Information Security Best Practices for Manufacturers in the Era of the Hacker

by Michael Ochi

Director of Product Marketing, QAD

A QAD Leadership White Paper for the Global Manufacturing Industry

CONTENTS

INFORMATION SECURITY BEST PRACTICES FOR MANUFACTURERS IN THE ERA OF THE HACKER

INTRODUCTION: INFO SECURITY MORE IMPORTANT THAN EVER

Hackers and information security professionals play ongoing and dangerous games of cat and mouse. Businesses, consumers and not-for-profit organizations, caught in the middle, hope that the information security professionals will keep the hackers at bay. Unfortunately, no matter how many layers of defense security professionals put into erecting controls and processes, hackers eventually break through – sometimes with devastating results.

Information security professionals attempt to minimize breaches and to spot and remediate breaches as effectively as possible to limit damage. Though security goals have remained the same, the pervasiveness of the generative artificial intelligence (genAI), internet, social media, IoT, mobile computing, and the ever-evolving hacker culture has considerably increased the risk and cost of information security.

No industry sector, even the public sector, escapes unharmed. Attacks reach non-manufacturing and manufacturing organizations alike, though research has shown that manufacturing was hit hardest for the fourth consecutive year (2021-2024)[1]. Some of the major non-manufacturing hacks in 2024 include:

- Change Healthcare's parent company paid $22M in ransom after an attack delayed prescriptions and healthcare services across the United States[2]
- Information stolen from Snowflake, a major data warehousing platform, was linked to downstream breaches at Ticketmaster, Santander, and AT&T. [2]
- The Port of Seattle, including SEA international airport, faced a week of significant travel disruptions due to IT outages downstream of a ransomware attack [3]

A short list of attacks in manufacturing and the supply chain include:

- Microchip Technology suffered an attack that decreased semiconductor production and order fulfillment, leading to $21.4M in expenses [4]
- Applied Materials lost up to $250M in sales following a supply chain ransomware attack[5]
- The Port of Nagoya, Japan's largest, was unable to load and unload containers for two days which impacted major companies including Toyota[6]

How should manufacturers deal with the rising risk and cost of information security? Some vigilant manufacturers have invested heavily in augmenting their information security expertise, practices and tools. Some manufacturers are in denial to the point where they may have been hacked without knowing it. Most manufacturers are in-between, trying to prevent breaches without inflating information security budgets. For those manufacturers in the latter two categories, it makes sense to step back and ensure you are thinking realistically about today's information security challenges.

INFORMATION SECURITY BEST PRACTICES FOR MANUFACTURERS IN THE ERA OF THE HACKER

RETHINKING INFORMATION SECURITY IN MANUFACTURING

Think Digital

Many manufacturing executives believe that key applications like ERP, particularly on-premise, are safe. Perhaps they feel safe because they have not yet been hacked, at least to their knowledge. Perhaps they erroneously associate physical control of on-premise data centers with safety.

In a fast-paced world that increasingly relies on having constant on-the-go access to business systems, manufacturers often rely on VPNs and remote access software. Yet the April 2025 Threat Intelligence report from IBM found that external remote services were related to 21% of manufacturing cyber breaches.

Once attackers gained access, 29% of incidents led to extortion, and data theft accounted for another 24%. These breaches demolish customer trust, and companies often spend millions identifying how much data was stolen and remediating the damage. 18% of attacks involved credential harvesting, which enabled attackers to have continued access through the “front door”.

Generative AI is enabling threat actors to write everything from more convincing phishing emails to official-looking websites and malicious code. Who can keep up with the current and evolving set of sophisticated digital attack techniques in terms of expertise and cost? We have seen that manufacturers struggle to do so. Manufacturing executives should concentrate on addressing the breadth, cost and evolving digital nature of information security threats as a top business priority and a central Governance component of their ESG programs.

The Rising Cost of Information Security

Most manufacturers find it difficult to keep up with the expertise required to play the cat-and-mouse game of cybersecurity. The U.S. Bureau of Labor Statistics forecasts a 33% increase in security analyst jobs through 2033[7]. Though manufacturers are targeted at the highest rate, these skills are highly demanded in industries that are more attractive and lucrative for new college graduates, such as finance and professional services. Global manufacturers pay dearly for in-house security expertise. In addition, the price of related software and tools to prevent, detect and mitigate the breaches is often prohibitive to manufacturers who prefer the do-it-yourself approach.

Staying in-house and lacking the willingness to make the needed investment in security expertise and tools put entire businesses at risk. How do breaches hurt manufacturers?

- In the worst-case scenario, manufacturing operations are halted. The cost of a manufacturing plant shutdown varies by manufacturer type but is estimated to average $260,000 per hour[8]
- The global average cost of a data breach is $4.88M, and rising year over year.[9]

INFORMATION SECURITY BEST PRACTICES FOR MANUFACTURERS IN THE ERA OF THE HACKER

Cloud – A Safe Haven for Manufacturers?

For the first decade of the "Cloud" and "Software as-a-Service," (SaaS) an inhibitor to adoption was security. Organizations were afraid of losing control over their information security and were afraid that Cloud providers added risk to the information security equation.

