MARSH RISK CONSULTING

RISK IN CONTEXT BLOG – NOVEMBER 2018

How cyber ecosystems are reshaping risk management frontiers

Cyber, a term traditionally reserved for the futuristic world of sci-fi, is now one of the most hotly discussed topics amongst organisations of today. Have you ever wondered how we got here?

The co-existence and integration of computer technology which now pervades our lives has meant that you can find a "cyber" element in all aspects of our day-to day interactions – from smart phones and tablets to wearable technology to implantable devices with wireless interfaces – shaping the foundation of what has been dubbed by organisations as "cyber ecosystems."

Rapid advancement in technology coupled with globalisation has seen exponential growth in the adoption and application of technology. This in turn drives the need for efficient communication and a robust interconnectedness for organisations to improve shareholder value, increase market share, intensify competition for dominance and seek strategic integration and fiscal alignment.

Cyber ecosystems spawning from globalisation

In order to achieve the objectives of globalisation, organisations have implemented strategic information technology solutions, such as automation for higher productivity and product differentiation i.e. "better, faster and cheaper," to improve shareholder value. For example, the manufacturing sector saw their journey towards globalisation lead to rapid expansion of supply chain and logistics activities, which in turn enabled their technology advancements – both information technology and operational technology. The evolution of globalisation driving technology advancement has been similarly observed across various other industries.

As organisations seek market dominance and brand differentiation on a global scale, they find it imperative to embrace virtualisation and digitalisation using big data, real time analytics, Software as a Service (SaaS), in-app innovations and cloud hosting to enhance both customer experience and leverage brand equity.

For consumers, the consequence of these technology implementations is that products and services can only be accessed by using proprietary technology platforms interfaced to the organisations providing such products and services. This typically requires consumers to disclose personally identifiable information and in some cases their

biometric data for identity verification. In these scenarios, the cyber risks stem from a lack of native/embedded security mechanisms in these endpoints that make them vulnerable to hacking.

The technology implementations (hardware and software), the proprietary communication platforms, the data acquisition mechanisms, peer-to-peer social/business interactions through machine-to-human, human-to-human and machine-to-machine communication protocols and third party interactions are what constitute a **cyber ecosystem**.

Every organisation has a cyber ecosystem that is unique to their own operating environment. An organisation's cyber ecosystem can be more broadly defined as the interconnected information infrastructure of interactions among persons, processes, data, information and communications technologies, along with the environment and conditions that influence those interactions.[1] That is, a community (or ecosystem) of computers and the rules that govern their communication (interconnectedness) and behaviour, the Internet of Things (IoT).

