kellyservices.us
http://www.kellyservices.us/US/Business-Services/Business-Resource-Center/Management-Tips/Cyber-Security-for-Your-Team/#.U-S0lvmSx8E

Cyber Security for Your Team

Last October, software giant Adobe announced its system had been hacked and the sensitive data of approximately 2.9 million customers had been stolen. Two months later, America's largest bank, JPMorgan Chase, stated that hackers had stolen the user information of 465,000 clients. And just weeks after that, on Black Friday, major retailer Target acknowledged that credit and debit card data of 40 million accounts had been stolen.

If these hugely publicized incidents that compromised the financial information of millions of consumers weren't scary enough, when news of the security bug Heartbleed was made public on April 7 th of this year, governments, companies and individuals worldwide scrambled to fix any apparent vulnerabilities in their networks and security measures.

As a manager, you know that whether it's your customers' financial details, your employees' personal information or your company's intellectual property, sensitive data pertaining to your business operations needs to be protected at all cost. In order to do so, you need an understanding of the threats to your data and how to minimize them.

Cyber Crime

Cyber crime is rife, whether in the form of hacking or with help from inside victim organizations. PC World states that in the United States alone, small businesses have a 20 percent chance of being attacked. Worse, hacked companies stand a 60 percent chance of going out of business within six months after the breach. Larger companies with more robust security systems are supposedly less vulnerable and often have more resources to remedy attacks. But as the examples above demonstrate, when hackers gain access to their systems, millions of people are affected.

Human Error

Targeted attacks by skilled criminals aren't the only way sensitive information can become compromised. According to Raul Condea of CoSoSys, over 85 percent of data loss is due to human error. Everyday actions such as remotely accessing the office's network from home, incorrect use of file sharing apps and failing to use encryption can all contribute your data's vulnerability. Add to that the quantity and variety of equipment and platforms used and you have a recipe for disaster.

Data Loss Prevention

Data loss prevention isn't a simple stopgap solution, but one that requires an ongoing two-pronged approach. This involves a combination of a secure company network and careful implementation of best practices by all employees. Let's take a closer look at each.

Secure Company Network

Obviously, those who don't hold IT jobs can't be expected to understand every aspect of cyber security. However, having a global overview of the most important points can be very useful for managers in implementing best security practices company-wide. Here are some important points to keep in mind:

- **Compatible equipment.** By adopting and maintaining one operating system (i.e. Mac vs. Microsoft and iPhone vs. Android) across all company-issued equipment, you can minimize incompatibilities and subsequent glitches that could compromise data.
- **Security software.** Security software that includes firewalls and anti-virus features is an absolute must. This recent article by PCMag compares the best security suites on the market today.
- **Encryption.** Making use of your computers' encryption features can add a necessary layer of protection to sensitive data. Consider encrypting all company emails, as well as those files and folders on your network that contain sensitive information.
- **Storage.** Cloud-based storage offers two distinct benefits: it can be accessed from anywhere and it can't be accessed physically (unlike a hard drive or hard copy paper file). Choose a cloud storage provider that offers quality security features, as well as an intuitive interface that makes for easy use, to help secure the storage drives linked to your network.

Best Practices

When it comes to your employees, implementing a cyber security strategy is an ongoing endeavor. Pay attention to the following points:

- **Train your employees regularly.** From onboarding to regular reviews, training your employees about safe Internet use can play a large part in keeping your company's data safe.
- **Require passwords for device and app access**. Installing passwords on all equipment, from desktops to smartphones, forms a first layer of defense against data leakage.
- **Limit access to sensitive data.** Even if all your company's computers are on a single network, employ password protection to make sure drives or folders with sensitive data are off-limits to those who don't need to know.
- **Restrict the use of company equipment to business purposes.** By prohibiting personal use of company devices, you reduce the risk of viruses, malware and other threats that are oftentimes the result of recreational online traffic.

To learn more, visit the National Cyber Security Alliance's website Stay Safe Online. And remember, cyber crime is a costly threat. Staying informed goes a long way in keeping your company and employees safe online.

Source: http://guides.wsj.com/small-business/technology/how-to-keep-your-business-information-secure/; http://fcw.com/Articles/2010/01/25/FEAT-Cybersecurity-training-a-must.aspx; http://www.pcworld.com/article/2046300/hackers-put-a-bulls-eye-on-small-business.html; http://www.staysafeonline.org/business-safe-online/; http://www.net-security.org/article.php?id=2017; http://www.pcmag.com/article2/0,2817,2425215,00.asp; http://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/; http://heartbleed.com/; http://www.pcmag.com/article2/0,2817,2369749,00.asp; http://www.pcworld.com/article/2105100/loaded-and-locked-3-seriously-secure-cloud-storage-services.html