CYBER RESILIENCE THINK TANK

Employees Behaving Badly?

Why Awareness Training Matters

mimecast®

CYBERSECURITY.
WHO KNEW IT HAD AN EMOTIONAL SIDE?

Well, it does. Tugging at the heartstrings and provoking the minds of humans can influence a corporate culture, making it one that is security-forward, cyber-aware and proactive about preventing bad things from happening at their own hands.

The flip-side is a culture that doesn't care. One that isn't aware of the myriad cyberthreats targeting not only an organization's network and data centers, but directly targeting humans. This is a culture that clicks without regard and unknowingly behaves badly when it comes to security.

What your employees do—how they behave—when you're not looking over their collective shoulder is entirely up to you. The decision: to implement awareness training or not to implement awareness training. The choice is yours, but a resounding number of organizations choose the latter.

Quick Fact: Only 11% of organizations continuously train employees on how to spot cyberattacks. 24% admit to monthly training, and 52% perform training only quarterly or once a year.

*Global research from Vanson Bourne, commissioned by Mimecast.

LACK OF TRAINING IS HURTING YOU.

Only 11% of organizations continuously train employees on how to spot cyberattacks. 24% admit to monthly training, and 52% perform training only quarterly or once a year.

This isn't good enough. Especially when nearly 40% feel that training their staff is the best way to protect their organization from email-based cyberattacks. So, why is the frequency of security training so low? Maybe it's due to the 33% that want to address threats via increased investment in technology, or the 29% that opt to see improved business processes.

According to Joshua Douglas, Chief Information Security Officer at TRC Companies, Inc., educating humans and making them cyber-aware is critical.

He said, "To me, awareness training is all about educating individuals on what potentially risky situations look-and-feel like, so they can make smart choices to avoid potentially disastrous situations."

So, why isn't awareness training a priority for most?

Marc French, Chief Trust Officer at Mimecast said, "Security teams are constantly fighting a fire – and training isn't a fire. It comes down to time, resources and conflicting priorities."

But the consequences of not prioritizing awareness training are real.

"The only way to keep awareness alive is to provide continuous training so cybersecurity is top-of-mind. Without regular training, your culture will suffer," said Douglas.

> “***To me, awareness training is all about educating individuals on what potentially risky situations look-and-feel like,*** *so they can make smart choices to avoid potentially disastrous situations.”*

JOSHUA DOUGLAS
CISO
TRC COMPANIES, INC.

What Are Your Employees Doing When You're Not Looking?

BEHAVING BADLY AT WORK.

Almost 30% use their company-issued device for personal reasons for at least one hour per day.

55%

Further, **55% display the same browsing behavior for at least 30 minutes every day.**

LACK OF CYBERSECURITY AWARENESS IS THE CULPRIT.

25%

Nearly one-in-four employees aren't aware of the most basic threats to their organization – like phishing and ransomware.

50%

About half say **their employer doesn't provide mandatory cybersecurity training.**

60%

Nearly 60% of employees say **they are either not aware of their company's policy on web-use at work** – or there aren't established policies in place at all.

* Google Consumer Research, commissioned by Mimecast

BUILDING A CULTURE THAT CARES.

When it comes to defining an organization's mission and vision, a lot of time is spent refining and getting it right. However, when it comes to making security part of corporate culture, this isn't the case. Michael Madon, Senior Vice President and General Manager of Mimecast Security Awareness Products said, "With security, creating a mission typically equals checking a box when really, it's about commitment and underscoring the importance of security – this should be part of a company's guts and what makes it successful."

"Engagement means not checking a box. It's about going from compliance to commitment."

Douglas believes that security awareness programs either succeed or fail based on one of the four key "Cs": Compliance, Commitment, Complexity and Culture.

"Out of all of them, Culture is the hardest to change and move the needle, but at the same time, it's the one that has the most impact," he said, "When you change the hearts and minds of humans, they ultimately can help drive success for cybersecurity."

> ***Engagement means not checking a box.*** *It's about going from compliance to commitment."*

Michael Madon
SENIOR VICE PRESIDENT
& GENERAL MANAGER
MIMECAST

Six Ways to Make Security Awareness Part of Your Culture

Awareness training is paramount when it comes to shifting culture. The key is to make sure senior leadership rallies behind it to create commitment for a strong and lasting cybersecurity program. Here's how to get started:

1 **FIRST, GET BUY-IN** and commitment from senior leadership.

