BACK-TO-SCHOOL: Educating Your Team on Cybersecurity Best Practices

By: Josh Prager

As the school season kicks into gear, it's not just students who can use a refresher on best practices and critical information. For small and mid-size businesses, this time of year serves as a prime opportunity to educate and reinforce cybersecurity best practices within your team. With cyber threats evolving daily, it's crucial to ensure that your entire organization is well-versed in the latest security protocols. Here's a comprehensive guide to help you get started.

Cybersecurity 101: Why Education is Essential in Today's Digital Classroom

With increasing reliance on digital platforms for daily operations, the risk of cyber threats has escalated exponentially. Cyberattacks are not just a concern for large corporations; small and mid-size businesses are often prime targets due to perceived vulnerabilities. According to Verizon's 2024 Data Breach Investigations Report, small businesses (SMBs) accounted for 41.45 percent of all security incidents. Educating your employees on cybersecurity helps create a fortified frontline defense against these threats, minimizing potential damages.

ALMOST

42%

OF ALL CYBERSECURITY INCIDENTS HAPPEN TO SMALL BUSINESSES

SOURCE: VERIZON 2024 DATA BREACH INVESTIGATIONS REPORT

Human error played a part in 68 percent of breaches, showing just how crucial employee actions and mistakes are in cybersecurity. Cybersecurity education is not just about protecting your business; it's about safeguarding your data and maintaining trust. A well-informed team is less likely to make mistakes that could lead to costly breaches and regulatory fines.

Cyber threats have grown more sophisticated. Everything starts and ends with email. Phishing emails, malicious links, and fraudulent attachments are common entry points for cyber criminals. In some cases, simply having a malicious email in your inbox can compromise your system. With stricter regulations and increased scrutiny, businesses must ensure they comply with data protection laws, underscoring the importance of continuous education and vigilance among your staff.

ABCs of Cyber Threats: Recognizing Common Cybersecurity Threats

Understanding the most common cybersecurity threats is the first step in defending against them. Here are a few that every employee should be aware of:

Phishing: This is the most prevalent cyber threat. Phishing attacks trick employees into providing sensitive information or clicking on malicious links. Email is the biggest vector for breaches, with phishing and pretexting via email accounting for 73 percent of incidents. For example, a well-crafted email that appears to be from a trusted source can lead to significant data breaches.

Malware: Malware, or malicious software, can infiltrate a system through infected email attachments or downloads. Once installed, it can steal data, encrypt files, or even take control of the entire system.

Ransomware: Ransomware is a type of malware that encrypts a victim's data and demands a ransom for its release. Recent high-profile cases, such as the Optum and CDK incidents, highlight the devastating impact ransomware can have on businesses. To learn more about the CDK breach, refer to my colleague Pawel Pikul's article, "CDK Hack: Understanding The Impact And How To Protect Your Business."

Data Breaches: Data breaches occur when sensitive information is accessed without authorization. This can result from weak passwords, unpatched software, or successful phishing attacks.

Smishing and Vishing: Employees should also be aware of less common but equally dangerous threats like smishing (SMS phishing) and vishing (voice phishing). These attacks exploit human trust and familiarity with communication platforms. Unexpected calls, texts, or communications from unknown numbers should always be treated as suspicious.

Delayed Detonation: Some emails may contain links that initially seem legitimate but mutate to malicious sites after a delay, bypassing initial security checks.

Juice Jacking: This occurs when malicious actors infect public USB charging ports to steal data from or inject malware into connected devices. Avoid connecting your devices to public USB charging ports at places like airports.

Employees must recognize these threats and know how to respond. Encourage them to report suspicious activities immediately, even if they're unsure. This proactive approach can prevent minor issues from becoming major incidents.

Homework Time: How Educating Employees on Cybersecurity Best Practices Strengthens Your Security Posture

Educating employees on cybersecurity is a cornerstone of any strong security strategy. Here's how it helps:

Key Components of an Effective Cybersecurity Training Program:

- **Regular Training Sessions:** Frequent, up-to-date training sessions keep employees informed about the latest threats and how to handle them. Cybersecurity training should be continuous, with quarterly or bi-annual sessions to reinforce key concepts and maintain cybersecurity awareness.
- **Role-Specific Training:** Tailoring training to specific roles ensures everyone knows how to protect the information they handle. For example, leadership might benefit from training focusing on safeguarding sensitive data and making informed decisions about cybersecurity investments, while operational staff focuses on recognizing and reporting suspicious activities and understanding daily cybersecurity best practices.
- **Engaging Training Methods:** Simulations, interactive modules, and real-life examples make training engaging and memorable. Use of storytelling techniques to illustrate the impact of cyber threats and make learning fun. Incorporating gamification elements, such as quizzes and competitions is always a good way to get the team together. And real-world scenarios and role-playing exercises can help employees understand the practical implications of their actions or inactions.

A well-structured training program does more than educate; it fosters a culture of security. Employees become more vigilant and develop a keen sense of awareness, reducing the likelihood of human error, which is often the weakest link in cybersecurity.

