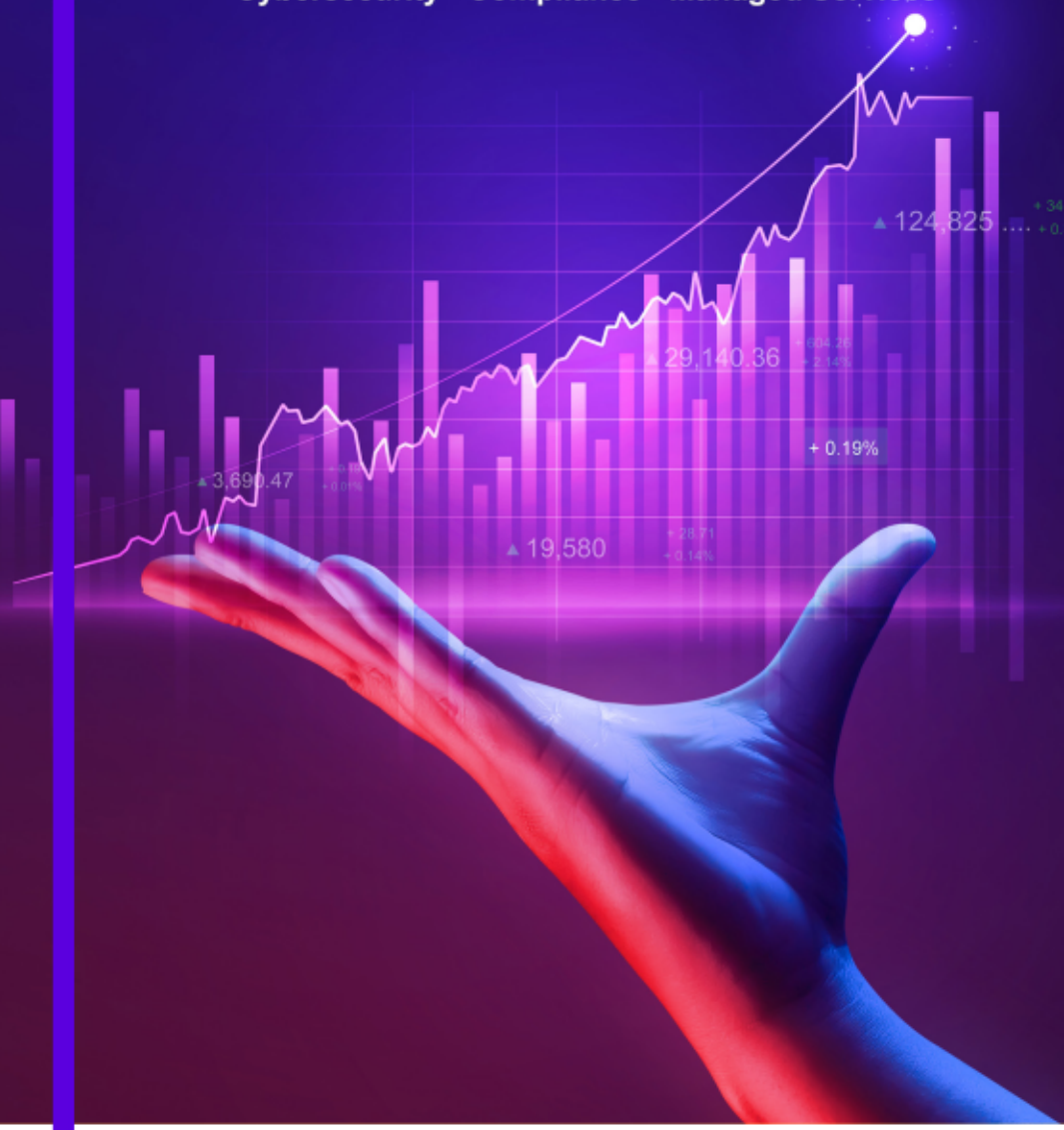
ITNS Consulting

Cybersecurity - Compliance - Managed Services

SECURITY AWARENESS TRAINING

YOUR SMALL BUSINESS' BEST INVESTMENT



EMPOWERING EMPLOYEES TO BE SECURITY SAVVY STOPS CYBERATTACKS AND SAVES MONEY

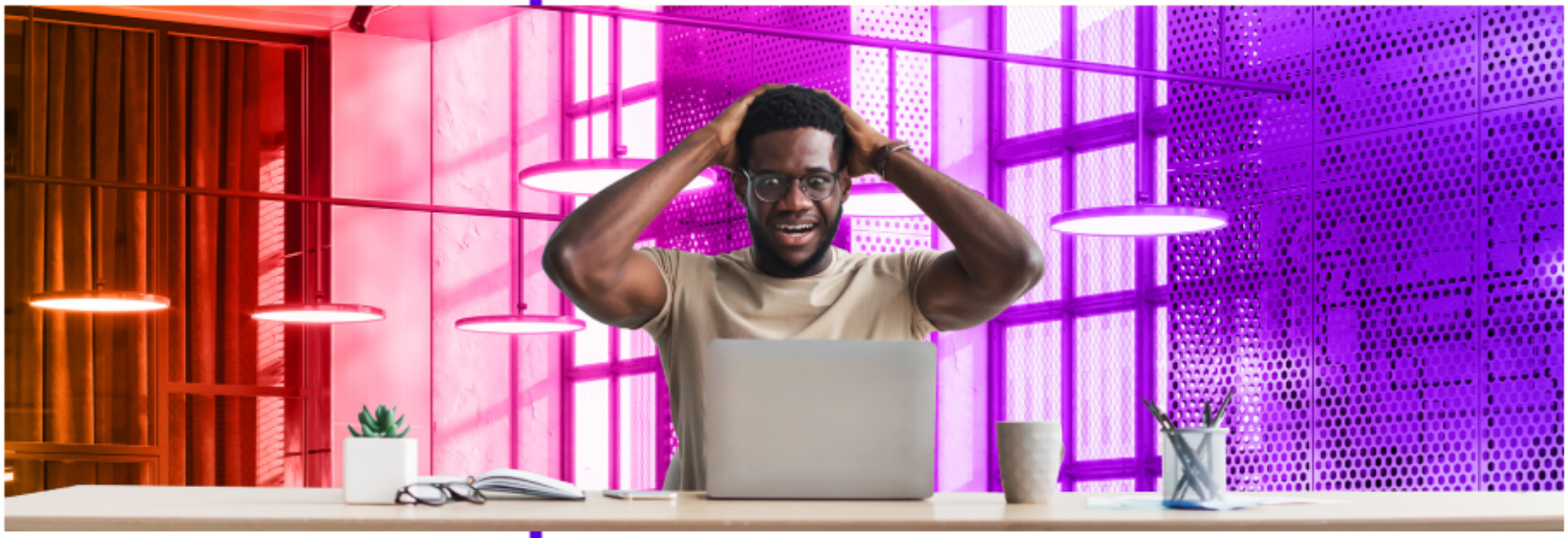
Employees are at the heart of your company's security. They are the last line of defense against cyberattacks and the first ones to notice when something unusual is happening at work. This makes them your most valuable security asset.

However, they can also be a vulnerability. When an employee makes a mistake, like mishandling data, clicking on a malicious link or giving a cybercriminal their password, they are opening the doors to expensive compliance failures and security nightmares for your organization.

The everyday choices employees make have a tremendous impact on your company's security and success. That's why it's critical to educate them on the risks they might face and how to practice good cyber hygiene to keep your business compliant and safe from cyberattacks.

How can you empower your team to fight cybercrime? Create a comprehensive security awareness training program that arms them with the knowledge they need to avoid pitfalls — your company is only secure when everyone knows they are part of the security team.

When you have a well-trained team, they can promptly flag a possible threat. The faster you identify a threat, the better your chances of minimizing the impact it has on your business. After all, security is about more than just technology; it's about people and processes, too.



HOW DO EMPLOYEE CHOICES IMPACT SECURITY?

Every time someone logs on to your company's network, answers an email or takes work home, they're taking an action that could have security repercussions whether they mean to or not. The actions that employees take can result in insider risk for your organization.

As companies become increasingly dependent on technology to get the job done, employees have more opportunities to take actions that could be harmful. Insider threats have nearly doubled in the past two years both in frequency and cost.[1] While insider risk is not something that can be eliminated completely, it can be mitigated, and security awareness training is an affordable and effective way to do it.

HUMAN ERROR IS RESPONSIBLE FOR AN ESTIMATED 82% OF SECURITY BREACHES.[2]

EVERYONE NEEDS TO BE ON BOARD TO BUILD A STRONG SECURITY CULTURE

Companies with a strong security culture have a high level of security awareness — and that's a powerful asset. However, many businesses face challenges in getting the entire leadership in their company on the same page about the vital role their security culture plays in both defense and compliance. Taking a zero-trust approach to cybersecurity can safeguard your business by removing implicit trust and consistently authenticating each level of a digital interaction. Many companies have been implementing a zero-trust strategy to lower the risk of remote work and insider threats, limit third-party risk, manage cloud risk and improve their security culture.

