SECURANCE CONSULTING
Advantage of Insight AI

Unscammable: The Guide to Fostering a Culture of Security Awareness

www.securanceconsulting.com

THE PROBLEM

Human error accounts for most cyber breaches and incidents. In fact, **77 percent of successful social engineering attacks originate from a phishing email.**[1] Software and systems are coded to perform certain tasks and be aware of only those things they are programmed to notice. Humans, however, are curious, and trickable, as we see from the mounting success of social engineering attacks, such as phishing, pretexting, and baiting. In plainer terms, most breaches do not happen in isolation. They happen because someone made a choice. User decision-making is a threat to enterprise security.

The question is, how do organizations inform or control what choice an employee will make in a social engineering situation? The answer might not surprise you. It's education and reinforcement. Through education, humans gain mindfulness of their actions, which leads to healthy habits and safer decisions. When this education is reinforced, particularly from the management level, it's even more effective.

> **22%** of all breaches in 2019 were the result of social engineering.[2]

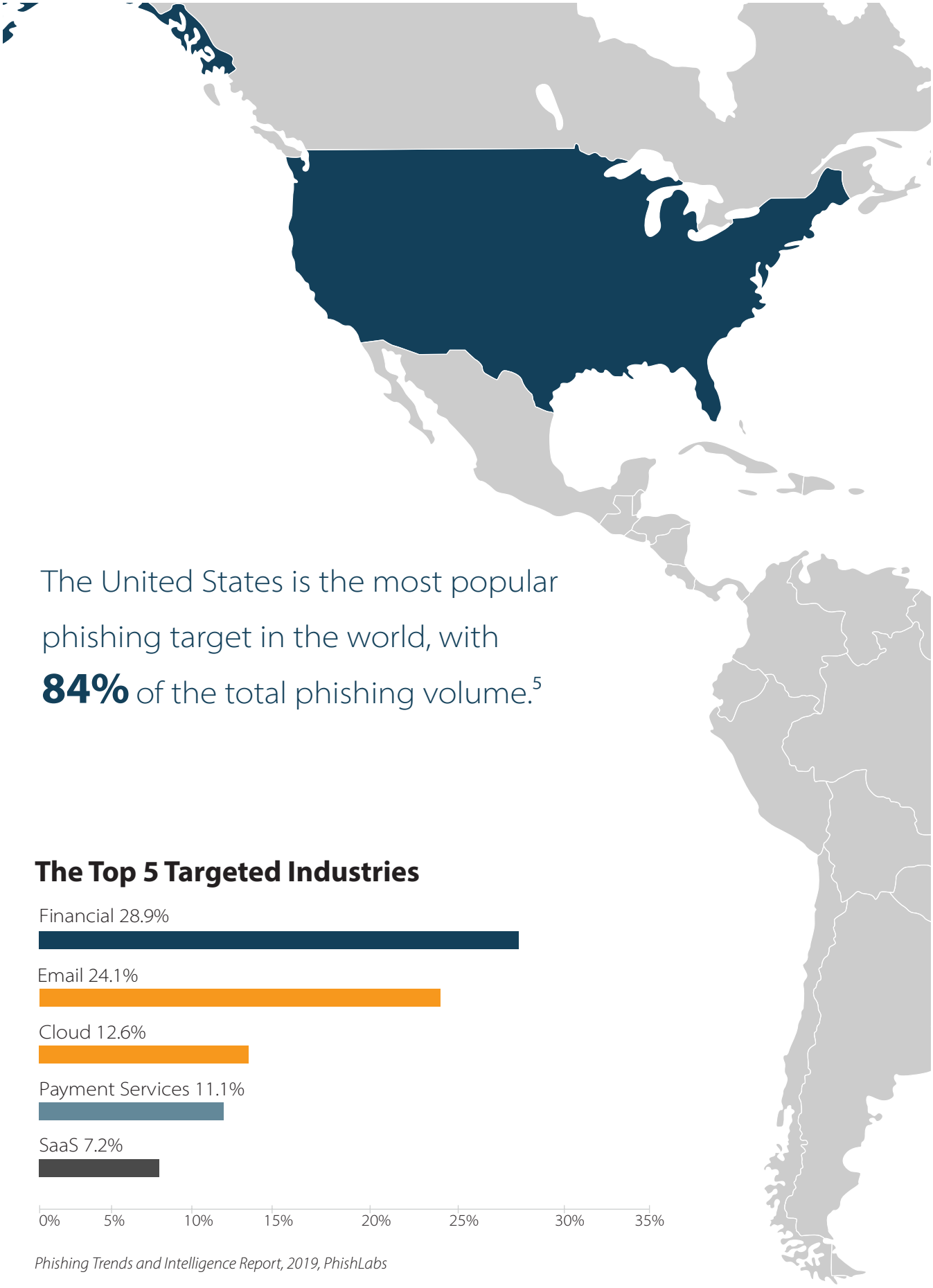
In a recent survey composed of 15,000 responses, 96 percent reported that they had experienced more or the same amount of phishing attacks from the previous year. Ninety-five percent said they train their staff to identify and avoid them. This is consistent with the move to a more people-centric security model, by which organizations engage employees via computer-based training and simulated phishing attacks to teach them about the importance of avoiding social engineering incidents and the real-world consequences of falling victim.[4]

