Global Threat Intelligence Center

Monthly Threat Report

December 2021

Contents

Cybercrime's big hits of 2021

Lead Analyst: Bruce Snell, Vice President, Security and Transformation, US

It seems, year after year, attacks increase in impact and visibility and 2021 did not deviate from past patterns. Instead of looking at the increase in numbers of incidents, breaches, and vulnerabilities, I'd like to take a look at some of the trends that have caught the attention of the security and business worlds.

Cyberattacks directly impacting the physical world

If there was one breach everyone remembers from 2021, it's the Colonial Pipeline breach. It was such big news that I was fielding questions from friends and family who have absolutely no involvement in cybersecurity. The breach was top of everyone's minds because it had a direct physical impact on peoples' lives. When Colonial discovered ransomware had infected their billing systems, they quickly shut down the pipeline. They did so to prevent the spread of malware into the OT (operational technology, or the physical systems responsible for their operations) side of their business, and because they couldn't bill for any of the fuel they would be delivering to customers.

Typically, a breach of this size results in mass emails telling people to change their passwords and monitor their credit reports. This time, the breach directly resulted in gas shortages and fistfights at the gas pumps. While Colonial received quite a bit of public outcry for the pipeline being down, it was a smart move on their part to have a controlled shut down instead of allowing attackers to lock it down using ransomware. This attack represented the most significant cyberattack against critical infrastructure in the United States to date. It served as a wake-up call to the general population and the federal government, increasing awareness and concern over the safety of the nation's key assets.

> Kaseya showed that **attacking a middleware or infrastructure provider** was a reliable way for cybercriminals to focus higher up the supply chain.

Attacks against the supply chain

Another big trend in 2021 was attacks against the supply chain. We've seen significant incidents such as the breaches of Kaseya and Solarwinds (which happened in 2020). What made these two attacks unique was not the exploits or methods used to gain access, but the 'trickle-down' impact felt by the end-users. Where some people considered Solarwinds an outlier, Kaseya showed that attacking a middleware or infrastructure provider was a reliable way for cybercriminals to focus higher up the supply chain and have their malicious payload distributed to thousands of organizations with relative ease. Good operational and security practices call for IT organizations to keep their applications up to date to prevent the exploitation of vulnerabilities. However they need to remain aware of the risks that an organization can be breached while following industry best practices around patching. Cybercriminals can infect the updates at source.

Federal regulation or industry regulation?

A common thread in some of the more visible attacks of 2021 was an increase in the federal government's engagement in response to significant breaches. While federal regulations like HIPAA, GLBA, GDPR, and others have been around for some time, one could argue they have not had as much an impact on cybersecurity as intended. The federal government took an active role in the investigation (and partial recovery of the paid ransom) of the Colonial Pipeline breach. President Biden went so far as to issue an executive order intended to improve the nation's cybersecurity posture.

While the federal government tries to respond to these increasing cyberthreats, is this response the most effective solution? Have past cyber regulations helped improve our overall security level? Perhaps the best approach is to rely on the industry itself. Industry-wide best practices can bring us much closer to dealing with the issues at hand because they can go to a deeper level of relevant detail - specific directions around steps to secure an environment are much more effective than a general set of guidelines that typically make up a governmental regulation.

We should also push the market to demand more from vendors. Organizations could require a higher level (along with proof) of cybersecurity from their vendors. If this happened, we could see more rapid adoption of cybersecurity best practices. Organizations should be driving security as a competitive differentiator. If vendor B can match the price and quality of the other vendors competing for your business, and show proof of a higher level of security, it could end up saving you money in the long run when the next Solarwinds-type breach comes out.

