SMALL BUSINESS DIGITAL CHAMPIONS
AN AUSTRALIAN GOVERNMENT INITIATIVE

(ndp) National Disability Practitioners

NDS National Disability Services

FACT SHEET **Session 3** **Cyber Security – Part 1**

This will be the first session which will focus on Cyber Security. Successful digital transformation is not possible if cyber security isn't understood and integrated into your strategic plan. We will also explore digital tools to help you check emails and password integrity.

- ❑ Overview of objectives of digital transformations
- ❑ Value and costs of being hacked
- ❑ Cyber security definitions and points of vulnerability
- ❑ Managing your risk
- ❑ Minimum recommendations

Defining Digital transformation:
The integration of digital technology into all areas of a business which should fundamentally change how you operate and deliver value to customers. It's also a cultural change that requires organisations to continually challenge the status quo, experiment, and get comfortable with agile and responsive trial and error.

As we proceed through these sessions it is important to start with revisiting the objectives for digital transformation and the areas of importance in creating a digital strategy.

Hopefully by now many of you will have begun mapping out your digital strategy. This takes a commitment from the senior management team who will ultimately drive this strategy. But all staff must be involved. The leading cause for unsuccessful digital strategies is failing to engage staff and failure to collect critical information on the details of all processes and procedures. When a digital strategy is foisted on a workforce it will be criticised and undermined.

Objectives for Digital Transformation

- ❑ Improve Customer Experience
- ❑ Increase Efficiency
- ❑ Improve Business Decision Making
- ❑ Create SEO (Search Engine Optimisation)
- ❑ Improve Cyber Security
- ❑ Improve Innovation
- ❑ Transform the business

A successful Digital Strategy is split into the following key areas of development.

Each other of these key areas must be detailed with clear definitions of your goals and a development plan of who is responsible, KPI's for delivery and what resources will be committed. Mapping out what is currently happening throughout the business and new ideas on how to use technology to improve these areas are also important. Don't worry about whether the technology to achieve these goals exists, focus on the ideas, the strategies and the end results required. A digital strategy should be split into the following areas.

- Business Goals – Transformational targets - Big picture, but not a vision statement. But goals which relate to the new goals of your organisation on this digital transformation journey. What do you expect from your executive management, your staff and your technology companies? What are the end goals to map your success back to?

- Outcomes – Specific desired results across each area of the business. This should include estimated percentages of improvement, engagement and profitability. The map to which you quantify success.

- Personas – Users and Needs – Who are the engagement key stakeholders? What level of security can they access your systems? Develop the levels of access and who can access the system. Through their phones, home computers, work stations only, any other devices?

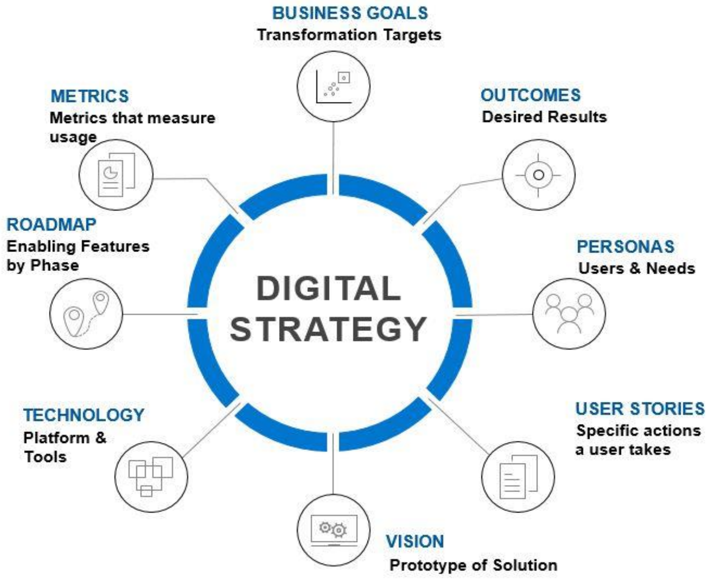
- User Stories – Specific actions a user takes – how do people use your current systems? How would you like them to use the systems in the future? The beginning of mapping which leads into Vision.

- Vision – Prototype of solution – The actual mapping of the system you are looking to develop. Detailed wireframes of the processes, step by step in the system.

- Technology – Platform and tools – What are your legacy systems and what type of systems do you want into the future? (not by name, but by function)

- Roadmap – Enabling features by phase. The strategy for mapping the timing and KPI's of the successful strategy.

