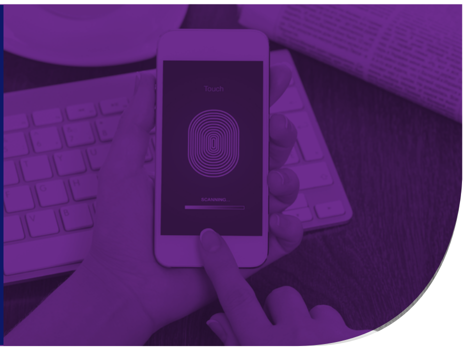
WHITE PAPER

Cybersecurity for Everyone, Not Just the IT Department

RECOGNIZING SECURITY RISKS ASSOCIATED WITH HUMAN ERROR AND SAFEGUARDING YOUR BUSINESS



CompTIA

CompTIA CYBERSECURE

It’s the worst case scenario. You’ve just been notified that your company has experienced a data breach. It could be your company’s confidential information or your employees’ personal data that has been compromised. As you handle the crisis at hand, you keep thinking “how did this happen?” It’s a question that a growing list of CIOs have grappled with recently.

What if the cause of the breach was something as simple as an employee leaving for the day with their laptop open and logged into your network? While everybody may understand the importance of information security, it’s likely that human error is the root cause of your problem.

So, what can you do? **Implement training.**

And don’t limit your training to new hire orientation. Mandate company-wide training that will effectively protect your IT infrastructure.

After all, you wouldn’t buy a brand new Maserati and then hand the keys over to a new driver, would you? Hold your company to that same standard and take action to safeguard your business.

The Digital World is Vulnerable

The IT landscape has shifted dramatically in the past five years. Not only are businesses exploring new models for technology, such as cloud computing and mobility, but they are also viewing technology more as a strategic endeavor that can directly accelerate growth. These two drivers are somewhat complementary to each other, but the dual pursuit definitely creates a more complicated picture for businesses as they consider their IT strategy.

It's not just businesses that are growing. The abundance and sophistication of hackers, combined with greater reliance on interconnected applications, devices and systems, has created a cybersecurity environment that's challenging for even the best-prepared organizations.

According to CompTIA's 2015 report Trends in Information Security, 79 percent of companies believe cybersecurity threats are on the rise and 29 percent of those companies have confessed to a data loss incident in the past year – up from just 19 percent in 2013.[1]

The effects a data breach can have on a company are somewhat obvious: loss of business, damaged reputation and cost of resolving the incident—to name just a few. But the impact on consumers is exponential. In fact, the global cost of cybercrime against consumers is $113 billion.[2]

There's no doubt there is work to do in the cybersecurity space. While there's a series of factors that complicate security readiness – such as malware and hacking – the human element in cybersecurity is still a valid concern.[3]

In fact, companies report the human element as the largest factor behind security breaches. According to the "IBM Security Services 2014 Cyber Security Intelligence Index," over 95 percent of all incidents investigated involved human error as a contributing factor.[4]

We're Not Robots

We're human and we make mistakes. But, if your company has experienced a data breach, you know that your first question is, "How did this happen?" Identifying the cause as a simple human error that could have been prevented is upsetting to say the least. That said, **recognizing the human element as a security risk is the first step toward a complete IT strategy. Creating a culture of high performance that consistently minimizes risk is the key.**

With 52 percent of organizations recognizing that the element of human error in cybersecurity threats is increasing, business leaders are taking proactive approaches to prevent an incident and protect their bottom lines.[5]

The IBM and Ponemon Institute's "2015 Cost of Data Breach Study" found the average cost of a data breach has increased from $3.52 to $3.70 million; with the average cost per record to resolve an attack due to human error or negligence $134 per record.[6] Asking what human behaviors are leading to cybersecurity problems is a good place to start.

With more Generation Y employees in the workplace and overall social media use increasing, what your employees are sharing with the world may be a concern. And it's not just what they may be disclosing, but also where they are sharing information, as social networking sites are a prime target for cyber-criminals.

