# Creating stronger cybersecurity maturity

## Complementing your security intelligence with trusted consulting expertise

**Organizations across Asia Pacific are faced with a myriad of daily cyberthreats and risks across often-complex technology environments, which are also likely amid transformation. No business is immune to cyberattacks, irrespective of industry, location, budget, resources or capabilities. To stay ahead of attackers, trusted cybersecurity consulting expertise can be a major asset for Asia-Pacific CISOs, providing deep insights into threats, as well as helping to secure adequate sponsorship from the business.**

According to the NTT Security Holdings Global Threat Intelligence Report 2022, 24% of all incident response engagements with NTT's Digital Forensics and Incident Response team in 2021 were related to ransomware – a 240% growth from just 7% in 2019. The challenge, however, is understanding how your organization can best prepare against such attacks. To independently cover all bases is impossible, but a trusted security partner can help make your cybersecurity investments work smarter as well as harder.

Industries with high levels of cybermaturity, such as financial services, remain targets because of the prized data they hold. But the introduction of more rigorous regulations has forced adversaries to widen their focus and target more vulnerable organizations such as those in manufacturing, retail, hospitality and other industries undergoing significant digital transformation.

The NTT Security Holdings Global Threat Intelligence Report 2022 also highlights how geopolitical tensions and ongoing supply chain disruption have affected industry targeting. Attacks more than doubled over the past year in the technology, telecommunications, and transport and distribution sectors. Technology and telecommunications attacks increased because of a greater reliance on digital environments and shift to remote working. Notably, attacks on critical infrastructure are escalating, targeting technology, transport and manufacturing enterprises.

> “ Industries with high levels of **cybermaturity, such as financial services, remain targets** because of the prized data they hold.

 

Organizations in these industries feel the impact of attackers causing chaos or disruption, or extorting vast sums of money through the theft of valuable data or intellectual property. They may be unable to continue their business operations, or suffer significant damage to their brand reputation and competitive advantage. But, in addition to external threats, enterprises across the board need to be just as conscious of internal threats, from accidental data breaches by employees to malicious insider sabotage.

**Train employees to work in a security-aware manner** – not to be the weakest link, nor the strongest link, but a key component

Because of an increased reliance on digital systems for communication, storage and processing information, there is a greater need to step up cybersecurity awareness training. It is much easier for an adversary to take advantage of someone who doesn't know what a phishing email looks like than to fool an IT professional into giving up credentials or personal information that might compromise the security of the entire organization.

## Integrating secure-by-design into cloud and network transformation

Threat actors are taking advantage of the lack of hardening on security configuration, configuration drift and lack of understanding of the shared-responsibility model implemented by organizations that have shifted to cloud-based services. Digitalization within industries such as manufacturing, for example, has progressed at a rate of knots across both the IT and operational technology (OT) environments, such as industrial networks.

The shift of workloads from on-premises data centers to public cloud is happening quickly, creating new challenges for security teams – particularly, how to secure an environment that is dynamic, highly distributed and potentially vulnerable by design. As a result, attackers are targeting application layers at unprecedented levels. According to the NTT Security Holdings Global Threat Intelligence Report 2022, web-application (42%) and application-specific (30%) attacks continue to rise. These two attack types accounted for 72% of all attacks (32% in 2018, 55% in 2019, and 67% in 2020). Specifically, the Asia-Pacific region experienced the largest increase in web-application and application-specific attacks.

There are huge benefits in moving to the cloud, such as increased agility and flexibility, as well as the ability to innovate faster. But there can also be issues that need addressing, namely cloud misconfigurations. The shift to operating multicloud environments is complicated, and it can be difficult to detect and manually remediate mistakes. Respondents to the VotE: Cloud, Hosting & Managed Services, Workloads & Key Projects 2021 survey cited concerns about security (46%), controlling cost (39%), data sovereignty (30%), lack of platform expertise (30%) and vendor lock-in (25%) as factors limiting a greater – or more effective – use of cloud.

The impacts of hybrid and remote working are also being felt. Security threats now come from everywhere, thanks to hybrid working – on-premises, in the cloud, and from the IoT sensors you're adding to your network. Every new device brings a new security threat. Now, 87% of top-performing organizations are investing in their cybersecurity capabilities, compared with just 41% of underperformers. A key focus in this area is the move from perimeter-based security to identity-based security (2022 –2023 Global Network Report).

Network modernization has led to an increasing number of systems becoming linked across multiple entities — including overseas offices, subsidiaries, educational institutions, factories and laboratories. And while this has brought significant productivity and efficiency benefits, it also opens the possibility of a major security incident if adequate security and privacy controls weren't properly considered and embedded into the initial design phases. Regardless of the drivers, organizations should assess their current state before designing, operating and managing IT/OT systems and processes.

> However, the question often arises:"Who's securing what?" **The increased use of public cloud and highly connected supply chains has exposed new and challenging attack surfaces, leaving many vulnerable to cyberattacks.**

 

## The battle for skills

Against the backdrop of transformation efforts is a dearth of security talent. The increased demands being placed on security teams to strengthen cybermaturity often can't be matched with the right skills and resources to satisfy the need.

