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

RISK & INNOVATION

Four Steps To Achieving Cyber Resilience

OVERVIEW

We are living in a period of unprecedented technological change. Building resilience to these changes is becoming increasingly imperative.

By 2020, it is expected that there will be tens of billions of devices connected to the Internet of Things (IoT). But new technology means new risks. What if someone hacks a car? Or a power plant? By the same token, financial losses incurred through data breaches are likely to reach trillions of dollars. There are also positive opportunities. GE estimates that IoT devices will be generating $11.1 trillion annually by 2025, touching 43 percent of the global economy. Meanwhile, it is expected that 4.2 billion people will be online by 2020, or 54.5 percent of the global population, exchanging and sharing goods and information. Mitigating the risks while embracing the opportunities is key.

The internet asks a lot of questions of its users. How should the internet interact with nation states? What opportunities can it offer criminals? How should legislation and regulation apply to the seas of data that constitute the heart of the new digital economy? We are still coming to terms with these issues.

Building resilient firms that can provide solutions and adapt to these new challenges will be a major task in the coming years. Siloed risk management and recovery efforts will come to be seen as increasingly out-of-place in such a digitized world. To become more resilient in this age of continued digital disruption increasingly means understanding the full scope of cyber governance responsibilities. This means starting with a top-down approach in managing risk at the board and executive level, identifying and protecting the organization's most critical assets and understanding the impact to the enterprise should they be compromised. It means complying with international regulations and understanding organizational blind spots. And it means adapting to the latest techniques and trends in security and being prepared to respond should there be a failure in any of these areas. Cyber security cannot be approached piecemeal, but should be considered holistically, as a challenge facing the entire organization.

IN DEPTH

If leaders are to make the most of new technology, then they cannot only think about that technology: They need to take into account the business context in which that technology operates and the impact and risk exposure that it can potentially cause to the organization. There are two key areas to consider: The regulatory environment and organizational culture.

Regulatory Issues

Today's globalized, digitally integrated world means that most organizations are to some extent international. Whether it's a business which serves a global market, or a manufacturer hooked into global supply chains, awareness and adherence to local rules and regulations is crucial.

The EU is a good case in point. The EU General Data Protection Regulation (GDPR), due to come into effect in 2018, will require every organization operating in Europe to abide by several regulatory provisions – and this doesn't just mean companies based in Europe, but also those which offer goods or services to EU markets in a way that involves processing any European-owned data.

"GDPR can impose considerable punitive measures on companies that fail to comply with these regulations," warns Andrea Garcia Beltran, EMEA Cyber Sales Leader, Financial and Professional Services Group at Aon. "Failure to comply could mean fees of up to 4 percent of annual global revenues, and intensified investigations and auditing in the future."

Crucially, this new legislation will affect "organizations of every size, industry and geography that process data of EU citizens," says Kevin Kalinich, Global Practice Leader, Cyber Insurance, Aon Risk Solutions. "It applies broadly to personal data, including customer lists, contact details, genetic/biometric data and potentially online identifiers, such as IP addresses. Companies must obtain explicit clear and affirmative consent prior to processing personal data – assumptions based on silence do not comply."

These provisions include the regulation of corporate data protection policies, which means treating data stored on mobile devices with the precautions as data stored centrally. GDPR also requires the consolidation of data visibility tools and written reporting for data processors, as well as mandating that companies have a data breach notification protocol. However, there are upsides to new regulation. "Compliance will enable firms to update their current process and methodology to assess cyber risks and the related potential business impact," says Kalinich. "Once compliant, an organization's total cost of risk could be reduced."

The scope and potential severity of the legislation mean that liable companies need to move quickly before the law comes into effect on May 25th, 2018 to ensure compliance. In practical terms, this could mean the C-suite assessing their company's readiness for GDPR, and then putting in place teams that can carry out necessary changes before the regulations come into effect.

And the GDPR is just one example, in just one part of the world. Japan's PIPA, originally implemented in 2003 and due for extension in May 2017, is another. These challenges are global, and regions everywhere will need to come up with appropriate regulatory responses. Understanding legislation like this and building a responsive cyber policy is crucial.

Maintaining Cyber Awareness

The GDPR Regulation determines how an organization will manage, protect and administer data. Such regulations are put in place to protect businesses and also consumers from the damage cyber breaches can cause, explains Garcia Beltran. "And they will be most effective if organizations themselves take cultural steps to acknowledge and take appropriate measures to protect against known and unknown cyber vulnerabilities."

East Asia provides a good example of a region still transforming its attitude towards cyber risks. This can be seen in the gap between the cyber risk faced by leading Asia-Pacific firms and the levels of cyber insurance. Ponemon's 2015 Asia Pacific cyber impact report found that only 13 percent of potential losses to intangible assets (i.e. informational and data assets) were covered by insurance in the region, compared with 49 percent for tangible assets (such as goods or operating technology).

"Cyber risk awareness and understanding is still very low, but awareness is growing rapidly over time with incident frequency" says Sandeep Malik, Asia CEO, Aon Risk Solutions. Numerous studies have shown that the APAC region is the leading source of malicious cyber traffic, and organisations within the region are more likely to be targeted by hackers than in other parts of the world.

