Help you’re Employees Understand Data Risk Management

By [Sam Grier](http://itmanagersinbox.com/author/sam-grier/)

[](http://itmanagersinbox.com/wp-content/uploads/2010/05/riskmanagement.jpg)Theft of confidential information is a risk to the business and IT plays a large role in protecting the data. Not all data is electronic though. Files that identify customers and employees, Social Security numbers, credit card information and other account data are just some of the forms of sensitive data a company must protect.

Failing to protect confidential information can lead to identify theft and fraud. You can lose the trust of your customers and even end up defending yourself in a lawsuit. Data loss is often due to employees who are do not follow IT security policies or inadvertently expose the company network to risks.

According to the first annual ISACA IT Risk/Reward Barometer survey the top three ways employees add risks for IT and the business:

* Not protecting confidential work data appropriately (50 percent)
* Not fully understanding IT policies (33 percent)
* Using non-approved software or online services for their work (32 percent)

Many studies have shown that “[Lack of End User Training is a Large and Growing Threat to IT Security](http://itmanagersinbox.com/1161/lack-of-end-user-training-is-a-large-and-growing-threat-to-it-security/)”. This is why your employees play a very important role in IT security.

Tips For Protecting Your Company Data

Lock It Up

Computer and network defenses are important, but don’t forget all data is not electronic. Offices are filled with files containing sensitive or confidential information. Here are a few steps employees can take to secure data.

* Make sure every employee has a secure drawer or cabinet to lock up files.
* Centralize sensitive paperwork in a secure location and limit access to only employees who have a legitimate business use for the data.
* Remind employees to never leave documents out even if they will only be away from their desk a short time. Just open the secure drawer and lock it. It is a habit every employee needs.
* If you are shipping sensitive data off-site use a secure package and a shipping method that allows you to track the package.
* Employees with company laptops should be educated on how to secure them in their car and in their home.

Help Employees Keep Your Network Secure

It only takes a few seconds for spyware, viruses or other nasties to invade your network. IT departments use advanced tools to protect a network, but employees must understand their role in electronic security.

* Encourage employees to use strong passwords, the longer and more sophisticated the better. Teach your employees methods of remembering strong passwords so they do not write them down and enforce mandatory password changes.
* Block sites that are not work related or that are known to have risks associated with them. Educate your employees that they only have to visit the wrong website to become infected. To an employee what seems like innocent web surfing can be a huge risk to your network.
* Teach your employees to never open an email attachment from someone they do not know. Even if they know the person employees should always be wary of attachments. Give them a list of known file name extensions they should never open regardless of who it seems to be from.
* Educate your employees on the hazards of installing unauthorized software on their computer.
* A study last year found that 67% of employees use removable media such a personal USB thumb drives at work. Not only does this put your IT systems at risk from a potential virus, but with the size of removable media today gigabytes of company data can be downloaded to them. Consider blocking access to mass media devices via USB ports.

Employees And IT Policies

Nearly every company new hire will sign an IT security policy, but do they really read it? Many employees a simply not aware of IT policies that are setup to protect company data and the IT systems that support the business.

* There are some ways to make your employees more aware of IT polices.
* Educate them by using online or classroom training on IT policies
* Post IT policies on the company intranet site
* During new hire orientation don’t just get them to sign the policy, take time to go over it so they fully understand the policy and what role they play
* When changes are made to IT policies make sure all employees are made aware of them.

Education Is The Key

You can not rely on IT solutions alone to protect your IT systems and your company data. There are areas that put IT systems and the business at risk where educating your employees is they key.

Some areas to highlight:

* Educate and train employees about company expectations for protecting data
* The use of unauthorized software on company computers and company cell phones
* Include security awareness training during new-hire orientation
* Establish a security aware culture by using frequent reminders like posters and emails about IT security and company data.
* Teach employees about security considerations when on the phone and connecting to the Internet, social networking, and collaboration sites.
* Teach employees about physical security, such as only allowing employees with badges to enter buildings.

Are Your Employees Security Aware?

Protecting confidential data in all forms is critical to the business and IT has a large role in making sure the data is secure. A disgruntled employee can cause tremendous damage to a company, but the biggest risks are employees who don’t take proper care of company data.

Constantly review your IT polices and make changes if needed. Educate your employees so they understand they play a very important role in protecting your company data. Employees do not want to put your company at risk, but for most data security does not cross their mind. They think the IT staff will handle all that.

Helping your employees understand their role in protecting sensitive and confidential information as well as overall network security is a sound best practices you should put in place right away.

The SANS (SysAdmin, Audit, Network, Security) Institute offers a very good set of security guidelines called “[Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines](http://www.sans.org/critical-security-controls/)”. If you think your security policies are lacking or need updating this would be a good read.