THE one BRIEF
AON EXPLORES THE WORLD'S MOST PRESSING BUSINESS ISSUES

RISK & INNOVATION

Seeing The Big Picture: Cyber And The C-Suite

OVERVIEW

Thirty-seven percent of business respondents to a recent survey said they had experienced a "material or significantly disruptive security exploit or data breach" in the last two years, and other studies have found that 90 percent of companies have suffered a cyber attack of some kind.

Over the last few decades, as risk of cyberattacks have increased, the way companies have approached cybersecurity has evolved. Only a few years ago, cyber was considered the responsibility of select functional groups within an organization – primarily information technology (I.T.). It is now a much larger, distributed challenge that touches and impacts nearly every part of an organization, beyond I.T. and on to risk, human resources, legal, compliance and corporate communications. Numerous functional teams now play a role in responding to and managing cyber breaches, from quantifying and mitigating the risks to remediation after an attack occurs.

With attacks increasing, functional departments are now beginning to plan and budget for more comprehensive ways to understand, protect and address their cyber risk. "Cyber-spend" – which can include diagnosis of issues, defense, insurance, and more – is one of the fastest-growing areas of organizations' budgets.

Due to the integrated nature of cyber, cyber risk issues have now made their way to the boardroom, with members of the C-suite developing overarching strategies to protect their company's assets, reputation and bottom line. The challenge of managing a problem of this scale, with cyber criminals developing new ways to breach increasingly sophisticated technical defenses, is that elements of prevention still normally fall under the remit of a number of different departments within an organization.

All too often, companies continue to address such cyber risk in a distributed, disparate way. In today's interconnected world, preventing, mitigating and managing cyber-related fallout simply cannot be done in silos. Organizations need to solve these distributed problems with an integrated approach and solution.

IN DEPTH

"In the early 2000s, the focus was on data theft and fraud monetization," explains Aon's Chief Security Officer, Anthony Belfiore. "In 2012, however, the online banking services of a number of the largest U.S. banks were attacked. These 'denial of service' attacks, which bombard a particular service and keep it offline, were a wake-up call for both the industry and government, demonstrating that even organizations with vast resources to defend themselves against cyberattacks were still vulnerable."

With the Wall Street attack, cybersecurity moved to a new phase in which risk managers began to work more closely with other parts of their organization. Traditionally, cybersecurity has been seen as I.T.'s issue. However, Belfiore states, "Technology alone cannot solve this. CHRO's, COO's, legal, compliance – there's an ecosystem of constituents that need to come together to solve this challenge."

The C-Suite is increasingly aware of the risk of these cyberattacks significantly impacting their companies' data and reputation. That awareness, however, is not matched by an adequate understanding of how they should respond, or whether traditional responses are sufficient.

The Challenge

The challenge is significant. There were 430 million new unique pieces of malware developed in 2015, a 36 perent rise compared to the year before, according to security software firm Symantec. A recent survey of 591 companies, also conducted by Symantec, found 21 percent of those surveyed would take between two to seven days to detect an attack, 40 percentsaid that they could detect an attack within twenty-four hours – and, surprisingly, 2 percent said their average detection time would be greater than one year. Companies are increasingly concerned – 52 percent of respondents to Ponemon's 2015 Global Cyber Impact Report said they expected their cyber risk exposure to increase in the next two years.

Creating perfectly safe software is difficult, and software is often released with vulnerabilities that are unknown to the developer, and that may only get patched after a successful cyber breach is discovered. In 2015 alone, over 169 million personal records were exposed and there was a 38 percent rise in cyber security incidents detected.

"The reality is that cyber attackers will continue to evolve at accelerated rates and will attempt to stay a step ahead of corporate defense," argues John Bruno, Executive Vice President; Enterprise Innovation & CIO at Aon. "The attacks are unrestricted, fluid, dynamic and malicious. Time spent thinking about how to defend yourself must include scenario plans that were once thought to be unlikely, and more importantly time needs to be spent on planning for effective response reducing the severity of an attack versus prevention only."

The Catalysts for Cyber Confusion

By its nature, cybersecurity is a dispersed, complex challenge. Any part of a company's infrastructure could be targeted, from customer data to infrastructure – and the number of vulnerabilities is only set to increase as the growth of the Internet of Things leads to a proliferation of connected devices.

These risks reinforce the siloed nature of corporate responses. Part of the problem is that different aspects of the response, such as diagnosis, defense, and risk transfer, typically in the form of insurance, tend to be offered by different providers. The result is that no one function or external provider has the whole picture of an organization's defenses.

