Physical Protection of Cyber Assets

When it comes to securing cyber assets, many people often think only of mitigating cyber risks like spam, phishing and malware. However, cyber assets can also be compromised physically. This article examines the physical exposures your cyber assets face and provides steps for mitigating these risks.

Secure company facilities
The physical security of a facility depends on a number of security decisions that can be identified through a comprehensive risk-management process. It is easy to think about physically securing your company's facility as merely an exercise in maintaining control of access points and ensuring there is complete visibility in areas that are determined to be high-risk—either because of the threat of easy public access or because of the value of information located nearby. However, maintaining facility security also includes the physical environment of public spaces. For instance:

- Employees whose computers have access to sensitive information should not have their computer monitors oriented towards publicly accessible spaces such as reception areas, check-in desks and waiting rooms. Employees should be trained to not write out logon information on small pieces of paper affixed to computer equipment viewable in public spaces.
- Easy-to-grab equipment that could contain sensitive or personal information, such as laptops, tablets and mobile phones, should be located away from public areas. If you have an environment where employees are working in a waiting room or reception area, train them to not leave these types of devices out on their desks unsecured.
- Consider using cable locks as an easy way to increase security for laptop computers. Most laptops feature a lock port for a cable which can be connected to the user's desk. Be sure to store the key to the cable lock in a secure location away from the desk the computer is locked to.
- If extremely sensitive information is stored on a laptop, consider installing tracking software. Most tracking software programs run unnoticed, and allow stolen computers to be located more easily. Many also allow administrators to wipe the hard drive remotely if necessary.
- Consider implementing a badge identification system for all employees, and train employees to stop and question anyone in the operational business area without a badge or who appears to be an unescorted visitor.

Minimise and safeguard printed materials with sensitive information.
The most effective way to minimise the risk of losing control of sensitive information from printed materials is to minimise the quantity of printed materials that contain sensitive information. Establish procedures that limit the number of copies of printed reports, memoranda and other material containing personal information.

Safeguard copies of material containing sensitive information by providing employees with locking file cabinets or safes. Make it a standard operating procedure to lock up important information. Train employees to understand that simply leaving the wrong printed material on a desk, in view of the general public, can result in consequences that impact the entire company and your customers.

Ensure mail security.
Your organisation's post centre can introduce a wide range of potential threats to your business. Your centre's screening and handling processes must be able to identify threats and hoaxes and eliminate or mitigate the risk they pose to facilities, employees and daily operations. Your company should ensure that managers understand the range of screening procedures and evaluate them in terms of your specific operational requirements.

Dispose of rubbish securely.
Too often, sensitive information, including customers' personal information, company financial data, and company system access information, is available for anyone to find in the rubbish. Invest in business-grade shredders and buy enough of them to make shredding convenient for employees. Alternatively, subscribe to a trusted shredding company that will provide locked containers for storage until documents are shredded. Develop standard procedures and employee training programmes to ensure that everyone in your company is aware of what types of information need to be shredded.

Dispose of electronic equipment securely.
Be aware that emptying the recycle bin on your desktop or deleting documents from folders on your computer or other electronic device may not delete information forever. Those with advanced computer skills can still access your information even after you think you've destroyed it.

Disposing of electronic equipment requires skilled specialists in order to ensure the security of sensitive information contained within that equipment. If outside help, such as an experienced electronic equipment recycler and data security vendor, is not available or is too expensive, you should at a minimum remove computer hard drives and have them shredded. Also, be mindful of risks with other types of equipment associated with computer equipment, including CDs and flash drives.

Train your employees in facility security procedures.
A security breach of customer information or a breach of internal company information can result in a public loss of confidence in your company and can be as devastating for your business as a natural disaster. In order to address such risks, you must devote your time, attention and resources (including employee training time) to the potential vulnerabilities in your business environment and the procedures and practices that must be a standard part of each employee's working day.

And while formal training is important for maintaining security, the daily procedures you establish both in how you normally conduct business and in the way you model good security behaviours and practices are equally important. In short, security training should be stressed as critical and reinforced through daily procedures and leadership modelling.

Establishing procedures and training employees to physically protect your company's cyber assets will allow for a secure work environment. For additional information or sample workplace policies, contact your Crendon Insurance Brokers Ltd representative.