CERTITUDE™ SECURITY

Manufacturing Executive Anxiety:

Cyber Risk Explained

Contents

CERTITUDE™ SECURITY

TheTransformation of Manufacturing

The manufacturing sector has experienced significant change in the last decade, evidenced by vast innovations in product development, customized workflows, and greater visibility into supply chains. While the advantages are significant, the drawbacks are severe, including data breaches, fraud risk, and supply chain disruption.

Based on research from IBM, just one data breach in 2019 cost companies an average of $3.92 million overall, the equivalent of $150 for every record lost or stolen. This may explain why **60% of manufacturers point to cyberattacks as an issue that causes them "great concern," according to the 2020 findings from MAGNET.**

Over 90% of organizations believe that the cyber threat landscape will stay the same or worsen in 2020. To address cybersecurity concerns, **76% of organizations plan to increase their cybersecurity budget in 2020, according to a survey conducted by FireEye.**

With a robust cyber defense plan in place, manufacturers can predict and protect against these increasingly prevalent attacks.

The Business Impact of Cyber Attacks

Insufficient protection against cyber threats can result in numerous negative outcomes. As manufacturers work on addressing affected aspects of their operations, other areas of their business that require ongoing maintenance may be neglected.

Consider these sobering statistics from ServiceMax, Kaspersky Labs, IBM, Verizon, and Hiscox:

- Downtime costs average businesses approximately $4,166 per minute.
- A full hour of unplanned downtime results in productivity losses averaging $336,000.
- In 2017 and 2018, close to 33% of data breaches led to layoffs.
- Companies with fewer than 500 employees suffer losses of more than $2.5M on average.
- 43% of all cyber attacks are aimed at small businesses.
- 53% of respondents reported a cyber incident in 2019.
- 65% experienced one or more cyber attacks from a weak link in their supply chain.
- 51% include cyber KPIs in their contracts with suppliers.
- 74% evaluate supplier network security once a quarter.

Prominent Cyber Attack Tactics in 2020

No single business or industry is impervious to cyberattacks. They affect one and all. Due to the highly connected nature of manufacturers' work processes and the products they develop, manufacturers are particularly vulnerable. Even one stolen credit card number can have a cascading effect that leads to sensitive records or company data falling into the wrong hands.

Several of the most common methods of cyberwarfare in 2020 are the same used in previous years. The only difference is their level of sophistication:

- Hacking
- Social engineering
- Targeted malware
- Exploitation of software vulnerabilities
- Misuse by authorized personnel

There's a reason why hostile actors resort to these means of entry, because they work. This explains why cyberattacks have been the top concern for manufacturers for three years in a row, according to MAGNET. A better comprehension of these methods can be helpful in devising a defensive strategy.

Assessing the Modern Cyberattack Landscape

Hackers not only have more attack points to exploit because of the highly connected nature of everyday equipment, appliances, devices, and merchandise, but also more techniques available. While some of these methods are difficult to decipher and hard to prevent, others are easily accomplished by seeing what works and what doesn't:

Brute-force:

From cracking passwords to copying and pasting usernames, this method is mostly done through trial and error. Using a process of elimination also enables thieves to find encryption keys.

Stolen credentials:

Pickpocketing, the use of credit card skimming devices, and phishing are common methods of data theft.

Backdoor:

This process involves the bypassing of normal security measures by taking advantage of internal networking flaws, outdated plug-ins, or malware installation.

Exploitation of inherent vulnerabilities:

Many IOT devices do not have security features built into them, they're prime targets for hackers to abuse.

Malware: A Brief Overview

Malware is designed to give bad actors unauthorized access to computer systems, causing financial harm and performance disruptions. Security experts estimate roughly 350,000 new malicious programs are developed on a daily basis. According to AV-TEST Institute, commons types include:

Command and control:

These eponymous servers are used by hackers as a feeding source, allowing them to deliver malicious programs and software once they've gained entry to a computer or network.

