Ransomware Preparation Guide: Prevention, Mitigation, and Recovery for Manufacturers

OVERVIEW

Ransomware is a major cyberattack vector against U.S. original equipment manufacturers (OEMs) of all sizes. Over half of all cyberattacks on manufacturers are from ransomware and, of these, over 80% are due to human errors. Ransomware attacks continue to grow in volume, sophistication, and impact, and they will accelerate more rapidly as artificial intelligence (AI) is built into these attack vectors.

Ransomware attacks typically involve the victim unintentionally downloading software that is maliciously designed to encrypt data so that it can't be used by the data's owner(s). The "ransom" is a demand from the attacker for financial resources with the claim that the victim will be provided a decryption key to restore their data. These attacks not only result in deep financial losses, but also disrupt operations (causing significant downtime).

Operational technology (OT) systems monitor and control physical process industrial environments. Manufacturers rely on OT systems to transfer data from design to product manufacturing, and these OT systems are particularly vulnerable to cyberattacks like ransomware. This is because a) OT systems are not designed to be secure; b) OT systems control critical infrastructure (many manufacturers are integrated into this infrastructure), making them a prime target for attackers aiming to disrupt supply chains or the economy; c) OT networks are typically connected to the internet, providing attackers easy access; and d) ransomware attacks against OT systems have high stakes because of the severe consequences that can befall manufacturers.

Additionally, manufacturers' production operations are especially vulnerable to ransomware attacks because they typically start with a design (data) which is then imported (data flow) into a machine for the generation of a product, part, or component. Since the entire process is data-dependent, holding this data hostage is especially profitable for the attacker.

What are the consequences of a ransomware attack on manufacturers?

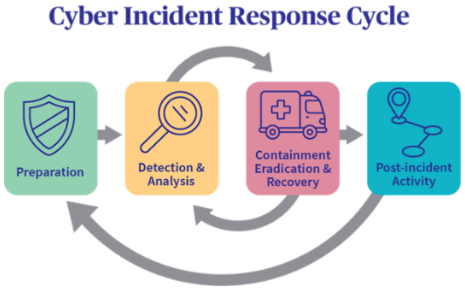
- Operations are disrupted, causing downtime and financial loss. These attacks can also result in business loss and even bankruptcy.
- Worker safety is compromised.
- A manufacturer's reputation can be damaged, and they may lose customers.
- In addition to the direct cost of the ransom, if the decryption key is not provided after payment, a manufacturer faces greater losses as their systems must be rebuilt. The Sophos State of Ransomware Report (2021) states that only 8% of the victims retrieve all data after paying the ransom (and 29% recover less than half of their data).

PREVENTING AND MITIGATING RANSOMWARE ATTACKS

To prevent and mitigate ransomware attacks you should focus on three action items immediately. These top priorities are a) create a cyber-informed workforce (see CyManII capabilities to assist with this); b) back up your data securely so that, if attacked, you can restore your own machines and systems to decrease downtime; and c) develop and practice an incident response plan. Doing this will significantly reduce your cyber risk profile. Please consult with CyManII for assistance on all three of these priorities and any other challenges you face as you read and incorporate the following guidance.

Top Three Ways to Prevent and Mitigate Ransomware Attacks – Do These Immediately!

1. Create a cyber-informed workforce. Approximately 84% of ransomware attacks against U.S. manufacturers stem from *human error*. Thus, basic cybersecurity training goes a long way toward preventing these attacks. CyManII offers this training in several modalities (in person, on-line, hybrid, etc.). The cost for this is always low but takes CyManII membership status into consideration. See Appendix 1 for current offerings.
2. *Securely* back up your data as soon as possible. In the context of OT, backing up means a) making copies of important data stored on OT devices and industrial facilities and b) keeping them in a separate storage system in a data center or in the cloud. Remember to test your backups for proper disaster recovery. See Appendix 2 for best practices and common methods for backing data up securely. If you are unsure how to back data up in a secure manner, reach out to CyManII and we can provide guidance.
3. Develop and practice an *Incident Response Plan.* A Cybersecurity Incident Response Plan is a document that gives your leadership and information technology (IT)/OT team instructions on how to respond to a serious security incident, such as a data breach, data leak, ransomware attack, or loss of sensitive information. According to the National Institute of Standards and Technology (NIST),[1] there are four phases to effective incident response plans: 1) preparation, 2) detection and analysis, 3) containment, eradication, and recovery, and 4) post-incident activity. Many resources can help you develop an Incident Response Plan, but the most important thing is to get one ready and practice it—this will significantly decrease downtime and financial loss in the wake of a cyberattack. Resources include:


