LogRhythm®
The Security Intelligence Company

INDUSTRY 4.0: DEFENDING MANUFACTURING SYSTEMS FROM CYBERTHREATS

With new opportunities and innovations come new risks

Industry 4.0: Defending Manufacturing Systems from Cyberthreats

The manufacturing sector is on the cusp of its own digital revolution. Industry 4.0, as it has become known, will harness the connected sensors embedded in machinery running factories and logistics operations across the supply chain. It will extract data, model processes and transform operational efficiency.

It promises seamless collaboration with connected partnering organizations, supporting innovation on a scale previously unheard of. According to consultancy Accenture[1], it could add $14.2 trillion to the world economy over the next 15 years by improving productivity, reducing operating costs and enhancing worker safety.

The Internet of Things (IoT), a vital pillar supporting Industry 4.0, is picking up rapid momentum, according to analyst IDC[2]. It found 73 percent of decision makers have already deployed an IoT system of some kind within their business or plan to within the next 12 months.

Innovation in manufacturing will see IoT joined by 3-D printing, robotics and cognitive computing to change how manufacturers can acquire and apply knowledge. New technologies can provide unlimited access to information and knowledge, just as the information itself becomes even more valuable, says IDC in its report Information Digital Transformation in Manufacturing.

With opportunities and innovations come new risks

But there is a downside. Connecting all the machines in the factory to external information flows means the machines are susceptible to attacks by hackers, industrial spies or even national agencies—from anywhere in the world.

Almost 90 percent of political and economic decision makers see IT security as the greatest challenge to achieving a complete transition to Industry 4.0, according to a recent Deutsche Telekom cybersecurity report[3]. Or, to put it another way, companies that fail to come to grips with information security will struggle to benefit from Industry 4.0—and will fall behind counterparts who are able to transition.

Yet the industry seems unprepared. While 25 percent of cyber attacks will involve the IoT by 2020, IoT is set to account for less than 10 percent of IT security budgets, according to research from Gartner[4].

Evidence of the cybersecurity threat to the manufacturing sector is already building. U.S. industrial control systems were hit by attacks at least 245 times from October 2013 to November 2014, the U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) found[5]. Incidents in the critical manufacturing sector rose to 65 in fiscal 2014—up 30 percent on the year before.

Hackers seek to infiltrate general business and financial systems as well as attacking control systems. For example, in 2016 aerospace supplier FACC said a single hacking incident had cost the financial accounting department around $55 million[6].

Outside of manufacturing, across all industries, there is plenty of evidence that cyber threats are becoming better organized, more sustained and increasingly severe. Manufacturing needs to learn lessons from the wider world to defend itself accordingly and accrue the benefits of Industry 4.0.

> We believe the majority of information security spending will shift to support rapid detection and response capabilities, which are subsequently linked to protection systems to block further spread of the attack.
> - Gartner VP Neil MacDonald

Growing cyber threats across industries

The 2016 Global State of Information Security Survey, from consultancy PwC, reported a 38 percent year-on-year surge in detected security incidents[7]. This marks a steep 12-month rise compared to the 66 percent compound annual growth rate of detected security incidents in the five years to 2015.

Meanwhile, the 2016 research found that it isn't just enterprises experiencing a flood of attacks. Small- to medium-sized businesses reported on average 3,577 attacks last year—a significant leap from 693 in the same period 12 months earlier[8].

However, other sources suggest businesses do not know about the majority of attacks they sustain. One cybersecurity company recently estimated that as many as 71 percent of compromises go undetected[9].

As the volume of attacks changes, the perpetrators are also evolving. They are well organized and well funded. They have sophisticated technical skills to create custom malware for very specific targets, and they are relentless in pursuit of their objectives.

Moreover, almost anyone with malicious intent can purchase malware and rent botnets on the Dark Web—an area of the internet not indexed by commercial search engines. Easy access to tools lowers the bar for criminals, nation states and terrorists to mount cyber attacks against manufacturing companies of all sizes.

The increasing ferocity of cyber threats comes as manufacturers' IT environments have become more varied and complex. Legacy industry-specific systems and enterprise resource planning (ERP) might still run the nuts and bolts of the business, but new IoT-related technologies are also entering the fray. At the same time, business executives bring their own devices to work and use cloud-based applications under the radar of IT. The organizational perimeter is becoming more difficult to defend.

The World Economic Forum says the theft of information and the intentional disruption of online or digital processes are among the leading business risks that organizations face today[10]. Research by BAE Systems found more than half of U.S. companies now regard the threat from cyber attacks as one of their top three business risks[11]. If manufacturers do not see information security as a board-level priority, they should.

