5 Deadly Mistakes You Are Making with IT Security

bis

BUSINESS INFORMATION SOLUTIONS

We Get IT Done!

In the world of IT security, hackers are always busy circumventing various cyber defenses and security companies are always found racing to react to these emerging cyber threats. This is just simply part of today's business world but there are steps you can take to help keep your company data safer and knowing which mistakes to avoid is the key. Here are 5 mistakes to avoid making.

1. Allowing employees to install their own network

As computing infrastructures become more diffused and decentralized, keeping machines and data secure becomes more challenging. These days, companies are able to hire and keep the best employees regardless of where they live. All those far-flung devices can become infected with malware that may also infiltrate the company's network and make off with valuable company data. Mobile devices also are susceptible to data leaks because they can be lost or stolen, as well as more easily accessed by an outsider. When data disappears, financial, legal and reputational problems can quickly follow.

What should you do to help prevent this from happening? Create a secure connection to the company network and ONLY use this network.

To reduce the chance of malware infection, use security software and practice good computer hygiene by using the latest versions of all applications. It's risky to rely on employees to take care of updating applications, be sure that your IT provider has monitoring and patch management tools on outside machines just like the ones on the local network. Installing encryption software is a great way

2. Not having a Security Awareness Training Program in place

A recent IBM study showed that the root cause of 95% of recent data breaches was human error. The best security technology in the world can't help you unless employees understand their roles and responsibilities in safeguarding sensitive data and protecting company resources. This will involve putting practices and policies in place that promote security and training employees to be able to identify and avoid risks.

Your company's security strategy will only work if employees are properly trained on it. Therefore, the importance of providing information security awareness training cannot be understated. Make sure employees know how and when it's safe to share information.

An effective security awareness program should include education on specific threat types, including but not limited to:

- **Malware**
- **Trojans**
- **Viruses**
- **Social Engineering**
- **Phishing**

3. Not requiring automated password changes

An important area to address is the importance of password construction and security. Seems minor? It's not. Believe it or not, password cracking is remarkably easy, particularly for advanced hackers. And this "minor" step that users take every day could make a significant difference in protecting your firm's sensitive information. Current data shows that it takes up to 16 months on average for companies to notice a security breach. In those 16 months, the bad actors have been stealing sensitive data that will be released into the wild and can never be retrieved.