Ransomware, everywhere

Of course, we can't look back at 2021 without cybercrime's public enemy #1, ransomware. We've not observed a measurable increase in the technical sophistication of ransomware throughout 2021, but there has been a dramatic shift in the 'business' of ransomware. We observed a rise in two areas of ransomware: double extortion and ransomware-as-a-service (RaaS). Double extortion ransomware starts with the traditional method of encrypting data and demanding a ransom to unlock it. It then adds data exfiltration into the mix, copying the encrypted data to a remote location, typically in the cloud. The attacker then tells the victim of double extortion – that, in addition to paying to unlock their encrypted devices, they must pay an additional amount for the attacker to delete their exfiltrated data. If the victim doesn't pay, the attacker either publishes the data online or sells it off to other cybercriminals for their nefarious use. While double extortions were rare in 2020, by the middle of 2021, they had become commonplace. Some attackers even went as far as triple extortion, where the attack included a denial-of-service to put additional pressure on the victim.

RaaS has turned ransomware into its own industry. With RaaS, a cybercrime group can create a repeatable business model with their malware. RaaS allows even technically unskilled cybercriminals to launch full-blown ransomware campaigns. The attacker basically leases what is essentially a professionally developed and maintained malware/attack suite from the RaaS provider. RaaS often includes 24/7 technical support, forums, and even user reviews of the malware. RaaS also offers different cost models such as a flat fee, affiliate programs, software licensing, and profit-sharing. Cybercriminals are operating like startups, with the added benefit of gaining the ability to go dark and later reappear with a new name and infrastructure if law enforcement pressure gets too heavy. Unfortunately, we should expect to see this, and every other big trend from 2021 to continue to grow and evolve in 2022.

> As security practitioners, we must **pay close attention to the threat landscape** as it evolves.

How do we stand against the tide?

It can seem very daunting for security professionals, especially when you look at all the forces arrayed against you. However, organizations can improve on some identifiable controls to help defend against the rising threats in 2022.

1

Operational Technology (OT) Security – as attacks against critical infrastructure rise, it is important to pay attention to security around OT. Due to the nature of the systems in play, you can't just apply traditional IT security tools and concepts to OT assets. If you run a traditional port scan on a shop floor, you are likely to knock machines offline. However, we have seen a dramatic rise in the number and quality of tools available specifically for OT and Internet of Things (IoT) security. OT security is something we have been focusing on for quite some time no, and we have seen organizations slowly expand their security programs to include OT.

2

Application Security – the Kaseya and Solarwinds incidents should serve as a wake-up call for the need to improve application security. DevSecOps (development, security, and operations) creates a framework for embedding security into the product development lifecycle. Bugs in code turn into vulnerabilities which lead to exploits and hacks. By using application security tools that development teams can embed as part of the development process, they can more quickly find security holes in their code and fix them before the code gets into the hands of customers. It's also important to set up regular application scanning to ensure newly discovered vulnerabilities already exist in fielded code. By investing in a DevSecOps program, organizations can help prevent the next Solarwinds.

3

Extended Detection and Response (XDR) – this is the next step in the evolution of security. Organizations can advance the self-isolation concepts of EDR (endpoint defense and response) and expand the detection capabilities to include security tools such as firewalls, web gateways, and related technologies. Extending these functions can provide a way to dramatically improve response times and reduce the capability for malware to spread through your network. As breaches become more public, organizations realize that the cost of a false positive is dramatically lower than the cost of a breach and are increasingly willing to enable active isolation and defensive technologies. Take Colonial Pipeline as an example: they isolated their IT environment from the OT environment to prevent the spread of ransomware. The promise of XDR is taking that defense to a more granular level. Instead of isolating an entire network, why not isolate the first breached system to keep it from spreading

4

Backups – Of course, the above suggestions will not make your network bulletproof, so you must also think about how you recover when you suffer a breach. Having a solid backup infrastructure in place will dramatically decrease your downtime when responding to a breach. Even if you pay to unlock a system that attackers have hit with ransomware, not all attackers enable you to unlock your data successfully. On top of that, you can never be sure that malware still isn't hiding out, waiting to strike again (most organizations who pay a ransom are hit again). You must have a disaster recovery plan in place that includes restoring from known good backups.

