LevelBlue

SOLUTION BRIEF / MAY 2024

LevelBlue Cybersecurity IQ Training

Increase Employee Cybersecurity Awareness; Measure and Report on the Cybersecurity IQ of Your Organization

Organizations seeking to improve their security posture and to help reduce cybersecurity risks, must consider the human element of their attack surface.

In addition, most organizations have an internal security policy requirement for cybersecurity awareness training or they must comply with mandates for regulatory compliance such as PCI DSS, HIPAA, SOC 2, ISO 27001, GDPR and more.

In short, every organization today, regardless of size or industry, needs to implement cybersecurity awareness training for employees.

Increase Employee Cybersecurity Awareness

LevelBlue Cybersecurity IQ Training helps to simplify working toward compliance requirements for security awareness training and to measure the overall security awareness of your employees and organization. LevelBlue Cybersecurity IQ Training is comprised of 18 video training lessons and quizzes, including modules for PCI DSS and HIPAA.

Designed to be engaging, educational, and impactful, the lessons provide learners with a basic understanding of how their actions impact security within the organization. More importantly, employees are educated on best practices and individual accountability in maintaining security.

A Cybersecurity IQ test measures the security awareness of your employees and organization as a whole, with weighted risk scoring based on the different roles of your learners.

- Improve and measure the human element of security, which is often the weakest link.
- Establish a benchmark for organizational and individual security awareness and continually measure improvements against that benchmark.
- Address compliance requirements for security awareness training and internal policies.
- May potentially reduce cybersecurity insurance premiums by documenting progression in employee cybersecurity awareness*.

* Subject to terms and conditions of any specific customer cybersecurity insurance policy.

How it Works

- Organizations control the pace of training for their employees.
- A baseline Cybersecurity IQ Score is established for each employee and for the organization as a whole with a ten-question, pre-training test to gauge their cybersecurity knowledge.
- Organizations can apply weighted risk scoring for individuals based on their role, influence in the organization, and access to critical business data.
- Employees complete 18 video lessons (approximately 3.5 hours of content), which they access online — one executive video lesson is optional.
- After each lesson, employees are required to take a quiz (80 percent is considered passing); post-lesson quizzes are not counted toward an individual's final Cybersecurity IQ Score.
- After completing the required lessons, each employee takes a post-training, ten-question test to gauge their cybersecurity knowledge.
- Pre-lesson and post-lesson test scores establish the employee's Cybersecurity IQ score.
- Organizations are able to track individual and cumulative Cybersecurity IQ scores across learners.
- At the end of training, organizations receive a report with each employee's Cybersecurity IQ score and the cumulative Cybersecurity IQ score for the organization.

Cybersecurity IQ Video Training Module

PCI Security Standards

In this lesson, learn the importance of the Payment Card Industry Data Security Standards (PCI DSS) and how to go beyond compliance to prove that your organization is proactively adhering to the standards and mitigating the risk of a data breach.

Acceptable Use of Computer Systems

This lesson goes beyond common sense and outlines the importance of a company computer use policy.

Defining the Security Landscape

Cybersecurity breaches are happening at an alarming rate. This lesson is an introduction to the various tactics used to infiltrate organizations, educating employees on how to protect business-critical assets.

Installing Software From Unknown Sources

New software is enticing, but it can wreak havoc in the office. Learn how to properly use software and avoid unknown or unsolicited programs or files that could lead to a breach.

Onsite Social Engineering

Learn how to avoid being taken advantage of by scammers who are using human nature to get their foot in the door and access to sensitive information.

Physical Security and Removable Media

Does your organization have an "open door policy" that is too risky? For example, are social engineers getting access to sensitive data? From piggy backing to dumpster diving, learn what signs might signal an attack.

Security Protocols Regarding HIPAA

Learn the security protocols surrounding the Health Insurance Portability and Accountability Act (HIPAA). Gain insight into the regulations and information security best practices for complying with HIPAA to help defend against a breach and bolster the security of patient data.

Defending Against Cybersecurity Fraud

Discuss ways to prevent cyber criminals from accessing your workplace to commit cyber fraud. From ransomware to wire fraud, you will be educated on the schemes and tactics used by cyber criminals. You will also learn best practices for defending against these types of attacks.

Executive Cybersecurity Defense

Specifically designed for executive management, get best practice recommendations on how to defend against an attack aimed at executives and their families, as well as approaches to help reduce risk by creating a high level of security awareness across the organization.

Mobile Device Security

Utilizing personal mobile devices to conduct business is now commonplace. However, convenience can come at a price. Learn proper cybersecurity on the go.

Password Development and Security

Underscore the need for every employee to understand the importance of highly secure passwords and learn best practices for password creation.

Remote Social Engineering

One opened email or one clicked link are simple acts that could lead to devastating consequences. Learn how to spot attacks that are highly effective at gaining access to corporate data.

Security Practices for the Internet of Things

Learn about the IoT environment, infrastructure, security risks, and privacy concerns. Get best practices and tips for improved security and learn effective ways to apply the same security protection protocols on these devices as you would apply to other network-attached equipment.

Social Media Dangers

Friending, following, tweeting, checking in, and linking up — everyone is doing it. Employees learn how to socialize more safely.

Preventing Virus and Malware Outbreaks

The complexity of recent virus attacks demonstrates the need for training and ongoing education. In this lesson, learn about antivirus technologies and how to detect malware.

Safe Web Browsing Habits

Online pop ups, deceptive links, and clickable graphics can all lead to spyware and other potentially dangerous traps. Learn common tactics used by cyber criminals and how to avoid scams.

Security of Protected Data

Protecting sensitive information is the objective for all security measures. Learn the fundamental ways employees can work together to help protect personal and customer data.

Using Cloud Services

Migrating workloads to the cloud? Learn what to look for when selecting a cloud service provider.

LevelBlue

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.