Reported impacts of successful phishing attacks included:

- Financial losses, including fraudulent wire transfers, legal fees, and fines
- Data privacy and compliance issues (e.g., GDPR, PCI DSS, HIPAA)
- Greater burden on IT teams (e.g., cleanup, incident response, reconnaissance)
- Damage to the reputation of information security teams and organization as a whole
- Costly investments in new technology, including multi-factor authentication (MFA)
- Frustration from customers and employees following a data breach[4]

Given that the threat of social engineering does not seem to be abating anytime soon, organizations must continue to build resiliency by instating and enforcing a formal security awareness program.

> **48%** of malicious email attachments are Microsoft Office files, up from just 5% in one year.[3]



The United States is the most popular phishing target in the world, with **84%** of the total phishing volume.[5]

The Top 5 Targeted Industries

Phishing Trends and Intelligence Report, 2019, PhishLabs

PUTTING AWARENESS INTO PRACTICE

Recently, a long-time Securance client achieved a remarkable feat— during a social engineering campaign run by Securance, not a single employee opened a phishing email attachment, clicked a link, or entered any personal credentials. In our 18 years of testing, Securance had never seen success of this caliber. During past assessments, we had aided our client in strengthening the human element of security, and now we were finally seeing our recommendations and their tenacity at work together.

> Over **3.4 billion** email scams or phishing emails are sent every day. This adds up to **1 trillion** email scams per year.[6]

The Long Haul

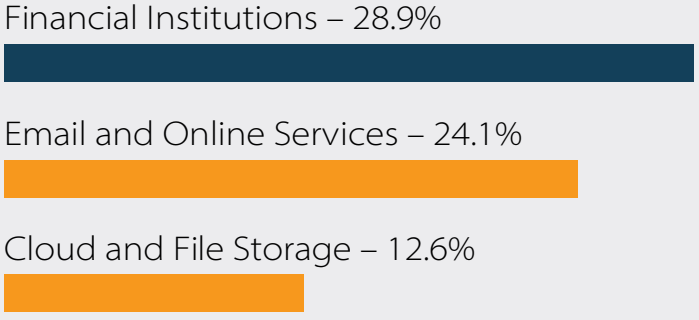
"Technically, our program started about five or six years ago with a standard computer usage policy," said the IT Manager, "but it wasn't until about two years ago, when we first started using our current security awareness platform, that we felt we could build a comprehensive program."

