

Are you your IT department's worst nightmare?

Company policies on using hardware, software and the Internet are becoming increasingly strict as employers attempt to protect confidential intellectual property. Employees may view the Internet, laptops and other mobile devices as efficient and convenient tools, but IT managers see them as windows to the world outside the company's protected walls. In addition, the use of social networks such as wikis, blogs and peer-to-peer networks may dramatically change how information is exchanged between businesses and consumers in the future.

Many professionals take their laptops and company information assets home with the best intentions of getting ahead on work-related matters. However, many things could happen to these laptops once outside the safety of the workplace. The loss or theft of a mobile device containing sensitive data can increase a company's vulnerability to fraud and result in loss of reputation and unanticipated expenses and/or legal penalties.

From experience conducting technology risk assessments and implementing new security strategies with more than 500 companies, Jefferson Wells found the following employee behaviors emerge as the

10 most common employee-related threats that could potentially cripple a company.

1. Taking an unencrypted laptop out of the office.

To protect sensitive company information, employees should use commercial security solutions to encrypt files on laptops or remove sensitive files from laptops before leaving the office.

2. Transporting sensitive company information on portable media.

USB flash drives, cellular phones, digital cameras and other types of portable media should be treated the same way as a laptop. Encrypt or remove sensitive information before leaving the office.

3. Listing company e-mail addresses on blogs and social networking sites.

A company is liable for every post, upload or e-mail sent using its name or hardware. Employees should be discouraged from using company e-mail addresses on these sites and instead use personal e-mail addresses.

4. Accessing personal e-mail accounts on company-assigned smartphones and PDAs.

A company e-mail program may have the proper controls, firewalls and filters in place, but personal e-mail accounts may not. Even if hardware is secure, viruses can automatically download by opening an e-mail from a personal account.

5. Connecting unapproved wireless equipment to company networks. This is similar to building a bridge from inside the company,

inviting anyone driving by to enter. The potential existence of wireless access points on your company network should be tested regularly.

6. Installing applications onto a company computer.

Unapproved application downloads could be rogue applications in disguise. Rogue applications, or malware, have malicious intent, whether it is taking sensitive information off the server, corrupting the network or using a computer's IP address as a vehicle to send spam mail.

7. Placing passwords in visible areas.

Employees should always protect their passwords by creating complex passwords that incorporate upper- and lowercase letters and numbers. As a general rule, passwords should be difficult to guess, easy to remember and never visibly posted.

8. Opening e-mails or clicking on Web links from unknown recipients.

Viruses come in all forms and have different purposes. Some are just e-mail scams, whereas others automatically download malicious software that could be used to take over a computer or use the user's e-mail address to send spam. Only open e-mails or access Web links from sites you know and trust.

9. Forwarding e-mail with off-color jokes or images to co-workers.

Not only does this put employees and companies in danger of harassment suits, but viruses or malicious downloads can come into the company through these e-mails.

10. Frequently e-mailing large

data files that could impact company bandwidth. A secure file transfer capability that is set up for sending and receiving large data files, such as a secure file transport protocol (FTP) server, should be considered instead of e-mail.

Some of the worst offenders of these 10 behaviors may not even be aware of the possible implications of their actions. It is advisable to work with your human resources department and/or legal counsel prior to deploying any new or revised security and control policies. Increasing awareness of

risky IT behavior should help employees and IT departments work together to create stronger companies with fewer technology vulnerabilities.



Paul Rozek is the director of technology risk management for the Milwaukee office of Jefferson Wells. He has more than 28 years of diverse experience in IT governance and frameworks, IT audit and compliance, business continuity planning and information security. He can be reached at paul_rozek@jeffersonwells.com or (414) 347-2345.