Deloitte.

Ransomware in critical infrastructure

Ten questions and actions to tackle this major threat

Introduction

Critical infrastructure (CI) is the essential scaffolding of our economies, which makes it a high value target for state-based cyber espionage and asymmetric warfare. However, increasingly CI is being targeted by active ransomware criminal groups. In this article, Deloitte considers how ransomware is evolving globally and we call out what could and should be done about it.

As far back as 2015, a highly sophisticated group showed the world that cyber attackers could cause a real-life disruption of electricity supply to citizens, businesses and infrastructure alike—by effectively taking down parts of Ukraine's power grid. Hundreds of thousands of residents were left without electricity for up to six hours, and some electricity distribution control centres took months to return to normal operations.[1] After infiltrating power companies' operational networks, the group suddenly shut down electric substations, wiped operators' workstations in the control centres, and flooded the customer service phone lines to ensure total panic. What would the consequences have been if the electricity shortage had lasted much longer?

This hit home just a year later, when a related group launched a piece of malware designed to take over industrial control systems (ICS) in even more critical components of an electric grid.[2] The group decided to simply demonstrate its capabilities through a short-lived attack, but it could have shut down and damaged transmission substations—which means it could have brought down entire regions for days or weeks at a time. Water supply, emergency services, hospitals, gas stations and other essential services are not equipped to withstand a sustained power shortage. What happens then?

Can ransomware groups disrupt electricity supply and other essential services in their escalating quest to earn larger rewards? Let's consider what we know. Cyber spies and criminals have probed power grids around the world, spying on their internal workings and establishing footholds to strike when they wish to do so.

It has been reported that ransomware groups claim to have access to critical infrastructure including a nuclear power plant.[3] In 2021, several water facilities have been compromised with potentially dangerous outcomes, including by ransomware groups. In May that year, a ransomware attack on a single pipeline operator in the US resulted in fuel shortages across a wide region for gas stations, airports, the military, and even home heating.[4] Meanwhile, factories around the world have been successfully targeted with ransomware specially built to attack operational technology (OT) systems running manufacturing processes.

Ransomware groups are conducting increasingly sophisticated attacks against critical infrastructure, public services, and private corporations. The capability for severe and widespread disruption is quite clear.

Critical infrastructure ecosystems are vulnerable to malicious cyber disruptions. Attacks can wreak havoc on normal function and even cost lives. The relevant question is how can we make our infrastructure more resilient?

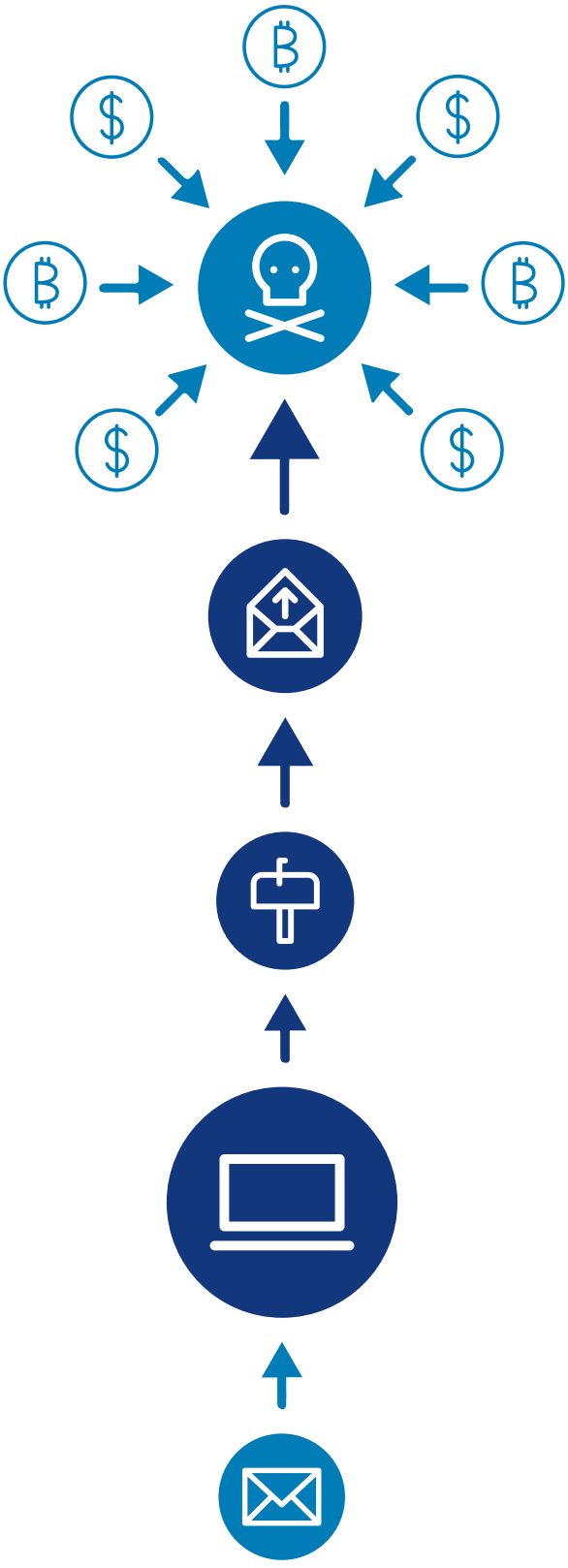
What is ransomware?