- Metrics – Metrics that measure usage, data, analytics, feedback and communication.



There are many benefits to companies investing in both technology-enabled initiatives and leadership capabilities. The financial benefits are impressive.

9% of companies generate more revenue

12% have an overall higher market value

And 26% are more profitable

The opposite is true if investment isn't made. This session is focused on Cyber Security. Without investment if proper cyber security planning and protection your business will experience costs across a number of key areas:

- □ Loss of productivity
- □ Additional costs in tracking the breach
- □ Additional costs in repairing and rebuilding both files and databases
- □ The costs of losing Intellectual Property
- □ The costs of legal action both in trying to recover business costs but also in any legal fees in cases brought against you by your clients or stakeholders affected

Cyber Security:

The investment, training and understanding of cyber security for businesses can be expensive and frustrating for business owners and their staff. Over the last 20 years we've relished in the advancements which has seen the ease of use of the internet accessible to almost every age demographic. But with this ease of use, comes complacency and an increase if cyber-crime.

Cybercrime takes two forms:

- Crimes where computers or other information communications technologies are an integral part of an offence (such as online fraud)
- Crimes directed at computers or other technologies (such as hacking).

The Australian Criminal Intelligence Commission (ACIC) is concerned about cybercriminals who are trying to make a profit from Australians. Australia is an attractive target for organised crime syndicates due to our nation's relative wealth and high use of technology such as social media, online banking and government services. Due to the possible lucrative financial gains for organised crime syndicates, the cybercrime threat is persistent.

The Cyber Security Review, led by the Department of the Prime Minister and Cabinet, found that cybercrime is costing the Australian economy up to **$1 billion** annually in direct costs alone.

Cybercrime is diverting funds from our economy and causing other damages including:

- Damage to personal identity and reputation
- Loss of business or employment opportunities
- Impact on emotional and psychological wellbeing

A few examples of cybercrime include ransomware and credential harvesting malware:

- **Ransomware**—this is a type of malware that facilitates extortion. It usually infects a victim’s computer after the victim opens a malicious email attachment. Following infection, ransomware locks a computer’s content and displays a message requiring victims to pay a ransom for a decryption key that will supposedly allow them to regain access. The emails delivering ransomware to Australian victims use branding of trusted and well known Australian corporations as part of their social engineering techniques.
- **Credential harvesting malware**—this is malware designed to harvest a user’s credentials when they are logging onto a website. This is done completely covertly so the victim is unaware their credentials are being stolen. The malware that facilitates this harvesting is usually delivered to a victim’s computer or device via an email with a malicious attachment or by clicking on a website posted on social media.

As the principal threats to Australians from cybercrime are from offshore, recovery and tracing these criminals are incredibly difficult. Cybercriminals who are impacting Australian victims work together even though they may live in different countries or even different continents. This makes cybercrime activities inherently fluid and flexible.

This is why serious investment in the protection of your information, your staff’s information and your client’s information has never been more important!

Cyber Security Definitions

API: An application programming interface is an interface or communication protocol between a client and a server intended to simplify the building of client-side software

Bot: An Internet bot, also known as a web robot, is a software application that runs automated tasks over the Internet. Typically, bots perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone

Botnet Malware: The botnet malware typically looks for vulnerable devices across the internet, rather than targeting specific individuals, companies or industries.

Cyber Ransom or Ransomware: Ransomware is a type of malicious software designed to block access to a computer system or computer files until a sum of money is paid. Most ransomware variants encrypt the files on the affected computer, making them inaccessible, and demand a ransom payment to restore access

VPN: A virtual private network (VPN) protects computing devices by extending a private network across a public network, and enables users to send and receive data across shared or public networks as if it was directly connected to the private one. Applications running may benefit from the functionality, security, and management of the private network. Encryption is a common and although it is not fool-proof, it is an important part of effective cyber security. (Examples: Ghost VPN, Nord VPN, Express).

Security or Cyber Hygiene: Refers to best practices that computer system administrators and users can undertake to improve their cybersecurity while engaging in common online activities, such as web browsing, emailing, backups and sharing files.

Multi-Factor Authentication: Or (MFA) is an authentication method in which a computer user is granted access only after successfully entering two or more pieces of evidence (or factors). It's common practice that these factors are something the user and only the user knows.

