CYBER SECURITY

Ransomware Resilience in OT Environments

Assess your readiness

Ransomware is a form of malicious software, known as malware, used to encrypt data or files on information technology (IT) systems and operational technology (OT) environments in order to block access to a computer system until a sum of money is paid.

Table of contents

1. Understand ransomware

Ransomware is a form of malicious software, known as malware, used to encrypt data or files on information technology (IT) systems and operational technology (OT) environments in order to block access to a computer system until a sum of money is paid. Cyber attackers use ransomware to target all types of data and systems, from employees' passwords and social security numbers, to critical infrastructure, as in the case of the much publicised 2021 attack on the Colonial Pipeline in eastern US (see section 1.1.3). In this case a ransomware attack disabled communication between IT and OT systems, preventing the distribution of oil supplies[1].

Ransomware is one of the latest cyber threats gaining popularity due to its sophisticated operation and direct financial benefits for attackers. Ransomware attacks rose by 151% in 2021, with an average of 270 cyber attacks per organisation, representing a 31% increase from 2020, according to the World Economic Forum's (WEF) 2022 Global Cyber Security Outlook[2]. The average cost of OT-specific malware attacks for critical infrastructure organizations was $4.82M. Critical infrastructure organizations had an average cost of a data breach $0.99M higher than the $3.83M for organizations in noncritical infrastructure industries.[3]

Malware may infiltrate and remain present within a computer system for many months without being detected, all the time gathering sensitive information and identifying vulnerabilities in that organization's cyber security controls. As ransomware attacks become more readily available through direct purchase of malicious software or 'ransomware as a service' (RaaS) offerings, attackers can reap the benefits of the latest developed technology, without any intellectual investment themselves. As systems are infected and become inoperable to the end user, ransom payment requests are issued to regain access to the information. These methods of payment, typically via cryptocurrency, are nearly untraceable by law enforcement, further adding to the appeal and making ransomware the number one cyber threat for businesses, according to ENISA Threat Landscape 2021[4].

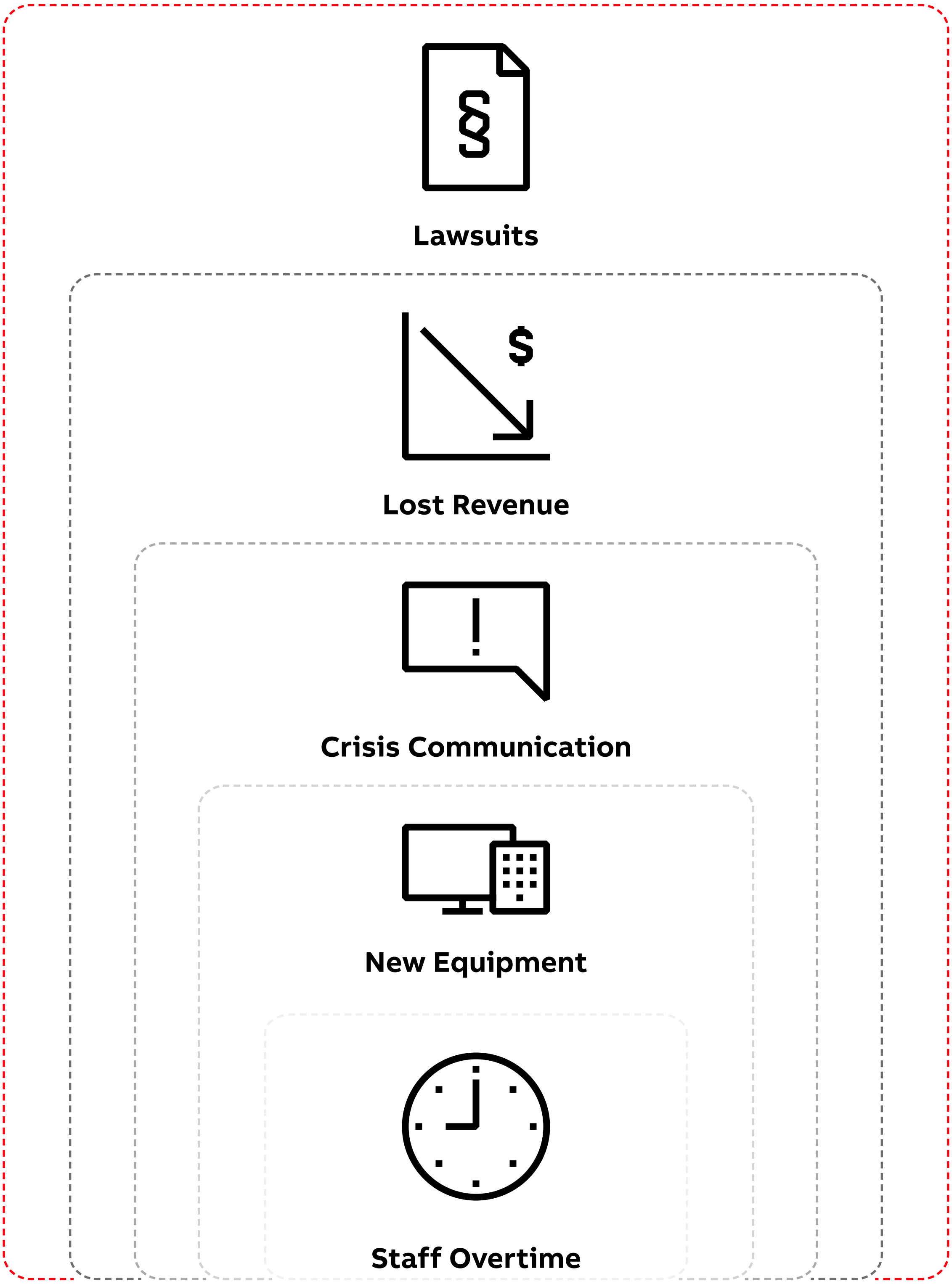
Threat actors target and infect as many systems as possible before being detected, gaining access via a range of methods (see 1.1.1 and 1.1.2), but encryption is only initiated after a critical mass of systems has been reached, or specific conditions met, such as a predefined date. Most ransomware payments are made by organizations that want to protect their revenue stream, hence the perception that paying is the quickest way to regain control of one's assets. Alternatively, an organization may have good file and recovery systems in place, and may assume they are safe and refuse to pay the ransom. Both perceptions are often wrong, however. Attackers often have a second goal in mind, which is to include data exfiltration and data deletion. If both occur, we could see trends in which the threat actor can leverage their target for a second payment through the use of exfiltrated data or use published data to a leak site to assure payment is made even if you are capable of restoring the system independently.

