crawford
Technology Consulting

☎ 08 8215 4231
✉ CYBER@CRAWFORDCONSULTING.COM.AU

FROM CONFIDENTIAL COMPANY DATA TO PERSONAL INFORMATION, THE GROWTH OF THE INTERNET AND CONNECTED DEVICES MAKES DATA MORE VULNERABLE TO ATTACKS.

BELOW IS OUR 3-STEP PLAN FOR STRATEGY AND AWARENESS.

1

APPLICATION SECURITY

This is the most basic form of security that most organisations will understand.

✓	WHAT	WHY
	Antivirus	Last line of defence for a computer. Prevents viruses from executing on the computer.
	Antispam	Dodgy emails equate to 60% of all emails. Preventing emails from reaching users will reduce likelihood a user opening virus.
	Firewall	Prevents hackers from accessing your network over the Internet and planting viruses into your system.
	Web Protection	Prevent users from browsing to sites that may contain viruses.
	Backups	If all else fails, you will need to recover data from backup. Ensure your backup is not at risk of being wiped out by a virus.

2

USER TRAINING

The human element is often the weakest point in security. Most attacks target the user, looking to trick them into opening an email or clicking a link.

Here are some items your business needs to consider highlighting with users.

- **WEAK PASSWORDS**
  use a combination of upper case, numbers, and symbols
- **OVERCONFIDENT USERS**
  know how to spot fake emails or dodgy links.
- **OWNERSHIP**
  being proactive when they think they have introduced a threat rather than staying silent and waiting for the network to fall over.
- **REMOTE ACCESS POLICY**
  educate your users on how to identify safe public Internet out of the office, versus something that is risky.
- **REITERATE**
  have a plan to remind users of all the above

3

BUSINESS RECOVERY

Regardless of your security, you always need a backup plan. It is important to understand the two facets to business recovery.

DISASTER RECOVERY (DR)

The DR plan explains how you will recover the data in the event of a disaster. It should include:

- Recovery plan for each of the applications on your network (emails, files, database)
- Who is responsible
- The method of recovery
- Expected turnaround time

Basic insurance coverage is generally called Cyber Risks Extension, and cover the cost to repair systems relating to a cyber-attack, including ransom payments.

BUSINESS CONTINUITY PLAN (BCP)

The BCP plan details how your business will continue to trade should a disaster hit. It should include:

- Plans for events outside of your control (DR, theft, power outage, flood, Internet outage, access issues to office)
- Plan activation and response teams

Comprehensive insurance coverage is generally called Cyber Stand Alone and cover for the cost to repair systems relating to a cyber-attack, as well as business interruption.

ENSURE YOU CONSIDER INSURING AGAINST THIS RISK.

IN 2016, 33% OF AUSTRALIAN BUSINESSES EXPERIENCED A CYBER RELATED ISSUE. 60% OF ALL ATTACKS TARGET SMALL TO MEDIUM BUSINESSES. THE AVERAGE COST OF A CYBER-ATTACK TO A BUSINESS IS $276,323. (SOURCE: HTTPS://WWW.STAYSMARTONLINE.GOV.AU)

SHOULD YOU NEED MORE HELP, PLEASE CONTACT CRAWFORD CONSULTING
☎ 08 8215 4231
✉ CYBER@CRAWFORDCONSULTING.COM.AU