2FA: Two-factor authentication (2FA) is a second layer of security to protect an account or system.

The Value of a Hacked PC

Although it may seem that accessing a PC is difficult and that anti-virus protection stops most viruses from causing damage. Nothing could be further from the truth. Cyber criminals are well ahead of the standard protection products currently in the market. You may believe that accessing your computer would not yield financial benefit, but here are only a few of the opportunities when someone accesses your computer illegally:

Bot Activity: Allows hackers remotely to act from your computer to commit crimes, fraud and removes any trace that this has been done remotely.

Account Credentials: Allows financial and website credentialing which provides the hacker to access other encrypted information you might be privy to as well as set up fake eBay and PayPal auctions.

Financial Credentials: Allows access to your bank account, credit card, stock trading and superannuation data.

Hostage Attacks: Allows the creating from your computer of fake antiviruses, ransomware, email ransom and webcam extortion

Reputation Hijacking: Allows hackers to pose as you or your company on social media, which can lead to legal action against individuals or companies.

Virtual Goods: Allows access to license keys which can be resold, online gaming or goods being purchased and product sales fraud.

Email Attacks: Allows the hacker to pose as the user to harvest large amounts of data and perpetrate scams and spam attacks

Web Server: Allows the hacker to create Malware and Phising fraud, use your computer to access child pornography and other illegal acts of piracy.

As you can see many assets are at risk, including:

- □ Product privacy and confidential information
- □ Sensitive information and data
- □ Identity theft
- □ Computer damage and software malfunction
- □ Customer and client privacy breaches
- □ Financial losses

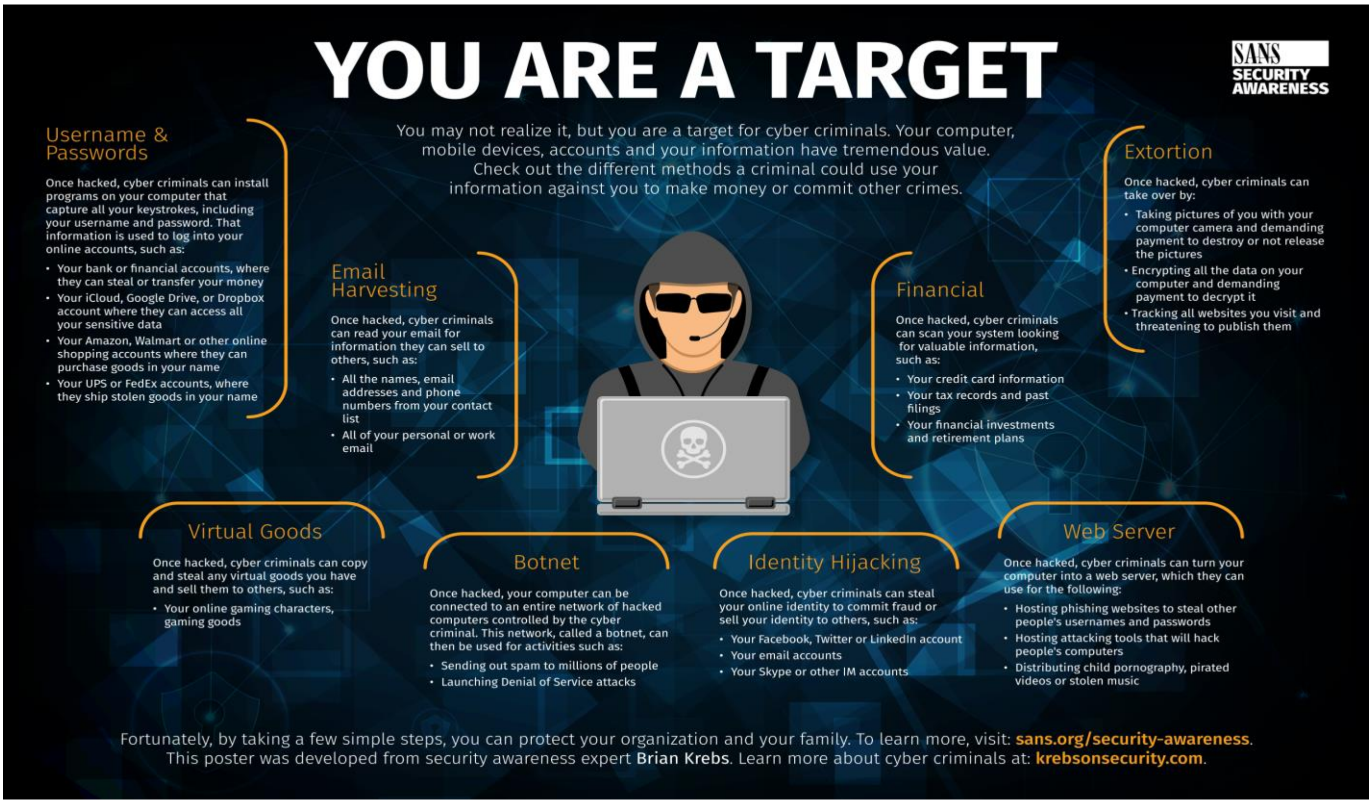
You Are A Target:

SMALL BUSINESS DIGITAL CHAMPIONS
AN AUSTRALIAN GOVERNMENT INITIATIVE

(ndp) National Disability Practitioners

NDS National Disability Services

This graphic was developed by security awareness expert Brian Krebs. When you review this presentation in your own time, take a moment to read in more detail how cyber criminals use your information across these key areas.



YOU ARE A TARGET

SANS SECURITY AWARENESS

You may not realize it, but you are a target for cyber criminals. Your computer, mobile devices, accounts and your information have tremendous value. Check out the different methods a criminal could use your information against you to make money or commit other crimes.

Username & Passwords

Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:

- Your bank or financial accounts, where they can steal or transfer your money
- Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data
- Your Amazon, Walmart or other online shopping accounts where they can purchase goods in your name
- Your UPS or FedEx accounts, where they ship stolen goods in your name

Email Harvesting

Once hacked, cyber criminals can read your email for information they can sell to others, such as:

- All the names, email addresses and phone numbers from your contact list
- All of your personal or work email

Financial

Once hacked, cyber criminals can scan your system looking for valuable information, such as:

- Your credit card information
- Your tax records and past filings
- Your financial investments and retirement plans

Extortion

Once hacked, cyber criminals can take over by:

- Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures
- Encrypting all the data on your computer and demanding payment to decrypt it
- Tracking all websites you visit and threatening to publish them

Virtual Goods

Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:

- Your online gaming characters, gaming goods

Botnet

Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:

- Sending out spam to millions of people
- Launching Denial of Service attacks

Identity Hijacking

Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:

- Your Facebook, Twitter or LinkedIn account
- Your email accounts
- Your Skype or other IM accounts

Web Server

Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:

- Hosting phishing websites to steal other people's usernames and passwords
- Hosting attacking tools that will hack people's computers
- Distributing child pornography, pirated videos or stolen music

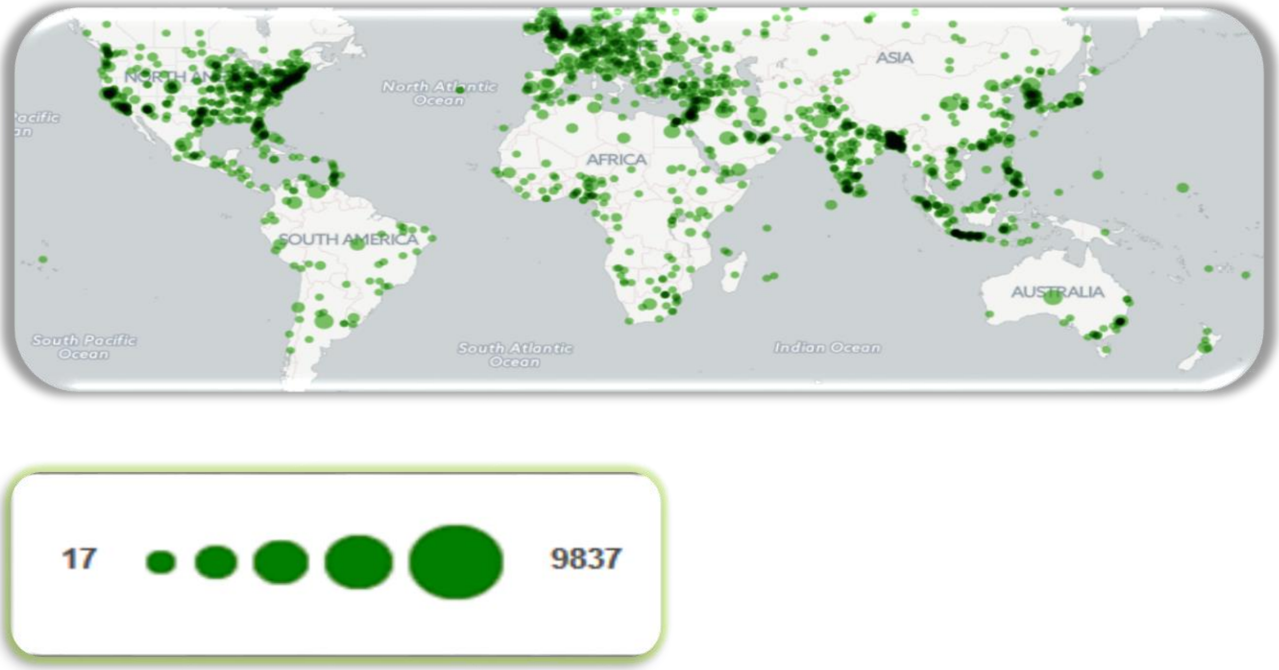
Fortunately, by taking a few simple steps, you can protect your organization and your family. To learn more, visit: **sans.org/security-awareness**.
This poster was developed from security awareness expert **Brian Krebs**. Learn more about cyber criminals at: **krebsonsecurity.com**.

