InfoTECH SOLUTIONS
I.T. SERVICES FOR BUSINESS

http://www.infotech.us/

# Employees and Cybersecurity

For any organization, its employees are its biggest assets. But, what happens when your biggest assets turn out to be your greatest threats or liabilities? That is how cybercrime can change the game. In a recent study, it came to light that employee actions account for about 70% of the data breaches that happen. This whitepaper focuses on what you can do as an organization to better prepare your employees to identify and mitigate cyber threats.

## A top-down approach to IT security

First things first--change your organizational mindset. IT security is not ONLY your IT department, CTO or Managed Service Provider's (MSP) responsibility. You need to truly believe that IT security is everyone's business, and that includes everybody working in your company, from the C-level execs to the newly hired intern. Everybody needs to understand the gravity of a cyberattack and its impact. Only then, will they take cybersecurity seriously.

## Policies

The next step is to formulate IT policies and lay down the best practices for your staff to follow. Ideally, your IT policy should cover the following:

### Passwords

1. Rules regarding password setting
2. Password best practices
3. The implications of password sharing
4. Corrective actions that will be taken in the event the password policy is not followed

### Personal devices

1. Rules regarding the usage of personal devices at work or for work purposes.
   Answer questions like
   a. Are all employees allowed to use personal devices for work or do you want to limit it to those handling lesser sensitive data, or to those at higher in the corporate hierarchy as you assume they will need to be available 24/7? Regardless, you should spell out the regulations that they must follow. For example, requiring a weekly or monthly check for malware and updates to anti-malware software, etc., If only certain kinds of devices, software or operating systems may be approved as they are presumed to be more secure, then that should be addressed in the policy

2. Discuss best practices and educate your employees on the risks related to connecting to open internet connections (Free WiFi) such as the ones offered at malls or airports.

### Cybersecurity measures

1. Document the cybersecurity measures that you have in place for your business. This should include your digital measures such as the software you have deployed to keep malware out--like anti-virus tools, firewalls, etc., and also the physical measures such as CCTV systems, biometric access controls, etc.,

2. Another example of a good practice is how you handle employee turnover. When someone quits your organization or has changed positions, how is the access issue addressed? Spell out the rules and regulations regarding the removal of a user from the network, changing passwords, limiting access, etc.,

## Employee Training

Employee training will form a big part of the cybersecurity initiative that you will take on as an organization. You need to train your employees to identify and respond correctly to cyberthreats. Here are some employee training best practices that you can make a part of your cybersecurity training program.

### Create an IT policy handbook

Make sure you have a handbook of your IT policy that you share with every new employee, regardless of their position in the company. This IT policy handbook must be provided to everyone--right from the CEO to the newest intern in your organization. Also, ensure this handbook is consistently updated. IT is evolving at great speed and your handbook must keep up.

### Make cybersecurity training a part of your official training initiatives

Cybersecurity training should be a part of your corporate training initiatives for all new employees. You can also conduct refresher sessions once in a while to ensure your existing employees are

up-to-date on the latest cyberthreats. At the end of the training session, conduct tests, mock drills, certification exams. Good training includes assessment. Provide follow up training for those who need it. This strong emphasis on training will ensure your employees take cybersecurity seriously.

### Day zero alerts

As discussed, the cybercrime landscape is constantly evolving. Every day, cybercriminals are finding new vulnerabilities to exploit, and new methods to steal your data or to hack into your system. Day zero alerts are a great way to keep your employees updated. Has a new security threat been discovered or an important plug-in released for the optimal functioning of a browser? Send an email to everyone spelling out clearly what the threat is and what they can do to mitigate it. Then, follow up to verify they took the necessary steps.

## Transparency

Let your employees know who to contact in the event of any IT related challenges. This is important because someone troubleshooting on the internet for a solution to something as simple as a zipping up a file could end up downloading malware accidentally.

Being a victim of cyber-attack can prove disastrous for your business as it has the following repercussions.

- **Affects your brand image negatively:** Business disruption due to downtime or having your important business data including customer and vendor details stolen reflects poorly on your brand.
- **It can cause you to lose customers:** Your customers may take their business elsewhere as they may not feel safe sharing their PII with you.
- **Can cost you quite a bit financially:** Data breach makes you liable to follow certain disclosure requirements mandated by the law. These most likely require you to make announcements on popular media, which can prove expensive. Plus, you will also have to invest in positive PR to boost your brand value.
- **It makes you vulnerable to lawsuits:** You could be sued by customers whose Personally Identifiable Information (PII) has been compromised or stolen.

In light of such serious ramifications, it makes sense for organizations to strengthen their first line of defense against cybercriminals--their own employees.

**For more information please contact,**
Brian Wyble | Account Executive | InfoTECH Solutions, L.L.C.
Phone: 337-896-3681 | Email: bwyble@infotech.us