Cybersecurity and Data Protection

An alarming aspect of the wide-spread use of technology, one that individuals and businesses, including staffing companies, must effectively address, is cyber crime. Cyber attacks come in a variety of forms and are often an attempt to bring down a computer system, or an intrusion seeking to access and steal intellectual or proprietary data and information. At risk are such things as trade secrets, corporate reputation, employee data, customer data, and even physical damage to equipment. These attacks have reached the staffing industry. Notably, in 2012, executive search firm, Korn/Ferry International was a victim of sophisticated cyber attacks which accessed the company's databases potentially exposing individual social security, driver's license and credit card numbers to theft.

Threats to Data

Headlines about cyber attacks, security, and data privacy breaches abound, and have increased the focus on the vulnerabilities of IT security and the profile of cyber criminals. The cost of these attacks to the global economy is estimated to exceed $1.5 trillion. The wide-spread problem has grabbed recent headline with the likes of Target and Michael's sustaining massive, and very public, data privacy breaches.

Responsibilities of Businesses

Businesses, including staffing companies, which possess personally identifiable information, have numerous responsibilities under state, federal, and – in some cases – international law. Businesses have a responsibility to shareholders and customers to safeguard proprietary, confidential, and trade-secret information. Regardless of its size, businesses must comply with the laws that pertain to their possession or ownership of data. Actions may be brought against business as a result of breaches, including actions filed under federal laws such as Gramm–Leach–Bliley Act, Computer Fraud and Abuse Act, Electronic Communications Privacy Act, HIPAA, and numerous individual state and local consumer protection laws.

Pursuing Cybercriminals

Data breaches may result liability for the cybercriminal. Such wrongdoers may face prosecution for claims caused by security breaches, including actions filed under the Computer Fraud and Abuse Act and the Economic Espionage Act.

Practical Steps

Although not a complete shield to the above threats, staffing companies can take certain practical steps to mitigate the risks. At a minimum, staffing companies should consider the following 5 steps:

1. Identify Important Data

Owners should inventory and record the type and location of important data. Specifically, owner should determine: (i) whether the data is widely accessible by employees and others involved with the business; and (ii) what measures have been taken to guard the data.

2. Create a written security policy for employees.

Owners should create a written security policy for employees. At a minimum, the policy should address whether employees should be allowed to have personal data on business devices. Conversely, owners should also determine whether business data should be permitted on employees' personal devices and what to do in case a device is lost or stolen. Employees should be educated about the policy and the policy should be readily available. Owners should monitor compliance with the policy and enforce the policy uniformly.

3. Have formal procedures for New Employees, Departing Employees and Third Parties.

New Employees should be briefed on protection expectations early. Owners should explain the importance of safeguarding data. Departing employees should have access to data limited and monitored as departure date approaches. All hardware and access devices should be returned. Third party access to data should be subject to contractual restrictions such as a Non-Disclosure Agreement.

4. Use stronger passwords.

If a business' password is a common word, or something that can be guessed based on public information, consider changing it to something more difficult to crack. It is recommended that owners create passwords that are at least 12 characters long and contain upper and lower case letters, as well as numbers and special characters. Also, using the same password across multiple accounts should be avoided--the more passwords between cyber criminals and a business' data, the better.

5. Encrypt your data.

Owners cannot always keep cyber criminals out of their computer systems, so it is highly recommended that owners take steps to protect the data contained within those systems. One means of accomplishing this is the use of encryption. Disk encryption tools come standard on most operating systems. These types of programs essentially convert data into unreadable code that is not easily deciphered by cybercriminals.