Ransomware is designed to encrypt its victims' files. It causes data to be unavailable to system users and software—data that is often sensitive or required to run critical business processes. The attackers then demand payment via online platforms in return for providing the decryption key. In a widely reported attack, a group using the Ragnar Locker ransomware demanded a US$10 million ransom but it has been alleged that the victim was able to negotiate down to US$4.5 million.[5] This amount is similar to what was paid by the US pipeline operator.[6] Meanwhile, cyber criminals often threaten to double the ransom amount if their victims do not engage within a short timeframe. There have even been much larger requests including a string of ransom demands reported in excess of US$40 million each.[7] The record may be held by attackers demanding a single US$70 million ransom payment in 2021.[8]

In addition, and in what has become a trend since 2020, threat actors also extract large quantities of sensitive information prior to encrypting the victim's databases. They then threaten to publish this information unless the ransom is paid. This tactic, known as **'double extortion'**, puts additional pressure on the victim to pay the ransom in order to avoid legal or regulatory issues resulting from a breach of personal information. According to Deloitte's Cyber Trend & Intelligence Report 2021, stolen data from more than 150 companies per month has been disclosed on ransomware leak sites since August 2020.[9]

We are now seeing yet another tactic: public-facing services such as customer service centres and corporate websites of ransomware victims are additionally hit by distributed denial-of-service (DDoS) attacks. These **'triple extortion'** attacks aim to completely cripple and slow down an organisation's ability to respond and recover from the attack, and even to communicate with its customers, without paying the requested ransom.

While it is generally advised not to pay a ransom—not least because doing so may put the victim organisation at risk of legal liabilities and there is no guarantee it will be able to recover all its data—ransomware attacks often cost more that the requested ransom. As early as 2017, a global shipping giant estimated a loss of US$300 million due to an attack by the NotPetya ransomware.



The ransomware landscape

The ransomware attack on a US pipeline operator is just one many in 2021 by criminal groups like DarkSide, one of the largest along with Conti/Ryuk, REvil/Sodinokibi, Clop, Maze and Netwalker. REvil alone is reported to have earned at least US$80 million in revenue in 2020.[10] Ransomware groups continue to expand and evolve.

According to Cybersecurity Ventures,[11] ransomware attacks are expected to happen across the world every 11 seconds in 2021. Aided by unprecedented digitisation (accelerated in the COVID-19 pandemic through lockdowns requiring remote access), 2020 was characterised by a significant increase in cyber-criminal activity, in particular ransomware attacks. Research from Bitdefender indicates a seven-fold rise in ransomware attacks over the first half of the year.[12] Another analysis found that ransomware has been by far the most prevalent type of attack against industrial organisations relying on OT in 2021,[13] with more than half of the attacks affecting physical operations.