Cyber Incident Response Cycle
Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-incident Activity

a) https://hyperproof.io/resource/cybersecurity-incident-response-plan/
b) https://ised-isde.canada.ca/site/cybersecure-canada/en/certification-tools/develop-incident-response-plan-fillable-template-and-example
c) https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
d) And this short video from NIST is a great place to begin: https://www.youtube.com/watch?v=pgeDvqmYTbM

ADDITIONAL FACTORS TO CONSIDER AS YOU MATURE YOUR COMPANY'S CYBERSECURITY POSTURE

[1] "NIST Cybersecurity Framework (CSF) 1.1 and 2.0," Hyperproof, accessed May 28, 2024, https://hyperproof.io/nist-cybersecurity-framework-solution/.

After completing the top three steps above, there is much more you can do to prevent and mitigate cyberattacks and ransomware attacks. These additional factors are outlined in the next sections and are organized by 1) Before the attack, 2) During or Immediately After the attack, and 3) After the attack. All of these will enhance your security posture, but focusing on the Top Three is critical!

BEFORE the Attack (#1 and #2 are the priorities)

1. Back up your data *securely* and have a plan in place to restore after an attack. Practice this plan before an attack occurs.
2. Make sure your systems (hardware/software) are using the latest operating systems and perform regular (at least monthly) patches of the software for both the network and the machines/devices on the network.
3. Consider having cyber insurance in place. Having insurance, at some level, will lower the cost of a ransomware attack.
4. Consider developing and implementing a "BYOD" (Bring Your Own Device) policy. Virtually all small and medium manufacturers allow their employees to connect to the network with personal devices, and many encourage those personal devices to be used to control machines or systems on the factory floor. While this is sometimes acceptable, you should develop a plan to minimize the associated cyber risks and implement this as a policy for every employee.
5. Invest in password security and multi-factor authentication. Usernames and passwords are no longer a sufficient security control measure. It is worth considering investing in 2nd Factor Authentication (2FA) as an additional layer of security. There are several types of 2FA, such as SMS, digital certificates based on PKI (Public Key Infrastructure) technology, biometrics, and soft and hardware tokens. Consider which methods best match your company and its resources.
6. Secure your corporate emails. About 41% of ransomware attacks are initiated via employee email practices and deploy attacks such as phishing. Phishing is a form of social engineering intended to deceive employees into revealing sensitive data that can then be used for the attackers to penetrate your network, machines, and devices. The first line of defense is to "create a cyber-informed workforce" so that your employees recognize phishing attempts. After this, consider protecting corporate emails with a protocol called S/MIME. S/MIME protects emails that are sent from your company in three main ways: by providing strong assurances when backed by a trusted Certificate Authority of the sender's identity, protecting the communication's confidentiality while in transit on mail servers through the use of encryption, and confirming message integrity through validation processes that can ensure the message isn't altered.
7. Complete regular security audits. Security audits can detect cyber vulnerabilities ahead of their exploitation by adversaries and thus can help identify security weaknesses and allow them to be addressed prior to attacks.
8. Have an Incident Response Plan in place and practice it so that everyone knows what to do and who is responsible for specific actions. Such a plan will reduce the impact of an attack, provide assurance to investors, and allow for a more rapid recovery (less downtime), all of which increases productivity and profitability.

DURING OR IMMEDIATELY AFTER the attack:

9. Determine which systems/machines were impacted, and immediately isolate them.

   a. If several systems, machines, or subnets appear impacted, take the network (both IT and OT) offline at the switch level. It may not be feasible to disconnect individual systems during an incident.
   b. Prioritize isolating critical systems and machines that are essential to daily operations.
   c. If taking the network temporarily offline is not immediately possible, locate the network cable (e.g., ethernet) and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
   d. For cloud resources, take a snapshot of volumes to get a point-in-time copy to review later for forensic investigation.
   e. After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Isolate systems in a coordinated manner and use out-of-band communication methods such as phone calls to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access or deploy ransomware widely prior to networks being taken offline.

