nccgroup

FOX IT
part of nccgroup

Insights

Pragmatic cyber security advice for senior executives

Sector focus:

Cyber criminals are stepping up attacks on industrial, financial and tech companies. What can we learn?

Business Viewpoint

Global. Transformative. Resilient.

Sector focus:

Cyber criminals are stepping up attacks on industrial, financial and tech companies. What can we learn?

Cyber security incidents increased rapidly in the first half of the year, but the attacks on industries were not spread evenly. Hackers have their favourites. Companies within the Critical Infrastructure, Operational Technology and Industrials sectors (which typically include Energy and Utilities, Transport, Defence and Construction amongst others) were among the most targeted by ransomware, phishing and malware attacks.

According to global data from our Incident Response statistics, in the second quarter of this year financial services, Industrials, Energy and Operational Technology continued to be the most common industry targets. By industry, technology companies recorded the highest percentage of security incidents that were escalated (38%).

38%

Technology companies recorded the highest percentage of security incidents that were escalated

So, why are these industries being targeted?

And how can companies in these industries prevent cyber attacks or minimise damage if an attack breaches their defences?

Industrials

Thoughts from Charlotte Davis, Head of Industrials, NCC Group

Until the last couple of years, companies within the industrials sector weren't necessarily considered to be prime targets for cyber criminals. This was, in part, due to the lack of connectivity of operational technology (OT), and because the architectures on which they operated were air-gapped from externally facing networks by default.

As we evolve to smart industrial environments (driven by Industry 4.0 and Society 5.0) and critical assets and networks that are connected to the Internet – the "Internet of Things" (IoT) and Industrial IoT (IIoT) – to improve efficiency, OT is becoming an increasingly viable and attractive target.

Typically ransomware has been considered almost exclusively from a traditional IT systems perspective, however as the Colonial Pipeline ransomware attack in 2021 highlighted, OT in industrial companies can be an asset of strategic and national importance.

Other recent cyber attacks to target industrials include the "parasite" malware – which targets utilities and aerospace companies, among others. It uses open-source tools to compromise infrastructure and leverages known virtual private network vulnerabilities for initial access – and a cyber crime group known as Xenotime, which is thought to have attacked oil and gas companies.

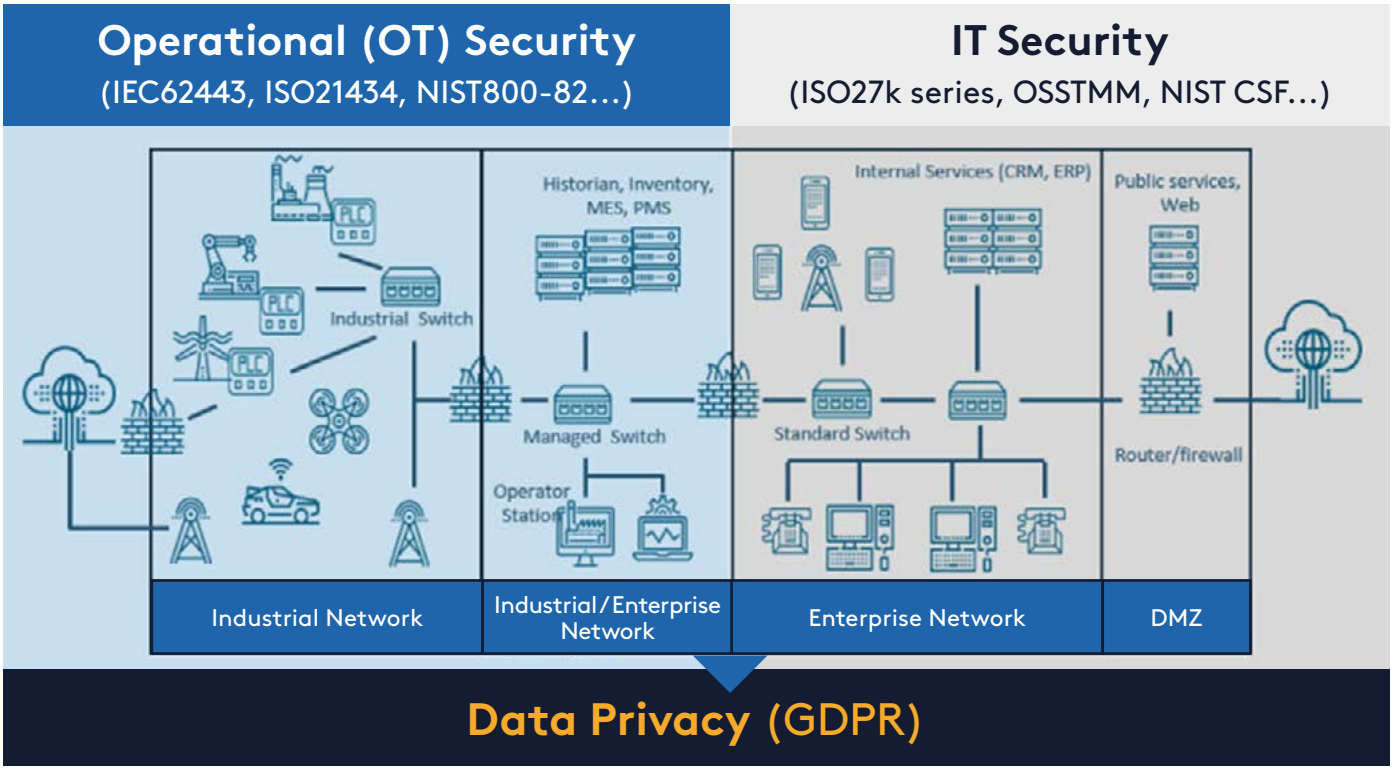
Cyber criminals have proven their ability to hold an organisation to ransom and increasingly this has impacted industrial environments and their ability to maintain operational viability. While financial gain is fundamentally the motive for cybercrime we are also identifying trends towards devastating supply chains, and regional and national infrastructure. As always, there is the danger of being caught in the crosshairs of nation state attacks either directly or indirectly and in recent months many organisations have seen Threat Intelligence advisory action as a result of this very scenario. We see increasing evidence of threat actors who target industrial and logistics businesses working within critical infrastructure to gain access to sensitive data or intellectual property (including in some instance PII) to then be weaponised for nefarious geopolitical means.

