Securing operational technology

How vulnerable is our national critical infrastructure?

On any given day, the chances are that if you work in a utility, oil and gas, manufacturing or alternative energy organization, you have had to fend off a cyberattack. Activist groups, individual troublemakers, criminal organizations and rogue states are targeting Operational Technology (OT) and our national critical infrastructure daily, in an attempt to disrupt services and cause havoc.

Cybercrime forces companies of all sizes in almost every sector to take stock; but for those organizations that make up our critical infrastructure, the threat of a cyberattack has serious repercussions that reach far beyond the disruption to the individual business. We all depend on the reliable functioning of our critical infrastructure – and to some degree, we take it for granted that it will always be there for us.

Well-publicized attacks (and those never made public at all) tell us however, that this isn't always the case. So what can we do to better protect ourselves against the threat of a serious breach?

> The UK National Security Council has identified cyberattacks as a 'tier one' risk to national security, alongside terrorism and major international conflict.
>
> **Financial Times, October 2014**

Connected ICS and SCADA systems are more vulnerable to attack

In many organizations, much of the critical infrastructure technology environment predates the internet when managing Industrial Control Systems (ICS) and Supervisory Control And Data Acquisition systems (SCADA) was easier than it is today. Years ago, systems were largely proprietary and isolated, and operations managers worked on-site. There was no need to connect them to the corporate network or internet – and the internet was not what it is today. Management of the systems rarely fell under IT control.

But these systems are increasingly connecting to the internet in an attempt to streamline business, improve communication in the supply chain, and find new intelligence from the latest technology trends such as big data and the Internet of Things (IoT).

Added to this, there's a growing desire for engineers to connect to these control systems remotely. Thirty or so years ago, physical threats were the biggest concern – now it's more likely to be a cyberattack that poses the greatest threat. But often, the complexity of these networks means that operations managers are reluctant to relinquish control over their OT; and IT departments are unwilling to take responsibility for what they see as uncontrolled environments with archaic hardware.

New connections inevitably mean new threats

Global research from Ponemon shows that nearly 70% of critical infrastructure managers reported at least one security breach that led to the loss of confidential information or disruption of operations in the past 12 months. In addition, 78% said a successful attack on their organization's ICS or SCADA systems is at least 'somewhat likely' within the next 24 months. Yet only one in six respondents described their organization's IT security program or activities as 'mature.'

Recent years have seen some well publicized SCADA attacks – such as Stuxnet, that disrupted Iran's uranium facility in 2010 – yet security is still not a priority for many organizations that form our global critical infrastructure. Only 28% of people that took part in the Ponemon survey said that security was ranked as a top five strategic priority for their organization – and yet minimizing downtime was a top priority for the majority of respondents. In other words, minimizing downtime is a priority, but not enough is being done to reduce risk.

Is enough being done to address evolving threats?

Standards and guidelines for cybersecurity already exist, and in many cases have been in place for years. Yet reported cyberattacks continue to grow and many of these attacks could have been avoided by the rigid application of security controls. That said, there is a growing awareness globally of the threat of cyberattacks against critical infrastructure and SCADA systems.

In the US, the National Institute for Science and Technology (NIST) continues to work hard, and the Obama Administration published the Framework for Improving Critical Infrastructure Cybersecurity in February 2014; ANSSI, France's national agency for computer systems security, recently drafted two working documents on how to protect critical infrastructure; in Germany, the federal interior ministry unveiled draft legislation in August 2014 that would pave the way for the introduction of tough new cybersecurity measures to protect 'critical infrastructure'; and the UK launched its own sub-group earlier in 2014.

That's all great news, but these guidelines and frameworks are only that.

Industry under attack

- In June 2017, the Petya ransomware attack hit airlines, hospitals, banks, and utilities around the world, causing them to shut down their computer systems.
- Three months earlier, the global WannaCry ransomware attack closed parts of the UK's National Health Service, causing it to run some services on an emergency-only basis.
- In October 2016, the Mirai malware created botnets on IoT devices to launch a massive distributed denial-of-service attack that disrupted all US internet traffic.
- In 2015, a new malware type called BlackEnergy was discovered in US industrial control systems that operate critical infrastructure. It had capabilities for both espionage and sabotage.

"We have seen a number of attacks to critical industries in areas like the Middle East and the US and these had a major impact on operations."

Michael Chertoff, former head of US Dept. of Homeland Security, October 2014

More encouraging is the development of OT solutions, which supplement IT security to tackle new challenges like IoT. It's essential that OT concepts become embedded in industry so that organizations can continuously monitor and control their own systems and IT environments, and do everything possible to reduce the risk of cyberattack.

