(ISC)²

SIX REASONS WHY TOP-NOTCH CYBERSECURITY TRAINING MATTERS

Training is an important investment companies make in employees because it offers many benefits – from performance improvement to employee retention. However, in order for organizations to realize these benefits, the training has to "stick," meaning it has to transfer from the classroom (in whatever form that takes) to employees' day-to-day activities. Otherwise it's worthless.

Here are six reasons why top-notch cybersecurity training matters for your organization and how you can make it stick.

1. COMPLEMENTS ON-THE-JOB EXPERIENCE

In many industries, professionals are required to complete a certain level of education, pass an exam, or get certified before they can independently perform their job duties. Accountants need to become CPAs. Attorneys need to pass the Bar. And professionals often need to keep their credentials up-to-date with ongoing course work and professional development.

However, in the world of IT security, attaining a certain level of education or credentials isn't usually a requirement. As a result, corporations sometimes forgo training in exchange for on-the-job experience. But that doesn't mean training isn't critical for protecting your organization's data and systems. In every industry, information security professionals need to stay up-to-date with security trends, evolving challenges, and new technology.

2. EVERY COMPANY IS AT RISK

It's no longer a matter of if your organization will be targeted, it's more a matter of when and how often. So your cybersecurity professionals constantly need to be prepared for a potential attack. Corporations are at risk because they house confidential data about their company and customers that perpetrators are looking to steal and exploit. Your IT personnel must understand – and stay up-to-date on – how to protect your organization's critical assets. The risk is too great if they don't.

3. IT'S A TREACHEROUS CYBERSECURITY LANDSCAPE

Protecting your corporation's assets has become more challenging than ever. With BYOD, the cloud, and other trends creating so many more access points for perpetrators to find their way in – and so many more opportunities for employees to unknowingly (or intentionally) let them – it's critical that your cybersecurity team is on top of the latest security developments and trends. They also need the knowledge to teach your employees how to keep their devices safe at work and at home. As perpetrators look for new ways to attack and opportunities to exploit, you need to be prepared so you can minimize internal and external threats in an ever-evolving technology and threat landscape.

4. QUALIFIED PROFESSIONALS ARE A RARE BREED

With the global shortage of qualified cybersecurity professionals is approaching 3 million globally, training has never been more important. Firewalls, network monitoring tools, biometrics, and encryption can help keep perpetrators at bay. But there's nothing as valuable as a trained team who knows what to look for to protect your organization from a potential attack. Once those professionals on the front lines have been hired, you need to invest in their continuing education and training in order to stay ahead of ever-changing threats in cloud security, cyber forensics, and more.

5. INSTANT RETURN ON INVESTMENT

By investing in your cybersecurity talent, you will be better prepared to address the next wave of vulnerabilities and attacks, and design new ways to combat them before they develop into a crisis. Certification can help provide this all-important link and give your cybersecurity professionals the knowledge and training they need, which ultimately provides an immediate return on your investment.

6. REINFORCES BEST PRACTICES

While there are many programs out there, you want to make your selection carefully. Look for a training program that:

- Is based on industry best practices in real-world scenarios.
- Is broad enough to help your employees design, build, and maintain a secure business environment.
- Offers certification training that requires continuing professional education to help users retain the knowledge.
- Stays current on emerging threats, technologies, regulations, standards, and practices.
- Offers an industry-accepted standard of quality to increase confidence that candidates are qualified and committed to information security.
- Ensures your employees use a universal language, circumventing ambiguity with industry-accepted terms and practices.

LEARN FROM THE BEST

Best known for its acclaimed Certified Information Systems Security Professional (CISSP®) certification – considered the gold standard in the field – (ISC)² is the world leader in educating and certifying cybersecurity professionals. CISSP certification ensures that your information security leaders have the breadth and depth of expertise necessary to establish holistic security programs to protect any organization's information assets.

(ISC)² can help you define and deliver a tailored corporate training solution that works for your organization so your personnel have the knowledge and ability to face ever-changing cybersecurity threats. (ISC)² provides programs and services that are customized to meet your team training needs.

To learn more, visit: www.isc2.org/Enterprise