Cloud service providers and SaaS have now demonstrated more than a decade of mature solutions. Cloud providers, aware of buyers' security concerns, have invested heavily in security tools, processes and practices. In addition, Cloud providers are in the business of serving many clients – a compromised Cloud can infect many or all customers. Therefore, security is central to the success or failure of a Cloud provider. Cloud providers, arguably, are the most motivated of businesses to try to keep a step ahead of hackers and, if they fall a step behind, are motivated to have the means to minimize impact.

Given the ever-evolving sophistication of hackers, security-conscious Cloud providers now offer a far safer environment at a lower cost than on-premise. Cloud providers with a deep commitment to security have the scale to make investing in security expertise, programs, processes and tools pay off for all concerned.

Managed service providers, often dealing with less scale than cloud providers, and lacking application security knowledge, may offer little to no security improvements over in-house on-premise. Similarly, many manufacturers lack the means and resources to ensure excellent information security and to constantly improve the security to meet the evolving threat environment.

INFORMATION SECURITY BEST PRACTICES AND TOOLS

What do manufacturers need to do to keep attackers at bay? While there are many important info security techniques for on-premise and Cloud hosted solutions, there are three key security methods for manufacturers: (1) Fast and fastidious patching, (2) ongoing penetration testing and threat detection, and (3) immediate incident response. In more detail:

- Responsible patching is essential. Red Hat published a dozen critical severity patches for their RHEL product in 2024 alone[10] No matter how fast Red Hat issues patches, there may be a gap exposing systems to zero-day attacks. The average observed breakout time - the duration between initial attack and gaining access to another host within the environment - was 48 minutes in 2024, down from 62 minutes in 2023 and 84 minutes in 2022[11]. It is incumbent on the manufacturer or the manufacturer's cloud provider to apply patches on a timely basis to reduce the likelihood of breach.
- Even with diligence, manufacturers should assume that sooner or later there will be a breach, which is why penetration testing and incident response are essential. The sooner a breach is detected and contained the lower the costs and impact on customers and brand.[9]

Most manufacturers consider ERP, factory floor and supply chain solutions mission-critical. What are the best information security practices for the increasing number of manufacturers using solutions like cloud ERP? When considering information security for critical business systems, companies should look for the following from a vendor:

- A dedicated, full-time intrusion detection program that is tested regularly.
- A dedicated incident response team with related processes for customer communication that tie into backup, recovery and disaster recovery processes.
- Centralized, attentive patching regardless of instance location, for all solution elements (OS, database, app servers/platforms, integration software, ERP and supply chain software, related application software). That implies a global "follow the clock" systems management approach.
- A cloud/application practice that maintains all appropriate security certifications and that will share test results and provide a schedule of ongoing compliance. Commitment to certification formalizes the commitment to information security.
- Cloud services that do not "lock in" customers. That means the security and management layer should meet industry-specific compliance such as "qualified infrastructure" requirements in life sciences.
- A cloud services team that will work with the manufacturer's security professionals to ensure that the manufacturer's self-directed policies and compliance requirements are understood and met.

This is only a partial list. What manufacturers need to address in the digitally-oriented world of information security right now is a considerable challenge. The tidal wave of generative AI and global trade volatility will continue to raise the stakes on information security in manufacturing.

SUMMARY: THE RIGHT CLOUD IS THE FAST PATH TO INFORMATION SECURITY

It is ironic that security, once a key reason for companies to avoid Cloud, is now an excellent reason to move to Cloud. Security is one of the key reasons why companies are increasingly more interested in deploying cloud business systems than on-premise.

Regardless, every manufacturer should consider how best to secure information and prevent and remediate breaches – the business depends on it. Given high security costs, more value chain collaboration and changing application integration needs, manufacturers that deal with security entirely in-house face a difficult road ahead.

Cloud ERP and supply chain solutions can help reduce the tension between security-related risk and cost. Not all cloud solutions, however, are created equally in terms of security. It is incumbent on manufacturers to openly look at cloud ERP and supply chain solutions as a way toward better security but to do so responsibly – to ensure the Cloud or clouds they choose can meet the commitment and criteria required to keep up with or perhaps even ahead of the hackers.

Your Strategic Assessment: To find out how you can obtain an assessment that clarifies where you stand today on cloud security, contact a client advisor at QAD. With nearly two decades of running customers' production systems in the Cloud, QAD Adaptive Applications have an excellent track record of availability, performance, security and rapid, successful implementations.

SOURCES

[1] IBM X-Force Threat Intelligence Index 2025

[2] Top 10 Cyber-Attacks of 2024, InfoSecurity Magazine

[3] Port Cyberattack Archive, Port of Seattle

[4] Microchip Technology Reports $21.4 Million Cost From Ransomware Attack, SecurityWeek

[5] Top 10 Manufacturing Industry Cyber Attacks, Arctic Wolf

[6] Japan's Nagoya port resumes operations after ransomware attack, CSO Online

[7] Occupational Outlook Handbook - Information Security Analysts, U.S. Bureau of Labor Statistics

[8] Average Cost of Downtime per Industry, Pingdom

[9] Cost of a Data Breach Report 2024, IBM

[10] Red Hat Security Advisories, Red Hat Customer Portal

[11] CrowdStrike 2025 Global Threat Report

QAD

Tel: + 1 805 566 6100
www.qad.com