CYBERSECURITY
AWARENESS CULTURE

CYBERSECURITY IS NOT A TECHNOLOGY PROBLEM. IT'S A PEOPLE PROBLEM.

It's a common misconception that the greatest cyber risks exist outside your organization. However, internal risks are higher than ever before. According to a study by IBM, employees are responsible for 60% of cyber attacks on businesses due to accidental errors or by intentional fraud on the organization.

WHY IT'S IMPORTANT TO CREATE A CYBERSECURITY AWARENESS CULTURE

"When it comes to human factor, sensitive data suffers the most. Around nine-in-ten SMBs (88%) and enterprises (91%) that have experienced a data breach affecting the public cloud infrastructure they use, said social engineering was part of the attack" (Kaspersky Lab Report).

Social engineering (e.g., phishing emails) is a common method of cyberattacks. These highly-targeted attacks are on the rise and can appear to come from a legitimate source, like a company, co-worker, or financial institution. Phishing attempts can easily trick the targeted victim into clicking on a link or handing over confidential information.

Cyberattacks aimed at deceiving employees into relinquishing confidential information are preeminent threats to organizations today. That's why creating a cybersecurity awareness culture is imperative to your organization's security and overall prosperity.

WHAT DOES IT TAKE TO CREATE A CULTURE OF SECURITY?

Governance's Role in IT Security

A cybersecurity awareness culture starts with top leadership's attitude towards cybersecurity, which is critical for organizational buy-in. It is ultimately top leadership's responsibility to define corporate procedures on cybersecurity and develop a plan to educate and train all employees on cybersecurity policies.

It is critical that an organization's governance adopts a threat-based cybersecurity strategy and makes the right investments to mitigate identified vulnerabilities, thereby reducing their cyber liability. This can be done by:

- Defining corporate cross-functional procedures for cybersecurity
- Developing a plan to educate and train all departments on cybersecurity policies
- Staying committed to communicating the plan to all employees on a regular basis

EVERYONE is responsible for IT Security Controls

Enforcing a mandatory user awareness training program and providing educational resources can equip your employees to proactively identify cyber threats. It's not just the IT team or leadership's responsibility to know the risks and identify threats. ALL employees should understand their individual cybersecurity responsibilities.

Warren Averett
CPAs AND ADVISORS

Cybersecurity is a component of information security

Organizations should address all forms of data security when implementing policies and procedures and training employees.

It's important to note that information security encompasses cybersecurity, which means that it's the overall act of keeping data in all forms secure. The three basic principles of information security are often referred to by using the acronym CIA:

- Confidentiality – keeping data safe and secure
- Integrity – preventing data from being compromised or altered from its original state
- Availability – ensuring that data is readily available for authorized users to access when needed

On the other hand, cybersecurity is implemented through cyberspace and is the act of protecting sensitive information stored or accessed by the internet from a cyberattack. Information security is that act of protecting data not only from cyberspace threats, but also from threats that exist outside of the internet and should be considered in planning and procedures.

Mobile devices and apps are a primary threat vector in today's environment

If your organization has a bring-your-own-device policy in place without proper protocol and an advanced mobile device management (MDM) tool, you could be exposing your organization to threats.

From the unique operating and security features or device brands to the increasing malicious users focused on vulnerabilities and malware that target a mobile device's app store, maintaining an acceptable level of security for user devices is more important than ever. MDM tools are often cloud-based tools that function as an inventory system to track all mobile devices and serve as a hub to distribute security policies to the device, thus preventing access to company resources and protecting data.

CREATING A CYBERSECURITY AWARENESS CULTURE SHOULD BE THE GOAL OF ALL ORGANIZATIONS AIMING TO PROTECT DATA, EMPLOYEES, CUSTOMERS AND VENDOR RELATIONSHIPS.

While buy-in from leadership is the ultimate catalyst for the cultural shift, every employee should be educated on his or her personal role in keeping the organization's sensitive information secure. It is not the responsibility of just one person or department.

Warren Averett
CPAs AND ADVISORS