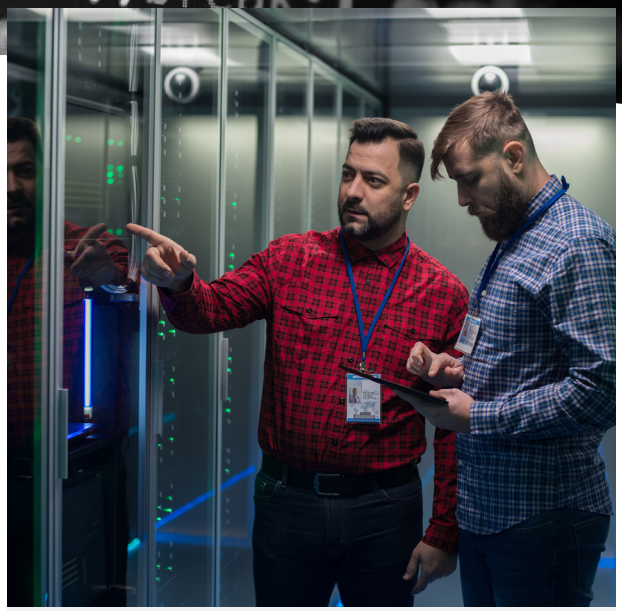
CYBERSAFE CASE STUDY **MANUFACTURING**

CEO Asks Cybersafe To Assess His Company's Network Security Practices



A breach can cost manufacturing companies hundreds of thousands of dollars a day just by shutting down their production. Our client wanted to learn how they could improve their overall security posture.

THE CHALLENGE

Cybersafe Solutions met with the CEO of a $50-million-a-year manufacturing company because he realized the severity of potential ransomware threats. In this case, our client understood that if a cyberattack affected the business, then it would be his name, reputation, and career on the line and not his IT staff.

The challenge was simple: This company had no policies, procedures, or understanding as to what the network looked like from a cybersecurity standpoint. It had recently upgraded its network to next-generation firewalls and antivirus software, but the company lacked the visibility to determine what was resident in its network and running on its endpoints. It also lacked asset inventory controls to identify installed third-party applications and any unpatched vulnerabilities. Lastly, the company had no way of determining whether its network perimeter was exposed to the outside world.

This lack of visibility left a major security hole in the network. The company was concerned about the threat of ransomware and maintaining day-to-day operations: utilizing robotics, providing shipments, and receiving orders, all of which could be disrupted during a data breach. Production would be completely shut down, costing the company hundreds of thousands of dollars per day, not to mention damaging its reputation.

OUR SOLUTION

The multi-step solution started immediately with a compromise and risk assessment:

- We examined the company's IT endpoints—desktops, laptops, and servers—and interrogated them for signs of compromise and other suspicious code.
- We checked for the presence of persistence mechanisms used to maintain system access across reboots.
- We examined volatile memory for signs of manipulation and/or hidden processes.
- We identified disabled security controls such as anti-virus programs and Windows Defender.
- We verified that critical operating system files were unaltered.
- We identified unauthorized or unwanted remote access tools.
- We provided a detailed report that gave the company's IT team a plan of action to tighten up security.
- We documented the appropriate steps for mitigating the risk for a breach.

Once we completed the compromise and risk assessment, we worked with IT and the executive team to develop a set of security policies and procedures, a written, living document that states how the company plans to protect the company's digital assets and is updated as technology and employee requirements change.

CONTINUED →

CYBERSAFE SOLUTIONS®

CYBERSAFE CASE STUDY **MANUFACTURING**

STEPS TAKEN TO IMPROVE CYBERSECURITY

1. Run a Compromise & Risk Assessment

2. Develop living document of security policies & procedures

3. Designate a security officer

4. Implement Real-time Network & Endpoint Security Monitoring

5. Introduce security awareness training & phishing tests

OUR SOLUTION (CONTINUED)

As part of this plan, a designated security officer was named. This particular organization was required to have a designated security officer in place who was responsible for coordinating and implementing the security program throughout the organization.

We also implemented real-time network and endpoint security monitoring to detect, respond to, and contain threats. With this monitoring, our team of cyber experts can identify attackers and their victims, methods, and intents. Monitoring also adds an internal layer of protection against cloud threats and insight into external threat vectors. Without monitoring, there is no way to prove who is responsible for an attack, who got in, and how to prevent it from happening again.

Last but not least, we introduced security awareness training and phishing tests, because the human factor is the weakest link in the security chain. All employees need to be aware of their roles and responsibilities when it comes to security.

All users now have ongoing security awareness training to protect against social engineering attacks and to reduce the risk of end-users clicking on phishing emails.

ASSESSMENT & RESULTS

During the compromise and risk assessment, we found several machines with hacking tools, missing security patches on domain controllers, an unsecured communication protocol, open ports with outbound connections to the internet, weak patch management, and, oddly enough, a misconfiguration in the newly installed firewalls.

If these issues were not discovered at the time we were evaluating the network, then our client very well could have been a victim of some sort of ransomware attack. We worked with the company's IT team to remove, update, and correct all of these issues expeditiously, and implement both our aforementioned network and endpoint security monitoring services.

Now that the organization has worked with a team of cybersecurity experts to improve its overall security posture, the board of directors and CEO can spend more time focusing on the core part of their business.

CYBERSAFE SOLUTIONS®