There is also increasing evidence that paying cyber attackers perpetuates the RaaS model, with nearly 80% of organizations that paid a ransom reporting that they suffered repeat ransomware attacks, usually within a month and at the hands of the same attackers, according to a recent report from Cybereason[5].

To summarize, ransomware attacks on both IT and OT system are increasing, becoming more sophisticated and represent a significant financial and reputational threat to organizations across multiple industry sectors. The threat actor does not stop after the initial ransom; in fact, double extortion ransomware attacks are increasing, as are repeated attacks on the same target.

In this paper, we will discuss what form ransomware attacks can take; what steps to take if a ransomware attack occurs; and basic measures organizations must take to detect, analyse, contain and eradicate the threat.

Cyber Attack
Holistic cost view



Lawsuits

Lost Revenue

Crisis Communication

New Equipment

Staff Overtime

1.1. Typical infection vectors for OT systems

In cyber security, an infection, or ''attack vector'', is a method or pathway used by a hacker to access or penetrate the target system. This section describes the various infection vectors which may directly or indirectly impact the OT environment. Direct infections occur within the OT network space itself, while Indirect occur outside of the OT space (typically at the IT or Enterprise level), an example being email 'phishing' campaigns designed to induce users to reveal personal information. Due to dependencies between systems, both infection types carry the potential for critical impact on operations as a whole.

1.1.1. Direct attack

Direct ransomware attacks are defined as those that target and gain access to critical computer networks or distributed control systems (DCS), often using remote access solutions or an outdated operating system, with the intention of stealing sensitive or proprietary information. For example:

- **Internet-facing device vulnerabilities and misconfigurations (remote access)**

  Even within the OT space, outward facing connections are sometimes required to support efficient operations. Whether its an industrial internet of things (IIoT) device, remote access point, or production information being sent to a corporate office for analysis, these connections need to be securely implemented and properly maintained with the appropriate security patches.

  The remote access tool itself is often not to blame; instead poor implementation, configuration or maintenance of the remote access connection can leave the network vulnerable to ransomware and other cyber attacks. In addition, outdated or weak password protection, or multiple employees using the same password, can also make it easier for hackers to access an OT system and launch a ransomware attack.

- **Weak system architecture / segmentation and filtering rules**

  Weak system architecture: how the various software components of a computer network or system are designed, structured and behave – is another vulnerability that can leave organizations open to cyber attacks. An outdated internet firewall, for example, may give hackers access to IT and OT systems without the organization's knowledge. Underling this point, 48% of the organizations surveyed for the SANS 2021 OT/ICS Cyber security Report[5] did not know whether their industrial control system (ICS) had been compromised.[6] A 'flat' or over-simplified IT network, one where all devices are interconnected, is another red flag; not only do attackers have multiple ways to infiltrate the network, if one element is compromised, then the entire system is put at risk.

