DIGITAL IMMUNITY™
STAY PRODUCTIVE, STAY SECURE

To Patch or Not to Patch: That is NOT the Question!

3 Avoidable Costs of Patching – Or NOT Patching – In Manufacturing OT

Introduction: The Threat is Real

Cyber-security, easily the biggest threat to business today, has typically been thought of as a corporate Information Technology (IT) problem. Most businesses include cyber security as part of their ongoing business strategy. There are, however, significant security threats to Operational Technology (OT) that can have serious and wide-ranging impact beyond just the financial losses incurred. The motivations of cyber-attacks range from financial gains to espionage to the malicious disruption and destruction of production lines and property.

As a result of Industrial Internet of Things (IIoT) and Industry 4.0, OT systems are becoming increasingly integrated with IT systems and networks, as well as being directly connected to the Internet. As companies converge their IT and OT assets to improve information integration in support of a digital transformation, the attack surface increases. OT assets are exposed to IT assets and vice versa, creating new opportunities for attackers. As a result, manufacturing is one of the most aggressively targeted industries for cyber-attacks, according to EEF's 2018 Cyber Security for Manufacturing report. According to EEF, 48% of manufacturers have suffered cyber-attacks, half of whom sustained financial or other business losses.

"Manufacturing losses due to attacks in 2016 reached over $3 billion dollars."

As the threat has increased, so have the costs of successful attacks. The National Center for Manufacturing Sciences (NCMS) estimates that manufacturing breaches cost between $1M and $10M per incident. According to the Alliance for Manufacturing Foresight, losses due to attacks in 2016 reached over $3 billion dollars. In 2017, the pharmaceutical manufacturer Merck "experienced a $1.75 billion silent cyber loss and a $250 million affirmative loss as well from Petya related impacts, according to Property Claim Services (PCS) estimates" (Reinsurance News, November 7, 2018). According to Property Claim Services (PCS) the total industry loss from the Petya / NotPetya cyber-attack has now passed $3 billion.

The number of vulnerabilities, according to a report from Risk Based Security, continues to climb. Between January 1 and June 30 of 2018, 10,644 vulnerabilities were published, compared to 9,690 during the same period in 2017, which was already a 31% increase over

2016. 17% of those vulnerabilities in 2018 – 1809 vulnerabilities, or 5 per day – were considered critical with a severity rating between 9.0 and 10.0 on the CVSS rating scale.

Keeping up with vulnerability patching in the IT world is next to impossible. In the OT world, the task is exponentially more difficult, and comes with a high price tag. OT leadership engineers do not like to patch as it impacts production uptime and revenues. But not patching can be just as costly. In this paper we'll look at the costs of patching – or not – in OT and how those costs can be avoided.

#1: The Cost of Emergency Patching

In the corporate space, patching takes place on an ongoing basis. In the OT world, normal patching typically takes place in a 6 month, or longer, window, during normal plant shutdowns. In some cases patches are only applied annually. Emergency patching, however, is a different story. Once a patch is considered critical, a manufacturing CISO may mandate a 3-day window in which all systems must be patched. This kicks off a resource intensive process:

- A ticket is opened in the IT project tracking system
- The OT system owner is identified and contacted
- The IT project owner and the OT system owner have scheduling meetings
- An agreeable time is scheduled. IT resources prepare the update package
- The update process requires two people and takes 30 minutes per device to complete
- Rollback situations due to bad updates take additional time to complete, increasing downtime
- 1-2 reboots are required per update

Clearly this becomes a very resource intensive process. And that's just one server. Multiply that by the number of endpoints per production line and the number of plants and you will begin to get an idea of the overwhelming resource cost for emergency patching in OT. In one customer instance, an emergency patch took 10 people over 18 hours to complete. The opportune time for many companies to apply patches is on weekends and holidays so

as not to impact critical production requirements, requiring overtime, weekend and holiday pay rates. The resource cost can be substantial!

The downtime cost can be even greater. For one manufacturing customer who generates $10B a year in production revenues, the cost of unplanned downtime is more than $20,000 per minute. The frequency of emergency patching has also increased. Where these situations previously occurred two or three times a year, manufacturers are now faced with addressing emergency patching situations more than once per month.