10. Power down machines and devices (if you are unable to disconnect them from the network to avoid further spread of the ransomware infection).
    a. Note: This step will prevent your organization from maintaining ransomware infection artifacts and potential evidence stored in volatile memory. It should be carried out only if it is not possible to temporarily shut down the network or disconnect affected hosts from the network using other means.
11. Triage impacted machines and systems for restoration and recovery.
    a. Identify and prioritize critical systems for restoration on a clean network and confirm the nature of data housed on impacted systems.
    b. Prioritize restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation, or other critical services, as well as systems they depend on.
    c. Keep track of systems and devices that are not perceived to be impacted so they can be deprioritized for restoration and recovery. This enables your organization to get back to business in a more efficient manner.
12. Examine existing organizational detection or prevention systems (e.g., antivirus, Endpoint Detection and Response, Intrusion Detection Systems, Intrusion Prevention System) and logs. Doing so can highlight evidence of additional systems or malware involved in earlier stages of the attack.
    a. Look for evidence of precursor "dropper" malware, such as Bumblebee, Dridex, Emotet, QakBot, or Anchor. A ransomware event may be evidence of a previous, unresolved network compromise.
    b. Operators of these advanced malware variants will often sell access to a network. Malicious actors will sometimes use this access to exfiltrate data and then threaten to release the data publicly before ransoming the network to further extort the victim and pressure them into paying.
    c. Malicious actors often drop ransomware variants to obscure post-compromise activity. Care must be taken to identify such dropper malware before rebuilding from backups to prevent continuing compromises.

13. Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis. If you are uncertain, this is a good time to call the local Federal Bureau of Investigation (FBI) field office.
14. Initiate threat hunting activities.
15. For enterprise environments, check for:
    a. Newly created Active Directory (AD) accounts or accounts with escalated privileges and recent activity related to privileged accounts such as Domain Admins.
        i. Anomalous VPN device logins or other suspicious logins.
        ii. Endpoint modifications that may impair backups, shadow copy, disk journaling, or boot configurations. Look for anomalous usage of built-in Windows tools such as bcdedit.exe, fsutil.exe (deletejournal), vssadmin.exe, wbadmin.exe, and wmic.exe (shadowcopy or shadowstorage). Misuse of these tools is a common ransomware technique to inhibit system recovery.
        iii. Signs of the presence of Cobalt Strike beacon/client. Cobalt Strike is a commercial penetration testing software suite.[2] Malicious actors often name Cobalt Strike Windows processes with the same names as legitimate Windows processes to obfuscate their presence and complicate investigations.
        iv. Signs of any unexpected usage of remote monitoring and management (RMM) software (including portable executables that are not installed). RMM software is commonly used by malicious actors to maintain persistence.
        v. Any unexpected PowerShell execution or use of PsTools suite.
        vi. Signs of enumeration of AD and/or LSASS credentials being dumped (e.g., Mimikatz[3] or NTDSutil.exe).
        vii. Signs of unexpected endpoint-to-endpoint (including servers) communications.
        viii. Potential signs of data being exfiltrated from the network. Common tools for data exfiltration include Rclone,[4] Rsync, various web-based file storage services (also used by threat actors to implant malware/tools on the affected network), and FTP/SFTP.
        ix. Newly created services, unexpected scheduled tasks, unexpectedly installed software, etc.
    b. For cloud environments:
        i. Enable tools to detect and prevent modifications to Identity and Access Management (IAM) network security, and data protection resources.
        ii. Use automation to detect common issues (e.g., disabling features, introduction of new firewall rules) and take automated actions as soon as they occur. For example, if a new firewall rule is created that allows open traffic (0.0.0.0/0), an automated action can be taken to disable or delete this rule and send notifications to the user that created it as well as the security team for awareness. This will help avoid alert fatigue and allow security personnel to focus on critical issues.

[2] "Cobalt Strike," MITRE, last modified October 2022, https://hyperproof.io/nist-cybersecurity-framework-solution/.

[3] "Mimikatz," MITRE, last modified August 2022, https://attack.mitre.org/versions/v12/software/S0002/.

[4] "Rclone," MITRE, last modified September 2022, https://attack.mitre.org/versions/v12/software/S1040/.