  System architecture is a critical aspect of any cyber infrastructure. Acting as the foundation in which all other components are built upon, users must ensure that this structure is sound, designing to support current and future operations. Without appropriate architecture and segmentation in place, access cannot be appropriately restricted, ultimately leaving the system more vulnerable to attack and the spread of malware.

- **Third parties and managed service providers**

  Third-party service providers such as maintenance engineers can unwittingly leave organizations open to direct ransomware attacks on OT systems. Take the example of a routine configuration change: the engineer may gain access via an external laptop, or plug in an external USB stick, neither of which may have the same level of cyber security as the system they are working on. Companies, particularly in the engineering space, must be aware that having a closed, protected network will not automatically protect them from being infected by malware or viruses introduced– inadvertently or otherwise – by third parties. In this instance, it is important to establish clear guidelines around OT systems and network access.

- **Precursor malware infection**

  As previously mentioned, malicious software can remain undetected in IT and OT systems for long periods, often laying the groundwork for a full ransomware attack in the future. This is often referred to as 'precursor malware', and the resulting ransomware attack may be evidence that the network was previously compromised, often without the target's knowledge.

1.1.2. Indirect attack

Indirect cyber attacks, while not as high-profile or immediately impactful as direct campaigns, also pose a significant threat, either by themselves or, as detailed in the previous section, as a precursor or prelude to a more serious direct ransomware attack. IIoT devices can open companies to risk, but many recent, high-profile cyber attacks have been conducted from a laptop, by hacking someone's virtual private network (VPN), or are a simple phishing/malware attack. During these types of indirect attacks, cyber criminals may layer tactics to steal, disrupt or destroy data through intermediary sources.[7]

The scope of a cyber security risk assessment should therefore not just cover the cost impact of an indirect attack and how to budget for foundational data protection tools, such as malware protection software and firewalls, but should also extend to operations infrastructure. In fact, the internationally recognized IEC 62443 cyber security standard contains guidelines and recommendations that cover ICS and systems applications and products. The Colonial Pipeline ransomware attack (see 1.1.3) – where hackers initially targeted IT systems, eventually forcing the operator to sever communication with OT systems, demonstrated the risks associated with interdependent IT and OT networks.

- **Phishing**

  Phishing is the act of sending emails to multiple users in the guise of a known or legitimate person or organization in an effort to get them to reveal information or unknowingly help the attacker by activating a malware. Spear phishing is also another type of email, but in this instance targets specific individuals in an organization. These are two of the most popular methods of initiating a ransomware attack by infiltrating IT systems, often without the individual being aware.

- **Drive-by download**

  The term ‘drive-by download’ refers to the unintentional download of malicious code to a computer or mobile device that leaves the user vulnerable to a cyber attack. This can be something as simple as downloading and installing a driver from a website that may also contain malicious software, or even opening a webpage using an outdated internet browser that is not equipped to detect and alert you to the threat of drive-by attacks. Even plugging a smartphone into a DCS computer for charging can result in that system being infected.

1.1.3. Use case

To highlight the severity of an indirect ransomware attack, a recent example from the media has been chosen, which highlights how system interdependencies can impact the infrastructure as a whole. The Colonial Pipeline Company[2] in the U.S. was hit with ransomware in 2021. Though only their IT infrastructure was compromised, dependencies on those networks triggered a halt on all production and distribution processes for multiple days while systems were recovered. The Colonial attack was multidimensional, in that it also affected the wider US economy and national security, since the pipeline transports nearly half of the east coast's fuel supplies.[8] Some key points are highlighted below to offer additional background on the case, along with the associated impact resulting from the attack.

Background[3]	Threat	Impact
Colonial Pipeline Company	Threat Vector: Ransomware	Network isolation to contain impact
Largest refined oil pipeline system in the US	Additional threat vectors leveraged	Halt all operations
Approximately 5,500 miles of pipeline (about twice the width of the United States)	Objective: Encrypt critical information and leverage for monetary gains	IT network compromised
Delivers 100 million gallons per day	Ransomware group: Darkside	Operations offline for 5 days
	Offers “Ransomware as a service” model to customers	Public distress
		$5,000,000 Paid in ransom
		Most disruptive cyber attack on record at that time

2. Preparation

One can take several actions to reduce the likelihood of a ransomware attack and reduce the impact if the unthinkable were to happen.

Below are 20 topics that aim to reduce the risk of a ransomware attack, ten dedicated to prevention and ten for recovery. These items should be reviewed to ensure they are considered part of one's organization's plan to minimize the risk and impact of a ransomware attack or other cyber incident.

