14 NOVEMBER 2024

Unlock the Full Potential of Your Cyber Policy

Speakers

Gow-Gates

INSURANCE BROKERS

cfc

Marie D’Have

Team Manager, Executive and Professional Risks

As Team Manager of Gow-Gates' Executive and Professional Risks team, Marie oversees key Financial Lines for the Corporate and Risk Solutions division, ensuring comprehensive coverage and risk management strategies for clients. Marie brings a strong legal and insurance background, having spent six years as a qualified lawyer in Belgium before transitioning to the Financial Lines team at Marsh in Belgium and subsequently in Australia.

Simon Goodall

Cyber Incident Manager

With over 20 years of experience in the IT industry, Simon is a seasoned professional recognised for his extensive expertise in cybersecurity and incident response. Throughout Simon's career, he has taken lead on over 200 ransomware incidents, demonstrating exceptional proficiency in high-pressure situations. Known for his strategic approach, Simon combines technical acumen with a commitment to continuous learning and improvement, making him a highly sought-after speaker and consultant in the cybersecurity field.

Agenda

- CFC overview
- Why does my business need proactive cyber insurance?
- How does CFC proactively protect our customers?
- How does CFC Response help our customers?
- Questions?

Your **cyber team**

> CFC has been trading cyber in Australia for over two decades. We pride ourselves on our extensive experience in cyber underwriting and our world-class teams.

Underwriting

+12

Andy Hall
Cyber Practice Leader

Philippa Davis
Cyber Team Leader

Claims

+20

Ash Burdon
Cyber Claims Manager

Hayfa Riaz
Cyber Claims Team Leader

Incident Response & Proactive Cyber

+140

Jason Hart
Global Head of Proactive & Response

David Rudduck
CEO, CFC Response AU

Conor Naughton
DFIR Technical Lead

Simon Goodall
Cyber Incident Manager

Callan Orgill
Cyber Incident Manager

Why does my business need **proactive cyber insurance?**

Business Email Compromise

Protect your business and employees from phishing attacks designed to steal your money, goods or information.

How does Business Email Compromise (BEC) work?

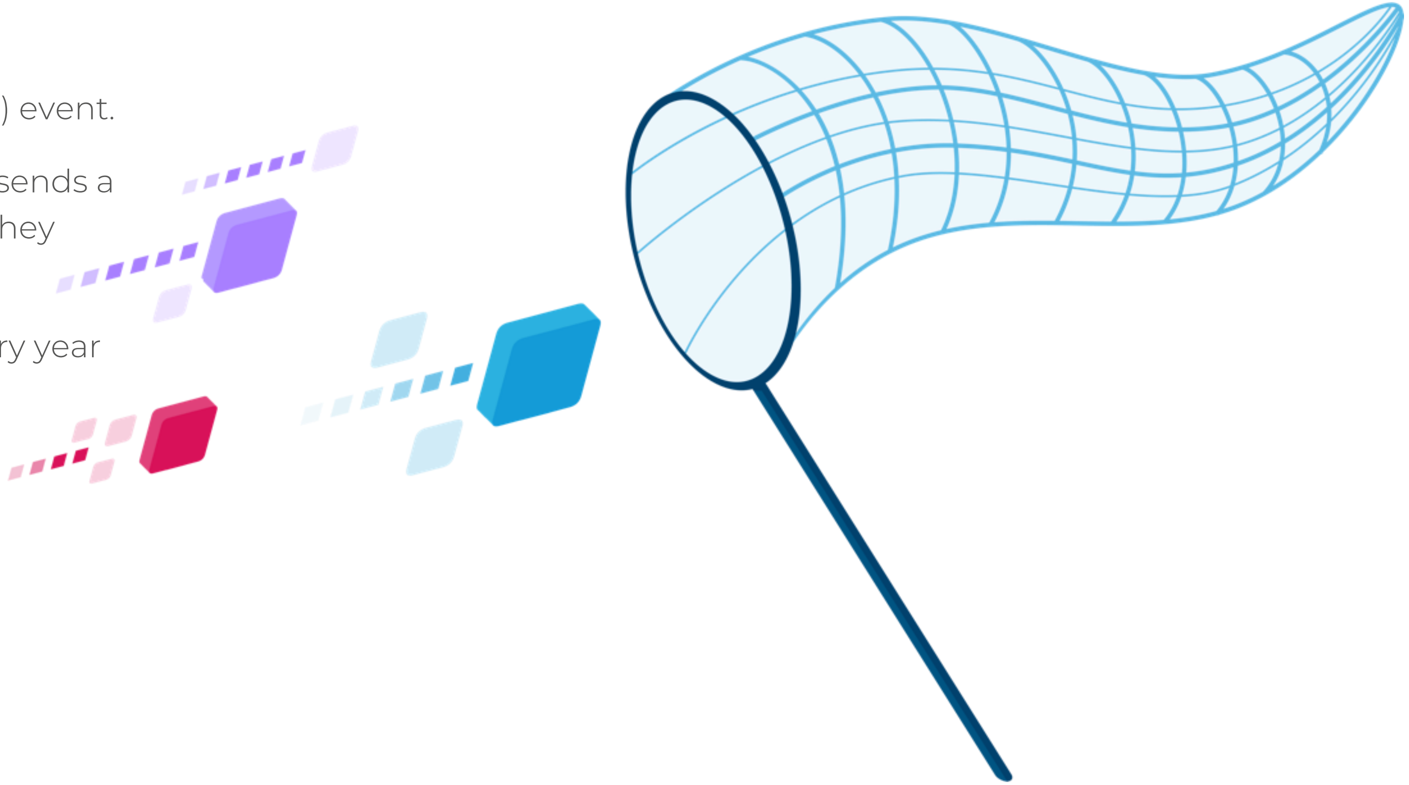
- Incident is usually triggered as a result of a targeted phishing or spear phishing attack.
- Threat actor gains access to a corporate mailbox and is able to leverage the identify and trust of the mailbox owner.
- Often the precursor to a Funds Transfer Fraud (FTF) event and may lead to a Data Breach event.