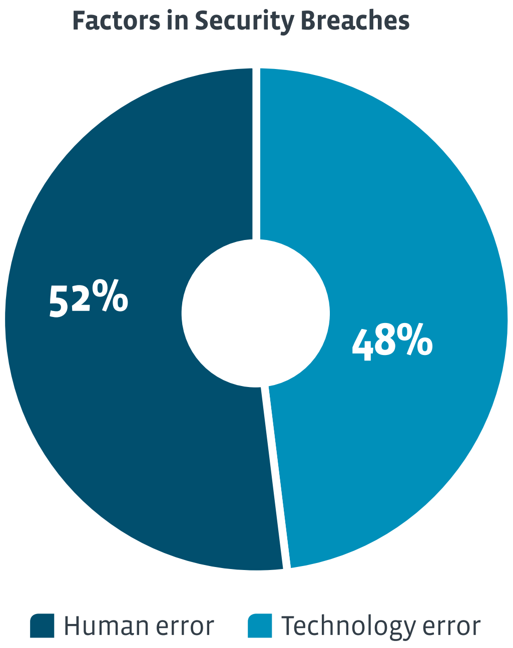
According to Cisco's "2013 Annual Security Report" the highest concentration of online security threats are on mass audience sites, including social media. The report revealed that online advertisements are 182 times more likely to deliver malicious content than pornography sites, for example.[8]

Furthermore, these social media mavens may not fully recognize the threat. The Cisco report shows that more Generation Y workers said they feel more comfortable sharing personal information with retail sites than with their own employers' IT departments.[9]

Top 5 Reasons Human Error Leads to Security Incidents[7]

1. Increased use of social media by staff.
2. Failure of staff to understand new threats.
3. General negligence/carelessness with websites and applications.
4. Lack of security expertise with websites and applications.
5. Failure of IT staff to follow security procedures and policies.

HUMAN ELEMENT A MAJOR PART OF SECURITY RISK[11]



Top Human Error Sources

- **42%** End user failure to follow policies and procedures
- **42%** General carelessness
- **31%** Failure to get up to speed on new threats
- **29%** Lack of expertise with website applications
- **26%** IT staff failure to follow policies and procedures

But one of the most difficult factors to overcome is general carelessness. This behavior is the primary outcome when security and convenience collide. End-users often know what best practices in security are, but they choose a more convenient solution in the pursuit of efficiency.

Let's talk about passwords, for example. We all know that a strong password includes a combination of random letters, numbers and symbols. But that's hard to remember when you have 10 different passwords to keep track of at work. So what do we do? Either use the same password for everything or use a weak password that we can easily remember.

And what about your employees' mobile devices? Smartphones and tablets that travel to and from the office every day – potentially carrying confidential company information – can be security risks in themselves.

But would it surprise you to know that lost devices are no longer the sole mobility security incident companies are guarding against?

In the past year, companies have also seen employees disable security features on mobile devices (31%) and experience mobile malware (30%).[10]

With cybersecurity threats ranging from general negligence to mobile malware, how can companies effectively communicate the importance of information security?

Most firms already know what they should be doing but may not be taking action to trigger a significant change. With regard to human error, better training for everyone is the clear answer.

Better (Not More) Training

Cybersecurity training is becoming a major initiative for many businesses for two reasons: keeping the technical team up to speed with the dynamic environment, and keeping general staff from creating unnecessary risk as they use technology more and more in their daily jobs.

One third of companies are seeing an additional benefit – the training they are pursuing leads to new knowledge that changes the organizational mindset.[12]

A Harvard Business Review article examined the structure and mindset of the U.S. military in relation to cybersecurity best practices and procedures. The article found a high performance culture to be the key factor in decreasing human error and preventing security breaches. At the heart of this culture are six interconnected principles, which help weed out and contain the impact of human error.[13]

1. **Integrity** – Cultivating a deeply internalized ideal that leads people to eliminate short-cuts and immediately own up to mistakes.
2. **Depth of Knowledge** – Facilitating a thorough understanding of IT systems that allows those responsible to readily recognize when something is wrong and take the correct measures to handle it.
3. **Procedural Compliance** – Setting up standards and procedures that employees are expected to follow.
4. **Forceful Backup** – Recognizing that some high-risk actions should be performed by multiple people to ensure accuracy.
5. **Questioning Attitude** – Encouraging a mindset that allows employees to trust their gut when something seems amiss and proactively take corrective action.
6. **Formality in Communication** – Using clear and concise language that leaves no gray area.[14]

Sure, the ideal workforce embodies those principles and sets out to execute them every day. But, how do companies get to that place?

The first step is to take charge.

A recent survey by Oxford University and the UK's Centre for the Protection of the National Infrastructure found that concern for cybersecurity was significantly lower among managers inside the C-suite than among those outside it. The reality is that if CEOs don't take cybersecurity threats seriously, their organizations won't either.[15]

