Cybersecurity Training: Who, What, When, Where, and Why

By Lisa Traina, Partner

There are many controls and safeguards organizations can — and should — put in place to reduce their risk of a cyber attack. One very vital tool in mitigating that risk is ongoing cybersecurity training.

The role employees and others with access to your network play in cybersecurity can’t be overstated. Just one click on one link in a malicious email or web page can lead to a major cybersecurity breach. Comprehensive, ongoing cybersecurity training is crucial to keeping your network users aware of current and emerging cyber risks and informed about how they can help protect your organization.

Let’s look at the who, what, when, where, and why of cybersecurity training.

Who

- Include all stakeholders. That means every employee and board member as well as any volunteers, members, and others with access to your network, including via Wi-Fi. Consider holding a special seminar for non-employees.
- Leadership involvement is key. A culture of security starts at the top. That means every member of your leadership team should attend the training, sit in the front row, and actively participate.
- Select the trainers carefully. It may seem like a member of your IT team would be the best choice to lead cybersecurity training, but that isn’t necessarily the case. IT personnel are often too busy working on the daily issues that crop up to focus on current threats and developments. They also might use “tech speak” that won’t be easily understood by the audience. Choose someone who understands the cyber risks and issues and has strong teaching and presenting skills.

What

- Keep the training simple and direct. Use clear language.
- Ensure attendees understand the important role they all play in protecting your organization. Stress that just one click can infect your whole system, and illustrate the point with real-life examples of breaches caused by an unsuspecting employee.
- Expect limited cyber vocabulary. Be sure to explain terms such as phishing, vulnerabilities, malware, and ransomware.
- Make sure attendees understand:
  - The importance of using strong passwords, not sharing them, and using different passwords for different accounts
  - Why they shouldn’t use email to exchange confidential or secure information
  - The dangers of visiting unsafe websites
  - The risks of using public Wi-Fi networks
- Discuss new threats, how they could affect your organization, and what to watch for.
- Provide real-world examples of cyber attacks and breaches.
- Consider conducting a phishing test beforehand, sharing the results during the training, and retesting a few weeks later. Some organizations reward those who pass the test with a pizza party or the option to wear jeans to work one day.

> The role employees and others with access to your network play in cybersecurity can’t be overstated.

When

- New threats emerge continually so it's important to hold training often, perhaps quarterly. Consider augmenting this by sharing quick tips on a monthly basis to help keep cybersecurity top of mind.
- Document attendance to make sure all employees receive training. Have an option for those who have to miss the session, such as a repeat date or recording.
- Make sure new employees receive cybersecurity training as part of the onboarding process, perhaps through a face-to-face meeting with your information security officer. New employee training should include:
    - Review of your organization's tech usage and cybersecurity policies
    - Information on current and emerging cyber risks

Where

- In-person training tends to be more effective at limiting phishing risks.
- A webinar can be a good option if attendees are in multiple locations or timing is a challenge. Be sure to stress the importance of watching the webinar.

Why

- We're all overloaded with too many emails, texts, and more. This can make it hard to spot warning signs or suspicious activity.
- Even with the best controls in place, humans are susceptible to phishing, social engineering, and other threats.
- New threats emerge constantly. Ongoing cybersecurity training is vital to keeping all your network users apprised of current threats.

CapinTech offers phishing tests and training that can be customized to meet your organization's needs. Contact us at capintech.com to learn more.

About the Author

Lisa Traina, Partner
CapinTech
ltraina@capincrouse.com
o 505.50.CAPIN ext. 2000

Lisa uses her more than 30 years of experience to assist organizations in implementing measures to secure data and manage risks efficiently and effectively. She is a nationally recognized speaker and author, and serves on the AICPA Cybersecurity Task Force. Lisa founded Traina & Associates in 1999 to provide IS security services to a broad range of industries. Traina & Associates joined CapinCrouse in January 2017 and is now CapinTech.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to nonprofit organizations, financial institutions, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessments, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.