IN 2025, 70% OF CEOs WILL MANDATE THAT ORGANIZATIONS EMBRACE A CULTURE OF RESILIENCE TO BETTER COPE WITH THE HIGH VOLUME OF EVOLVING THREATS, INCLUDING CYBERCRIME, SEVERE WEATHEREVENTS, CIVIL UNREST AND POLITICAL INSTABILITY.[4]

60% OF ORGANIZATIONS WILL EMBRACE ZERO TRUST AS A STARTING POINT FOR FOSTERING A STRONG SECURITY CULTURE BY 2025.[3]

A major barrier to your organizational risk management might be a lack of strategic alignment. Often, a company's leadership overlooks strategic risk management because they don't realize the potential damage cyberattacks can cause.

SECURITY AWARENESS TRAINING HAS CONCRETE BENEFITS

Looking at some of the concrete benefits of security awareness training shows exactly how valuable the training is and why smart companies are making this small investment that gives them a big security advantage. Expecting your staff to study your policy and adopt security procedures on their own is unrealistic. The training you give your employees leads to adoption. They are informed and better understand risks post-training.

IMMEDIATELY EXPAND YOUR SECURITY TEAM WITHOUT ADDING HEADCOUNT

Worryingly, 45% of respondents in a recent survey said that they are not responsible for maintaining security because they don't work in the IT department. That's a disaster waiting to happen. Security awareness training changes this mindset. When employees gain security savvy, they realize that maintaining security to fight back against cybercrime is everyone's job.

By partnering with us, you can easily access the security expertise you need to mitigate today's sophisticated attacks without having to hire in-house.

MAINTAIN COMPLIANCE WITH NATIONAL, LOCAL, REGIONAL AND INDUSTRY-SPECIFIC REGULATIONS

Data privacy and cybersecurity regulations are tightening in many industries, and the price of a compliance failure is high. Security awareness training is required under many data privacy and data handling statutes. Implementing this training equips your employees to identify potential risks and defend your organization from cyberattacks. By fostering a strong cybersecurity culture across your organization, you can not only minimize insider attacks but also ensure security compliance.

LOWER SECURITY EXPENSES, LIKE THE COST OF PHISHING

Phishing is expensive whether the attack is successful or not. If it hits, you've got a potentially devastating incident on your hands. If it doesn't, the matter still requires investigation. The cost of just dealing with the headache of phishing altogether can be devastating for your business. According to the DBIR 2022 report, 82% of breaches involved phishing or social attacks.

LEADING COMPANIES RELY ON SECURITY AWARENESS TRAINING TO PREVENT CYBERATTACK DISASTERS

Security awareness training gives companies an edge against cyberattacks by boosting cyber resilience, making them less likely to be crippled by a cyberattack. About 84% of leading organizations cite security awareness training as a key building block of cyber resilience.[5]

TRAIN EMPLOYEES TO RESIST YOUR TOP DATA SECURITY THREAT: PHISHING

The biggest security risk that any organization faces today is phishing. It is the number one cause of a data breach. Phishing is also the risk that employees encounter the most — and fail to detect the most as well — often opening their organization up to dangerous cyberattacks like ransomware.

EMPLOYEES AND PHISHING ARE A DISASTROUS COMBINATION

58% 58% of employees have clicked on at least one malicious URL on their mobile devices.[6]

16% 16% of employees have downloaded malware or riskware apps on their mobile devices.[7]

75% More than 75% of supply chain attacks include three steps — phishing is one among them.[8]

Cybercriminals are adept at using hard-to-detect ways, like impersonating a well-known brand, to fool their targets into falling for a phishing message. They are so good with these that your employees cannot usually spot a sophisticated phishing email without training.

HELP EMPLOYEES AVOID MALICIOUS ATTACHMENTS

Inexperienced employees often fall for phishing lures that entice them to click on malicious links, download suspicious files and email attachments, enter their credentials on a fake site and even correspond with cybercriminals. That's a huge problem for businesses like yours.

If a malicious file is attached as a Microsoft Office document, it can be even harder for your employees to understand whether the email is legit or not. Security awareness training teaches employees how to identify suspicious attachments carrying malware that masquerade as routine files.