Naturally, these recommendations will minimize the impact of any cyber incident or system failure independent of the root cause.

Disclaimer: The preparation steps and preventive measures have been selected for having the most impact with ransomware resilience in mind. Other threats might shift focus. When designing a cyber security program, a risk based approach should be followed.

2.1. Minimize the likelihood

It is better to avoid being a victim in the first place, and several actions and solutions will reduce the likelihood of an attacker being able to successfully deploy the ransomware in your system.

2.1.1. Defensible design

By leveraging a reference architecture, such as ABB's ICS Cyber Security Reference Architecture, one will have the foundation to add security while still being able to adopt digitalization and leverage data. The key is managing and controlling the OT system's data flow.

2.1.2. Hardening

Hardening is a powerful security control to reduce the attack surface by ensuring that each device is configured correctly and that no unnecessary applications or services are installed. Hardening supports the principle of least function, a cornerstone concept in cyber security.

2.1.3. Removable media

A sub-set of hardening is to limit and control the use of removable media such as USB disks. This dramatically reduces the risk of malware as removable media is one of the most used methods to spread malware.

2.1.4. Access control

Another critical concept in cyber security is the principle of least privilege, achieved by implementing access control to manage who is allowed access to which system and what they can do. For instance, no one should use an admin account for regular operations as this account provides the user unrestricted access to everything.

2.1.5. Software updates

All software has vulnerabilities that attackers can exploit. Therefore, it is crucial to install updates regularly. Remember that this applies to any software including network equipment and mobile devices, in addition to computers.

2.1.6. Malware protection

Malware protection (also known as antivirus or blocklisting) prevents known bad applications from executing on protected computers. This reduces the risk of known malware (aka viruses) being used in an attack forcing the attacker away from conventional methods. This will ultimately eliminate many attackers with limited knowledge and experience.

2.1.9. Monitoring

Monitoring is about collecting and storing data, either for automatic analysis and detection of malicious activity in a Security Information Event Monitoring (SIEM) system or to have a record of what has happened to go back to as part of the forensic work after an attack. Event and network monitoring capabilities are viable solutions, and using these in conjunction is the best approach for a holistic system view.

Important: Monitoring tools are useless if no one is using them. Personnel must look at these systems and respond accordingly to detect malicious activity.

2.1.7. Allowlisting

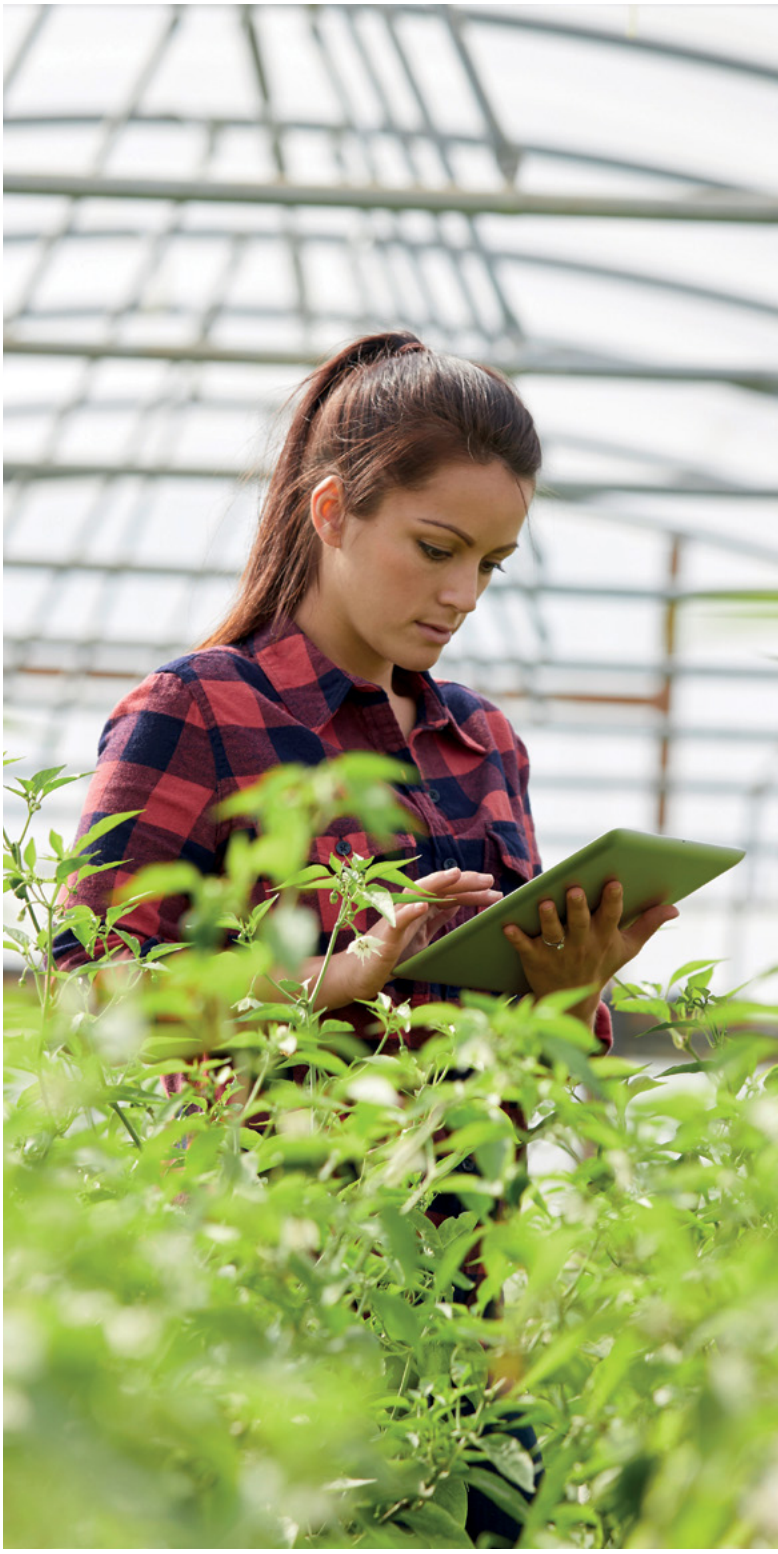
Allowlisting is the opposite of malware protection (blocklisting) and is a powerful tool against malicious software. It only allows known good applications to execute making it very hard for attackers to execute their malware.

