CYBERSECURITY

Why cybersecurity matters for automotive executives

usa.siemens.com/industrial-cybersecurity

SIEMENS

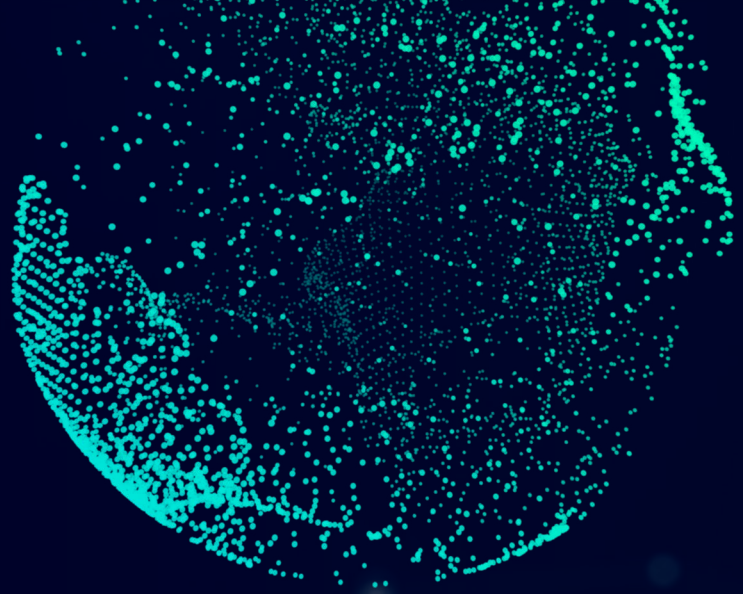


Table of contents

Cybercrime can seriously damage an enterprise by interrupting production, damaging reputation with customers and prospects, and crashing stock share price. But there are further hidden costs, including lost opportunities, strained supplier relationships, drained resources, and lower employee morale.

> Gartner predicts that by 2025, **40% of boards of directors** will employ a dedicated cybersecurity committee overseen by a qualified board member."
>
> – Security Magazine

In today's progressively connected world, cybercriminals seem to effortlessly infiltrate and exploit information technology (IT) and operations technology (OT) systems. Attacks could range from shutting down a plant's operations, to **altering the programming of machinery**, resulting in plants producing deadly products.

Automotive manufacturers **need protection**

> Just one cyberhack can cost an automaker $1.1 billion. The cost for the industry as a whole could reach $24 billion by 2023."
>
> – GlobalTradeMag

From Q4 2019 to Q1 2020, **there was a 156% increase in ransomware attacks in the manufacturing sector**. Deployment of ransomware – altering or shutting down an OT, IT or other computer system with malware until money is paid to the hacker – is just one tactic in the expanding world of cybercrime.