It is important to also understand that hacking into work information can be done from a number of locations and devices:

The Social and Digital Touch Points

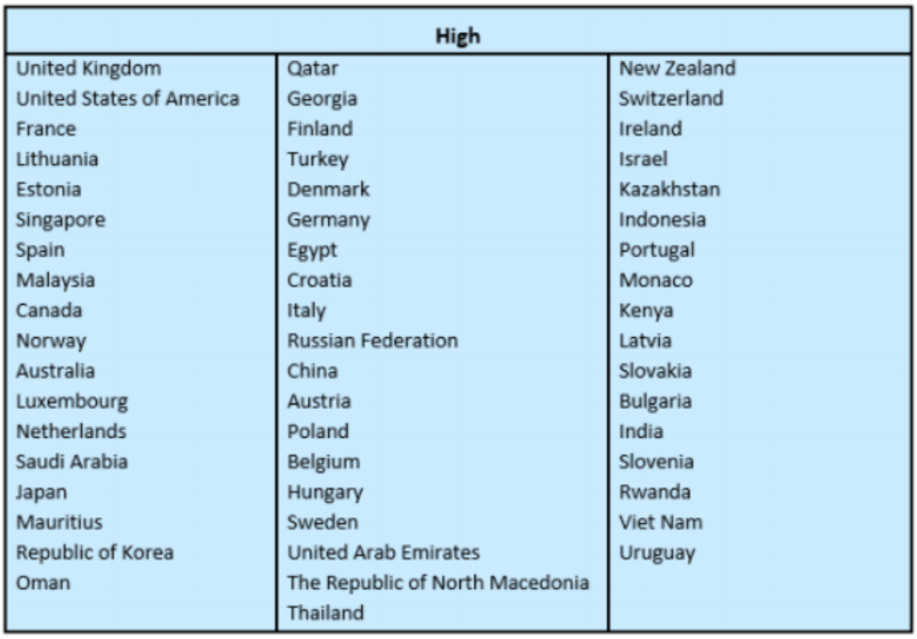
☼ ----- ☻	Home	Car	Office	Appointments	Shop	Office	Car	Home
Smartphone	√	√	√	√	√	√	√	√
Computer – Desktop	√		√			√		√
Tablet	√		√	√		√		√
TV – Interactive	√				√			√