But despite this growing risk, and with the exception of regulatory initiatives like PIPA, organizations are still working to adapt their strategies to improve their resilience to the threat.. In the meantime, the discrepancy between coverage and risk level means that information and system assets are too often exposed without appropriate protection. This problem is compounded by an insurance sector that has historically underserved the Asia-Pacific market in comparison to North America; the reason being that there is much less litigation in AsiaPac, says Kalinich. "While companies in the region are adopting technology at a rapid pace, cyber insurance purchases lag way behind property and general liability insurance even though there are increased cyber exposures, such as business interruption, which could be equal to losses in North America," he says. Due to this lack of 'demand', "cyber insurance companies have not flocked to Asia – yet."

The difficulties facing APAC regions are just one example of how approaches to cyber risk need to be understood in terms of organizational culture. Cyber teams would do well to understand any blind spots that might be inadvertently opening up vulnerabilities in cyber policy. Not only will this reduce the potential risk, but it should also reduce the cost of cyber insurance.

Companies also need to make sure their C-Suite and their cyber teams are speaking the same language – this seems straightforward, but what might seem rudimentary for a cyber specialist may be too technical for a C-level executive. "Experts in this space sometimes tend to use technical language when describing cyber security, which sounds like a foreign language when presented to CEOs and boards. It's important for information security experts to communicate with executive leadership in terms they can understand and for leaders to become more knowledgeable about cyber security concepts and issues" says Jim Trainor, Senior Vice President, Aon Risk Solutions and former Assistant Director of the FBI's Cyber Division in Washington, DC. Making sure an organization can face risks effectively means making sure that the nature and scale of those risks is effectively communicated.

Four Steps To Reducing Your Cyber Vulnerability

There are a number of strategies that can help organizations ensure smooth operations. Rocco Grillo, Executive Managing Director at Stroz Friedberg, an Aon company, and head of the firm's Cyber Resilience business provides cybersecurity tips for leaders to keep in mind as they operate in today's digital, connected, and regulated world.

1. **Identify your critical assets.** Organizations need to identify their most critical assets and have alignment with the board and executive team down to the individuals who are responsible for protecting them. Organizations must assess what data is critical, where it is stored, how it flows across the organization, and who really needs access to it. This could include customer data and intellectual property which could be stolen, or operating and manufacturing technology which could be sabotaged. This can help to serve as the foundation for any organization as they develop, test, and validate their security program. Furthermore, organizations must recognize the impact to the business should these critical assets be compromised and be prepared to respond to limit the impact to the organization while restoring normal business operations.
2. **Conduct a comprehensive risk assessment.** Once alignment on critical assets has been established from the top down it will be easier, to pinpoint vulnerabilities and assess cyber preparedness. Organizations should review cybersecurity deficiencies and vulnerabilities across all key enterprise areas including business practices, information technology, IT users, security governance, and the physical security of information assets. Risk could also manifest itself as losses due to business interruption or reputational damage.
3. **Take a holistic approach to cyber governance.** Mitigating cyber risk is not just an issue for tech teams. The scope of risk means that guarding against attacks should involve key players across all enterprise functions and entities. Educating employees and leaders at all levels on the scale of risk, and getting in place provisional crisis plans will help build a truly cyber-resilient organization.
4. **Keep your defenses sharp.** A secure environment requires ongoing validation and can become vulnerable in an instant. Deploy techniques such as pen testing or red teaming exercises to ensure your applications, networks and endpoints aren't vulnerable.

Rising To The Challenge

Addressing ever-changing cyber threats could be a complex task, not least because of the challenges of ensuring sufficient levels of technical knowledge. "Since most lines of insurance base risk, pricing, limits, retentions and coverage on 10 – 20 years' worth of actuarial benchmarking and specialized underwriting expertise, there is not a lot of cyber risk management experience," says Kalinich. "Cyber risk management expertise requires a combination of technology acumen, insurance knowledge, understanding of legal and regulatory concepts, quantitative awareness and critical thinking. Given the growing demand, there are unprecedented opportunities in the global jobs marketplace for many new cyber resiliency champions to ensure organizations protect their balance sheets from cyber exposures."

As with everything, a holistic understanding of the challenges – be they regulatory or organizational – and a holistic application of the right solutions will be essential in building resilient companies that can adequately meet the demands of a rapidly changing cyber landscape.

TALKING POINTS

"Ex post detection and remediation of cyber breaches is akin to treating the symptoms of a disease but not the actual pathology itself. Existing information security practices may prevent some incidents, but the overall problem continues to plague businesses and government agencies alike. Once one accepts the near inevitably of cyber attacks and undertakes to minimize their impacts, then one can prepare a reasoned strategy." – Sean Kanuck, Former U.S. National Officer For Cyber Issues

"One of the main takeaways was that cyber risk is now so serious it is something for boards to directly address as part of their corporate risk oversight. In the past, cyber risk was an issue that was dealt with by some department on the 4th floor, but that's no longer acceptable." – Van Lamoen, Head of Governance and Active Ownership, Robeco

"Prior planning is significant. CEOs and boards need to understand things like the topography of their network, where their data center is located, what kinds of operating systems are in use, where the most sensitive data is housed, where are they most vulnerable, etc. All of these things need to be evaluated at the leadership level prior to a breach to inform an effective cyber response." – Jim Trainor, Senior Vice President, Aon Risk Solutions