5

Awareness training – A co-worker once asked a client, 'how many employees do you have.' The response was: '22,531.' He then asked, 'How big is your security team?' and the response was, '22,531.' This is an excellent anecdote because it emphasizes the importance of security awareness. When you boil down most breaches to the initial vector, it usually is someone 'clicking something they shouldn't.' Organizations with an active security awareness training program can dramatically reduce their attack surface. It can be something as simple as routine phishing quizzes or monthly educational webinars by the security team. Anything that gets employees thinking, 'Should I open this attachment?', or, 'Should I click this link?', will make you more secure than you were before you started the program. You don't need to teach everyone to be a security expert; you just need to teach them to do their jobs in a secure manner. Not everyone needs to be a security samurai, but everyone needs to be thinking about keeping the organization secure.

In closing

As security practitioners, we must pay close attention to the threat landscape as it evolves. Looking at historical threat trends and comparing them against our established defenses can help an organization get ready for the next big threat that is just around the corner.

Highlight Article

Failing to plan is planning to fail – OT/ICS environments need robust IR practices

Lead Analyst: Ashish Thapar, Vice President, Consulting Services, Asia Pacific

We have been experiencing a convergence of Information Technology (IT) and Operational Technology (OT) systems, along with the increased use of IoT in industrial or Critical Information Infrastructure (CII) environments. This convergence is challenging many organizations to define, review and implement the security best practices and architectures that address the intricate threat landscape of OT/ICS (industrial control systems) environments. From a business perspective, there are numerous advantages in extracting business intelligence data and driving more effective management and automation. However, unless organizations can successfully implement comprehensive and effective security controls, cyberthreats continue to pose significant risks, potentially diminishing these advantages.

Cyberattacks on OT/ICS environments highlight the need to be prepared, to respond to security incidents quickly and effectively. As described in NTT's Global Threat Intelligence Report 2021[1] ,' threats to OT/IoT' is listed as one of the top threats for which organizations are not prepared. We have good insight into this from numerous cybersecurity maturity assessments, incident investigations and our strategic security consulting work. Based on this visibility, most OT/ICS environments still show relatively low maturity when considering IR (incident response) readiness. IR in OT/ICS also requires a different approach since the threat profile, the tactics, the techniques and procedures, and the level and nature of impact vary significantly from the typical IT environments.

Incident response readiness is one of the most overlooked areas in OT/ICS settings and needs holistic and pragmatic handling. Without an effective IR solution, organizations may face a catastrophic impact on OT/ICS environments, leading to loss of business productivity/reputation, impact on critical physical/national assets, and even people's lives/livelihoods. Recent high-profile attacks have demonstrated the need to ensure deep and wide visibility along with effective automated IR across the converged IT-OT-IoT environments.

Organizations are facing some clear challenges that reduce the effectiveness of a typical IT incident response plan in an OT/ICS environment:

- Lack of documentation related to key ICS components such as human-machine interfaces and SCADA; as well as blind spots, such as in unique OT baseline protocols (e.g., Modbus, BACnet, DNP3) and network traffic.
- The possibility for irreversible damage (including loss of life) can be unacceptably high if anything goes wrong while capturing key artifacts such as logs, memory, or disk images for forensic purposes.
- Remote IR approaches may not work with isolated plant/site/factory environments.
- Typical live incident response techniques may not be suitable due to risk of system/process availability.
- Lack of clarity on roles and responsibilities as it relates to timely incident containment interventions (e.g., taking an OT versus an IT asset offline or shutdown of a system).

[1] https://hello.global.ntt/en-us/insights/2021-global-threat-intelligence-report

Organizations can take advantage of global frameworks or best practices to help strengthen their security posture in the OT/ICS environments. The NIST Cyber Security Framework [2] (CSF) provides a comprehensive way to approach many facets of cybersecurity controls for such environments, and organizations should consider global standards such as IEC 62443[3].

There is currently a significant variation in OT/ICS incident response preparedness across geographies and CII industries. Some CII organizations were better prepared than others when this unplanned digital transformation (read disruption) hit their OT/ICS environments. Such organizations may have been better able to address the IT/OT convergence risks and associated threats. The key to that maturity lies, in part, in the adherence to NIST CSF core functions (i.e., identify, protect, detect, respond and recover). A zero-trust approach helps drive a risk-averse mindset instead of allowing access to any resource from anywhere, anytime and by anything. The more informed CII owners are working towards fully understanding their OT/ICS stack and the usual traffic patterns/flows while enhancing their overall cyberdefense. It can be critical to understand key differences in the technical requirements and capabilities of an organization's OT and IT environments.

