Human firewalling

Overcoming the human risk factor in cyber security.

KPMG International

home.kpmg/cybersecurity

Foreword

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

Companies spending millions of dollars today on modern cyber security technology solutions continue falling prey to hackers using clever phishing schemes like these.

While firewalls and other technologies can be the bedrock of an organization's cyber security program, they can't protect everything. Studies show that 88 percent of reported breaches include some element of human error.[1] For busy employees whose inboxes are inundated with messages on a daily basis, it's easy to be fooled by a malicious email — and hackers know it. That makes it critical for businesses to develop and maintain a comprehensive cyber security strategy that clearly addresses the human factor.

Many organizations typically address cyber security with their employees only once a year — often at a company-wide event during October, 'Cyber Security Awareness Month.' While these events are valuable, the security awareness message presented often fades quickly and fails to make any meaningful — and necessary — change in employee behavior.

At KPMG, professionals work with the Behavior Management and Communications team of Labcorp's Office of Information Security. They've seen evidence that, to protect an organization, a cyber security program must move beyond annual 'check-the-box' activities, as there is a crucial difference between being compliant and being secure. What is needed is a more integrated, holistic approach that incorporates cyber security measures into each employee's workday in such a way that proven best practices become a habit rather than a choice.

The ideal result is a cultural shift in which employees acknowledge the importance of cyber security, adopt a cyber security mindset, see themselves as part of the cyber security team, and are inspired to learn and do more.

The following pages describe some of the key elements of a successful integrated cyber security Behavior Management and Communications program and the steps to begin creating one for your organization.

> Cyber security 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 need to be aware of the program and be on board.
>
> — **Jacqueline LaScala, Labcorp**

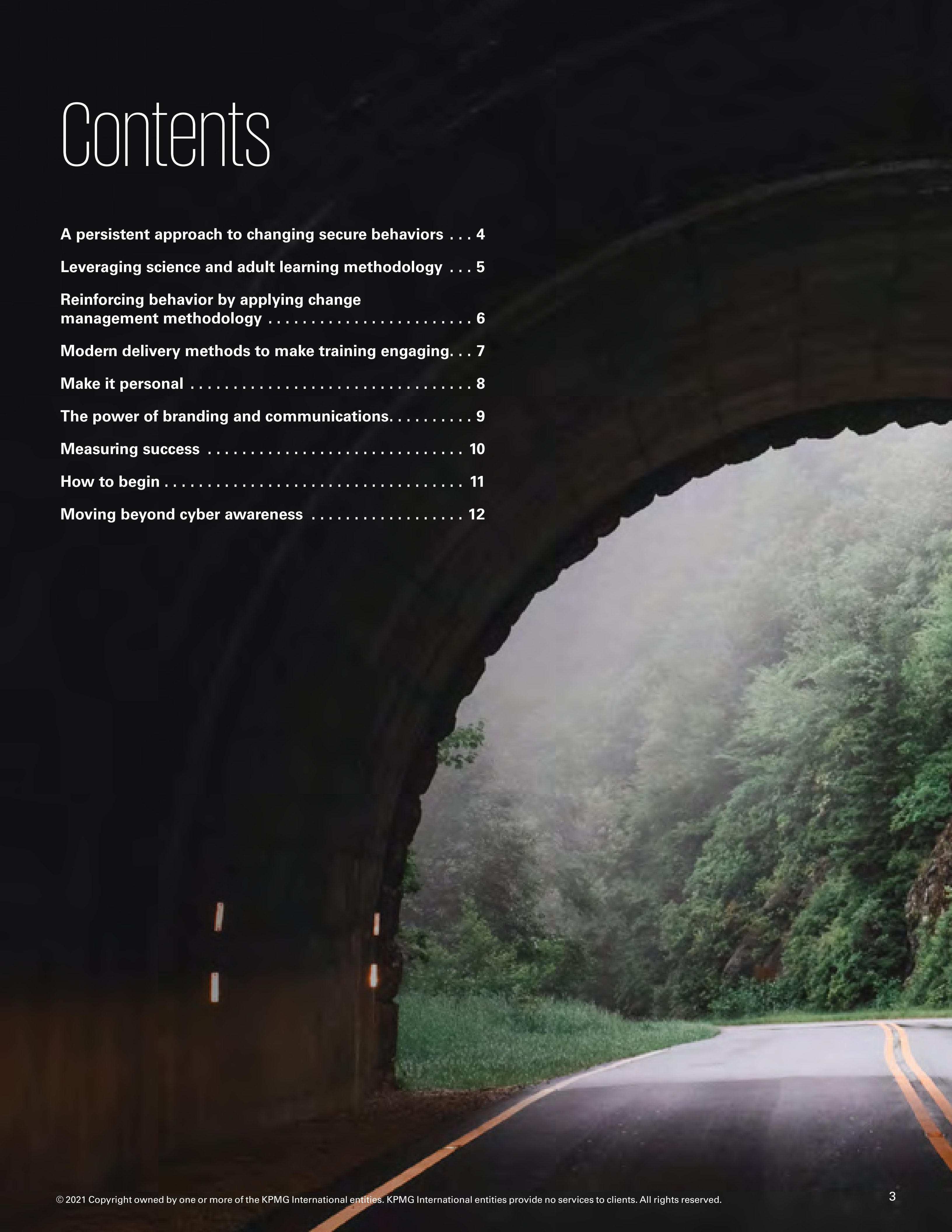
> T-shirts and coffee mugs don't cut it anymore. A modern cyber security program projects a consistent and persistent message that cyber security is part of 'how we do business'. Cyber security awareness needs to evolve from an event to an integral part of who a company is.
>
> — **Fred Rica, KPMG in the US**