Not without challenges

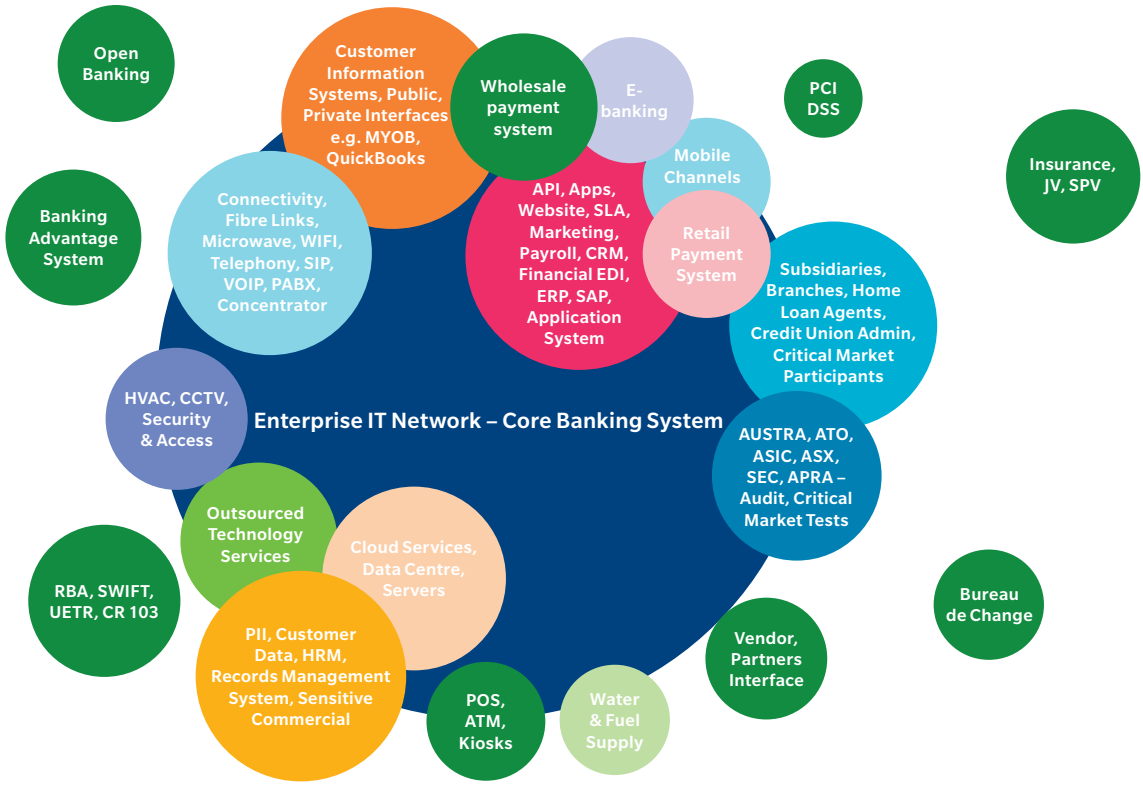
The effective deployment of technology solutions or digital platforms will rely on an organisation's understanding of the key risks in the context of their cyber ecosystem. It is imperative to give consideration to cyber ecosystem governance in a risk management context as means for ensuring that security and the right behaviours are promoted as a condition to engage within the perimeter of a cyber ecosystem.

In reality, this can be challenged by a mismatch between the rapid pace of advancement in technology versus the much slower pace of human learning and adjustment.

Malevolent activities in cyber ecosystems have increased exponentially with digitalisation. Likewise, malicious use of the internet has transformed the cyber threat landscape from one dominated by macro-based malwares to more complex script-based malwares developed by organised international criminals. This combined with a future stained by cryptojacking, ransomware and worming malware can be a daunting thought for businesses.

FIGURE 1 A typical Cyber Ecosystem Conceptual Map

SOURCE: MARSH DATA



1 https://definedterm.com/cyber_ecosystem

It's not all bad news – there are cyber insurance products that companies can purchase to mitigate some of these emerging risks. It is important that a company has an in-depth understanding of and periodically reviews what their cyber policy does and does not cover given the fast-paced and evolving cyber risk landscape. Ideally, a cyber policy should be tailored to a company's unique cyber risk profile. Every company should have a comprehensive cyber risk management strategy, and cyber insurance should be a core component. An essential financial instrument in the risk management toolbox, cyber insurance is complementary to cybersecurity, not an alternative.

Cyber ecosystem risk profile – the reality

Recent cyber risk review surveys conducted by Marsh across a number of different industries (aged care, financial institutions, manufacturing, education, power and utilities) in the Pacific region between 2016 and 2018 found that poor general management practices (25%) and poorly articulated business model or strategy (14%) were among the key contributors to an organisation's network breach. These two factors combined makes up almost 40% of an organisation's risk profile.

Organisations who took part in the risk reviews have identified the following key effects and challenges as a result of advances in cyber/technology capabilities:

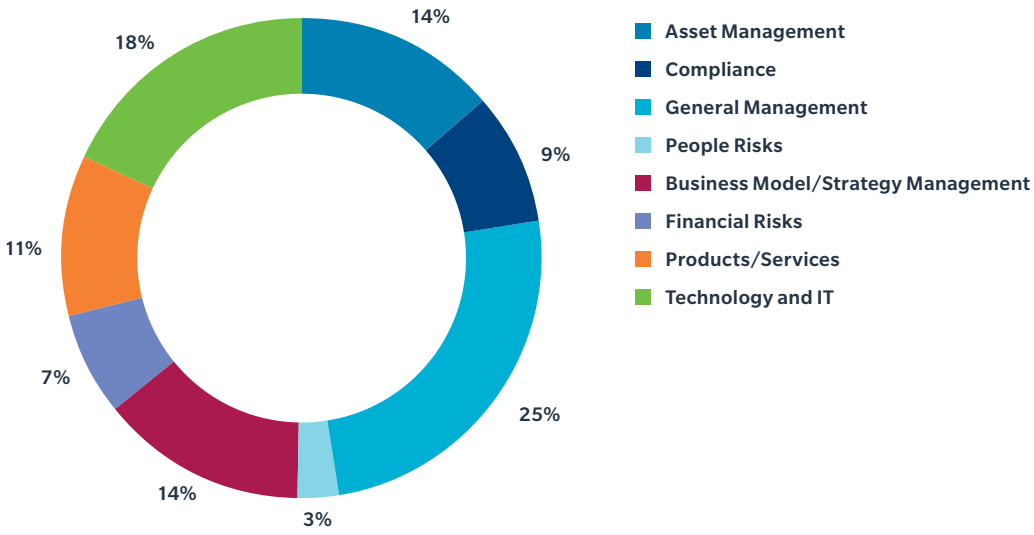
- Loss of face-to-face interaction
- Rapid changes in communication modes across different platforms
- Need for interoperability between different platforms
- Increased attack surface/exposure areas
- Greater expectations around management accountability by stakeholders and regulators
- Corporate governance and increased risk reporting requirements
- Likelihood of attracting high profile media attention during a cyber incident, thus impacting brand and reputation

Businesses are being further impacted by the blurred line between government and non-government malevolent parties as evidenced in recent network breaches (e.g., SamSam ransomware, Reddit data breach, state-sponsored cyber actors targeting network infrastructure devices including Australia). These incidents have shed light on the scalability and ease of propagation of cyber threat, making all organisations vulnerable.

FIGURE 2

Cyber ecosystem risk profile

SOURCE: BASED ON MARSH CLIENT DATA COLLECTED OVER THE LAST 12 MONTHS



How can businesses effectively manage cyber risks?

There are a number of approaches:

1. Manage internally by investing in specialist resources
2. Outsource cyber monitoring and protection functions through a Managed Service Providers (MSP)
3. Investing in cyber risk financing including insurance

