The New Era of Cybersecurity Sovereignty

By Tim Wallen, Regional Director for the UK, US and Emerging Markets, Logpoint

This article takes a look at the growing role of cybersecurity on the global level.

Ever since the US banned Kaspersky products from government departments back in 2017, there have been questions raised over the potential for nation states to use cybersecurity solutions to their own ends. More recently, we've seen Chinese technology come under question, with Huawei products due to be stripped out of the UK's 5G infrastructure by 2027 and TikTok banned in the UK parliament.

The cumulative effect of these actions is an increase in awareness among organizations of their dependence on their cybersecurity defenses. They now need to know how these are built and whether they can be trusted. For this reason, we've seen initiatives such as the Software Bill of Materials (SBOM), which aims to create transparency by detailing the tech that has gone into constructing software components.

Trust and transparency

SBOM has proved invaluable, improving supply chain security and enabling organizations to quickly determine if their software is vulnerable to exploits that then come to light, a good example being Log4J based on Java, which is one of the most widely deployed pieces of open source software in the world. Without SBOM, it would have taken organizations much longer to track down which Java applications had used the code.

But now sophisticated attacks perpetrated by nation state actors have also heightened tensions. The invasion of Ukraine unleashed a litany of state sponsored cyber-attacks against their critical national infrastructure. This prompted the FBI and CISA [1] in the US and the NCSC [2] in the UK to warn businesses of additional indicators of compromise (IoC) associated with new strains of malware. And sure enough, earlier this year reports [3] began to emerge of Russian hacktivists targeting critical national infrastructure in the UK while a leak of classified US intelligence documents is believed to have revealed that the pro-Russian group Zarya had already infiltrated Canadian gas networks with the aim of disrupting supply.

In addition to this geopolitical agitation, businesses have also had to contend with the lasting effects of the pandemic which have seen a shift in working practices to a remote or hybrid workforce, resulting in increased exposure of company assets. They've also had to deal with the cost of living and energy crises which have seen costs spiral and questions raised over how countries can become more self-sufficient in their food and energy production.

Such issues have focused attention on the need to ensure business resilience. The ability of the organization to adapt to these disruptions while maintaining business as usual (BAU) and safeguarding its people and data is of increasing importance. Cyber resilience takes that a step further and is the ability of the business to protect itself from cyberattacks through its detection, response and recovery capabilities.

If that sounds familiar, it's because it also aligns with United Nation's Sustainable Development Goals (SDGs), which aim to create a blueprint for peace and prosperity. The seventeen goals formulated in 2015 are, says the UN, an urgent call for action by all countries which need to be achieved by 2030. From a commercial perspective, the SDGs place the onus on businesses of all sizes to do business responsibly and to pursue opportunities to solve societal challenges. Particularly relevant here are SDG #9 which seeks to advance the use of a resilient infrastructure and SDG #16 which calls for effective, accountable and transparent institutions or in this context, businesses that take steps to keep their data secure and hold themselves accountable to their staff, customers, and partners.

These concepts are also reflected in company Environmental, Social and Governance (ESG) policies. The World Economic Forum [4] has called for cybersecurity to be considered part and parcel of ESG which are now mandatory of many businesses. It states that cyberattacks present a huge risk to the value of companies and ultimately the stability of society. Moreover, it warns that businesses are using cyber insurance as a safety net at present to safeguard against risk instead of implementing the necessary governance, which is neither advisable nor sustainable.

Bolstering the business

What all these changes point to is the need for businesses to become more proactive in their approach to cybersecurity. Not only is this in their own interests but it's also in the interests of the wider society in which they operate. Continuing political unrest is also focusing attention on national self-sufficiency and so there's a growing need to have in place cybersecurity that is trusted. As a result, organizations are now looking to improve their resilience and protect their digital transformation through cybersecurity sovereignty by sourcing technology solutions and support closer to home.

Much like the concept of data sovereignty that saw businesses place their data in the cloud locally for compliance and data governance purposes, cyber sovereignty sees organizations favor security solutions that can be provided and supported locally. The components within these solutions, their code and ongoing development are all known and verifiable. Moreover, the solution will have been designed in accordance with regional as well as national compliance obligations, such as the second version of the Network and Information Systems (NIS) Directive, NIS2, which is now being implemented and will be mandatory from October 2024 across the EU. Plus of course the vendor will store data within the jurisdiction, meaning it complies with data protection regulations.

It's an approach that makes sense given that the types of attacks being leveled at organizations are often geo-specific. Phishing and ransomware attacks are localized and targeted, for instance, with the second version of the Locky [5] malware variant even found to have been coded to unencrypt data if the endpoint was located in the ransomware group's home country of Russia. So sharing regional intelligence makes sense, which is why we've seen ransomware tracked regionally [6], such as in the Middle East and North Africa (MENA) region, which has seen a surge in particular malware variants such as RedLine, Remcos, NjRAT, Emotet, and AsyncRAT; information which defenders can then use to focus their threat hunting and defense.

