MICHAEL CORCIONE
PARTNER
HKA

Hostile Terrain – Navigating the Cybersecurity Landscape

Businesses must navigate a complex web of commercial, technological, skills and resource challenges – among many others – to manage risk. In one particular sphere, both complexity and risk have risen to business-critical levels. The cyber threat landscape and risks arising to corporations' most critical data, systems, and business processes are more ominous than ever. Recent attacks are unprecedented in sophistication and reach, as an increasing number of high-profile breaches are showing.

Attacks on IT product and service providers such as Microsoft[1] and Solar Winds[2] – both hit within the last nine months – expose thousands of client businesses worldwide. The malicious cyberattack against global IT provider Kaseya in July was one of the most viral malware infections so far, impacting some 1,500 organizations, from local governments to a Swedish supermarket chain.[3]

Businesses suffer interruption, reputational damage, and financial costs – ranging from lost revenue and remediation costs to ransom payments and potential penalties from regulators. No entity is off limits. The Health Service Executive in the Republic of Ireland had to shut down following a ransomware attack in May this year. Another cyberattack forced Brazil-based JBS, the world's largest meat processor, to close facilities in the US, Canada and Australia in May. CNA, one of the US's biggest insurance companies, with a suite of cyber insurance products, paid hackers $40 million to decrypt its highly sensitive client data in March.[4] Two months later, the southeast of the US saw panic at gas stations after Colonial Pipeline suspended operations before paying hackers a $5m cryptocurrency ransom.

Governments are trying to counter these constantly mutating cyber threats with increasingly sophisticated regulatory requirements. We are also seeing the enforcement actions and penalties that follow – notably, the $860 million fine imposed on Amazon by the Luxembourg's National Commission for Data Protection for alleged mishandling of personal information.[5] Although hotly disputed, this hefty penalty sets a precedent for other regulators and legislators.

It's prudent to remind ourselves of the nature of our adversaries. Organized cybercriminal gangs are extremely well resourced, in terms of cash, equipment and expertise. Unlike their corporate prey, they are not constrained by the costs of taxes, statutory employee benefits, bureaucracy, or regulation. Many also enjoy the added protection and/or support of state sponsors. While tech-savvy lone hackers operating from their bedrooms can still wreak inordinate havoc, now any actor with criminal intent and limited resources can access the necessary malware, stolen databases, IT infrastructure and hackers via 'cybercrime-as-a-service' on the Dark Web.[6] Ireland's HSE was a victim of the Conti ransomware-as-a-service (RaaS) operated by a Russia-based cybercrime group.

[1] https://gizmodo.com/the-biggest-hacks-of-2021-so-far-1847157024/slides/4
[2] https://gizmodo.com/the-biggest-hacks-of-2021-so-far-1847157024/slides/3
[3] https://gizmodo.com/the-biggest-hacks-of-2021-so-far-1847157024/slides/2
[4] https://gizmodo.com/the-biggest-hacks-of-2021-so-far-1847157024/slides/6
[5] https://www.finextra.com/blogposting/20702/amazons-886million-fine-for-alleged-breach-of-data-privacy--why-so-high
[6] https://av.sc.com/corp-en/content/docs/SCB_Fighting_Financial_Crime_Deep_dive_Cybercrime_as_a_Service_August_2017.pdf

HKA

Responsibility for recognizing and managing these clear and present risks cannot be siloed in IT and legal departments. Cybersecurity is a strategic priority demanding an enterprise-wide approach and close attention at board level.[7]

> "As well as managing compliance checks on an ongoing basis, the cyber 'arms race' demands continuous improvement of company defenses to deter new and ever-more advanced attacks"

Most of my engagements with companies have been reactive to a data breach or other event. This can be a new regulation that a company must adhere to, or in some cases, the company has failed to comply with a regulation, and is served remediation requirements by the regulator. Other incidents include service disruptions, system compromises, insider attacks, and monetary theft via the use of technology. All these events are calls to action – and all the more painful and costly because they are reactive, especially when the planned response is non-existent or inadequate.

An effective cybersecurity strategy not only has robust security policies, program plans and charters that are bespoke to the organization, it must also be proactive. As well as managing compliance checks on an ongoing basis, the cyber 'arms race' demands continuous improvement of company defenses to deter new and ever-more advanced attacks.

A solid Incident Response Plan (IRP) that is practiced and well understood is also critical so as to minimize the damage from any incident – to both finances and reputation. A key IRP component is ensuring you have identified all the necessary response resources, including forensic capabilities to investigate the root cause – this analysis is integral to any cybersecurity strategy.

Unfortunately, the cybercriminals enjoy another advantage over the organizations they select and probe. An acute shortage of skilled information analysts and security experts is hampering efforts to beef up companies' compliance programs and incident response capabilities. In a 2020 survey of cybersecurity professionals worldwide, more than half of respondents (56%) said that staff shortages were putting their organizations at risk. The annual (ISC)[2] Cybersecurity Workforce Study of its practitioner members projected a global skills gap of nearly 3.12 million people.[8] Asia-Pacific accounted for almost two thirds – more than 2 million posts. Latin America was missing more than half a million cybersecurity specialists, North America 376,000, and Europe 168,000.[9]

Emerging technologies only increase this under-supply and the onus on businesses to invest in their cybersecurity and privacy protection. Digitalization, cryptocurrency, blockchain and digital assets pose threats as well as competitive opportunities. The Internet of Things can open new backdoors for cybercriminals even as it expands networking and functionality for service providers and their customers. As major corporates such as Microsoft and AT&T accept Bitcoin payments, other businesses cannot afford to ignore this alternative means of exchange. Blockchain has

[7] https://www.reuters.com/legal/legalindustry/what-boards-directors-need-know-about-cyber-incident-response-2021-08-18/
[8] https://edition.cnn.com/2021/05/28/tech/cybersecurity-labor-shortage/index.html
[9] https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

multiple ramifications for streamlining efficiency and enhancing security – from supply chain traceability to financial transactions and smart contracts to high-value consumer goods. But with this and other technologies comes complexity and novel risks.

Risk management and incident response require specialist, in-depth expertise in cybersecurity, digital forensics, and remediation. This is in addition to the legal resources required to resolve questions around post-incident reporting, employee and corporate liability, privilege and negligence, litigation, and expert witness testimony.

We must decode the mounting complexity of this cyber landscape to chart a secure path for businesses and their clients and customers.

If you require any further information, please contact Michael Corcione at michaelcorcione@hka.com.