CYBERSAFE LEGAL

Tip 4: Boost your network security – both physical and technical

As the data and confidential information your business uses becomes increasingly valuable, ensuring your networks have adequate security becomes more crucial. When discussing network security, we need to look at both the physical dimensions of this security as well as the technical.

Listed below are some basic steps every organisation can take to protect their digital assets, information systems and data.

1. **Secure the Perimeter:** The most basic step of network physical security is protecting the perimeter. In short, you want to keep people as far away from your network systems and data centre as possible.

Basic physical security methods include fence-mounted intrusion detection systems, obvious and hidden deterrents and a good building security plan that can prevent outsiders from gaining access to your systems.

2. **Internal security Measures**: Ensure that all wiring closets and other locations where the network infrastructure components are placed have been physically secured from both the public and employees. This is essential given that a large number of network hacks involve employees or company insiders

Lock all cabinets and doors.

Require proof of user authority to access the location of the infrastructure.

Ensure wireless access points are out of side and not easily accessible.

Verify that any cabling is out of sight and not accessible. And disconnect any unused ethernet ports: either directly or via a switcher/router configuration.

3. **Access Control:** If it is possible, limit facility entry points and ensure that anyone gaining access must come in contact with a receptionist/security person and pass by some kind of surveillance cameras at the entrance to the facility.

Track and monitor all people entering the facility and determine the time of access and length of stay.

Time limit access and ensure that contractors/guests have a limited right of access and cannot re-enter after leaving.

4. **Install surveillance cameras over the entire site:** It is best to use surveillance cameras at all levels of the facility – exterior perimeter, all entrances to the data centre or facility.

Ensure that all camera footage is stored and recorded so that it can be reviewed when needed.

5. **Implement a policy for network security:** Every organisation would benefit from a written document outlining the user policies in relation to your information systems – who has access, what privileges they have and what limitations they have. This policy should also include an assessment of critical business data assets and contain a disaster recovery plan.

6. **Create a culture of cyber security amongst your users.** The easiest way to break into a network is by exploiting the weakest link. In most cases this is your users and employees.

Ensure that every member of staff understands the importance of network security and what they can do to support this.

7. **Strong password practice:** the network is better protected when all users are required to have strong passwords. More than 8 characters long, a combination of upper and lower case, numbers and symbols is best practice.

Use of dual factor authentication and appropriate password managers can also help.

8. **Employ antivirus software firewall protection:** This seems obvious, but a trustworthy firewall can block inappropriate or unauthorised access to your network systems. Good firewalls can monitor all the web traffic and provide reports on user behaviours and inconsistencies. It helps to provide a shield around your systems and prevent unwanted access to your networks.

Antivirus software can detect and block hostile or malicious software from being downloaded onto your systems.

9. **Adopt a patch management program:** One of the easiest ways for hackers to gain access to information systems and networks is when old versions of software are not updated. Software companies issue patches, many aimed at increasing security, on a regular basis. Ensure that patches are uploaded as soon as they are issued to further protect your systems.