The road to "no clicks" has since been long but fruitful, as evidenced by the organization's recent results. The choice to commit to regular internal testing, rather than just one-off annual assessments, has set this organization apart from many of its industry peers. The security awareness platform they utilize has helped increase awareness and decrease risk, but fostering a supportive environment for employees to learn took time.

Reception

One of the main challenges with implementing security awareness training, according to the IT Manager, was ensuring staff felt comfortable being tested. "We performed security audits with social engineering elements before, but staff instinctively became paranoid when they saw auditors in the building. During that time, they were hyper-vigilant of their activities, such as locking their workstations when they stepped away from their desk, but it was a seasonal awareness. Things went back to normal after the auditors left."

Top Phishing Targets



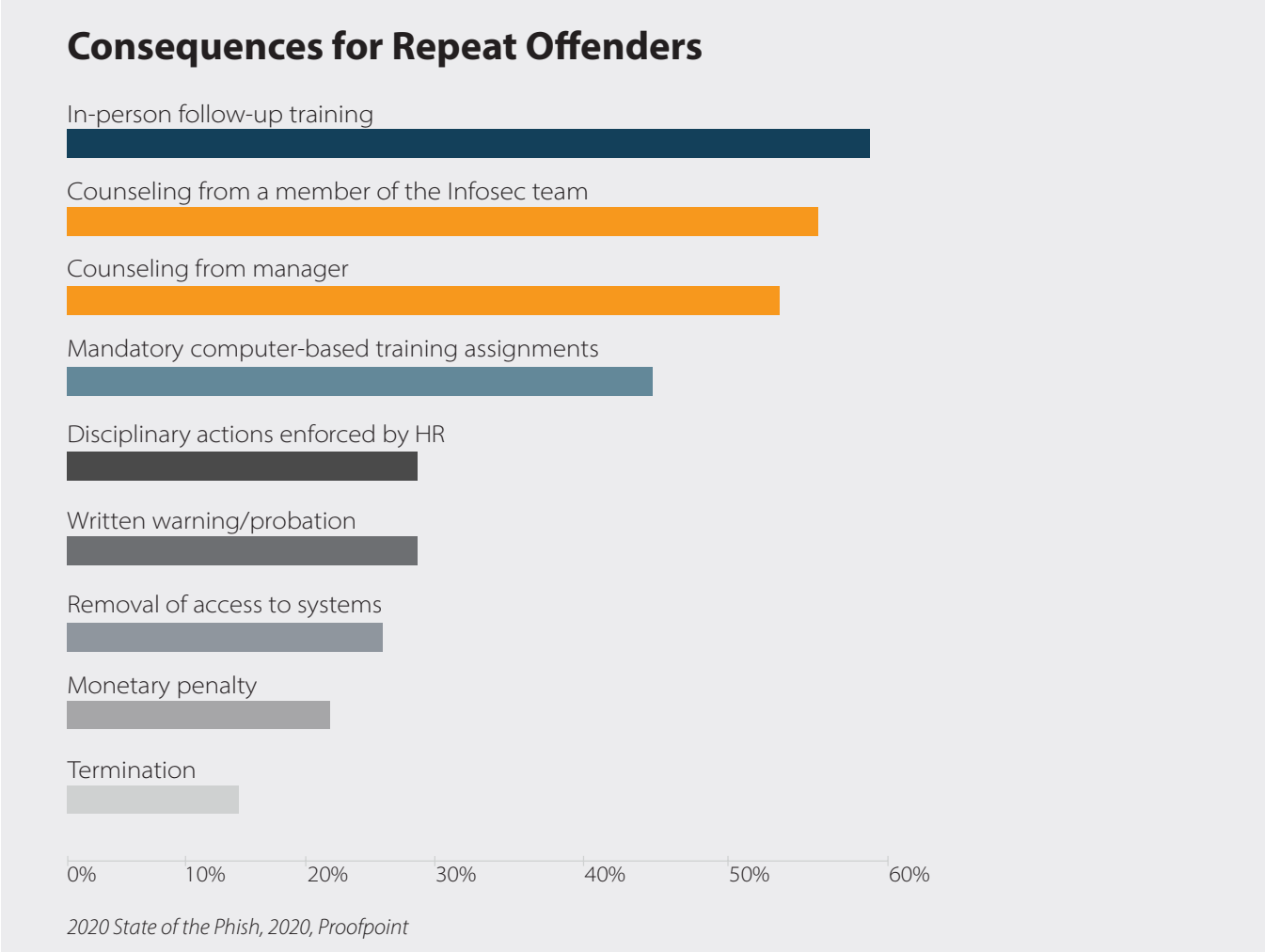
Phishing Trends and Intelligence Report, 2019, PhishLabs