Fred Rica
Principal, Cyber Security Services
KPMG in the US

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

[1] Jeff Hancock, "The psychology of human error," Stanford University, 2021.

KPMG



Contents

A persistent approach to changing secure behaviors

To be effective in today's fast-evolving world of continually emerging cyber threats, businesses should be seeking to evolve their cyber security awareness efforts beyond the annual company-wide talk by the Chief Information Security Officer (CISO) on the need for more vigilance around data protection. Organizations should pursue a more integrated, holistic approach that embeds cyber security practices into the employee's workday.

Statistics show that human error is the initial infection point for many breaches: opening an email, downloading a file or clicking on a malicious link.[2] Even with adequate firewalls, antivirus tools and other technology-based solutions, hackers can infiltrate a company through human error using social engineering tactics, like phishing, through which people are fooled into revealing sensitive information.

It's a serious problem: phishing accounts for more than 80 percent of reported security incidents, and statistics show that about US$17,700 is lost every minute to these attacks.[3]

A 'phishing reporter' button is one simple solution that can help businesses identify and prevent costly phishing attacks. There are several vendors offering this solution. Ideally, the button is ever-present within an organization's email environment, acting as a 'billboard' that keeps cyber security top-of-mind.

By making this action simple, staff can immediately report suspicious emails for investigation, essentially making them first responders by acting 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 can help to drive secure behavior, making staff part of the organization's solution to cybercrime.

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

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 cyber security demands persistent personal engagement that draws on adult learning and behavior-reinforcement techniques to create cohesion on the need for secure behavior. It should also leverage the highly visible and vocal support of the C-suite and senior leadership, as they lead by example by behaving securely and making cyber security a priority. This is the technique of 'modeling'.

Engage staff on an emotional level. Cyber security awareness programs should inspire every employee to be a better digital citizen and improve cyber security practices both at work and at home. There are two key messages needed to achieve this:

— why cyber security matters

— what's in it for them individually and personally.

People typically resist change. Therefore, making change palatable requires it to strike an emotional chord. That happens when security awareness techniques used at work are shown to also help protect the personal well-being of employees and their families at home, where they have no cyber security practitioners to provide support.

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

[3] "Top cyber security facts, figures and statistics for 2020," CSO website, March 9, 2020.