[1] Growth game-changer drives progress and prosperity https://www.accenture.com/gb-en/insight-industrial-internet-things-growth-game-changer

[2] Information Digital Transformation in Manufacturing http://www.idc.com/getdoc.jsp?containerId=US41144316

[3] 2015 Security Report: Are cyber attacks the greatest risk to Industry 4.0? https://www.telekom.com/media/company/293678

[4] IoT to play a part in more than a quarter of cyber attacks by 2020, says Gartner http://www.computerweekly.com/news/450288414/IoT-to-play-a-part-in-more-than-a-quarter-of-cyber-attacks-by-2020-says-Gartner

[5] ICS_CERT Monitor (Feb 2015) https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

[6] Prepare And Defend: Building An Armory Against Cyber Attacks http://aviationweek.com/mro-enterprise-software/prepare-and-defend-building-armory-against-cyber-attacks

[7] Global State of Information Security Survey 2016 (press release) http://www.pwc.com/us/en/press-releases/2015/global-state-of-information-security-survey-2016.html

[8] IDG 2016 Global State Of Information Security Survey http://www.idgenterprise.com/resource/research/2016-global-state-of-information-security-survey/

[9] Surfacing Critical Cyber Threats Through Security Intelligence https://logrhythm.com/pdfs/whitepapers/lr-security-intelligence-maturity-model-ciso-whitepaper.pdf

[10] Surfacing Critical Cyber Threats Through Security Intelligence A Reference Model for IT Security Practitioners https://logrhythm.com/pdfs/whitepapers/lr-security-intelligence-maturity-model-ciso-whitepaper.pdf

[11] 60% of US businesses have increased cyber security spend following recent wave of cyber attacks http://www.baesystems.com/en/cybersecurity/article/60-of-us-businesses-have-increased-cyber-security-spend-following-recent-wave-of-cyber-attacks

Old defenses are no longer sufficient

As threats change, so must the response. The first chapter in cybersecurity saw organizations use multiple technologies to defend their networks, applications and data. Firewalls, antivirus software, intrusion-detection systems and endpoint security all play their part, but together, they are insufficient to defend against the threats manufacturing organizations now face. Hackers often sniff out weaknesses in defenses long before they launch an attack. Strategies that only aim to keep out attacks are failing and have failed in some of the largest attacks to hit the headlines.

Herein lies the problem. Once an attack penetrates corporate systems, it can go undetected, giving the business no chance to respond. Recent research that studied 691 data breach investigations worldwide, spread across all industries, illustrates the problem[12]. In all, 71 percent of compromised victims did not detect the breach themselves. Financial institutions, law enforcement agencies and other third parties were usually the first to suspect a company had been compromised. On average, it took organizations 87 days to detect a compromise. That is nearly three full months. Once detected, it took organizations an average of a week to respond. A week is a long time when valuable personal data, intellectual property or commercial information is being corrupted or stolen.

Keeping threats out is important, but forward-thinking organizations acknowledge they will not always succeed. Their philosophy is, "If we are not compromised right now, we could be at any moment." They work under the assumption that the network is untrusted. If there is not an attack within their network, there soon will be. They understand that no defense system is perfect. Breaches are inevitable.

Leading chief information security officers (CISOs) are focused on two metrics relating to this new approach to security: mean time to detect (MTTD) and mean time to respond (MTTR). With these two measures, organizations can understand how they are protecting their vital data, not just the organization's perimeter.

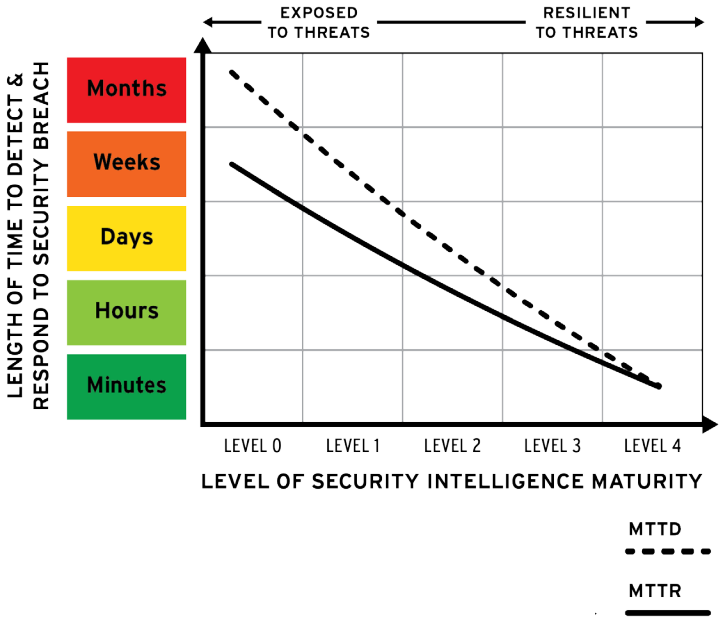
But under the old way of thinking, few resources are targeted at understanding threats that penetrate the system or measuring the response. If a company spends all its resources building and maintaining defense systems, it has nothing left to detect and respond to attacks that succeed.

