Incident Management & Fostering a Security-Aware Culture Report

Victor Onukwu

November 11, 2023

Table of Content

Incident Summary

An unauthorized individual recently breached our organization’s database, compromising sensitive customer data, including names, addresses, and social security numbers. This incident poses a significant risk to the privacy and security of the affected individuals and could potentially harm our organization’s reputation and trustworthiness.

To strengthen our security-aware culture and prevent such incidents in the future, I recommend implementing the following control strategies:
Regular security awareness training for all employees (AT-1, AT-2, AT-3)
Enforcing strict access control measures (AC-1, AC-2, AC-3)
Conducting regular incident response drills (IR-1, IR-2, IR-4).

I have also developed a comprehensive incident response plan that includes clear roles and responsibilities, communication protocols, escalation procedures, and coordination with external entities. By implementing these controls and strategies, we can foster a security-aware culture and be better prepared to prevent and respond to future security incidents

Introduction

In recent events, our organization experienced a significant security incident. An unauthorized individual managed to gain access to our database, compromising sensitive customer data. This included personal information such as names, addresses, and social security numbers. The incident not only poses a substantial risk to the privacy and security of our customers but also threatens the reputation and trustworthiness of our organization. In response to this, I have taken steps to address the issue and strengthen our security measures. This report will outline the details of the incident, its impact, and my recommended response in accordance with the NIST SP 800-53 framework. I have also provided practical suggestions for cultivating a stronger security-aware culture to mitigate future incidents and present a comprehensive incident response plan. Our goal is to ensure the highest level of security for our customers' data and maintain their trust in our organization.

Security-Aware Culture Recommendations

Awareness and Training (AT)

This involves implementing regular security awareness training for all employees. The training should cover the importance of security measures, how to recognize potential threats, and the correct actions to take when a threat is identified. It's crucial that this training is not a one-time event, but rather a continuous process that keeps up with the evolving threat landscape. This could include periodic refreshers, updates when new threats are identified, and additional training when systems or procedures change. The control codes related to this strategy include AT-1 (Security Awareness and Training Policy and Procedures), AT-2 (Security Awareness Training), and AT-3 (Role-Based Security Training)

Access Control (AC)

This involves enforcing strict access control measures. Access to sensitive information should be limited to only those who require it for their job functions. This principle, known as "least privilege", is a key aspect of access control. Additionally, implementing multi-factor authentication can provide an extra layer of security. This means that even if a user's credentials are compromised, an attacker would still need another form of identification to gain access. The control codes related to this strategy include AC-1 (Access Control Policy and Procedures), AC-2 (Account Management), and AC-3 (Access Enforcement)3

Incident Response (IR)

This involves regularly conducting incident response drills. These drills can help ensure that all employees know their roles and responsibilities during a security incident, and can respond effectively. The drills should simulate a variety of scenarios so that employees can experience how to respond to different types of incidents. After each drill, a review should be conducted to identify areas for improvement, and the incident response plan should be updated accordingly. The control codes related to this strategy include IR-1 (Incident Response Policy and Procedures), IR-2 (Incident Response Training), and IR-4 (Incident Handling)

Incident Response Plan

Roles and Responsibilities

Define clear roles and responsibilities for each team member during a security incident. This includes who is responsible for communicating with employees, who will liaise with law enforcement, and who will lead the technical response.

- Incident Response Team Leader: Oversees the response to ensure it is effective, pulling in necessary resources and stakeholders, and escalates as necessary.
- Security Analysts: Determine the severity of the incident, who the attackers were, what the vulnerabilities exploited were, and suggest the necessary measures to prevent future similar incidents.
- IT Operations: Assist in the containment and remediation of the incident, and in the analysis of the systems affected.
- Human Resources/Legal: If an employee is involved, they will need to be a part of the investigation. Legal can advise on the legal requirements for reporting the incident to affected customers and to regulatory bodies.

Communication Protocols

Establish clear communication protocols, including how to report an incident, who to report to, and how information about the incident should be disseminated.

- Internal Communication: Regular updates should be given to both the response team and to company leadership. All communication should be clear, concise, and free from jargon to ensure understanding.

- External Communication: The PR team should control all messages that are sent out of the organization to ensure a consistent message. Legal should be consulted on all external communications.

Escalation Procedures

Develop a clear escalation process for security incidents. This includes when to escalate, who to escalate to, and what actions should be taken at each escalation level.

- Evaluation: The incident response team leader, along with security analysts, evaluates the severity of the incident and decides whether to escalate it.
- Notification: If escalated, the senior management and, if necessary, the board of directors are notified. Other departments such as legal, HR, and PR may also need to be notified.
- Action: The necessary actions are taken to contain and remediate the incident, which could involve third-party specialists.

Coordination with External Entities

Identify when and how to engage external entities. This can include law enforcement, regulatory bodies, and third-party cybersecurity firms.

- Law Enforcement: In cases of serious incidents, law enforcement agencies will need to be contacted. This should be done as soon as it becomes apparent that it is necessary.
- Regulatory Reporting: Many industries have mandatory reporting requirements for security incidents. Legal should be involved in this process to ensure compliance.
- Customers: If customer data was compromised, they need to be informed. This should be done in a way that is clear and concise, and provides them with steps they can take to protect themselves.

Post-Incident Activities

After the incident has been handled, it’s important to conduct a post-incident review. This includes:

- Incident Documentation: Document all details of the incident, including how it was detected, the steps taken to respond, who was involved, and what systems or data were affected.
- Incident Analysis: Analyze the incident to understand how it occurred and why the security measures in place didn’t prevent it. This could involve a detailed technical analysis, as well as a review of the response process.

- Lessons Learned: Identify lessons learned from the incident and the response. What could have been done better? What changes need to be made to prevent similar incidents in the future?
- Implement Changes: Implement the necessary changes to the organization's security posture, policies, procedures, and/or infrastructure based on the findings from the analysis and lessons learned.
- Communication: Communicate the findings and changes to all relevant stakeholders. This could include employees, management, board members, and possibly customers (depending on the nature of the incident and the type of data affected).

Conclusion

In conclusion, the recent security incident has highlighted the importance of maintaining a robust security-aware culture within our organization. The unauthorized access to sensitive customer data is a serious concern, and immediate steps are being taken to address this issue. We are implementing regular security awareness training, enforcing strict access control measures, and conducting regular incident response drills. These measures, guided by the NIST SP 800-53 framework, will help us prevent such incidents in the future. Furthermore, we have developed a comprehensive incident response plan to ensure an effective and timely response to any future security incidents. This plan includes clear roles and responsibilities, communication protocols, escalation procedures, and coordination with external entities. By fostering a security-aware culture and being prepared for potential incidents, we aim to protect our customers' data and maintain their trust in our organization. We are committed to continuous improvement in our security posture and incident response capabilities.

References

National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53, Revision 5). https://doi.org/10.6028/NIST.SP.800-53r5

Security Boulevard. (2021, February 23). NIST SP 800-53: A Practical Guide to Compliance.
https://securityboulevard.com/2021/02/nist-sp-800-53-a-practical-guide-to-compliance/

NIST. (2013). IR-8: Incident Response Plan. In NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations. Retrieved from NIST SP 800-53 Rev. 4