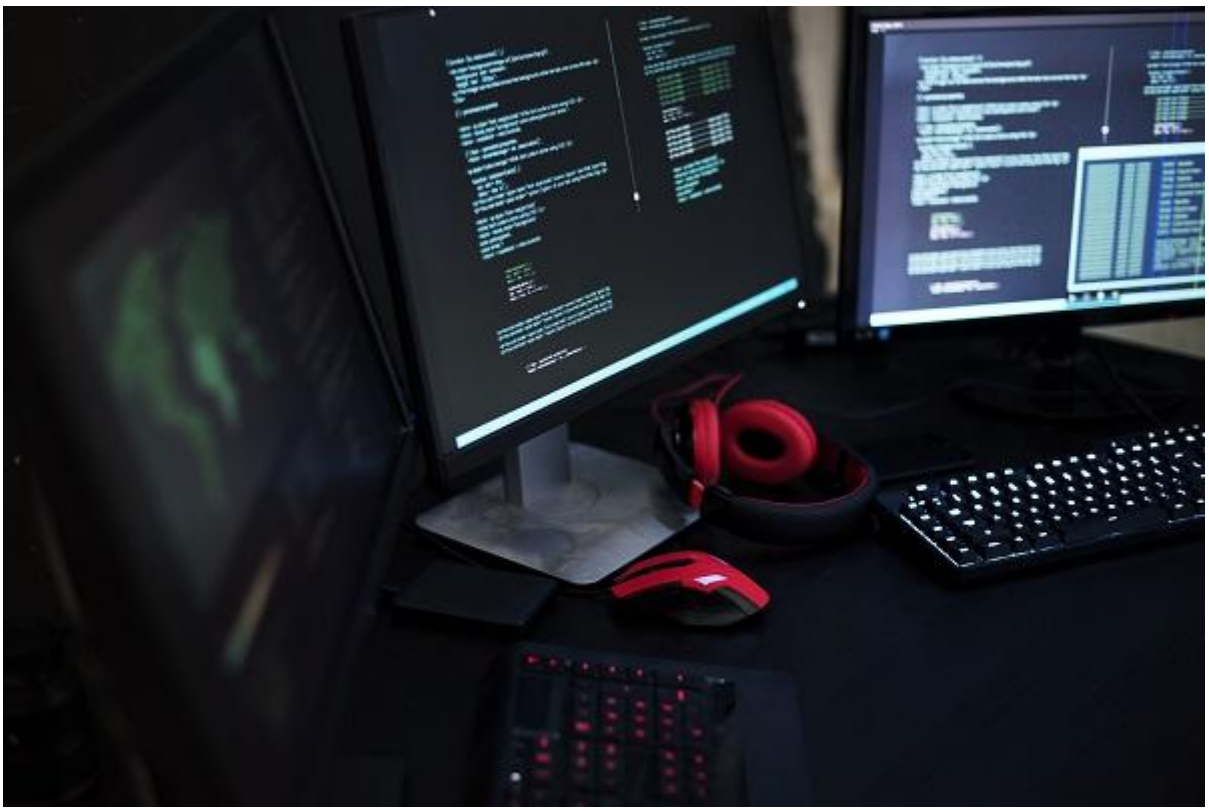
September 25, 2018

Important guidelines to enhance cybersecurity for businesses



One of the most important elements of cybersecurity is constant monitoring of the nature of security risks.

The approach of cybersecurity is to focus resources on crucial system components and to protect the biggest known threats without leaving components defenceless against less dangerous risks. Within an organisation the people, processes and technology must function in collaboration to create an effective defence against cyber-attacks. Let’s quickly look at them individually:

- **People**

Data controllers must understand and comply with basic data security principles, for example passwords, attachments in e-mails and storage of data.

- **Processes**

Data controllers must have a framework for dealing with attempted and successful cyber-attacks. This framework must include the manner in which the Company identifies cyber-attacks, protects systems, detects and responds to threats and recovers from successful attacks.

- **Technology**

Technology in the organisation should be updated and protected, for example computers and routers, networks and the cloud, firewalls, malware protection, antivirus software and email security solutions.

- **Staff**

Staff should be aware of cyber risks and be trained on a regular basis to be diligent in identifying possible cyber breaches.

Important elements of cybersecurity

Ensuring cybersecurity in the current business environment requires a more proactive and adaptive approach to the coordination of efforts throughout an information system, which includes Application security, Information security, Network security, Disaster recovery, Operational security and End-user education.

Types of cybersecurity threats

The process of keeping up with new technologies, security trends and threat intelligence is a challenging task. It is essential, however, in order to protect information and other assets from cyber threats, which could take many forms:

- ***Ransomware*** is a type of malicious software that involves an attacker locking the victim's computer system files and demanding a payment to decrypt and unlock them. Payment will not guarantee that the files will be recovered or the system restored;
- ***Malware*** is a type of software used to gain access or cause damage to a computer, such as worms, computer viruses, Trojan horses and spyware;
- ***Social engineering*** is an attack that relies on human interaction to trick users into breaking security procedures and revealing sensitive information. Examples of social engineering include clicking on a link, downloading malware or trusting a malicious source;
- ***Phishing "419 scams"*** is the practice of sending fraudulent e-mails that resemble e-mails from reputable sources. The aim is to steal sensitive data such as credit card numbers and login information.

Implementing guidelines to enhance cybersecurity

Awareness and constant monitoring are important in ensuring cybersecurity. Implementing guidelines to identify and assess risks in the business environment is crucial to enhance cybersecurity.

- Never open an e-mail if it appears in your spam folder and never click on links that seem suspicious and unexpected.
- Ignore unexpected warnings for security software. They may appear via e-mail or may pop up in a new browser window. This scareware is designed to infect and access your data.
- Install and update good antivirus and anti-malware programs.
- " Social hacking" occurs when someone impersonates someone else in an attempt to get sensitive information or access your computer by installing software or clicking on a malicious link. Never give out personal information to strangers who call on the phone.

Conclusion

The implementation of practical, innovative security technologies can be overwhelming at first. Identifying cybersecurity risks and monitoring these risks are the first steps to cybersecurity. Implementing guidelines and an assessment framework for cybersecurity programs seek to enable critical information security infrastructure.

SERR Synergy assists businesses in compiling an Information Security Management policy where the physical information and cybersecurity risks of organisations are identified and managed to maintain the confidentiality, integrity and legitimate availability of data.

Don’t miss the next part of our analysis and practical guide to ensure cybersecurity and learn how cybersecurity relates to all aspects of Information Compliance legislation in South Africa.

About the Author: Retha van Zyl completed her BCom Hons (Economics and Risk Management) studies at the North West University. She joined our team in January 2016 and currently holds the title ‘Information Compliance Advisor’. She specialises in POPI and PAIA compliance, which includes compiling and submitting PAIA manuals to the Human Rights Commission. She also compiles and implements Information Security Management policies to identify risks associated with information security in each department within an organisation.