2.1.8. Intrusion detection

Intrusion detection systems, leverage data in the system to automatically detect malicious behavior (intrusions). Note that they do not block the intrusion, it simply alerts the user of the event. To automatically prevent intrusion, one needs an intrusion prevention system (IPS). However, these are not recommended for use in an OT system as an erroneous action may lead to unsafe operations, endangering people and the environment.

2.1.10. Training

One of the most effective tools to lower the risk of a cyber attack is training. Ensuring that the organization's personnel understands what cyber security is about, how attackers work, and what they can do to reduce the risks.



2.2. Minimize the consequence

Even with the best defenses, one may still fall victim to a ransomware attack. If this happens, one must have a plan on how to get back in operation while reducing the consequences of the attack.

2.2.1. Business impact analysis

A business impact analysis (BIA) determines how bad a cyber attack would be to the business. It is essential to know this as it sets the priority, and to some degree the company's cyber security budget.

2.2.2. Key recovery target

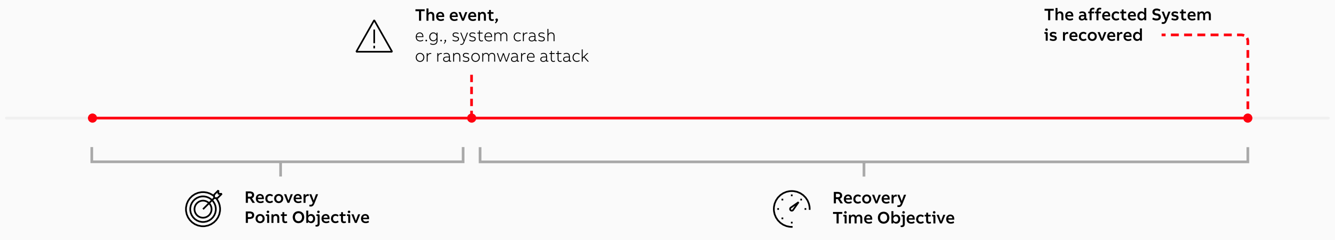
Not all systems are likely to be equally critical to production, and it is essential to know which system(s) to prioritize to minimize business impact.

2.2.3. Recovery point objective

The recovery point objective (RPO) defines the maximum targeted period in which data can be lost without an irreparable impact on the business. In industrial systems, RPO is often the time of the latest change to control projects and engineering data.

2.2.4. Recovery time objective

Recovery time objective (RTO) is the maximum time accepted to elapse between an attack and when the business process and production must be restored. This is typically derived from the business impact analysis (BIA).



2.2.5. Plans

- **Disaster recovery plan**

  A Disaster recovery plan (DRP) is a detailed document that describes and defines in a structured approach what to do in the case of a cyber incident. What must be done for the organization to restore business operations and minimize the effect of the disaster.

