The complex and challenging world of cyber risks

The rate at which digital technology is evolving and disrupting traditional business models, cyber risks seem to evolve even faster. Despite declining business confidence in the ability to manage cyber risk, business leaders are now clearly recognising the critical nature of cyber threats and are starting to identify and embrace best practices to mitigate risks.

By John Mc Loughlin 11 Dec 2019

John Mc Loughlin, CEO at J2 Software

Cyber risk has moved beyond data breaches and privacy, there are now sophisticated attacks that are disrupting entire countries, industries, businesses and supply chains. This is costing the economy billions and affecting businesses in ever sector. Unfortunately, cyber risk cannot be eliminated, but it can be mitigated and managed.

The savviest businesses are building cyber resilience through comprehensive, balanced cyber risk management strategie rather than concentrating solely on prevention. These more complex approaches account for the need to build capabilities understanding, assessing and quantifying cyber risks in the first place, as well as adding the tools and the resources to respond to and recover from cyber incidents when they inevitably occur.

Know the magnitude of cyber risks

As cyber risks become increasingly complex and challenging, there are encouraging signs in the 2019 Global Cyber Risk Perception Survey that businesses globally are starting to implement best practices in cyber risk management. Most businesses recognise the magnitude of cyber risk and many are shifting aspects of their approach to match the threat, ar most are doing a good job in traditional cybersecurity, protecting the perimeter.

Effective cyber risk management requires a comprehensive approach employing risk assessment, measurement, mitigatic transfer, and planning, and the optimal program will depend on each company's unique risk profile and tolerance.

This addresses many of the common and most urgent aspects of cyber risk that businesses today are challenged with, an should be viewed as signposts along the path to building true cyber resilience. Nonetheless, the survey shows that there remains a considerable gap between where cyber sits on the corporate risk agenda and the overall level of rigour and maturity of cyber risk management.

Many enterprises globally could benefit by applying strategic risk management principles to their cyber risk approach, supported by more expertise, resources, and management attention as they build cyber resilience.

Technology is dramatically transforming the global business environment, with continual advances in areas ranging from artificial intelligence and the Internet of Things (IoT) to data availability and blockchain. Especially in an 'Internet of Everything' era with digitally dependent supply chains and innovative technology, yesterday’s practices and mindsets are enough, and may actually inhibit innovation.

Embracing network security

Optimising security from the castle to the wider community is harder, but inevitable. It requires a shift from solely focusing enterprise security to embracing responsibility for network security across the entire supply chain.

The survey points to a number of best practices that the most cyber-resilient firms employ and which all firms should consider adopting:

- Create a strong cybersecurity culture with clear, shared standards for governance, accountability, resources and actions.
- Quantify cyber risk to drive better-informed capital allocation decisions, enable performance measurement, and fram cyber risk in the same economic terms as other enterprise risks.
- Evaluate the cyber risk implications of new technology as a continual and forward-looking process throughout the lifecycle of the technology.
- Manage supply chain risk as a collective issue, recognising the need for trust and shared security standards across the entire network, including the company's cyber impact on its partners.
- Pursue and support public-private partnerships around critical cyber risk issues that can deliver stronger protections and baseline best practice standards for all.

New tech increases exposure

Security challenges can manifest whenever new technology is integrated into business infrastructure, bringing new and additional complexity to the company's technology footprint. The risks and exposures presented by new technologies must weighed against the potential transformative business effects, and risk tolerance varies both by industry and by an individu company.

Businesses are embracing technological innovation, and most don’t see cyber risk as a barrier. But an assessment of nev technology cyber risk is not as rigorous and continual as it should be. The number of internet-connected devices is estimated to be 75 billion by 2025. As the world moves closer to an “Internet of Everything”, the amount and variety of digi assets that are stored, processed and shared by enterprises rises.

Even traditional sectors such as manufacturing expect almost 50% of the products they develop to be “smart” or “connecte in some way by 2020, opening up new revenue streams in data-driven services.

Supply Chain Risk

In increasingly interdependent digital supply chains, cyber risk needs to be a collective responsibility. In a world of hyper-connected supply chains, there is a critical need for trust among partners; a lack of trust risks impeding business performance and innovation.

Every business needs to understand, have confidence in, and play a role in the integrity and security of the components a

software of its digital supply chains. The concept of “technological social responsibility” - the recognition and acknowledgement by each company of its role and cybersecurity obligations within the supply chain - is on the agenda fo many industry leaders.

But while many companies recognise the potential risks their supply chain partners may pose to their own cyber posture, most don’t fully appreciate the risk in reverse.

Regulations and legislation

In recent years, regulators globally have enacted numerous measures to hold corporations and executives more directly accountable for ensuring effective cybersecurity and for keeping customers’ data safe. Many of these regulations and leg frameworks require a greater degree of transparency from companies at all levels of their data handling activities, and in their cyber risk management readiness.

According to the survey, government laws and regulations are less effective in helping businesses improve their cybersecurity posture compared to 'soft' voluntary industry standards and guidance.

Cyber investments

Effective cyber risk management requires quantitative risk expression. Although more businesses measure their cyber ris economically, there’s a long way to go for all businesses to embrace this best practice, and then to apply that quantified measurement to drive sound cyber risk investment decisions.

Investments in cybersecurity technology are rising quickly and far outpacing spending on cyber insurance. The global cy insurance market as measured by gross written premiums is forecast to be just under $8bn by 2020, compared to a $124 global cybersecurity market.

Many companies focus their cyber risk management strategy on prevention by investing in technological frontline cyber defences. Meanwhile, spending on other tools and resources for cyber risk management, such as cyber insurance or eve response training, remains a fraction of the technology budget.

This suggests that many businesses continue to believe they can eliminate or manage their cyber risk primarily through technology, rather than through a comprehensive range of planning, transfer, and response measures.

Best practices

Best practice calls not for parity of spending, but an investment strategy that, reflecting a company's unique risk profile an appetite, leverages the complementary roles of technology and insurance to deter cyber-attacks where possible and trans the risk of those that cannot be prevented. However, the emphasis on cybersecurity spending and technology over other measures reveals that many businesses have not yet embraced this truth.

Ownership of Cyber Governance

Despite cyber risk being ranked as a high priority, governance and ownership of it generally do not align with that ranking Those who should be focused on cybersecurity are not, IT and information security roles continue to be seen as the prim owners of cyber risk management.

Businesses must build cyber resilience, approaching cyber risk as a critical threat that, with vigilance and application of b practices, can be managed confidently.

ABOUT JOHN MC LOUGHLIN

John Mc Loughlin is a visionary entrepreneur that has been involved in the setup and management of a number of start-up businesses. For the past seven years, he has been working towards changing the security landscape for SMEs in South Africa through his company, J2 Software, which provides solutions around reducing risk and improving compliance. John industry specialist and thought leader in the security space, and his particular areas of expertise lie in planning and strategising.
View my profile and articles...

For more, visit: https://www.bizcommunity.com