Leveraging science and adult learning methodology

To drive behavioral change that can help enhance cyber security, KPMG professionals have learned that applying social cognitive theory (SCT) is an effective tactic.

Developed by Stanford University psychology professor Albert Bandura, a major tenet of SCT 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 learning method is particularly effective if people admire, trust or respect the person who is to be imitated. Simply put, people like to be like their heroes.

Applying this learning method to cyber security awareness could begin with the CEO sharing a 'fireside chat' with employees focusing on the importance of cyber security. It should cover what happens during a breach, how it could affect their job, what a worst-case scenario looks like, and the potential consequences for the organization. The message should also outline how the CEO and leadership team are working with the cyber security team to prevent breaches — and how each employee 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 leadership's commitment to appropriate cyber security practices and inspire employees to adopt that attitude and follow their lead.

[4] Cynthia Vinney, "Social Cognitive Theory: How We Learn from the Behaviors of Others," ThoughtCo, January 20, 2019.

Reinforcing behavior by applying change management methodology

Leadership's role in presenting the cyber security awareness message to employees is only the beginning of the behavioral-change process. The message should be persistently reinforced so that the proposed change becomes a habit.

KPMG firms have found that Prosci's ADKAR Model of Change Management, created by founder Jeffrey Hiatt, is an effective tool in this effort. ADKAR stands for:

A **Awareness of the need for change**

D **Desire to participate in and support the change**

K **Knowledge of how to change**

A **Ability to implement required skills and behaviors**

R **Reinforcement to sustain the change**[5]

The ADKAR model enables a program that continually reinforces why cyber security is important, why employees must remain vigilant both at work and at home, and the critical role they play in consistently supporting the cyber security team. For example:

- To drive **awareness**, employee login screens can display a reminder message such as: 'Report phishing.'
- To drive **desire**, a series of 'What if?' scenarios can outline potential ramifications and threats when not practicing secure behaviors.
- To drive **knowledge**, interactive phishing simulations can be run periodically, including in-the-moment educational information for those who fall victim.
- To drive **ability**, a button can be installed on email toolbars to report suspicious messages to the cyber security team.
- 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! Your efforts and vigilance have helped us prevent cybercrime through discovery of a malicious email."

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

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

Modern delivery methods to make training engaging

Effective Behavior Management and Communications programs require periodic training to keep all staff, including leadership, informed about industry best practices and policy changes.

However, companies should consider moving beyond traditional training methods, such as slide presentations and pre-recorded videos, to modern engagement methods that elevate cyber security conversations from mundane to informative and inspiring. By employing innovative technologies, for example, training can become interesting, competitive, engaging — even fun.

Gamification is one popular technology, providing scenarios that let employees practice new skills within 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). Training should cater to each learning style — eliminating barriers to entry and delivering information in the format preferred by the learner. In today's fast-paced digital world, brief, easily digestible segments appear to be the most successful.

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

Make it personal

Employees must feel personally invested if behavioral change is to be successful and sustainable. For example, explaining to staff how a particular online behavior can protect their children from online predators, in addition to protecting company data or themselves, can have a profound impact. Program elements should connect the dots to emphasize how workplace cyber security skills can be applied at home.

The concept aims to encourage employees to think of themselves as the CISO of their household. To help get that message to employees, companies can create an informative online platform, featuring a variety of cyber security resources that can be shared freely with employees' families and friends. Children and elderly parents can attend virtual events that focus on cyber security awareness and education.

With so many employees working from home today, taking a personal approach has become crucial. Beyond protecting corporate assets, many employees now find themselves managing cyber security for multigenerational families possessing diverse 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 a breach or attack.

Cyber security awareness programs should consider the constant evolution of workforces, and the specific environments in which employees work, in order to address all 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.

The power of branding and communications

A Behavior Management and Communications program should have an overall theme and brand. The theme — including a specific name, engaging tagline, and logo or masthead — should be applied liberally to all program components to make them part of the organization's fiber and culture.

