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

by Rob Janssens

Senior Manager of Process and Compliance, 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 keep the hackers at bay. Unfortunately, no matter how much brainpower and resources information security professionals put into erecting defenses and evading attacks, hackers eventually break through – sometimes with devastating results.

Basically, information security professionals attempt to minimize breaches and to spot and remediate breaches as effectively as possible to limit damage. Though security goals have not changed, the pervasiveness of the internet, social media, IoT, mobile computing and the ever-evolving hacker culture has increased the risk and cost of information security considerably. Skeptical? Consider what has happened in 2017.

2017 could go down as the year with the most high impact cyberattacks in history and may only hold that distinction until 2018. No industry sector, even the public sector, escaped unharmed. Attacks reached non-manufacturing and manufacturing organizations alike. Some of the major non-manufacturing hacks in 2017 include:

- Verizon had 14+ million customer records compromised.[1]
- Sabre, the giant reservations company, suffered an extensive breach that reached airlines, hotels chains and even Google.[1]
- A breach of the big 3 credit agencies, Equifax, exposed 145.5 million peoples' data.[2]
- Deloitte, one of the world's largest accounting and consulting firms, was hit by an attack that compromised customer data which ironically undercut the credibility of its cyber-security consulting business.[3]

A short list of attacks in manufacturing and the supply chain in 2017 include:

- The worldwide WannaCry ransomware attack caused Honda, Nissan and Renault to temporarily halt production.[4]
- WannaCry also forced electronics leader LG to close its service center until systems were patched.[5]
- A similar ransomware attack, nicknamed Petya, was responsible for a roughly 200 to 300 million-dollar negative impact on earnings to Maersk, the Danish-based container shipping and logistics leader.[6]
- A cyberworm called NotPetya infiltrated manufacturers later in 2017 and was cited as a key reason for the weakened earnings at pharma leader Merck and the world's second largest confectionary Mondelez Interational.[7]

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.

RETHINKING INFORMATION SECURITY IN MANUFACTURING

Think Digital More than Physical

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.

Unfortunately, the modern techniques of hackers are decidedly digital; seldom physical. Digital examples include hijacked web sessions, unsecure mobile hotspots, email and link phishing, insecure mobile apps and data, malware and hacking social media. In a recent IBM study on manufacturing security, physical breaches were in the distinct minority of attacks on manufacturers.[8] Some still argue that physical security should not be overlooked, but even those advocating physical security suggest that only 18% of attacks, maximum, are physical in nature.[9]

The most prolific cyberattack technique used to infiltrate manufacturers' data is known as SQL Injection, where databases and operating systems are compromised through the injection of spurious code. Nonetheless, there is a long list of cybersecurity breach techniques used against manufacturers.[9] Manufacturers should expect that more attack techniques will be developed – hackers, culturally, try to out-innovate one-another in twisted game of one-upmanship.

Who can keep up with the current and evolving set of sophisticated digital attack techniques in terms of expertise and cost? We will see that manufacturers struggle to do so, but it is interesting that many small and medium hosting and managed service providers still boast about their physical security. Instead, manufacturing executives should concentrate on addressing the breadth, cost and evolving digital nature of information security threats, by themselves or in partnership with qualified cloud providers.

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. ISACA, a security industry group, "predicts there will be a global shortage of two million cyber security professionals by 2019 and every year in the U.S., 40,000 jobs for information security analysts go unfilled.[10] 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 as an example, "Shutting down an auto assembly line costs the plant $1,250,000 or more per hour."[11]
- The average cost to remediate stolen or compromised data is $141 per record.[12] That means the predicted cost to remediate 100,000 compromised records is approximately $14 million.

Cloud a Safe Haven for Manufacturers?

For the first decade of the "Cloud," or "Software-as-a-Service," (SaaS) which is a common term for applications running in the Cloud, 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.

The cloud, or SaaS, is now nearly two decades old. Cloud providers have had a long period to improve their security tools, practices and processes. Cloud providers, aware of buyers' security concerns, have invested heavily in security. 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 evolve threat environment.

INFORMATION SECURITY BEST PRACTICES AND TOOLS

What do manufacturers need to do to keep attackers at bay? Whether on-premise, in the cloud, or a combination thereof, while there are many important info security techniques, 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. In the first 9 months of 2017, Microsoft alone issued over 900 security updates for server and operating system software.[13] No matter how fast Microsoft issues patches, there may be a gap exposing systems to zero-day attacks. 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.[12]

Most manufacturers consider ERP 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, companies should look for the following from a cloud ERP 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 software, related application software). That implies a global "follow the clock" systems management approach.

- A cloud security and management team that is **deeply familiar and dedicated to ERP**; ERP hosted via managed services of small third party cloud typically offer inferior security because the cloud team and the ERP team are not well integrated and unfamiliar with each-others' best security and management practices.
- 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 be able to span public cloud providers** like IBM Cloud, Amazon Web Services and others, and 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. Trends like the Internet-of-Things (IoT), new forms of value chain information sharing like blockchain and cloud-based supplier relationship management 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 Aberdeen found that in 2016, for the first time, more companies were interested in deploying cloud ERP than on-premise ERP.

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 diffcult road ahead.

Cloud ERP can help reduce the tension between security related risk and cost. Not all cloud ERP solutions, however, are created equal in terms of security. It is incumbent on manufacturers to openly look at cloud ERP as a way towards 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 a full decade live in production, QAD Cloud ERP has an excellent track record of availability, performance, security and rapid, successful implementations.

SOURCES

[1] 2017's biggest hacks, leaks, and data breaches — so far, ZDNet, September 20, 2017

[2] Equifax data breach affected millions more than first thought, CBS MoneyWatch, October 2, 2017

[3]After hack, security researchers probe Deloitte's security posture, by Zeljka Zorz, HELPNETSECURITY, September 27, 2017

[4]Honda Halts Car Production After WannaCry Infection, by Maritza Santillan, Tripwire: The State of Security, June 21, 2017

[5]LG Shut down due to Wannacry attack on its systems, by Ayobamidele Francis Mo bee, Digital Space Radio, August 23, 2017

[6]Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk by Danny Palmer, ZDNet, August 16, 2017

[7]Cyber 'Worm' Attack Hits Global Corporate Earnings, Reuters, August 2, 2017

[8]Security trends in the manufacturing industry: Intellectual property and operating information are the crown jewels, IBM X-Force® Research, 2017

[9]Countering the Threat of Physical Security Breaches, by Simon Williamson, The Data Center Journal, January 30, 2017

[10]The Fast-Growing Job With A Huge Skills Gap: Cyber Security, by Jeff Kauflin, Forbes, March 16, 2017

[11]Severe Weather and Manufacturing in America, Business Forward Foundation, 2014

[12]2017 Cost of Data Breach Study, Ponemon Institute, June 2017

[13]Microsoft Security Updates first 9 months of 2017 for server software (e.g. SQL Server, BizTalk Server, etc.) and OSes = 985. Source: Microsoft Security Tech Center – Security Update Guide search, January 1, 2017 through September 30, 2017.

QAD Inc.
100 Innovation Place
Santa Barbara, CA
93108 USA
Tel: + 1 805 566 6100
www.qad.com