In 2020, it was reported that ransomware attacks affected more than half (55%) of all companies in Asia Pacific.[14] Globally, India was one of the most impacted nations with a 39.2% increase in the number of attacks, followed by Sri Lanka, then Russia and Turkey. However, the most attacked nation and outright leader suffering ransomware attacks globally was still the USA with a 98.1% increase in attacks.[15] Over the last two years, ransomware attacks also became increasingly prevalent in Australia, particularly due to the emergence of ransomware-as-a service.

In Taiwan in early 2020, there were at least six publicly disclosed ransomware attacks on CI.[16] And over the past three years in New Zealand, the Deloitte cyber practice alone assisted clients with more than 400 cyber incidents—primarily data breaches and online fraud, but also ransomware. In many of the ransomware attacks, we observed that backups were destroyed and the log files tampered with, rendering investigation and recovery difficult.

The wide-ranging downstream impacts of the ransomware attack in the US in May 2021 were not a first. A year earlier, the largest domestic energy provider in Taiwan suffered a ransomware incident that caused disruptions at many of the nation's petrol stations, part of a string of targeted attacks on CI organisations in the country.[17]

These incidents have increased both public and private awareness of the domino effect of a cyber attack on a critical industry, and the need for both preventative measures and recovery plans[18] to avoid and mitigate local disasters.

In a troubling development, the focus is now shifting towards OT systems and networks, which underpin core physical operations for critical infrastructure and manufacturing organisations. An emerging strain of ransomware, EKANS, was found to include multiple functions dedicated to industrial control systems. The ransomware has already targeted electric utilities.[19]

The learnings

In 2018, there was a significant WannaCry ransomware infection at the Taiwan-based global leader in semiconductor foundries, the world's most valuable semiconductor company. This incident clearly demonstrated that everything is connected or exposed, even when critical systems are physically isolated. In cyber security speak, physical isolation is known as 'air gapping'.

The post-event investigation determined that an external maintenance provider infected an automated machining tool, which allowed the worm-type malware to massively replicate and spread throughout the network. It was projected to impact third quarter revenue of the company by about two percent and cause shipment delays due to the production shutdown. In this case the OT environment, including industrial control systems which run critical processes such as manufacturing, was directly affected.[20]

The attack highlighted that relying on air gaps as a fail-safe cyber protection for critical infrastructure control systems is neither realistic nor effective. Simply put, it is not an option. Air gaps don't work. In today's digitised world, they are extremely difficult to implement correctly in most environments and don't protect against important attack vectors.

The cyber incident in Taiwan also shows that high-risk operators' cyber awareness is critical, and requires both employees and contractors to be trained and monitored. Likewise, it is equally important to ensure that third parties, such as industrial vendors and maintenance companies, implement and maintain effective cyber security controls. This can only be achieved if suppliers are fully integrated into the organisation's cyber risk management framework and processes.

It's a trend

Over the last two years, cyber criminals have turned their focus from small, medium-sized individual businesses to large corporations and government organisations. And during the pandemic in 2020, industrial-strength traditional organised crime groups turned to the digital world, injecting further capital into ransomware operations to pursue lucrative payouts. Ransomware groups have now set the world's critical infrastructure firmly in their sights and embarked on what is termed 'big game hunting' campaigns, which explains a reported 500% rise in attacks on industrial organisations from 2018 to 2020.[21]

The landscape is further complicated by the recent prevalence of ransomware-as-a-service. Ransomware platforms and services are increasingly made available to affiliates on cybercrime forums, in some cases enabling them to get up to 84% of the ransom payments if their previous week's earnings exceed US$300,000.[22] Affiliate groups or 'syndicates' such as REvil/Sodinokibi, DarkSide, Ryuk, Maze and NetWalker use this 'franchise' model to significantly expand their attack volumes and revenue. This increases the syndicate's capital, its potential for scaling up, and its ability to continually invest in malware development to stay ahead of the competition and beat anti-malware protection methods.

