expressworks

Cyber Security and Human Behavior: A People-Centered Approach to Cyber Resilience

Insights on achieving a company culture of vigilance, where security is second nature

Organizations are Under Siege

The last twenty years of technological advancement has enabled incredible strides in human achievement. Yet, in many ways, technology has also made us more vulnerable to disaster than ever before.

Today, nearly every major organization in the world finds itself in some stage of digital transformation, working to take advantage of everything technology has to offer, from mobile apps and social media to cloud computing and "big data" analytics. As every conceivable piece of information is converted to 1's and 0's, sensitive data that was once locked away in secret file cabinets becomes available to any criminal with a talent for computer hacking.

Cyber crimes, and the damages they inflict, have continued a meteoric rise in recent years. In 2017 alone:[1]

- Almost 2 billion data records around the world were lost or stolen by cyberattacks in the first half of 2017.
- Two-thirds of firms breached had their share price negatively impacted. Data breaches cost shareholders over $52.40 billion.
- The number of lost, stolen or compromised records increased by 164 percent compared to the same period in 2016.
- Credit rating agency Equifax revealed that information on 143 million Americans was compromised.
- Cyberattacks are now the number one external risk factor facing businesses.

No industry is immune. And there is virtually no limit to what types of data cyber criminals pursue: customer records containing financial data and social security numbers, intellectual property and trade secrets, personal emails, digital photos ... the list goes on. As the losses mount, cyber crime shows no signs of slowing down. Every day it becomes clearer that businesses and government organizations alike must take unprecedented steps to prevent these attacks.

Source:
1. https://www.cnbc.com/2017/09/20/cyberattacks-are-surging-and-more-data-records-are-stolen.html

Security is a Team Effort

With cyber security top of mind, IT and security experts everywhere are racing to implement more robust technology to create impenetrable barriers around their critical data.

While state-of-the-art hardware and software certainly play a role in security, they are by no means a complete solution. In fact, weak technology is not to blame for most data breaches. More often, the culprit is human error.

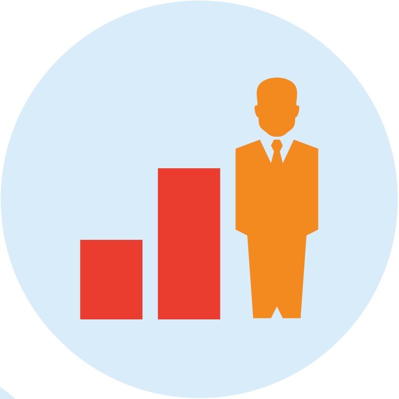
When it comes to cyber security, people are the weakest link. Countless cyber attacks begin through somewhat simple methods such as social engineering, phishing, viruses or malware, all of which fool unsuspecting employees to reveal confidential information or open a digital doorway. In this way, untrained personnel can render even the strongest technical defenses ineffective.

The good news is that people can be educated, motivated, and trained to respond differently. They can, as an organization, learn to think of cyber security as more than a technological solution, but a responsibility borne by everyone. People can stop being the organization's greatest weakness, and become its strongest line of defense.

The Facts on Cyber Security

99%

99% of data breaches are preventable[2]



84%

84% of security incidents are non-technical[3]

66%

66% of cyber security incidents are caused by employees[3]

Sources:

1. Touhill, Gregory J. and C. Joseph. Cyber Security for Executives: a Practical Guide. Hoboken, NJ: Wiley-AIChE. 2014.

2. https://www.forbes.com/sites/gartnergroup/2016/08/18/top-10-security-predictions-through-2020/

3. https://www.willistowerswatson.com/en/insights/2017/09/Cyber-risk-its-a-people-problem-too

The Expressworks Approach

To help clients deal with this most critical issue, Expressworks launched its cyber security practice in 2015.

As experts at designing and implementing organizational change, we use behavioral and cognitive science to engage employees in the mindset and actions that can stop cyber crime before it's too late. Drawing from multiple consulting disciplines, we help organizations bring technology, business processes and internal culture into alignment, to minimize the threat from within.

Our work focuses on three primary areas: building leadership support, realigning processes and positioning, and creating a culture of cyber resilience.

Building Leadership Support

Top executives have a lot to think about, but for most organizations, cyber security should be high on the priority list. As most security experts will attest, it's not a matter of if – but when – the organization will come under cyber attack. If necessary, leadership needs to be educated on the very real threats against them, and understand the potentially devastating consequences of a major data breach.

Without high-level commitment and support at the C-suite and board levels, security departments are left to compete for funding and resources, and well-intentioned security programs may never gain traction. Equally important, leaders must be highly visible and vocal champions of cyber security initiatives, lest employees ignore the call to action.

Realigning Processes and Positioning

No two companies are exactly alike, nor are their organizational structures. Thus, none handles cyber security in quite the same way. Understanding why the organization is set up the way it is, and how it could be rearranged to improve security, is an important part of the big picture approach.

For example, the chief security officer (CSO) and/or chief information security officer (CISO) will encounter both technical and non-technical challenges when executing a cyber strategy. Positioning these leaders in a model of cross-functional cooperation amongst various departments is critical to success. Equally important are the specific programs and processes the organization has in place to prevent data breaches. An early assessment of the organization's strengths and weaknesses can help address the most problematic vulnerabilities in priority order.

Creating a Cyber Resilience Culture

When today's organizations speak of their company culture, they most often include ideals such as diversity, innovation, and sustainability. At Expressworks, we believe a commitment to cyber security should be among those shared beliefs and behaviors. Security must become a goal and responsibility for every employee in every department. Only when people are motivated to take security seriously can an organization have confidence that its physical assets and sensitive information are in good hands. To that end, inspiring employees through education, communication, and leadership may be the single most important element of any security initiative.

Two Essential Keys to Information Security

1. Reduce human errors that expose sensitive data
2. Reinforce the right security behaviors

About Expressworks

Since 1984, we've worked with major companies around the globe to understand their unique challenges and deliver meaningful, measurable, sustainable change. Our cyber security practice focuses on influencing the human attitudes and behaviors that can make any organization more cyber resilient. With expertise in cognitive and behavioral science, we identify common employee errors and organizational barriers to security, and help you build a more vigilant culture where cyber security becomes second nature.

Contact Expressworks today to learn how to achieve cyber resilience through one of our one-day workshops.

Email us: cybersecurity@expressworks.com

Call us: 281-822-1545

Go online: www.expressworks.com/cyber-security