CYBER
TRENDS

IRIDIUM
RISK SERVICES EVOLVED

NAVACORD®

What to Expect and Look for in 2023

Wesley Robinson, B.Comm, CPLP
Risk Advisor, Iridium Risk Services

1. THE INCREASINGLY STRINGENT REGULATORY ENVIRONMENT AND BILL C-26

On June 14, the House of Commons introduced an “Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts”. Otherwise known as Bill C-26, this bill has since passed its first reading in the House of Commons and assuming everything goes to plan, will likely be passed into law by September, 2023 in its current form. The act itself is emblematic of a larger trend, where currently 137 out of 194 countries in the World have legislation to secure the protection of data and privacy. Of course, the level and type of regulation across countries varies widely. Countries such as the United States tend to focus on industry or sector specific regulation, and don’t enforce any kind of overarching federal regulation. Compare this to the European Union, who has had their General Data Protection Regulation in place since 2016 that captures all EU member states and does not discriminate by industry. As Bill C-26 is set to become law in Canada, it will add an additional layer of cybersecurity compliance for Canadian companies who broadly deal in industries that are vital to Canadian security. The law will capture a broad swathe of Canadian GDP in industries like Telecommunications, Banking, Power Generation and Transmission, and Transportation. Bill C-26 would provide the Privacy Commissioner the authority to make binding orders, including the power to impose fines and increase the maximum fines for privacy violations under the Personal Information Protection and Electronic Documents Act (PIPEDA). The bill also seeks to expand the scope of PIPEDA to cover additional organizations and sectors, including political parties, and to enhance the transparency of data processing activities by organizations. The implications for cyber risk professionals, legal professionals, and risk managers includes another layer of compliance and legislation to concern oneself with in advance of having a cyber breach.

2. CYBER WARFARE AND NATION STATE THREAT ACTORS

Nation-state actors have always played a significant role in the cyberattack landscape, with many countries using their cyber capabilities for intelligence gathering, theft of sensitive information, and other malicious purposes. Nation-state actors have the resources and expertise to carry out complex and sophisticated attacks that can have a significant impact on organizations and individuals. These attacks can be difficult to defend against and often cause the most damage to entities such as government agencies, critical infrastructure providers, and large corporations. In its 2021 Global Threat Report, CrowdStrike estimated that nation-state actors accounted for approximately 25% of all cyber attacks in 2020, with most of these attacks originating from China, Russia, and North Korea. Other studies estimate that nation-state actors may account for as much as 40% of all cyber attacks, depending on the region and the sector being targeted. Many cybersecurity technology companies and government agencies have been reporting lower incidents of Russian state-sponsored hacking activity as a result of the continuing Russia-Ukraine War. However, the war continues to highlight the use of advanced tactics such as malware campaigns and the targeting of critical infrastructure, government and military organizations. These attacks are part of a larger trend of cyber activity by state-sponsored groups in the Eastern European region including official and un-official Russian allies such as North Korea, Iran, Syria, and China. Lloyd’s of London has responded to this long-term threat by positioning their cyber insurance policies to take steps that add specific clauses to limit systemic exposure to state-backed attacks of a magnitude that would cause a significant impact on the target country. It is yet to be seen how easy these clauses will impact claims scenarios where more often than not state-backed threat actors do not take official credit for their attacks, and instead rely on proxy groups to inflict damage. What is certain is that cyber warfare is not going anywhere, and will require constant vigilance from governments, private industry, and the risk management community at large to combat.