Analyst firms are strongly advocating a rebalancing of the cybersecurity budget, shifting some funds from pure prevention to detection and response.

Gartner vice president and research fellow, Neil MacDonald says in a report, "In 2020, enterprise systems will be in a state of continuous compromise. They will be unable to prevent advanced targeted attacks from gaining a foothold on their systems. Unfortunately, most enterprise information security spending to date has focused on prevention, in a misguided attempt to prevent all attacks."

"We believe the majority of information security spending will shift to support rapid detection and response capabilities, which are subsequently linked to protection systems to block further spread of the attack[13]."

Gartner recommends that organizations respond by creating processes and investing time and technology in quickly understanding the nature and impact of breaches to their systems.



[12] Surfacing Critical Cyber Threats Through Security Intelligence A Reference Model for IT Security Practitioners https://logrhythm.com/pdfs/whitepapers/lr-security-intelligence-maturity-model-ciso-whitepaper.pdf

[13] Surfacing Critical Cyber Threats Through Security Intelligence A Reference Model for IT Security Practitioners https://logrhythm.com/pdfs/whitepapers/lr-security-intelligence-maturity-model-ciso-whitepaper.pdf

Legacy IT compromises manufacturing's data security

Against the backdrop of emerging threats in information security lies the specific state of IT in manufacturing. Typically, manufacturing industries are highly capital intensive with very low margins. While management recognizes the productivity gains resulting from IT investment, in general, the amount spent on IT per employee or as a proportion of revenue is lower compared with industries such as pharmaceuticals or financial services. Long upgrade cycles also set the manufacturing sector apart, as applications are often linked to a specific manufacturing process that can remain in place for years.

As a result, manufacturing firms can be littered with legacy technology—both in terms of enterprise software (e.g. ERP) and hardware (e.g. workstations set up to do a specific task). Old applications, databases and hardware may work as expected for the task in hand, but they expose the business to risk. When legacy systems become unsupported by the vendor, new security patches will not be available when vulnerabilities become exposed.

While firewall and antivirus software may try to protect the perimeter, any malicious code that gets behind these defenses can compromise systems that have not been upgraded.

For example, in 2010, the Stuxnet virus hit Iran's aging Bushehr nuclear plant. Computer security experts who studied Stuxnet believe it was engineered specifically to attack the Siemens-designed working system of the Bushehr plant and appeared to infect the system via the laptops and USB drives of Russian technicians who had been working there.

Manufacturing firms also labor under the illusion they will not be targeted by hackers, especially those who are not household names. Yet LogRhythm has seen its customers in the manufacturing sector specifically targeted for the purpose of industrial espionage. In one case, a rival firm had hired hackers to orchestrate an attack designed to steal intellectual property and research and development (R&D) data. It may not be publicly known, but no firm should think it is immune to hacking attacks.

Aging IT infrastructure and applications can make the manufacturing sector vulnerable to cyber attacks, but firms are more likely to invest in plant upgrade than in IT security, exacerbating the problem. The question is: What to do about it?

Building better defenses through security intelligence

Businesses leading the fight against cybercrime understand that, to mitigate attacks, they need to monitor threat activity, gather intelligence and create processes that make a rapid response automatic.

While organizations currently collect information about security breaches, too often the activity is not co-ordinated or well managed. Those responsible for IT security in manufacturing can gather data from a number of sources, including firewalls, intrusion detection systems, application gateways, antivirus and anti-malware software. The idea is they can identify any symptoms of an attack wherever it hits the IT estate.

But there is a problem. These "security sensors" provide so much data that the situation might be likened to a fire hose pumping information about events at the rate of thousands or tens of thousands of gigabits per hour. This intense stream of data can effectively blind a security team to any real threats, as they become difficult to distinguish from background noise. The volume of data also makes a rapid response impossible.

In 2013, U.S. retail giant, Target, suffered a massive cyber attack for this very reason. Hackers walked off with the payment card data of 40 million customers, along with non-payment personal data of another 70 million customers. The event was only discovered by an outside agency.

It took weeks of deep forensic investigations to pinpoint the cause of the security breach. Investigation revealed that before the theft of the sensitive information, the company received digital warning signs that something was amiss with the point-of-sale system. Months earlier, the merchant had installed a $1.6 million malware detection system that correctly identified and alerted security professionals to attackers' suspicious activity on multiple occasions. However, the company failed to follow up on these security alerts.

