PONDURANCE

Practical Cybersecurity:

A Road Map for Manufacturers

pondurance.com

INTRODUCTION

Cybercriminals are continuing to target manufacturers of every size and category. Last year, the manufacturing industry experienced the fourth-largest number of cyber incidents, with only the public administration, information, and finance industries experiencing more activity.[1] As much as 96% of cybercriminals who targeted manufacturers were financially motivated, looking for a large cash payout.

Such motivation makes the manufacturing industry an especially attractive target for ransomware attacks because manufacturers often pay the ransom to minimize any disruption to their operations. After all, even a small amount of downtime for a manufacturer can stop the production line and interrupt the supply chain. In addition, many manufacturers work with legacy systems that provide ease of use but can't be properly patched or updated, leaving them vulnerable to an attack.

As a manufacturer, you may know these challenges and recognize that protecting your operation from disruption is a constant endeavor. But with the right people, technology, and policies in place, you're more likely to find and fix vulnerabilities, detect and thwart threats, and avert disaster. Navigating your cyber risks isn't necessarily easy, but you don't have to do it alone. This eBook can help you cut through the clutter, complexity, and confusion.

In the next five chapters, we'll explore the five key components of a sound cybersecurity framework for manufacturers based on the NIST Cybersecurity Framework.[2] And we'll cover industry best practices and solutions like risk management, incident response planning, and managed detection and response (MDR) — tools you can use to build an effective, practical threat management strategy.

Chapter 1: Identify

You can’t protect what you can’t see, so the first step to creating a solid cybersecurity framework in the threat management life cycle is making sure you know where you are most vulnerable. As IT and operational technologies converge, manufacturers have larger attack surfaces than ever before with multiple entry points into their networks — and that can mean multiple vulnerabilities for cybercriminals to exploit.

At the start of your cybersecurity planning, you must know what apps you’re running and on what devices, how your network is structured, what data you’re using and storing, and how your customers, supply chain vendors, and employees are accessing it all. Then, you need to prioritize those assets so you can manage risks accordingly. These base components of creating a cyber risk profile for manufacturers are vital for keeping your network safe from attack.

56%

of manufacturers were hit by a ransomware attack in 2023, compared to 55% in 2022.[3]

PONDURANCE

Chapter 1: Identify

YOUR ROADMAP:

- Create a risk profile. Identify IT assets connected to operations or supply chain systems, your digital assets, including data, devices, cloud and on-premises infrastructure, software, and networks by conducting a comprehensive inventory. Prioritize assets or asset groups based on business value and vulnerability.
- Find the attack surfaces and specific risks in your environment by conducting a comprehensive vulnerability assessment, including penetration testing.
- Determine and document your cybersecurity policies and procedures for operations, backup and recovery/business continuity, risk management, and compliance. These documents should include your cadences for routine threat management activities such as backups, vulnerability scans, updates and patches, and training.
- Set identity access management (IAM) policies across all assets, then remove unauthorized devices, systems, software, and users from the network.
- Develop and test incident response plans that include step-by-step instructions for handling different incidents and types of attacks based on your specific environment.
- Include the supply chain in your assessments and evaluate it based on the risk it poses to your business.

The success of your cybersecurity framework strategy relies on comprehensive testing and planning. The objective expertise of a third-party vendor can be valuable at this stage, especially when it comes to uncovering your blind spots. Consider exploring your options for risk management, internal and external security testing, compliance consulting, and virtual chief information security officer services.

Chapter 2: Protect

Protecting data and infrastructure is an ongoing and multi-threaded effort for manufacturers. Taking a risk-based approach is key to bringing your routine threat management activities to life, as documented in your cybersecurity framework policies and procedures.

Hacking and malware were the top two attack patterns on manufacturers in 2022, with social engineering attacks ranking in a distant third place.[1]

PONDURANCE

Chapter 2: Protect

YOUR ROADMAP:

- Implement IAM controls based on the principles of least privilege and separation of duties. Review these controls quarterly.
- Configure systems, software, and devices for security, implementing built-in safeguards such as firewalls, data encryption, and multifactor authentication. Apply uniform configurations to like devices and disable unnecessary features.
- Equip and monitor every endpoint device with effective and up-to-date antivirus software.
- Create regular secure backups on a frequency consistent with your recovery time and recovery point objectives.
- Update your asset inventory monthly.
- Conduct routine vulnerability scanning, with weekly vulnerability threat feeds, monthly external scanning, quarterly internal scanning, and annual penetration testing.
- Keep systems and software updated and patched based on vulnerability scan results and as directed by vendors.
- Routinely test and update your backup and recovery mechanisms as well as your business continuity plan.
- Provide foundational cybersecurity awareness training to all employees, followed by refresher training and phish testing on an ongoing basis to keep cybersecurity top of mind.