Ransomware:

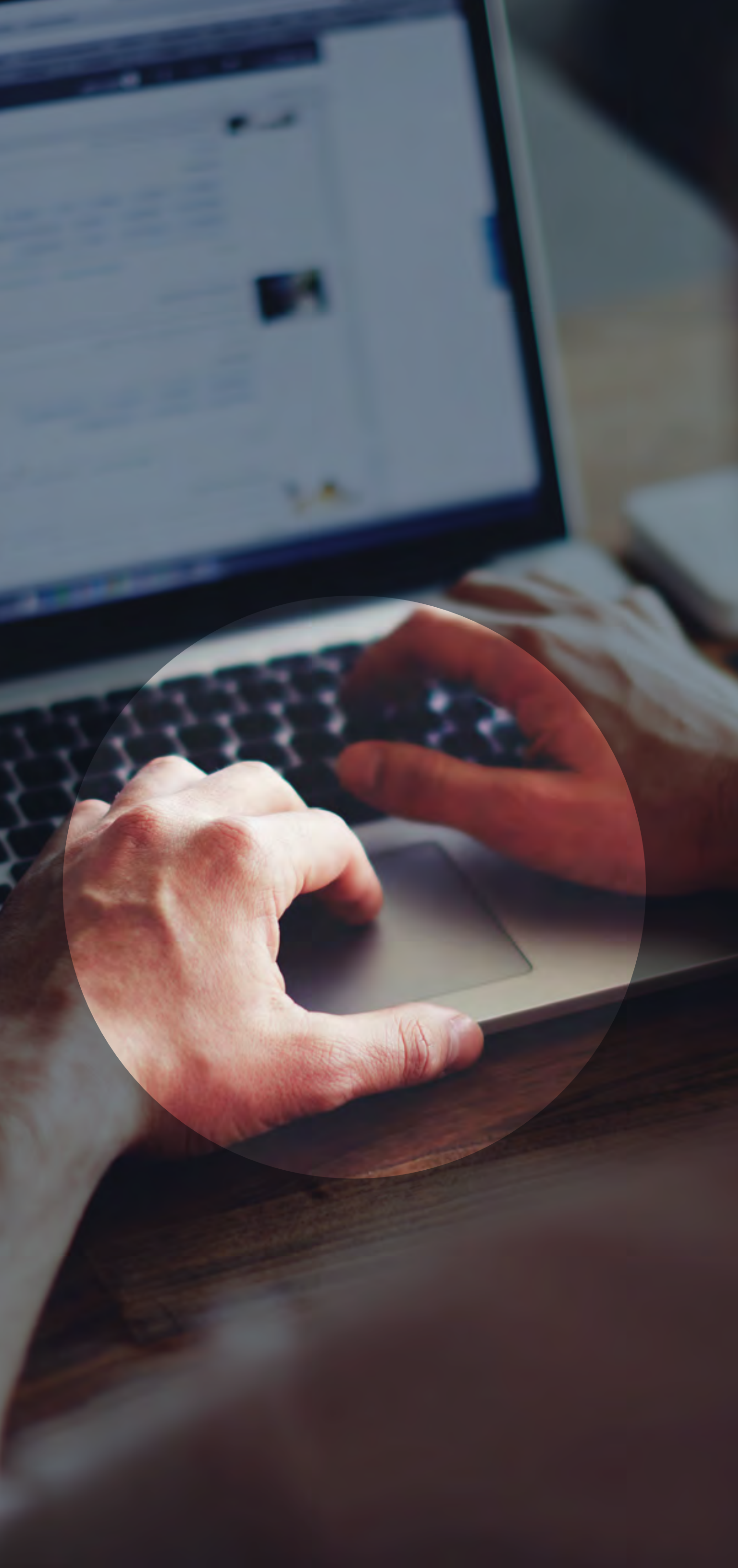
Malware uses encryption technology to lock down computer systems, requiring the victim to pay a sum to recover access. However, there's no guarantee the lockdown will be lifted.

