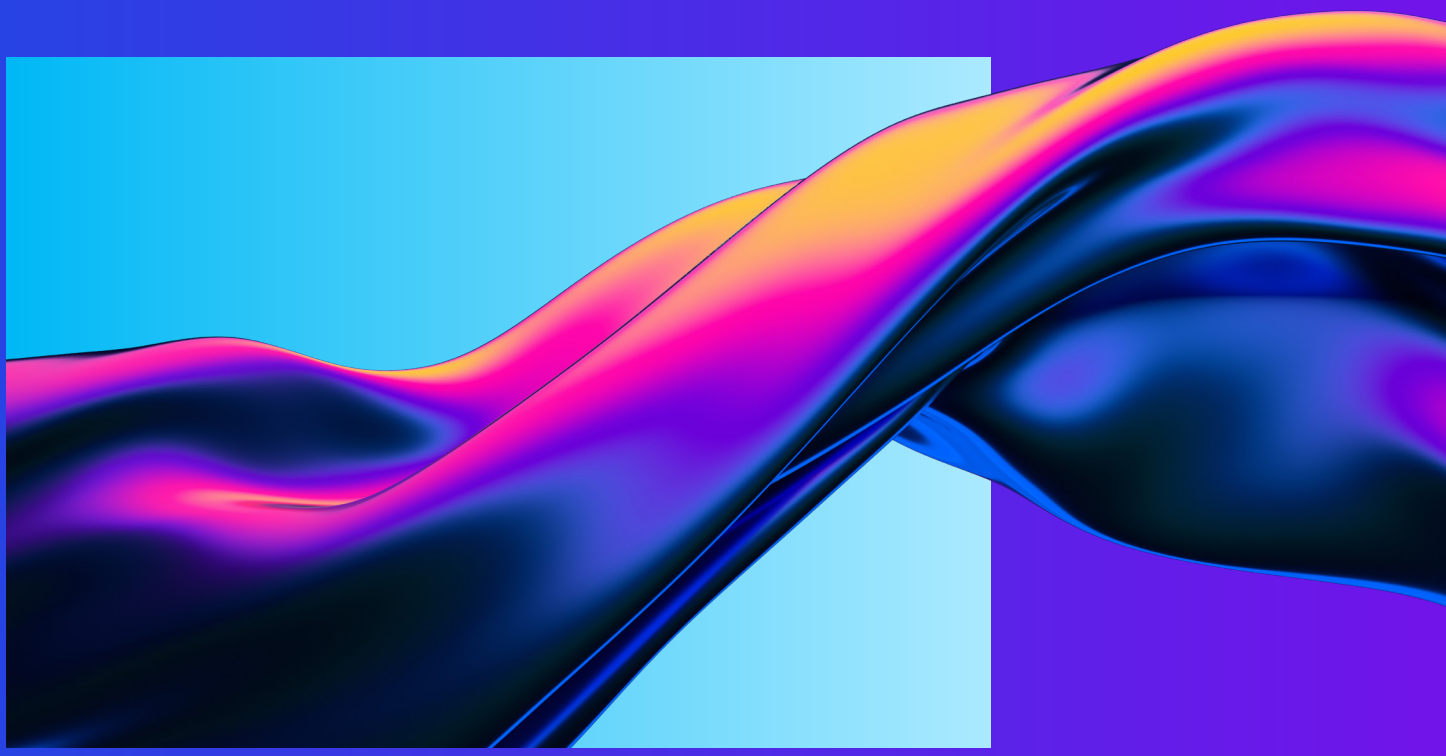
KPMG

Human firewalling

The science of secure behavior



kpmg.com/us

Contents

Your bank sends you an email that states, "Your accounts have been locked because of suspicious activity. Please update your information at this link." Or your video streaming service says that, "There is some trouble with current billing information. Please respond now!" Or a retailer announces, "Good news! You've won an iPad! Claim your prize by clicking here."

Companies spend millions of dollars on cybersecurity technology solutions, but still fall prey to hackers through phishing schemes like these.

While firewalls and other technologies can be the bedrock of an organization's cybersecurity program, they can't protect everything. Studies show that 95 percent of reported breaches include some element of human error.[1] Employees are busy, and their inboxes inundated with messages. It can be easy for the inattentive or uninformed worker to be fooled by a malicious email. It is, therefore, critical for a comprehensive cybersecurity strategy to address the human factor.