As a result, ransomware cyber attacks have become one of the most significant threats to our nations, our essential services, and by extension our citizens and livelihoods.

Indeed, all our essential services are increasingly at risk, as a successful cyber attack on critical infrastructure can:

- disrupt operations and the supply of electricity, oil, gas, water, waste management, and transport
- further threaten the safety of workers and citizens as dependent services, including emergency services and health facilities, suffer shortages or are compromised as collateral damage
- impact revenue, result in reputational damage, and lead to litigation or regulatory consequences due to the unavailability of service
- bring a whole economy to a standstill in a serious and sustained scenario, due to the domino effects described earlier, and the possibility of public disturbance and civil unrest
- be leveraged to weaken a country's government and essential services in preparation for a conventional military attack by another nation-state.

Why are ransomware attacks so successful?

By denying access to core internal systems, ransomware can cause an organisation to run its operations in a highly degraded state, necessitating the use of manual processes and mobile phones. This was the case in 2020 in New Zealand for instance. In many incidents reported by Deloitte specialists, the post-incident reviews identified critical systems inside the organisations having suffered from classic cyber hygiene gaps and missing controls. Critical software updates had not been applied; there was weak management of privileged and remote access; passwords were stored in text files; there were limited security monitoring and response capabilities, and poorly secured backup systems. This often meant attackers were able to completely 'own' a network, and sometimes remain undetected for months, before deploying ransomware.

In addition to the growing sophistication of global threat actors, changing expectations have increased the risk of the ransomware threat to critical infrastructure. To meet stakeholders' desires for simplicity, efficiency and value while meeting constant budgetary constraints, organisations increasingly embrace significant technological change. Widespread trends include converging IT with OT and introducing cloud and Industrial Internet of Things (IIoT) technologies. In addition, COVID-19 lockdowns have forced many organisations to quickly enable remote access for their OT personnel. All these changes result in OT environments being more exposed to cyber threats.

2020 demonstrated that all organisations and nations are vulnerable to the unexpected. And governments and large organisations around the world are determined to find ways to effectively combat ransomware and other cyber threats to CI.

Did you know?

It can take less than **45 minutes** to ransom an entire network for a large, distributed global organisation

31% of ransomware victims experience destructive outcomes

More than **50%** of ransomware attacks on industrial organisations may affect OT networks directly or indirectly, while some ransomware programs can now disrupt ICS specifically

It takes **201 days** on average to identify a cyber breach, giving attackers on average more than six months to prepare and launch their ransomware attack

50% of ransomware attacks leverage the supply chain, i.e. vendors or contractors

Source: Deloitte analysis; news reports.

Addressing the threat head-on

Singapore's *OT Cybersecurity Masterplan*[23] is an example of a concerted effort that can serve as a blueprint for the region. The masterplan is part of the city-state's determination to enhance the cyber resilience of its CI sectors and public and private sector organisations. The masterplan aims to improve cross-sector intelligence sharing, protection efforts, and response capabilities in order to mitigate cyber threats in mission-critical OT environments.

CIOs, CISOs and cyber security teams are improving their awareness and response plans around the ransomware threat. Such efforts need to cross boundaries so that every worker understands exactly what ransomware is, how it infects organisations, and how to combat it. Training employees on how to prevent, recognise, and defend against cyber attacks is a commonly neglected countermeasure, although it is both cost-effective and critical to improving an organisation's cyber resiliency against ransomware.

The blurring of boundaries between IT and OT requires advanced defensive capabilities. To become resilient—especially in the face of the evolving threat landscape and ongoing technological changes—it is most important to create transparency around these risks so that leadership, Boards and the C-suite can better monitor and address them. This will enable CI organisations to maintain safety and reliability while modernising their operations.

Ten questions to move forward

The following ten key questions should help you kickstart or re-evaluate your efforts to protect critical operational processes and systems against the threat of ransomware:

1. **Has your organisation identified the most critical business processes that depend on technology?**
   What are they? Who owns them? This analysis needs to be narrowed down to those core processes that simply can't operate effectively without the technology.