Spyware:

Thieves use this method to collect sensitive information, such as passwords and usernames, without the owners' knowledge. This is made possible because such an attack rarely alters software functionality.

Adware:

Highly detectable, adware automatically displays advertising materials upon downloading a corrupted file, causing frustration for users because these programs are hard to uninstall.



Improving Cybersecurity: Key Operational Challenges

In many ways, wall-to-wall digitization of modern society and the manufacturing industry has served as a double-edged sword. Digitalization has enhanced convenience, efficiency, and productivity. Conversely, the pace with which digitization has taken place has made it difficult for manufacturers to implement countervailing defensive measures. Hackers are constantly refining their means of attack, looking for any outlet they can expose and exploit. In certain respects, cybercriminals have used manufacturers' products against them, as more internet-connected devices allow for more opportunities to steal sensitive trade secrets or financial information.

Fortunately, organizations focusing on cybersecurity are devoted to thwarting cyberattackers' malicious plots. The cost of these comprehensive defensive measures can cut into manufacturers' budgets. However, **given that cybercrime is poised to cost businesses of all types $5.2 trillion over the next five years, the cost of doing nothing is far greater, according to Accenture.**

Protecting Your Business: Best Practices in Cybersecurity

The best way to mitigate risk is by aligning your strategy with your business's vision, strategic objectives, and corporate goals. Manufacturers can achieve this goal by falling back on best practices and honing in on security gaps. Consider these five steps: Identify, Protect, Detect, Respond, and Recover.

Identify

- Conduct strategy, risk, and security assessments
- Analyze asset and risk management
- Review supply chain impact analyses

Protect

- Establish controls for user access
- Train employees to enhance security awareness and best practices
- Perform ongoing network maintenance

Detect

- Maximize event awareness
- Maintain threat detection
- Implement vulnerability analysis to enhance prevention

Respond

- Develop a incident response plan for probable worst-case scenarios
- Create a communications plan to mitigate effects of breach
- Strategically inform customers of incidents and their anticipated impact

Recover

- Coordinate with external contacts to expedite the recovery process
- Perform vulnerability testing to guard against follow-up attempts
- Assess IT infrastructure to identify potential flaws that exist and how to remedy them

Certitude Security™ is Your Partner in Protection

Cybersecurity is a difficult battle, but Certitude Security™ works alongside hardworking manufacturers to build an effective strategy and action plan that protects workflows and defends against application and network incursions.

Most of the danger lies in the fact that you don't know, what you don't know. As a viable partner in prevention, Certitude Security™ provides cyber threat assessment services to identify gaps in securing critical business services, and help prioritize resources to mitigate probable risks and threats. Certitude Security™ also co-develops viable plans that reduce danger in your organization by offering services such as strategy planning, initial threat assessments, continuous assessments for device and software vulnerabilities, implementing security frameworks and data backup systems, improving policies and procedures, and much more. **A byproduct of this intense focus is improved peace of mind, knowing that you are enhancing your duty of care in a threat-heavy digital environment. Contact us to learn more.**

CERTITUDE™
SECURITY

certitudesecurity.com

Sources
After the Fall: Cost, Causes and Consequences of Unplanned Downtime. ServiceMax, 2020. Retrieved from:
https://lp.servicemax.com/Vanson-Bourne-Whitepaper-Unplanned-Downtime-LP.html?utm_source=blog&utm_campaign=vansonbourne2017
2020 Ohio Manufacturing Report: Technology, Talent, and Transformation. Magnet, 2020. Retrieved from:
https://www.manufacturingsuccess.org/2020-state-of-northeast-ohio-manufacturing-report
FireEye Cyber Trendscape 2020 Report
Hiscox Cyber Readiness Report 2019
2020 State of Malware Report. Malwarebytes, 2020. Retrieved from:
https://docs.google.com/document/d/1OtVOaBUU7HPuHK5yZ2MG6RMdw6DOKhAVDgJ0fXsOjc0/edit (client-approved outline)