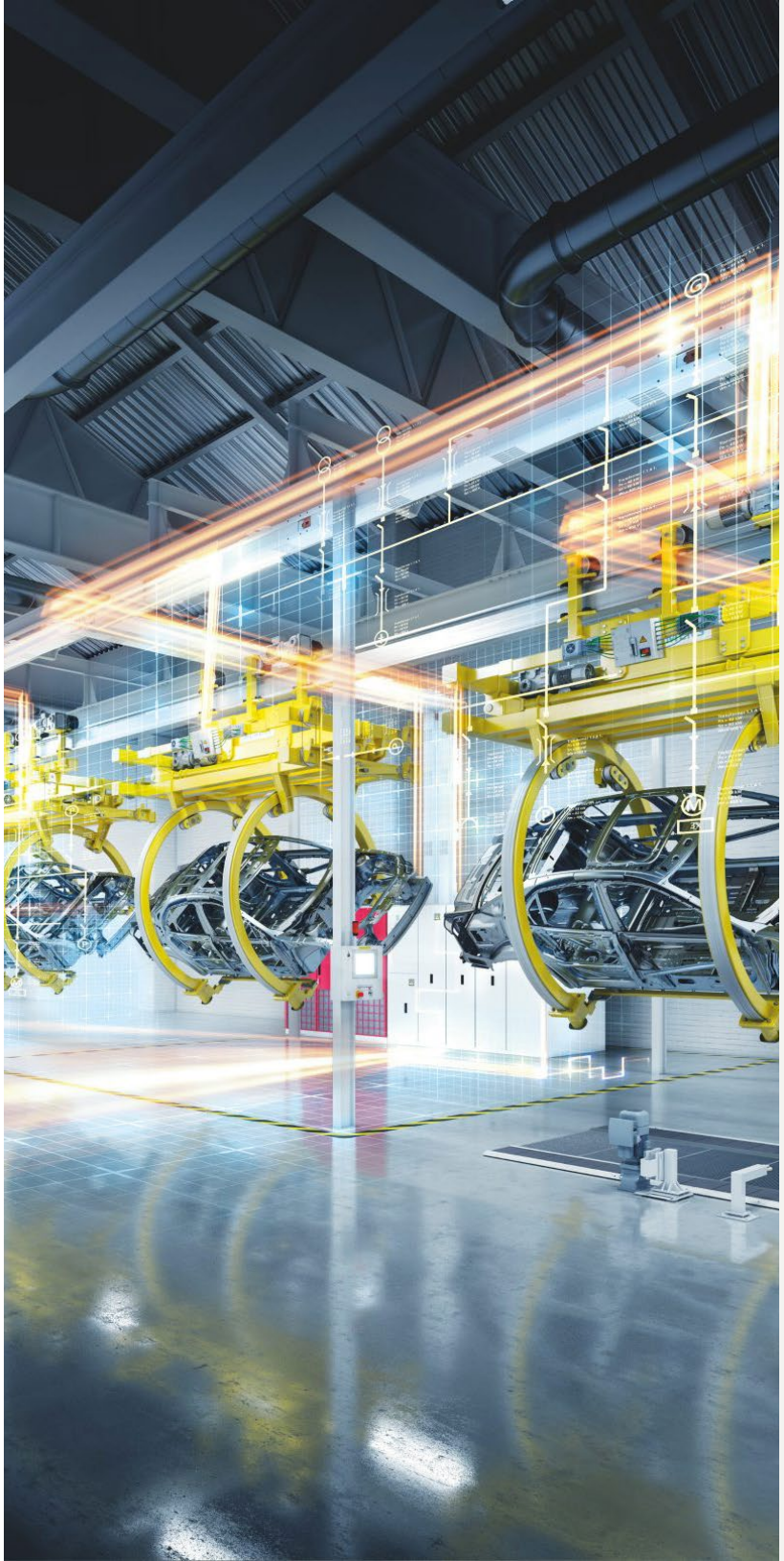
Forbes correctly estimated in 2017 that cybercrime would cost businesses $6 trillion annually by the end of 2020. **Cybercrime Magazine** projects that number will reach $10.5 trillion by 2025.

The automotive industry is not immune from cyberattacks. In the **June 2020 ransomware attack on Honda's global operations**, hackers derailed operations in North America, Turkey, Japan, Italy and the UK. A company spokesman **explained at the time** that "Honda experienced a disruption in its computer network that has caused a loss of connectivity, thus impacting our business operations."

The company shut down operations as it scrambled to contain the situation.

A report by **TechRepublic** suggested that "the company seemingly failed to employ the necessary security measures to mitigate the attack ahead of time." This is often true in incidents like these, despite Honda suffering a previous ransomware attack in **June 2017 by the WannaCry ransomware** worm, which halted production at one of its plants in Japan. That same attack also affected **Nissan and Renault**, forcing both manufacturers to shut down operations at plants in Britain, Japan, India, France and Romania.

In short, this issue is only becoming more urgent for automotive business leaders.



What are **the challenges?**

Intellectual Property theft is a major motivator for cyberattacks in manufacturing. Data breaches can expose sensitive personal records, but cybercriminals can also hack important business data.