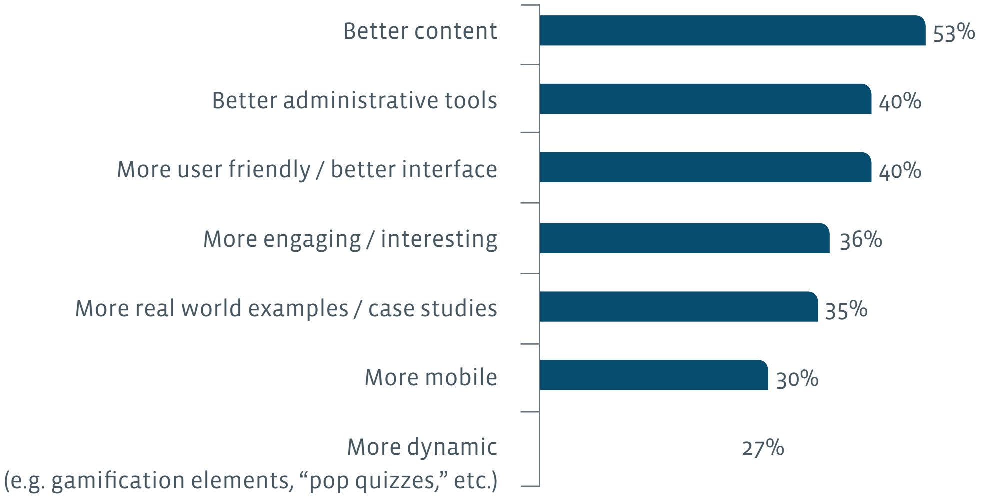
Establishing uniform standards and centrally managed training and certification, and then making everyone accountable for their actions, is the best way to take charge.

But, better training is easier said than done. Most businesses struggle with the thought of providing education. It's not their forte, and the effects can be difficult to measure. Few training programs offer direct correlation to business results, and it is especially complicated in an area like cybersecurity where the desired effect is the absence of any incident.

Still, most businesses have some notion of providing foundation training. Currently, 54 percent of companies are offering some form of cybersecurity training, typically done through new employee orientation or an annual refresher course.[16]

Businesses readily acknowledge that they would like to see better content in their cybersecurity training. Organizations are also looking for a training tool that offers better administration tools, as well as more real world examples to make for a more engaging and user-friendly program.

CRITERIA NEEDED FOR BETTER SECURITY TRAINING[17]



Introducing CompTIA CyberSecure™

CompTIA CyberSecure™ is online cybersecurity training for everyone in an organization. This self-paced training course teaches employees security best practices vital to protecting your business. Offered as a 60-minute online course, CompTIA CyberSecure covers online and offline behaviors that reduce cybersecurity risks.

This program provides results-driven behavior modification training on information security for every member of your organization. The training uses an innovative approach to create a fun and interactive online course to keep employees engaged.

But what makes CompTIA CyberSecure different from other online training modules?

First, the training is based on CompTIA research to determine what corporate stakeholders like you want your staff to know about cybersecurity. Second, the CompTIA IT Security Community – a group of the industry's leaders in the IT security space – developed the CyberSecure objectives that include: the importance of protecting yourself and your company from information leaks; understanding the basic categories of information security threats; nurturing a safe information mindset; cultivating a safe environment; and implementing safety strategies.

The result?

A comprehensive training program that protects your IT infrastructure, keeps learners engaged and effectively shifts the mindset of everybody in your organization when it comes to cybersecurity.

Developed by CompTIA's IT Security Community and based on CompTIA research, CompTIA CyberSecure provides results-driven behavior modification training on cybersecurity for every member of your organization.

Cybersecurity is for everyone, not just the IT department. All the time and capital you've invested in a robust security plan means nothing if human error is not addressed. Protect your company, your employees and your security investment by ensuring everyone in your organization is executing best practices when it comes to information security.

More information is available at **www.cybersecure.org**.

CompTIA Worldwide Headquarters
CompTIA Certification, LLC
3500 Lacey Road, Suite 100
Downers Grove, Illinois 60515

630.678.8300

CompTIA.org

[1] CompTIA's 2015 Trends in Information Security
[2] 2013 Norton Report, Symantec
[3] CompTIA's 2015 Trends in Information Security
[4] the IBM Security Services 2014 Cyber Security Intelligence Index
[5] CompTIA's 2014 Trends in Information Security
[6] The IBM and Ponemon Institute 2015 Cost of Data Breach Study: Global Analysis
[7] CompTIA's 2014 Trends in Information Security
[8] Cisco 2013 Annual Security Report
[9] Cisco 2013 Annual Security Report
[10] CompTIA's 2015 Trends in Information Security
[11] CompTIA's 2015 Trends in Information Security
[12] CompTIA's 2015 Trends in Information Security
[13] Harvard Business Review: Cybersecurity's Human Factor: Lessons From the Pentagon
[14] Harvard Business Review: Cybersecurity's Human Factor: Lessons From the Pentagon
[15] Oxford University and the UK's Centre for the Protection of the National Infrastructure
[16] CompTIA's 2014 Trends in Information Security
[17] CompTIA's 2015 Trends in Information Security