https://chatgpt.com/share/67150e8f-2008-8006-9fb6-a361f3585d64

SMALL BUSINESS CYBERSECURITY CASE STUDY SERIES

Case 3

NATIONAL CYBERSECURITY ALLIANCE

Stolen Hospital Laptop Causes Heartburn

SCENARIO:

A health care system executive left their work-issued laptop, which had access to over 40,000 medical records, in a locked car while running an errand. The car was broken into, and the laptop stolen.

ATTACK:

Physical theft of an unencrypted device.

Encryption is the process of scrambling readable text so it can only be read by the person who has the decryption key. It creates an added layer of security for sensitive information.

RESPONSE:

The employee immediately reported the theft to the police and to the health care system's IT department who disabled the laptop's remote access and began monitoring activity. The laptop was equipped with security tools and password protection. Data stored on the hard drive was not encrypted – this included sensitive, personal patient data. The hospital had to follow state laws as they pertain to a data breach. The U.S. Department of Health and Human Services was also notified. Personally Identifiable Information (PII) and Protected Health Information (PHI) data require rigorous reporting processes and standards.

After the theft and breach, the health care system began an extensive review of internal policies; they created a discipline procedure for employees who violate security standards. A thorough review of security measures with internal IT staff and ancillary IT vendors revealed vulnerabilities.

IMPACT:

The health care system spent over $200,000 in remediation, monitoring, and operational improvements. A data breach does impact a brand negatively and trust has to be rebuilt.

LESSONS LEARNED:

1. Companies must establish and train employees on secure handling of work-issued devices.
2. Devices must be safely stored when not in the immediate presence of the employee.
3. Companies must take steps to encrypt data wherever it is stored or transmitted. Employees should have a clear understanding of the importance of encryption and how to use it.
4. Companies must understand and know their responsibilities under the data breach notification laws of the state(s) in which they operate.
5. A regular review of the company's security practices is imperative in modern organizations to prevent incidents, discover vulnerabilities, and to reduce impact of incidents.

DISCUSS:

- Knowing how the firm responded, what would you have done differently?
- What are some steps you think the firm could have taken to prevent this incident?
- Is your business susceptible to this kind of attack? How are you going to reduce your risk?

RESOURCES:

- NIST Small Business Cybersecurity Corner: https://www.nist.gov/itl/smallbusinesscyber
- National Cybersecurity Alliance: https://staysafeonline.org/cybersecure-business/

This resource, funded through NIST Federal Award 70NANB19H165, is intended to be used for general education purposes. The content of the case studies is a combination of publicly available information, business-submitted information, and fictional details to create an educational scenario.