2. **For these critical business processes, is there a comprehensive 'tree of dependencies' that covers technology systems, suppliers, and people?**
   It is vital to understand this mapping as it allows an organisation to pinpoint the components that have the potential to cause system failures or to introduce ransomware. And start assessing the resulting failure scenarios.

3. **Do we have individual cyber risk assessments on these critical business processes and their dependencies?**
   This will give visibility of the specific vulnerabilities and risks that are outside risk appetite parameters.

4. **Is there a framework of non-negotiable cyber controls for technology that underpins critical business processes?**
   We know from good practice frameworks, such as the Australian Cyber Security Centre's Essential Eight,[24] and other research that many cyber incidents tend to exploit a small number of cyber hygiene issues and control weaknesses. In regulated sectors, non-negotiable controls will also directly stem from mandatory standards, guidelines, or maturity models.

5. **Is cyber risk owned by your organisation's business leaders and do they operate together, collaboratively, and effectively?**
   This is frequently an issue in organisations where ineffective cyber risk management leads to serious vulnerabilities remaining unresolved. This happens when formal decisions around accepting risk or funding remediation are isolated, uncoordinated, or simply not made—and so not acted on.

6. **Is your organisation proactively managing the risk of key suppliers involved in critical processes and systems?**
   Suppliers can inadvertently introduce ransomware and other malware in core OT systems. Many operate with outdated contracts that lack accountability or clarity around responsibilities for cyber security controls. Identifying such suppliers, assessing their cyber security controls, and monitoring their effectiveness are all key ways to avoid opening up further attack vectors and risks to critical systems.

7. **How are legacy critical systems being protected?**
   Unsupported software and devices from legacy industrial control systems are vulnerable to common malware, let alone targeted attacks. Many legacy employees with the system 'know how' may have already left the organisation. In some cases, the incident recovery team has to rebuild using year-old backup data. Organisations need to decide how to protect legacy systems and be prepared to rebuild industrial processes from scratch—including these systems.

8. **Is there excessive reliance or complacency around 'air gaps'?**
   We explored earlier why 'air gaps' usually fail and lead to false confidence about the protection level of industrial control systems, which are at the heart of OT. Organisations cannot afford to rely on this concept. While network segmentation controls can and should be reinforced, it is equally important to monitor connections, detect unexpected behaviours, and be able to respond quickly with tried and tested containment measures and recovery processes.

9. **How resilient is your workforce to cyber risk?**
   Most cyber incidents involve human failure, including in well-disciplined industrial environments. Leading organisations are therefore identifying their high-risk workers and making targeted interventions to improve awareness and resiliency. It is important to help workers understand how to avoid introducing risks, as well as to identify and report suspicious system behaviours.

10. **Has sufficient crisis management and recovery testing been done for a ransomware attack on a critical system?**
    It is still common for organisations that attempt a system restoration from backups to discover it is much harder than expected (or that the backups are inoperative or also infected with ransomware). Organisations need to thoroughly practice response processes—including rebuilding systems from scratch—with their management teams, suppliers, and other third parties. In this way, they can remediate technical issues, identify what information is needed and who is responsible to respond effectively, align leadership and develop muscle memory around decision-making, and clarify how to communicate with regulators, customers, and the media.

Endnotes

[1] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016.

[2] Andy Greenberg, "'Crash Override': The Malware That Took Down a Power Grid," *Wired*, June 12, 2017.

[3] Dmitry Smilyanets, "An interview with REvil's Unknown," *The Record by Recorded Future*, March 16, 2021.

[4] Charlie Osborne, "Colonial Pipeline attack: Everything you need to know," *ZDNet*, May 13, 2021.

[5] Deloitte CyberSOC EMEA Center, *Double-extortion incidents - Cyber Threat Intelligence*, October 2020.

[6] C. Eaton and D. Volz, "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom," *The Wall Street Journal*, May 19, 2021.

[7] Camille Singleton, "Ransomware 2020: Attack Trends Affecting Organizations Worldwide," *Security Intelligence*, September 28, 2020.