Many organizations address cybersecurity measures with their employees only once a year—often at a company-wide event during October, which is Cybersecurity Awareness Month. While these events are valuable, the security awareness message presented often fades quickly and fails to make any meaningful change in employee behavior, with many falling back into routine, lax practices.

In our work together within the Behavior Management and Communications team within Labcorp's Office of Information Security, we've seen evidence that to protect an organization, a cybersecurity program must move beyond these annual check-the-box activities, as there is a big difference between being compliant and being secure.

What is needed is a more integrated, holistic approach that incorporates cybersecurity messages into each employee's workday in such a way that it shifts cybersecurity from being a conscious choice to being a habit. This persistent engagement approach draws on behavioral science, coupled with adult learning methodology, that includes positive reinforcement techniques to create "stickiness" and drive secure behaviors. A key component of this approach is a highly visible, marketing-style management and communications program that creates internal branding for cybersecurity that is immediately recognizable by employees.

The result is a cultural shift in which employees acknowledge the importance of cybersecurity, support the cybersecurity mindset, see themselves as part of the cybersecurity team, and are inspired to engage to learn more.

In the following pages, we'll describe the key elements of a successful integrated cybersecurity behavior management and communications program and the steps to begin creating one at your organization.

> Cybersecurity awareness can't be a one-and-done issue. It's not a campaign; it's an ongoing program that must become part of the fiber and the culture of the organization. Everybody, from the board and executive team to the senior leadership team and all staff, needs to be aware of the program and on board.
>
> **—Jacqueline LaScala**

> T-shirts and coffee mugs don't cut it anymore. A modern cybersecurity program projects a consistent and persistent message that cybersecurity is part of how we do business. Cybersecurity awareness needs to evolve from an event to an integral part of who we are as a company.
>
> **—Matt Miller**

Matt Miller
Principal, Cyber Security Services
KPMG LLP

Jacqueline LaScala
Director, Behavior Management & Communications, IT Office of Information Security
Labcorp

[1] Source: IBM, "2014 Cyber Security Intelligence Index"

Bios

About Matt Miller

Matt is a principal in the New York office of KPMG LLP's Advisory Services practice and is the U.S. Cyber Security Services Banking industry lead. With 20+ years of experience Matt's focus areas include insider threat and internal fraud, 3rd party risk, quantitative and qualitative risk assessment, and incident management. In addition to managing programs or advising clients, Matt has published and presented on many subjects, including leveraging capability maturity models to improve risk management, addressing vulnerability in technologies and critical business applications, and establishing governance and metrics to enable effective risk management programs. Matthew will focus on advising our clients in the financial services industry and optimizing our cyber solution offerings.

Prior to joining the firm, Matt worked at a top Investment bank where he led the information risk and fraud programs in the Risk Division, established the firm's Insider Threat program and operated a firm-wide and global data risk management in Technology Risk. Previously Matt worked as a Principal equivalent in several cyber security focused consulting firms.

Areas of expertise

- Cyber Security
- Information Risk
- Insider Threat
- Fraud

Education and qualifications

Bachelor of Science degree in Computer Science and Business from the University of Puget Sound.

About Jacqueline LaScala

Jacqueline is the director of Behavior Management and Communications for Labcorp's Office of Information Security. She has an extensive background in information security, sales, marketing, and communications, with more than 30 years of experience with companies including the *Miami Herald*, the *Atlanta Journal-Constitution*, Microsoft, Mayo Clinic, and the Federal Reserve Bank of Atlanta. For the last eight years, her focus has been on developing a leading-edge behavior management program that applies the principles of social cognitive theory and adult learning methodology to the human side of securing information. Jacqueline's goals are to evolve the personal practice of protecting information from being a choice to a habit and to inspire people to want to learn how to be more secure at work and at home.

Jacqueline is a graduate of the University of Florida, where she received her bachelor's degree in advertising with a minor in psychology. She holds several cybersecurity industry certifications, including Certified Information Security Manager (CISM) and CyberSecurity Awareness Practitioner (CSAP), and is a certified ADKAR Change Management Practitioner. Jacqueline is recognized in the industry for her work in behavior management in healthcare.