3. CYBER EVENTS AND THE RESPONSIBILITY OF THE BOARD OF DIRECTORS

One trend that is certain to continue in 2023 is the Board of Directors response to a Cyberattack. Directors have come under increased scrutiny over the last decade to take data protection and security seriously as well as to guard against potential revenue loss that can stem from cyber attacks. All over the world, Boards have been called to task to safeguard their organizations and have even been drawn into legal action in highly visible breaches such as those that affected Target in 2013, Equifax in 2017, the Marriot in 2018, Capital One in 2019, and SolarWinds in 2020. In most cases, directors are less likely to suffer personal liability arising out of these breaches while the organization suffers business interruption or reputational damage, which can negatively impact the share price of a public company and can seriously harm the outlook of a business as consumers and vendors lose trust. For this reason, the Board must continue to take these threats seriously and should be heavily involved in the business continuity planning process for the companies they advise, ensuring that incident or disaster response plans are in place and regularly tested throughout the organization.

4. THE RISING COSTS OF REMEDIATION

According to the 2022 Cost of a Data Breach Report by the Ponemon Institute, the global average cost of a data breach is $4.41 million USD, which is a significant increase from the previous years of $3.86 million in 2021 and $3.79 million in 2020. This same report has also pointed out similar increases in the cost per stolen record. These trends are symptomatic of a larger issue as responding to a cyberattack has become more costly year over year, and when compared to the cost of a breach prior to the Covid pandemic, most sectors have seen exponential increases in cost. There are many reasons for these increases, including the growing complexity of attacks, the growth of the cyber insurance market, and the need for specialized expertise when a breach occurs. In fact, the cost of remediation appears to have risen in line with the rise in premiums for cyber insurance. According to a recent report by Howden Insurance Brokers, the last two full quarters (4Q21 and 1Q22) saw average annualised increases of more than 120%. The Insurance industry however appears to be settling after multiple years of significant rate increases, and there are signs that 2023 will see a more stable cyber insurance market than the three years prior. The complexity of attacks, the geopolitical landscape, and the cost of niche-specific experts are all likely to continue a general upward trend in costs that will make it difficult for cyber insurers to keep costs manageable and loss ratios sustainable.

5. ARTIFICIAL INTELLIGENCE

Only two months after the release of ChatGPT by Artificial Intelligence (AI) research and development firm OpenAI, the world has been engrossed by the capabilities of a chat function that can not only answer difficult questions but can do so in full sentences complete with rationale for its argument. This technology goes beyond traditional search functions, providing a full answer to your question instead of providing sources for the user to comb through and formulate an answer for themselves. Artificial Intelligence models such as ChatGPT have provided a stark reminder to the average person that artificial intelligence is here for good, with the potential for everything from mass layoffs to an inability to be able to differentiate human generated articles from computer generated thought leadership. What does this mean for cyber risk? AI can be used to defend against cyber criminals with smart monitoring and EDR solutions but also have the potential to automate and improve many aspects of the cyber attack process, making it easier for attackers to carry out sophisticated and targeted attacks. For example, AI can be used to automate the process of discovering and exploiting vulnerabilities in software, as well as to carry out phishing attacks that are more personalized and effective. AI can also be used to automate the analysis of large amounts of data to identify patterns and anomalies that may indicate a security breach. These tools can and have been used to create convincing fake content, such as fake images and videos, that can be used for social engineering attacks, funds transfer fraud schemes, and deepfake scams. It is yet to be seen whether artificial intelligence will prove to be a force for good or bad in the world, but as with any new technology, the only certainty is the years of uncertainty that lie ahead.

Sources:

- https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
- Check Point Software Technologies Ltd. (2021, November 22). Check Point Research: Ukrainian organizations under cyber attack by Russian APT groups. [Press release]. Retrieved from https://www.checkpoint.com/press-releases/check-point-research-ukrainian-organizations-under-cyber-attack-by-russian-apt-groups/
- Kaspersky. (n.d.). Ukrainian cyber attacks by Russian-speaking groups on the rise. [Press release]. Retrieved from https://www.kaspersky.com/about/press-releases/ukrainian-cyber-attacks-russian-speaking-groups-rise

Contact an Iridium Risk Advisor today to learn more about prioritizing cybersecurity and protecting your organization against ransomware threats.