[8] Robert McMillan, "Ransomware Hackers Demand $70 Million to Unlock Computers in Widespread Attack," *The Wall Street Journal*, July 5, 2021.

[9] Deloitte Cyber Intelligence Center, *Deloitte Cyber Trend & Intelligence Report 2021* [in Japanese], 2021.

[10] Singleton, "Ransomware 2020," September 28, 2020..

[11] Steve Morgan, "Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021," *Cybersecurity Ventures*, October 21, 2019.

[12] Bitdefender, *Mid-Year Threat Landscape Report 2020*, 2020.

[13] Eduard Kovacs, "Many Ransomware Attacks on OT Organizations Involved Ryuk: IBM," *SecurityWeek*, October 27, 2021.

[14] R. Dallon Adams, "Ransomware attacks by industry, continent, and more," *TechRepublic*, October 12, 2020.

[15] Check Point Software Technologies, "Global Surges in Ransomware Attacks." accessed November 26, 2021.

[16] In Taiwan the regulatory reporting requirements are comprehensive in eight industry sectors when it comes to personal data breaches. However, the requirements to disclose attacks on OT systems are far less clear.

[17] Taiwan News, *Taiwan's CPC suffers malware attack, experiences system outage*, May 4, 2020.

[18] CIO Tech Team, "Deloitte Roundtable: Extinction level events: how ransomware has changed disaster preparedness," *CIO TECH ASIA*, January 21, 2021.

[19] Dragos, *EKANS Ransomware Misconceptions and Misunderstandings*, June 18, 2020.

[20] TSMC, "TSMC Details Impact of Computer Virus Incident," press release, August 5, 2018; Liberty Times Net, *C.C. Wei press conference: 'The impact of the virus on Q3 revenue is reduced to 2%'* [in Chinese], August 6, 2018.

[21] Dragos and IBM Security X-Force, *Ransomware in ICS Environments*, December 2020.

[22] Deloitte CyberSOC EMEA Center, *Double-extortion incidents*, October 2020.

[23] Cyber Security Agency of Singapore, *Singapore's Operational Technology Cybersecurity Masterplan 2019*, October 1, 2019.

[24] Australian Cyber Security Centre, *Essential Eight Explained*, June 26, 2020.

Authors and contributors

Authors

David R. Owen
Australia Critical Infrastructure Cyber leader
+61 2 8260 4596
dowen@deloitte.com.au

Etienne Janot
Senior manager
+886 2 2725 9988 (ext. 7766)
etjanot@deloitte.com.tw

Karen Grieve
Director
+61 2 9322 7321
kagrieve@deloitte.com.au

Key Contributors

Max Lin
Asia Pacific Cyber Emerging Technologies leader
+886 2 2725 9988 (ext. 7779)
maxylin@deloitte.com.tw

Key contacts

Max Lin
Asia Pacific Cyber Emerging Technologies leader
+886 2 2725 9988 (ext. 7779)
maxylin@deloitte.com.tw

Australia

David R. Owen
Critical Infrastructure Cyber leader
+61 2 8260 4596
dowen@deloitte.com.au

Chinese Mainland/Hong Kong

Boris Zhang
Partner
+86 21 6141 1505
zhzhang@deloitte.com.cn

India

Gaurav Shukla
Partner
+91 80 6188 6164
shuklagaurav@deloitte.com

Japan

Haruhito Kitano
Partner
+81 80 3591 6426
haruhito.kitano@tohmatsu.co.jp

Korea

Young Soo Seo
Partner
+82 2 6676 1929
youngseo@deloitte.com

New Zealand

Anu Nayar
Partner
+64 4 470 3785
anayar@deloitte.co.nz

Southeast Asia

Tse Gan Thio
Executive Director
+65 6216 3158
tgthio@deloitte.com

Taiwan

Max Lin
Asia Pacific Cyber Emerging Technologies leader
+886 2 2725 9988 (ext. 7779)
maxylin@deloitte.com.tw

Deloitte.

Designed by CoRe Creative Services. RITM0884435