Recognizing that maintaining effective security steadily became more difficult with each passing year, particularly with the rise of advanced persistent threats (APT), they knew a more proactive approach would be required— one that would create a positive outlook toward security awareness.

"We're here to help them, not to get them in trouble," the IT Manager said of the organization's employees. "There's a certain trust factor you need to gain, which takes time, but while they once thought we were out to trick them, the attitude has changed. Now, employees are applying the skills they learn in the office to their personal lives. That kind of real-world effect helps them understand the benefit of the training we do, which contributes to building the trust factor."

> **84%** of organizations said employee awareness improved following the implementation of a consequence model.

As many security professionals know, measuring the effectiveness of a program is critical to understanding if it benefits or harms an organization. For example, organizations must evaluate how they punish employees for repeat offenses, if at all. Does the current program create stress, decrease morale, or stunt employee buy-in? If employees are to be reprimanded for noncompliance with established awareness regulations, the whole organization, particularly HR and Legal, must agree on and document a formal escalation process.



2020 State of the Phish, 2020, Proofpoint

In the study of 15,000 responses noted earlier, 42 percent of respondents said there are ramifications for users who continue to click on simulated phishing attacks. Of those, 39 percent said punishment made a difference; 7 percent said it did not; and an overwhelming 54 percent said they did not measure the impact of punishing employees for repeat offenses.[4]

Without analyzing the effects of our decisions, whether it be which training we assign to employees, the frequency of testing, or deciding to implement a procedure for reprimanding employees who continually put the business at risk, we cannot know the impact of any choice we make, thus rendering our efforts, time, and investments futile. As much as we test employees, we must even more rigorously test the process.

Elements of Success

So, what makes a successful program? When asked, our client immediately stated, "Senior management support. All directors require employees to complete training in a timely manner, and staff are held accountable for it."

The truth is, an organization can invest in the best security awareness tool in the world, but without accountability coming from the top, the entire initiative is doomed to fail. Our client requires all staff, including new hires, consultants, temps, and interns, to complete introductory security awareness training within the first two weeks of joining the organization. "If they have an account in our system, they're required to take the training and are added to our automated phishing campaign."

> "We want everyone to look at it as a learning opportunity to be aware at all times, not just of work email and physical security, but also at home."