For some manufacturers, these ongoing action items are more than can be managed with in-house resources. And building internal resources can be challenging when budgets are low and cyber talent is hard to find. Despite best efforts, critical activities can fall through the cracks, leaving gaps in your cybersecurity strategy. As a result, manufacturers of all sizes often turn to MDR providers to augment the capabilities and capacity of the security team. Consider outsourcing security testing and controls validation activities such as penetration testing, vulnerability management, and application security testing.

Chapter 3: Detect

Cybercriminals look for easy targets to pay their ransom demands, and many manufacturers fit their criteria. Manufacturers often work on legacy systems that can't be patched or updated, making them vulnerable to cyberattacks. But even manufacturers with the strongest security controls and cybersecurity frameworks can be compromised, and the faster a security incident can be identified and contained, the lower the costs associated with it. That's why detecting incidents as soon as possible is crucial.

Unfortunately, it can take months to detect and contain a breach. On average, it takes 277 days — 204 days to identify a breach and another 73 days to contain it — according to IBM Security's *Cost of a Data Breach Report 2023*. Across all industries, a breach with a life cycle over 200 days costs an average of $4.95 million versus $3.93 million for one with a life cycle of less than 200 days, representing a difference of 23%. The differences in impact are substantial when you can detect and contain a threat in minutes versus hours, days, or even months.[4]

Manufacturers, like other small and midsize businesses, are struggling to detect and respond to threats and vulnerabilities, according to a 2022 Forrester study. Eighty-nine percent of businesses reported a significant lack or some lack of resources to detect and respond to endpoint-based and network-based threats. This lack of resources keeps businesses reactive rather than proactive in their cybersecurity defense efforts.[5]

Chapter 3: Detect

YOUR ROADMAP:

- Maintain full visibility into data, devices, logs, cloud-based and on-premises systems infrastructure, software, and networks.
- Implement 24/7 monitoring for threats and incidents across all environments.
- Know how data normally flows through your organization. Deploying a network sensor can help, alerting you when data is suddenly flowing in an unexpected direction or path — a strong indicator that something could be amiss.
- Maintain and monitor logs that record events such as IAM activity, changes to systems or accounts, and the initiation of communication channels.
- Deploy security tools such as SIEM that can aggregate these logs and look for deviations from expected network behavior.
- Consider implementing other security tools such as endpoint detection and response, file integrity monitoring, and intrusion detection system.
- Consider implementing next-generation firewalls, which can provide in-depth information such as deep packet inspection and intrusion prevention capabilities.
- Separate real incidents from the noise of alerts so you can prioritize anomalies for investigation. Fine-tuning your SIEM can help reduce false positives, resulting in a more manageable volume of alerts to investigate.
- Test and tune your detection mechanisms on a regular basis.

If you're like most manufacturers, you either lack the security expertise and budget to implement 24/7 monitoring and detection or lack the tools to monitor and detect malicious activity across your network, endpoints, logs, and cloud. As an affordable and highly effective alternative, you should consider leveraging an MDR services provider.

MDR services are ideal for manufacturers that are bogged down with false positives and suffering from "alert fatigue." Acting as a business's security operations center (SOC), MDR providers can use context and historical timelines to identify the threats that truly require the attention of security resources.

Chapter 4: Respond

When a cyberattack happens, it's critical to have an incident response plan in place that can immediately guide you through each stage of response. During an incident is not the time for determining your policy on paying a ransom or identifying your key stakeholders. That's what your incident response plan is for.

Your incident response plan is not a one-and-done exercise. It's a living document that must be tested and updated regularly. All individuals must understand their roles and responsibilities in order for your business to respond effectively. It's also not a one-size-fits-all document. Your planned response to ransomware will be different from your response to a data breach, which will be different from your response to a lost or stolen device. Your incident response plan should include different playbooks to reflect different potential risks and scenarios.

It should also reflect different potential threat vectors. Malicious cyberattacks occur through a wide range of threat vectors. System intrusion, social engineering, and basic web application attacks represent 83% of attacks in the manufacturing industry, according to the Verizon report. The motivation for 96% of these attacks is financial gain.[1]

Finally, your incident response plan should be designed to close the loop on incidents. Manufacturers that are able to conduct investigations to identify root causes of attacks and mitigate those threats are best equipped to avoid them in the future.

