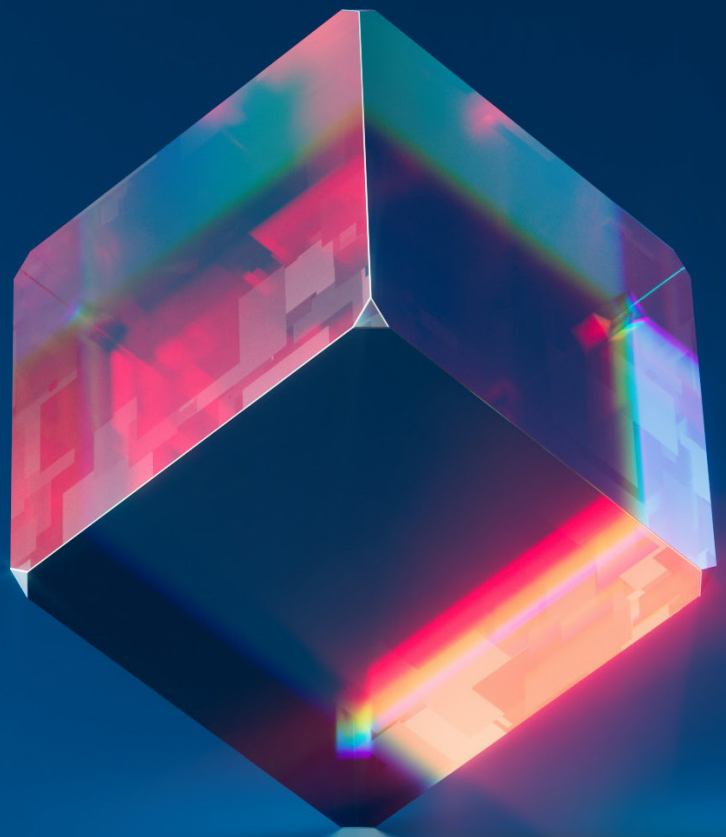
CYREN

The Missing Piece in Your Security Awareness Program



Executive Summary

Security Awareness Training (SAT) has long been a central approach for companies seeking to educate their employees about cybersecurity in the workplace in general, and about detecting potential phishing attacks in particular.

In general, companies of all types and sizes utilize email as their primary mode of communication. Confidential information and other sensitive business data are among the content of more than 100 billion email messages exchanged daily. The responsibility for maintaining the confidentiality and integrity of the information included in the message falls on the often-overstretched IT Security team.

95%

Human error is the source of 95 percent of cyber security breaches, according to an IBM study.

Malicious actors need only a single person to click a link once to gain a foothold into an organization's network, which may result in a potentially devastating cyber incident. Clearly, more needs to be done to ensure that businesses empower their employees to be part of the solution rather than being a bystander or an enabler when it comes to socially engineered cyberattacks. The good news is that many companies have adopted SAT in some form. SAT has long been a solution for organizations to educate their employees about email security and, specifically, about spotting phishing and social engineering attacks.

Though security experts constantly – and rightly – highlight the need for security awareness programs, the quality and efficacy of these programs may vary considerably. Security awareness is a challenging program to execute as it involves an audience that often does not understand security nor is security a primary focus of its day-to-day roles. Organizations are usually required to show 100 percent employee participation. Failure to do so may be disastrous, resulting in not just a security breach but also significant harm to the organization's brand and image. Furthermore, budgets for security awareness campaigns are typically limited so the security managers must know how to make the most of the resources they have.

When it comes to improving the SAT performance, your primary best practice should be identifying the actual reasons that are holding you back from achieving the intended impact. The true goal of any SAT is behavioral change. However, having your SATs in place and seeing practical results are not the same. The focus should not be on the theoretical performance scores and iterative training but on improving the company's overall cybersecurity posture by changing the employees' security alertness behavior. Equip your employees with the right platform and tools so they are empowered to be part of the solution. They should be able to easily identify emails they believe are phishing, seamlessly notify the IT specialists and get the IT feedback – all directly from their inbox.