AFTER the Attack – Reporting and Notification

Note: Refer to the Contact Information section at the end of this guide for details on how to report and notify about ransomware incidents.

a) Follow notification requirements as outlined in your Cyber Incident Response and Communications Plan to engage internal and external teams and stakeholders with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.
b) Share the information you have at your disposal to receive timely and relevant assistance. Keep management and senior leaders informed via regular updates as the situation develops. Relevant stakeholders may include your IT department, managed security service providers, cyber insurance company, and departmental or elected leaders.
c) Report the incident to, and consider requesting assistance from, the Cybersecurity and Infrastructure Security Agency (CISA), your local FBI field office, the FBI Internet Crime Complaint Center (IC3), or your local U.S. Secret Service field office. Contact information should be included in your Incident Response Plan (see below).
d) As appropriate, coordinate with communications and public information personnel to ensure accurate information is shared internally with your organization and externally with the public.
e) If the incident resulted in a data breach, follow notification requirements as outlined in your cyber incident response and communications plans.

Containment and Eradication

If no initial mitigation actions appear possible:

a) Take a system image and memory capture of a sample of affected devices (e.g., workstations, servers, virtual servers, and cloud servers). Collect any relevant logs as well as samples of any "precursor" malware binaries and associated observables or indicators of compromise (e.g., suspected command and control IP addresses, suspicious registry entries, or other relevant files detected). The contacts below may be able to assist you in performing these tasks.
b) Preserve evidence that is highly volatile in nature—or limited in retention—to prevent loss or tampering (e.g., system memory, Windows Security logs, data in firewall log buffers).
c) Consult federal law enforcement, even if mitigation actions are possible, regarding possible available decryptors, as security researchers may have discovered encryption flaws for some ransomware variants and released decryption or other types of tools.

To continue steps to contain and mitigate the incident:

a) Research trusted guidance (e.g., published by sources such as the U.S. Government, Multi-State Information Sharing and Analysis Center [MS-ISAC], or a reputable security vendor) for the particular ransomware variant and follow any additional recommended steps to identify and contain systems or networks that are confirmed to be impacted.
   - Kill or disable the execution of known ransomware binaries; this will minimize damage and impact to your systems. Delete other known associated registry values and files.

b) Identify the systems and accounts involved in the initial breach. This can include email accounts.

c) Based on the breach or compromise details determined above, contain associated systems that may be used for further or continued unauthorized access. Breaches often involve mass credential exfiltration. Securing networks and other information sources from continued credential-based unauthorized access may include:

   - Disable virtual private networks, remote access servers, single sign-on resources, and cloud-based or other public-facing assets.

d) If server-side data is being encrypted by an infected workstation, follow server-side data encryption quick identification steps.

   - Review Computer Management > Sessions and Open Files lists on associated servers to determine the user or system accessing those files.
   - Review file properties of encrypted files or ransom notes to identify specific users that may be associated with file ownership.
   - Review the TerminalServices-RemoteConnectionManager event log to check for successful Remote Desktop Protocol (RDP) network connections.
   - Review the Windows Security log, SMB event logs, and related logs that may identify significant authentication or access events.
   - Run packet capture software, such as Wireshark, on the impacted server with a filter to identify IP addresses involved in actively writing or renaming files (e.g., smb2.filename contains cryptxxx).

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

   - Outside-in persistence may include authenticated access to external systems via rogue accounts, backdoors on perimeter systems, exploitation of external vulnerabilities, etc.
   - Inside-out persistence may include malware implants on the internal network or a variety of living-off-the-land style modifications (e.g., use of commercial penetration testing tools like Cobalt Strike; use of PsTools suite, including PsExec, to remotely install and control malware and gather information regarding, or perform remote management of, Windows systems; use of PowerShell scripts).
   - Identification may involve deployment of EDR solutions, audits of local and domain accounts, examination of data found in centralized logging systems, or deeper forensic analysis of specific systems once movement within the environment has been mapped out.

f) Rebuild systems based on prioritization of critical services (e.g., health and safety or revenue-generating services), using pre-configured standard images, if possible. Use infrastructure as code templates to rebuild cloud resources.

g) Issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility once the environment has been fully cleaned and rebuilt, including any associated impacted accounts and the removal or remediation of malicious persistence mechanisms. This can include applying patches, upgrading software, and taking other security precautions not previously taken. Update customer-managed encryption keys as needed.

h) The designated OT/IT or OT/IT security authority declares the ransomware incident over based on established criteria, which may include taking the steps above or seeking outside assistance.

Recovery and Post-Incident Activity

a) Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services.
   - Take care not to re-infect clean systems during recovery. For example, if a new Virtual Local Area Network (VLAN) has been created for recovery purposes, ensure only clean systems are added.

b) Document lessons learned from the incident and associated response activities to refine and inform updates to organizational policies, plans, and procedures and guide future exercises of the same.

c) Consider sharing lessons learned and relevant indicators of compromise with CISA or your sector ISAC to benefit others within the community.