Looking at the cyber-attacks across Australia in the last three months



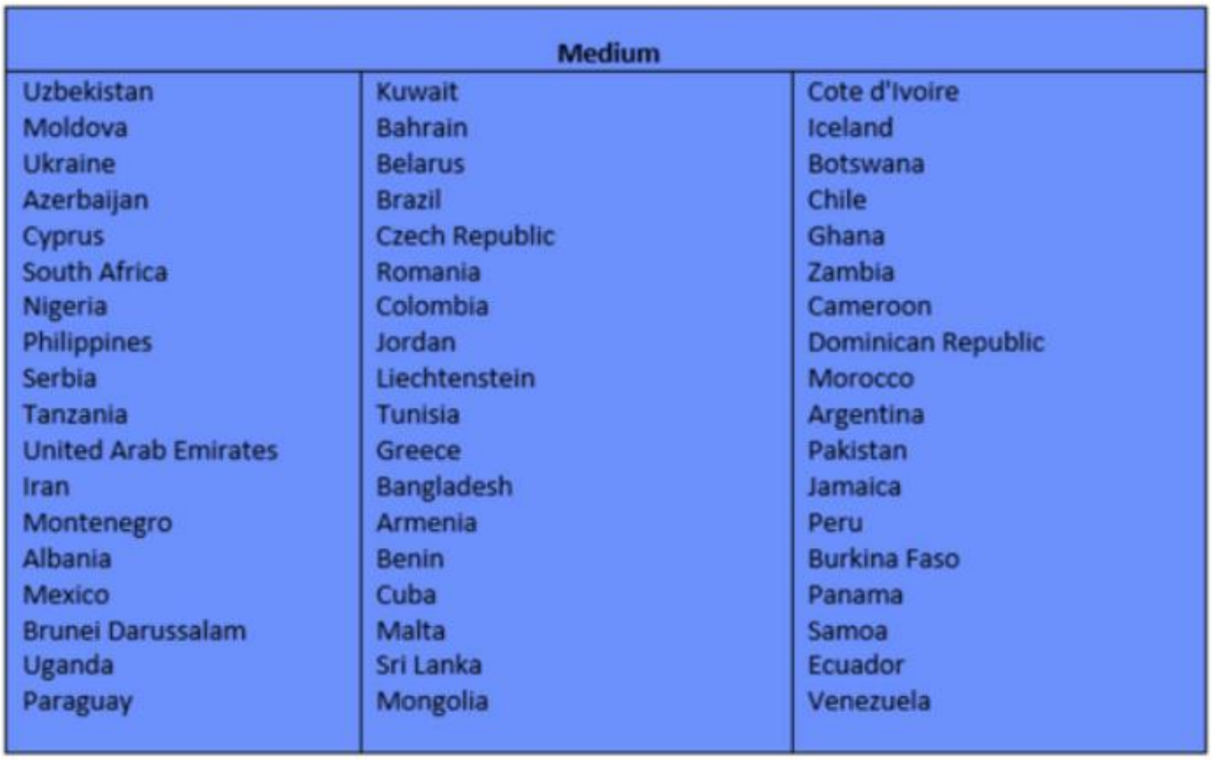
- □ Gen Y and Millennials are the least concerned about Cyber Security than any other demographic
- □ Australia has dropped from 2nd to 11th in the world in its ability to protect itself from cyber attacks

Countries with the best cybersecurity



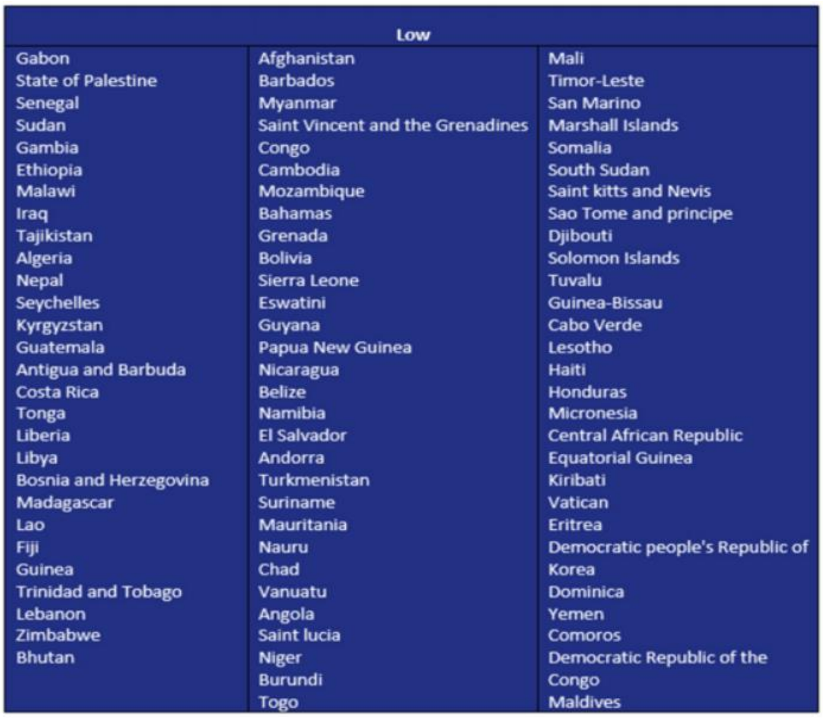
High		
United Kingdom	Qatar	New Zealand
United States of America	Georgia	Switzerland
France	Finland	Ireland
Lithuania	Turkey	Israel
Estonia	Denmark	Kazakhstan
Singapore	Germany	Indonesia
Spain	Egypt	Portugal
Malaysia	Croatia	Monaco
Canada	Italy	Kenya
Norway	Russian Federation	Latvia
Australia	China	Slovakia
Luxembourg	Austria	Bulgaria
Netherlands	Poland	India
Saudi Arabia	Belgium	Slovenia
Japan	Hungary	Rwanda
Mauritius	Sweden	Viet Nam
Republic of Korea	United Arab Emirates	Uruguay
Oman	The Republic of North Macedonia	
	Thailand	