According to reports [7], the US is the most targeted country in the world when it comes to being hit by malicious traffic associated with web applications (66%) and cyber espionage (54%). It also tops the charts regarding the average cost of cybercrime. But the US is also the second-best prepared country to defend itself against cyberattacks principally because it has home-grown cybersecurity solution providers that can answer its needs.

In addition, we're seeing a renewed focus on the resilience of critical infrastructure and more stringent regulation. The NIS2 referred to earlier, now even extends beyond CNI providers, compelling businesses associated with essential and vital national services to assess risk and implement rigorous cyber security processes, thereby bringing thousands of entities within scope. The UK government [8] has confirmed that it will take similar steps to improve cyber resilience.

Making the transition

These demands for greater resilience will undoubtedly force businesses to reappraise their current systems and processes and look at where they can strengthen defenses. But it also provides an opportunity to benefit from tailored threat intelligence. Technologies currently utilize international attack frameworks such as MITRE ATT&CK which detail the tactics, techniques and procedures (TTPs) associated with specific attack types, and act as a sort of global library for threat intelligence. But if defense technology is developed and supported regionally, this threat intelligence can be supplemented with other regional intelligence, like in the MENA example above, and provide real valuable insights.

The Nordic Council, for example, is seeking to create a common cybersecurity strategy [9] across the Nordic region with the Nordic Defense Cooperation (NORDEFCO) set to play a key role in the development of cross-border collaborative cyber security solutions. The aim is to share threat intelligence between Denmark, Finland, Iceland, Norway, and Sweden to futureproof society against cyber threats.

The challenge will be how to swap out technology cost effectively and without any disruption. For some businesses, there will be a need to let systems amortize but for many already looking to replace systems such as legacy Security and Incident Event Management (SIEM) solutions, it makes sense not just to look at replacing this with a modern SIEM that is capable of threat detection and response but one that is developed within their continent. Replacing such legacy infrastructure can also pave the way for the organization to use new emerging technologies.

Moving to a single converged Security and Incident Event Management (SIEM) platform, for example, can help by allowing the business to monitor endpoints, network access and look for anomalous behavior without the need to invest in point solutions such as Endpoint Detection and Response (EDR). Using an agent, endpoint logs and telemetry can be fed into the SIEM, analyzed, and then automatically investigated and contextualized using another integrated solution: Security Orchestration, Automation, and Response (SOAR).

This is just one way organizations can embrace the concept of cybersecurity sovereignty and make the transition in an efficient and cost-effective manner. There are, of course, plenty of others, from sourcing a local Managed Security Service Provider (MSSP) if you outsource your security to forming regional threat intelligence sharing alliances with others within the same sector. But ultimately, doing so promises to futureproof the business against attacks going forward from threats such as covert surveillance, data exfiltration, or ransomware that could result from future political conflict.

References

1. "CISA and FBI Update Advisory On Destructive Malware Targeting Organizations in Ukraine", CISA, 28 April, 2022. https://www.cisa.gov/news-events/alerts/2022/04/28/cisa-and-fbi-update-advisory-destructive-malware-targeting-organizations-ukraine
2. "NCSC advises organisations to act following Russia's attack on Ukraine", NCSC, 18 March 2022. https://www.ncsc.gov.uk/news/organisations-urged-to-bolster-defences
3. "Russian hackers targeting Western critical infrastructure, UK says", Reuters, 19 April 2023. https://www.reuters.com/world/europe/russian-hackers-targeting-western-critical-infrastructure-uk-says-2023-04-18/
4. "Cybersecurity is an environmental, social and governance issue. Here's why", World Economic Forum, 1 March 2022.

https://www.weforum.org/agenda/2022/03/three-reasons-why-cybersecurity-is-a-critical-component-of-esg/

5. "A closer look at the Locky ransomware", Avast, 10 March 2016. https://blog.avast.com/a-closer-look-at-the-locky-ransomware
6. "Growing malware families in MENA demand increased threat intelligence, says expert", ITP.net, 18 April 2023. https://www.itp.net/security/growing-malware-families-in-mena-demand-increased-threat-intelligence-says-expert
7. "List of Countries which are most vulnerable to Cyber Attacks", Cybersecurity Insiders. https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks/
8. "Government response to the call for views on proposals to improve the UK's cyber resilience", 30 November 2022. https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/outcome/government-response-to-the-call-for-views-on-proposals-to-improve-the-uks-cyber-resilience
9. "Nordic Council seeks deeper regional cybersecurity cooperation", Defense News, 27 March 2023. https://www.defensenews.com/global/europe/2023/01/17/nordic-states-to-develop-common-cybersecurity-strategy/