beazley

Article

Cyber security roundtable - Financier Worldwide

December 14, 2021

Beazley's Head of Cyber Services, Raf Sanchez, recently took part in the Financier Worldwide roundtable, which examined the issue of pandemic-generated disruption over the past two years, and the impact of burgeoning cyber-crime on the global economy. Below is an excerpt, featuring his input to this important discussion. The full roundtable featured experts from Arete, Control Risks, Cooley LLP, Microsoft, Perkins Coie LLP, Tokio Marine HCC and Zai Lab alongside Beazley, and can be accessed via the Financier Worldwide website.

Could you provide an overview of the cyber risks currently facing businesses, organisations and governments across the globe? What are some of the common types of cyber threats, and how have they evolved in recent years?

Organisations face a sophisticated, well-funded and innovative cyber-criminal landscape where there is very little chance of being punished, let alone physically apprehended. Although there are many threats aimed at acquiring sensitive government or commercial information and others that are destructive in nature, most cyber threats are those that have financial gain as their ultimate purpose. Within financially motivated cyber-crime we see automated attacks aimed at acquiring user credentials, for example email phishing campaigns, automated and manual attacks that leverage vulnerabilities in common platforms to obtain access to networks and, possibly most importantly, we see ransomware attacks that involve extorting organisations for the return of their valuable data in exchange for large sums of cryptocurrencies.

In your experience, how are companies coping with the regulatory environment around cyber and data? To what extent are they meeting their compliance requirements?

Privacy and cyber security laws, regulations and standards abound, and this is part of the problem for organisations that face a series of sometimes conflicting, or at the very least abstract, requirements that are often not aligned with the true challenges that organisations face.

While compliance with these requirements is critical, organisations also must balance these against operational concerns that may require crucial spend elsewhere. Compliance with laws and regulations not only improves cyber risk profiles but can also be used by organisations for competitive advantage. Supply chain risk has become a real concern over the past 18 months, so an organisation that can assure its customers of its robust cyber risk profile is likely to win out over competitors that cannot offer the same assurances.

What advice would you offer to boards and senior management in terms of protecting their company networks and the data housed within them? What key questions should they ask when reviewing and reinforcing frameworks, policies and processes?

Senior management should understand that to holistically protect their organisations, they must understand that electronic data and communication forms a crucial part of their organisations' reputation, goodwill, customer trust, revenues and operations. Buildings, stock and equipment are tangible and the risk of their theft or destruction may be easier to imagine than the risk of theft or destruction of intangible assets such as databases, websites or even goodwill and reputation. Electronic data and communications form a crucial basis for most organisations' operating models, so any framework, policy or process should ensure that those intangible resources are measured, assessed and protected.

Given that the chances of falling victim to a successful cyber-attack are high, how should companies prepare in advance to respond quickly and effectively to potential scenarios? What are the essential elements of the planning process?

First, organisations need to understand that cyber risk involves much more than 'cyber-attack'. There are many ways in which organisations can be damaged by the misuse of data and digital systems, from simple user errors to exposure to vendor problems, aggregated supply-chain risk and cloud platform outages. Organisations must understand the universe of challenges they face and identify the correct stakeholders that need to be involved in dealing with these. Once an organisation has this basic understanding it can begin to plan how to react. Ideally, it will identify gaps in its own capabilities and resources and seek to supplement these by buying cyber insurance, retaining external vendors and so on.

In what ways has the appetite for cyber insurance increased in recent years? How would you describe trends in the coverage, limitations and premiums on offer?

As organisations were forced to comply with lockdown restrictions at the beginning of the pandemic, they found themselves more exposed to a greater threat of disruption because they had inadvertently opened the door to cyber criminals who moved fast to exploit staff, processes and networks that were suddenly exposed beyond the corporate firewall through mandatory home working. This is a risk that is not going to go away; many organisations have said that hybrid and remote work are here to stay, and so the appetite and requirement for cyber insurance that protects against malicious attacks has naturally increased. It is important to not only cover organisations against these

risks, but to help them prepare better so that they are not caught on the back foot as cyber criminals seek to exploit new working practices.

Could you outline the main risks that cyber issues pose to D&Os on a personal level? What measures should a company take to ensure that robust D&O liability cover addresses cyber security and data breaches?

Many organisations think that they are resilient to cyber events, but our experience is that they are not. A large part of any cyber incident is the potential impact that it has on reputation, and it is difficult for organisations to pinpoint just how seismic the impact of a cyber-attack will be until it happens. Taking the right steps can stop a small attack from becoming something so serious that you must notify all clients, employees and regulators about it. Once that happens, organisations face huge reputational risks. We expect an increase in D&O claims linked to cyber-attacks in the coming years, and undoubtedly there will also be an increase in third-party litigation arising out of cyber events.

Looking ahead, how do you expect the cyber security landscape to evolve, in terms of its impact on companies? What major trends are on the horizon?

Unfortunately, the cyber-criminal landscape will continue to develop because the techniques, tactics and procedures currently being implemented are so effective at generating excellent financial rewards. Attackers are ‘reinvesting’ their gains in new tooling, research and resources so that they are constantly able to stay several steps ahead of organisations’ defensive efforts. There is also increasing specialisation so that certain groups concentrate on certain strategies, for example ‘initial access brokers’ specialise in selling access to networks that they have infiltrated, and this leads to those groups becoming very effective in their chosen area of operations. Despite the efforts of various stakeholders in the risk management space, from private organisations to insurers, tech vendors and governments, ransomware will continue to be a trend that we do not see dissipating any time soon. Article first published in Financier Worldwide

beazley