- **(Crisis) communication plan**

  A crisis communication plan is crucial during an emergency or incident. It is a blueprint of different scenarios and typically defines communication regarding when to respond, who is authorized to respond, and to whom.

  Do not let anyone communicate externally as it is important not to cause panic or say something that may impact the company's reputation.

- **Contact list**

  Have an up-to-date list of internal and external contacts needed to respond to a ransomware attack, including law enforcement and insurance companies. Updating your emergency contacts and contracts keeps you ready if a disaster strikes.

2.2.6. Backups

Backups are always important especially when it comes to ransomware. Without a backup you are forced to pay the ransom and trust that the attacker provides the decryption key and that the decryption works.

Keep in mind that it is a possibility that some ransomware attackers will try to find and destroy or infect existing backup sets in the network, making it hard for incident response teams to recover system(s).

- **Backup and restore procedure**

  The backup and restore process must be checked periodically to ensure all the needed components are available, known and functional in critical situations.

- **Backup validation**

  If a disaster strikes, one of the last lines of defense might be a recovery from an offline backup, which should be regularly tested to ensure that the backup will work when needed.

2.2.7. Spare components

Standby hardware is essential to rebuilding or restoring a system if one suspects that the ransomware has infected the components of the hardware such as the bios. In some cases law enforcement can require affected systems not to be touched until forensic investigations are finished, leading to production not being reestablished which could have a severe business impact if spare parts are unavailable.

Depending on the RTO, different preparations must be made, ranging from having a complete running copy of the system (hot spare), or a copy of the system (warm spare), to spare parts of the hardware (cold spares).

2.2.8. Alignment between SLA and business goals

Service level agreements (SLA) must be aligned to meet the defined recovery time objective. SLAs must support the organizations business goals regarding reaction times and provide incident response guarantees.

2.2.9. Documentation

The regularly updated documents, from the BIA to a detailed network diagram that describes systems and data flows within the organization's network, are critical when deal with a catastrophic event such as ransomware.

2.2.10. Training

It is not enough to have plans such as a disaster recovery plan. One must train all involved parties on it regularly. This is in addition to training on how to restore backups, use tools, and even who to call in the event of a disaster.

2.3. Ransomware preparation guide

Throughout this section, a multitude of topics have been addressed which will aid users in preventing potential attacks on their systems, while also highlighting keys areas in preparing for worst case scenarios. To offer additional support on the topic, ABB has created a short interactive e-book which provides a user-friendly guide to addressing these concerns in one's own environment.

To learn more visit our web page at www.abb.com/cybersecurity/service and click on Ransomware Recovery e-book or use the QR code to get to the e-book directly.

3. What to do if disaster strikes

As technology (and associated threats) continue to evolve, it is becoming increasingly difficult to prevent cyber attacks from occurring. With the number of ransomware attacks escalating globally, it is now no longer a question of **if** a system will be the target of an attack but rather **when** this attack may occur.

Given this reality, situational awareness, an understanding of the IT environment (network awareness) the threats and vulnerabilities it faces (threat awareness) and how to respond and mitigate against future attacks (mission awareness)[9] – from board level down through the employee hierarchy is critical. In the world of cyber security, measures can be taken to prevent attacks from occurring within systems; however, human beings must also be made aware of the organization's risk profile. This should include how attackers can see them on the internet or if there are any remote connections they can exploit. Employess should also be kept up to date with cyber security best practices so they can remain vigilant and respond appropriately to any initial indications of a cyber attack in their infrastructure.

Situational awareness, as defined above, is key in this scenario. ABB has outlined basic steps that will help users to gain this awareness and guide them through the stages of detection, analysis, containment, and eradication of these cyber threats. The following items are a mix of regulatory requirements and industry best practices, refined to provide users with the best overall visibility into their infrastructure in case of emergency.

Situational awareness is key to detection, while crisis communication provides clarity and direction and shows responsibility!

Best practices for creating **Situational Awareness**

Monitoring and correlation of system events, detect anomalous or suspicious activity, and known-bad conditions.

Storage of event history (for a reasonable amount of time) to allow for retrospective analysis for indicators of compromise (IOCs).

Keep the threshold (complexity) of incident reporting as low as possible to not deter people from reporting what they see.

Keep people informed about the progress of the incident handling (to a reasonable level of detail) to let them experience the positive impact their reporting had.

Treat analysis and response as an iterative loop – response actions can generate insights which are relevant to the analysis.

Don‘t be shy to involve additional “outside“ resources (outside your team or even outside the organization).

Feed back results from response actions to analysis.

Institutionalize and fine-tune stakeholder communication.

Ensure focus on relevant information by using templates.

