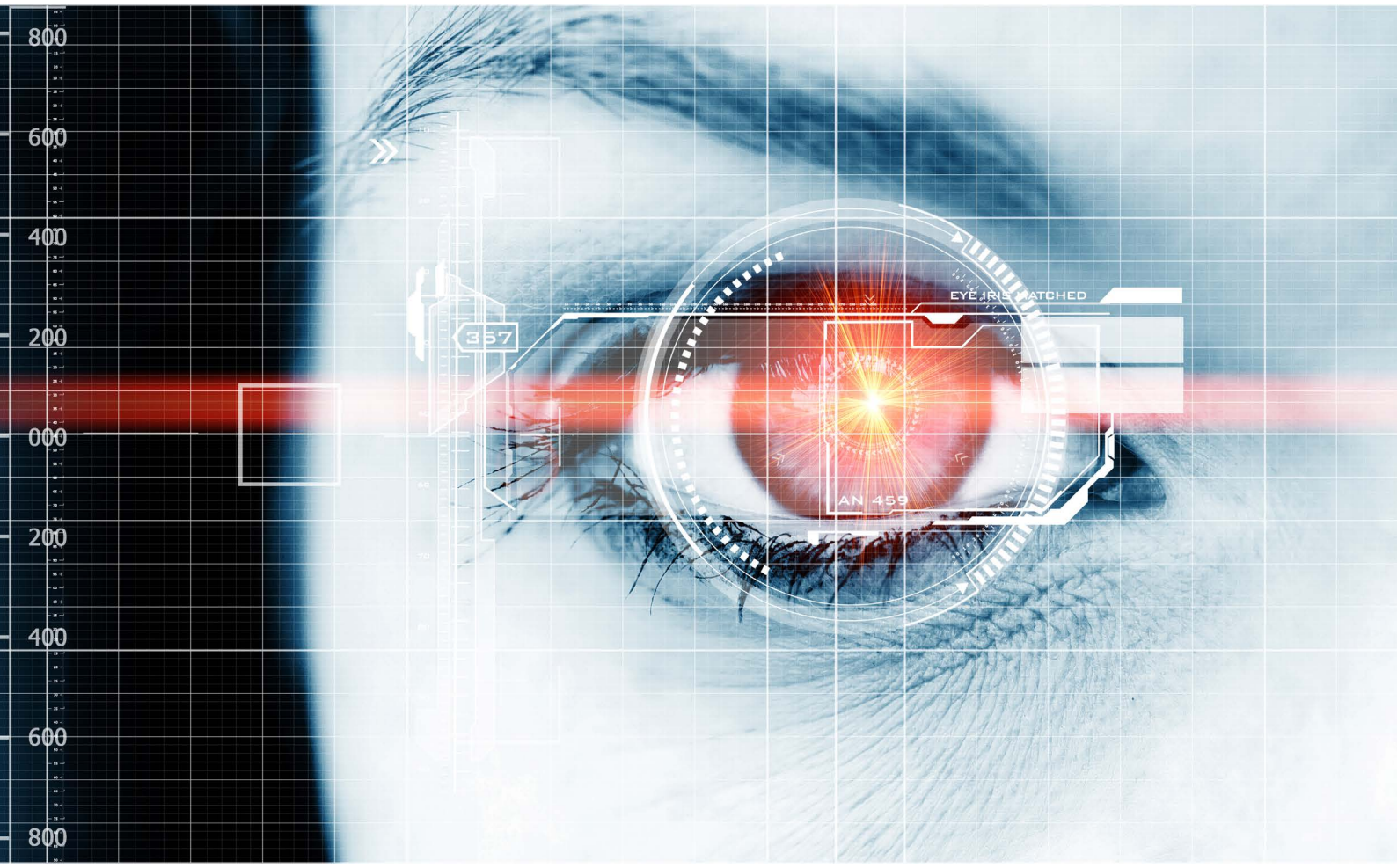
THE PEOPLE FACTOR IN CYBER BREACH:

