NEWPORT BOARD GROUP

CYBER-SAFETY: IT TAKES YOUR ENTIRE ENTERPRISE

AUTHORS

David R. Wilson
Managing Director
Newport Board Group

Marcus McInnis
Former Director of Operations, Center for Cyber Security Innovation (CCSI) at Lockheed Martin

In recent years attempted cyber-attacks have increased in frequency, focus and sophistication. In the early days of hacking, attackers could be categorized in three groups. The first group were called script-kiddies or ankle bitters: technically savvy young people, motivated by a desire to show they could out smart their computer industry elders. At the other end of the hacking spectrum were state actors. They were and still are well funded, well resourced, very knowledgeable and capable groups sponsored by national intelligence authorities. In the middle was a broad range of independent characters operating at the edge of the law, motivated by money and notoriety, who became progressively smarter at what it takes to launch complex cyber campaigns with state of the art tools.

It is not a question of whether your company will become a target- just when.

LEAVING STATE ACTORS ASIDE, TODAY'S HACKER MOTIVATION IS FINANCIAL.

The promise of quick financial gain and the low risk of getting caught motivates cyber attackers to seek vulnerabilities in cyber controls and find new ways into companies. The number and scope of successful, financially motivated attacks, even against organizations that use sophisticated technology to protect against them is large—and growing. Cyber-attacks can be very profitable. Carrying them out requires only a computer and access to a network, easily acquired skills, and a little imagination. Just think: a cyber attacker can perform the equivalent of a bank robbery while sitting at home in pajamas and slippers anywhere in the world! But more often than not, it is a very well-funded organized crime group that has access to the latest cyber tools, the smartest hackers and a new-found patience that has made them even harder to detect. Not surprisingly, secondary markets have arisen to 'off-load' the spoils and generate additional layers of financial motivation. You may doubt your company's data or proprietary

CYBER-SAFETY: IT TAKES YOUR ENTIRE ENTERPRISE

information has sufficient value to interest a cybercriminal. On the contrary: these days even your company's email listing has value on the global black market. Therefore, it is not a question of whether your company will become a target- just when. This applies as much to emerging growth and middle market companies as to large global firms.

Recent studies show that authorized users' inadvertent actions on organizations' networks are to blame for well over half of cyber breaches – and the cost of these data breaches is going up . The technical control systems designed to protect cyber security are unable to prevent cyber breaches because the initial threat vectors almost always involve phishing or 'human factor' components not addressed by technical controls . In many cases users are fooled into making costly security mistakes in the course of carrying out seemingly legitimate communications . These violations / security flaws reflect a failure to implement a full security framework.

MAY, 2016, 119 MILLION LINKEDIN USER WERE HACKED.

One of them was the identity of Mark Zuckerberg, the CEO of Facebook. Unfortunately, he had used that same LinkedIn password for other accounts including Twitter. Zuckerberg's reuse of passwords led to the hacking of multiple accounts. This is a current example of the 'human factor' breach involving a most sophisticated user. The Verizon Enterprise Solutions 2016 Data Breach Investigations Report documented more than 100,000 incidents and 2,260 breaches in 82 countries, revealing vulnerabilities that account for 85% of successful attacks. A key finding: many successful attacks resulted from the actions of authorized users of the systems and networks. According to Marc Spitler, a senior manager of Verizon's security research team, "most adversaries use a three-pronged attack strategy." The first part typically consists of sending phishing emails, hoping an employee clicks on a malicious link, providing the attacker with access to the network. There are no technical controls to prevent this type of threat vector. It's a people problem.

Organizations have invested heavily in technology to protect data and networks and in progressively more advanced techniques to authenticate end users. These investments have reduced the risk of conventional cyber-attacks and limited the extent of the damage they cause. However, these technical controls have failed to reduce the rate of increase in successful cyber-attacks.

NO TECHNICAL SYSTEM CAN PREVENT THE MAJORITY OF CYBER-ATTACKS

without proper behavior and support from those who are authorized to access and use enterprise systems.

*The Verizon Report says that **63% of documented breaches** involve identity compromise resulting from poor end-user disciplines.*

CYBER-SAFETY: IT TAKES YOUR ENTIRE ENTERPRISE

Further, rogue software can be readily introduced into protected networks through users' inadvertent actions. Users are fooled into taking actions (such as described above) that hurt the organization and compromise the integrity of data and programs by responding to cyber communications that seem legitimate, but in fact are not. These problems occur even in firms that have made substantial investments in technical controls. While these technical security systems help make cyber-attacks more difficult to pull off and reduce their potential scope, they cannot eliminate successful attacks without also addressing the behavior of the authorized users of the systems and networks. Bottom line:

Cyber-attack prevention will continue to be ineffective until end ***users become an active part of the cyber security system.***

Successful efforts to make the end user an active part of the cyber security system must involve both training and awareness campaigns to create a change in culture that actively supports cyber protection and defense. This requires far more that an occasional nod to "basic training" for the troops. It calls instead for an intentional and continuous focus that brings about a developed culture, one which protects and defends against cyber-attacks.

THIS IS NOT EASY.

Most cyber-attacks are devised to be invisible to end users. People find it hard to remember everything they should be doing to protect systems and data when they are busy attending to their jobs. To address these problems, every organization must have a program that teaches and reinforces cyber practices in a way that informs and motivates end users to both eliminate the daily behaviors that increase cyber risk, and implement new behaviors that make all users active parts of the cyber-security system. This is a change in culture, and changing culture in an organization requires a sustained and focused effort starting with senior management.

