Employers Council®

Management Tips

Employers Council, the nation's largest employers association, has provided expert assistance and thoughtful guidance to employers since 1939. We collaborate with our members to develop effective, successful employer-employee relationships by providing "one-stop shopping" in every facet of human resources and employment law. Employers Council offers the broadest array of professional services under one roof. We walk alongside our members, offering guidance, support and expertise.

For more information about our services, contact the Utah office at 801.364.8479 or SaltLakeCity@EmployersCouncil.org.

Ryan Nelson, Attorney
Utah President

HR's Role in Cyber Security

February 1, 2018 / Employers Council

To remain profitable and relevant, businesses must do more than simply keep in step with a vast number of competitors. Organizations need the speed and other capabilities that technology can provide. Faster electronic-based technology and ever-increasing capabilities sound like a dream, but of course, there is another side to consider. The cost of computer-based crime is staggering to the world economy. According to Juniper Research, the rapid digitization of consumers' lives and the records of business will increase the cost of data breaches to $2.1 trillion globally by 2019, so it stands to reason that companies assume a substantial risk in utilizing technology.

A risk this costly must be controlled. So, how can a business properly manage its technological resources and mitigate this risk? Which department assumes this responsibility?

While some might say cyber security is the sole responsibility of an organization's IT department, the more informed view places the responsibility upon the entire organization and calls for HR to play a major role. Why HR? Consider the following:

Many security breaches are caused by human error. The "2017 Cost of Data Breach Study" by IBM shows that human error accounted for 24 percent of company data breaches in the U.S. in 2017. Employees are human and they make mistakes: they lose equipment, they write down passwords and/or use the same password for personal and business accounts, they send confidential information via email in error, they respond to phishing scams and open email messages that have viruses attached, and they fail to consistently follow protocol put in place for security. There are any number of reasons why employees make these mistakes, but the main reason is that they have not been properly trained. The opportunity for these errors to occur increases significantly when employers require employees to use their personal devices for work.

Some employees actually intend to harm an organization and seek to damage its resources and/or reputation. This can happen when the employer/employee relationship goes bad, regardless of whether the initial problem ends in a separation of employment.

Employees do not always dispose of company information in an approved manner. We have all heard the horror stories of sensitive hard-copy information being thrown out, intentionally or not, in its complete, readable form. And since electronic information lives "out there" forever, how can employees make sure this information is secure?

So how can HR help mitigate the risks associated with employees' use of company-wide technology?

- Work with IT to identify risks for data breaches and develop proper procedure, protocol, and employee training to properly address the risks identified.
- When it comes to hiring new employees, use pre-employment tests such as honesty and integrity tests to get the right people in the door.
- Once you have the correct people, use your onboarding process to get them off on the right foot in all areas, especially the security of your company's sensitive data/information.
- Develop and follow proper procedure for terminating an employee's security access immediately upon separation of employment.
- Stay up-to-date on the latest scams and train employees on how to handle them.
- Make sure only those employees with the need to know access your company's secure data.
- Don't let employees slide; even on the "small" stuff. If an employee fails to follow security procedures, be sure to re-educate and discipline as necessary.

Cyber security issues will never go away—they will continue to grow as technology shifts and changes. And, obviously, employees will always be human and subject to human error. Nonetheless, organizations must still work to reduce security breaches caused by the mistakes of mere mortals. Identify your organization's risks and develop policies and procedures to address them. Remain vigilant toward new issues and scams and take a proactive approach. Train and re-train employees as necessary and hold everyone accountable for the cyber security of your organization.