The new era of WFH:

Staying Cyber Secure

Insane Technologies and CFC Underwriting Ltd.

April 2020

cfc

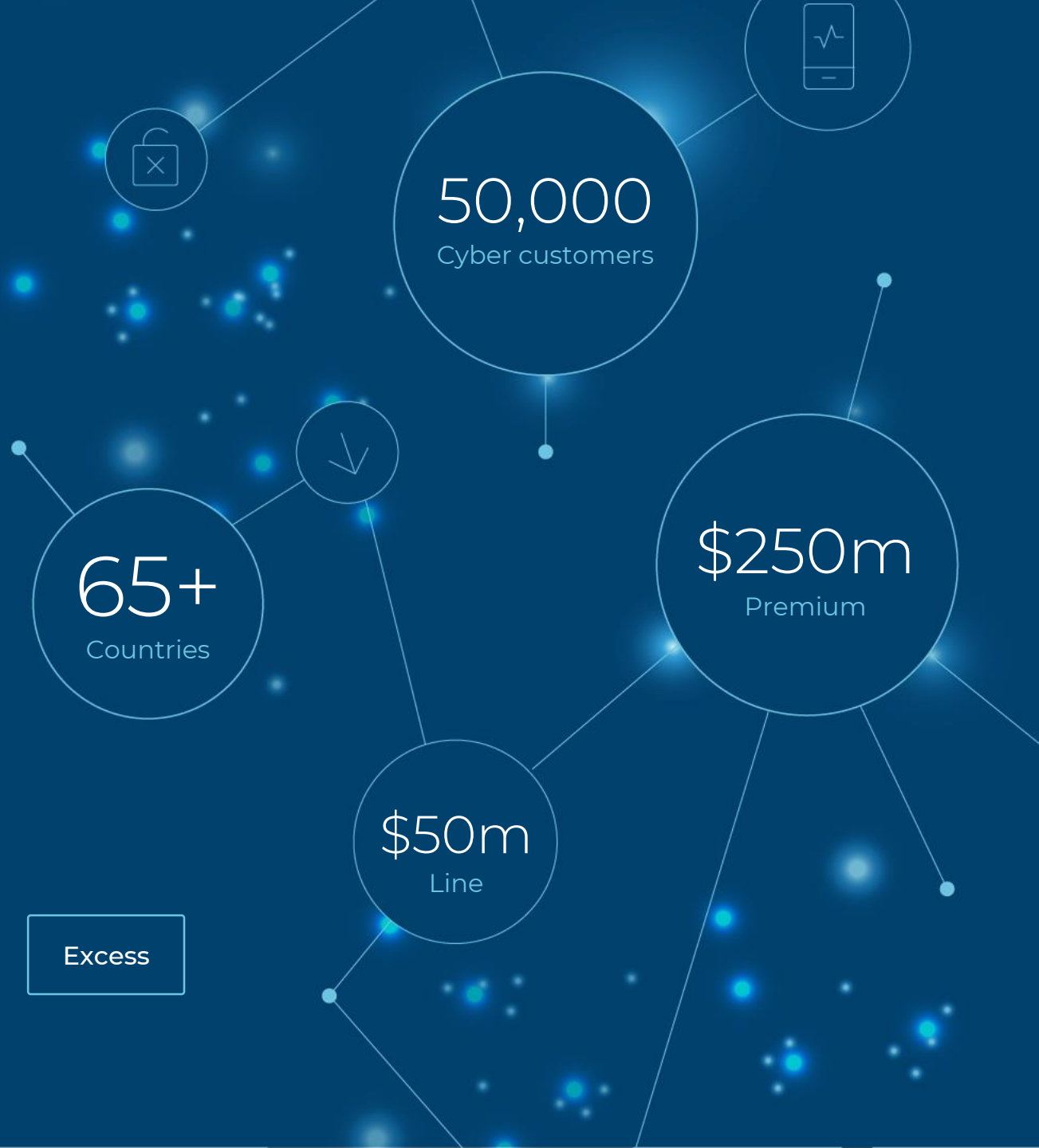
@insane technologies
DATA PROTECTION SPECIALISTS

cfc | Cyber

Pioneers in cyber insurance

With 20 years' experience in cyber insurance, CFC was one of the first companies to offer cyber insurance and has one of the largest cyber underwriting teams in the world. Our award-winning cyber insurance products are trusted by over 50,000 **businesses** in more than **65 countries**.

CFC's dedicated in-house cyber incident response team is backed by a panel of expert global response partners and operates the world's first cyber incident response app.