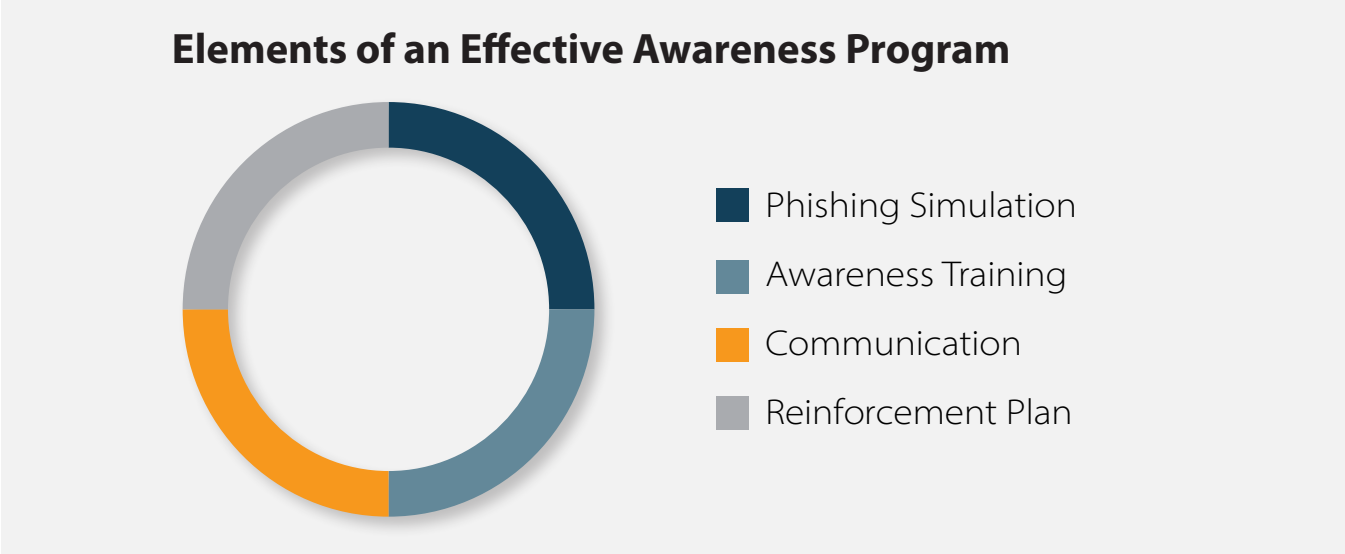
The automated phishing campaign is another critical part of how the organization has established a culture of security awareness and one that they refer to as "the most crucial element in driving down click rates." Within the platform, they scrutinized thousands of templates and categories and filtered by difficulty to find materials that would challenge and strengthen the organization.

The automated phishing campaign sends out emails to random employees over a two-week period continuously throughout the year. The random nature of the test, coupled with the frequency of testing, ensures authentic responses and promotes long-term preparedness. Executive personnel are not exempt from this campaign either. "Their time is valuable, but so is the information they have access to," explained the IT Manager. "The program we use has specific executive-level training, which is a condensed version of what we send to the rest of the organization, but we thought that was counterintuitive. If they are being targeted more for more sensitive information, why would we give them less training? Leveling the playing field in this way means equal responsibility across the entire organization."

> Over **27 billion** records were exposed between January and June 2020.[7]

They have also made reporting suspicious emails easier by utilizing a plug-in for their email client that allows users to send phishy emails to their internal security team. The employee is sent a thank you email for their vigilance to positively reinforce the diligent behavior. Our client revealed that 90 percent of emails reported are simply spam, not phishing attempts, but they never shame an employee for being wrong. "We want everyone to look at it as a learning opportunity to be aware at all times, not just of work email and physical security, but also at home," he added. "During our campaigns, we usually have a rate of 30 to 40 percent of phishing emails reported. In our latest campaign, we had 54.8 percent, so that's improvement we can measure. And we tell everyone: if you're not sure about a suspicious email, ask."

Another component of success has been the visual reminders around the office. "We want to keep the initiative fresh in everyone's minds," explained the Information Security Analyst. "We have posters in bathroom stalls, by sinks, entrances and exits to buildings, stairways, and in the breakroom. They cover topics like how to lock your computer when you step away from your desk and what to look for in a phishing email. There was some resistance initially against all the messaging, but now people are seeing a benefit in their personal lives and avoiding phishing scams in their personal inboxes."



In terms of reprimanding employees who are slow on the security awareness uptake, the IT Manager says his organization has instated an escalating scale of remediation. Everyone is given a freebie click every six months. If an employee clicks on a malicious link, the system shows them what they should have noticed was awry with the email. If the same user clicks a second malicious link, they're assigned additional phishing training of about 15 minutes in length. If they become a three-time repeat offender within three months of their second misstep, they are assigned an additional 45 minutes of training. A fourth time within three months of the third offense results in a face-to-face meeting with the employee, security personnel, and the employee's supervisor.