Some key lessons from recent OT/ICS attacks and our experience working with several customers include:

- OT/ICS domains require a fresh perspective that follows a secure by design approach as any perceived 'Air Gap' is more of a mirage now.
- Organizations do not need to reinvent the wheel as there are best practice frameworks for them to leverage (e.g., IEC 62443 and NIST CSF).
- Robust and effective incident response readiness is critical to the success of safe and secure OT/ICS operations.
- Use the Mitre ATT&CK[4] for ICS to help understand actions an adversary may take while operating within an ICS network.
- Since most cyberattacks traverse from the enterprise IT side (level 4-5 of the Purdue reference architecture model), it is critically important the IT and OT teams work collaboratively to implement robust controls to prevent, detect and respond to these threats. IT and OT operations simply cannot remain siloed.

There is **currently a significant variation in OT/ICS incident response preparedness** across geographies and CII industries.

- Organizations must have complete knowledge of IT/OT/IoT assets, usual traffic patterns and protocol usage. Organizations also need visibility on segmentation/micro-segmentation/traffic policies to manage anomalous events better and respond to any early indicators of compromise.
- Organizations must get used to performing cyber incident response drills in their OT environments (or incident simulation exercises). This can help organizations stay nimble, address shortcomings, and do so before they are under attack, rather than while they are under attack.

We are helping customers on their journey through OT security maturity assessments, ongoing OT security advisory, creation of posture improvement roadmaps and OT/ICS incident response readiness exercises with a focus on the principles of secure by design and cyber-resilience. We support enhanced levels of threat detection visibility through the use of OT-IDS/IPS technology, DFIR proactive and reactive support services, and fusion SOC/MDR/XDR initiatives. We hope that organizations with heavy investments in the OT/ICS space are becoming more prepared and are driving timely and tangible actions to be in a position where they are better safe than sorry.

2 https://www.nist.gov/cyberframework

3 https://www.iec.ch/blog/understanding-iec-62443

4 https://collaborate.mitre.org/attackics/index.php/Main_Page

Highlight Article

A look at current challenges in data privacy

Lead Analyst: Ashleigh Meiring, Vice President, Data Privacy and Protection, NTT Ltd.

Regulations on data privacy and how organizations should manage, transfer and secure data, continued to evolve around the world in 2021. By all accounts, it's not getting easier for organizations to navigate the global data privacy landscape. Here are the key changes from 2021, and perspectives on what to focus on in 2022.

In August 2021, China passed the Personal Information Protection Law (PIPL). Although it's the first of its kind for the country, it's one of many countries that have adopted laws similar in nature to the European Union's (EU) General Data Protection Regulation (GDPR) since 2018. In addition to the state-level and industry-specific regulations that global companies need to navigate it's no wonder then that organizations are finding the data privacy realm increasingly complex to navigate.

Organizations need to be increasingly savvy and proficient in the legislative, organizational, technical and contractual aspects of data privacy, and able to demonstrate compliance.

The continual stream of new data privacy legislation, each with its own nuances, has raised some philosophical and political questions around what these new rules mean for the rights and freedoms of individuals. These include:

- How do we ensure that only the right people have the right access to data?
- Do individuals have the tools to enforce their rights and ensure those rights are protected?
- How are the rights of a juristic person (a business entity or corporation) protected in countries like South Africa?
- What is juristic personal data and how does it interact with the laws surrounding IP?
- How does the management of differing rules relate to cross-border transfers in global organizations? Do we take a global or local approach to data privacy?

These are big questions (and, to be fair, age-old questions) that organizations are unlikely to solve in the next year, but still require careful consideration.

Philosophical questions aside, what key challenges have organizations been tackling in 2021, and what methodologies will help them in 2022?