Our cyber products

- Private enterprise
- Large corporate
- Healthcare
- Excess

*Cyber cover is also offered as standard on most CFC policies

Cyber risk

70% of Australian businesses are aware that cyber exposures are a risk

10% of businesses currently buy cyber insurance cover

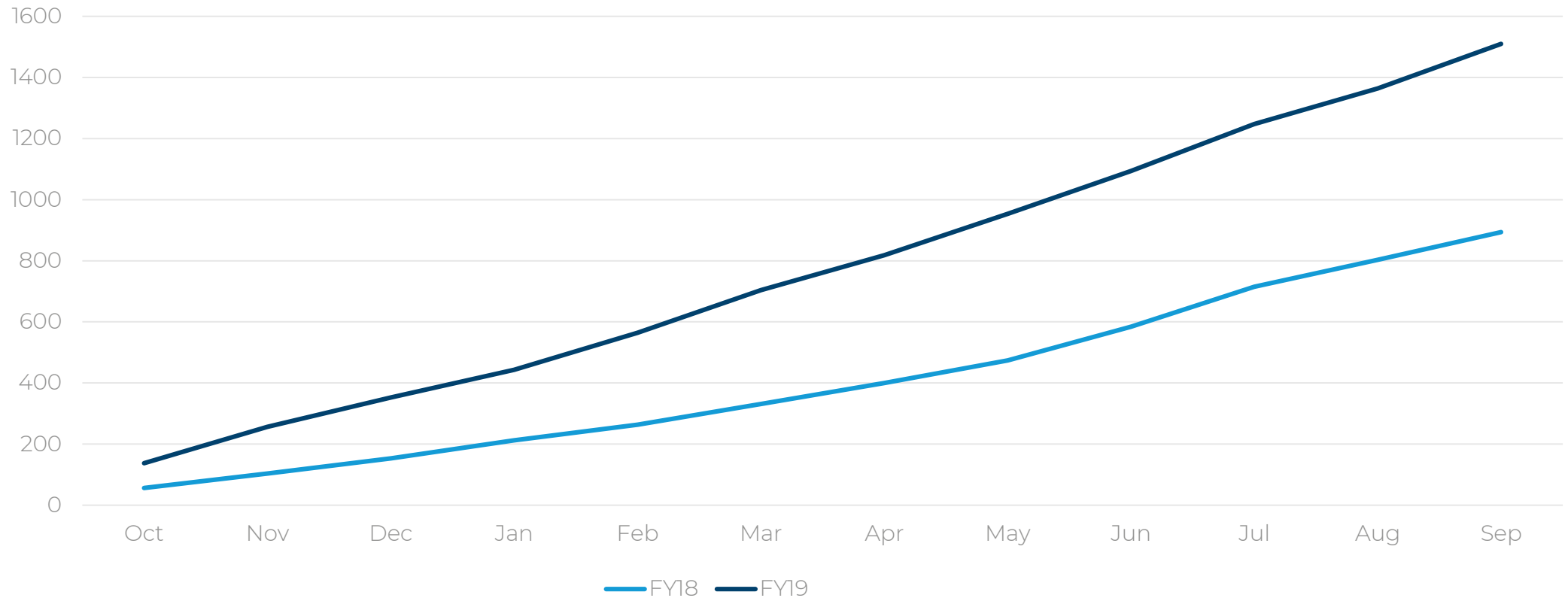
$7.5bn is the estimated size of the global cyber insurance market (AUD)

80% Proportion of that premium that currently comes from US domiciled businesses

Cyber claims update

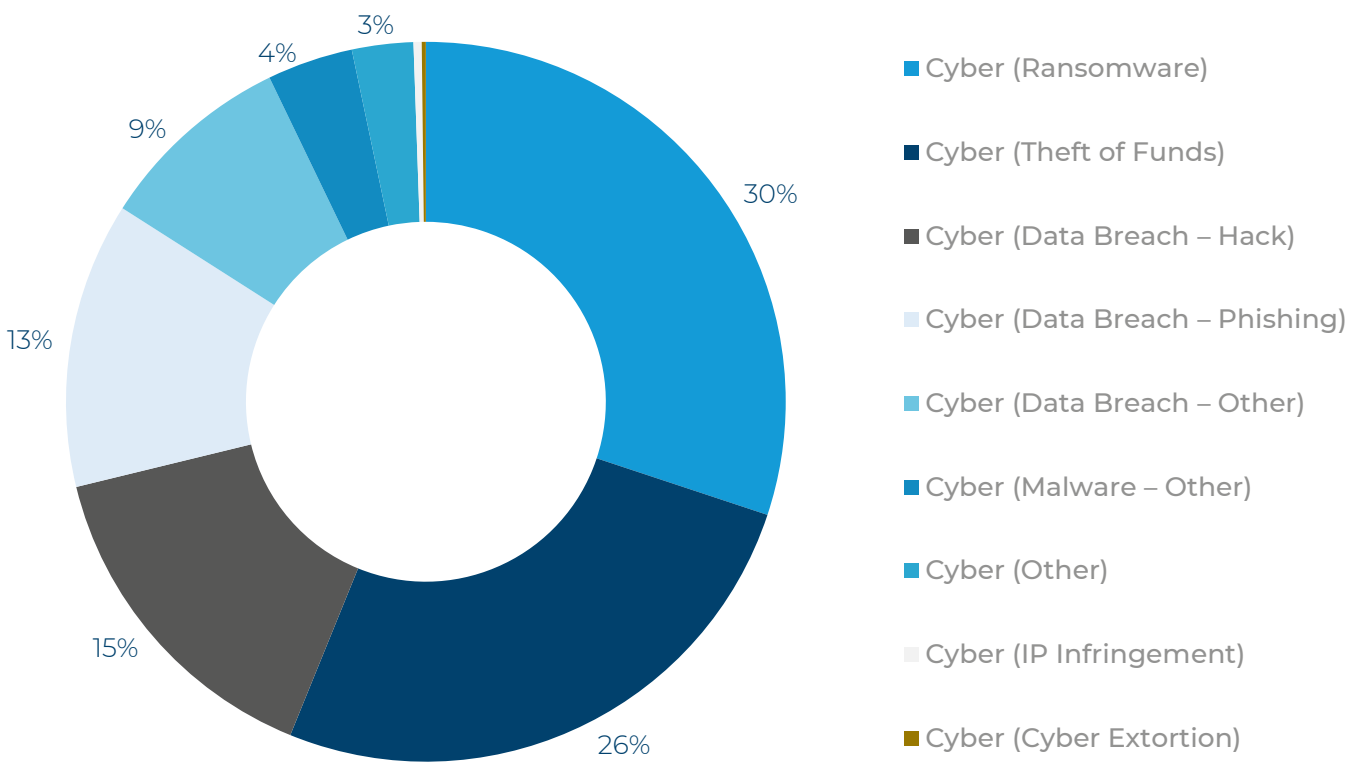
Cyber claims volume is up significantly on last year