Additional Resources

- https://www.cisa.gov/stopransomware/ive-been-hit-ransomware
- https://securityintelligence.com/posts/2022-x-force-threat-intelligence-index-ransomware-resilience-tops-findings/
- https://www.embroker.com/blog/cyber-incident-response-plan/
- https://www.cisa.gov/news-events/news/cisa-fbi-nsa-ms-isac-publish-updated-stopransomware-guide

APPENDIX 1 – CyManII CYBERSECURITY WORK FORCE TRAINING MATERIALS

CyManII Learning Library On-Demand and Live Offerings May 2024

Cybersecurity Basics – CyManII offers the following training that provides basic cyber hygiene to individuals in the workforce. This training is designed to provide awareness around various cybersecurity incidents and areas of vulnerability in any environment.

- CyManII Cybersecurity Awareness
- Cisco Networking Academy – The Cybersecurity Threat Landscape
- Introduction to Incident Response
- Cyber Threat Management
- Cisco Ethical Hacker

Coming Soon to Cybersecurity Basics (June 2024)

- Business Continuity and Disaster Recovery
- Security Fundamentals
- End User Security Awareness
- Hands on Hacking
- Intro to IoT Pentesting
- NIST Cybersecurity and Risk Management Frameworks

OT Cybersecurity Training – CyManII offers training for individuals working in the manufacturing sector that offers training around operational technology, the industrial internet of things (IIoT) and cyber-physical systems. The CyManII OT Cybersecurity training provides basic hygiene as well as conceptual learning applications to non-cybersecurity professionals working in the manufacturing sector.

- Cybersecurity for Implementers – Part 1: Right Start
- Cybersecurity for Implementers – Part 2: Controls
- Industrial Control Systems – Operational Technology
- OT Cybersecurity RAPID Course

Live Offerings – The following courses are live offerings that CyManII conducts virtually and onsite in the small and medium space.

- What is Operational Technology
- The OT/IT Convergence
- OT Cybersecurity and Critical Infrastructure
- OT Defense in Depth Strategy
- Risk Management for OT Systems
- OT Cybersecurity for Additive Manufacturing
- Preparing for CMMC 2.0
- Industrial Control Systems Security 800-82-R3

Coming Soon (Summer 2024) – OT Cybersecurity for Leaders and Managers – In this program, managers and leaders will gain a deep understanding of OT and its impact on business operations. The training covers a wide range of topics, including cybersecurity, process optimization, and strategic decision-making. Participants will learn how to effectively manage OT systems, enhance productivity, and ensure the safety and security of critical infrastructure.

APPENDIX 2 – SECURE BACKUP OF DATA FOR OT SYSTEMS AND MANUFACTURERS

Basic Principles of Secure Data Backup

- Isolate backups either on premise or in the cloud
- Understand where your critical data resides
- Encrypt the backups
- Keep multiple copies of the data (especially the most critical data) at multiple locations.

Best Practices for Secure Backups

1. Identify Critical Data: Identify the most critical data that needs to be backed up, such as configuration data, production-relevant data, and measurement data.
2. Use Secure Storage: Store backups in a secure location, such as a data center or cloud storage service, to prevent unauthorized access.
3. Use Encryption: Use encryption to protect backups from unauthorized access and ensure the confidentiality and integrity of the data.
4. Regular Backups: Perform regular backups at varying intervals to ensure that data is up-to-date and can be restored in case of a disaster.
5. Test Backups: Regularly test backups to ensure that they can be restored successfully, and that data is recoverable.
6. Use a Secure Backup Solution: Use a backup solution that is specifically designed for OT environments and provides features such as data deduplication, compression, and encryption.
7. Monitor and Audit: Monitor and audit backup processes to ensure that they are running correctly, and that data is being backed up securely.

Common Backup Methods

- Cloud Backup: Store backups in a cloud storage service, such as Amazon S3 or Microsoft Azure, to provide secure and scalable storage.
- On-Premises Backup: Store backups on-premises in a data center or server room to provide secure and controlled storage.
- Hybrid Backup: Use a combination of cloud and on-premises backup solutions to provide a hybrid backup strategy.

Additional Resources

- https://www.proarch.com/blog/ot-security-best-practices-getting-backups-right