Cross-border data transfers

Of particular focus in the EU, but not unfamiliar to organizations operating in countries outside of the EU that are subject to similar laws, is the topic of cross-border data transfers. On 4 June 2021, the European Commission issued new standard contractual clauses (SCCs) for personal data transfers to countries outside of the EU. This follows the Schrems II decision and the EU Data Protection Board's associated recommendations, adopted in July 2020 and June 2021, respectively. Nearly a decade old, the commission determined that the original SCCs were outdated and no longer aligned with an increasingly digital world. As of September 2021, the current clauses are no longer valid and existing cross-border transfers relying on the previous SCCs will need to be updated by 22 December 2021.

In terms of scale, any organization transferring personal data of EU residents outside of the EU must update their agreements within the next year. Fortunately, the EU has taken a forward-looking, modular approach to the SCCs based on practical use cases, supporting organizations with guidance on implementing appropriate measures. However, the scale of this effort shouldn't be underestimated, especially for multinational organizations who might have hundreds, if not thousands, of local, regional and global agreements in place with clients, partners and suppliers.

Approaches to dealing with cross-border data transfers

We're a business-to-business organization operating in many countries. Addressing the cross-border data transfer issue is about having a clear understanding of who we're sharing personal data with, who our clients are, and how we deliver our services to them, taking into consideration the entire value chain. Operationally, we're identifying impacted contracts and beginning the process of reviewing and updating them, taking a prioritized approach aligned to the new SCCs. Furthermore, we need to have good technical and organizational measures in place, including appropriate security, to ensure the protection of personal data in transit, in motion or at rest. We're also considering, like many other organizations, where it's realistic to limit cross-border transfers and localize data within specific regions or countries.

Looking at the broader market, most companies have continued with business as usual and followed a global approach to their technology strategies by adopting the new SCCs and implementing supplementary measures. While others have taken a local (and perhaps more conservative) approach, processing local data only in the EU and using only EU providers. The cost-benefit analysis of a local approach is very interesting. It places relationships with global providers who don't have local data capabilities to support this requirement at risk as well as introduces adding complexities to operating multi-national organizations where cross-border transfers are required for daily operations, requiring significant investment to set up local infrastructure, systems and operations. Alternatively, organizations may be required to invest in supplementary measures to support ongoing cross-border transfers, which likewise require investment and expertise.

Strategically, how organizations approach updating the SCCs with clients differs. Some organizations have adopted a 'take it or leave it' approach. This tactic has its pros and cons – it's straightforward to execute, but in the case of disagreements, it could be detrimental to key relationships. Other organizations might find mutually beneficial mechanisms. This can be a relationship-centric approach, and negotiations of said mechanisms might require a prolonged implementation time, putting additional pressure on legal expertise on meeting the December 2021 deadline while still managing day-to-day operations.

With no common, global approach to legislation, organizations are left mainly to themselves to decide what works for them across legislative, organizational, technical, and contractual aspects to ensure adherence to new regulations.

> Addressing the **cross-border data transfer issue is about having a clear understanding of who we're sharing personal data with, who our clients are, and how we deliver our services** to them, taking into consideration the entire value chain.

Dealing with regulators

Another common topic at industry events and roundtables is the role of regulators. Regulators, even more experienced ones, are still finding their feet. Part of this is due to the speed at which digital transformation occurs, versus the general time it takes to develop legislation. But regulators are also introducing additional governance measures which vary by country.

For example, under South Africa's Protection of Personal Information Act (POPIA), prior authorization is required from the Information Regulator for cross-border transfers of some special categories of personal data, or data relating to minors. On the other hand, the Swiss Data Protection and Information Commissioner only require notice of transfer subject to applicable guarantees, with no express authorization required. Exact requirements for cross-border transfers vary between countries and it begs the question of how active regulators plan to be, how they'll cope with the number of requests from organizations, how they could enforce penalties if anything goes wrong and how they'll discover if any organization did break the law.

Furthermore, it questions what support regulators will provide to the industry, in terms of processes, people and training, to enable organizations, especially multinationals, to execute their own tasks effectively. We've already seen some good practices emerge from more established regulators in this regard and most regulators provide a wealth of resources, templates and guidance on their websites.

