COMPUTER SECURITY – BEWARE OF LENDING YOUR EARS OUT

Cybersecurity, to some, is simple and easy. As with your business premises, they say, merely position guards – in this case technology – at the entrance doors to your enterprise's computer system. To them this is logical as it allows passage to what must enter and exit whist keeping unwanted perpetrators out.

To an extent they're correct. But they miss one important point – the threat to computer systems is much more complex than that.

This month's bulletin

In this bulletin we look at computer security. We share information which covers more than just the guards at the portals to your computer metropolis, as technology is merely one of the lines of defence against cyber threats and malicious agents.

Risk indicators

A lack of computer security can have devastating effects on a business. Tell-tale signs that malicious activity is already taking place within your computer system, could be the following:

- Theft of company assets by making use of the computer system
- Company website had been hacked
- Ransom attacks
- Loss of money due to phishing
- Unauthorised disclosure of confidential organisational information
- Errors in transaction processing without being able to hold someone accountable
- Malware attacks resulting in unavailable computing resources

And even if none of the above is happening in your business, without the necessary precautionary measures against cyber-attacks, it can happen at any moment.

It involves three key issues

Computer security deals with preventing and detecting unauthorised access to and/or use of an organisation's computing, information and data resources. Computer security is therefore the way to:

1. Enforce segregation of duties relating to individual employees in an organisation in terms of roles assigned to them by the organisation.
2. Prevent internal staff to exceed their mandates and/or introduce mechanisms that can detect and report such prohibited activities.
3. Prevent and/or detect unauthorised individuals or systems accessing the organisation's computing, information and data resources.

Computer security requires an inclusive approach

The US National Institute of Standards and Technology Cybersecurity Framework suggests the following all-inclusive approach to achieve the required computer security outcome:

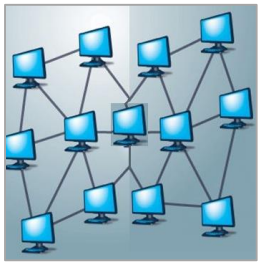
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

The solution lies in the combination

From the above table it is clear that safeguarding your computer system's access and exit points as we've hinted with tongue in the cheek in the introduction to this bulletin, is merely one of a number of activities to ensure the protection of the complete system. Access control, together with awareness and training, data security, information protection, maintenance, and protective technology, must function alongside one another to offer comprehensive protection (see the PROTECT section in the table above). Only when combining and maintaining these six elements will you be able to ensure the highest level of computer security.

Inroads and access points into a computer system

Computer infrastructure today consists of numerous applications that can be accessed in countless ways. For example, an application can be accessed from more than one device in a local area network, in a multi-branch network, even via the internet. In a business such applications can include accounting systems, HR records, filing systems and e-mail, to mention only a few.



One way to look at this is the concept of an access path which is followed by the device that a user would use to gain access to an application, as well as all the components within the computer infrastructure that the user's device requires access to in order to fulfil the user's request. But this is a very basic example. Within the computer environment there are multitudes of access paths of which each poses the risk of security vulnerability. Some of these access paths are highly technical and are often exploited by hackers to gain unauthorised access to computer systems.

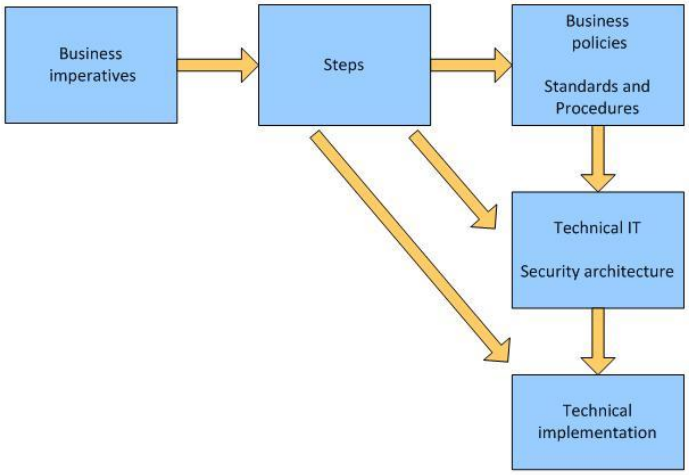
A computer security framework for a business

Three important components
Although computer security is far-reaching and complex, in essence it entails three broad components:

1. addressing business-related issues,
2. translating these into technical computer requirements, and
3. aligning the above two.

If not aligned, specific computer security risks arise. And often these risks are not considered or even evident. In addition, if an organisation's total computer environment lacks integrity, it may compromise the whole organisation, leaving it completely vulnerable.

The diagram below illustrates the computer security framework for a business. It starts with the requirements of the business which translates into business policies. (It is important to note that these policies cover the full business spectrum, not only IT policies.) Policies, in turn, get substantiated in standards and procedures. Only then can all of this translate into technical computer requirements and implementation of computer security measures. Business imperatives come first with IT requirements at the end, not the other way around.



Mechanisms to ensure computer security

In most instances mechanisms to ensure computer security consist of standard measures within the business and IT industries that are readily available and easy to apply. Again, the business imperatives come first, with these measures often going hand in hand with and supporting even non-IT related best practice standards within businesses.

Use what is available to you
Ensure segregation of duties between valid end users by enforcing system logon procedures and creating permission settings specific to individual users' roles and applications as assigned by the organisation. Such segregation of duties within the IT environment is typically enforced by system settings, logon procedures, database access protocols, security authorisations and a myriad of other configuration settings in the remainder of the organisation's IT infrastructure. These, in addition to components such as firewalls and proxies – a tool that your computers can use to protect IT users and their information – safeguard the organisation from unauthorised external access by unapproved individuals or systems.

Develop a computer security architecture to ensure that the organisational policies regarding computer security are appropriately implemented. This will structure all the components within the organisation's computer system and their settings in a cohesive manner.

Principles that apply
Within the computer security architecture a number of principles apply:

1. **Organisational measures:**
   - Ensure that computer security and risk policies as well as organisational practices are in place.
   - Train staff to be aware of and to adhere to computer security policy and practices.

2. **Technical measures**
   - Users must identify and authenticate themselves by means of passwords, biometrics or any other appropriate mechanism when requesting access to computing or information resources.
   - Every user must have some form of profile in every component in the system that they use to fulfil their duties. These profiles restrict their rights.
   - Every component must ensure its own integrity and/or prevent/detect unauthorised access.
   - The computer security architecture must take the business imperatives and requirements into account. For example risks in the banking industry differ considerably from those in a manufacturing environment. Each type of industry and each entity within those industries would therefore have different security policies and computer security architectures.
   - The multitudes of software components within any computer environment form numerous access paths to individuals and systems within this environment to be able to fulfil their duties. These access paths can and are being exploited by unauthorised users or systems (perpetrators). Hence all access paths need to be taken into account in computer security architecture.

Forget about ad hoc measures

When it comes to computer security in a business, ad hoc measures do not work. There is only one correct and all-encompassing approach. First address the business-related issues, then translate these into technical computer requirements and, finally, align the two.

Computer security also entails not lending your ears out. The risk is, if you do, that you may only pick up those what-I-want-to-hear messages from the "some say" brigade – messages which, if you apply them, may cause your business to be under-protected and vulnerable.