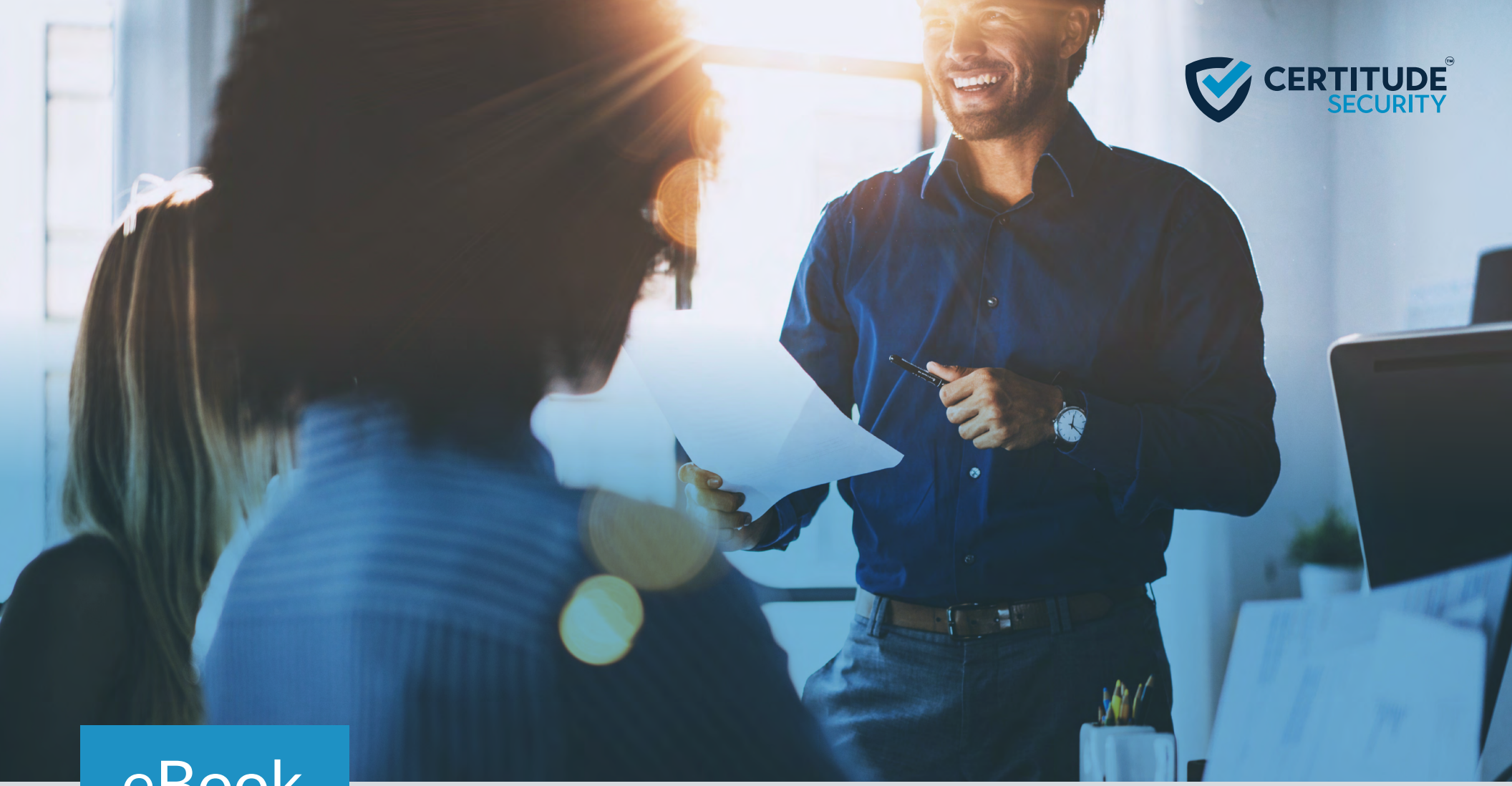


CERTITUDE SECURITY

eBook

Manufacturer Insights:

Cyber Risk Expectations Versus Reality

Contents

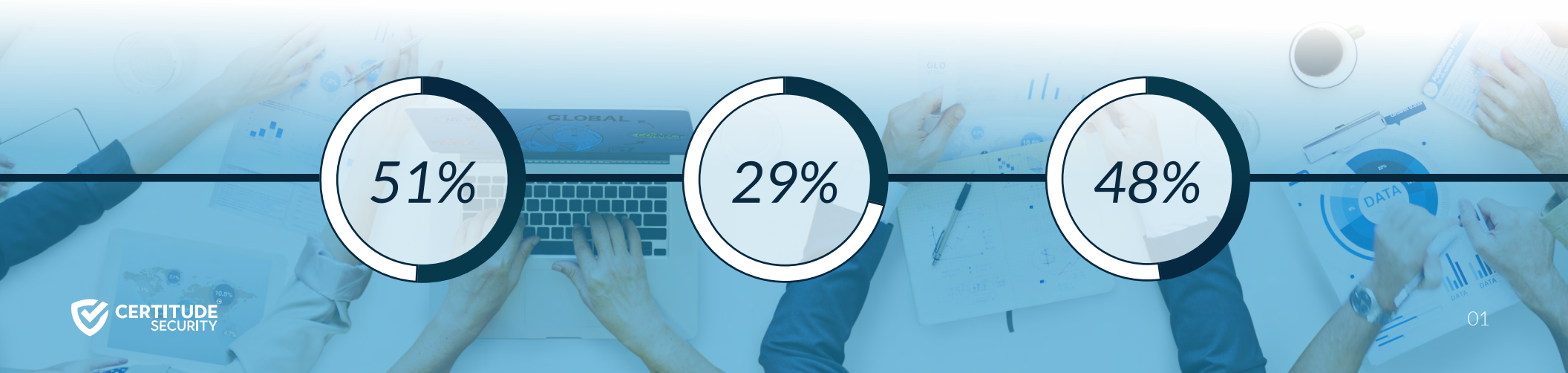
Cybercrime in the Manufacturing Industry: A Growing Threat

Cybercriminals are equal opportunity offenders.
They'll seize on the opportunity, regardless of the person, business or industry.

Hackers have found that the manufacturing industry currently offers the optimal return on investment. Based on studies conducted by IBM, manufacturers account for roughly 8% of all cyberattacks, placing manufacturers within the top 10 of the most preyed-upon industries.

Globally, **51% of organizations do not believe they are ready for a cyberattack or breach event.** Moreover, **29% of organizations with a response plan have not tested or updated them in the last 12 or more months.** According to a joint report published by the Manufacturers' Organization and the American International Group, **48% of manufacturers have experienced a cybersecurity incident** within the past 12 months, with roughly half experiencing a financial loss as a result.

Manufacturers must take proactive measures to understand the nature of these threats and coordinate the development of effective countermeasures.



Welcome to Industry 4.0

From smartphones to convenient mobile wallets, the world has become more digitized as manufacturers continue to pump out state-of-the-art technologies that make day-to-day activities more convenient. The digitization of manufacturing has sparked what's come to be known as the "fourth industrial revolution," or Industry 4.0, characterized by electronics and IT to streamline mass production. From cloud applications to internet-of-things devices (IoT), smart sensors and large-scale machine-to-machine systems (M2M), the capabilities of Industry 4.0 innovations have revolutionized modern society and cultural norms. As Gallup reported, over **85% of Americans regularly use at least one of six products with artificial intelligence components,** such as voice-activated personal assistants, navigation apps, and video streaming services.

However, as consumers and business owners have become increasingly connected, their vulnerability to data theft has also risen, and manufacturers are struggling to keep up.

Over 85% of Americans regularly use at least one of six products with artificial intelligence components.

Top Cyber Threats in Manufacturing

While organizations frequently make headway against cyberattacks, attackers constantly develop new techniques. **Because so many appliances, devices, and equipment have online capabilities, cybercriminals have more potential points of access,** which may lack the security elements necessary to predict and protect against probable threats and attempted breaches.

As reported by IndustryWeek, the most critical cyber threats facing manufacturers include the following:

Identity theft: Hackers will often use malware to access their targets' Social Security or credit card numbers.

Phishing: This method uses emails to steal sensitive data by crafting verbiage, logos and letterhead that appear legitimate.

Spear phishing: Phishing attacks that target specific high value recipients, such as CEOs and CFOs.

Compromised web pages: These websites are designed to create havoc for visitors by having them click on a link that's loaded with malware or viruses, affecting the victim's network or computer.

Spam: Undesirable emails distributed in large quantities that reduce productivity and may install malicious software.