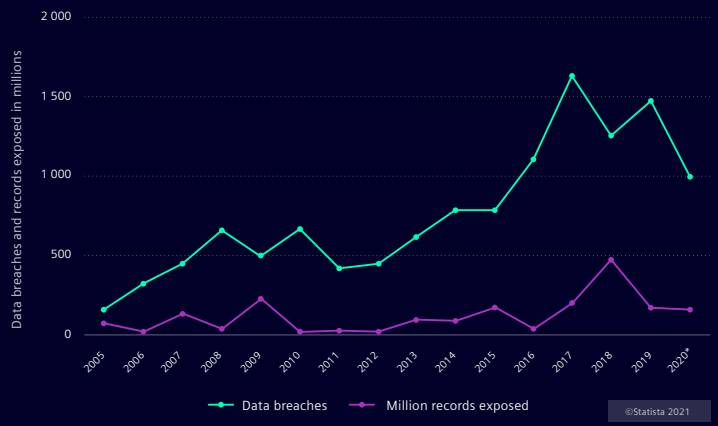


Figure1. Annual number of data breaches and exposed records in the United States from 2005 to 2020

Manufacturers are a target due to "the relatively slow rate of adoption of technologies and processes resulting from Industry 4.0," according to **Security Magazine**.

"Businesses that don't have the systems and technology can't see what is happening within their own plant floors and supply chains. Without this visibility, business decisions are based on speculation, not data – cutting manufacturers off at the knees when it comes to being accurate, forecasting future needs, or mitigating customer and supply chain risk." While legacy systems may fulfill basic production requirements, they can be limited in cybersecurity functionality.

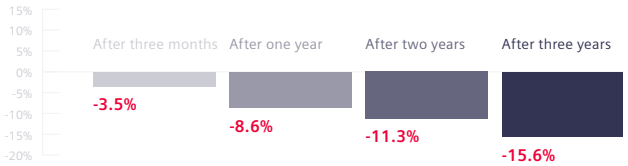
Legacy systems are common and often a weak point in manufacturing facilities.

COVID-19 has made protecting your systems even more complex. Working from home means employees may not have the safest systems or practices in place. Manufacturers are increasingly utilizing remote network access solutions to monitor or troubleshoot operational equipment, while in-person tasks are limited. Cybercriminals often target employees through phishing to infiltrate systems, due to a lack of training or adherence to cybersecurity practices at a personnel level.

A breach will sink your **shareholder value**

A data breach seriously impacts any organization. The damage incurred to a company's reputation can last years. According to Paul Bischoff at Comparitech, **shareholder value will continue to drop each year, due to lack of investor trust.**

According to Comparitech, this is the average share price decrease over time following a data breach:



Market leaders and Fortune 500 companies from multiple vertical industries were included in the Comparitech study.

On average, companies that suffered breaches since 2017 saw their stock performance bottom out 100 days after disclosure. This is a stronger negative reaction to breaches than the stock changes that occurred to companies attacked in the mid-2010s.

Shareholders have high expectations and they are becoming less forgiving of cyberattacks, not more.

Cyber incidents result in **production downtime**

Manufacturing operations combine OT control systems and IT systems with the internet. This makes it easier for cybercriminals to infiltrate the entire system infrastructure and sabotage operations. Mistakes can also happen from within. According to **MSSP Alert**, "Employee errors cause 52% of all [industrial cybersecurity] incidents."

After successfully identifying a security breach, your company will have to find out the extent of the breach and what systems were affected. That could mean entire manufacturing operations must be shut down until a full diagnostic of the situation can be executed, which could cause weeks or months of production downtime. Who will end up paying the cost of that downtime? And what is that cost?

> The average cost of ransomware-associated downtime is now 94% more than in 2019. "
>
> – Continuity Central