Cyber claims volume TY v LY

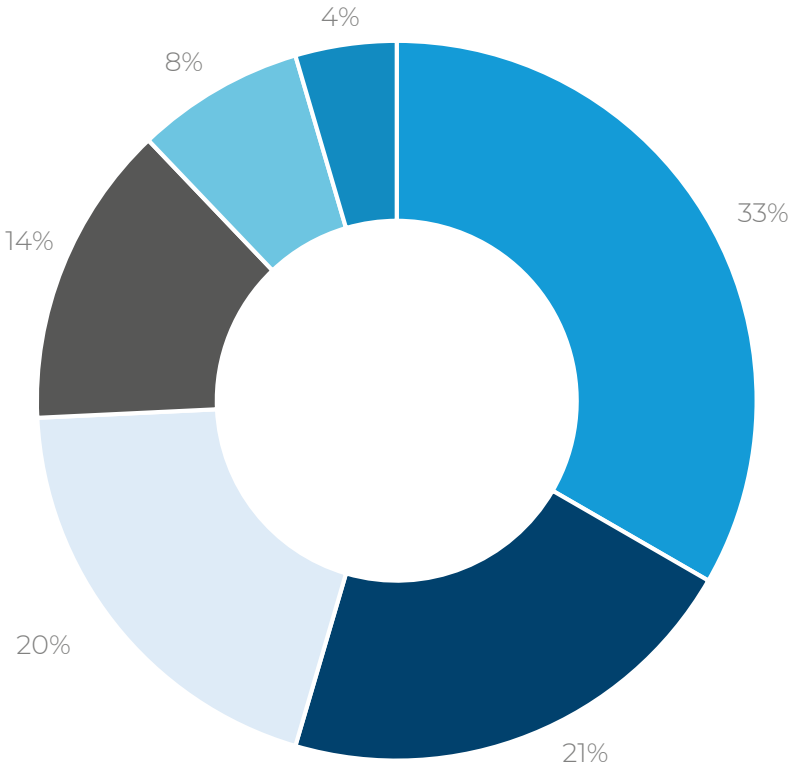


Cyber claims (by count)