Beyond awareness: A persistent approach to changing secure behaviors

To be effective, businesses need to evolve their cybersecurity awareness efforts beyond the annual company-wide talk by the chief information security officer (CISO) on the need for more vigilance around data protection. Instead, organizations should pursue a more integrated, holistic approach that embeds the message of cybersecurity into the employee's workday so that it becomes subconscious.

Statistics show that the initial infection point for many breaches is caused by human error—opening an email, downloading a file, or clicking on a malicious link.[2] Even with adequate firewalls, antivirus, and other technology-based solutions, hackers can infiltrate a company through humans using social engineering tactics, such as phishing, through which people are fooled into revealing sensitive information. It's a serious problem: Phishing attacks account for more than 80 percent of reported security incidents, and statistics show approximately $17,700 is lost every minute due to phishing attacks.[3]

A simple solution to support identification and prevention of phishing attacks is a phishing reporter button. There are several vendors offering this solution. Ideally, the button is ever present within an organization's email environment, acting as a "billboard" to keep cybersecurity top of mind. By making this action simple, staff can immediately report suspicious emails for investigation, essentially making them first responders as human firewalls.

The reporter button can also be used in conjunction with a strong phishing simulation program to teach staff how to identify potentially malicious emails and take action to avoid falling victim. Encouraging the use of the reporter button drives secure behavior, making staff part of the organization's solution to fighting cybercrime.

Cybersecurity awareness programs designed to drive behavioral change among employees should have two fundamental goals.

One is to **move security awareness from being a choice to being a habit.** In other words, the message must reach the part of the brain where it becomes second nature. No longer a one-day meeting or annual training module, this approach to cybersecurity involves persistent and personal engagement that draws on adult learning and behavior reinforcement techniques to create cohesion around the message of secure behavior. It should also leverage the highly visible and vocal support of the C-suite and other senior leadership, as they lead by example by behaving securely and making cybersecurity a priority. This is the technique of modeling.

The second goal is to **engage staff on an emotional level**—that is, to inspire them to want to learn how to be better digital citizens and improve their cybersecurity practices, both at work and at home. There are two key messages needed to achieve this:

- **Why** cybersecurity matters
- **What's in it for them,** individually and personally

Most people resist change. Therefore, making change palatable requires us to strike an emotional chord, which happens when we demonstrate how the security awareness techniques they learn on the job can help them protect their families and personal well-being in the home, where they don't have cybersecurity practitioners to provide support.

---

[2] Source: "Why Human Error is #1 Cyber Security Threat to Businesses in 2021," The Hacker News website, February 4, 2021.

[3] Source: "Top cybersecurity facts, figures and statistics for 2020," CSO website, March 9, 2020.

Leveraging science and adult learning methodology

To drive behavioral change related to cybersecurity, we have learned that the application of social cognitive theory (SCT) is an effective tactic.

Developed by Stanford University Psychology Professor Albert Bandura, a major tenet of the theory focuses on observational learning, also referred to as modeling. That is, the way people learn desirable (or undesirable) behaviors is by observing other people and mimicking those learned behaviors to maximize rewards.[4] This method of learning is particularly effective if people admire, trust, or respect the person who is to be imitated. Simply, we like to be like our heroes.

Applying this learning method to cybersecurity awareness could begin with the CEO delivering a "fireside chat" to employees that focuses on the importance of cybersecurity. It should cover what happens in the case of a breach, how it could affect their job, what a worst-case scenario might be, and what the consequences to the organization might be. The message should also outline how the CEO and the leadership team are working with the cybersecurity team to prevent breaches and how employees can help.

Reinforcing the message by cascading it through leadership demonstrates that the topic is important at all levels of the company. The goal is to reflect a high level of commitment to good cybersecurity practices expressed by leadership to *inspire* employees to adopt that attitude and follow their lead on prevention.

[4] Source: "Social Cognitive Theory: How We Learn from the Behaviors for Others," by Cynthia Vinney

Reinforce behavior by applying change management methodology

Having leadership present the cybersecurity awareness message to employees is only the beginning of the process of driving behavioral change. The message should be persistently reinforced so the change becomes a habit.