We are calling this program, which makes the end user an active part of the cyber security system, a 'Safe-Cyber' program.

Leadership must develop clear policies for cyber behavior that explain what is expected from managers and employees who have access to systems and networks. Every user must be trained on them. Every employee must take responsibility and accountability for acting in a Safe-Cyber-compliant manner. Like visitors to a jobsite or plant who are required to wear a hardhat and eye protection, and can only go in safe areas, visitors to a system or network must be informed of expectations and requirements and be limited to what they can access.

A robust Safe-Cyber program should seek to integrate a deep layer of caution, awareness and know how into the actions employees take as they go about their daily work. The goal is to motivate people to stop, slow down, think twice, and make a wiser decision.

CYBER-SAFETY: IT TAKES YOUR ENTIRE ENTERPRISE

Analogous to the more traditional programs of manufacturing plant safety, a Safe-Cyber program starts by establishing a ***set of expectations for Safe-Cyber behaviors from the top of the organization to the front line.***

Effective awareness campaign will incorporate techniques based on the latest findings and techniques in brain science, behavioral psychology, and persuasion.

THESE TECHNIQUES INCLUDE:

- Active practice: encouraging everyone to apply cyber security concepts to the context at hand instead of acting in a passive, rote manner
- Spaced retrieval (reinforcing information regularly over a period of months to strengthen pathways to permanent retention)
- Interleaving (weaving in new concepts with others introduced previously)
- Memory cues (mnemonics, vivid images, analogies, slogans, etc.)

THE AWARENESS PROGRAM MUST BECOME INGRAINED THROUGHOUT THE ORGANIZATION.

The awareness program must create an informed workforce that acts in a Safe-Cyber manner in all situations, creating a strong front line of defense against cyberattack. The Safe Cyber initiative team defines the program, the communications, the help desk functions, and oversees on-going implementation.

ITS COMPONENTS SHOULD INCLUDE:

1. Messages from the leadership that relate Safe-Cyber behavior to the company's goals and strategy.
2. Building Safe-Cyber goals and outcomes into the regular performance and appraisal process.
3. Adding Safe-Cyber to corporate asset protection programs.
4. Providing regular communications on cyber events, near misses, celebrating individuals who helped avoid a breach or incident, etc.
5. Providing regular, continuous and repeated training and updates to all employees.
6. Regular testing of Safe-Cyber practices involving all employees.
7. Establishing a Safe-Cyber help desk where employees can get immediate support if they see something that looks like a threat.
8. Creating a Safe-Cyber dash board that tracks progress in a Safe-Cyber program.

The need for awareness programs around cyber security is not a new insight. NIST (National Institute of Standards and Technology) SP 800-53 guidelines, which are referenced in the February 2014 Framework

CYBER-SAFETY: IT TAKES YOUR ENTIRE ENTERPRISE

for Improving Critical Infrastructure Cybersecurity, require an ongoing awareness campaign among all system users to assure a culture of cyber awareness and necessary protective behaviors.

FINALLY, THIS IS THE RESPONSIBILITY OF THE SENIOR LEADERSHIP OF THE ENTERPRISE.

This is not just the concern of the CIO, the CISO, or the Director of Training and Personnel Development. Culture change must start at the top. Safe-Cyber practices must be established by the Board and the CEO, who have the best perspective on the risk to the organization from a cyber breach. Reputation, the continuity and viability of the business, its intellectual property, the trust of its customers and other partners and its financial health are all at stake. The CEO, the CFO, and the General Counsel all play an important role in defining and emphasizing the importance of a Safe-Cyber culture in the organization.

What must leadership do? The senior management of any organization must lead in setting a culture of cyber safety, awareness, and behavior. Every person in the organization must understand their role in safeguarding the health and wellbeing of the organization and its future. An accountability and support system should be established that implements the Safe-Cyber awareness program, and provides users answers to their questions, timely advice, and knowledge of who and when to call if they see a potential threat.

Finally, and most importantly, there needs to be a continuous campaign of cyber protection awareness that addresses behavior at every level of the enterprise. Manufacturing, petrochemical, shipping, and other industries have for years developed a culture of safety. A similar kind of program and campaign can work for cyber threats. Without that, cyber breaches will continue to threaten the survival and success of organizations everywhere.

WORKS CITED

- [1.] IBM's Tenth annual Cost of Data Breach Study by Ponemon Institute.
- [2.] SANS Institute report "Phishing" An Analysis of a Growing Threat";
- [3.] Business Email Compromise (BEC); FBI reports $2.3B cost to businesses past three years (2013-16) in 'communication' spoofing as a growing threat vector.

A NEW CATEGORY OF FIRM

Newport Board Group is a unique national business advisory firm of CEOs and senior executives who provide experience based consulting to the leaders of emerging and mid-market businesses to help them grow, improve operations, align teams, and prepare for major events and transactions. With practices in almost 20 major cities, we provide CEO Advisors and seated Board Directors, project consulting and interim executive services.

NEWPORT BOARD GROUP CONTACT

David R. Wilson, Managing Director
EMAIL David R Wilson@newportboardgroup.com | **PHONE** (508) 942-7081