Count me in to WIN

swashlabs℠

Course Outline

The Risk Environment

Why Digital Risk Mitigation?

- Most organizations are ill-prepared for most current digital risks
- Many people equate “cybersecurity” with “network security”
- Incorrectly categorize or prioritize other forms of digital risk
- Most digital risks exploit behavior, not infrastructure
- Piecemeal or single-source solutions are inadequate
- All organizations are vulnerable to digital risk
- A behavioral approach can mitigate most personal digital risk

Basic, Big Picture Vulnerabilities

The biggest vulnerabilities in the current digital risk environment:

- Filesharing Access and Security
- Website Security
- Unsecured Wi-Fi Networks
- Malware and Phishing
- Device Security

FILESHARING

- People in small organizations often have access to shared drives and files they don't actually need
- Things are shared haphazardly out of a (perceived) need for expedience or on a “just in case” basis

WEBSITE SECURITY

- Small political organizations often have a website built by a friend or for free
- Websites built on a Content Management System like WordPress require active management, which means plugins and the CMS itself must be updated

UNSECURED WI-FI NETWORKS

- All unsecured Wi-Fi networks (home, office, hotel, coffee shop) carry the risk of device or data compromise
- Unsecured Wi-Fi connections out in public – at hotels, airports, and coffee shops – are much more risky

MALWARE AND PHISHING

- All devices and users may be compromised by malware, ransomware, advanced persistent threats, and phishing attacks
- Phishing is extremely common, and can be broadly targeted
- In rarer cases, a targeted phishing attack called spearphishing can occur

SECURITY UPDATES AND DEVICE SECURITY

- Security vulnerabilities in device operating systems and platforms have contributed significantly to many recent major security breaches

Types of Risks and Mitigation Techniques

Risk Type: Credentials Risk

The risk of having your login credentials compromised is, arguably, the most potentially problematic type of digital risk for an individual.

Your best path to avoiding credentials compromise as an individual or within a small organization includes the following:

- Using two-factor authentication
- Using a password manager
- Learning to recognize phishing attempts

TWO-FACTOR AUTHENTICATION

- Two factor authentication makes it harder for someone to actually complete a breach
- Text message is the most common form, and the easiest to use
- A more secure version requires an authenticator app, like Authy, or Google Auth
- The most secure method of two-factor authentication is the physical USB key

PASSWORD MANAGER

A password manager makes it easy to do the following:

- Change passwords regularly
- Use different passwords for every platform
- Use strong, complex passwords at all times.

Password managers like LastPass or 1Password act as an encrypted vault, keeping track of your passwords.

RECOGNIZE PHISHING ATTEMPTS

Phishing definition

“Phishing is an attempt by an outside party to gain access to login credentials or financial information by fraudulent means, specifically by impersonating a legitimate or trustworthy individual or institution and doing so via electronic communication.”

The most common method used to deliver this fake message is either by instant messaging or spoofed email, i.e. an email that looks like it comes from someone you know, or a trusted institution like a bank or enterprise software service provider, like Google or Microsoft.

Spearphishing

Spearphishing is the targeted version of Phishing, in which a specific organization or individual is targeted by malevolent external groups or individuals

Difference between hacking and phishing risks

Hacking is an intrusion by an external actor that makes use of relatively advanced techniques to gain unauthorized access to and/or control of a network or device.

Phishing is not hacking, and involves the unauthorized acquisition of and use of login credentials to gain improper, fraudulent access to a platform or system.

Risk Type: Malware Risk

Malware risk is what people tend to think of as cybersecurity. These are viruses, ransomware, spyware, and other threats that wreak havoc on your hardware and can compromise your data.

The best ways to guard against these malware threats are:

- Endpoint Security
- System Updates

ENDPOINT SECURITY

- Usually "anti-virus" or "malware scanning," but now also includes cloud backups and security, device encryption, and live, active threat tracking
- These include many paid and free varieties, and come from providers like Symantec, Norton, Trend Micro, Avira, and others
- When properly configured, these systems can locate, isolate, and neutralize malware before it can do much damage while, in some cases, also aiding in recovery

SYSTEM UPDATES

- Most system updates are initiated for security reasons, so you should always let everything update itself when it asks.

Risk Type: Access Control

SECURE FILE SHARING, STORAGE, AND ACCESS CONTROL

- Most organizations use Google Drive, Office 365, Dropbox, or a similar cloud-based file-sharing system to collaborate on documents and other files.
- If someone has a compromised email address, whoever has gained improper access to that email address now has access to everything shared to that account, including shared documents and drives.
- You should be thoughtful and intentional about who has access to which drives and files on your file-sharing system. That access should be regularly updated and audited.

VPN

- Everyone uses unsecured Wi-Fi networks, and the risks are significant
- A VPN encrypts what you're transmitting and provides a real layer of security against unwanted observation

Parting Thoughts and Best Practices Checklist

1. Doing some of this is better than doing none of it. Work in the pieces that are easy, practical, and possible to adopt first.
2. Do one thing at a time.
3. Don't check your email on autopilot - phishing and spearphishing attacks take advantage of cognitive laziness.
4. If you can, train your organization on these basics regularly.
5. Your cybersecurity and operations security posture should be: Proactive, Resolute, and Engaged.

For your reference and review, here are the 7 basic best practice steps to engaging in digital risk awareness, which will aid you in fostering both a new personal outlook and a proactive organizational culture that is geared towards digital risk mitigation.

Basic Best Practices:

○ Use two-factor authentication whenever possible, via text message, phone app, or physical USB key

○ Use a password manager

○ Use a VPN (or at least your personal mobile hotspot) for situations where you would be using public Wi-Fi

○ Implement an endpoint security solution for your devices, which may include Antivirus as well as a strong device password/locking method and automated backup where possible

○ Let your devices run system updates

○ Be intentional and vigilant about filesharing, storage, and access control, reviewing user access lists on a regular basis to remove privileges when no longer needed, and as part of the exit checklist when a project ends or an employee leaves

○ Learn to recognize phishing/hacking attempts