> Security is an ongoing initiative, and organizations must continually evolve to keep pace with malicious actors.

"It's a communicative process," said the IT Manager. "We want to know, why is this not clicking? What can we do to help? Usually the answer is, 'I just need to be more careful.' We've only had to have sit-down meetings twice, and those people have now had a zero click rate for over a year."

In an attempt to be proactive about reinforcing policies, our client established a committee with the authority to instate and carry out consequences for employees who continuously put the organization at risk through their negligence. However, the program they have in place has been so successful that the committee only met once to kickstart the initiative and has never had to meet again.

Enterprise security is everyone's responsibility.

Even more effective than the remediation process has been the incentive process. Our client implemented a contest for the first half of 2020, which includes all employees and only has one criterion: no clicks. The winner will receive a gift card. A third of the way through the challenge, 98 percent of employees are still in the running.

Our client also hosts monthly security awareness newsletters on their intranet, which contain strategies to remain vigilant around the holidays, the newest phishing scams, and other additional education. It all supports the effort of building a comprehensive approach.

Future Goals

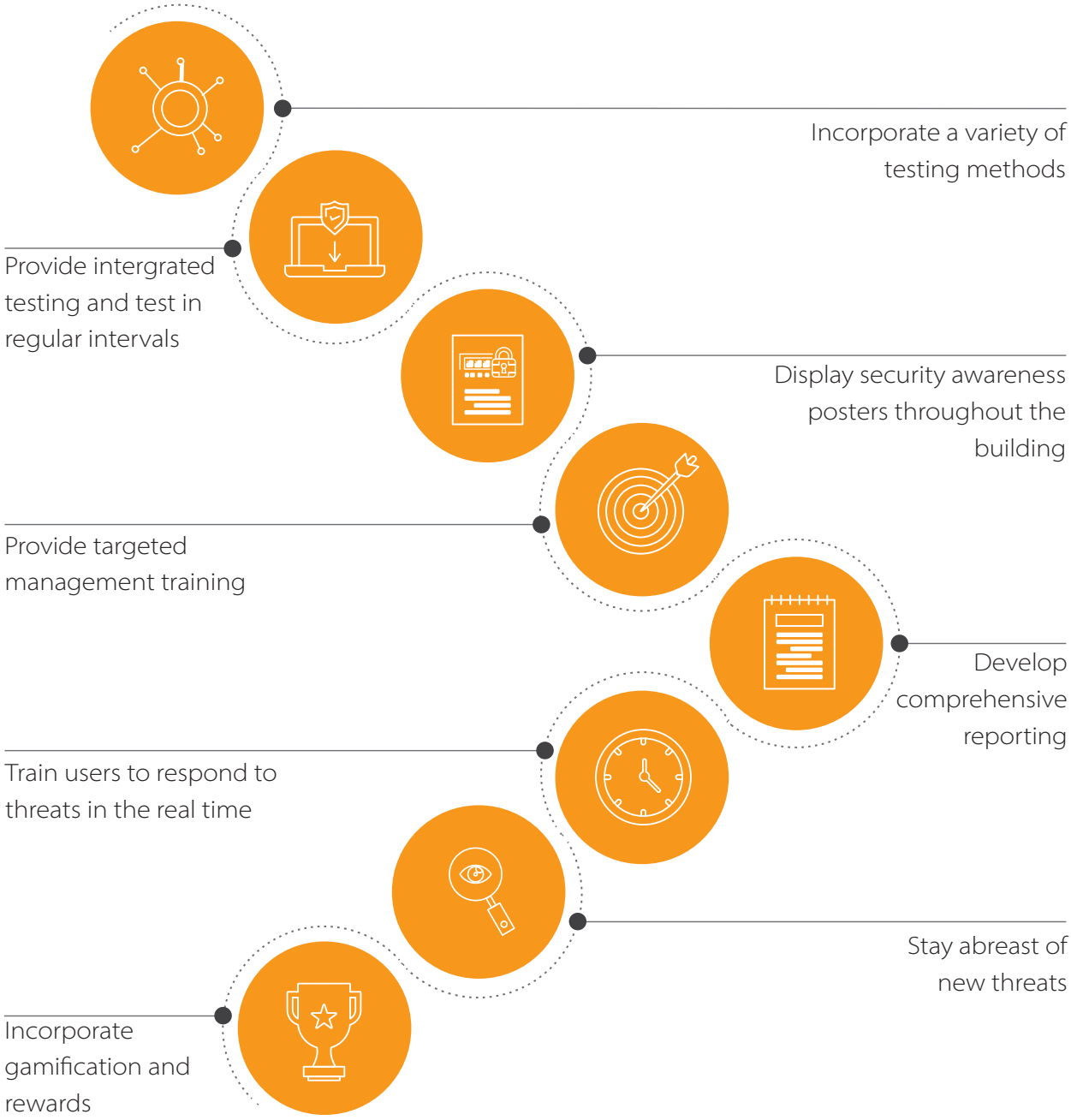
Despite our client's success, they recognize that there are always ways to improve the program and employee engagement. Security is an ongoing initiative, after all, and organizations must continually evolve to keep pace with malicious actors. Their biggest goal in terms of reducing risk is simply to reduce clicks, and that is a matter of repeating the cycle of testing, education, and reinforcement. Our client realizes that security is never a short-term goal. Because of this, they have focused on developing and reinforcing a security awareness program that provides useful, relevant information and creates a standard across the enterprise that everyone is equally responsible for maintaining effective security.