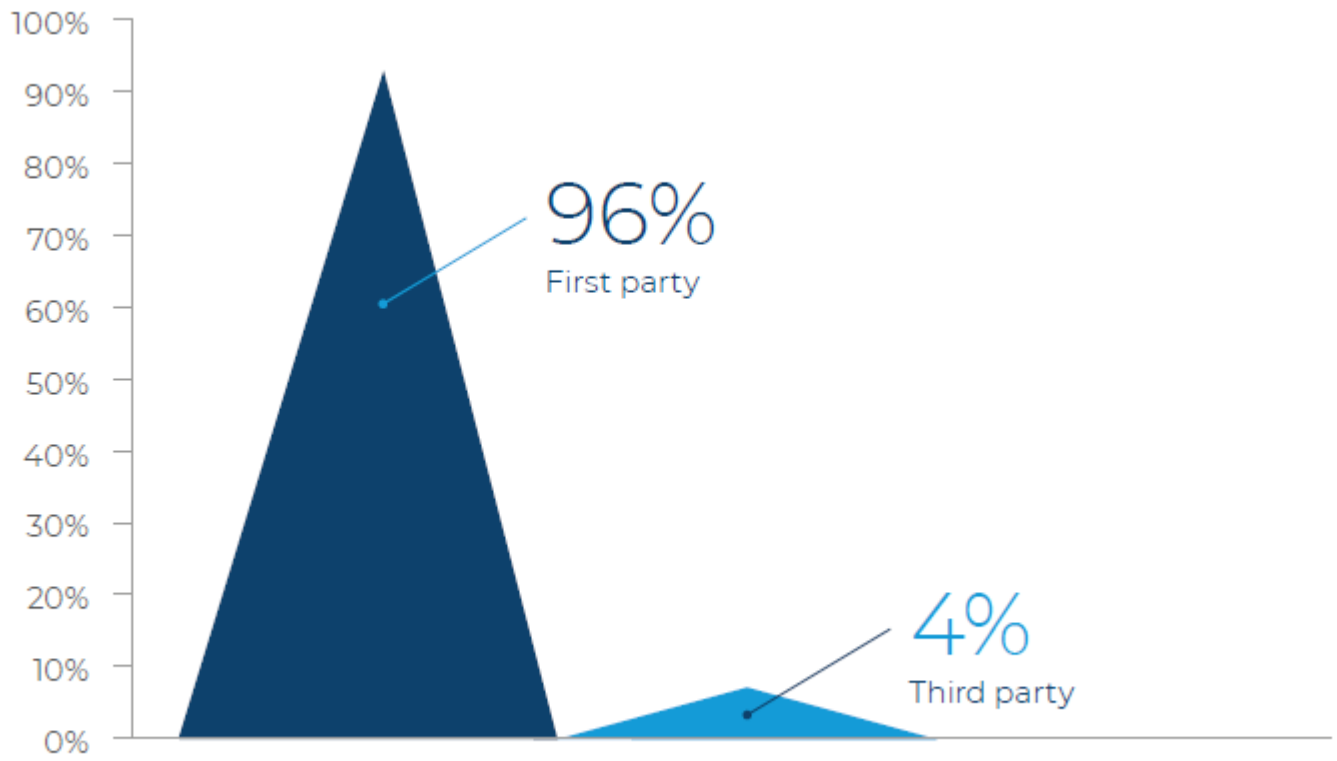
All Countries



Australia only



First party v. third party claims

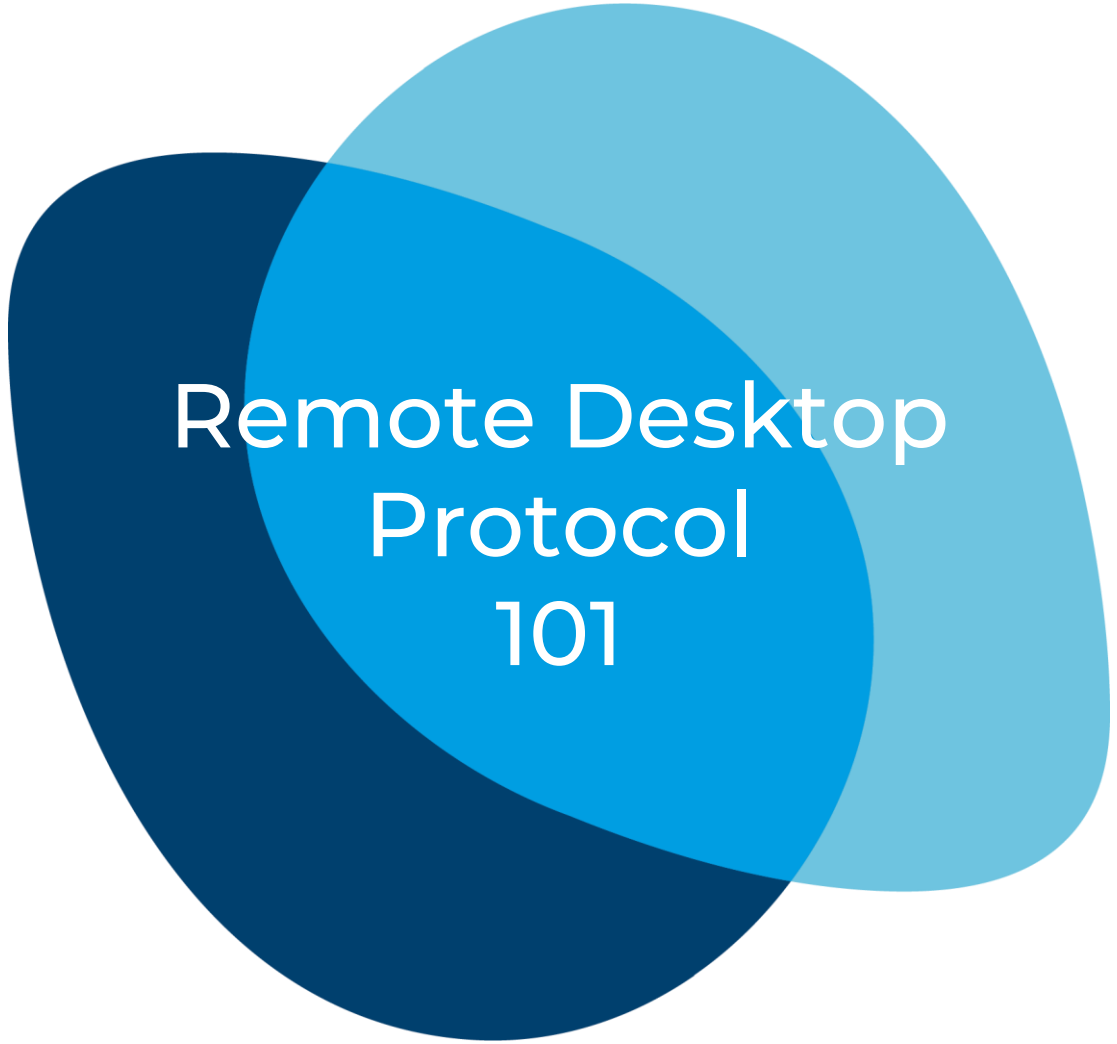


CFC Underwriting cyber claims statistics, 2018

Insane Technologies

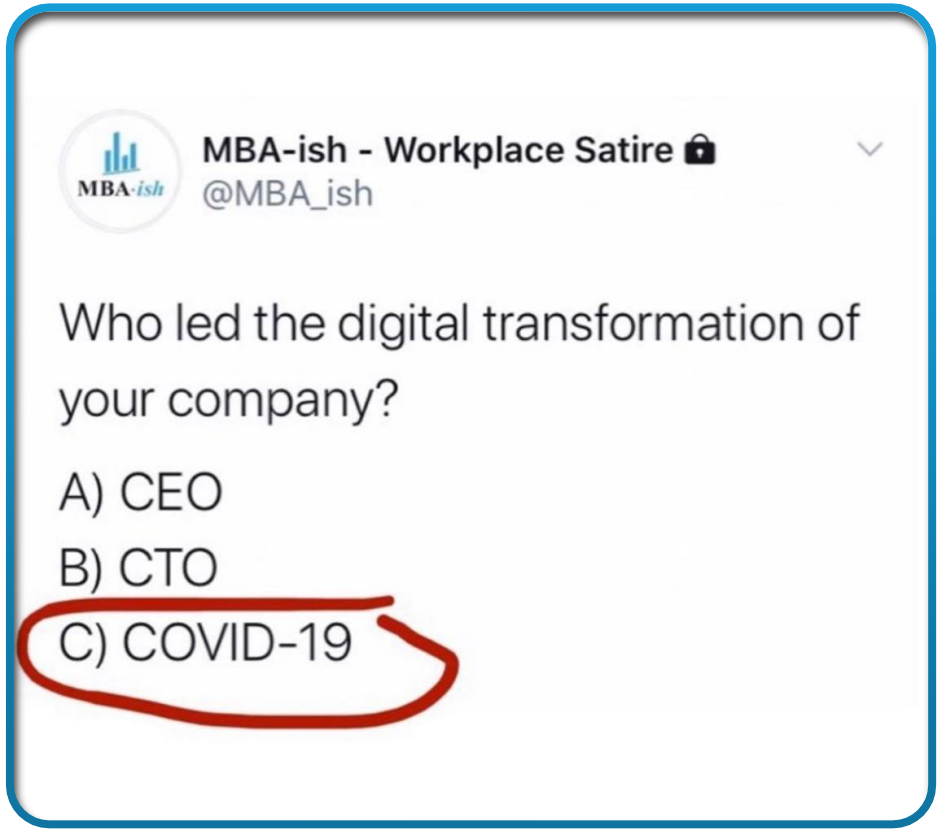
- Award winning company **Founded in 2000** by David Rudduck
- **Working with** CFC Underwriting since 2018 as a **primary Cyber Incident Response partner** for Australia
- **Incident Response**, **Digital Forensics** and **eDiscovery** to victims of cyber-incidents through their insurance programme
- Certified Security Professional (ACS), CISSP, GCFE and GCFA qualified.