Business Consequences of Cyberattacks and Data Breaches

As threats and breach attempts increase in number, the costs of these attacks have followed suit. According to analysis conducted by IBM and the Ponemon Institute, **the average cost of a data breach now stands at $3.92 million and has risen consistently over the past five years.** In 2019, the number of records exposed topped 8.5 billion, a three-fold surge compared to 2018, caused by misconfigurations of sensitive material. On a per-breach basis, roughly 25,575 records were exposed in 2019, containing proprietary business or customer information.

Consider manufacturers that are obligated to sign confidentiality clauses that include fines per breached record. The breached record fines range from $100 to $1,000 per record. If the average breach **exposes 25,575 records, that equates to breach of contract fine ranging from $2,557,500 to 25,575,000.**

These incidents can lead to financial ruin and cause lasting effects on overall productivity, damaged credibility, and increased downtime.

The Direct and Indirect Costs of Downtime and Business Interruption

Business interruptions, data corruption, and production downtime have a cost, impacting finances, even if the security incident seems relatively minor. For example, IBM and the Ponemon Institute discovered it takes an average of 279 days before a breach incident is recognized, and 314 days when including the number of days required to contain the attack.

The adverse consequences of downtime and business interruption are both direct and indirect in terms of monetary losses:

Direct

- Lost revenue
- Fines and penalties from regulatory or government organizations
- Costly legal fees and settlements if affected customers file charges
- Devoting more resources to IT and data recovery to the detriment of other departments

Indirect

- Reduced overall work productivity and output caused by network outages
- Public relations fallout, resulting in damaged reputations and/or brand recognition
- Loss of trust from key stakeholders and/or loyal customers
- Customer complaints and negative word of mouth
- Missing out on new business opportunities

Recovery Fatigue: The Hidden Costs of Cybersecurity

If the consequences of cyberattacks weren't harsh enough, the recovery process can be equally problematic, even when manufacturers rely on third-party IT service vendors. Business owners like to be in charge and aware of every activity that pertains to the company's performance, a significant challenge when recruiting outside help. This can result in elevated stress from difficult interactions with customers who demand answers beyond "We're doing the best we can." The longer it takes to bring business applications back online, the shorter customer patience grows.

The hidden customer relationship management costs are exacerbated by the effect on productivity and revenue lost due to these incidents. According to research conducted by Gartner, **IT service disruptions consume an average of 238 minutes per day and $5,600 in lost work productivity for each minute offline.** When including the stress and fatigue cybersecurity incidents create, **IT interruptions waste a daily total of 288 minutes to resolve.**

IT service disruptions consume an average of 238 minutes per day and $5,600 in lost work productivity for each minute offline.

Closing the Gap: Best Practices in Manufacturing Cybersecurity

There are many factors stimulating changes within cybersecurity to stop the increase in successful breaches, such as contracts with trading partners, Fortune 500 customers, and the DOD. Then **we must consider regulatory and/or compliance with DFARS, ITAR, CMMC, ISO, HACCP, and PCI.** We also see increased interest from boards and private equity making sure risk is understood and reasonable measures are taken to protect themselves and their customers.

However, there's work to be done as breaches proliferate. Hiscox, a specialty insurer who has offered cyber coverage for over 20 years, defines what constitutes as "bad" preparedness (list to the right) when it comes to recognizing and responding to cyber threats.

- Cybersecurity is dealt with on ad-hoc basis with no clear line of responsibility
- No formal cyber strategy, no dedicated cyber budget
- Over reliance on technology and light on people
- Slow response to incidents
- Inconsistent employee awareness training
- No evaluation of supply chain vulnerabilities
- No simulation of cyberattacks or employee responses

Enhancing Cyber Risk Preparedness with Certitude Security™

The best way to enhance your productivity and reduce your risk is with a security strategy you can trust. Certitude Security™ works alongside manufacturers to build an effective strategy and action plan that protects workflows, while defending against application and network incursions.

We support manufacturers and their strategic objectives by:

- End-to-end cyber strategy planning to streamline resourcing in support of business priorities
- Implementation of security frameworks designed to prevent cyber incidents
- Refine and align IT policies in keeping with compliance and industry protocols
- Employee social testing and awareness training
- Assessment of device and network vulnerabilities on a scheduled basis
- Monitoring supply chain risk to report on third-party exposure from vendors
- Continuous cyber threat assessments and translating data into insights and actions
- Assist with efforts to recover damaged data to reduce business interruption and downtime

Certitude Security™ provides the certainty you need to protect your data and reduce your exposure to cyberattacks. For more information, contact a Certitude Security™ representative.

certitudesecurity.com