The cost of emergency patching can take a significant toll on revenues and profits and morale. Unfortunately, traditional solutions in today's market simply do not address this requirement; and in many cases, updates required to the solution itself can exacerbate the problem and the cost.

You need to avoid these costs by eliminating emergency patching and the costs incurred. There is a better way!

#2: The Costs of Bad Patching in OT

In early 2018, the mobile services company Branch, a customer of Amazon Web Services, applied patches to the Spectre and Meltdown vulnerabilities, a flaw that affects nearly every computer chip manufactured in the last 20 years. If exploited, hackers can gain access to data, which has been cached in an effort to speed up memory access. This flaw is so pervasive that it was considered catastrophic (CSO Magazine, January 2018). For Branch, however, the patch proved more damaging than the flaw. Having applied the patch, Branch engineers noticed slowdowns and errors in their cloud servers, including a round of unexpected server reboots. AWS spent multiple days with numerous engineers attempting to analyze and find the root cause. They reworked their architecture and applied more server capacity to compensate. Then they remembered the patch they had applied, and it suddenly made sense. In this case, the fix to the vulnerability caused significant degradation of performance as some of the data fast tracks were pulled back.

In the OT world, the results of installing a bad patch can be significantly costlier. Emergency patching, even planned patching, as described above, consumes many resources to plan

and implement. And the cost of unplanned downtime can be substantial. But what happens when that patch causes havoc on the system? Downtime doubles, further impacting revenues. Resource costs go up as the rollback process increases the implementation time.

OT systems, which are required 24/7, are often well behind the technology curve, both in hardware specifications and in operating system versioning. In most cases, an impact to system resources can render the system inoperable, taking down a production line. According to Aberdeen Research, the average cost per hour of downtime is $260,000. Should a plant be impacted like Branch was, the slow downs, errors and reboots would wreak havoc on production and revenues. One customer told us that they incurred 14 hours of downtime on a line due to the deployment of a single bad patch, at a cost of almost $5000 per minute

Because these systems are critical to production, they are often not patched, which increases the window of vulnerability and the risk.

> **"NotPetya ransomware forced Maersk to reinstall 4,000 servers and 4,500 workstations, resulting in loss of millions of dollars."**

Numerous manufacturing companies experienced issues when patching the Meltdown-Spectre vulnerabilities. Many other companies were warned off as a result of the stability issues. In the case of NotPetya ransomware, which forced Maersk to reinstall 4,000 servers and 4,500 workstations and resulted in the loss of millions of dollars, many companies were spared only because they were late in installing an upgrade to their Ukraine-based accounting software.

You need a way to avoid being impacted by bad patching! There is a better way!

#3: The Cost of NOT Patching in OT

Patching, in manufacturing OT environments, is a losing battle. With the rise in the number of connected devices and the amount of vulnerabilities, the "patching gap" continues to widen. Many of the well-known breaches, like that of Equifax in 2017, could have been prevented if available patches had been applied. Availability – uptime – is the key focus in

OT as downtime, planned or unplanned, can be costly. This often leads to a much more hands-off approach to patching and software updates, which only increases the window of vulnerability and risk of compromise by a cyber attacker. And compromise can come at substantial cost.

Two of the biggest threats to manufacturing companies today are espionage and extortion. According to NCMS (cited above), over 90% of malware aimed at manufacturing has the primary goal of espionage – the theft of intellectual property, trade secrets, etc. 21% of manufacturers have lost intellectual property directly resulting from cyber-attacks and more than 90% of data stolen is considered secret or proprietary. Data stolen can be sold to competitors in the market place, giving them an unfair advantage in both technology acquisition and deal negotiations. Data is often held for ransom, used to extort a company to keep data from being publicly released. The cost of cyber-espionage from China alone, according to a report from the Foundation for Defense of Democracies and reported by the Alliance for American Manufacturing, is approximately $300 billion annually. According to the author, Zach Cooper, "Chinese espionage has not only damaged U.S. companies, but has also helped China save on research and development expenses while catching up in several critical industries. Perhaps most worryingly, China is reversing many of the U.S. military's technical and industrial advantages and creating potential vulnerabilities should a conflict arise."

"TSMC, a Taiwanese chip maker, lost more than $250M as a result of ransomware."

