the 2019 survey by Marsh and Microsoft said they now have cyber insurance, up from 35% in 2017.

Recently, a third factor in this evolution has emerged as the insurance industry has sought to clarify how property and casualty (P&C) policies might respond to a cyber event. Traditional P&C insurance is intended to respond to physical perils, but policyholders' evolving risk profiles and the failure of traditional policy language to keep pace have resulted in unintended cyber event coverage, commonly known as "silent cyber" risk.

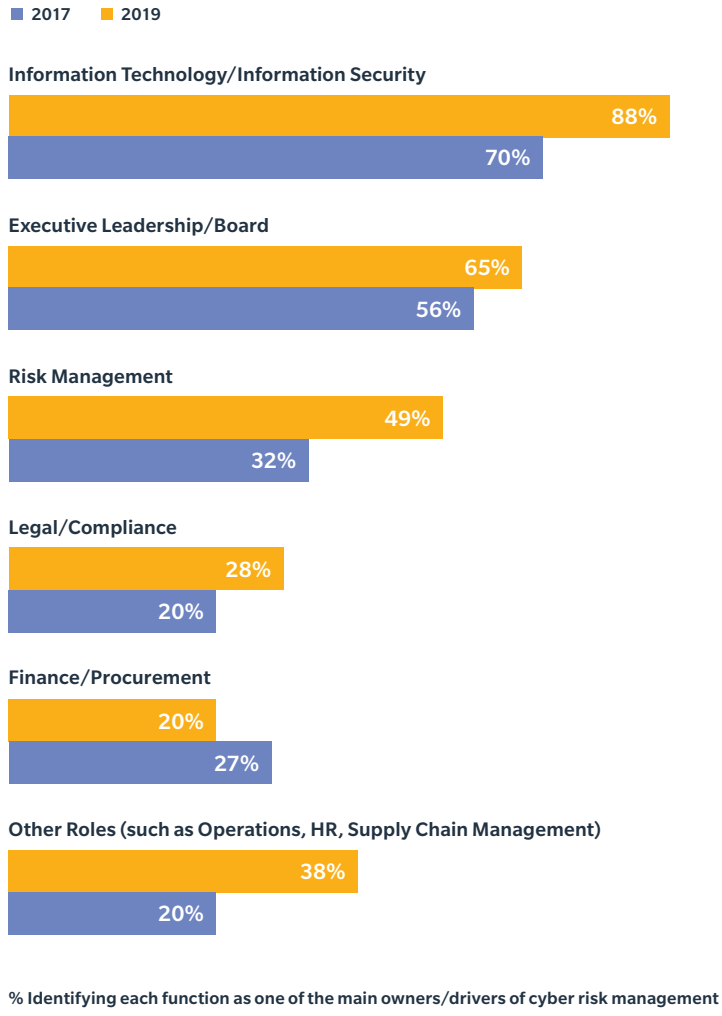
The insurance industry, led by Lloyd's of London, is now taking the position that all P&C insurance policies must either expressly exclude or include cyber coverage; effective January 2020, Lloyd's insurers can no longer remain "silent." Although it is still unclear what this means for policyholders, traditional P&C markets appear to be moving toward exclusion—not inclusion—of cyber risks.

FIGURE 1

IT staff continue to be main owners of cyber risk management at most firms.

SOURCE: MARSH MICROSOFT GLOBAL CYBER RISK PERCEPTION SURVEY

Q: Please rank the three functions which are the main owners or drivers of cyber risk management in your organization.



% Identifying each function as one of the main owners/drivers of cyber risk management

As new technologies and devices add complexity to organizational risk profiles, board members and C-suite executives must be aware that traditional insurance markets are moving to exclude cover for much of that risk. Faced with a seemingly perfect storm of increasing risk and narrowing coverage, a clearer and more nuanced approach is necessary to manage the risks of doing business — one that includes not just a broad cyber insurance program but also the treatment of cyber issues as operational risks.

Boards and C-Suites "Silent" on Cyber Risk Management

The uncertainty about how and where coverage of cyber risks can be found in insurance policies should challenge companies to evolve their cyber risk management strategy. After all, 80% of organizations polled in our survey said cyber threats now rank as a top five risk concern, up from 62% in 2017. But are organizations taking strategic action?

Our findings suggest there is another form of "silent" cyber risk. Despite cyber risk being viewed as of greater concern than any other risk, including natural disasters or climate change, organizations' overall confidence in their ability to manage cyber threats has declined: Only 11% reported high confidence in their ability to understand, prevent, and respond to cyber risks.