We have found that Prosci's ADKAR Model of Change Management, created by founder Jeffery Hiatt, to be an effective tool in this effort. ADKAR stands for awareness, desire, knowledge, ability, and reinforcement. Using the ADKAR model, it is possible to design a program that continually reinforces why cybersecurity is important, why employees must pay attention both at work and at home, and the role they play in supporting the efforts of the cybersecurity team. For example:

A Awareness of the need for change	To drive **awareness,** employees' log-in screens can display a reminder message, such as "Report phishing."
D Desire to participate in and support the change	To drive **desire,** a series of "what if?" scenarios can outline potential ramifications of not practicing secure behaviors.
K Knowledge of how to change	To drive **knowledge,** interactive phishing simulations can be run periodically that include in-the-moment educational information for those who "fall victim."
A Ability to implement required skills and behaviors	To drive **ability,** a button can be installed on their email toolbar to make it easy to report suspicious messages to the cybersecurity team.
R Reinforcement to sustain the change.[5]	To **reinforce** that behavior, employees who report suspicious emails can receive a response thanking them for being vigilant and taking action. If the report does uncover malicious activity, the employee can receive additional acknowledgment of their help, reinforcing good behavior: "Thank you! Because of your efforts and vigilance, you helped prevent cybercrime through malicious email."

These strategies not only make employees feel like they are part of the team, but they also encourage feelings of accountability and ownership. It is also critical to create an environment that is supportive, rather than punitive, so if an employee does accidently click a link they shouldn't have, they aren't afraid to report it.

[5] Sources: "Top cybersecurity facts, figures and statistics," CSO website, March 9, 2020. and Prosci Change Management Methodology, Prosci website.

Modern delivery methods make training entertaining

Effective behavior management and communications programs require periodic training to keep all staff, including leadership, informed about best practices and policy changes to.

However, companies should consider moving beyond traditional training methods, such as slide presentations and prerecorded videos, to modern delivery methods that elevate the cybersecurity conversation, from mundane to inspiring. By employing innovative technologies, training can be interesting, competitive, engaging, and even fun.

A popular technology is gamification, which can provide scenarios through which employees can practice the skills they learn in a safe environment. Gamification has been shown to increase learner motivation and engagement levels, and can influence behavioral change.[6]

People learn in different ways. There are three main cognitive learning styles: visual (seeing and reading), auditory (hearing and speaking), and kinesthetic (doing).[7] Training, therefore, should be made available to accommodate each learning style, eliminating barriers to entry, and delivering information in the format preferred by the learner. In today's fast-paced digital world, we found that brief, easily digestible segments are most successful.

Make it personal

Employees must feel personally invested if behavioral change is to be successful and sustainable. For example, explaining to the staff how a particular online behavior can protect their children from online predators, as opposed to solely protecting company data or themselves, can have a profound impact. Program elements should connect the dots between the cybersecurity skills learned at work and how they can be applied at home.

The concept is to encourage employees to think of themselves as the CISO of their household. To help get that message to employees, companies can set up an online environment that hosts a variety of resources on cybersecurity to be shared freely with the employees' friends and family members. Children and elderly parents can be invited to virtual events focused on cybersecurity awareness and education.

Making it personal is even more crucial today with so many employees working from home. In addition to protecting corporate assets, many employees now find themselves in charge of cybersecurity for multigenerational families with widely varying levels of technical sophistication, including online shoppers, gamers, and children attending school online. This increase in remote access to private services inevitably leads to greater risk of breach or attack. Cybersecurity awareness programs should consider the constant evolution of the workforce and the environment in which employees work to address the specific risks accordingly.

In practice, when employees feel that their company is taking care of them by helping to keep their families safe online, they are more likely to help keep the company safe from cyber threats.

---

[6] Source: "Games Companies Play: How Your Company Can Implement Gamification To Motivate Employees," Forbes website, February 18, 2020.

[7] Source: Robert Half, "3 Different Learning Styles and How to Use Them in Your Career," August 5, 2016.

Give your program an overall theme and communicate regularly

A behavior management and communications program should have an overall theme and brand. The theme, including a specific name, logo or masthead, and strong tagline, should be applied liberally to all program components to become part of the fiber and culture of the organization.