> "It is critical to have an incident response plan in place that can guide your business through each stage of response."

PONDURANCE

Chapter 4: Respond

YOUR ROADMAP:

- Review the security event to confirm it's not a false positive and then work quickly to triage the incident to investigate the type and source of the attack and assess the potential scope of the impact.
- Stop the incident immediately to reduce the impact on manufacturing operations. Contain the threat by isolating or shutting down the affected systems, networks, servers, databases, and devices to prevent further spread to your network.
- Preserve evidence and collect critical information while it's still available. Gather logs, memory dumps, audits, network traffic reports, and disk images — any evidence that can be used to analyze the origin, impact, and intention behind the attack.
- Eradicate the threat and prevent future occurrence. Patch the entry point to ensure the attacker cannot regain access.
- Determine if any sensitive information was breached or data loss occurred.
- Initiate communications with internal and external stakeholders, as outlined in your incident response plan. Work with your communications team on the content and timing of public statements.
- Engage with your legal team and examine any compliance or regulatory risks to determine potential violations. Contact law enforcement and any other required government agencies.
- Perform a root cause analysis to determine the attacker's steps to gain access to your systems and update protection and detection mechanisms accordingly.
- Perform a vulnerability analysis throughout your manufacturing systems to ensure all vulnerabilities have been addressed.
- Keep a log of all incident response activities and results of investigations.

Chapter 4: Respond

It often makes sense for a manufacturer to seek outside expertise at this point to minimize the damage of an attack. Having 24/7 access to SOC and incident response capabilities can dramatically shorten your mitigation and recovery time. Ideally, you've engaged an MDR provider that can move seamlessly into incident response when the time comes.

"A key value proposition of MDR is performing most of the incident response process," according to Gartner's Market Guide for Managed Detection and Response Services. "Timely and accurate incident response takes time and skill, which many organizations just don't have, especially when multiple threats need to be addressed simultaneously."[6]

PONDURANCE

Chapter 5: Recover

“The goal of recovery is to move from the immediate aftermath of an incident to full restoration of normal systems and operations,” reports the National Cybersecurity Alliance.[7] Like all the other components of the threat management strategy, it requires thoughtful planning to fully restore normal systems and operations. Recovery often begins immediately on the heels of — or overlaps with — incident response.