Countries with some cybersecurity commitment



Medium		
Uzbekistan	Kuwait	Cote d'Ivoire
Moldova	Bahrain	Iceland
Ukraine	Belarus	Botswana
Azerbaijan	Brazil	Chile
Cyprus	Czech Republic	Ghana
South Africa	Romania	Zambia
Nigeria	Colombia	Cameroon
Philippines	Jordan	Dominican Republic
Serbia	Liechtenstein	Morocco
Tanzania	Tunisia	Argentina
United Arab Emirates	Greece	Pakistan
Iran	Bangladesh	Jamaica
Montenegro	Armenia	Peru
Albania	Benin	Burkina Faso
Mexico	Cuba	Panama
Brunei Darussalam	Malta	Samoa
Uganda	Sri Lanka	Ecuador
Paraguay	Mongolia	Venezuela

The worst countries - I'd like to point out that many popular Australia holiday destinations are on this list:



Low		
Gabon	Afghanistan	Mali
State of Palestine	Barbados	Timor-Leste
Senegal	Myanmar	San Marino
Sudan	Saint Vincent and the Grenadines	Marshall Islands
Gambia	Congo	Somalia
Ethiopia	Cambodia	South Sudan
Malawi	Mozambique	Saint kitts and Nevis
Iraq	Bahamas	Sao Tome and principe
Tajikistan	Grenada	Djibouti
Algeria	Bolivia	Solomon Islands
Nepal	Sierra Leone	Tuvalu
Seychelles	Eswatini	Guinea-Bissau
Kyrgyzstan	Guyana	Cabo Verde
Guatemala	Papua New Guinea	Lesotho
Antigua and Barbuda	Nicaragua	Haiti
Costa Rica	Belize	Honduras
Tonga	Namibia	Micronesia
Liberia	El Salvador	Central African Republic
Libya	Andorra	Equatorial Guinea
Bosnia and Herzegovina	Turkmenistan	Kiribati
Madagascar	Suriname	Vatican
Lao	Mauritania	Eritrea
Fiji	Nauru	Democratic people's Republic of Korea
Guinea	Chad	Dominica
Trinidad and Tobago	Vanuatu	Yemen
Lebanon	Angola	Comoros
Zimbabwe	Saint lucia	Democratic Republic of the Congo
Bhutan	Niger	Maldives
	Burundi	
	Togo	

Where are your points of vulnerability?