It's becoming increasingly easy for would-be hackers to see and infiltrate connected systems. In 2012, researchers at a Chicago-based cybersecurity company set out to measure how many ICS are openly exposed to the internet. They closed the count at 2.2 million unique IP addresses linked to ICS at energy-related sites.

Using the publicly-accessible search engine Shodan, they built search queries using the names of 182 SCADA suppliers and their leading products, and many devices revealed not only their presence, but also hardware and firmware metadata that could help a hacker pinpoint documented security flaws. Search engines are capable of revealing public interfaces to huge numbers of systems – the most worrying of which are the web-facing controls for critical infrastructure, such as power plants, transport networks, and security services.

> **"Companies of our size unfortunately experience cyberattacks nearly every day."**
>
> Patricia Wexler, JPMorgan spokesperson

What can we do?

The four pillars of operational technology security

The first step in controlling risk is to understand your exposure across all areas of the business and prioritize those deemed critical. Next, is to establish your level of capability in four key areas:

1. Detecting anomalies, threats or incidents and knowing how quickly you can respond.
2. Controlling and securing the data flow between defined networks.
3. Controlling and managing user access to systems, and how systems can access one another.
4. Identifying and protecting the growing array of network endpoints, beyond PCs and mobile devices, to include IoT and OT.

As these networks are extremely complex and often use proprietary hardware and protocols, it is vital that assessments are conducted by specialists who fully understand the intricacies of control networks.

What does the research say?

- Almost 70% of critical infrastructure managers reported at least one security breach that led to the loss of confidential information or disruption of operations in the past 12 months.[1]
- 78% of critical infrastructure managers said a successful attack on their organization's ICS or SCADA systems is at least somewhat likely within the next 24 months.[2]
- Cyber-risk is the world's number seven risk overall in 2018.[3]
- Just 48% of companies claim that all their critical data is securely stored.[4]
- 55% of global organizations across all sectors believe a data breach is inevitable at some point.[5]
- Ransomware attacks jumped in malware detections, up from 1% in 2016 to 7% in 2017 at a global level.[6]
- Globally, only 49% of organizations had a formal incident response plan. This is up from 48% in 2017.[7]
- It is calculated that USD 3 trillion is the total global impact of cybercrime.[8]
- 50% of critical infrastructure managers say their IT security activities have not yet been defined or deployed.[9]
- It's estimated that 1.8 million more cybersecurity professionals will be needed by 2022.[10]

Building the right OT security model for your business

The last thing that any organization wants is to make the headlines following a security breach. The damage to reputation can be enormous, as can the financial costs. It's not a case of if it will happen, but when, so it is essential that you have a mature, detailed incident response plan, and monitoring systems capable of providing a comprehensive and real-time view of network activity. Timely incident response is imperative following a breach and many organizations don't have spare resources waiting to leap into action when an incident happens. It might be worth considering a monitoring and incident response partner to provide the right resources to help you return to business as usual as quickly as possible should a breach occur.

Do you have the skills in-house?

Understanding risk exposure, preparing an incident response plan and continuously monitoring risk in your organization takes time and expertize. You may not have these skills in-house, or you may have tried and failed to recruit people with the right skills – there's a growing global skills shortage in this sector that will take years to improve.

Many organizations look to outsource these critical functions to reassure themselves that systems are monitored around the clock and experts are on hand to provide essential advice and support when needed.

> **NTT responded to many client incidents over the past year. Globally, just 49% of organizations had a formal incident response plan in place. This is up from 48% in the previous year.**
>
> NTT Security Risk: Value 2018 Report

1, 2, 9. Critical Infrastructure: Security Preparedness and Maturity, Ponemon, 2014 3. Lloyds City Risk Index 2018 4,5,7. NTT Security Risk: Value2018 Report
6. NTT Security, 2018 Global Threat Intelligence Report 8. Risk and responsibility in a hyperconnected world: Implications for enterprises, McKinsey 2014
10. Frost and Sullivan 2017 Global Information Security Workforce study

Ten steps to improving your operational technology security footing:

