Facts of the case:

The Randcom intrusion involves 2 incidents: customers were lured by a fake website giving personal information and credit card information, and payroll employees opened an attachment hiding a keylogger malware from an internal attacker, which caused fund loss. Additional facts:

- Randcom's system was a hodge-podge of different platforms, software, and web services. There were legacy systems everywhere. What worked then was still in use, despite minor upgrades. The new software was band-aided to the legacy patchwork with some middleware, and the most advanced software was on the server side. Client-side applications were often outsourced with more emphasis on visual appeal at the presentation layer rather than ensuring resilience.
- Overemphasizing Randcom 2.0 had left Randcom's legacy systems unprotected.
- Randcom's executives barely championed cybersecurity as a part of the company culture. Randcom never educated its people on the dangers and risks to data as a corporate asset. Employee ignorance, phishing emails, and malware. Managers didn't care if employees shared passwords or left them written in the open. There was no clean desk policy. Employees could print any document and leave it in the open or copy it on USB devices.
- Randcom had rarely changed its processes in decades. There was no separation of duties. A payroll employee could also be assigned to help with building an employee benefits database with full access. Randcom interns were rotated across multiple departments, but their old access privileges were never deactivated.
- Randcom never implemented its cybersecurity process policy.
- Randcom didn't request password changes or data encryption.

After the attack, the Randcom security team looked at various web, access, and query logs to infer something that could shed more light on the two incidents. The CIO asked the executive team to schedule an urgent meeting and ask federal investigators for help. The company needed to face losing its customers, reputation, and credit rating.

Direct causes:

Customers and employees clicked the spoofed email.

Root causes:

Although one attacker did these two incidents, these two attacks could be seen as separate. Thus, I will clarify two root causes for each incident.

Firstly, the root cause why customers were lured by to a fake website is most users and staffs lacked awareness of security and the Randcom provided some unclear information which was used by the hacker. A 5 Whys analysis was used and is provided below.

- Fact: Customers' computers were compromised.
- 1why: Customers clicked the spoofed email.
- 2why: They couldn't identify if the email comes from the Randcom, so they believed they could purchase cheap Rand Card through the spoofed email.
- 3why: Customers are unaware of spoofed emails
- Random didn't give useful and detailed information in time. The Randcom only announced that the Rand Card would be available for purchase online in a few months but no exact time.
- 4why: The process and services of the Randcom focused more on availability and performance rather than security. They didn't realize all information and vulnerable could be used by hackers.
- 5why: Most leadership and staff in the Randcom did not attach importance to cybersecurity. They didn't implement training about security.

Secondly, the root cause of why the fund system was compromised was a combination of factors, including poor processes, inadequate technology, and ineffective people management. The Randcom failed to implement a security process, educate people and protect whole systems. A 5 Whys analysis was used and is provided below.

- Fact: The Randcom fund system was compromised
- 1why: Payroll employees clicked the spoofed email, so that hacker could obtain employee passwords and information in order to infiltrate the Randcom's system and siphon money from payroll
- 2why: The employee had not been trained on this poor security practice, payroll system is easy to be utilized by hacker
- 3 why: Payroll was a legacy system having limited protection, and there was no separation of duties in the Randcom processes.
- 4why: The CIO didn't have enough time and fund to revamp the entire architecture.
- 5why: Most leadership and staff in the Randcom did not attach importance to cybersecurity. They never implemented its cybersecurity process policy.

Alternative courses of action:

1. Improve security training and awareness programs among the whole company. Randcom needs to imbue a culture of prevention and accountability in its employees and customers. Everyone, including the board, IT team, customer services team, payroll team, and so on, must realize the importance of security and know common attack vectors.

- Risks: The company's culture change is difficult. It needs time and may delay product development.
- Advantage: After this incident, everyone should learn the importance of security, although the tuition was high. 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 technology in a safe way.

2. Execute security policy and password policy in practice. Implement Separation of Duties

and Least Privilege.

- Risk: The security process may change employees' original patterns, decreasing their excitement and commitment. Separation of Duties and Least Privilege is hard work. Randcome needs to clear every employee's current duty and expected duty. It may require an additional expense if Randcome needs to hire or fire some people.
- Advantage: There is already a security policy in the paper: predict, prevent, detect, and respond. The Randcome doesn't have to draft the policy from zero.
- Return: A security process can provide the Randcom with t the maximum resistance and the fastest response to the attack.

3. Every system must be scanned to ensure that there are no other malicious software, vulnerability, and back doors. After that, every system needs protection and continuous monitoring. In addition, All important data need to be encrypted.

- Risk: It will spend some money. It also needs time and may delay product development.
- Advantage: Randcom has a professional CIO, which can help the company protect its system correctly.
- Return: The systems are the ultimate targets of attack. A safe system and advanced technology will protect the data and assets of the Randcom.

4. Ask trusted and professional third-party organizations to protect the systems.

- Risk: the company needs to accept the threat from the third-party organization, which will spend much more money.
- Advantage: Generally, the protection from third-party will be quick. It can save time.
- Returns: This way can also protect the data and assets of the Randcom.

Recommendation:

My recommendation is alternatives one and two are essential and necessary, which can correct the root cause of people and process perspective. Alternatives three and four can both fix the root cause of in technology perspective. Randcom can choose one from alternatives three and four and combine it with alternatives one and two 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.

Human Resources. Possible employees change after Separation of Duties and Least Privilege

Product development and services delivery: possible change, redevelop, delay, or cancel.

Lessons Learned

From this case study, I learned that technology, processes, and people is three-headed

Janus for a company’s security. Each of them could be a threat to the company’s security. Most companies just focus on upgrading advanced technologies to protect them. However, a bad process or a thoughtless employee could make all technologies useless and cause serious consequences.

Assignment Case Study Questions:

People, processes, and technology failure points:

The people failure points at the Randcom include a lack of employee training and awareness, ineffective management of IT personnel, and a culture that did not prioritize IT security. The process failure points include inadequate IT security processes and a lack of incident response planning. The technology failure points include outdated and inadequate IT security technology and a lack of investment in security solutions.

Ethical dilemma

The ethical dilemma for the Randcom is the balancing act between greater public access and protecting consumer privacy. On the one hand, the company wants to provide access to its services to a wider audience, but on the other hand, it must protect the confidential data of its customers. The CEO is not unethical as the incidents were the result of systemic failures and not deliberate action on their part. However, the CEO does have a responsibility to ensure the protection of customer data and to implement the necessary measures to prevent future breaches.

Reference

Rooney, J. J., & Heuvel, L. N. V. (2004). Root Cause Analysis For Beginners. Quality Progress, 37(7), 45–53. https://ldh.la.gov/assets/medicaid/hss/docs/NH/RootCauseForBeginners.pdf

Serrat, Olivier. (2009). The Five Whys Technique. Asian Development Bank. https://hdl.handle.net/1813/87747