As the IT-OT convergence creates a paradigm shift for the Industrial sector, our ability to keep OT secure requires more consideration and specialist security expertise. In many instances, the connectivity of these networks is a new phenomenon, and therefore the cyber threats and their attack signatures are being explored for better understanding.

That said, basic cyber hygiene and security controls within IT and OT, and the prevention of lateral movement between parallel network architectures, are the most cost effective and efficient ways to build a strong security posture across an entire organisational or network architecture.

These measures include:

- Conducting Architectural Design reviews for network visibility to understand your organisation's critical assets, monitor them on an ongoing basis and understand if and which security controls are needed in the long term
- Ensuring your business continuity and disaster recovery plans include IoT and OT, if your organisation uses them
- Consistently monitoring environments to identify vulnerability to cyber attacks before they can be successful, using security incident and event management tools, such as Microsoft Sentinel XDR
- Creating network segmentation via process controls or technologies such as a "data diode" – hardware that allows data to travel only in one direction. By using a data diode, your business can prevent malware or ransomware from moving laterally between IT and OT environments
- Checking that your organisation follows industry best practice and international cyber-security standards, including adopting best practice NIST 800-5310 for IT and NIST 800-8211, and ISA/IEC 62443 for ICS and OT. This includes aligning security patch processes to mitigate security threats to OT.



You can work towards attaining component and asset certification to these standards or work with a partner to align your products, processes, and services to such standards (with support and guidance from an ISA/IEC 62443 specialist).

Find further advice to protect OT systems in our technical article, and explore recent attacks within the industrials sector in our **Threat Intel Report**, on page 18.

Banking, insurance and financial services

Thoughts from Sara de la Torre,
Head of Financial Services and Insurance,
NCC Group

How do financial institutions tackle the growing and most sophisticated exposure to cyber attack?

The convergence of digital transformation and globalisation will reshape the financial services' industry over the next five years. As this convergence materialises, data privacy and cybersecurity has become the top business risk and an executive board priority. With the current geopolitical instability and cyber compliance rising around the world, scrupulous end-to-end cybersecurity becomes a core focus.

As cyber attacks are increasingly becoming more frequent and sophisticated, financial institutions are using more risk driven, advanced analytical models and technology to understand and mitigate cyber threats, whilst leveraging the best advisors and practitioners with new skills and technology.

Executive boards from financial institutions are rolling out several initiatives to combat increasing cyber risks. The cyber approach in banking is looking to achieve three key objectives: security for the web, mobile applications and blockchain, risk exposure and risk quantification and the review of existing cyber resilience, on ongoing basis.

Financial institutions recognise that cybersecurity must be acknowledged as a core, strategic risk which underpins many strategic initiatives, which contribute to addressing sustainability, driving growth, protecting data privacy and maintaining business reputation. For these reasons, financial institutions are looking to improve their overall cybersecurity with a holistic approach.

In the Digital Economy and with the growing adoption of digital assets and Decentralised Finance (DeFi), cybersecurity becomes a source of competitive advantage with the right strategy, governance, and execution. Our experience helps organisations transform cyber into an opportunity and we treat cybersecurity as a business, not just a technology challenge.