EMPOWERED EMPLOYEES PROTECT COMPANIES FROM TODAY'S MOST DANGEROUS THREATS

A new cyberattack is launched every 39 seconds.[9] That's bad news for organizations that aren't prepared since only 16% of employees are able to recognize sophisticated threats without security awareness training.[10]

RANSOMWARE AND MALWARE

Ransomware attacks have surged by 13% to 25% in one year, which is more than the past five years combined.[11] However, ransomware isn't the only malicious software on the block. Payment skimmers, cryptominers, Trojans and other nasty malware types can also cause damage to your business. According to a recent study, 70% of malware-related breaches involved ransomware, one of the most common tactics used by capable threat actors in system intrusions and supply chain attacks, irrespective of the size of your business.[12]

How security awareness training helps prevent this

Employees encounter these threats every day but are unlikely to detect them without training — if your employees are adequately trained, aware of threat patterns and know which actions lead to a threat, they will behave responsibly.

ACCOUNT TAKEOVER

A bad actor taking over a user account is a nightmare for every small business, especially if the bad guys hijack an account that contains sensitive customer data. Account takeover (ATO) fraud takes a number of forms, including phishing attacks, phone scams or credential compromises.

How security awareness training helps prevent this

Effective training keeps your users aware of the signs of an ATO as well as the dangers of ATO risks, like phishing and credential compromise, and prevents these attacks from landing.

BUSINESS EMAIL COMPROMISE

In a common business email compromise (BEC) scenario, bad actors target a victim and pose as a company the victim's organization would do business with to fraudulently obtain money or sensitive data. BEC also endangers a company's reputation and relationships, with employees encountering this hazard daily.

How security awareness training helps prevent this

Employees who have strong cybersecurity awareness are more likely to be suspicious when they experience unusual behavior when communicating with third-party service providers or suppliers.

BRAND IMPERSONATION AND SPOOFING

Bad actors will often use cloned or “spoofed” legitimate email messages from a well-known company like Microsoft to send phishing messages that trick unwary readers into taking an action to do things like correct a problem, collect a prize or snag a deal.

How security awareness training helps prevent this

When employees know what to look for, they can easily identify phishing emails and flag them. When your staff is unaware of spoofing emails, they may click on bad links, which could result in a data breach and downtime for your entire company.

DATA BREACH

Employees are bombarded with malicious messages daily. However, getting tricked by a phishing email isn’t the only way employees can cause a data breach. Errors like sending someone the wrong file and other data handling mistakes are just as dangerous.

How security awareness training helps prevent this

Security awareness training arms employees with knowledge that helps them resist threats like phishing while making them more thoughtful in general about how their actions and behaviors impact security.

REMOTE AND HYBRID WORKERS

We are living in an era where 60% of knowledge workers are working remotely and 18% of them have no plans to go back to the office.[13] The modern way of working remotely, coupled with greater use of public clouds, highly connected supply chains and cyber-physical systems, exposes your business to new and challenging attack surfaces.

Often, employees think they can get away with risky behavior like writing down passwords or opening suspicious emails when working remotely. Plus, cybercriminals know that remote workers are more likely to fall for phishing tricks and less likely to report a problem or ask for help if they don't even know whom to ask.

How security awareness training helps prevent this

Security awareness training makes your remote workforce more cognizant of why maintaining security matters regardless of where they are. It also teaches them what to do if problems arise.

INSIDER RISK

Every employee is an insider, and every employee brings a certain degree of risk to the table whether they intend to or not. A recent study reveals that negligent employees were responsible for 56% of insider threats, while malicious insiders caused 26% of attacks.[14]

How security awareness training helps prevent this

A strong security culture is a major determinant in reducing your company's overall risk, and security awareness is the foundation on which it is built. If security is top of mind for everyone, employees make fewer mistakes and notice suspicious behavior faster.

START A SECURITY AWARENESS TRAINING PROGRAM AND REAP IMMEDIATE BENEFITS

Don't wait! Security awareness training is just what the doctor ordered to reduce risk and keep your business safe in today's volatile threat landscape.

Contact us today to schedule a no-obligation consultation.

References: 1,14 The Cost of Insider Threats, 2022 | 2,6,7,8,11,12 DBIR, 2022
3,4 Gartner, 8 Cybersecurity Predictions for 2022-23 | 5 IBM Cyber resilient Organization Study, 2021
9 University of Maryland | 10 HIPAA Journal, 2021 | 13 Gartner, 7 Top Trends in Cybersecurity for 2022

ITNS Consulting

Cybersecurity - Compliance - Managed Services

Partner with ITNS Consulting, today!
Phone: 608-563-1975
Email: infosec@itnsconsulting.com
Website: https://itnsconsulting.com