The outcome was disastrous. As a result of the breach, the company's shares initially plunged 11 percent. Sales fell 3.8 percent as the number of transactions dropped 5.5 percent during the holiday season. In the first quarter of 2014, earnings dropped 16 percent. In the second quarter, the company reported that the data breach cost $129 million, on a pre-tax basis. The company is the subject of class action and other lawsuits while paying for credit monitoring for tens of millions of customers.

Introducing an intelligent approach to information security

Manufacturers need a new approach to managing the data output from security tools. Leaders in the field are adopting the idea of security intelligence—analogous to business intelligence—which gathers corporate data in one place to provide reports, insight and early warning alerts to act on.

The role of security intelligence is to unlock the insight contained within this security data, helping organizations clearly identify those threats that could cause damage and present actual risk and providing the information necessary for a rapid response.

The main objective of security intelligence is to deliver the right information at the right time with the appropriate context to significantly decrease the amount of time it takes to detect and respond to damaging cyber threats. In other words, the goal is to significantly improve an organization's MTTD and MTTR.

Security intelligence helps organizations capture, correlate, visualize and analyze forensic data to develop actionable insight to detect and mitigate threats that pose real harm to the organization—and to build a more proactive defense for the future. Advanced analytics and machine learning can be applied to security data to discover previously unseen threats and respond more rapidly.

Reduce time to detect and respond to cyberthreats with the LogRhythm Security Intelligence Maturity Model

The LogRhythm Security Intelligence Maturity Model™ (SIMM™) helps companies understand their business risk posture based on their security intelligence capabilities and organizational characteristics. It offers the following hierarchy:

- **Level 0**: A company has not invested in security intelligence capabilities at all and is therefore at high risk of successful cyber attacks
- **Level 1:** A company addresses minimal compliance related requirements
- **Level 2**: A company has an efficient compliance posture and is gaining visibility with improved capabilities to respond to threats
- **Level 3**: A company is vigilant in seeing and quickly responding to most threats
- **Level 4:** A company is capable of withstanding and defending against the most extreme attacks from determined adversaries

Robert Lentz, former chief information security officer for the U.S. Department of Defense, has been working with maturity models in security for years. He says recent significant and successful cyber events might well prove to be the tipping point, where businesses and governments together finally acknowledge the fragility of their enterprises, the grave threat to national and economic security, and the need for executive-level oversight.

"The LogRhythm Security Intelligence Maturity Model offers a compelling framework to help organizations advance in their journey to combat advanced cyber attacks while simultaneously restoring confidence in the internet," he says.

Conclusion

Information security is becoming paramount in manufacturing. As the sector seeks to benefit from the massive opportunities offered by Industry 4.0 and associated technologies, its leaders are rethinking how they defend systems, now connected to the outside world, from attack.

As manufacturing IT encompasses the IoT, 3-D printing and widespread collaboration, defending information systems from outside threats is no longer tenable. The most innovative companies are now seeing that defenses should also be accompanied by security intelligence to spot dangerous breaches, help organizations protect vital data before it becomes compromised and provide a basis for ongoing improvements in security.

The stakes could not be higher. Industry 4.0 offers manufacturing industries a brave new world in which they can get closer to customers and consumers, innovate in design, slash costs and work towards mass customization. Security intelligence is the foundation on which they can make sure the new world is also a safe one.

About LogRhythm

LogRhythm, a leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company's patented award-winning platform uniquely unifies next-generation SIEM, log management, network and endpoint monitoring, user entity and behavior analytics (UEBA), security automation and orchestration and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides unparalleled compliance automation and assurance, and enhanced IT intelligence.

LogRhythm is consistently recognized as a market leader. The company has been positioned as a Leader in Gartner's SIEM Magic Quadrant report for five consecutive years, named a 'Champion' in Info-Tech Research Group's 2014-15 SIEM Vendor Landscape report, received SC Labs 'Recommended' 5-Star rating for SIEM and UTM for 2016, and earned Frost & Sullivan's 2015 Global Security Information and Event Management (SIEM) Enabling Technology Leadership Award.

LogRhythm is headquartered in Boulder, Colorado, with operations throughout North and South America, Europe and the Asia Pacific region.

> **"The LogRhythm Security Intelligence Maturity Model offers a compelling framework to help organizations advance in their journey to combat advanced cyber attacks while simultaneously restoring confidence in the internet."**
>
> - Robert Lenz, Former CISO, U.S. Department of Defense

Contact us:
1-866-384-0713
info@logrhythm.com | www.logrhythm.com
Worldwide HQ, 4780 Pearl East Circle, Boulder CO, 80301

LogRhythm®
The Security Intelligence Company