What **could happen**

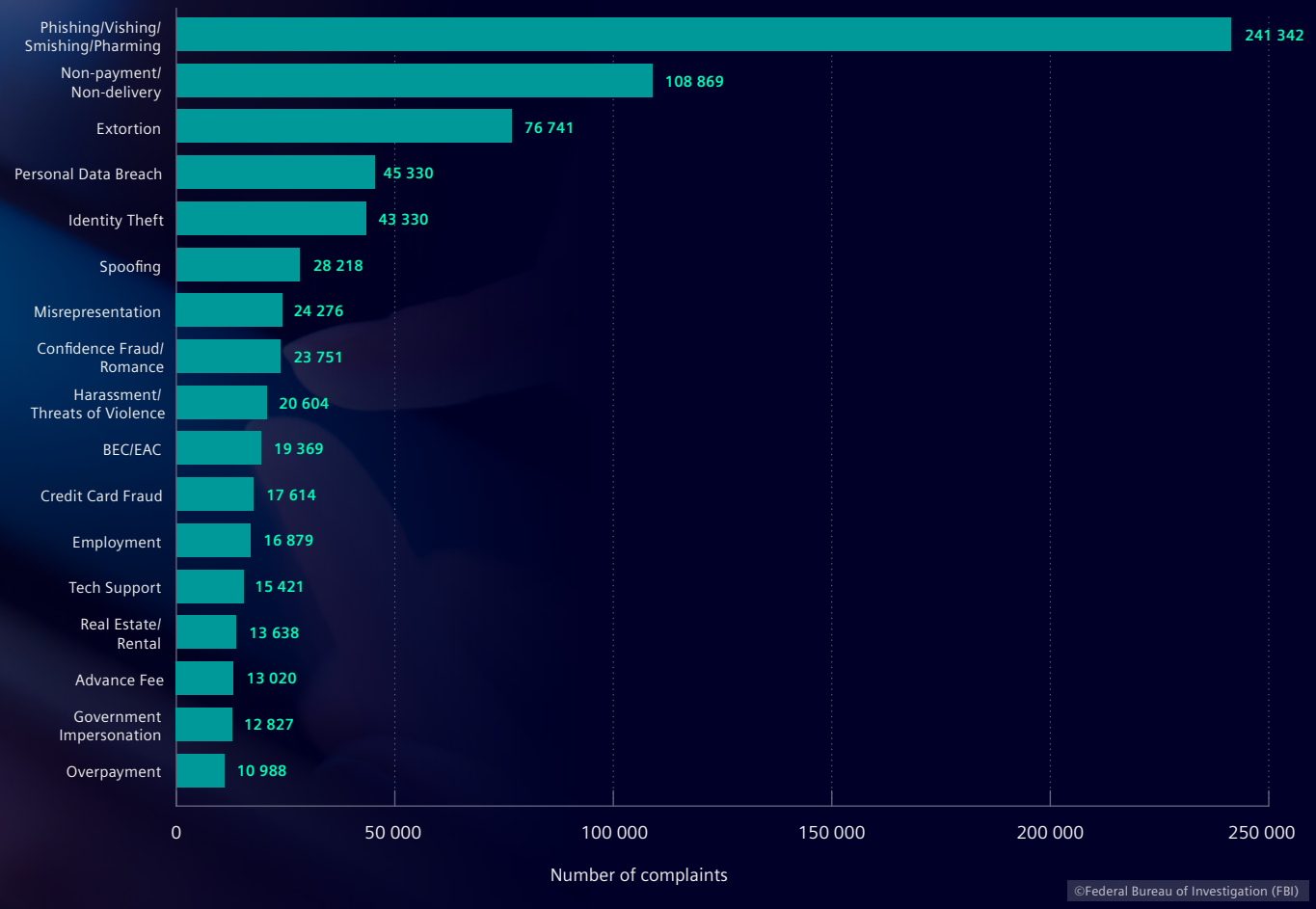


Figure 2. Types of cybercrime most frequently reported in 2020

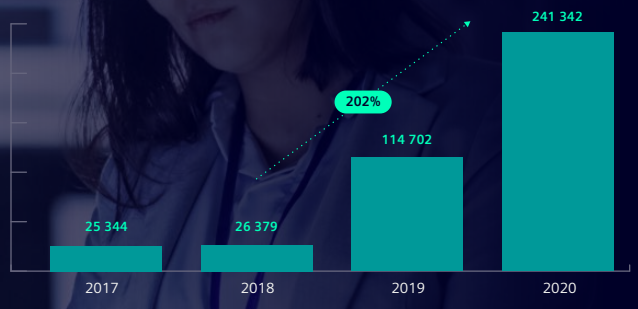


Figure 3. IC3 Complaint Statistics 2020 - Phishing/Vishing/Smishing/Pharming Comparison Last Four Years

Phishing

Phishing attacks are the most common and fastest growing cybercrime according to the FBI. Hackers use legitimate looking emails to trick individuals into clicking or opening malicious links or attachments. If safeguards are not in place, the cyberattacks can wreak havoc. Phishing is also very commonly used to deliver a ransomware strike.