If 2021 was about finding your feet, 2022 will be about standing on them

With clarity around new legislation looming, organizations are now thinking about what this means for them, on a technical level, in terms of systems, supply chains, procedures and more.

My peers and I are asking the same questions: How do we design the privacy office to address all these requirements, especially in light of local nuances? Do we establish a shared services center that supports our global operations or rely on local expertise? Do we take a global conservative policy to data privacy or a less conservative approach knowing that there'll be additional work to do in individual countries? How do we interact and deal with regulators in each country and influence policy decisions? How do we reorganize our privacy structures across the business, given the global talent shortage for data privacy expertise?

Finding the right talent is crucial. There are now discreet specializations and emerging fields and job roles, e.g., the Privacy Engineer. But because data privacy is a relatively new field, individuals are looking to industry bodies such as the **International Association of Privacy Professionals (IAPP)**, or the **ISACA** for certification, courses, training and resources to support skills development and operationalization.

In many ways, the journey the privacy industry is on is very similar to what the broader security industry went through a few years ago (and, to some degree, is still undergoing). Working with the associations mentioned above can help organizations provide training and e-learning internally to share a high-level view of privacy and help upskill employees to support data privacy programs.

In short, 2022 is, most likely, going to be about leadership. Ensuring that executives understand what privacy is about and the implications across the organization's value chain, implementing tabletop exercises for scenario-based training, and getting their buy-in and support in building a privacy-aware culture. Strong leadership will be key to organizations mitigating the risks of a breach and non-compliance.

It'll require that leaders make some bold decisions to set their organization up to be future-fit in the wake of ongoing changes in the data privacy landscape.

NTT's Global Threat Intelligence Center

The NTT Global Threat Intelligence Center (GTIC) protects, informs, and educates NTT Group clients through the following activities:

- threat research
- vulnerability research
- intelligence fusion and analytics
- communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking their threat and vulnerability research and combining it with their detective technologies development to produce applied threat intelligence. The GTIC's mission is to protect clients by providing advanced threat research and security intelligence to enable NTT to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT's threat research is focused on gaining understanding and insight into the various threat actors, exploit tools and malware – and the techniques, tactics and procedures (TTP) used by attackers.

Vulnerability research pre-emptively uncovers zero-day vulnerabilities that are likely to become the newest attack vector, while maintaining a deep understanding of published vulnerabilities.

With this knowledge, NTT's security monitoring services can more accurately identify malicious activity that is 'on-target' to NTT Group clients' infrastructure.

Intelligence fusion and analytics is where it all comes together. The GTIC continually monitors the global threat landscape for new and emerging threats using our global internet infrastructure, clouds and data centers along with third-party intelligence feeds; and works to understand, analyse, curate and enrich those threats using advanced analysis techniques and proprietary tools; and publishes and curates them using the Global Threat Intelligence Platform (GTIP) for the benefit of NTT Group clients.

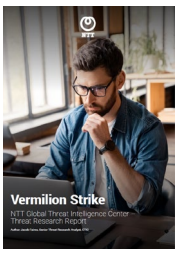
Our **Global Threat Intelligence Center** goes beyond a traditional research-only approach by combining focused research with detective technologies. This results in **true applied threat intelligence** to protect our clients with effective tools and services which reduce security risks and threats.

Recent assets

2021 Global Threat Intelligence Report

Our 2021 Global Threat Intelligence Report (GTIR) is the culmination of the data the Global Threat Intelligence Center gathered and analyzed throughout the year. We produce this report by collecting a broad set of global data (log, event, attack, incident and vulnerability) to identify key cybersecurity trends of which businesses need to be aware.

Download report



Vermilion Strike Report

During our threat research the GTIC used information from a public blog to initiate a deeper dive into Vermilion Strike. Vermilion Strike is a Linux reimplementation of the Cobalt Strike Beacon, built from the ground up by threat actors.

Download report

If you haven't already, **register to receive the Monthly Threat Reports** directly to your inbox each month. Sign up for our **Emerging Threat Advisory** and security bulletins for visibility of emerging threats and vulnerabilities that are being actively exploited across the world, sourced from our global threat intelligence platforms.


NTT