Common Challenges to Cyber Risk Mitigation

1. **Not understanding risk assessment and diagnostics.** While there is increasing emphasis on technology solutions to heighten cyber security, a significant proportion of cyber breaches still derive from human error or process issues.
2. **Not clearly defining payout triggers.** If a company is attacked there may be conflict with the insurer as to whether the insurance policy covers that type of attack. Pricing rationale is often inconsistent.
3. **Not getting a true sense of the full, company-wide scale of a company's cyber risk.** Because of this, the uptake of cyber insurance remains slow – despite the growing potential for cyber breaches to cause significant damage to both the bottom line and reputation. Only 12 percent of the potential loss to information assets is currently covered by insurance, and only 19 percent of companies have cyber insurance coverage, according to Ponemon's 2015 Global Cyber Impact Report survey.

Thinking differently: a holistic solution

The solution, explains Bruno, is to deal with the risks in a holistic manner. "The risk manager should be the 'hub' that is pulling data from each 'spoke' across the organization and using it to identify gaps that need to be addressed or best practices that could translate into better coverage terms," he says.

Belfiore states that many organizations do not even have teams that can articulate the exposure and it becomes the role of the risk manager to drive cyber preparedness, cyber risk transfer (insurance) and cyber remediation (claims preparation) in the case of an event.

With a risk as complex, all-pervasive, and rapidly-changing as cyber, boards need to first accept that most measures today to prevent cyber breaches are insufficient. All the high-end cybersecurity in the world will not be enough if a single employee accidentally reveals their password, or leaves an unlocked laptop unattended. Some of the biggest, most damaging cyber breaches of recent years have come about through inadvertent human error.

The first step needs to be building a better understanding of the nature and level of the cyber risk – and protection – organizations currently have. This is, of course, easier said than done and boards first need to assess and agree what data is the most important.

"Companies need to evaluate the impact and characteristics of the attack to determine whether it qualifies for an immediate insurance claim," explains Bruno. "By integrating claims preparation into the remediation program, companies can accelerate the recovery process and unify elements of the response."

Belfiore notes that few organizations have mature enterprise risk programs and others think about cyber as only a subcomponent of a risk program. This means that they are unable to fully assess how cyber resilient they really are – or aren't – across the organization.

Longer-term, ongoing analysis of cyber risk – as well as monitoring of systems to identify breaches when they occur – requires reliable, compatible data that can be collected in a consistent and uniform manner across the organization, and assessed via a common set of criteria. This will enable complex security risk topics to be distilled into categories that all departments can understand, give executives the chance to see a unified view of their organization's readiness to defend against cyberattacks, and give them the high-level oversight to prioritize, budget for and address any weak links.

Being Prepared

With 25 percent of cyber breaches stemming from human error, focusing on shifting mindsets and attitudes towards data security can be one of the most effective – and cost-effective – ways to reduce overall cyber risk. To drive this change in mindset, the C-suite needs to encourage cybersecurity thinking to become embedded at all levels of the organization, and for leadership in all departments – not just IT or risk management.

Finally, companies need to know exactly what to do if a cyber breach occurs. A cybersecurity plan which does not include ways to react to and recover from breaches is incomplete. Any plan needs to combine technology solutions with insurance, staff training, plans of action, and practice cyberattack drills – similar to any effective crisis management plan.

With the rise of data-driven approaches to business and the growth of new connected technologies, the range of cyber threats is likely to increase, as is the number of critical functions within firms which are vulnerable to cyberattack. The challenge will be to assess and communicate that risk across the whole organization. The key is a more holistic approach – making the risk manager the hub of activity across the assessment. This more holistic approach needs to start with the C-Suite – breaking down silos from the center to make their organizations more cyber-resilient.

TALKING POINTS

"We have agreed that cybersecurity is a global issue that can only be solved through global partnership. It affects all of our organizations... and the United Nations is positioned to bring its strategic and analytic capabilities to address these issues." – Lazarous Kapambwe, President of The United Nations Economic and Social Council

"This Government has made cyber security a top priority. Too many firms are losing money, data and consumer confidence with the vast number of cyber attacks. It's absolutely crucial businesses are secure and can protect data." – Ed Vaizey, former U.K. Minister for the Digital Economy

"It's easier to create a rule-bound culture for network administrators and cybersecurity personnel than it is for an entire workforce. Yet the latter is certainly possible, even if a company has a huge number of employees and an established culture. Witness the many companies that have successfully changed their cultures and operating approaches to increase quality, safety, and equal opportunity." – Harvard Business Review

FURTHER READING

- Cyber Resilience: Everything You (Really) Need To Know – World Economic Forum, July 8, 2016
- Cybersecurity 101: Why It Matters To Your Business – ITPortalPro, June 5, 2016
- It's Time To Think Of Cybersecurity As A Business Enabler – Forbes, July 1, 2016
- Statement By Vice-President Ansip And Commissioner Oettinger Welcoming The Adoption Of The First EU-Wide Rules On Cybersecurity – European Commission, July 6, 2016
- Wireless defense strategies in the IoT era – The Register white paper, June 2016
- 2015 Global Cyber Impact Report – Aon


Empower Results®