CYBER INCIDENTS IN SMALL BUSINESSES

What You Can Learn From Their Experiences

It's a common misconception that small businesses are too small to become the target of cybercriminals and the dirty tricks they have up their sleeves. If you're a small business owner, you might even believe this myth yourself. Today, every company stores sensitive information on its IT system, making them targets regardless of how big or small they are.

This infographic shows you real-world examples of small businesses that have suffered cyberattacks and why having an incident response plan is so important.

The National Cyber Security Alliance's Case Studies

CASE STUDY 1

INCIDENT

A government contracting firm found out that an auction on the dark web was selling access to their business data, including their client database of military personnel.

This breach was a result of a phishing attack when a senior employee downloaded a malicious email attachment, believing it was from a trusted source.

RESPONSE

The IT team cut off communications to the vulnerable server and pulled the system offline to run network security scans and uncover any additional breaches. Also, each government agency that could be affected was alerted.

The company's leadership sought the help of a recognized cybersecurity forensics agency, aided by the U.S. Secret Service.

IMPACT

The company had to spend more than $1 million to mitigate the breach's impact on the business and operations were shut down for several days, disrupting business. The company even had to purchase new security software licenses and install a new server.[1]

CASE STUDY 2

INCIDENT

An employee used a company debit card at a local ATM in South America when a small team from a 10-person consulting firm was completing a client project there.

A month later, the company got overdraft alerts from its bank only to discover $13,000 in fake withdrawals in South America and a $1,000 overdraft fee.

Several false debit cards were manufactured and used at ATMs across South America by hackers who installed ATM skimmer devices to record card account credentials.

RESPONSE

The company informed their bank and closed the impacted account. Their attempts to get the bank to reimburse them were unsuccessful, so they cut off all ties with the bank.

A new bank promised them sophisticated anti-fraud safeguards. The corporation revised its travel policies, prohibiting the usage of company-issued debit cards. Employees can now electronically prepay expenses, pay cash or use a major credit card as needed.

IMPACT

Losses of almost $15,000 were incurred due to the firm's entire cash reserve being wiped out.[1]

CASE STUDY 3

INCIDENT

Upon discovering an ACH transfer of $10,000 being initiated by an unknown source, a construction company contacted their bank. It was identified that, in just one week, cybercriminals made six transfers worth $550,000 from the company's accounts by installing malware on the company's computers and capturing the banking credentials with a keylogger.

An employee opened an email he thought was from a materials supplier, but it really came from a phishing imposter account that contained malware.

RESPONSE

In the initial weeks, the bank was only able to recover $200,000 of the money stolen, leaving a $350,000 shortfall. To offset the fraudulent transfers, the bank pulled over $220,000 from the company's line of credit.

Due to a lack of cybersecurity planning, the company's response to the scam was delayed. Later, it hired a cybersecurity forensics agency to assist them in conducting a detailed cybersecurity analysis of their systems, determine the source of the event and recommend security software upgrades.

IMPACT

The company pursued legal action following the closure of the bank account to recover its losses. The remaining $350,000 was recovered with interest. However, no funds were received to cover the time and legal fees.[1]

What you can do

to protect your small business

- **Limit access** to sensitive accounts
- **Train your employees** on email security
- Ensure **best-in-class cybersecurity** measures
- Perform ongoing **vulnerability testing and risk assessments**
- Hire an **IT service provider**
- Build an **incident response plan**

What is an incident response plan?

A written set of guidelines to help your company detect and respond to security incidents. The plan is well-designed to mitigate security breaches, data loss and service interruptions, and to ensure the successful recovery of the affected system. With incident response plans, you can reduce security risks, downtime, and the financial and reputational consequences of a cyberattack.

When your organization can detect and respond more quickly to a security incident, the less of an impact it will have on your data, customer trust, reputation and revenue. **Consider partnering with an IT service provider like us** to implement a customized incident response plan for your organization.

Contact us today

for a no-obligation consultation

[1] Small Business Cybersecurity Case Study Series, NIST