Brown & Brown

PROPERTY & CASUALTY

Manufacturing Giant Faces Cyberattack

OT Impacts and Considerations

By Salman Ansari

In today's digital age, even industry giants are vulnerable to cyberattacks. In 2023, a major household goods manufacturer faced a cybersecurity incident that disrupted operations, highlighting the critical need for robust digital infrastructure protection, especially within manufacturing and operational technology (OT) systems.

Company X isn't alone. These ongoing attacks serve as a reminder of the heightened vulnerability of manufacturing and OT systems. From toy companies, travel organizations and major household names, what makes manufacturers such attractive targets for cybercriminals?

- **Interconnected systems:** Modern factories rely on a mix of old and new machinery, often with interconnected IT and OT systems. This complexity creates vulnerabilities attackers can exploit, potentially halting production.
- **Valuable data:** From product designs and blueprints to customer information and supply chain details, manufacturers hold a wealth of valuable data. This data can be stolen for industrial espionage or held for ransom, creating a significant financial burden.
- **Global economic impact:** Cybercriminals know that disrupting production for even a short period can have a ripple effect throughout the supply chain.

In the aftermath of the attack, Company X reacted swiftly, isolating affected systems to prevent further damage. Recognizing the severity, they engaged law enforcement and activated business continuity plans. This likely involved a shift to manual administration and communication processes, which was a necessary sacrifice to help mitigate the fallout.

Reports suggest the attack might have involved ransomware, potentially explaining the significant financial impact. Early estimates indicate losses exceeding $400 million, with a large portion likely attributed to the following factors:

- **Production slowdowns:** compromised systems likely impact production scheduling, leading to delays and hindering output
- **Supply chain disruptions:** disruptions in OT systems could affect communication and coordination with suppliers, impacting the flow of raw materials and finished goods
- **Inventory management issues:** inefficiencies could hamper inventory control, potentially leading to stock inconsistencies and shortages

Company X reportedly incurred nearly $50 million in breach-related costs by the end of 2023 and expects additional costs in 2024. Below is a potential breakdown of the breach-related Company X might have faced:

- Direct Costs:
  - Remediation efforts (IT restoration, forensics)
  - Third-party consultant fees
  - Legal and compliance expenses
- Indirect Costs:
  - Lost sales due to production slowdowns and product shortages
  - Reputational damage

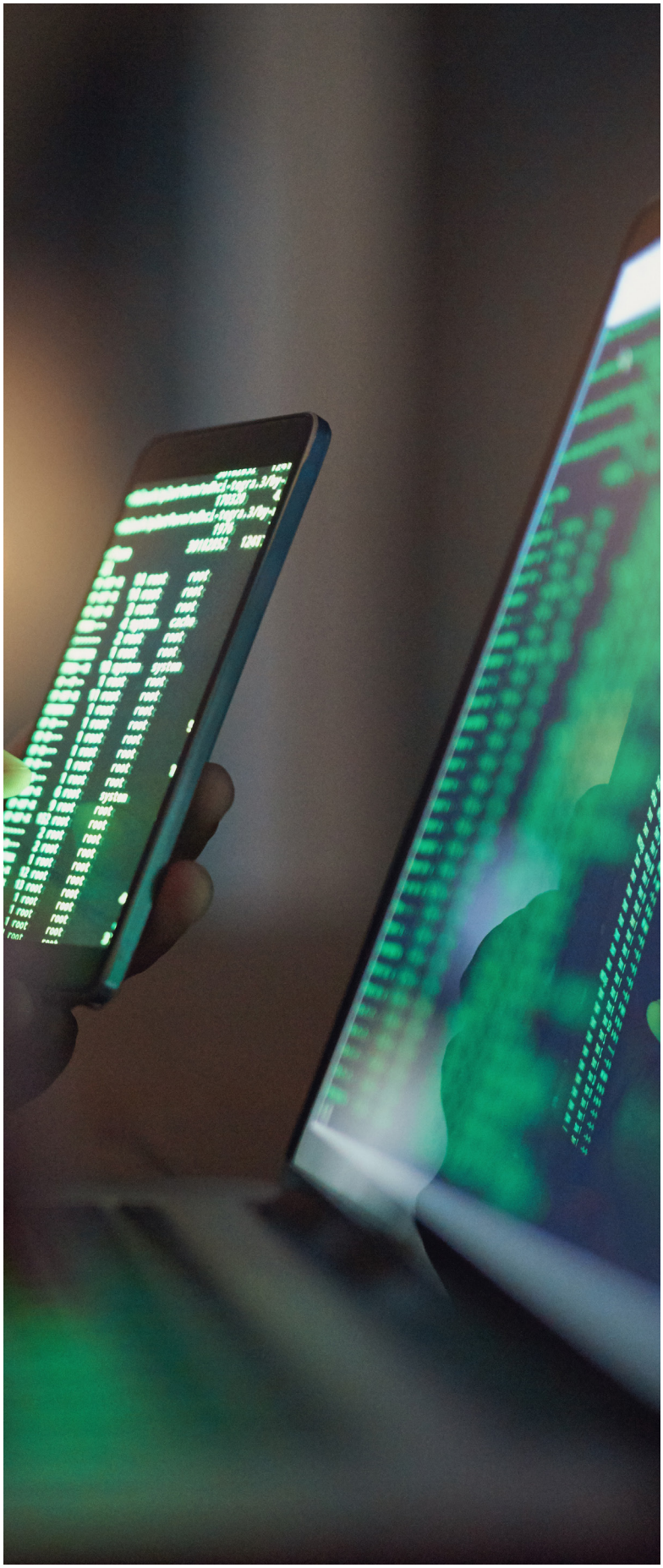
Like fortifying a complex machine, there are ways to make your manufacturing operations less vulnerable. Below are some key components of a robust cybersecurity strategy.

- **Regular security assessments:** These are like routine maintenance checks, identifying system weaknesses before attackers exploit them.
- **Network segmentation:** Separate your IT and OT systems, creating firewalls to isolate potential breaches and prevent widespread disruption.
- **Employee training:** Educate your employees on cybersecurity best practices, making them aware of phishing attempts and suspicious activity. They are your frontline defense against social engineering attacks.

In the fast-paced manufacturing world, even a minor security breach can be a catastrophic system failure.

By taking a proactive approach to cybersecurity, manufacturers can help their operations run smoothly, protect their data, and avoid production delays.

At Brown & Brown, we understand the unique challenges manufacturers face in the cyber world. Our Advanced Risk Quantification process, utilizing Cyber In-Site™, helps companies model potential cyber breaches and their financial impact. Think of it as a stress test for your complex machine, identifying potential weak points before they cause a breakdown.



How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.

Brown & Brown

Find Your Solution at BBrown.com