Ensure single path of communication with clear responsibilities (who communicates what to whom and when) to avoid mixed messages.
Often stakeholders include representatives at similar management levels, e.g. from IT and OT. There should only be one set of communication for a given target audience and it should be clearly defined what is being communicate to whom, when and by whom. It can create great confusion and distract attention from the actual response if management gets mixed messages and initial response teams need to spend time on explaining and fixing communications.

Below, several scenarios have been outlined to depict potential cyber attacks that may occure within an ICS environment. These instances highlight scenarios which may not have been originally considered when assessing cyber risk within ones environment.

Example attack scenarios:

- An industrial controls environment had no event or network monitoring capabilities, and thus did not detect a remote access jump host which had been compromised. This event went undetected for several months until the intruder decided to install ransomware on the machine after first exfiltrating sensitive data.
- When analyzing an OT system and searching for indicators of compromise (IOCs), a user realized that their event logs were only stored on the individual endpoints (e.g. firewalls, local windows logs). Due to capacity limitations, the system could only retain approximately one week of information. With this lack of historical events, no statement could be made as to whether a malicious attempt was made earlier.
  Please Note: In most cases, it is not economically reasonable to maintain all historical information required for digital forensics in house – in this scenario, involving external resources like service providers, consultants and public agencies may be beneficial.
- In scenarios where users do not have a holding statement prepared for emergency use, they must derive a direct response to the incident at hand. This scenario can create contradictory responses throughout the various departments of an organization, and may also result in delayed communication response times.

3.1. Basic steps for detection and analysis

Protecting business operations begins with detecting potential threats, analyzing the nature and level of the threat and then, quickly and efficiently applying appropriate cyber security tools and best practices to isolate the threat and limit the potential damage to the OT system or network and overall operations. The following steps have been outlined to provide guidance in defining a process around what to do first after noticing ransomware.

1 Determine which systems are impacted, and immediately isolate them to stop the spread of the malicious threat.

2 If you are unable to disconnect devices from the network, shut them down to avoid further spread. Be aware that shutting a computer down may lead to loss of evidence, and a reboot may prevent access to the computer unless you pay the ransom.

3 If existing, turn off any wireless functionality.

4 Identify the attacker's initial access, methods, and systems and accounts used. This is best accomplished by using your event monitoring solution.

5 Verify if data was exfiltrated and if credentials have been stolen. Tools to help with this work includes network intrusion detection systems and your event monitoring solution.

5 Attempt to determine ransomware strain as this can help to discover existing guidelines or decryption methods.

6 Triage impacted systems based on the disaster recovery plan and defined key recovery targets.

7 Document what has happened. Keep the complexity low as possible to not deter people from reporting their observations and actions.

8 Execute the communication plan. Keep involved parties informed about the progress to keep them engaged and let them know their work's positive impact.

10 Alignment with functional safety practices can leverage synergies.

3.2. Basic steps for containment and eradication

Here is a guide for performing the short and longer term containment and eradication measures necessary to allow systems to be used in production, while rebuilding clean systems and actions to take to prevent similar attacks in the future.

1 Review your cyber insurance contract requirements.

2 Prepare for forensic analysis by staging equipment.

3 Define approach to forensic investigation.

4 Consult law enforcement regarding decryption tools available and for guidance about the identified ransomware.

5 Consider using the decryption tools provided, but be careful as they may do irreparable harm to the data if failing or if the tool is not the right one for the ransomware.

6 Even if the overall guidance is not to pay the ransom, there might be scenarios where you must make a business decision to do just that. Make sure you have an experienced negotiator.

7 Contain any systems that may be used for further or continued unauthorized access, such as virtual private networks (VPN), remote access, single sign-on (SSO), cloud connections.

8 Examine existing detection and prevention systems.

9 Conduct extended analysis to identify outside-in and inside-out persistence mechanisms.

3.3. Basic steps to recovery and post-incident actions

It is essential to cautiously bring affected production systems back online to prevent additional attacks or malware infections. Test, verify, and monitor affected systems to ensure they are back to normal and there is no indication of malicious activity. Within two weeks of the incident, one should perform a retrospective, including preparing complete documentation of the incident and whether anything in the incident response process could be improved.

1 Rebuild the system as outlined in the disaster recovery plan (DRP).

2 Reset passwords for all affected systems and accounts.

3 Address all identified vulnerabilities and security gaps.

4 Address any identified vulnerabilities and visibility gaps.

5 Declare the ransomware incident over.

6 Document lessons learned from the incident and associated response activities. Involve all stakeholders.

7 Treat analysis and response as an iterative activity where response actions generate insights that are relevant to the analysis.