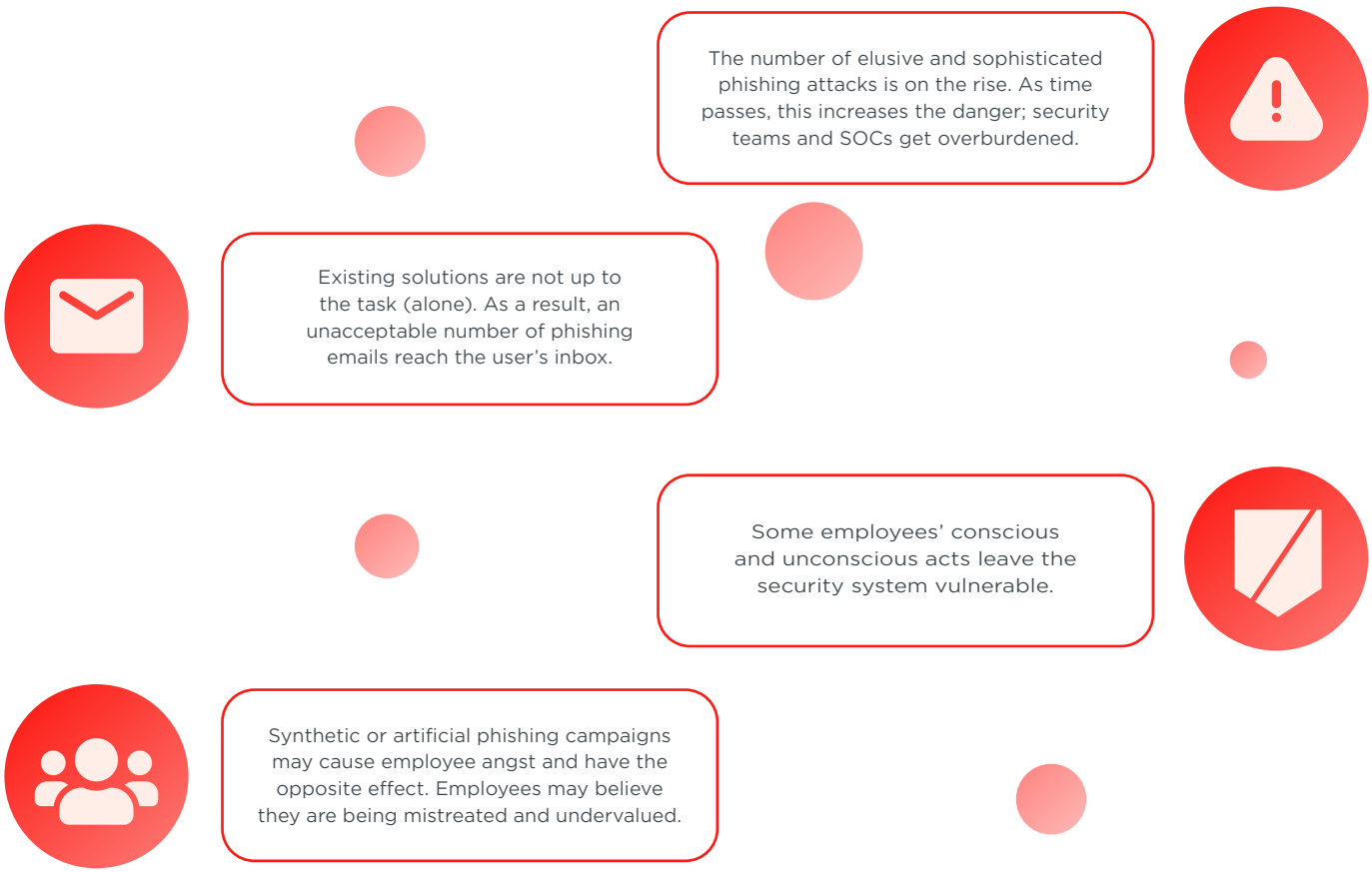
Introduction

SAT is a valued best practice to put in place within all organizations. It should assist in raising awareness of the risks posed to businesses through channels such as email, particularly with phishing attacks. To be effective, training should be provided regularly; however, in practice, it is typically conducted 2-3 times a year, predictably to fulfill compliance standards. This approach to SAT is inadequate to make a significant impact on a company's cybersecurity posture.

Employees, or a company's "human layer", should be recognized as a vulnerable link in the cybersecurity chain. More work must be done to ensure that organizations empower their employees to be part of the solution rather than seeing them as part of the problem. Employees handle the most sensitive data in a business, maintain critical connections with vendors and customers, and retain necessary login credentials. Your employees are human, and they will unavoidably make human errors – that is why cybersecurity training is essential. Businesses invest a lot of money to do it properly, but ignoring how humans behave, learn, and react in these situations is part of the reason your SAT may not be paying off.

Challenges

There are a lot of reasons why the SAT has fallen short of its promise. Some of these reasons are listed below:



Best Practices for Augmenting Security Awareness Training

It is crucial to strike a balance between the compliance-related necessity for training and the goal of changing the cybersecurity posture of your company. SAT is often motivated by regulatory requirements; it is a duty and is seen as a checkbox activity that will assist the business in obtaining the rubber stamp of approval needed to claim compliance with regulations. This method does not foster a proactive nor practical approach to security, which is why companies still face security risks while having completed all the required actions.

SAT can be about so much more than regulatory compliance. It is all about putting those resources to good use and involving every person in the company in building those protections from the inside out. There must be a shift in attitude so that SAT is no longer viewed as a checkbox activity, but rather as the strategic priority, designed to keep your company safe.

Harnessing Crowd Wisdom to Improve your SAT's Impact

Unfortunately, SAT has a reputation for being one of those things that makes all employees grumble since it typically implies another lengthy training session when they will be told what constitutes good and poor security. This is neither interesting nor motivating, and it puts the whole burden on the employees.

