RISK INSIGHTS Technology

Ntegrity

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 the 2011 Cisco Connected World Technology Report, a study involving almost 3,000 university students and young professionals under age 30, 70 per cent of young employees frequently ignore their company's information technology (IT) policies.

Generation Y, generally those born in the early 1980s to late 1990s and also known as the 'Net Generation', have grown accustomed to sharing everything about their personal lives on Internet sites such as Facebook® and YouTube®. This poses a dilemma for an employer: If young employees don't safeguard their own personal information, how can you entrust them with your company's sensitive data? Companies with the need to be Internet-savvy must hire young talent…but are these employees worth the risk?

Eye-opening Statistics

The Cisco report cites 80 per cent of young employees think their company's IT policy is outdated or they don't even know about it. Additionally, 25 per cent of those in the study had been a victim of identity theft before age 30.

Why are young employees negligent about IT security? The study found that some young employees' attitudes and beliefs towards IT policies include:

- They forget about the policies.
- They think their bosses aren't watching.
- They believe the policies are not convenient.
- They think they don't have time to consider the policies while they're working.
- They feel they need to access unauthorised programs to get their job done.
- They believe security is the IT department's responsibility, not their own.

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. Generation Y workers are more apt to blur the line between using IT for both personal and work-related purposes, which can increase the risk of negligence.

> Eighty per cent of professionals under age 30 think their company's IT policy is outdated—or they don't even know about it.

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.

- 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 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 Wi-Fi networks.
- Smartphones. They provide information at your fingertips, but 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 authorised 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; however, negligent use, including sharing critical company information, can be a risk.
- Other communication applications, such as peer-to-peer (P2P), Skype and instant messaging tools. These applications 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 they need to get the jobs done. It's important to know the risks and educate young employees to use the 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. Other special considerations for managing young employees and mitigating the risk include:

- Review your company's IT policy. If it needs to be updated, ask recent graduates for advice on updating the policy to reflect current changes and trends in IT.
- Make sure young employees (and 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 NTEGRITY Insurance Solutions Ltd for more information on how to avoid IT security risks.