Three key objectives to combat increasing cyber risks against financial services, banking and insurance:

1. Security for the web, mobile applications and blockchain end to security lifecycle solutions are being deployed with advanced analytics (machine learning), rule-based frameworks and cyber engineers' driven approaches.

2. Risk exposure and cyber risk quantification, just like any other traditional financial risk, with value at risk simulations, stress testing scenarios vs risk appetite and dashboarding following the governance, risk and compliance guidelines.

3. Review of existing cyber resilience with vulnerability assessments, attack simulation and cybersecurity frameworks which challenge the existing landscape and identify new types of attacks.

Thoughts from Pepijn Slappendel, Head of Fraud Management, Fox-IT

FOX IT
part of nccgroup

One of the many effects of the pandemic was a surge in ecommerce and online banking – and cyber criminals were quick to spot an opportunity

Fraudsters targeted two main groups: people using online banking for the first time, who were somewhat technologically naïve, and young people – the TikTok generation – who have grown up with online technologies.

Police raids on call centres

Earlier this year, Interpol made hundreds of arrests and seized millions of dollars in a crackdown on organised crime in telecommunications and financial services. The operation, codenamed, "First Light", covered 76 countries. It focused on social engineering fraud, in which criminals manipulate or trick people into giving out confidential or personal information which can then be used for criminal financial gain.

Police in participating countries raided national call centres suspected of telecommunications or scamming fraud, particularly telephone deception, romance scams, email deception, and connected financial crime.

The operation, codenamed, "First Light", covered 76 countries

Phishing for data

Currently, voice phishing or vhishing is the dominant type of fraud in most countries. The fraudster's aim is to build trust with their victim, perhaps by pretending to be from a bank helpdesk or even spoofing a customer service number.

During the scam, they will use remote access tools to gain access to devices and sensitive information, and convince customers to navigate security measures such as two-factor authentication, to deposit large sums of money into the fraudsters accounts. And many customers will do this, as they feel they are doing the right thing given the deliberate manipulations the fraudsters are subjecting them to.

It may look like a normal and perfectly legitimate transaction by a customer. However, a bank would never ask a customer to give it remote access to their accounts.

What we can see is that fraud is becoming less technological. We're seeing the rise of low-tech fraud.

Fraudsters are looking for the weakest link, and right now this could be customers themselves.

Fraud is becoming less technological.

We're seeing the rise of low-tech fraud.

So, how can you mitigate cyber threats in financial settings?

Detection

In the case of social engineering scams, it is vital to monitor the entire customer journey, including device registrations and customer log-ins, not just online transactions. Try to detect cyber attacks at an early stage and prevent them from happening.

The challenge that banks have is that customers today use many different channels. It's no longer only internet banking or using an ATM. They also use mobile and various financial apps such as PayPal. That makes it easier for fraudsters to hide their tracks between the channels and remain undetected.

Build a single point where all data is correlated and track each of your customer's journeys.

Stronger user authentication

This is the key preventive measure that can be applied. Use multiple devices to, for example, verify a customer's identity and approve banking transactions by scanning a QR code when the customer is logging in. That means a fraudster can't make a transaction on their own unless they have been able to register their own device on the victim's bank account. Multi-factor authentication makes life harder for fraudsters.

Educate your customers

When a social engineering script for fraud is seen to work it becomes widely used. The scripts change regularly. In the Netherlands, for example, one social engineering script used to be a child texting their parent saying that he or she has lost their phone and needs money to return home from holiday. That was the dominant scam until people became aware of this story. Now it's a bank helpdesk fraud – it has recently become more widely used in the UK as well.

Banks will always know which fraud story is most common and can use this knowledge to raise awareness with their customers. The stories may change but the techniques and technologies they use remain broadly similar. Fortunately, these threats can be mitigated through a methodical approach to cybersecurity and the right technology.

About Insights

Insights is a program designed for sharing pragmatic cyber security insights with senior executives. You can expect a magazine and interactive online event about a trending topic each quarter. Register here for the free virtual Insights event: Growing Threats.

About NCC group

It's a new era of risk. Defy it with NCC Group's end-to-end cyber security and resilience solutions, and confidently embrace technology to support sustainable growth and success.

From governments to tech giants, financial institutions to expanding businesses, for over 30 years we have proudly provided them with strong security solutions...and with a global team of over 2,400 experts, we're ready to do the same for you.

With NCC Group, take your business to the next level. Unleash innovation without the obstacle of cyber threats.

More than a solution. **A partner.**

You're not alone on your security journey. NCC Group is your partner. Be it rolling up our sleeves with your in-house team or developing strategy with your board, we help you have control over your appropriate level of security. Yes, we deliver industry leading security solutions, but we'll also reduce stress, save your business time, and help you prepare for, or even face, a crisis together.

www.nccgroup.com

UNI106269