Every element of the program — login 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, an effective program should include ongoing communications that are both regularly scheduled and event specific. For example, a communications program should include four key elements.

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

Advisories that are positional, for example, to establish proper use of third-party software apps or stating when not to use them.

Notifications that are informational, for example, announcing the rollout of a new cyber security tool.

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.

Measuring success

Tracking and reporting the success of the cyber security 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 cyber security website
- Resiliency rate from simulated phishing programs
- Participation in staff contest events
- Completion of training modules
- Feedback via employee surveys
- Engagement with the cyber security team through a department-specific branded email address

How to begin

The preceding sections have outlined a model cyber security 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 cyber security 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.

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.

Cyber security 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).

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

Moving beyond cyber awareness

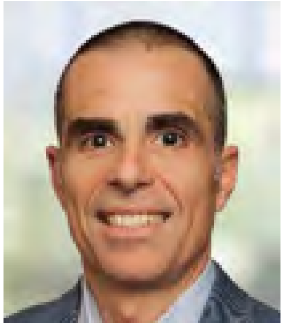
As phishing and similar attacks become more sophisticated, cyber security risks are soaring. By investing in the human element of cyber security, organizations can foster workforces that are not only savvier about cyber security but also a crucial extension of the cyber security team through their commitment to keeping the organization safe.

While firewalls and other cyber security technologies are indispensable to enhancing protection in today's ever-expanding digital environment, 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 both understand the tenets of cyber security and embrace their role in supporting security efforts by making secure behaviors an integral part of their daily life.

By moving beyond 'check-the-box' compliance and applying the science of SCT and adult-learning methodology, businesses can evolve beyond traditional 'security awareness' to a more effective and contemporary Behavior Management and Communications program — helping employees become better digital citizens at work and at home.

About the authors



Fred Rica

Fred Rica is a Principal in KPMG Cyber Security and the National Sales Enablement Leader for KPMG in the US. He is a skilled technology professional with significant experience in cyber security and technology risk management. A nationally recognized authority on information security, he has performed and managed hundreds of security assessment, design and implementation projects over the last 30 years. He has helped many of the world's foremost users of technology solve complex risk-management issues.

Fred has a bachelor's degree in Finance from Rutgers University. He is a frequent presenter and commenter on the topic of information security and risk and has spoken at numerous conferences, including the Black Hat Briefings, RSA Conference and the NACD Summit. He is often quoted in major print media and has appeared on major networks.

Jacqueline LaScala

Jacqueline LaScala 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.

For the last 8 years, her focus has been on developing a leading-edge behavior management program that applies the principles of SCT and adult learning methodology to the human side of securing information.

Jacqueline is a graduate of the University of Florida and holds several cyber security industry certifications, including Certified Information Security Manager (CISM) and Cyber Security Awareness Practitioner (CSAP), and she is a Certified ADKAR Change Management Practitioner. Jacqueline is recognized in the industry for her work in behavior management in healthcare.

Contact us

Fred Rica
Principal
Cyber Security Services
KPMG in the US
E: frica@kpmg.com

Jacqueline LaScala
Director
Behavior Management and Communications
Office of Information Security
Labcorp
E: lascalj@labcorp.com

Akhilesh Tuteja
Global Cyber Security Leader
KPMG International, and Partner
KPMG in India
E: atuteja@kpmg.com

Matt O'Keefe
ASPAC Region Cyber Security Leader, and Partner
KPMG Australia
E: mokeefe@kpmg.com.au

Dani Michaux
EMA Region Cyber Security Leader, and Partner
KPMG in Ireland
E: dani.michaux@kpmg.ie

Prasad Jayaraman
Americas Region Cyber Security Leader, and Principal
KPMG in the US
E: prasadjayaraman@kpmg.com

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure, please visit "https://home.kpmg/xx/en/home/misc/governance.html" home.kpmg/governance.

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

Design by Evalueserve.
Publication name: Human firewalling
Publication date: October 2021
Publication Number: 137704-G