MANUFACTURING CYBERSECURITY

What CFOs Need to Know

CERTITUDE SECURITY

As cyber threats grow more sophisticated to monetize breaches, manufacturing companies must pay closer attention to their IT assets, private networks and information security standards. Cybercrime is projected to cause about $6 trillion in damages annually by 2021,[1] leading to a dramatic increase in cybersecurity costs. Cyber risk is a manufacturers reality and a financial risk that cannot be ignored. Understanding and prioritizing mitigation expenditures is a major operational challenge, but the consequences of poor IT security cannot be understated.

Almost half of all manufacturing companies experienced **at least one data breach in the past 12 months.**[2]

From malware attacks and ransomware to phishing scams and more, there's no shortage of cyberthreats manufacturers must guard against.

For U.S. companies, the average cost of a data breach was around **$7.91 million** in 2018, or $148 per stolen record.[3]

Although manufacturers typically do not store much consumer information, intellectual property and employee data is equally valuable to cybercriminals.

The four leading causes of reported breaches in Manufacturing were 1. Web applications, 2. Privilege misuse, 3. Cyber-espionage and 4. Miscellaneous errors.[4]

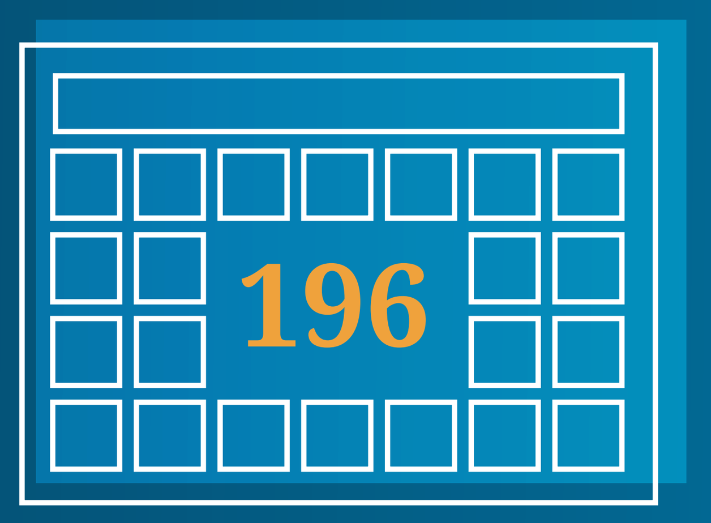
The three most common actions used to breach manufacturer systems were Hacking, Social, and Malware.

Cyberattacks targeting Internet of Things devices are increasing year-over-year by **upwards of 217%.**[5]

Taking full advantage of Industry 4.0 requires comprehensive threat detection and vulnerability management tools.

Companies that experienced a data breach in 2018 took an **average of 196 days** to identify the security incident.[6]

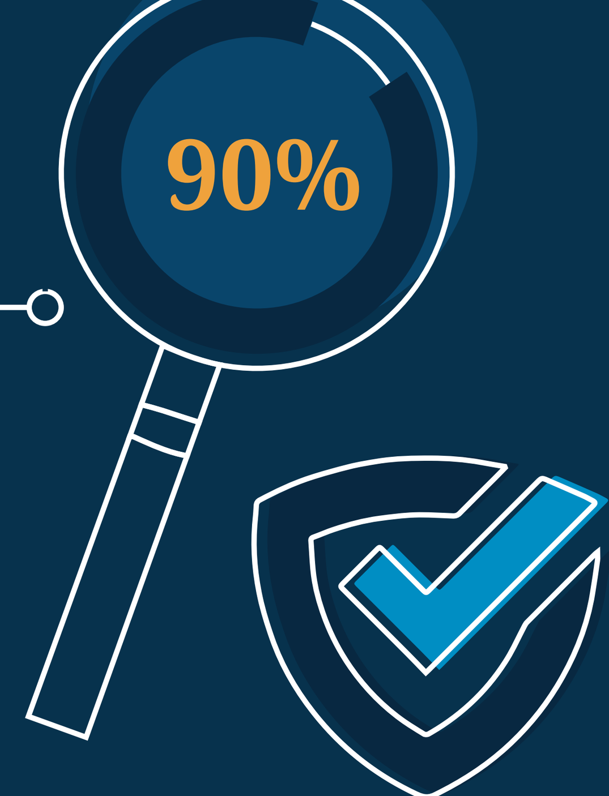
A lack of system and network visibility can magnify the financial impact and productivity losses of cybersecurity events.



Roughly half of all cybersecurity risks for manufacturers stem from having multiple cybersecurity vendors and applications.[7]

Adopting a unified threat management approach can help manufacturers eliminate inefficient processes and strengthen their overall IT security posture.

That's why throwing more capital at tools and then believing you are secure, virtually ensures loss. You don't know what you don't know. **The 80% to 90%** of problems hidden from you are culminating into pervasive issues within your business. Gaining better understanding to probable threats that could cause loss and developing a plan with clear priorities and budget, is the shortest and most cost-effective method to go from point A to point B.



The mindset and engagement of executive leadership, and specifically the CFO, to set a culture of security, further enables that organization to take steps to notify and educate all employees of their role in preventing cyberattacks. In the absence of controls, reporting, and enforcement measures, CFOs rely on hope to address their concerns.

That is why Certitude Security offers advanced threat assessment services that can help you identify, prevent and mitigate costly cyberattacks. We do not replace your internal IT team, we work with them to become more effective. For more information, visit us at www.certitudesecurity.com.

NOTE: An Incident is a security event that compromises the integrity, confidentiality or availability of an information asset.

A breach is an Incident that results in the confirmed disclosure, not just potential exposure, of data to an unauthorized party.

CERTITUDE™ SECURITY

[1] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[2] https://www.sikich.com/wp-content/uploads/2019/06/SKCH-MD-Report-2019-1.pdf

[3] https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

[4] Verizon 2019 Data Breach Investigations Report

[5] https://blog.sonicwall.com/en-us/2019/03/2019-sonicwall-cyber-threat-report/

[6] https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

[7] https://www.cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2018.html