THE SOLUTION

There are many security awareness solutions on the market today, and it's important to find one that fits an organization's business and security goals. Look for platforms that offer some or all of the following features:

- Social engineering training
- Administrator platform training
- Platform training rating system
- Training reminders
- Content customization
- High-quality content libraries
- Corporate branding capabilities
- Customizable reporting
- Phishing reporting button
- Unlimited phishing simulations
- CISO coaching
- Regular newsletters and educational materials
- User guides and periodic bulletins[8]

Elements of a Successful Security Awareness Program



REMAINING CHALLENGES

A comprehensive security awareness program will vastly help organizations reduce their risk of experiencing a costly data breach; however, there are some key considerations to keep in mind to improve security awareness in the long run.

Mobile

Even the most prepared user can still fall prey to mobile phishing or smishing (SMS phishing) attacks. Traditional phishing training teaches users to monitor their email for attacks, honing the focus on their workstations. However, users have been conditioned for years by their mobile devices to swipe, click, and expect instant results and information. Most people open and read SMS (text) messages reflexively without expecting them to contain malicious messages. Smishing attacks are also much more difficult for security teams to track and respond to. Finally, mobile-specific phish kits imitate login screens for authentic websites too accurately for most users to detect.5 Given how integrated mobile devices have become in users' personal and professional lives, their security must be heavily considered when developing a comprehensive user awareness program.

> Even the most prepared user can still fall prey to mobile phishing or smishing (SMS phishing) attacks.