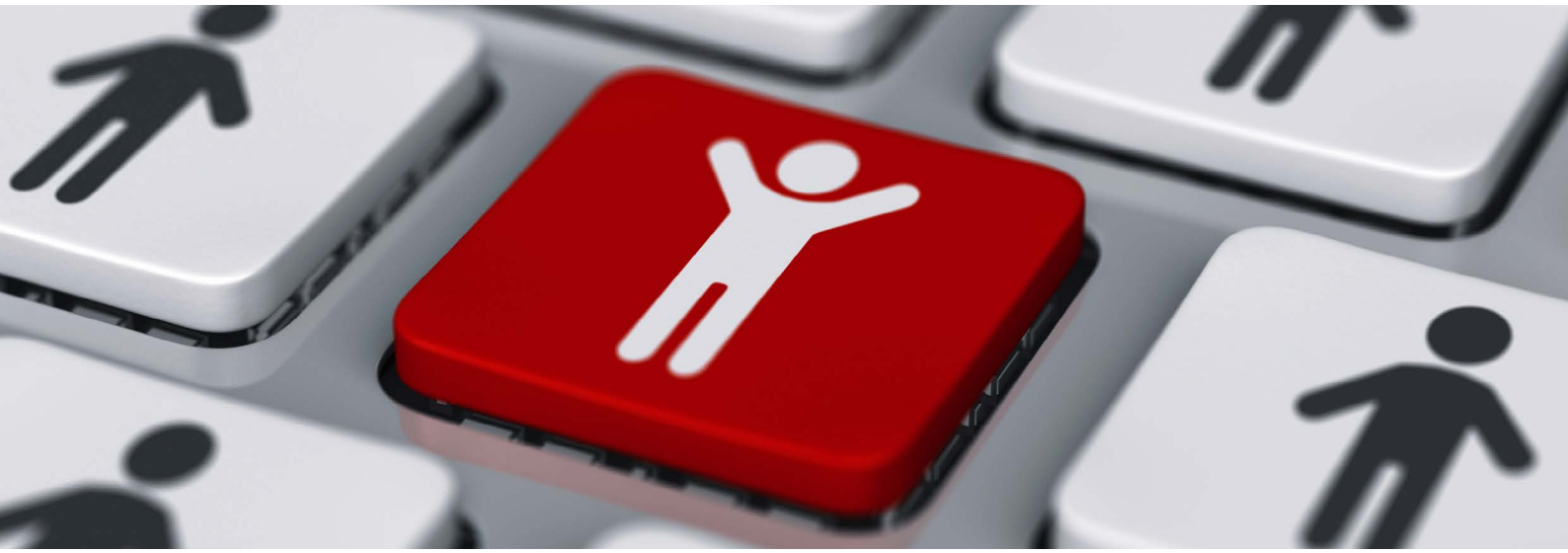
Three Key Elements for Building an Effective Human Firewall

By Peter Schablik and Scott M. Higgins



MAZARS

WeiserMazars



INTRODUCTION

Without a change in perspective, we risk losing the cyber war being waged on businesses by sophisticated nation states and criminal organizations. Traditional approaches to evaluating risks and controls are insufficient to prevent cyber-attacks. Risk assessments focusing on the people, processes and technology overemphasize the information technology organization. The critical focus needs to be on the "user"--since even a world-class information technology function can be interrupted by a single action performed by an individual user. Internal audit needs a fresh perspective that emphasizes the individual user--who is the front line of cyber readiness--in addition to any administrative, physical and technical controls. This whitepaper will provide a framework for conducting internal audits to evaluate three key elements of preparing users to be threat-ready.

Cyber-attacks aren't just getting more frequent, they are also becoming significantly more vicious and sophisticated. Gone are the days when an obviously fraudulent email arrived from a foreign country asking for a bank account number. Today's cyber-attacks are far more targeted and subtle, and the stakes are high regardless of company size or industry – no one is immune. A cyber breach can devastate a company, and carries the far-reaching negative impacts that continue to ripple outward long after the initial financial losses. These indirect damages include a tarnished brand reputation, lost relationships, and possible legal liability.

Cyber criminals count on the fact that busy people perform hundreds, if not thousands, of daily actions on a computer or device connected to the internet and they know that most of those actions are performed automatically and without much thought. As a result, the majority of today's data breaches result from human error, making cybersecurity a "people problem" as well as a technology issue. The solution to this people problem goes beyond IT, and it can't be solved by purchasing new hardware or software or implementing sophisticated and thorough network testing. Instead, it involves cultivating an entirely new employee mindset around cybersecurity--one that is motivated by more than facts and fear, one that is based on continually raising awareness and putting secure actions and decisions at the forefront of the company culture.

THE STAKES ARE HIGH

Cyber-attacks represent enormous losses for companies, making them one of the greatest risks for a business today. An organization that experiences a cyber breach faces dramatic and immediate financial repercussions. According to the latest figures from the Ponemon Institute, the average cost of a data breach

has reached nearly $6.5 million in the U.S. Some of the costs associated with compromised data are direct, and incurred when companies remediate the damage done. This may involve finding the malicious software or network vulnerability and fixing it, purchasing new hardware and software, repairing infrastructure, and making direct amends to customers or others whose information is now potentially at risk.