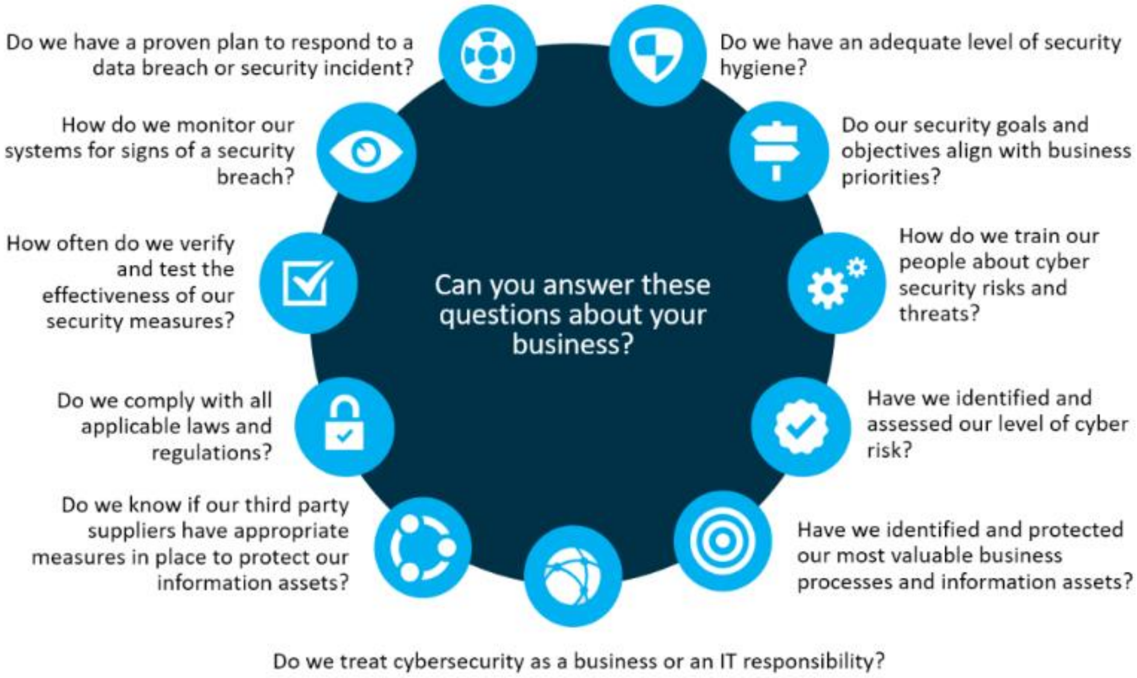
- ❑ **Website plugins** (a piece of software that acts as an add-on to a web browser and gives the browser additional functionality)
- ❑ **Website themes** (The templates that give your website it's look and functionality – created in programs like WordPress etc.)
- ❑ **Core databases**
- ❑ **Hosting or web server**
- ❑ **File permissions**
- ❑ **Password theft**
- ❑ **Brute force** (robo-systematic programed attacks)
- ❑ **Internal hack**
- ❑ **Your people!**

SMALL BUSINESS DIGITAL CHAMPIONS
AN AUSTRALIAN GOVERNMENT INITIATIVE

(ndp) National Disability Practitioners

NDS National Disability Services

Manage your Risk



Can you answer these questions about your business?

Do we have a proven plan to respond to a data breach or security incident?

How do we monitor our systems for signs of a security breach?

How often do we verify and test the effectiveness of our security measures?

Do we comply with all applicable laws and regulations?

Do we know if our third party suppliers have appropriate measures in place to protect our information assets?

Do we have an adequate level of security hygiene?

Do our security goals and objectives align with business priorities?

How do we train our people about cyber security risks and threats?

Have we identified and assessed our level of cyber risk?

Have we identified and protected our most valuable business processes and information assets?

Do we treat cybersecurity as a business or an IT responsibility?

Check for account details having been stolen: https://haveibeenpwned.com/

Password strength checks: https://haveibeenpwned.com/Passwords

: https://passwordsecurity.info/

Gibson Research Password tool and info: https://www.grc.com/haystack.htm

Password Managers:

LastPass https://lastpass.com 1Password https://1password.com Dashlane https://dashlane.com

Multi factor authentication
1234
****
Something you are
Something you have
Something you know

Backups: One of the largest loss of information is the lack of appropriate backup policy and procedures.

3 Copies
2 Media
1 Off-site

Minimum Recommendations:

□ Create and maintain a Password policy for your company
□ Disable unused themes and plugins on your website
□ Use a password manager and Multi-Factor-Authorisation or 2FA
□ Lock your PC when absent from it
□ Never ever use WEP security for WiFi (older unprotected public WiFi) – use WPA 2 (currently)
□ Whenever an employee leaves change your business WiFi access password(s)
□ Ensure employees are educated about Phising, spear phishing and BEC attacks
□ Employ the 3-2-1 strategy for backups. Ideally use a Network Attached Storage (NAS) device to utilise its automation features.

Breach Information:

https://www.webberinsurance.com.au/data-breaches-list

Resources:

Small Business Digital Champions online hub

www.ndp.org.au/learning-hub/small-business-digital-champions-project.

The hub will house all information related to the project, including fact sheets, webinars, online courses and more. Individuals can register to receive a monthly e-newsletter to keep undated on new resources.

SMALL BUSINESS DIGITAL CHAMPIONS

AN AUSTRALIAN GOVERNMENT INITIATIVE

(ndp) National Disability Practitioners

NDS National Disability Services