Businesses can reinforce SAT by enabling their employees to make choices rather than passing the baton to overburdened security staff. This will guarantee that SAT has the desired impact and, as a result, improve the efficacy of the organization's security. Therefore, crowd-sourced user detection is the way to go since it incorporates employees as part of the solution.

For example, it is now feasible to provide employees with tools that allow them to identify phishing indications inside the email payload, encouraging them to check any questionable emails they receive with the click of a button through an email extension. They will be able to determine whether the email is a danger or not in seconds, and if it is, this information will be shared with the automated platform to enhance the company's overall threat detection abilities.

Rather than being trained on artificial phishing campaigns, this new crowd-sourced approach will train them on their own inbox on their own emails, continuously, to identify potentially risky emails. The result will be increased productivity, improved identification, and reduced burden on IT teams, not to mention avoiding a potentially devastating cyber incident.

It is critical that the company set the tone and train by example. While management may approve SAT for compliance reasons, it is also important to communicate the broader business benefits of SAT, such as increased overall employee productivity and a reduction in the number of false alerts that the security team must manage, allowing them to focus on their "day jobs".

How Cyren Inbox Security Can Enhance your SAT Results

Better Threat Detection and Response

Companies can identify and repair contaminated emails not just from the reporting email account – Cyren Inbox Security enables them to do so from any M365 mailbox where the phishing threat is detected.

Improved Threat Intelligence

Customers can use Cyren Inbox Security to strengthen threat intelligence. The company's Global Security Team could double-check whether something was overlooked and ensure that remediation was successful and complete by sending Cyren data back into their security logs.

Increased User Engagement

Cyren Inbox Security empowers its client's staff to become more cyber-aware and cyber-engaged. The company will learn how quickly Cyren's noticeable Scan Email button was embraced by its users around the world during the proof-of-concept phase. Users simply click on the button to flag a suspicious email.

Users are notified of the results, which keeps them informed and interested. Sika, for example, used Cyren Inbox Security services and witnessed a 600 percent increase in user-escalated reports of phishing emails. Sika's user engagement continues to improve as employees use the system more.

Outlook

Cyren Inbox Security simplicity of installation and usage is one of its most appealing features. As a company develops and expands, Cyren will make it simple for fresh recruits and acquired employees to become involved in cybersecurity straight away. Data collected by Cyren Inbox Security can also be used to assess and identify the needs for future security awareness training programs.

Why Cyren Inbox Security brings results

- Malicious actors are constantly targeting companies with spam, malware, ransomware, and phishing.
- Once the phishing emails reach the mailbox, on- and post-delivery remediation is the only option to defend the mailbox.
- Cyren detection is based on dozens of indicators and collected evidence of phishing, BEC, and malware.
- On detection, Cyren Inbox Security can add a banner and deliver a warning, automatically remediate, and move the email to Junk or Deleted Items.
- Users can initiate a real-time scan or report the email as phishing. Both false positives and false negatives get reported.
- When users report an email as a threat, an incident is created, and an alert is sent to the administrator. Incidents are aggregated into cases based on similarity.
- Cases can be reviewed, resolved, and manually remediated by the administrator and SOC team analysts.

Summary

Having a Security Awareness Training program (SAT) is a prerequisite in today's organizations. However, a good number of companies that require their employees to undergo SAT do not enjoy the expected uptick in their cybersecurity posture. One of the most frequent reasons for that is the failure to consider human nature and individuality. As a result, the entire program may end up wasting valuable time and resources and create animosity among employees.

Enhancing your SAT program with Cyren Inbox Security will boost the SAT effectiveness and lead to a greater improvement in your company's cybersecurity posture. In addition, Cyren Inbox Security will encourage employees to feel and act as part of the solution.

For more information about Cyren Inbox Security visit https://www.cyren.com/products/cyren-inbox-security or schedule a demo today!

CYREN

Cyren is a messaging security company that protects enterprise email users from today's evasive threats and supplies threat intelligence solutions to security software integrators, hardware OEMs, and large service providers. Cyren's GlobalView threat intelligence network analyzes billions of email and web transactions daily and is trusted by companies like Microsoft, Google and Check Point, who utilize Cyren's APIs and SDKs to operationalize threat intelligence for their customers.

HEADQUARTERS

US Virginia
1430 Spring Hill Road
Suite 330
McLean, Virginia 22102
Tel: 703-760-3320
Fax: 703-760-3321

SALES & MARKETING

UK Bracknell
Maxis 1
43 Western Road
Bracknell
Berkshire
RG12 1RT

US Silicon valley
1250 Borregas Avenue
Sunnyvale, CA 94089
Tel: 650-864-2000
Fax: 650-864-2002

R&D LABS

Germany
Heidestraße 10
10557 Berlin
Tel: +49 (30) 52 00 56 - 0
Fax: +49 (30) 52 00 56 - 299

Iceland
Dalshraun 3
IS-220, Hafnarfjordur
Tel: +354-540-7400

Israel
10 Ha-Menofim St, 5th Floor
Herzliya 4672561
Tel: +972-9-8636 888
Fax: +972-9-8948 214

Cyren.com

@CyrenInc

linkedin.com/company/cyren