cfc


Remote Desktop
Protocol
101

Remote Desktop Protocol 101

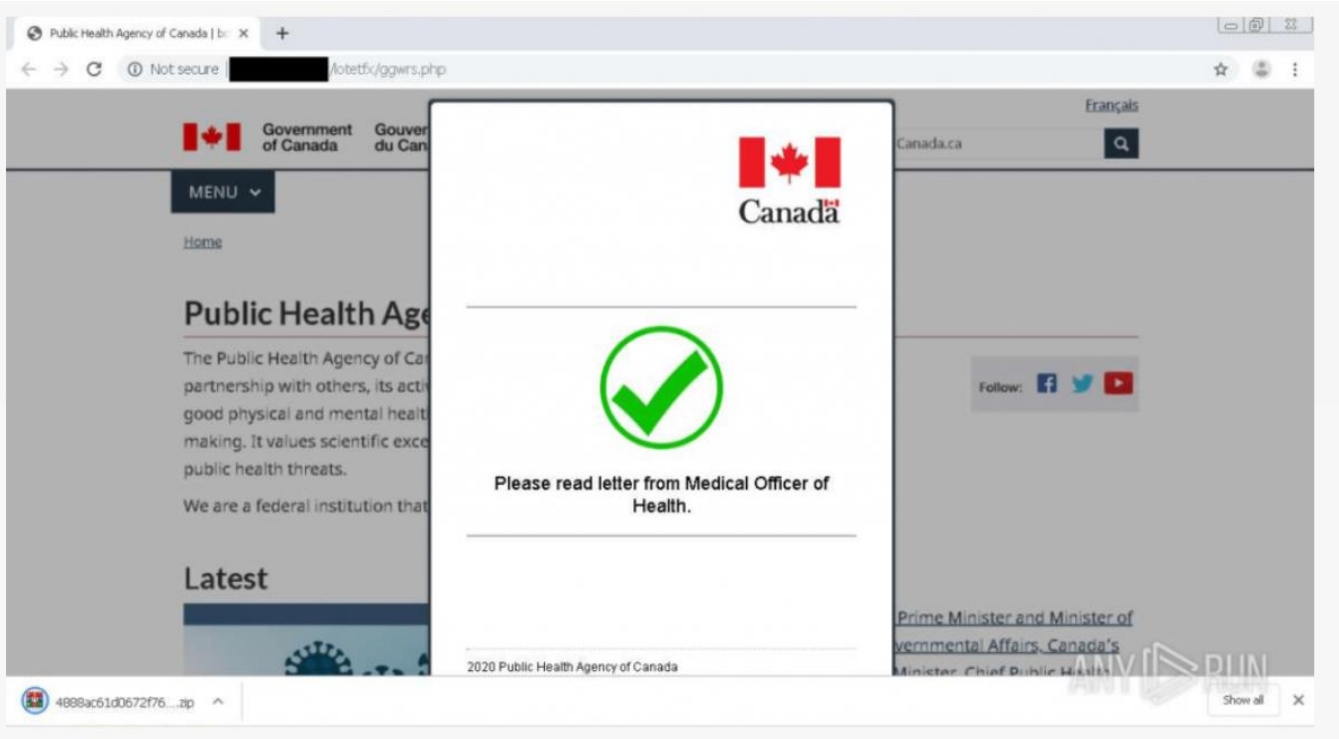
- VPN – Virtual Private Network. Allows companies to secure connections to other networks over the Internet.
- Pros and cons of using RDP or VPN
- The current **most common cause of a Ransomware incident is compromise of remote access via Remote Desktop Protocol (RDP)**.
- What does that mean during COVID-19?