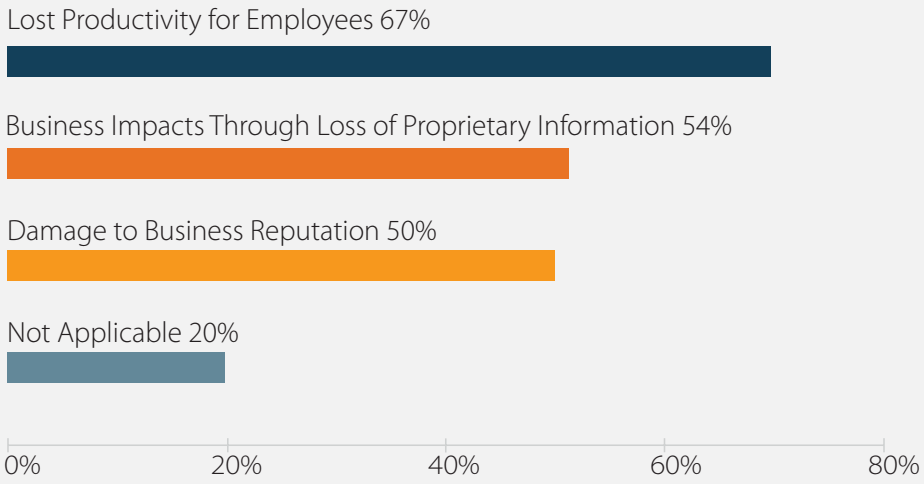
Threat Evolution

A program is only successful if the training and educational materials are preparing employees for current, real-world threats. Information security teams must remain abreast of new attack vectors and implement training to combat them.

Responsibility

This cannot be overstated: **security is everyone's responsibility.** Awareness training should be mandatory across the organization, including C-level executives, and everyone should be held accountable for completion. Creating a security-aware culture can entail different steps and components for various organizations. Everyone has different needs. If the organization decides to instate a system for reprimanding employees for negligence, both HR and Legal should be involved to protect all parties and ensure a fair remediation system. In a recent global study, it was found that 63 percent of organizations punish users who regularly fall for phishing attacks. Of those, 84 percent said the consequences model resulted in improved awareness. The table below depicts the most common consequences used by the study's respondents.

How Infosec Teams Measure the Cost of Phishing*



**Multiple responses permitted*

2020 State of the Phish, 2020, Proofpoint

CONCLUSION

While creating a culture of security awareness can take a great deal of time, the benefits of not falling prey to social engineering scams are invaluable. Developing a comprehensive security awareness program is crucial to protecting sensitive enterprise data, reputation, employees, and customers. An effective program should provide up-to-date, real-world training and educational materials, and both of those elements should be reinforced through senior management buy-in, open communication, and consistent follow-through.

In addition to an established program, conducting third-party security awareness assessments is important to objectively confirm user knowledge and efficacy at avoiding malicious attacks. Securance has conducted social engineering assessments for 18 years, and a 100-percent passing rate, such as achieved by the client described in this white paper, is incredibly rare. Most organizations either don't know where to start or need a professional opinion on their state of preparedness in the face of mounting threats. Working with a platform-agnostic firm can provide organizations in any industry the springboard they need to create a true culture of security awareness.

To learn more about how to develop a culture of user security awareness, Contact Securance today.

ABOUT SECURANCE

Securance has two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1) https://www.knowbe4.com/phishing-security-test-ga-se

2) https://enterprise.verizon.com/en-gb/resources/reports/dbir/2020/introduction/

3) https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

4) https://info.wombatsecurity.com/hubfs/Wombat_Proofpoint_2019%20State%20of%20the%20Phish%20Report_Final.pdf

5) https://info.phishlabs.com/hubfs/2019%20PTI%20Report/2019%20Phishing%20Trends%20and%20Intelligence%20Report.pdf

6) https://www.valimail.com/resources/email-fraud-landscape-q3-2019/

7) https://pages.riskbasedsecurity.com/en/2020-mid-year-data-breach-quickview-report

8) https://www.cyberriskaware.com/wp-content/uploads/2019/07/CRA-The-Ultimate-Guide-To-Security-Awareness-Training.pdf

9) https://docs.apwg.org//reports/apwg_trends_report_q1_2019.pdf

10) https://www.exclusive-networks.com/ch-de/wp-content/uploads/sites/22/2020/02/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf

Unscammable: The Guide to Fostering a Culture of Security Awareness

SECURANCE CONSULTING
Advantage of Insight AI

13904 Monroes Business Park • Tampa, FL 33635 • 877.578.0215

www.securanceconsulting.com