Pop Quiz: Metrics to Measure the Effectiveness of Cybersecurity Training Programs

Measuring the effectiveness of your training programs ensures continuous improvement and adaptation. Here are some key metrics to consider:

- **Phishing Simulation Results:** Track how often employees fall for simulated phishing attempts and how quickly they report them. Aim for a click-through rate of less than 15 percent in initial simulations, with a goal to reduce this to below 10.4 percent, the current global benchmark, within the first six months.
- **Incident Response Times:** Measure the time it takes for employees to report potential security incidents. While the discovery of incidents can take an average of three days, strive to reduce the time it takes for employees to report an incident after discovery. Aim for reporting incidents within a few hours.
- **Knowledge Assessments:** Conduct regular quizzes and assessments to gauge understanding and retention of cybersecurity concepts. Aim for a completion rate of more than 84 percent, the current NIST benchmark.

Simulations and interactive modules can significantly enhance training. Tools like **KnowBe4** and **Cofense** offer robust platforms for delivering effective cybersecurity training. These platforms can simulate real-world cyberattacks, helping employees recognize and respond to threats.

To ensure that training translates into daily practices, consider:

- **Routine Drills:** Conduct regular cybersecurity drills to test and reinforce training.
- **Spot Checks:** Perform random checks to see if employees are following security protocols.
- **Feedback Loops:** Create channels for employees to provide feedback on training effectiveness and suggest improvements.

Using technology to create engaging and realistic training scenarios helps employees better understand the nature of cyber threats and the importance of their role in maintaining security. Continuous feedback and adjustments based on these metrics helps to ensure that training remains relevant and effective.

Cybersecurity Challenges: Overcoming Obstacles in Implementing Training Programs

Implementing cybersecurity training is not without its challenges. Common issues include:

- **Resistance to Change:** Employees may resist new practices or see training as an unnecessary burden. They may see it as only something that happens at larger organizations or only to other people. Making cybersecurity training relatable by connecting it to personal life scenarios may help reduce this resistance. Showing employees how the skills they learn can protect not just the organization but their own personal information as well doubles the benefit for the resistant employees. Highlighting real-world incidents where lax security led to severe personal and professional consequences can underscore the importance of vigilance.
- **Apathy:** Worse than resistance is the apathetic employee. Some employees may just not see or understand the importance of cybersecurity. They may feel the organization has an IT team and it is their responsibility to ensure cybersecurity for the entire organization. Engaging training methods and real-life examples can go a long way towards addressing apathy. By demonstrating the risks and consequences of cyber threats for all aspects of the organization.
- **Time Constraints:** Finding time for training in busy schedules can be difficult. This challenge can occur at the management level, for managers who do not want to take their employees off “billable” time. It may also come from the employees directly who do not want to give up time from their normal schedule for any training let alone cybersecurity training. You can address this challenge by providing various training formats, including in-person sessions, webinars, and self-paced online courses. This flexibility allows employees to engage with the material at their convenience, ultimately ensuring better participation and retention.

By addressing these challenges head-on and making training relevant and accessible, organizations can improve their overall security posture and foster a culture of cybersecurity awareness.

Stay Ahead of the Curve: Keeping Your Team Updated on Cybersecurity Trends

Cyber threats are constantly evolving, making it essential for organizations to stay ahead. Here are some tips:

- **Continuous Learning:** Encourage a culture of continuous learning. Subscribe to cybersecurity news feeds, ensure all levels of employee and management attend webinars, and participate in industry conferences.
- **Update Training Regularly:** Ensure that your training programs are updated regularly to reflect the latest threats and best practices.
- **Emerging Trends:** Keep an eye on emerging trends such as AI-driven phishing attacks and sophisticated malware. Educate your team on these developments to ensure they are prepared. Key trends to monitor include:
  - ***AI in Cybersecurity:*** Both attackers and defenders are leveraging AI. Cyber criminals use AI to craft more convincing phishing emails and evade detection, while security professionals use AI to identify and respond to threats more quickly.
  - ***Zero Trust Architecture:*** This approach assumes that threats can come from anywhere, and it implements stringent access controls and continuous monitoring.
  - ***Cloud Security:*** As more businesses move to the cloud, understanding and mitigating cloud-specific threats is crucial.
  - ***IoT Security:*** With the proliferation of Internet of Things (IoT) devices, securing these endpoints is becoming increasingly important.

Staying informed about these trends and incorporating them into your training programs ensures that your organization is prepared to face new challenges head-on.

Classroom Resources: How Vertilocity Supports Clients in Cybersecurity Education

At Vertilocity, we understand the importance of cybersecurity education and that it can feel overwhelming. All of the steps outlined above are things almost anyone can do, but if you are looking for an expert that focuses on these issues regularly and consistently then you may want to consider incorporating a Managed Security Service Provider (MSSP) like Vertilocity. Along with our other MSSP services we also offer comprehensive training programs which we tailor to the unique needs of small and mid-size businesses. Our approach includes:

- **Custom Training Programs:** We design training programs specific to your organization's needs, ensuring that all employees are equipped with the knowledge required to help protect your business.
- **Regular Updates:** We provide regular updates and refresher courses to keep your team informed about the latest threats and best practices.
- **24/7 Support:** Our team is available around the clock to assist with any cybersecurity concerns and to provide ongoing support.

Our training programs are designed to be engaging and informative, using real-world examples and interactive modules to ensure employees retain and apply what they learn. We also offer advanced simulations to test and improve your team's response to cyber threats.

Take the Next Step in Securing Your Business

As we head into the back-to-school season, now is the perfect time to invest in your organization's cybersecurity education. Contact us today at MSP@vertilocity.com to learn more about our training programs and how we can help safeguard your business against cyber threats. By investing in cybersecurity education and creating a culture of vigilance, you can significantly reduce the risk of cyber incidents and ensure the continued success and security of your business.