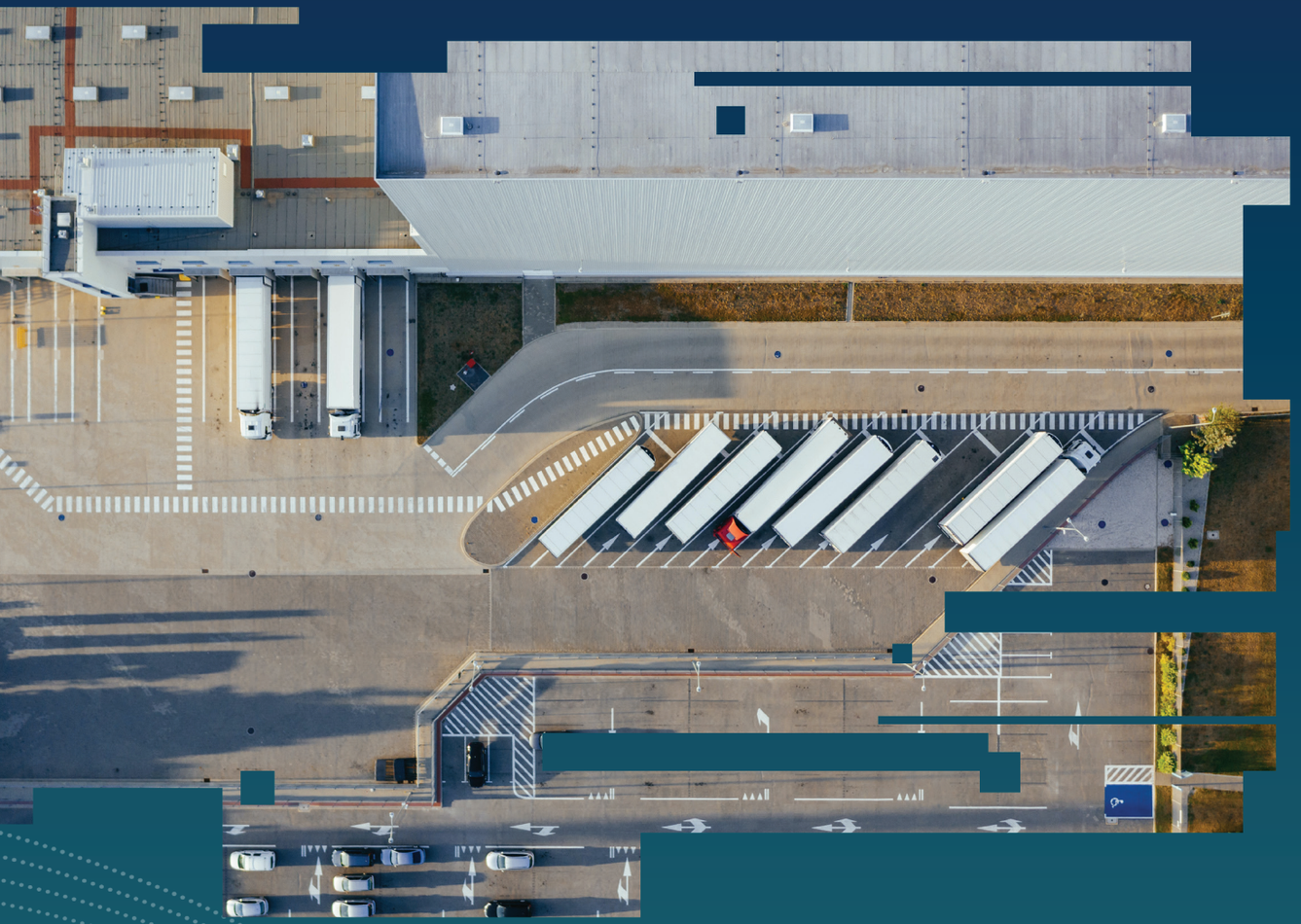
PONDURANCE

Chapter 5: Recover

YOUR ROADMAP:

- Confirm that all the necessary forensic evidence has been collected.
- Fully restore normal systems and operations. Repair, restore, or replace affected components, whether that means restoring system images, restoring data from backups, or replacing potentially compromised controls such as passwords or encryption keys.
- Leverage evidence and other critical information collected during the incident for post-incident analysis and reporting. Discuss the effectiveness of the incident response plan and make adjustments accordingly.
- Capture lessons learned that would reduce the risk of a future incident, minimize the severity of a future incident, or improve incident response time. Incorporate these improvements into your policies and procedures for operations, backup and recovery/business continuity, risk management, and compliance. Update employee training and the incident response plan accordingly. Communicate these updates to all stakeholders.

Following a cyberattack, many manufacturers experience production line downtime and supply chain interruptions, impacting service level agreements and causing repercussions for customers down the line. But you can make strategic moves to minimize the risk of disruption. Take this opportunity to put renewed emphasis on security across your business and take the necessary steps to improve your cybersecurity framework.



Learn more

Developing and implementing a practical threat management strategy is not optional for today's manufacturers. Cybercriminals are creative, opportunistic, and motivated individuals — and even businesses and nation-states. They have access to the latest tools, and they are constantly looking for available targets. Your best defense is a strong cybersecurity framework that includes 24/7 security operations.

To learn more about MDR, watch our on-demand webinar *Demystifying MDR for Security Conscious Buyers* or download our MDR info sheet.

To talk to an MDR expert or see a demo, contact us.

PONDURANCE

PONDURANCE

500 N. MERIDIAN ST., STE 500
INDIANAPOLIS, IN 46204

About Pondurance

Pondurance delivers world-class managed detection and response services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements and digital transformation accelerated by a distributed workforce.

By combining our advanced platform with our experienced team of analysts we continuously hunt, investigate, validate and contain threats so your own team can focus on what matters most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals and compliance and security strategists who provide always-on services to customers seeking broader visibility, faster response and containment, and more unified risk management for their organizations.

Visit **www.pondurance.com** for more information.

Sources:

1. "2023 Data Breach Investigations Report," *Verizon*, 2023.
2. NIST Cybersecurity Framework.
3. "The State of Ransomware in Manufacturing and Production 2023," *Sophos*, 2023.
4. "Cost of a Data Breach Report 2023," *IBM Security*, 2023.
5. "Attackers Don't Sleep, But Your Employees Need To," *Forrester*, July 2022.
6. Bussa, Toby, et al., "Market Guide for Managed Detection and Response Services," *Gartner*, Aug. 26, 2020.
7. "Cybersecure My Business," *National Cybersecurity Alliance*.