"The manufacturing industry was the most targeted industry by phishing attempts (38.6%). In addition to phishing, manufacturing was the No. 1 target (26.5%) for browser exploits which allow attackers to take advantage of vulnerabilities in operating systems and change users' browser settings without their knowledge."

– Peter Fretty, IndustryWeek

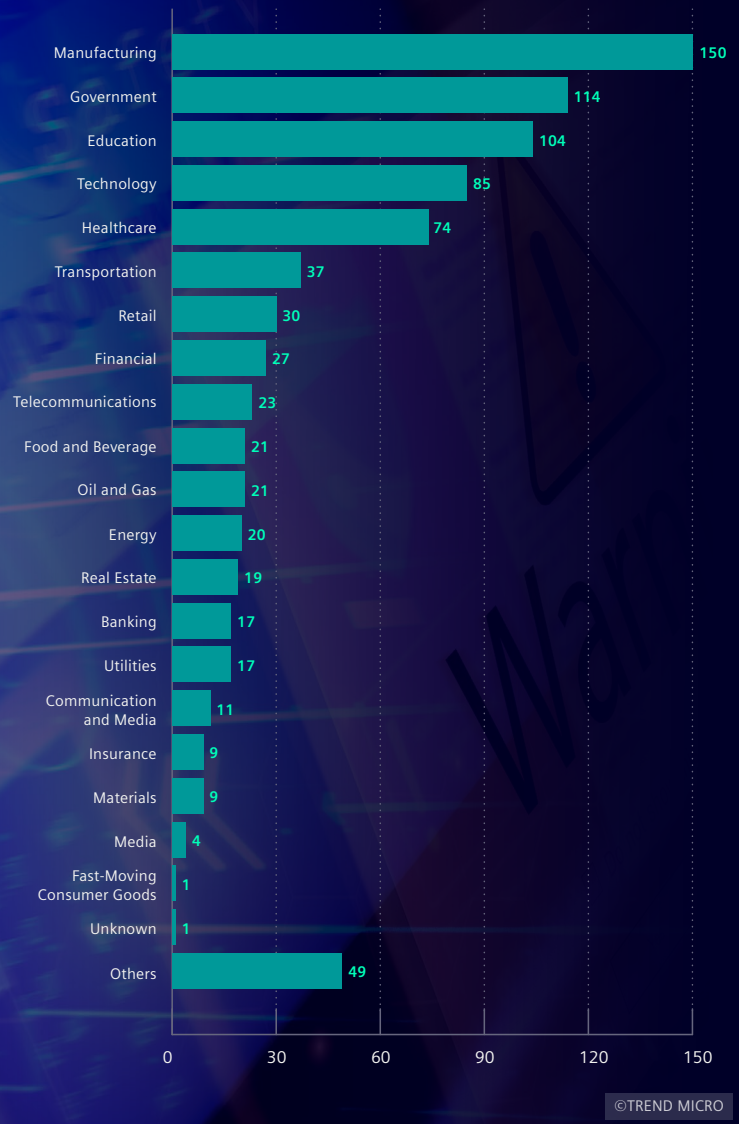


Figure 4. Industries affected by ransomware in Q3 of 2020 (data from Smart Protection Network)

Ransomware

"Ransomware threats have disrupted the manufacturing industry significantly in 2020. These attacks have resulted in substantial losses in production and disjointed operations. In a disturbing trend during the third quarter of the year, attackers appeared to be singling out manufacturing organizations as a victim of choice in their ransomware operations."

– TrendMicro

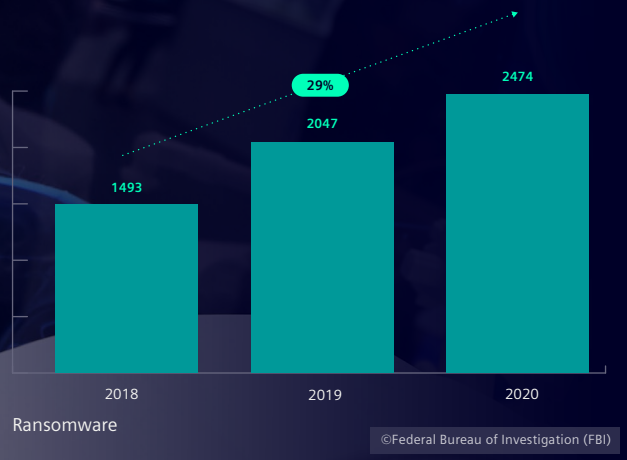


Figure 5. Last 3 Year Complaint Count Comparison — Ransomware

"Ransomware has become a major threat to the manufacturing industry as cyber-criminal groups increasingly take an interest in targeting the industrial control systems (ICS) that manage operations."