8 Maintain statistics of incidents to fine-tune risk assessments and, based on that, mitigation through your cyber security program.

4. Conclusion

In summary, ransomware poses a significant financial and reputational threat to businesses across multiple industries. Malicious actors, be they nation states, business rivals or cyber criminals intent on blackmail, are deploying ever more sophisticated tools to exploit vulnerabilities resulting from increased interconnectedness between OT and IT systems, as well as increased remote connectivity in the wake of COVID-19.

OT systems can be targeted by direct, coordinated attacks on critical networks or DCS infrastructure, or by indirect attacks using methods such as phishing emails, or by third parties inadvertently introducing malicious software into the network through external devices such as smartphones, laptops or USB sticks.

In this white paper, we have:

Identified the main types of ransomware attacks.

Described how and why cyber criminals target and infiltrate certain organizations and computer systems.

Oulined the basic steps on how to detect and analyse a ransomware attack should it occur.

Explained how to contain and eradicate ransomware once it has infected a system or network.

Illustrated how lessons learned from ransomware attacks can help inform cyber security best practice and mitigate future threats.

Robust cyber security and protection against ransomware should be a fundamental part of every business organization’s wider digital transformation. This journey begins with a cyber security assessment in partnership with trusted technology experts and suppliers.

After performing an assessment, our experts will be able to map out a strategic plan for closing the gaps in your situation. In some cases, aligning this strategy to services and products in ABB's Cyber Security portfolio will be the fastest and most efficient for accomplishing this goal. These basic steps will help your teams prepare for a disaster, how to respond, and how to communicate.

5. References

1. "… where a ransomware attack disabled communication between IT and OT systems, preventing the distribution of oil supplies**1**."
Robert Putman, ABB – 'Protect physical assets from cyber-attacks'

2. "Ransomware attacks rose by 151% in 2021, with an average of 270 cyber attacks per organisation, representing a 31% increase from 2020, according to the World Economic Forum's (WEF) 2022 Global Cybersecurity Outlook**2**." https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

3. "The average cost of OT-specific malware attacks for organizations is $2.6m**3**." https://new.abb.com/process-automation/process-automation-service/advanced-digital-services/cyber-security/abb-cyber-security-reference-architecture **- The Cost of OT Cybersecurity Incidents and How to Reduce Risk. Nozomi Networks. 2020.**

4. "These methods of payment, typically via cryptocurrency, are nearly untraceable by law enforcement, further adding to the appeal and making ransomware the number one cyber threat for businesses, ac-cording to ENISA Threat Landscape 2021**4**." https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

5. "There is also increasing evidence that paying cyberattackers perpetuates the RaaS model, with nearly 80% of organizations that paid a ransom reporting that they suffered repeat ransomware attacks, usually within a month and at the hands of the same attackers, according to a recent report from Cybereason**5**."
https://www.techtarget.com/searchsecurity/news/252521164/Cybereason-Paying-ransoms-leads-to-more-ransomware-attacks?utm_campaign=20220612_ERU-ACTIVE_WITHIN_240_DAYS&utm_medium=EM&utm_source=SGERU&source_ad_id=252521164&src=9958692&asrc=EM_SGERU_227556292

6. "48% of the organizations surveyed for the SANS 2021 OT/ICS Cybersecurity Report did not know whether their industrial control system (ICS) had been compromised**6**." https://new.abb.com/process-automation/process-automation-service/advanced-digital-services/cyber-security/abb-cyber-security-reference-architecture
https://www.nozominetworks.com/press-release/nozomi-networks-sponsored-sans-survey-finds-cyber-threats-to-ot-environments-continue-to-rise-severity-reaches-all-time-high/

7. "During these types of indirect attacks, cyber criminals may layer tactics to steal, disrupt or destroy data through intermediary sources.**7**" https://www.verizon.com/business/resources/articles/s/protecting-against-an-indirect-attack-in-cyber-security/

8. "The Colonial attack was multidimensional, in that it also affected the wider US economy and national security, since the pipeline transports nearly half of the east coast's fuel supplies**8**." https://www.cnbc.com/2021/05/08/colonial-pipeline-shuts-pipeline-operations-after-cyberattack.html

9. "Given this reality, situational awareness – understanding of the IT environment (network awareness), the threats and vulnerabilities it faces (threat awareness) and how to respond and mitigate against future attacks (mission awareness)**9**." https://www.mitre.org/capabilities/cybersecurity/situation-awareness

—

ABB
Operating in more than 100 countries

Authors:
Tobias Nitzsche
Cyber Security Practice Lead,
ABB Process Automation

Matthew Virostek
Global Cyber Security Product Manager - DCS Security,
ABB Process Automation

solutions.abb/cyber-security-services