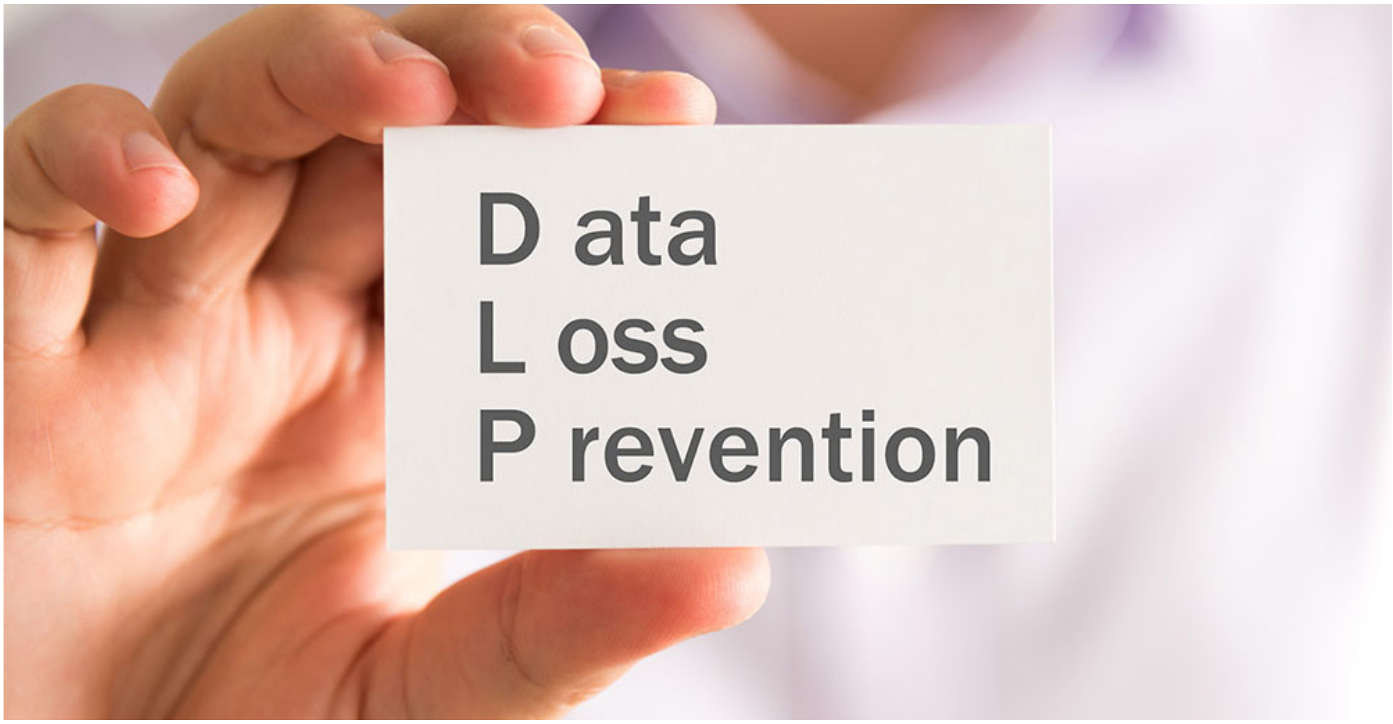
In the real world, it happens like this. Most usernames are the person's Email address and 60% of the time people use the same password across multiple accounts. So, if one site gets compromised your credentials are out in the wild and with a little social engineering the bad actors can have access to banking, retail, retirement, medical and other sites that have sensitive data. This is why the bad actors are trying to get your social media account passwords- so they can unlock the information about you to get to the real valuable data.

Requiring your employees to change their passwords routinely is a great practice. Making passwords long and strong, with a mix of uppercase and lowercase letters, numbers and symbols along with keeping them private should be a part of your company's policy.

4. Not have a Data Loss Prevention System in place

Keeping sensitive information secure from theft and vulnerability in today's digital world isn't as easy as putting a lock on the file cabinet. Email is the fastest way to get sensitive data into the hands of bad actors. It has been reported that only 50% of emails are encrypted and many people are sending credit card and social security numbers via email. When training new employees, you should always give employees instructions on what should and should not be sent via email via plain text. As well as a way to send sensitive data via encrypted Email.

Programs like Dropbox, Google One Drive, Box and hundreds of other applications allow for data to be sent from a network and stored into employee's personal accounts. No business owner would allow an employee to make copies of company data and store offsite at will. Yet this is what is happening thousands of times per day. Companies need to implement some form of Data Loss Prevention (DLP) system to protect sensitive data from getting into the wild.



5. Using devices that are not encrypted

Data theft is an uncomfortable reality for any modern business. Laptops get stolen, cloud storage accounts get compromised, disgruntled employees steal vital files, and thumb drives get left behind. And with modern devices capable of storing thousands of mission-critical data files, the loss of a laptop or phone can have very serious implications for any business. Losing vital trade secrets like designs for an upcoming product, the code for an app revamp or the balance sheets for the year gone by can all set you back months, if not years. Even worse would be the loss of client data and the reputation costs.

According to PC World Magazine, there are 82,000 new malware viruses created every day. The threats are increasing and spreading each year. There is no ONE filter to or design to catch them all so you must have a series of filters.

The best way of dealing with such an eventuality is to implement encryption across all devices you use – from any old Windows 7 desktop PC you still use, to the spanking new Windows 10 your business is mitigating to, and to even the smart phones your sales personnel use in the field.