CYBERRISKS&LIABILITIES_

Network Security

As the amount of sensitive information on your computer network grows, so too does the need for appropriate measures to ensure this data is not compromised. To properly secure your company's network:

- Identify all devices and connections on the network,
- Set boundaries between your company's systems and others, and
- Enforce controls to ensure that unauthorised access, misuse or denial-of-service events can be thwarted or rapidly contained and recovered from if they do occur.

Use the following tips to create a safe and secure network.

Secure internal network and cloud services.

Your company's network should be separated from the public internet by strong user authentication mechanisms and policy enforcement systems such as firewalls and web filtering proxies. Additional monitoring and security solutions, such as anti-virus software and intrusion detection systems, should also be employed to identify and stop malicious code or unauthorised access attempts.

- Internal network: After identifying the boundary points on your company's network, each boundary should be evaluated to determine what types of security controls are necessary and how they can be best deployed. Border routers should be configured to only route traffic to and from your company's public IP addresses; firewalls should be deployed to restrict traffic only to and from the minimum set of necessary services; and intrusion prevention systems should be configured to monitor for suspicious activity crossing your network perimeter. To prevent bottlenecks, all security systems you deploy to your company's network perimeter should be capable of handling the bandwidth that your internet service provider offers.
- Cloud-based services: Carefully consult your terms of service with all cloud service providers to ensure that your company's information and activities are protected with the same degree of security you would intend to provide on your own. Request security and auditing from your cloud service providers as applicable to your company's needs and concerns and ensure the provider's policies and workflows comply with your jurisdiction's regulations governing how data is handled and stored. Make sure to review and understand service level agreements, or SLAs, for system restoration and reconstitution time.

  You should also enquire about additional services a cloud service can provide. These services may include backup-and-restore services and encryption services, which can further bolster your data security.

Develop strong password policies.

Generally, two-factor authentication methods, which require two types of evidence that you are who you claim to be, are safer than using only static passwords for authentication. One common example is a personal security token that displays changing passcodes to be used in conjunction with an established password.

Additionally, password policies should encourage your employees to use the strongest passwords possible without creating the need or temptation to reuse passwords or write them down. That means using passwords that are random, complex and long (at least 10 characters), that are changed regularly and that are closely guarded by those who know them.

Secure and encrypt your company's Wi-Fi.

Your company may choose to operate a Wireless Local Area Network (WLAN) for the use of customers, guests and visitors. If so, it is important that the WLAN be kept separate from the main company network so that traffic from the

public network cannot traverse the company's internal systems at any point.

Internal, non-public WLAN access should be restricted to specific devices and specific users to the greatest extent possible while still meeting your company's business needs.

Where the internal WLAN has less stringent access controls than your company's wired network, dual connections—where a device is able to connect to both the wireless and wired networks simultaneously—should be prohibited by technical controls on each such capable device. All users should be given unique credentials with preset expiry dates to use when accessing the internal WLAN.

Encrypt sensitive company data.

Encryption should be employed to protect any data that your company considers sensitive, in addition to meeting applicable regulatory requirements on information safeguarding. Different encryption schemes are appropriate under different circumstances.

If you choose to offer secure transactions on your company's website, consult with your service provider about available options for a secure socket layer (SSL) certificate for your site.

Regularly update all applications.

All systems and software, including networking equipment, should be updated in a timely fashion as patches and firmware upgrades become available. Use automatic updating services whenever possible, especially for security systems such as anti-malware applications, web filtering tools and intrusion prevention systems.

Set safe web browsing rules.

Your company's internal network should only be able to access those services and resources on the internet that are essential to the business and the needs of your employees. Use the safe browsing features included with modern web browsing software and a web proxy to ensure that malicious or unauthorised sites cannot be accessed from your internal network.

If remote access is enabled, make sure it is secure.

If your company needs to provide remote access to your internal network over the internet, one popular and secure option is to employ a secure Virtual Private Network (VPN) system accompanied by strong two-factor authentication, using either hardware or software tokens.

Create a safe-use flash drive policy.

Ensure that employees never put any unknown flash drive or USBs into their computers. Businesses should set a clear policy so employees know they should never open a file from a flash drive they are not familiar with, and that they should hold down the Shift key when inserting the flash drive to block malware. By doing so, you can stop the flash drive from automatically running.

For more information about how to keep your network and your data secure, contact Sentio Insurance Brokers Ltd today.