Facts of the case:

Some attackers used ransomware to shut off one of the Cheddar factory's temperature control systems for two minutes and also claimed to have accessed cheese recipes. Cheddar had wired $49,999 to attackers and asked a consultant to do a risk assessment.

Additional facts:

- In the early 2000s, CEO Chad sank massive amounts of capital into a fully digital, precision-controlled factory. With the savings afforded by the digital infrastructure, the company scaled up nationally.
- Cheddar has spent $6 million on the security system.
- The control systems are networked, and Cheddar can get alerts if something is out of whack. Anyone with a login can access it. Tech had given the login to 2-3 people and logged in from his hotel when he was on vacation.
- If someone has access and shuts the thermization tanks down, it may cause listeria bad, a public health catastrophe.
- Consultant had found four pathways into the network that no one knew about. One system had been compromised by a bot. Another could give hackers access to the industrial control systems.

Direct causes:

Cheddar's temperature control systems were compromised by ransomware.

Root causes:

From the case, we can't know exactly how hackers attack Cheddar's systems. But we can infer what may have caused this event from the information.

Cheddar enjoys the savings and benefits their digital systems generate and bring. Although Cheddar leaders knew they needed security, they just wanted to purchase more technologies to solve the problem and ignored human and process vulnerabilities. Cheddar spent much money on security systems, but their employees and processes can still give hackers access. A 5 Whys analysis was used and is provided below.

- Fact: Cheddar's temperature control systems were compromised by ransomware.
- 1why: attackers find a way to access the system and load the ransomware on control systems
- 2why (potential): attackers may get the login account and password.
- 3why(potential): the tech personnel leaked the password when he logged in to the system in the hotel, or others who have had access leaked the login. There are no password controls or authentication controls in Cheddar.
- 4why: Employees are not aware of possible threats and attacks. Security measures are complex, expensive, and ineffective.

- 5why: Cheddar almost put everything online for convenience and savings. Cheddar leaders just focused on security technologies but ignored human and process vulnerabilities. They didn't realize technologies, humans, and processes could both be threats.

Alternative courses of action:

1. Improve security training and awareness programs among the whole company. Cheddar should notify its employees that every mistake in the system can cause a severe public health problem. Employees shouldn't log in to the system on an unknown network, and they're responsible when they give login accounts to others.

- Risks: The company's culture change is difficult. It needs time and may affect the working efficiency.
- Advantage: After this incident, everyone should learn the importance of security. It would be easier to educate employees when they know why security education is necessary.
- Return: alert employees can prevent most social engineering attack vectors. In addition, people with security awareness will implement processes and use technologies in a safe way.

2. Draft or improve security policies. Execute security policy and password policy in practice. We cannot know the exact security policies of Cheddar from the case. But they probably don't apply 2FA verification and VPN and don't implement risk assessment regularly.

- Risk: The security process may change employees' original patterns, decreasing their excitement and commitment.
- Advantage: Cheddar has invested much in security systems, so they may not need to spend much more additional expense on executing policies.
- Return: A security process can provide the Cheddar with the maximum resistance and the fastest response to the attack.

3. Follow the advice from the consultant. Take the thermization process offline right away and have people monitor the system when it's in use. Remove the networked temperature controls and the automated temperature adjustments. Or keep them but have people do the monitoring. Take the recipes offline.

- Risk: This will put the company's digital efforts in vain, which may disappoint stakeholders. It will raise costs all over — quality control, personnel, and maintenance.
- Advantage: Cheddar developed from a non-digital situation. They have experience.
- Return: offline can make Cheddar monitor and control product quality entirely. They don't need to worry about the health problem and recipes leak caused by cyberattacks.

4. Add a modest capital investment, and patch what the consultant found. Take the most critical parts offline or backstop them with analog systems. Implement physical separation.

- Risk: The system still has the possibility of being breached. It needs time and professional security personnel to assess and implement the measures.
- Advantage: Cheddar doesn't need to make a huge unaffordable change.
- Returns: Cheddar can reduce the loss and retain the convenience of digital production systems.

5. Do nothing on the systems

- Risks: If nothing is done, there might be more attacks to Cheddar.
- Advantages: most systems have never failed. To some extend, the systems are security
- Returns: this alternative requires no expenditure of resources, time, etc.

Recommendation:

My recommendation is alternatives 1 and 2 are necessary, which can correct the root cause of people and process perspective. Because Cheddar has a security foundation, they can Assess their current situation and make improvements or additions.

Alternatives 3, 4, and 5 aim to solve the root cause of in technology perspective. Selection is mainly based on cost and return. Although we all want to make the system more secure, Cheddar must also consider the additional charges brought by the decision. Cheddar needs to assess costs and benefits. If the loss is unacceptable according to the consultant's suggestion (alternatives 3), consider the compromise (alternatives 4): take the critical system offline or physically isolate and patch the vulnerability. If the cost of compromise is also unacceptable, then they have no choice but occasionally wire $49,999 to hackers and pray for their "professional ethics." (alternatives 5)

Cheddar can choose anyone from alternatives 3, 4, or 5 and combine it with alternatives 1 and 2 for a more comprehensive solution. Both actions can occur simultaneously.

Implications

Financial. Additional funding may be needed to protect systems and implement a training program. The financial team also needs to estimate the cost and benefits of systems offline and online.

Human Resources. HR should consider onboarding/offboarding employees if Cheddar implements alternatives three or four. HR also needs to be involved in training and security clearance requirements, educational needs for professionals,

The tech team needs to assess how to patch the vulnerabilities. They also need to clarify who has the right to get access and who indeed has the access.

The senior leaders must report to investors about this incident and the next step plans.

Lessons Learned

From this case study, I learned that while automatic production brings convenience, it also increases risk. In fact, the more complex the system is, the higher the risk is.(Lemos, R, 2021) Every organization that is seeking a digital transformation should carefully adopt complex systems.

In addition, security is not guaranteed just by investing money in technology. Technologies need to combine with humans and processes to protect the systems entirely.

Assignment Case Study Questions:

What are the people, processes, or technology issues that require corrective action?

People issue: tech personnel can give login to others arbitrarily and don't record the share.

Process issue: People can log in to the system from outside networks like the hotel's Wi-Fi. There is no regular risk assessment in Cheddar.

Technology issue: there are four pathways into the network that no one knew about. One system had been compromised by a bot. Another could give hackers access to the industrial control systems.

Reference

Scott Berinato, Andy Bochman. (2018)Case Study: Protecting the Cheddar. Harvard Business Review.

Lemos, R. (2021). Overly Complex IT Infrastructures Pose Security Risk. Dark Reading. https://www.darkreading.com/operations/overly-complex-it-infrastructures-pose-security-risk