And that need is growing to be one that requires a more experienced and strategic understanding of cybersecurity, both in terms of its role and impact across the business. Teams who have both a deep and wide understanding of technology as well as a "data-driven mindset" can help map current technology capabilities back to the business risk for better prevention, detection and response processes.

Skills also need to span an increasing variety of areas, namely the network, cloud, OT, IoT, applications and much more across the technology stack. This complex spread has meant gaining visibility across the entire technology environment is an almost impossible task for many organizations. The adage, "you can't manage what you can't see" is perhaps most pertinent when it comes to cybersecurity.

With a team so clearly stretched on all fronts, it's little wonder that the CISOs of many enterprises bring in additional cybersecurity expertise to enhance and complement their own team's capabilities.

## Greater visibility, knowledge and understanding

Knowledge is power. The more (read, "relevant") information you have, the better prepared you are to thwart attackers. With so many facets of security to focus on and invest in, it often appears a neverending battle to cover all bases. However, knowing what types of attacks your organization might be subject to means you can place greater emphasis on areas where you feel most vulnerable, utilizing constrained resources more effectively and efficiently.

Being able to proactively profile your organization's characteristics, such as industry, digital footprint and assets, against different attack trends enables a more accurate picture of the type of attack you might be subject to. Building a profile will help you think like an attacker, such as identifying how they might gain entry to your network and where the weakest points are. This helps you further prioritize security investments and training where it matters most.

For example, it stands to reason that in healthcare, patient data and personal information is most targeted by threat actors seeking to make financial gain. Yet in the pharmaceutical industry, where research and development and intellectual property are significant focus areas, it makes sense to ensure security efforts are focused on protecting these assets and the technology layers surrounding them. On the other hand, a manufacturing or critical-infrastructure organization needs to grapple with the threat of systems or process disruption far more than a data breach, and security and resilience controls need to be applied in that context.

External to your organization, vendor - and product - neutral security consulting competencies add even further depth to your understanding, depending on their expertise. For example, a multifaceted security partner with capabilities across the network, cloud, edge and data center domains can provide significant data and intelligence to inform services and help raise your cybermaturity levels.

> The heightened prevalence of threats, both internal and external, requires security professionals with proactive skills who can hunt the threats before threats hunt down the organization. **To stop attackers in their tracks, it is essential to know your assets and data flows, identify anomalous activities and compare them against the baseline of the expected set of behaviors.**

 

> As organizations are faced with the **challenge of identifying, measuring and mitigating cybersecurity risks, experts can provide guidance on how best to achieve their objectives while staying compliant with regulations and frameworks.**

## Regulatory frameworks and compliance

The need for security consulting services has never been more apparent, particularly as consulting provides a greater opportunity to understand your as-is state – that is, gaining greater visibility into your operating environment and where you currently stand – an essential, but often missing cog in the wheel of building greater cybermaturity.

Following on from this is the ability to define your to-be state, and what your desired levels of maturity are in line with the needs and requirements of your organization – here, compliance and adhering to regulatory frameworks play a major role. As organizations are faced with the challenge of identifying, measuring and mitigating cybersecurity risks, experts can provide guidance on how best to achieve their objectives while staying compliant with regulations and frameworks. The global trend towards security consulting services is expected to grow significantly in the coming years as organizations seeking to implement effective incident response plans need to build a solid understanding of what it will take to prevent an incident from happening in the first place.

Those with global consulting capabilities are especially useful when it comes to helping businesses understand and apply cybersecurity frameworks (such as NIST CSF) consistently across a variety of information assets, particularly as these relate to the network, cloud, applications, industrial networks and so on. This helps to enable a consistently applied process across all facets of your organization, in any location in the world. Although the NIST cybersecurity framework is not a panacea for all your security needs, it does provide a solid foundation on which to build your own incident response plans and strategies.

There is also a multitude of frameworks and regulations to consider across different regions, countries and industries. The complexity and expectation of understanding these could have dramatic impacts if not followed correctly. Getting help to understand where you might fall foul of regulators is invaluable. Even more so is being able to understand where potential attacks could arise because of vulnerable areas within your organization.

## Assess to progress

Security teams are under significant pressure, and with so much to cover, it can often feel impossible to even know where to begin. Yet, the best course of action is to simply start. Whether that's with a cloud security maturity assessment, OT security assessment or an incident response/ managed detection and response (IR/MDR) readiness assessment, gaining visibility of where you're at and then working out where you need to be is the first step in raising the level of cybermaturity across your organization.

Begin the process of understanding where you're most vulnerable, based on a better understanding of your profile and the type of attacks you could be subject to. Rome wasn't built in a day, and you certainly won't be able to do everything you want to. But investing budgets and resources in the priority areas that matter most will enable you to minimize the potential risks to your assets, such as supply chain vulnerabilities. By strengthening your cybermaturity and resilience you can ensure service delivery is not disrupted – maintaining customer trust and preventing loss of revenue.

To understand more about **NTT's cybersecurity consulting capabilities and how we can help your organization improve cybermaturity levels, visit** https://services.global.ntt/

NTT DATA

 


NTT DATA