Fox Rothschild

Building a Company Culture of

CYBER RESILIENCY

Fox Rothschild's Privacy & Data Security attorneys have created this helpful at-a-glance guide to supplement the information provided during the webinar.

Our program featured leading privacy and data security professionals who addressed how to effectively build a cyber-resilient company culture. The webinar stressed two overriding themes:

- The whole company — from the c-suite to front-line employees — needs to be cyber aware and play a role in developing a cyber-resilient culture.
- There is no one-size-fits-all approach! Companies should tailor their programs to their environment, industry and client base to implement meaningful and reasonable controls.

It truly takes a village to develop a robust and proactive environment for thwarting cyberattacks!

Types of Incidents Affecting Companies

A growing threat, **Ransomware** is an ever-changing form of malware designed to encrypt files on a device, rendering all files and the systems that rely on them unusable. Since 2016, over 4,000 ransomware attacks have been reported in the U.S. and ransomware remains the most prominent form of malware. In 2021, 37% of all businesses were hit by ransomware. Recovering from an attack cost businesses an average of $1.85 million. When hit by ransomware, 32% of victims pay the ransom and receive only 65% of their data back. Long gone are the days when you could easily thwart a ransomware attack. (Sources: Datto, 2019; Sophos 2021)

Phishing and **Wire Fraud** are also on the rise. Since COVID-19, such attacks have become their own pandemic and companies are losing billions of dollars each year as a result. It is critical that companies create a culture that incudes extensive communication and training regarding phishing detection. Having regular and increasingly sophisticated phishing exercises is extremely important, especially in the hybrid work environment.

Frameworks Companies Should Have in Place to Reduce Risk

Develop a roadmap that ensures cybersecurity controls are in place across all critical infrastructures and are tailored to your company's unique environment. Some of the key components include:

- Robust incident response plan and customizable business continuity plan to respond to zero-day or ransomware attacks. Test these on a regular basis at the executive level. Practice often – muscle memory is essential
- Stringent vulnerability management system
- Robust patch management policy to address issues as they occur
- Identify the company's crown jewels and determine when encryption is necessary
- Implement multiple protocols to identify users
- Segment access based on need and put additional security controls in place for domain administrators
- Third-party risk management, including having a cross functional team and outside counsel involved in reviewing vendor agreements; ensuring vendors pass cybersecurity questionnaires; have cyber insurance and continuously monitor their risk ratings. Evaluating vendors is a continuous process — it doesn't stop the day you sign the agreement — and buy-in on the risks of retaining certain vendors needs to escalate to the c-suite.
- Implement an employee communication and training program — employee buy-in is key

You're Only as Strong as Your Weakest Link – Employees are Critical to Cyber Resilience

A key component of developing a cyber resilient culture is to communicate and enforce this from the top down. The CEO and Board needs to continuously report on and reinforce the messaging through a mix of town halls, employee communications and trainings.

With a hybrid workforce, now more than ever, it is essential that employees understand their role in keeping the company secure. Key components of the plan should include:

- Securing employee buy-in. Network engineering is not intuitive and many think that IT has it covered. Understanding that they are the weakest link and play a vital role in thwarting cyber-attacks is critical.
- Share cyber dashboards in company meetings so employees understand the scale of attacks the company faces and their role in thwarting them.
- Build engagement and provide feedback to them when employees identify a phishing attack through a routine IT exercise.
- Continuous communication and training are key — sending out routine security reminders and phishing exercises to keep employees aware of their responsibilities in keeping the company's data and client's data secure.
- Provide additional training or even one-on one training if an employee routinely fails phishing exercises or cyber quizzes. Everyone learns differently, so use other tactics if an employee is struggling with module training.

Fox Rothschild

Employee Pushback – How to Deal With It From a Policy or Security Perspective

There has been a cultural shift over the past few years as companies no longer see cybersecurity as an IT-only issue. More companies are developing and enforcing a cyber risk management strategy from the top down. In addition, business and Privacy/IT professionals are cooperating to find middle ground — understanding employees' concerns while keeping the company safe. The key is to work together to find creative solutions to protect the company without disrupting business flow.

Hybrid Work Environment

With many employees working fully remote or hybrid, companies need to understand potential vulnerabilities and put structures and policies in place to govern them. Best practices for keeping the company secure in this evolving environment include:

Company-issued Laptops

Requiring the Use of VPN

To integrate employees into the network (if possible)

Mobile Device Management

Putting tools in place to keep these devices safe

Education

Explaining the reasons for these policies to employees

Mark G. McCreary, CIPP/US, CIPT
Co-Chair, Privacy & Data Security
215.299.2010 | mmcreary@foxrothschild.com

Copyright © December 2023 Fox Rothschild LLP | Attorney Advertising

Fox Rothschild