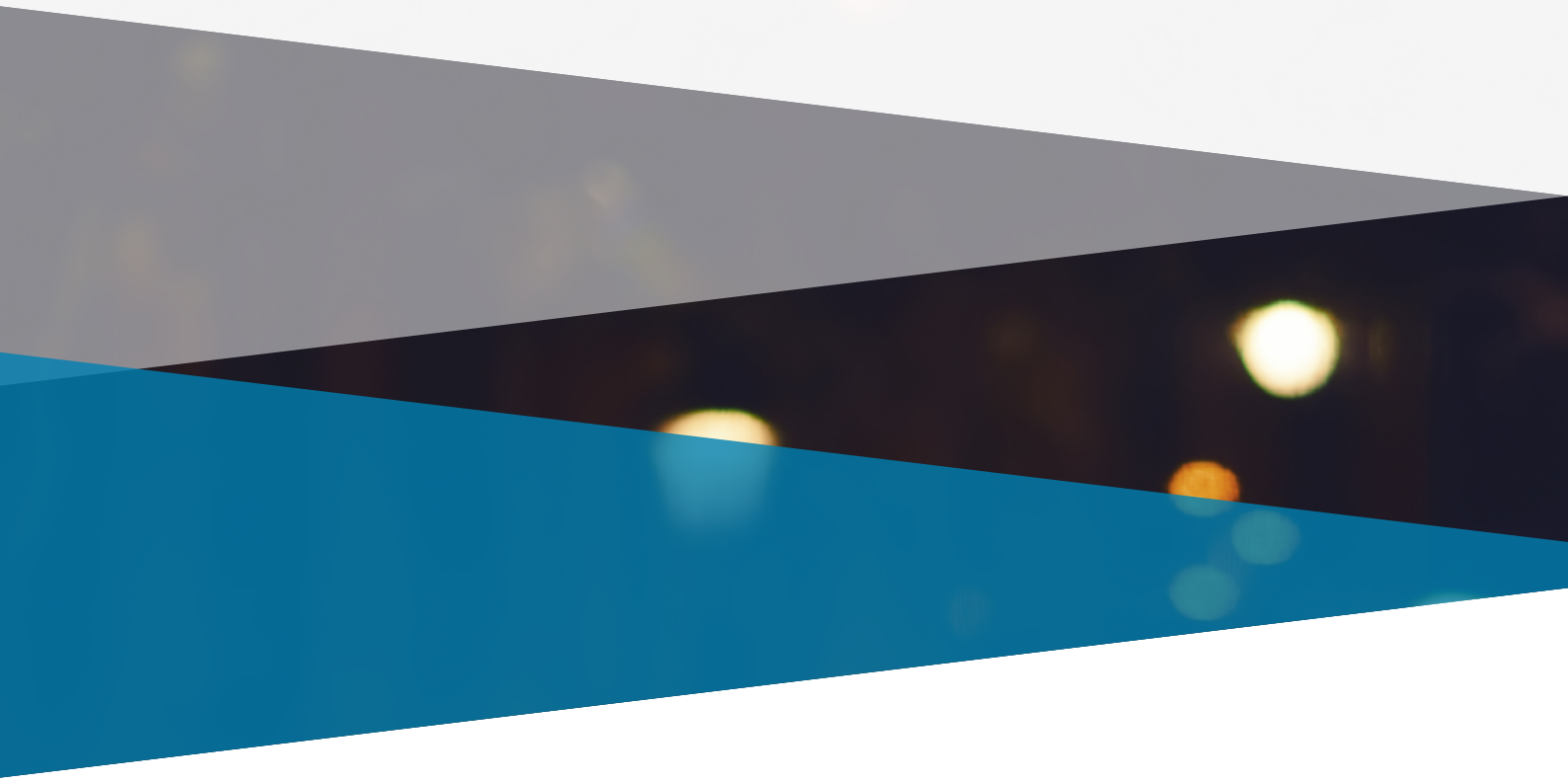
For many organisations, the option of outsourcing is preferred. Monitoring/managing cyber exposures is an ever-evolving task, working in a volatile environment where external factors and risks are constantly changing. Organisations that try to manage it all in-house (whilst still running their day-to-day business) often find themselves falling behind on the cyber front, as the pace of continually retraining and upskilling their staff fails to keep up with the rapid developments in the cyber world.

Where you have People, Process and Technology things will go wrong. To manage these risks, organisations must adapt their cybersecurity strategy to include vendors, partners and even customers. In addition, to secure their enterprise network as much as possible, they must closely evaluate their own people, processes and technology. Also, continually test their network for potential vulnerabilities or weaknesses; especially the lack of action on their part that could expose their organisation to penalties and reputational damage.

Organisations should be encouraged to undertake periodical Cyber Risk Reviews to assure the Board and executive management that Information Assurance is embedded in their Enterprise Risk Management Framework and Governance program. Cyber risk posture for businesses in same industry sector differ, what may be a key cyber exposure to one business may be less important to another.

Marsh Risk Consulting has extensive experience advising our clients on identifying and quantifying their cyber risks. Insurance solutions for cyber perils have evolved significantly over the last two years, insurance coverage has widen from “privacy breach only” to include complex triggers such as business interruption solutions packaged with cyber emergency response to resolve cyber incidents quickly and cost effectively. It is noteworthy, that while some insurance cover may exist within other insurance policies such as professional liability, fraud and crime or property policies, data extensions may exist elsewhere with exclusions for property damage and bodily injury, betterment and wear and tear, theft of funds, natural / physical perils.

Finally, organisations should ensure their Cyber policies have appropriate policy wording for the adequate coverage of broader aspects of executives’ fiduciary and regulatory obligations.



For more information, contact your Marsh representative or:

TUNDE FASHEUN
Senior Consultant – Marsh Risk Consulting
+61 2 8864 7213
tunde.fasheun@marsh.com