1. Understand your risk – conduct an annual risk assessment exercise to understand your current risk exposure. Maintain the board's engagement with cyber-risk.
2. Engage with a specialist partner with a track record of conducting similar technical risk assessments. Ensure you are getting the best from your existing technology and border defenses. Understand what is on your network and what protocols traverse it.
3. Secure configuration – keep hardware and software protection up-to-date – persistence pays off for the cybercriminal. Stay on top of basic protection. Work with suppliers to ensure proprietary systems are maintained. Build an asset register, paying particular attention to end-of-life/unsupported systems.
4. Establish a monitoring and detection system – continuously monitor all log data generated by your OT systems in order to baseline 'normal' activity. This enables real-time detection of attacks that go against this definition of normal behaviour.
5. Educate and train your employees – ensure they really know your policies and incident response processes. Systems are still more at risk due to unintentional consequences from various insiders than from malicious outsiders. Take time to educate your engineers on key security controls – engineers have little or no background in security. Make it a priority to teach them the basics.
6. Check passwords on connected devices – many connected devices are using weak or factory-set passwords that leave the front door wide open
7. Incident response – establish, produce, and routinely test incident management plans to ensure that there is business continuity and to prevent a cascading effect.
8. Secure network – manage the network perimeter and filter out unauthorized access.
9. Malware protection – establish anti-malware defenses and continuously scan for malware.
10. Patching schedules – ensure that SCADA systems are up-to-date with patching schedules and are not using default passwords. Patches may have subtle differences to those provided by Microsoft or Apple for example.

Conclusion

What's clear is that critical infrastructure and industrial plant control systems are coming under scrutiny from both attackers and defenders. Much is being done to create frameworks and draft legislation. But this will not be enough unless the industry takes control of the problem and invests in operational technology security to reduce the everpresent threats.

We will get better at identifying, locating, and penalizing the bad guys to deter the majority of attacks.

Until that day, business needs to remain vigilant to protect its own assets.

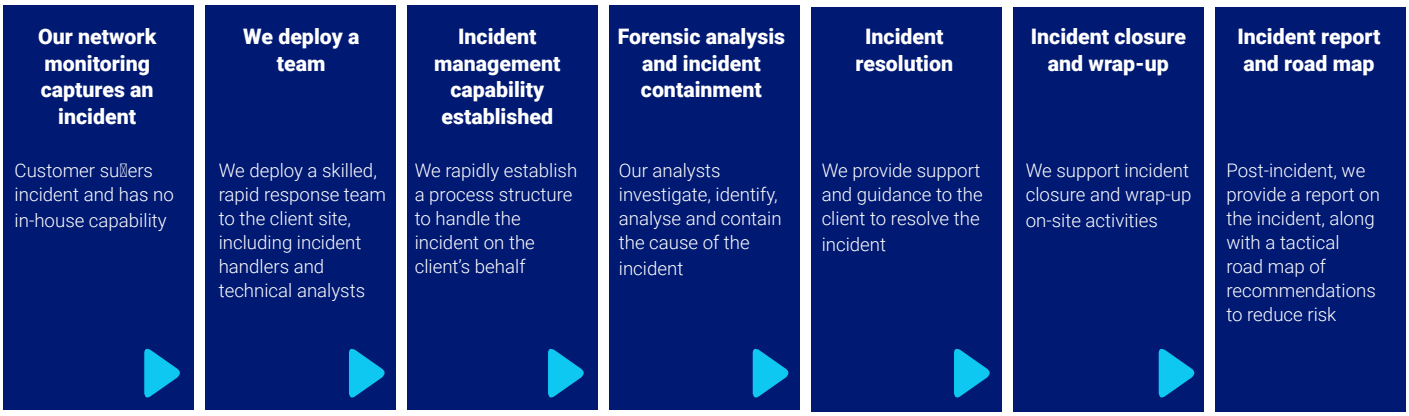

Figure 1: Operational technology solutions from NTT help you to reduce the risk of future incidents, as well as minimizing the business impact and cost

Working with NTT

You want to be confident that you have the right processes in place to both identify risk and to take immediate action if a breach occurs.

Information security and risk management is a continuous process and many organizations are now outsourcing this vital area to NTT where our teams work around the clock to monitor your security infrastructure, detect threats, and recommend solutions.

Our security experts will work with you to baseline normal network behaviour and identify OT security gaps using our proven Risk Insight process. We'll be with you every step of the way, with our Incident Response team should a breach occur and you require support to get back to business as usual as quickly as possible.

For those organizations that prefer to outsource their information security support, we offer Managed Security Services (MSS), where you gain access to our collective global knowledge and systems and our highly experienced people. A combination of these two elements applies a layer of intelligence and context across correlated events to increase visibility, understanding, and the ability to make informed business decisions regarding your risk profile.

For more information on how we can help you to identify security weaknesses and continuously manage your assets, visit **hello.global.ntt**.

Disclaimer: The work described in this thought leadership was performed while the company was known as NTT Security.


NTT