Top Five: COVID-19

1. Posing as government agencies

- The website directs victims to download a file: “Please read letter from Medical Officer of Health”



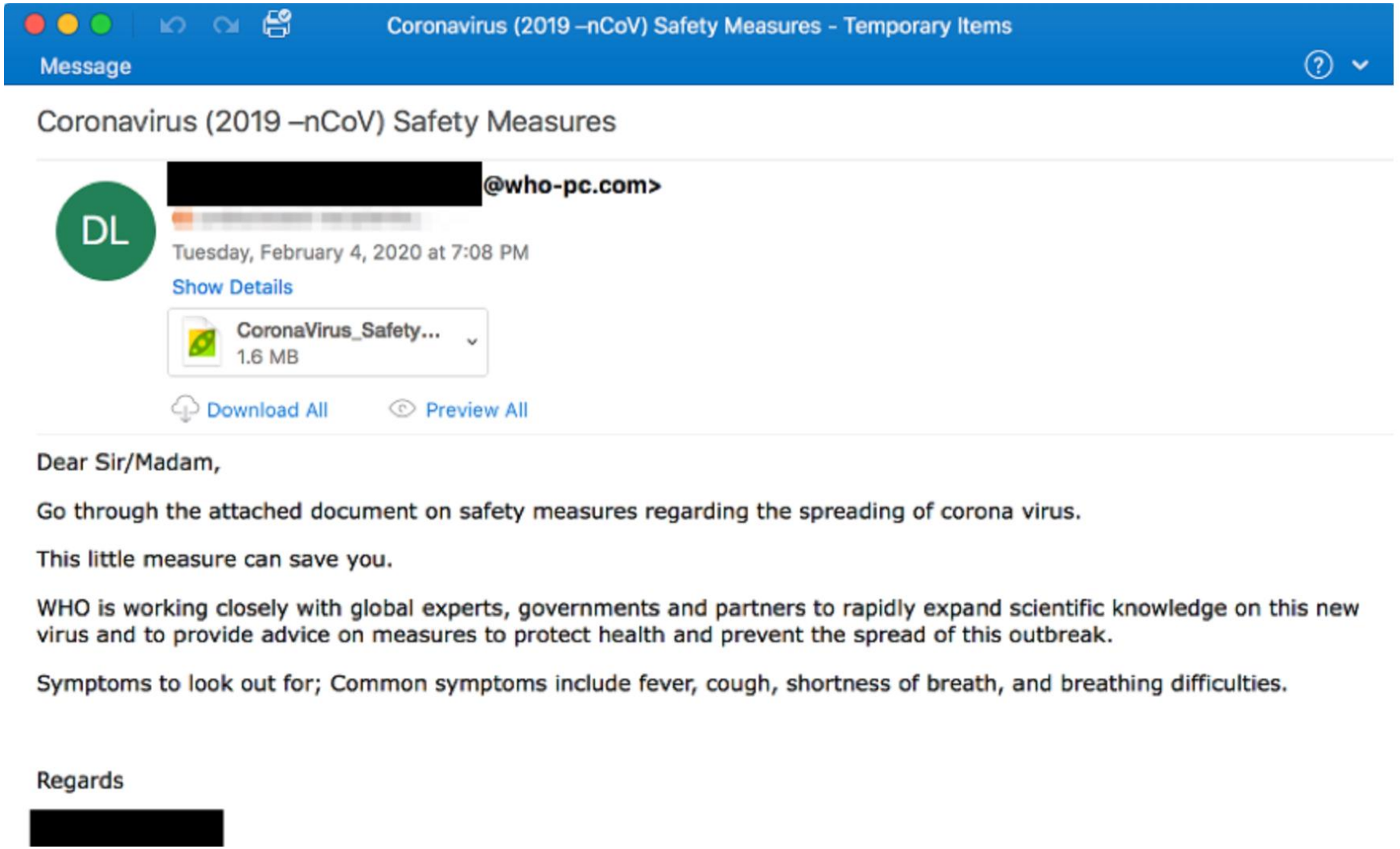
Case Study:
Remote Access Hacked

- Gold Coast based Property Manager
- Threat actor got into computers via “Remote Access”
- Ransomware run on 6x computers
- 1 BTC (AUD$10,000 at the time) per computer to decrypt
- No working backups
- Looking at $60,000 to recover business
- Security researcher was able to decrypt - $7,500 in IR fees

2. Targeting food delivery – credential stuffing

source: Lieferando

3. Playing on human vulnerabilities



Coronavirus (2019 –nCoV) Safety Measures - Temporary Items

Message

Coronavirus (2019 –nCoV) Safety Measures

DL [redacted]@who-pc.com>

Tuesday, February 4, 2020 at 7:08 PM

Show Details

CoronaVirus_Safety...
1.6 MB

Download All Preview All

Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of corona virus.