Beyond those direct expenses, however, lies more serious damage. The indirect costs of a data breach are far-reaching and can continue long after the immediate damage is repaired. Perhaps the most serious indirect cost is to a company's reputation and brand. Once customers, vendors, and partners find out that a company has fallen victim to a data breach, its reputation is tarnished, perhaps beyond repair. The company name and brand become associated with risk to sensitive information, to finances, and to security. When data is perceived as no longer safe, vendors, customers, employees, sales prospects, and anyone else who deals with the company loses trust, and regaining that trust is much more difficult than removing malware from the network or strengthening the company firewall. While a large company that falls prey to cyber criminals, like Sony or Target for example, can weather the storm and eventually regain its reputation, a less established brand may never recover.

A cyber breach also represents legal liability. When cyber criminals attack a company, they gain access to its most valuable assets—intellectual property, employment records, contracts, financial details, succession plans, compliance records…the list is endless. Exposure and/or loss of this type of sensitive corporate data can lead to lawsuits that are costly to defend, no matter the outcome. For example, a data breach could expose information about a pending acquisition or sale, make public information about a recently renegotiated contract with a client, or compromise plans to release a new product or service. All of these carry with them the risk of litigation.

THE PROBLEM IS THE PEOPLE

IBM's 2015 *Cyber Security Intelligence Index* revealed that 95 % of cyber breaches occur as a result of human error. Since nearly every employee at every level of an organization engages in many connected activities throughout the day, some of these actions represents risk when it comes to cybersecurity.

Meanwhile, cyber criminals are developing increasingly more sophisticated attacks that are designed to precisely hit their marks. According to the latest research from IBM Security Intelligence, the average number of security events detected dropped to 81 million in 2014 from nearly 92 million in 2013, but the number of incidents remained constant. In other words, while the attempts were lower by 12 percent last year, the amount of successful breaches remained the same. This shows that even though IT detection efforts are improving, so are the cyber criminals. This makes the human element in cybersecurity even more critical, and adds urgency to finding more effective methods to address it.

KEY ELEMENTS REQUIRED FOR LASTING BEHAVIOR CHANGE

Cyber criminals count on the fact that at least a portion of any employee population won't have the information or awareness necessary to fend off an attack.

The average employee typically doesn't recognize the role he or she plays in the company's cybersecurity defenses or truly understand the consequences of his or her actions. Even employees who are equipped with adequate knowledge and awareness may simply not care enough to take the time and effort during their busy day to make a better decision.

Fortunately, the significant risks that clicking, tapping, and browsing employees represent can be effectively mitigated with a well-thought-out and carefully delivered cybersecurity campaign that includes three key elements.

"CYBERSECURITY AWARENESS AND ACTIVE PARTICIPATION ARE NECESSARY FOR A STRONG CORPORATE CULTURE IN TODAY'S BUSINESS ENVIRONMENT. AND A STRONG CORPORATE CULTURE IS A VITAL ELEMENT IN ACHIEVING THE EXCELLENCE IMPLIED IN MOST COMPANY VALUES AND IN MEETING THE EXPECTATIONS OF SHAREHOLDERS AND CUSTOMERS ALIKE."
says Marcus McInnis, COO at Lone Star International and former Director of Operations for Lockheed Martin's Cybersecurity Innovation Center

Long Term Behavior Change

1. Make People Care.

Many companies make the classic training mistake of pushing lots of information at their employees without first taking the time to help them understand why the topic matters or why it should be relevant to them.

If employees don't care about a subject, they won't take the time to absorb the information you're providing, no matter how comprehensive or accurate. Instead, they'll simply click through even "mandatory" training and move on to the next task.

Any effective cybersecurity program must start with this human element—for example, mining behavioral psychology research and the art of persuasion for tactics and techniques that get employees invested in the subject and help them become more receptive to the learning or awareness activities that follow.

For instance, peer-to-peer recognition and group norms can be a powerful influence. Personal and direct language like "we're counting on you" and "it's up to all of us," along with comments by managers and company leaders can help convince employees that cybersecurity is important to the company and deserves their attention.

In the same way, a well-crafted merchandising campaign—using powerful, catchy slogans printed on buttons, pens, posters, t-shirts, or mouse pads—can help communicate that cybersecurity is a core part of the culture and work environment. Employees may change their behavior not only because they know the facts, but because they don't want to let down their coworkers and employer.