While myriad factors underlie this drop in confidence, two data points are telling:

- Organizations that perceive a lack of executive support or mandate to address cyber risk are significantly less confident about their capabilities to respond appropriately. A large majority of organizations — 88% — still view the information technology (IT) department as a primary owner of cyber risk management (Figure 1), with executive leadership and boards ranking second (named by 65%).
- However, only 16% of executives and boards say they spend more than a few days a year on cyber risk issues (Figure 2).

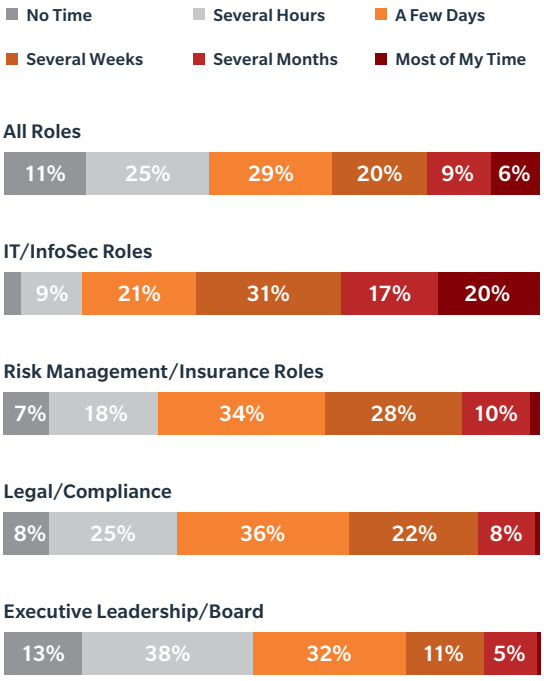
The disconnect is striking: Cyber threats call for a rigorous risk management strategy, but many organizations — and their leaders — are delegating or sidelining the issue.

FIGURE 2

Key decision-makers are not spending much time on cyber risk management.

SOURCE: MARSH MICROSOFT GLOBAL CYBER RISK PERCEPTION SURVEY

Q: Over the past 12 months, approximately how much of your total professional time has been spent on cyber risk and/or cybersecurity?



% Reporting time spent on cyber risk/cyber security issues by each role

Boards and C-Suites Should Lead the Charge

Our message is straightforward: Organizations must elevate cyber risk to a board-level issue and apply the same discipline and governance that other critical risks receive. Boards must embrace their oversight role, and include all key internal stakeholders in the cyber risk management process, not just IT; engage in cyber event planning, training, and incident response rehearsals; and invest in both cybersecurity technology and insurance, based on quantified measurement of organizational cyber risk.

Our survey shows that organizations that quantify their cyber-risk exposures are more likely to engage in both technological and nontechnological actions to manage the risk. For example, 50% of manufacturers that measure their cyber risk economically also engage in loss modeling, compared to 18% of manufacturers that do not quantify their cyber risk but engage in loss modeling. Loss scenario modeling is an essential driver of well-informed investment decisions and return on investment (ROI) measurement, and it strengthens an organization's ability to approach cyber risk strategically by enabling a shift away from technical jargon toward a dollar-based discussion in language understood across the business.

Likewise, 90% of manufacturers that quantify cyber risk invest in employee training, compared to 62% of manufacturers that don't quantify cyber risk but still invest in employee training. And those that quantify cyber risk are more than twice as likely to assess supply chain risk than those that do not (55% vs. 25%). Clearly, measuring the actual value at risk from cyber events provides crucial intelligence about the need to invest in actions that build resilience.

The Way Forward

How can board members and C-suite executives take more ownership of cyber risk, and ensure a strategic risk management framework is in place? How can they gain a more thorough understanding of their insurance programs and the protections these programs can offer? A good starting point is to ensure they are having the right conversations with risk professionals about their organizations' cyber exposures, and how their insurance programs will – or won't – respond.

Equally important are framing cyber risk exposures in economic terms to enable comparison with other enterprise risks; optimizing capital allocation across mitigation, insurance, or other resilience-building areas; and measuring the impact of cyber spending on risk reduction.

Finally, since cyber threats are now a strategic concern requiring executive ownership, the assessment, measurement, and management of cyber risk should be a consistent board meeting agenda item.

We are entering a new era in the management of cyber threats. As insurance policies will increasingly either affirm or exclude cyber risk, it becomes crucial for board members and C-level executives to understand the potential threats facing their organization and to embrace a strategic risk management approach to combat them.

For further information on Marsh's cyber insurance solutions, visit marsh.com, send an email to cyber.risk@marsh.com, or contact your Marsh representative.

SIMON BELL
Financial & Professional Lines
Leader - MENA
+971 50 450 1935
simon.bell@marsh.com

TALAL Y. DARRAS
Business Resilience Leader -
MENA
+971 56 174 0379
talal.darras@marsh.com