MetaCompliance®

UNLOCKING THE POTENTIAL OF SECURITY TRAINING

PREV PAGE
NEXT PAGE

Unlocking the Potential of Security Training

Table of Contents

PREV PAGE

NEXT PAGE

Unlocking the Potential of Security Training

Introduction:

The data breach is a common occurrence in today's evolving threat landscape. In 2015 alone, the Breach Level Index (BLI) recorded 1,635 incidents that affected organizations in government, healthcare, retail, financial services, and education. Nearly half of those events lacked a publically available number of compromised records. Even so, those incidents for which data was available exposed approximately 708 million individual records.

These figures represent an existential threat to organizations both large and small, especially when one considers the price of recovery. According to IBM's 2015 Cost of Data Breach Study, the total cost of a data breach rose from $3.5 million to $3.8 million last year. The study also observed a growth in value of the average per capita cost of a breach from $145 to $154.

Let's put those costs into perspective. With the average breach exposing between 3,000 and 100,000 accounts, organizations face a recovery cost ranging from about $500K to $15 million. That price tag is just for ensuring the security of each affected account. It does not cover the reputation costs and legal fees that often follow a breach.

All is not necessarily lost. In fact, most enterprises have the resources and manpower to rebound from those negative consequences. However, the same cannot be said for small- to mid-sized businesses.

SMBs commonly lack information security personnel and PR representatives capable of adequately responding to a data breach. With that in mind, a modest security incident could very well put an SMB out of business.

The recovery process also tasks organizations in the public sector, where security incidents boil down to who should be held accountable for the security failure. An event can cost a public servant their job or potentially their career in public service. Those repercussions are all too real, especially in instances where insider negligence, not external attacks, lead to a breach.

Unfortunately, insider data breaches are more common than one might think. The BLI found that accidental loss caused approximately one quarter (24 percent) of all breaches in 2015--more than malicious insiders, hacktivists, and state sponsored actors combined (18 percent).

To protect themselves organizations have to train their employees on corporate policies and best security practices. The real challenge is improving awareness through understanding and learning. However, in the real world of business where time is short and attention span shorter, chosing the correct type of cyber security training is important. Which type of program will have the greatest impact on employees' security awareness? Which method of digital security training is fit for purpose?

For those enterprises looking to create a consistent, flexible, and interactive security awareness training program, eLearning is the way to go.

PREV PAGE

NEXT PAGE

Unlocking the Potential of Security Training

eLearning vs. Classroom-Based Learning

To understand how eLearning can unlock the potential of security awareness training, it is important to identify how eLearning differs from classroom-based education. The answer is simple. It relates to how the "student" views themselves and their surroundings in each modality.

In a classroom setting, the student can use an important resource that is absent from most eLearning programs: close contact with their instructor(s) and fellow classmates. Such interaction enables the student to investigate learning materials as part of a team, which can help them build an understanding of important concepts on a deep level.

"Learning in the classroom in close contact with an instructor can offer real benefits," explains Robert Chapman in a post for *ComputerWeekly*. Chapman is the founder of Firebrand Training, an innovative IT and computing training company located in the UK. "Humans are designed to learn from one another using both verbal and visual clues to process and retain new information. Discussions and Q&A sessions will often stoke up new insights into subjects and help students to grasp a new concept."

From the teacher's perspective, visual clues such as wrinkled noses, furrowed brows, or glazed-over expressions among students could indicate that further explanation on a given topic is needed.

By contrast, in an eLearning setting, most communication takes place via email, chat, or a web-based discussion forum, which limits the types of cues students and teachers can detect while discussing course topics. Communication is generally more formal and direct in an eLearning atmosphere than in the classroom. As a result, most eLearning activities are self-directed insofar as the student is responsible for completing the coursework on-time and contacting their instructor should they require further explanation of the learning materials.

eLearning and classroom-based education are both effective educational models. Each has its own benefits and shortcomings. When it comes to security awareness training, however, eLearning has some clear advantages over the classroom.

PREV PAGE
NEXT PAGE

Unlocking the Potential of Security Training

Consistency, Flexibility, and Interactivity: The Three Benefits of eLearning Security

There are three main benefits to incorporating eLearning over classroom-based learning into a security awareness training program. Those are consistency, flexibility, and interactivity.

1. Consistency

In the classroom, instructors are constantly on the lookout for visual cues to help them gauge their students' understanding of course material. However, it is impossible for an instructor to pick up on each and every cue. One student might grasp a key concept perfectly, whereas another pupil might still be struggling with it. These variations in understanding might be in the students' control, or they might not. For instance, some students might invest less time than others in completing their homework, but others could be situated next to rowdy peers or at the back of the classroom where it is more difficult to hear the instructor or read notes written on a whiteboard.

On a day-to-day basis, the latter group of students receives a different learning experience than those located near the front of the room, and there's little they or the instructor can do about it. Someone will always need to be placed at the back of the room, and someone will always need to sit next to those who might be disruptive.

These problems are not evident in eLearning settings. The same learning message is delivered to each and every student by way of a laptop, smartphone, etc. Given the portability of those devices, no one needs to sit at the back of the room. No one needs to be placed near rowdy peers. Everyone receives the same level of access and attention that a digital medium can afford.

With that in mind, eLearning is optimal for teaching employees about practices by which they must all abide. Those include corporate policies, compliance regulations, and security best practices. Organizations need to trust that their employees are equally aware of how to avoid digital threats and how to positively contribute to an evolving security culture. As a result, it makes sense for companies to invest in eLearning, which is predicated on delivering a uniform learning experience to every registered user.

PREV PAGE
NEXT PAGE

Consistency, Flexibility, and Interactivity: The Three Benefits of eLearning Security

2. Flexibility

What makes eLearning consistent also makes it flexible. If course content can be accessed from a smartphone or laptop, that means students and their instructor(s) can discuss relevant learning materials on an ongoing basis. eLearning is not bound to a delimited class schedule, and so its content is always available.

Such flexibility is crucial for an organization made up of several employee sub-groups. Whether the company is an SMB or a public-sector agency, different groups of employees have different priorities, schedules, and deadlines that might separate them from other members of the organization's workforce. As a result, it might be impossible to train all employees at once in a classroom setting. eLearning fills in this gap by allowing employees to complete the course content according to their own schedules, which includes at work, during lunch, or even at home.

eLearning also allows for flexibility on the part of the employer. Those in charge of managing an eLearning-based security awareness training program can roll out new course materials when it is convenient, which allows an organization's workforce to complete their learning without affecting their productivity around important events such as new product launches, mergers, and even data breaches.

An employer can also deploy the same eLearning content as long as it is relevant for new employees. If a new piece of legislation or compliance regulation pops up, the employer can simply add a new module to their eLearning content. They do not need to create and schedule entirely new classroom sessions. They can simply build upon the learning content they already have and roll it out accordingly.

PREV PAGE

NEXT PAGE

Consistency, Flexibility, and Interactivity: The Three Benefits of eLearning Security

3. Interactivity

Last but not least, eLearning tends to be more interactive than the classroom. In the latter modality, lessons commonly make use of print and digital learning materials as part of a lecture- or discussion-based format. Participants can choose to read along with the instructor, and there might even be a few written assessments to test their knowledge of the course content. However, the students are for the most part passive learners. They are merely expected to receive and absorb knowledge related to them by an expert.

That is not the case with eLearning. The digital medium allows for more active learning exercises, such as gamification, discussions, problem solving, and demonstrations. Such interactivity is crucial for learning about specific digital threats. For example, many security-based eLearning content comes with tools by which employers can send out fake phishing messages to evaluate whether their employees can spot spam mail. To help employees understand the importance of not clicking on a suspicious link, employers can instruct their employees to click on a fake malicious URL, which can then demonstrate the consequences of a successful phish.

In most cases, employees can best understand a topic if they are given the opportunity to experience it firsthand. eLearning affords workers that opportunity when it comes to digital security via the use of demonstrations and real-time simulations.

PREV PAGE

NEXT PAGE

Unlocking the Potential of Security Training

Conclusion

Uninformed insiders pose a serious risk to your organization's data. With just one careless click, your enterprise might need to assume responsibility for paying hundreds of thousands if not millions of dollars in data breach recovery, reputation, and productivity costs.

Fortunately, organizations can reduce the probability of a security incident. It all starts with leveraging an eLearning solution to educate employees about digital threats and security best practices.

That's where Metacompliance comes in.
Metacompliance is an organization that specializes in providing Integrated User Awareness Management solutions which includes elearning, phishing, policy management and staff awareness services.

Metacompliance consults with companies to recommend processes and training changes that can better protect their organisation. To help implement those changes, the Metacompliance team can recommend one of their e-Learning modules to be delivered as standalone individual training, as content to be added into the company's existing LMS (learning management system), or as part of Metacompliance's own LMS called MetaLearning. All of its eLearning content is based on the 70:20:10 framework, which gives users a well-rounded educational experience by integrating experiential, social, and forming learning activities.

PREV PAGE
NEXT PAGE