– Danny Palmer, ZDNet

Cybercriminals access and encrypt systems and files of manufacturers, then demand ransoms in order to give back access and control of the plant. According to **Cybercrime Magazine**, hackers will attack businesses with ransomware every 11 seconds in 2021.

Peter Fretty from **IndustryWeek** clarifies why Steelcase, the world's largest office furniture manufacturer, was forced to halt global operations for roughly two weeks after a ransomware attack. Manufacturers can be easy targets, which he explains further.

> "The manufacturing industry is often the target of cyberattacks because (traditionally, at least) this industry was highly fragmented, with individual facilities each using different IT infrastructures and multiple disjointed systems... cybercriminals continue to exploit these holes."
>
> **– Peter Fretty, IndustryWeek**

To make matters worse, as working from home has become commonplace due to COVID-19, ransomware attacks have **increased by 148% since 2019.**

Your threat surface **has increased**

The interconnected nature of the manufacturing industry and the rate of digital innovation allow for increasingly far-reaching cybercrime. As factories, equipment, customers, and supply chains are interlinked, the impacts of cyberattacks grow exponentially.

This significantly expanded threat surface, otherwise known as the total sum of vulnerabilities in your enterprise, demands that manufacturers fundamentally change their perspective on addressing cybersecurity. It's not just an IT problem anymore.

COVID-19 has provided cybercriminals with the perfect environment in which to deploy an attack. With increased remote access to plant facilities, as more employees work from home, hackers can much more easily take advantage of system vulnerabilities and access infrastructure. As hackers gain more opportunities, business leaders must evaluate their security risks. Implications of compromised IIoT devices include not just downtime, but also damaged machinery and facilities, which could lead to catastrophic machinery failure or worse.

> By 2025, forecasts suggest that there will be more than 75 billion Internet of Things (IoT) connected devices in use."
>
> – Statista