2 **SELECT TRAINING SUBJECTS THAT PERTAIN TO EMPLOYEES' ROLES AND FUNCTIONS**
– and keep them short and easy.

3 **BE PERSISTENT – ANNUAL TRAINING DOESN'T WORK.**

4 **MAKE SURE TRAINING IS ENGAGING AND FUN.**

5 **UNDERSCORE THE IMPORTANCE OF BASIC SECURITY HYGIENE –**
provide real-life examples of how your organization failed, and consequently suffered a breach.

6 **KEEP TRACK OF PERFORMANCE AND THE EFFECTIVENESS**
of the trainings with testing of click-through rates.

DISCRETION CAN BE DANGEROUS.

According to Madon, the discretionary actions of employees are important for every aspect of the business, not just security. Knowing or not knowing what employees are doing in their discretionary time will ultimately determine the success of a company.

"There is an assumption that you can always watch employees because of technology. But this isn't true. Employees are always one step ahead," he said. "In security, there are privacy standards, and positive or negative behavior can impact these standards."

Gary Hayslip, Chief Information Security Officer at Webroot, said, "As a CISO, I would hope that employees would be somewhat educated on good practices for being on a computer and using the internet. With that said, time and again, I've found that this isn't the norm. I believe it's the responsibility of the organization to provide security awareness education and resources, continuously over time, to remind employees that security and threats are dynamic and continuously changing."

He continued, "When you have employees who don't trust or understand your security program, they ignore proper security controls and work around them. This begins a whole lifecycle of the organization's security program having to put out self-induced fires because they haven't done a good enough job evangelizing the value of their program."

> ***There is an assumption that you can always watch employees because of technology****. But this isn't true. Employees are always one step ahead."*

Gary Hayslip
CISO
WEBROOT

BAD HABITS HAVE CONSEQUENCES.

In general, employees are not doing bad things on purpose or out of malice, but their actions can greatly impact the security of your organization and data. 61% of organizations suffered an attack where malicious activity was spread from one infected user to other employees via email. How?

Here are common ‘bad habits’ your employees may not know can be dangerous, without awareness training:

1 **OPENING EMAIL FROM PEOPLE THEY DON’T KNOW.**

2 **CLICKING ON LINKS WITHOUT VALIDATING THEM FIRST.**

3 **OPENING ATTACHMENTS WITHOUT CARE.**

4 **USING WORK DEVICES FOR PERSONAL ACTIVITIES THAT MAY BE RISKY.**

CYBER RESILIENCE IS EVERYONE’S RESPONSIBILITY

Humans can be either a first line of defense, or the first line that cybercriminals seek to exploit when they attack an organization. Their behavior and the culture you influence greatly impact the effectiveness of your overall cyber resilience strategy.

“Employees should take their awareness training and challenge their information security teams to involve them in the shared responsibility for securing their organization,” said Douglas. “They should also become brand ambassadors if they have personal interactions due to a cyber threat.”

Douglas continued, “Every organization needs a solid plan to implement a security awareness program that can provide key KPIs that show how effective the training is and how it creates a trend in changes among employees. Without solid mathematical data, you can’t track behavioral changes.”

THE DOWNLOAD

HEY, CISOS:

YOU ARE YOUR OWN BEST RESOURCE

When it comes to making awareness training part of your cyber resilience planning, budget, staff and resources aren’t the only factors. Your own visibility can be more beneficial than you think.

“If you have little or zero dollars to play with, you can be your own best resource. Get out and be visible. If people recognize you as the ‘security guy,” they will reach out to you proactively with questions and concerns. You can use this valuable data to build an awareness program,” said French.

Humans have to be as resilient as your technology. If you take the time to train employees and give them educated ownership over their own security behaviors, they will want to protect the organization.

mimecast

THE STATE OF EMAIL SECURITY

The latest threats, confidence killers and bad behaviors – and a cyber resilience strategy to fix them

2018 REPORT

Ready to Strengthen Your Defense?

Learn More

Mimecast Limited (NASDAQ:MIME) makes business email and data safer for tens of thousands of customers with millions of employees worldwide. Founded in 2003, the company's next-generation cloud-based security, archiving and continuity services protect email, and deliver comprehensive email risk management in a single, fully-integrated subscription service.