Every element of the program—log-in screen messages, training materials, websites, emails—should reflect the brand's unique look and feel so everyone in the organization recognizes it and understands its importance.

In addition to widespread branding, another element of a persistent program is scheduled, as well as event-specific communications. For example, a communications program commonly includes four key elements:

Monthly bulletins that are educational, focused on a timely or relevant topic

Notifications that are informational; for example, announcing the rollout of a new cybersecurity tool

Advisories that are positional; for example, to establish proper use of third-party applications or state when not to use them at all

Alerts that are actionable and part of the incident response plan to engage employees during an attack or active investigation, and instruct them to take immediate action, such as changing passwords.

How to measure success

Tracking and reporting the success of the cybersecurity behavior management and communications program is imperative to success and sustainability. In many cases, progress is reported to the C-suite and board of directors.

There are several metrics around behavior management that can be considered to measure change, including:

- Number of suspicious emails flagged through the reporter button
- Participation in live events and presentations
- Number of reported emails that are malicious
- Visits to and interaction with the cybersecurity website
- Resiliency rate from simulated phishing programs
- Participation in staff contest events
- Completion of training modules
- Feedback via employee surveys
- Engagement with the cybersecurity team through a department-specific branded email address

How to begin

The preceding sections have outlined a model cybersecurity behavior management and communications program. However, an organization should design the details of its program to match its unique culture and business.

Establish a target: Program owners—those who initiate the design, development, and implementation of the program and are ultimately responsible for its success—should start by completing a gap analysis to assess employees' understanding of cybersecurity and establish a benchmark for the organization. They will need to engage with the company's senior leadership to help relay the importance of a behavior management program and will need the freedom to learn about the company's structure, leadership hierarchy, specific use cases, and culture. These insights will help determine the most effective means for communications, frequency of messages, tone, and approach.

Design it: Building and executing a comprehensive program requires collaboration. To begin, program owners should be professionals with a marketing, sales, and communications background. They should have superior writing skills with the ability to translate technical information into layman's terms. They should understand the science of SCT and adult learning methodology, as well as change management practices. The gap analysis, initial research, and benchmarking activities should be used to formulate a comprehensive strategic plan that captures the program's goals, objectives, tactics, and timelines.

Build it: In addition to the program owners, groups with various skills and expertise will be needed to fully develop and execute the program.

Program sponsors: These are senior leaders who are well-known and respected by staff; they should be enthusiastic and vocal supporters of the program and be willing to represent why the program matters, the role staff plays in supporting it, and clearly articulate what's in it for staff, both professionally and personally.

Cybersecurity practitioners: These subject matter experts will help the program owners develop content to be delivered to staff through multiple delivery methods (e.g., routine and timely communications, website content, training modules, and other passive and active elements).

Marketing and corporate communications: These teams can help develop the program's brand, look and feel, and initial program elements that are visible to staff. In addition, the program owners should proactively establish standard operating procedures with the corporate communications team for incident response/crisis communications.

Information technology (IT) practitioners: IT staff may be needed to deploy technology-based program elements, such as the phishing reporter button.

Final thoughts

Phishing and similar attacks continuously advance in their sophistication, thus increasing cybersecurity risks. By investing in the human element of cybersecurity, an organization can help its workforce become not only savvier about cybersecurity, but also an extension of the cybersecurity team committed to keeping the organization safe.

Firewalls and other cybersecurity technologies are necessary elements for protection in an ever-expanding digital environment, but they do not address the human element.

A holistic approach to protecting an organization requires an investment in people, the "human firewall," to ensure that employees not only understand the tenets of cybersecurity, but they also embrace their role in supporting the organization's efforts by making secure behaviors an integral part of their daily life.

No longer can we rely on an annual check-the-box compliance activity. By applying the science of social cognitive theory and adult learning methodology, we evolve beyond traditional "security awareness" to a more effective and contemporary behavior management and communications program to help employees become better digital citizens at work and at home.

Contact us

Matt Miller
Principal
Cyber Security Services
T: 212-954-4648
E: matthewpmiller@kpmg.com

Jacqueline LaScala
Director
Behavior Management & Communications
IT Office of Information Security
Labcorp
T: 336-436-8169
E: lascalj@labcorp.com

www.kpmg.com/us

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia