KOPPINGER & ASSOCIATES

CASE STUDY Cyber Breach

The Importance of Cybersecurity Awareness and Training

THE COMPANY

Nationwide operation with over 5,000 dealers, white and blue-collar workers.

- 50 – 75 employees
- Multi-state locations

THE CHALLENGES

The client was concerned about cybersecurity and the number of cyber-attacks targeting the small business sector. They were also the victim of social engineering fraud resulting in a $4K cyber insurance policy claim after a cybercriminal planted trojans, malware, and ransomware through their email system. They also struggled to properly protect client information as they use an online ordering system.

- Properly protecting client information
- Lack of employee education and awareness of cyber security concerns
- The company was hit by a cybercriminal

THE SOLUTIONS

Over 82% of social engineering attacks are caused by human error; this shows the importance of incorporating cyber security awareness and training into company policy. Working together with the IT staff, we identified hardware, software, and process deficiencies. Working with leadership, we reviewed and made the client aware of their multi-state breach notification statutes and legal exposure. To improve their cybersecurity and limit further legal exposure, we helped the client set up and implement an employee cyber awareness training program. As part of the program, regularly scheduled training and testing is mandatory, and employees have access to online videos and training courses to learn about and stay current with cybersecurity issues.

- Reviewed a risk assessment application with the client's IT staff
- Helped client implement an employee cyber awareness training program
- Assisted client in setting up access to online videos and training courses

THE RESULTS

Employees have been trained how to recognize valid emails and potential security threats and how to respond appropriately. They are now on heightened awareness and have prevented a known attempt at social engineering in which a criminal requested a $10,000 wire transfer into a bogus bank account, saving the company another costly data breach. Their cybersecurity knowledge has increased, and the client has peace of mind knowing their company is developing a security-focused culture.

- Client has made changes to create a security-focused culture
- Programs have reduced human error
- Training has prevented an attempted cyber attack