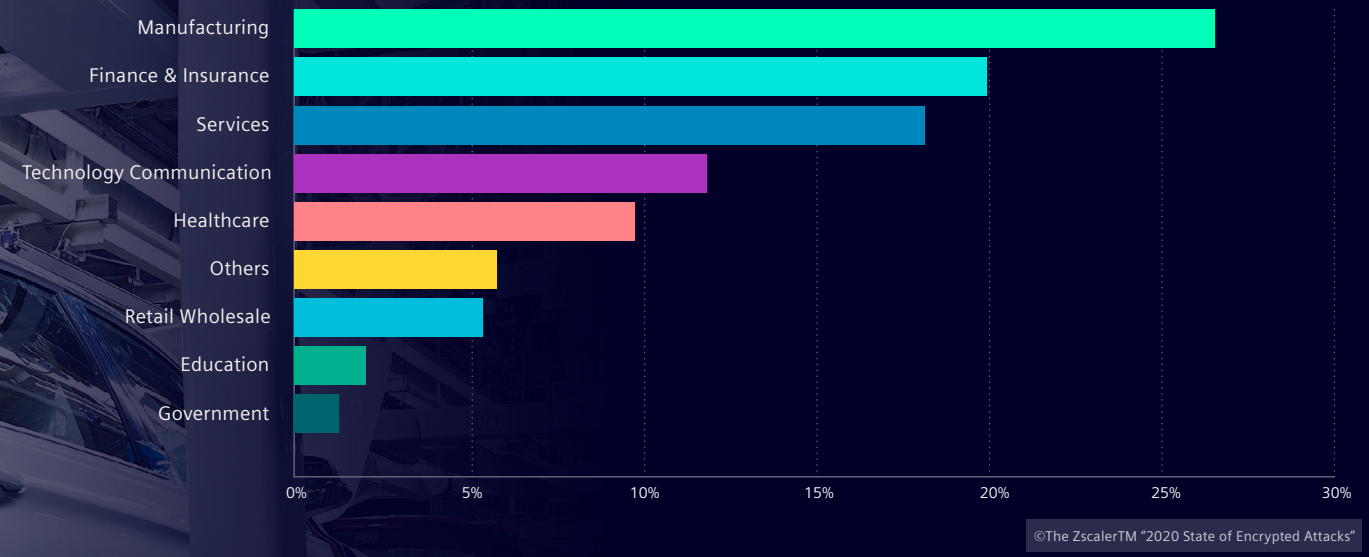


Figure 6. Browser exploits blocked over encrypted channels by industry

"A lot of OT networks are connected through a remote access solution, and many people do not understand how critical and insecure remote access tools can be,"

– Sharon Brizinov, security researcher

In February 2019, Toyota Australia became aware of a **cyberattack** when its email and other systems went down. It was reported that staff was sent home and told to communicate via phone and face-to-face meetings. Five weeks later, the manufacturer **revealed** that its branches in Thailand and Vietnam detected an unauthorized access of their IT systems, as well as other data breaches at Toyota and Lexus dealers in Japan. During this incident, cybercriminals accessed data from 3.1 million customers, including names, dates of birth and employment information. The company did not disclose further information regarding the hackers' ransom demands.

In one simple attack, the manufacturer suffered a data breach and fell victim to a ransomware threat. This incident underlines the need for continuous monitoring.

Cybersecurity **best practices**

Cybersecurity aims to evaluate system integrity, organizational maturity, and vulnerabilities in system design, firmware, software, hardware, policies, and procedures, in order to effectively safeguard the assets and people that allow for business continuity and core functions. Security by design should be deployed in a holistic manner to ensure that all functions of the business are secure and protected. The plant floor should be secured from cyber-intrusions originating from anywhere, including the IT network. Yet most manufacturers fail to comprehend that in order to ensure total system security, **cybersecurity activities require collaboration between IT and OT departments and an OT specific cybersecurity program**.

A considerable amount of cyberattacks are linked to **human error** and lack of risk awareness. Implementing cybersecurity awareness training is paramount to ensure the welfare of your business. **Employees are your biggest risk** when it comes to cyberattacks, and cybersecurity awareness training is proven to help reduce both system vulnerabilities and attack opportunities.

> 95% of all cyber incidents are human-enabled."
>
> – ResearchGate

The public relations side to when you're attacked

First off, **don't panic**. While that's easy to say, it's a bit harder to do. Panicking leads to fear, and fear leads to bad choices. Companies occasionally react to cyberattacks by trying to hide them from the public. Such strategies, which intend to reduce the organization's public shame, usually lead to worse consequences. Studies show that **shareholder values decrease more when organizations are not honest and transparent after an attack**.

Aside from production downtime losses, a cyberattack can incur many other types of costs, such as:

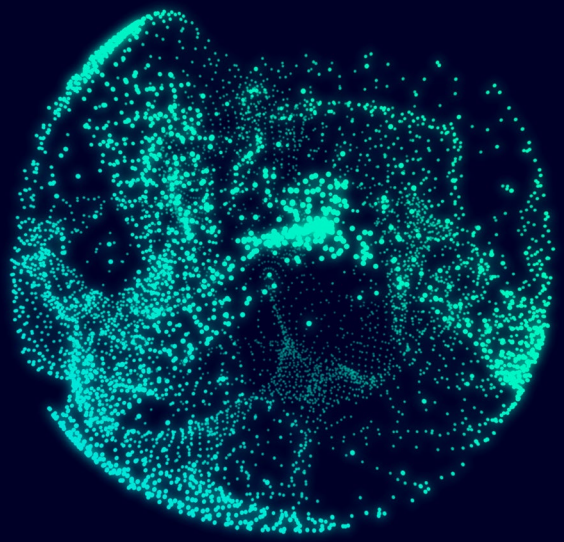
- **Fines**
- **Legal expenses**
- **Lost revenue**
- **Brand damage**
- **Cyber forensics**
- **Credit rating downgrade**
- **Decreased market value**
- **Lower moral**
- **Higher employee turnover**
- **Damaged supplier relationships**
- **Disappointed customers**

When faced with a cyberattack or data breach, you are running against the clock. After an attack is identified, manufacturers must undergo a full system diagnostic in order to identify the source, fix the vulnerability, assess the impact and reach, and secure the network by fighting off the attack. This can take weeks, or even months.