Ideally, this type of material will work to create a positive team environment where everyone's participation in cybersecurity is important, recognized, and even celebrated.

" Cybersecurity awareness and active participation are necessary for a strong corporate culture in today's business environment. And a strong corporate culture is a vital element in achieving the excellence implied in most company values and in meeting the expectations of shareholders and customers alike." Said Marcus McInnis, COO at Lone Star International and former Director of Operations for Lockheed Martin's Cybersecurity Innovation Center.

2. Build Awareness and Knowledge.

Once people care, it's possible to start building a level of awareness and knowledge that will ultimately drive real change in individual and group behaviors over time.

Here, it's important to design a program based on methods that actually work, rather than a "one and done" approach that simply ticks the "training" box. A successful awareness campaign alerts employees to key risks and enables them to instinctively make the right decisions when going online, using devices, and handling company information.

The need for effective solutions to counter the serious threat cyber attacks pose has been recognized by Federal agencies for more than a decade. In 2003, the U.S. government asked the National Institutes of Standards and Technology (NIST) to devise cybersecurity guidelines that would assist government agencies in better preparing for cyber-attacks

and avoid the serious implications they cause both for individual organizations and for the security of the nation as a whole.

In 2014, at the President's request, NIST outlined an even more comprehensive Cybersecurity Framework that reiterated the importance of these types of awareness activities. Both documents make it clear that companies need to do more than simply train people in good cyber practices. They must continually create awareness among employees at all levels.

This distinction was reinforced by standards released by the International Organization for Standardization (ISO) in 2012, which was aimed at helping to ensure the safety of online transactions and protect personal information exchanged via the Internet. As well as providing a structured framework for information sharing, coordination, and incident handling, ISO's standard specifically referenced the need for both training and awareness.

In the framework that NIST developed and ISO references, the "awareness" component of cybersecurity falls under the "Protect" function. According to NIST's documentation, protection involves developing and implementing the appropriate safeguards to ensure delivery of critical infrastructure services. It also supports the ability to limit or contain the impact of a potential cybersecurity event. NIST lists "Awareness and Training" under this important "Protect" area, and it supports the important distinction to be made between these two terms.

Training and awareness are not the same (although the two can work hand in hand), and each creates a different level of protection. An awareness program asks employees to do much more than sit down once a year for 30 minutes, memorize a list of facts and strategies, pass a test, and move on. Instead, awareness activities integrate a deep, instinctive layer of knowledge into the automatic actions employees take as they go about their daily work. It motivates people to stop, slow down, think twice, and make a wiser decision.

Employees must be equipped with, strategies, rules, and basic knowledge about cyber risks and how to mitigate them. They must understand how their actions and behaviors affect the risk of a breach and learn the correct actions to take in order to fend off cyber attacks and stay in compliance with company policies and procedures. Many companies have added cybersecurity to their employee education curriculum in an effort to proactively reduce their cyber breach risk.

Unfortunately, traditional training methods are not enough to effectively protect against this threat because, unlike other risks an organization faces, this one requires every employee to be in a constant state of alert. Employees must adopt a questioning attitude that will affect every action they perform each day.

Advanced learning techniques draw heavily on the recent research into brain science, behavioral psychology, and persuasion—techniques that really work to influence or redirect individuals to a desired outcome. The most effective awareness campaign incorporates up-to-date, research-based techniques like:

- Active practice—asking the audience to apply the concepts, instead of passively receiving the information.
- Spaced retrieval—fast learning leads to fast forgetting, while long-term retention results from information being retrieved regularly over a period of months to strengthen the pathways to permanent retention.
- Interleaving—presenting previous concepts interleaved with new concepts to expose the brain to a combination of events that closely relates to everyday experiences.
- Memory cues—taking advantage of the way human brains create memories to make concepts stick, by using mnemonics, vivid images, analogies, rhymes, or slogans.

Effective awareness also draws from other persuasive fields that specialize in getting targeted messages across, like advertising. Modern communication incorporates tried-and-true advertising principles like:

Make it short. People have moved to a culture of hyper-attention, which is partly a response to being confronted with nearly limitless amounts of information. People simply tune out anything that's too long, instead preferring to consume information in bite-sized pieces. This means that short, well-crafted messages have the best chance of getting through and engaging the audience. An effective cybersecurity awareness program will be presented in short, easily digestible, well-planned units. Micro bursts of information can be integrated in an employee's work day, so they aren't required to spend 40 minutes or more sitting in a teaching session, and they can still drive significant (and measurable) shifts in knowledge, awareness, and behavior over time.