The cost of not patching is also clearly seen in the disruption to production. Systems compromised by cyber attackers can impact both the integrity and the availability of production lines, resulting in substantial costs. We've already mentioned the substantial production loss suffered by Merck due to ransomware. In similar fashion, Honda was forced to halt production in one of its plants resulting in the loss of millions of dollars. One year later, TSMC, a Taiwanese chip maker, lost more than $250M, a third of its quarterly revenue, when the same ransomware impacted Windows 7 machines, knocking out production for days.

Manufacturing OT systems, left unpatched and unprotected, pose substantial risk to production and the company. Because OT systems now have so many different external connections, so many different types of platforms and systems that vary from legacy to

new, it can be very difficult to deliver the protection that is needed to ensure uptime and revenue. As a result, cyber criminals know that manufacturing companies are replete with easily exploitable systems full of vulnerabilities that make them a ripe target.

Patching – and NOT patching – can be very costly. ***There has to be a better way!***

Protecting OT systems from cyber-attacks is quite a dilemma. And there are substantial costs at stake. One manufacturing company decided to put firewalls in front of each critical OT system to protect against attacks. They deployed more than 1,500 firewalls at a cost of $1,800 per firewall. And that was just the beginning of the cost. Resource costs to implement, as well as ongoing maintenance and management, of the firewalls far exceeded the cost of the hardware.

What if you no longer had to worry about emergency patching for new vulnerabilities? What if you could roll out patches during the planned plant shutdown, giving you time to test patches and ensure bad patches won't affect production? And what if you could ensure that malicious code, known or unknown, file or file-less, could not run on your critical production systems, preventing espionage and disruption?

Now you can stop emergency patching, stop the execution of malware on critical OT system, and avoid the costs associated with patching – and NOT patching!

There is a Better Way: Digital Immunity PROTECT™

Digital Immunity's patented approach to protecting Windows-based systems provides OT teams with an option that, before now, was not available: the full-scale immunization of an endpoint that will stop the execution of file-based and file-less attacks. In addition, and perhaps equally important, Digital Immunity has architected the solution to use nominal resources on OT endpoints. This is critical to maintaining the performance objectives of a production operation.

Digital Immunity PROTECT™ is different because Zero Days and known vulnerabilities will be rendered ineffective in taking control of the Windows server or workstation, including devices such as HMI, MES, Data Historian, SCADA and other servers. This is accomplished by what we call Digital DNA Mapping. DI PROTECT™ will map the operation

of an OS and related Applications verifying the integrity in memory. This is far superior to whitelisting approaches employed by other vendors such as file identification and hashing. DI PROTECT™ maps at a deeper level, hardening the OS and the application, and thus recognizes and prevents an attempted deviation to the normal state and blocks this action while allowing the approved process to continue.

This is the Digital Immunity difference: full protection regardless of security patch level, and an endpoint sensor that is so light your systems can continue to perform at a high-level. The ability to be protected between patch cycles is invaluable. You no longer have to worry about the 'emergency' patch cycle, and you can run systems securely and patch in your own timeline, during scheduled downtime.

Now you can implement robust threat prevention that:

- Has a lightweight Sensor that runs in the kernel and requires less than 1% CPU utilization on critical systems without the need for system rebooting or downtime,
- Protects against file, file-less, known and unknown threats in memory, at run-time when applications are most vulnerable without pre-existing threat or vulnerability knowledge,
- Requires no signature updates, behavioral/AI algorithms, or external connections,
- Prevents zero-day attacks without the need for emergency patching,
- Provides deep forensic data in context for Incident Response, and
- Centralizes operational control through an intuitive console that gives you complete visibility across your OT and IT environment.

Now you don't have to sacrifice security on the altar of productivity. Contact Digital Immunity today to see how we can help you **Stay Productive, Stay Secure!**

Digital Immunity: Stay Productive, Stay Secure!

About Digital Immunity

Digital Immunity, Inc., an IQT Portfolio company that is revolutionizing cyber-threat protection, bridges the gap between real-time threat prevention and 24/7, mission critical environments so security no longer takes a back seat to production. We provide advanced cyber-threat prevention in Operational Technology, as well as controlled, mission critical IT environments with no impact to production or system performance. Our patented Digital DNA Mapping technology prevents advanced threats, including APT's and zero-day attacks, from executing in memory at runtime, hardening your mission critical operating systems and applications.

For more information, visit **http://www.digitalimmunity.com**.