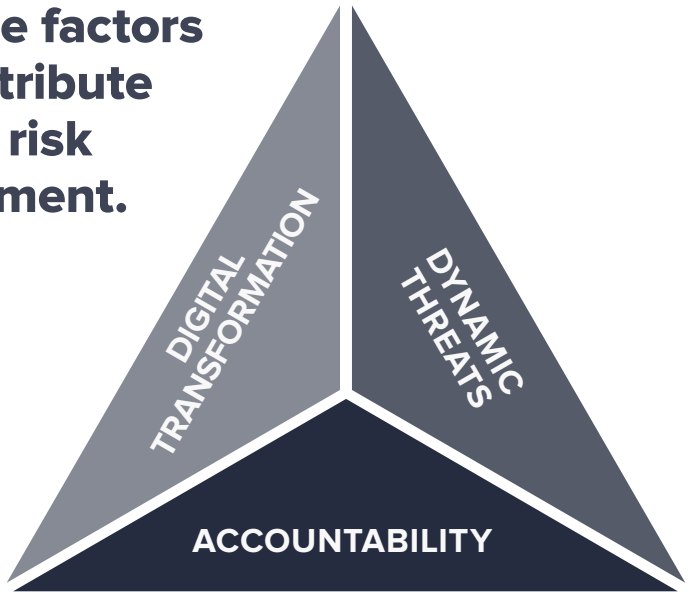
eSENTIRE

# IT, OT and IoT: Dotting your Cyber I's & Crossing your Cyber T's.

Modern manufacturing faces a trinity of issues: the blending of manufacturing IT and OT ecosystems and the adoption of emerging technology, the criminals who have learned how to exploit the opportunities presented by this transformation, and the resulting board and executive level of accountability to protect the business health from cyber risks.

## The three factors that contribute to cyber risk management.




The March 2019 ransomware attack on aluminium and renewable energy company Norsk Hydro shows how bad the problem has become. The attack encrypted the company's files and demanded a ransom to retrieve them, forcing the company to fall back to manual operations at its smelting plants in Norway, Qatar and Brazil and causing an as-yet unknown financial impact.

# Digital Transformation

Attacks on manufacturing firms will only continue to increase as operational (OT) and information systems (IT) converge and blend into one ecosystem, and the job of securing these systems sits in two different teams who are not used to talking to each other.

Criminals also exploit systemic vulnerabilities in operating systems or control systems, like SCADA and ICS. The 2018 Forrester SCADA survey indicates that 56% of organizations using SCADA or ICS systems experienced a breach in the past year. Only 11% indicated that they never experienced a breach. This finding suggests that many manufacturers don't know, or aren't willing to acknowledge that they have been attacked and infiltrated. A successful cyberattack against OT or a SCADA control system not only has the potential to damage the business financially, but also could result in physical consequences to such things as infrastructure and services, the environment, and possibly human life.

According to the 2018 FutureWatch report, manufacturing firms are among the fastest to adopt emerging technologies such as cloud (78%), big data analytics (56%), and IoT/IIoT (54%). In response, cloud security investment was a top priority (41%), with a focus on identity access management (43%), endpoint protection (34%), and a new focus on threat detection and response services (31%). While spend parallels technology and employee risks, the majority (43%) of firms primarily base their security efforts on traditional prevention technologies (firewalls and anti-virus), with 36% leveraging compliance logging and alert management tools and services, and the smallest contingent (20%) are investing in artificial intelligence used to detect aberrant activity, proactive threat hunting, and threat intelligence. In the next two years, 43% intend to leverage these proactive hunting and predictive detection and response practices to improve their security posture.

As trusted partners, third-party vendors often become the overlooked or unwitting accomplice in criminal activities. A Spiceworks survey of 600 IT and security decision-makers about their top concerns around their supply chain and the policies or procedures highlights this risk.

Even though the majority of respondents felt confident in the vendor to keep their data safe, nearly half (44 percent) of firms had experienced a significant, business altering data breach caused by a vendor. Human error and stolen passwords accounted for 26 percent of the breaches, while malware played a key role in half of the attacks.

Of the nearly 250 companies that experienced a breach, 32 percent affected personal identifiable data, 29 percent included payment information, and 24 percent exposed proprietary business data. What's worse, only 15 percent of firms reported that their vendors provided notification them when a breach occurred.

Third-party breaches can result in disrupted operations (27 percent), increased operational complexity and cost (52 percent), reputational damage (19 percent) and financial losses and penalties (26 percent).

# Dynamic and Targeted Threats

Today, cyber criminals are hunting their prey. Through the opportunistic and transactional ransomware attacks of the past few years, criminals identified more lucrative prey, such as law firms, healthcare institutions, and manufacturers. Criminals don't discriminate by annual revenue or employee count. Smaller and mid sized manufacturers are easier targets than their larger peers.

Nation state actors are hard at work stealing vital manufacturing IP and processes to help their country further its economic agenda. This is not simply the domain of national security or law enforcement to protect industry. Simple "smash-and-grab" criminals peddling fraudulent invoices, or crafty criminal syndicates know manufacturers will pay to avoid operational disruption and the accompanying financial losses and reputational damage. And law enforcement struggles to stop attacks that reside outside the country in places with destabilized governments and no extradition. These attacks will continue and these forms of crime pay well, but unlike other forms of lucrative crime, most cyber criminals act with impunity.

The vast majority of attacks begin with a simple email phishing campaign designed to harvest employee credentials or elicit fraudulent payment requests. This is known as Business Email Compromise (BEC), or "spoofing the boss".

# Accountability

Manufacturing firms self-ranked above financial institutions when it came to vulnerability to cybersecurity attacks, but below law firms and healthcare institutions. Over half of the respondents reported that unknown attacks posed the greatest risk, followed by non-malware born attacks and insider actions.

Manufacturing firms also recognized that cybersecurity is now a board level issue, but struggle to cope with the growing challenges of mitigation cyber risk. Managing the supply chain (59%), meeting regulatory and customer requirements (58%), and bearing the cost of ever increasing security demands (50%) represented the top challenges. To compound the issue, 42% of firms were challenged to measure and report the status of security programs, and 46% struggled to demonstrate the value of cybersecurity spend to executives and board members.

# Dotting Your Cyber I's & Crossing Your T's

Attacks on manufacturing firms will only continue to increase as operational (OT) and information systems (IT) converge and blend into one ecosystem. There are no magic bullets, but firms can follow this top ten security must have list to reduce the risk and improve their ability to respond and recover from an attack:

1. Identify and audit critical systems and data. Protect what matters.
2. Understand your obligations (legal, regulatory, supply-chain, and client).
3. Establish cybersecurity policies, procedures, and executive reporting mechanisms.
4. Conduct an annual risk assessment and security readiness exam (penetration testing, red-blue team exercises)
5. Require encryption of stored data (mobile devices, laptops, servers, etc.).
6. Use VPN security to protect data and user credentials in motion through a virtual private network.
7. Establish mobile and bring your own device (BYOD) rules and controls to enforce strong password and limit access to corporate assets.
8. Establish back-up systems and services.
9. Establish an incident response plan and team, and practice fire drills to hone your program.
10. Consider cyber insurance to cover investigation, disruption, lost revenue, and other costs not covered in non-cyber specific policies.

eSENTIRE®

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business-disrupting events. Protecting more than $6 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.eSentire.com** and follow **@eSentire**.