This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

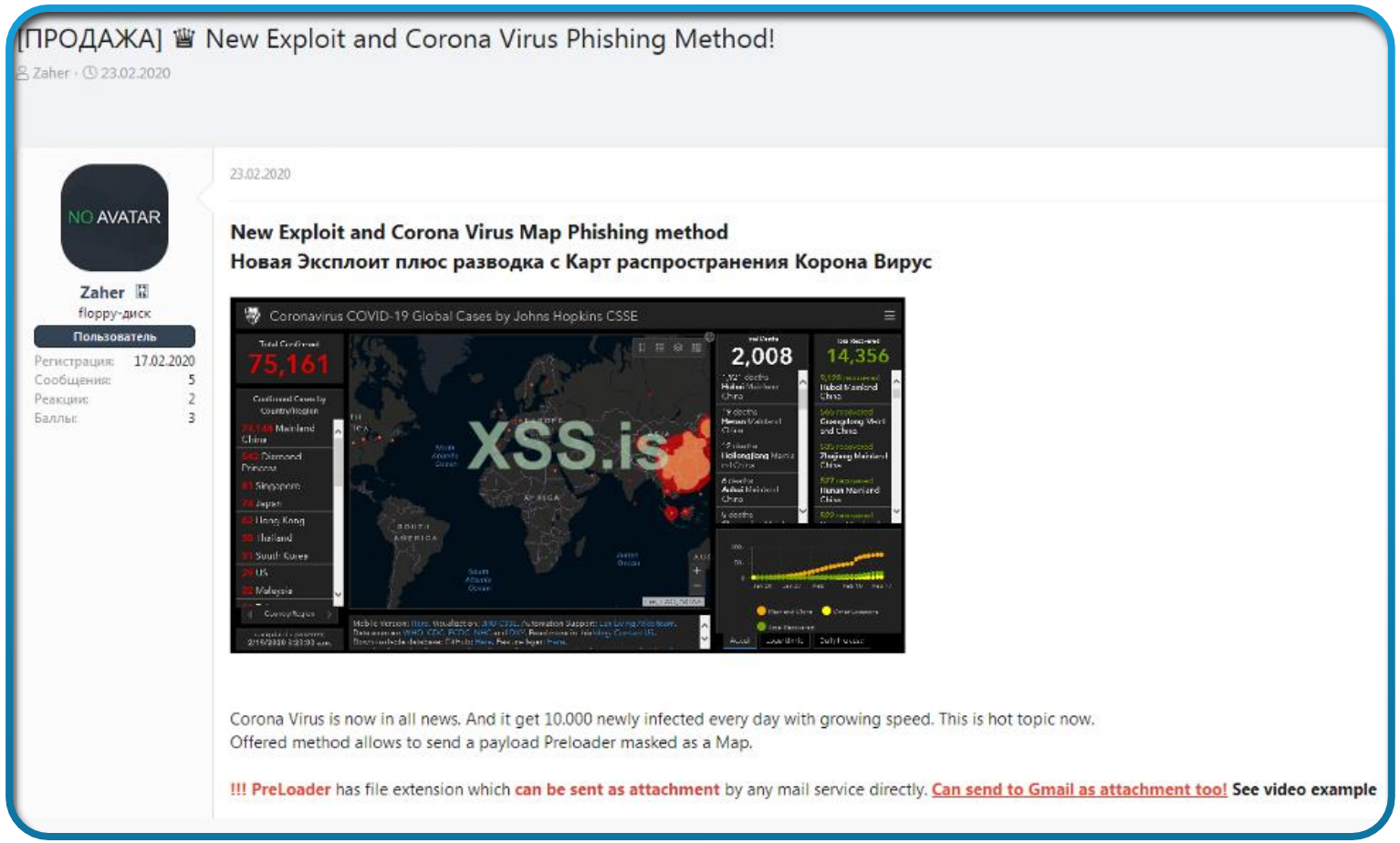
Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

[redacted]

cfc

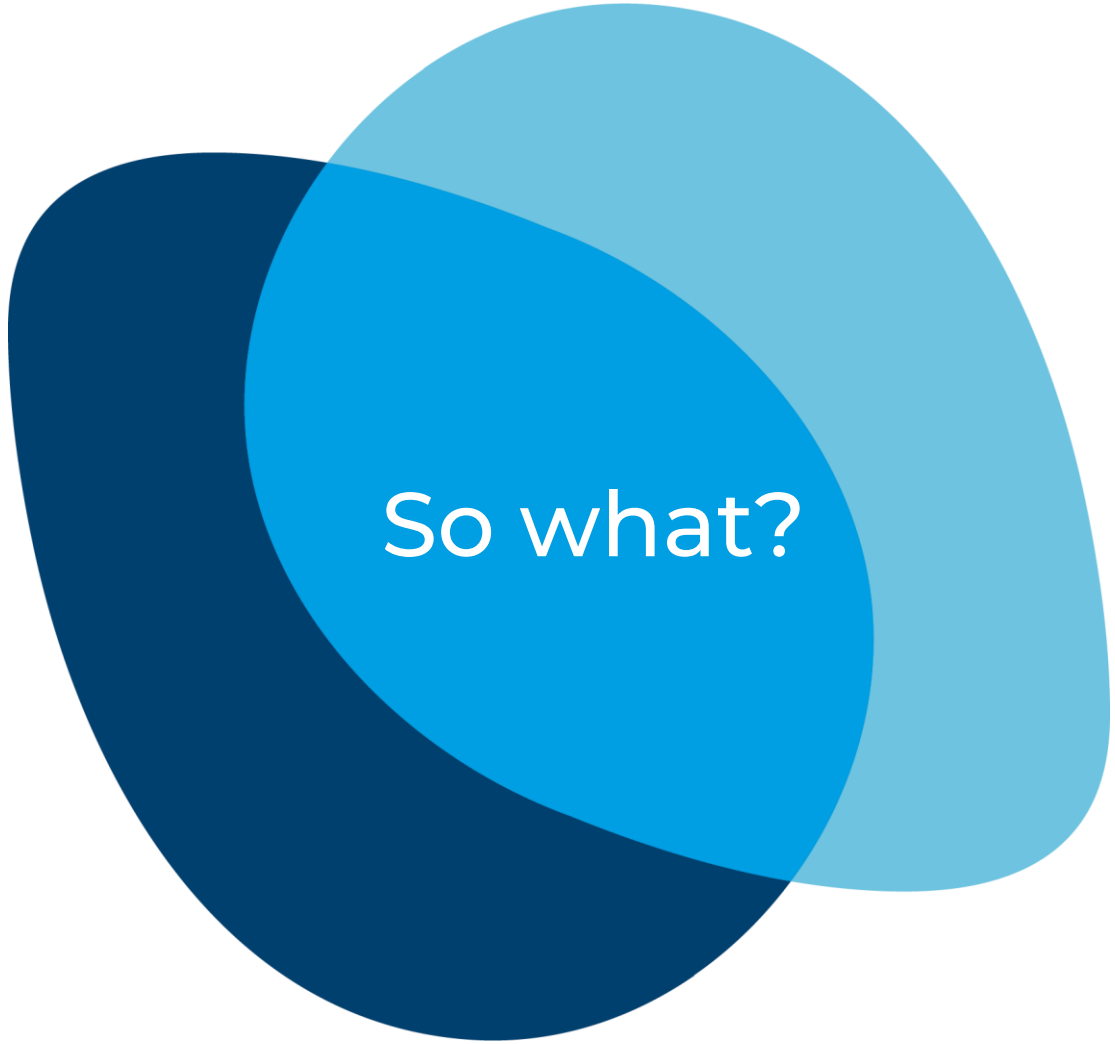
4. Creating malicious COVID-19 maps



5. BEC Scams

- Private school in NSW
- Email account of finance person hacked
- Threat actor sat in mailbox & monitored correspondence
- Finance person liaising with overseas investor
- Threat actor interjected on communications
- Finance person went to pay investor his shares
- $600,000 wired to the wrong account

