RISK Technology INSIGHTS

MM INSURANCE services

Young Employees and IT Security

Hiring young employees can bring fresh talent and innovation, giving your company an edge over your competitors. But that edge can quickly be erased, as young workers also bring additional technology risks. According to a Cisco Connected World Technology Report, 70 percent of young employees frequently ignore their company's information technology (IT) policies.

Millennials, generally those born in the early 1980s to late 1990s, have grown accustomed to sharing everything about their personal lives on social media sites such as Facebook, YouTube, and Twitter. Though these social platforms encourage users to share personal information, young workers should be actively encouraged to safeguard company data.

Common Misconceptions

Young employees, especially those new to a business environment, can have some common misconceptions when it comes to IT policies. Millennials can do the following:

- Forget the policies
- Believe their supervisors aren't monitoring computer or mobile device use
- Believe the policies are too inconvenient
- Think that the policies will make work inefficient
- Use unauthorized programs or applications to expedite work
- Assume that company security is handled entirely by the IT department

Additional Risks to Consider

Young employees can compromise IT security by leaving their computers or other personal devices unattended, increasing the risk that that both the equipment and company data could be lost, stolen or misused. Sending work-related emails to personal email accounts, and using computers and social networking sites for both work and personal reasons can also compromise IT security. Millennial workers may be more likely to blur the line between using IT for both personal and work-related purposes, which can increase the risk of negligence.

Though social media platforms encourage users to share personal information, young workers should be actively encouraged to safeguard company data.

Consider that not only young employees, but all employees can compromise IT security in the following ways:

- **USB flash drives:** While these are convenient portable devices for storing information, they make it too easy to take sensitive information out of the office and can be misplaced easily since they are so

small.

- **Wireless and wi-fi networks:** Whether it's an employee's personal Wi-Fi network at home or free Wi-Fi at the local coffee shop, it is important that employees use a secured virtual private network (VPN) and take other security measures when they log in on networks outside of your company.
- **Laptop computers:** Lightweight and handy for working remotely, laptops are also susceptible to viruses from improperly-secured networks.
- **Smartphones:** Though useful for obtaining information at your fingertips, smartphones are also another portable way to take sensitive data out of the office.
- **Collaboration websites:** Websites, such as a wiki or SharePoint site, are great tools for employees working together on projects; but it's critical that only authorized employees are logging in and accessing your company's projects on these sites.
- **Social media tools:** Sites such as Facebook and Twitter can benefit your business, but negligent use, such as including sharing critical company information, can be a risk.
- Other communication applications, such as peer-to-peer (P2P), Skype and instant messaging tools can be vectors for malware and a threat to information security.

Employers shouldn't necessarily prohibit employees from using technology, as this list includes many tools necessary to complete work-related tasks. It's important to know the risks and educate young employees to use technology properly.

Mitigating the Risks

Employers must find the balance between allowing young employees to use social networking websites and portable devices to do their jobs, while at the same time protecting company information. Employers should examine their exposures and consider what level of risk they are willing to accept. Here are some easy steps that will help secure your company's information safe:

- Review your company's IT policy. If it needs to be updated, speak with the professionals at Mindi McKinley Insurance Services for up to date cyber security information.
- Make sure all employees are aware of your company's IT policy and the consequences if the policy is not followed.
- Create strong, trusting relationships between young employees and your IT department.
- Create IT awareness materials so young employees are continually reminded of IT security risks and what they can to do prevent them.
- Train new young employees on data protection and IT security risks, and provide refresher training for seasoned employees to ensure everyone is aware of the risks and the importance of safeguarding company information.

Contact Mindi McKinley Insurance Services for more information on how to avoid IT security risks.