Make it personal. Online communication today is highly personalized—"mass customization" is the norm—and it has changed what people expect from any messages they receive. People now quickly screen out information that doesn't seem directly relevant to them—including the depersonalized boilerplate language common in traditional corporate training. The best material is written like natural conversation between two people. It invites a personal connection and creates a sense of understanding and belonging. It also takes the time to show people how and why the information is relevant to them, rather than simply imparting a laundry list of facts and rules.

Make it engaging. In a world of limitless information, we have to work harder to get people's attention—and the quality of the message matters. Companies today are discovering what advertisers have always known—that getting a message to truly resonate with an audience requires more than just telling them what you want them to know. Effective communication must gain their attention, spark their interest, and create a desire to know the information. When information is communicated in a manner that is as engaging as possible, it both captures and rewards the audience's attention.

3. Measure and Monitor.

When driving behavior change, there is no magic bullet. Progress will happen over time, and different methods will prove more or less effective for a particular company, culture, risk profile, and employee base.

As a result, creating and deploying a research-based, best practice cybersecurity program to employees is just the first step. Programs also need to be updated over time to reflect new risks, technologies, and threats. They should be carefully reviewed and measured—not just once, but systematically over time—to identify, implement, and test possible improvements that might make the program even more effective.

According to the NIST 2003 guidelines, CIOs, IT managers, and anyone else responsible for planning and deploying cybersecurity programs to employees should be "primary advocates for continuous improvement." These program owners should regularly monitor progress, measure results, and plan improvements or adjustments to the program that make the program more effective—as measured by results—for the employees receiving it.

Over time, measuring and monitoring should become even more nuanced and sophisticated. So, for instance, in year 1, a company might simply measure changes in attitudes on a cultural survey and improved performance on phishing simulations. But a more mature program might look at other criteria that signal awareness and engagement. Some of these, mentioned by NIST, might include:

- Frequency of executive/senior messages to staff on relevant cybersecurity topics
- Metrics that show a decline in security incidents or policy violations
- Increasing percentage of employees receiving or interacting with awareness materials
- Attendance at mandatory security forums or briefings

At a minimum, companies should deploy an annual (or bi-annual) survey that tracks attitudes, awareness, and knowledge of key cybersecurity risks, as well as an employee's level of confidence that he or she has the information needed to work securely. Repeating the same questions year on year will help demonstrate progress—or lack of it—as the program unfolds.

ASSESSING A COMPANY'S APPROACH

Most companies fall somewhere along a continuum when it comes to creating an effective human firewall and mitigating the risk human error poses in a potential cyber breach. To assess the effectiveness of a company's current approach, it's important to measure employee awareness, attitudes, knowledge, and motivation regarding the cybersecurity materials, policies, and trainings they have provided.

Carefully crafted survey questions are an invaluable tool for helping companies through this assessment process. These questions serve two purposes: They assist in establishing current employee knowledge and awareness levels in relation to company-provided cybersecurity information and policies, and they prove training and awareness campaign effectiveness (or highlight areas for improvement) when they are used as a post-campaign survey. In effect, they show how much the needle moves—and indicates where there is still room for improvement.

It provides valuable information to companies regarding the level to which cyber awareness has taken root in their corporate culture, and highlights shortcomings that could raise cyber risk and that warrant further action.

CONCLUSION

Used properly, the three key elements described here can cultivate a culture of cyber awareness where employees recognize and avoid risky situations and take action as instinctively as reaching for a seatbelt when they start a car. Awareness solutions, when coupled with sound teaching techniques and motivated employees, don't just arm people with knowledge--they equip and empower employees to put that knowledge to use in ways that make sense and that fit in with how they perform their jobs.

When employees are properly prepared to participate in their company's cybersecurity program, they will not view cyber attacks as technology-based threats that have little to do with them personally. Instead, they will be strongly motivated to safeguard company systems and information, recognizing that they play an important role in keeping data and systems safe and secure. When fully engaged, this creates a formidable human firewall capable of spotting and preventing even the most sophisticated cyber crime attempts, and is significant steps towards mitigating the human error behind 95% of the cyber breaches occurring today.

CONTACTS

Peter Schablik, CISA, CPA, MBA
Partner
WeiserMazars LLP
Tel: 617.501.4195
Email: Peter.Schablik@WeiserMazars.com

Scott M. Higgins, CISA, CRISC, CRMA
Director
WeiserMazars LLP
Tel: 267.532.4325
Email: Scott.Higgins@WeiserMazars.com