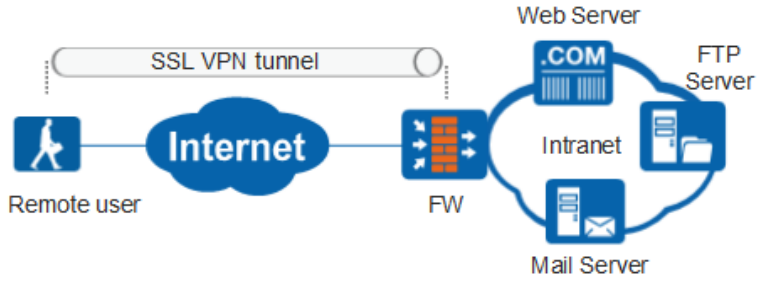
cfc


So what?

Personal Devices

Multi-Factor Authentication
Google Authenticator
Microsoft Authenticator
LastPass Authenticator

Password Manager
1Password.com
LastPass.com



SSL VPN
Remote Access

cfc

Employee Training

DO:

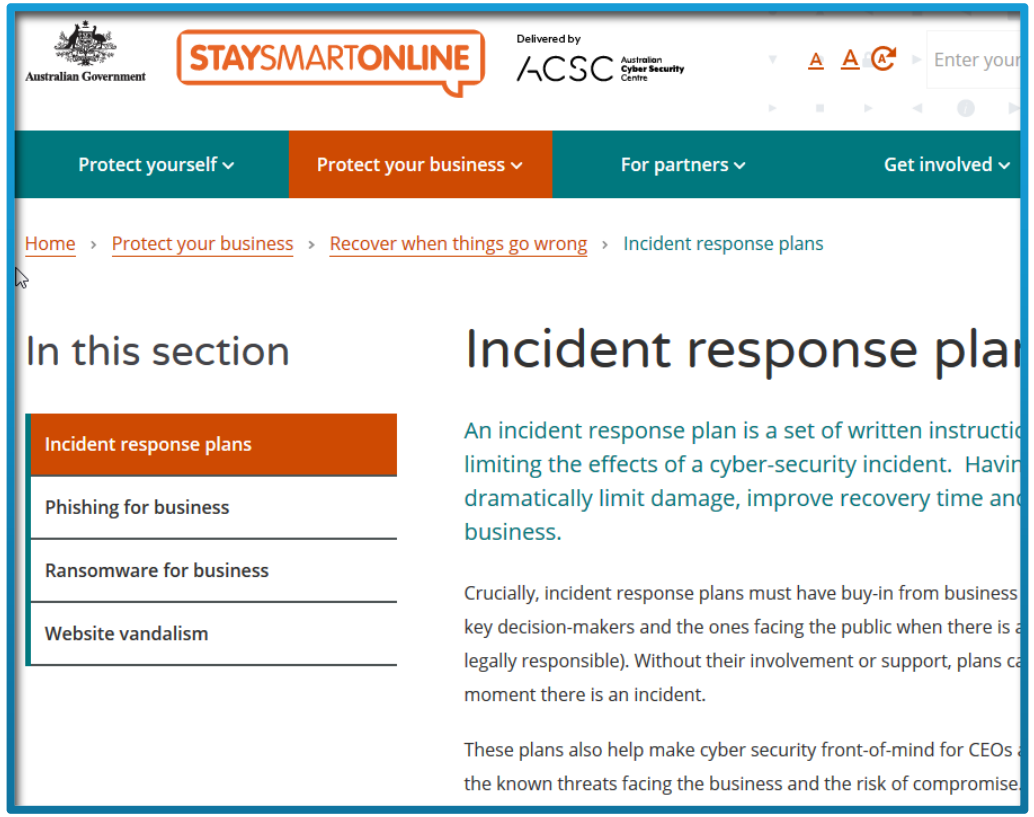
- Ongoing security training for all remote workers
- Monitoring employees the right way
- Check all of your devices for software or firmware updates
- Use a unique password for every online login

DO NOT:

- Don’t click suspicious links
- Don’t download attachments from unknown or untrusted sources
- Do not “Enable Content” in unknown Word documents
- Be careful not to share login credentials with unknown or suspicious providers (there is NEVER a legitimate reason for a third-party to require your login credentials)

cfc

Preparedness



Incident Response Planning

- Update Corporate policies
  - Include plans for digital assets due to system failure or cyber events
- Know who in the company actually needs VPN access
- Test out incident response plan ahead of time – tabletop exercise
- Cyber insurance!

Client questions

What are their challenges?

- Were you able to switch to working remotely with minimum disruption?
  - Or, are you having to implement methods to access the office remotely?
- Are most software and services being used cloud based?
- What devices are staff using to access company resources?
- Do you still have any legacy systems in your office?
  - Who is keeping an eye on them?
  - Is someone testing back-ups monthly?

cfc

cyber@cfcunderwriting.com