Outbrain gives a great example of how to communicate a breach in **the "Hackers of the Savior" attack**:

- **Announce the attack immediately**
- **List what you are doing to fix the breach**, and the expected timeline
- **Explain the consequences**—e.g., this affected X but not Y
- **Follow up with reports of what you've fixed**
- When it's resolved, **explain at a high level the changes put in place to ensure it won't happen again**

The best form of defense is to be prepared.
How do you know you are doing everything you can to prevent an attack?



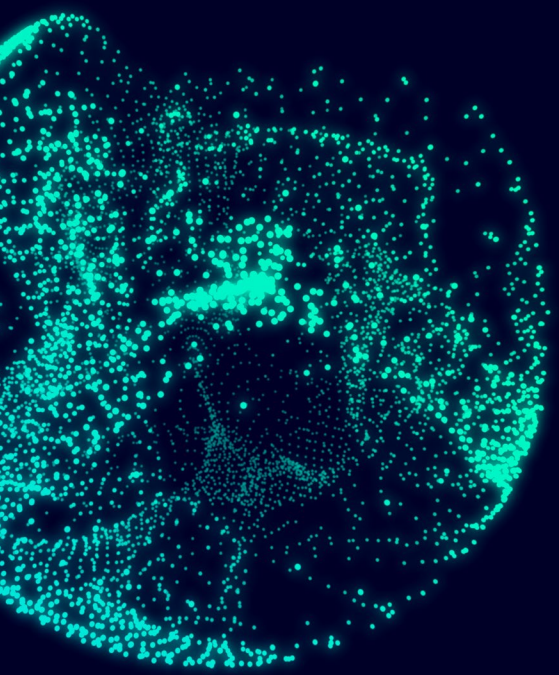
Why **Siemens?**

Siemens recognized early on that cybersecurity would be integral to the digital revolution. For example, the Industrial Internet of Things (IIoT) would be inconceivable without cybersecurity. Our customers want advanced digitalization. But without protection against cybercrime, sabotage or accidental manipulation, innovative digital solutions are at risk.

This means that "without trust, the digital revolution won't work," explains Stefan Jost-Dummer, Siemens Cybersecurity Chief of Staff. The way machines talk to each other makes the future of manufacturing possible. Software and connectivity inform and govern Operational Technologies. That's why Siemens has committed to prioritizing industrial cybersecurity at the highest levels. At the 2018 Munich Security Conference, Siemens and eight industry partners signed the first joint charter for greater cybersecurity. Initiated by Siemens, the Charter of Trust calls for binding rules and standards to build trust in cybersecurity and further advance digitalization.

Siemens has a demonstrated record of developing leading-edge cybersecurity solutions and providing expert cybersecurity services both around the globe and in the U.S, which adhere to strict industry-accepted industrial cybersecurity standards, like IEC 62443 and NIST.

> "The Industrial Internet of Things (IIoT) would be inconceivable without cybersecurity."
>
> **– Roland Busch, Siemens**



Siemens' dedicated and certified industrial cybersecurity experts average more than 10 years of OT network experience and would be happy to discuss your cybersecurity goals. **Just send a note to the e-mail address below or call the number.**

Let's **talk**

Your approach to industrial cybersecurity may already rely on Siemens' expertise, experience and our approach to Defense in Depth, along with our proven strategies, software and industrial hardware platforms.

Alternatively, you may be focusing on cybersecurity for your food and beverage manufacturing operation for the first time. In either case, a dialogue with a trusted advisor about your ongoing industrial cybersecurity needs should be on your to-do list.

Contact our cybersecurity core team for a conversation on how to protect your brand, your business, your manufacturing processes and your OT networks.

Chuck Tommey, GICSP, CEH, P.E.
IT/OT Networking Consultant
Cyber | Architecture | Digitalization
Siemens Digital Industries
Mobile: +1 (704) 707-6584
Email: chuck.tommey@siemens.com