Improving Cybersecurity Behavior

A study by Dell found that nearly 3/4 of organizations surveyed have admitted to experiencing a security breach within the last 12 months. In fact, since 2014 cyber security incidents have surged 38%. For the more cost driven among us, data breaches translate into $3.79 million in losses and associated costs.

Statistics like these should drive the point home that there is a very real need for incorporating better cyber security policies into the daily life of your employees. In essence, changing the culture of your organization to account for better security awareness.

“Cyber security is a complex issue and for most businesses, cannot be easily addressed with simple measures such as those deployed to protect your family’s home computer”

You’ll need much more than an off the shelf antivirus software package and hardtocrack passwords. That doesn’t mean that your strategy has to be overly complex... your cyber security strategy just needs to be more than hurdles placed in front of your employees in their attempt to do their jobs.
Building A Culture Around Cyber Security Behavior

Though people often talk about strategy when faced with difficult business situations, when it comes to changing your employee’s cyber security behavior, it might be better to replace a change in strategy with a change in culture. Developing a culture around solving a problem is more likely to result in success.

Something to understand about security awareness is that every person in your organization is a potential security breach. Even the CEO in a corporation, who may have a very strong security system with 23 passwords and a robust encryption system can become a potential security risk if a hacker bypasses all layers of the security policies by simply calling a secretary and asking for enough information to guess passwords. If every member of your staff isn’t trained in proper security awareness and how information can be used to breach security protocols, any security policies and systems in place are a waste of time and money.

Developing strong security policies for your business isn’t really about creating more bureaucracy with more rules and restrictions. It is instead about increasing the security awareness of your employees through any number of culture modifying practices.
Risky Business

When it comes to security awareness, every business faces the same risks. Computer systems can become infected in a variety of different ways and quite often risky employee behavior is at the root of intrusions. Whether it is visiting suspect websites or opening suspicious email messages, your employees need to be aware of proper cyber security behavior. The question then becomes how best to modify employee behavior to acknowledge the danger and prevent possible problems with their data integrity.

Since the most likely avenue for security breaches lies within your staff’s understanding of security threats, modifying your employee cyber security behavior is by far the most cost effective way to protect your most valuable assets from malicious intrusions.

How to Modify Behavior

While the obvious solution is to monitor employee computer use to make sure they are not putting computers at risk, that may not result in the desired behavior, especially if your employees often use private devices on the business network. The absolutely best step is to instill a culture of security awareness in your employees through training, human based reporting, and by promoting peer-to-peer recognition.
Training

Training is important and it helps a business ensure that everyone in the company is on the same page in regard to cyber security strategy. Properly training staff what to look for and how they can avoid being “tricked” by increasingly sophisticated hacking techniques is the foundation of all strong cyber security policies.

Some examples of typical training courses for your employees include:

- Intro to Malware, Ransomware and Spyware
- Understanding the S in HTTPS Access
- Best Practices for Choosing and Remembering Passwords
- Recognizing Sophisticated Spear Phishing Scams
- Exploiting Human Psychology with Social Engineering
- Securing Desktop Apps that Access Social Networks

All of these are important, but what if you could motivate your team to be more aware of those potential threats on a fundamental level?

www.thinksmartone.com
Human Based Reporting

On average, users click one of every 25 malicious messages delivered. Few organizations are able to eliminate clicking on malicious links, but installing a reporting system and motivating employees to use it is a fundamental part of stopping these simple hacking maneuvers. By getting your employees to report each and every email or malicious link that crosses their screens you can ensure everyone is always aware of potential threats.

Promote Peer to Peer Recognition

To make your staff aware of the need for tough cyber security behavior, you'll need more than a few meetings or occasional reminders. Developing tough security policies in place to protect their computer systems is a start of course, but for many businesses, more is needed. Motivation is based on a number of factors, but one simple method is recognizing successful practices. In this case, making sure you implement opportunities for recognition from their peers when someone consistently reports possible security threats is a valuable tool in instilling the culture of awareness that is key to any successful cyber security policy. You can also create forums and hold events that promote cyber security awareness where peers can gather and exchange ideas and discuss potential threats.
Recognizing Value through Extrinsic Motivation

Extrinsic motivation refers to behavior that is driven by external rewards such as money, fame, grades, and praise. This type of motivation arises from outside the individual, as opposed to intrinsic motivation, which originates inside of the individual.

Let’s be honest about motivation. There are some people who can be motivated by nothing more than a pat on the back and verbal recognition of a job well done. Not everyone is that altruistic however, and for those people, a change in behavior is often driven by the opportunity to earn tangible rewards. Setting up point systems that can be exchanged for goods and services is perhaps the best way to keep these particular employees invested in the success of any particular endeavor.

That’s where you might discover an opportunity for cyber security gamification and Salesforce has tools that can make that particular solution much easier.
ThinkSmart and Security Awareness

With ThinkSmart you can improve cyber security behavior through gamification and other motivation techniques from within Salesforce. For instance, with ThinkSmart for Salesforce you can:

- Track security training courses and reward the team for attending them.
- Create reporting systems for possible security breaches such as phishing attempts, malware discoveries, etc. The manager can create incentive rules that track these behaviors and the participants get rewarded each time they report a possible security breach.
- Set up peer-to-peer recognition of good practices. If someone reports a phishing email, a peer can recognize him publicly for doing so.
- Reward people for participating in events related to promoting cyber security (i.e., presentations or round-tables, creating a forum or participating in one, etc).

Using cyber security gamification to increase awareness of cyber security issues will not only increase the likelihood of success, it will also greatly increase employee engagement as you strengthen your security policies.

All these activities increase security awareness through motivation and can be administered from within the very tool that is among your most valuable resources. What better way to modify the behavior of your employees in relation to your cyber security policies than by leveraging the power of your CRM?

For more information about how ThinkSmart can help you create a culture of cyber security awareness in your organization, contact us today!

www.thinksmartone.com
ThinkSmart for Salesforce.com® is an app to motivate your team with incentives, using traditional incentive rules and gamification techniques. Accelerate sales, improve CRM adoption and data quality, recognize your team, build loyalty and improve training. An intuitive way to improve performance for any size company, all within Salesforce.

Learn More ...