Funds Transfer Fraud

FTF, which is also known as Wire Transfer Fraud, is one of the most financially damaging cyber incidents as it usually involves a significant amount of money lost.

How does Funds Transfer Fraud (FTF) work?

- Usually follows a Business Email Compromise (BEC) event.
- Scammer impersonates a legitimate business and sends a request for money to be paid into a bank account they have access to.
- Hundreds of millions of dollars in funds are lost every year due to this type of scam.



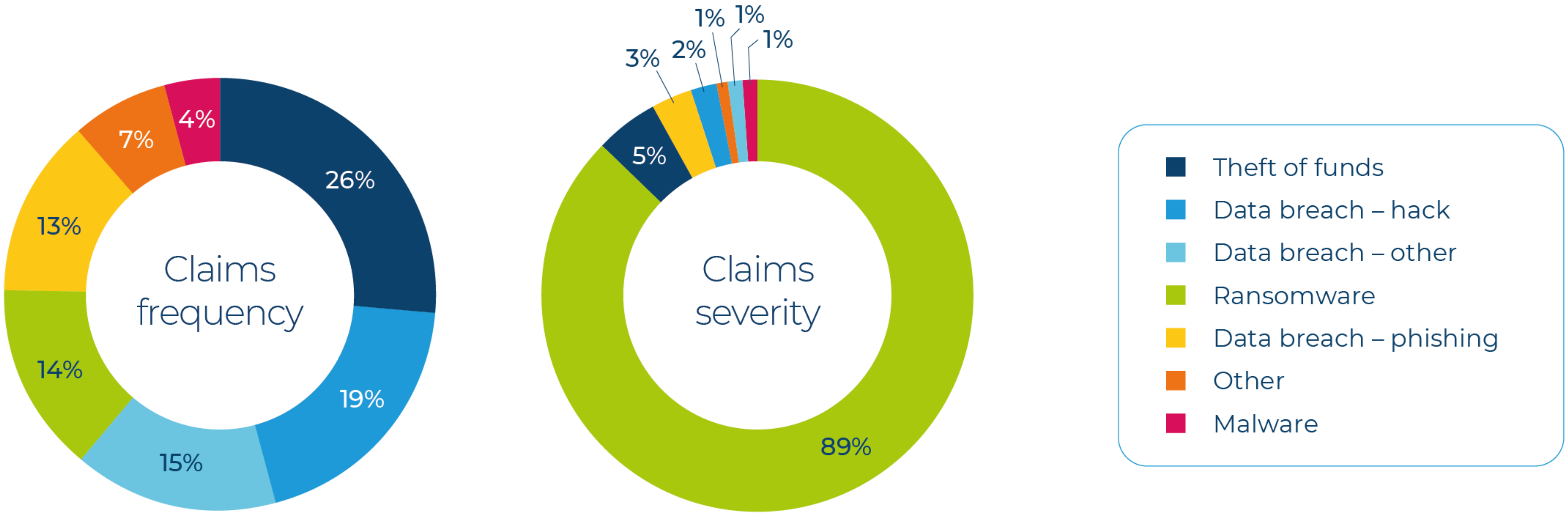
Ransomware

Ransomware is the most commonly publicised cyber incidents, mainly because these types of events typically stop a business in their tracks.

How does Ransomware work?

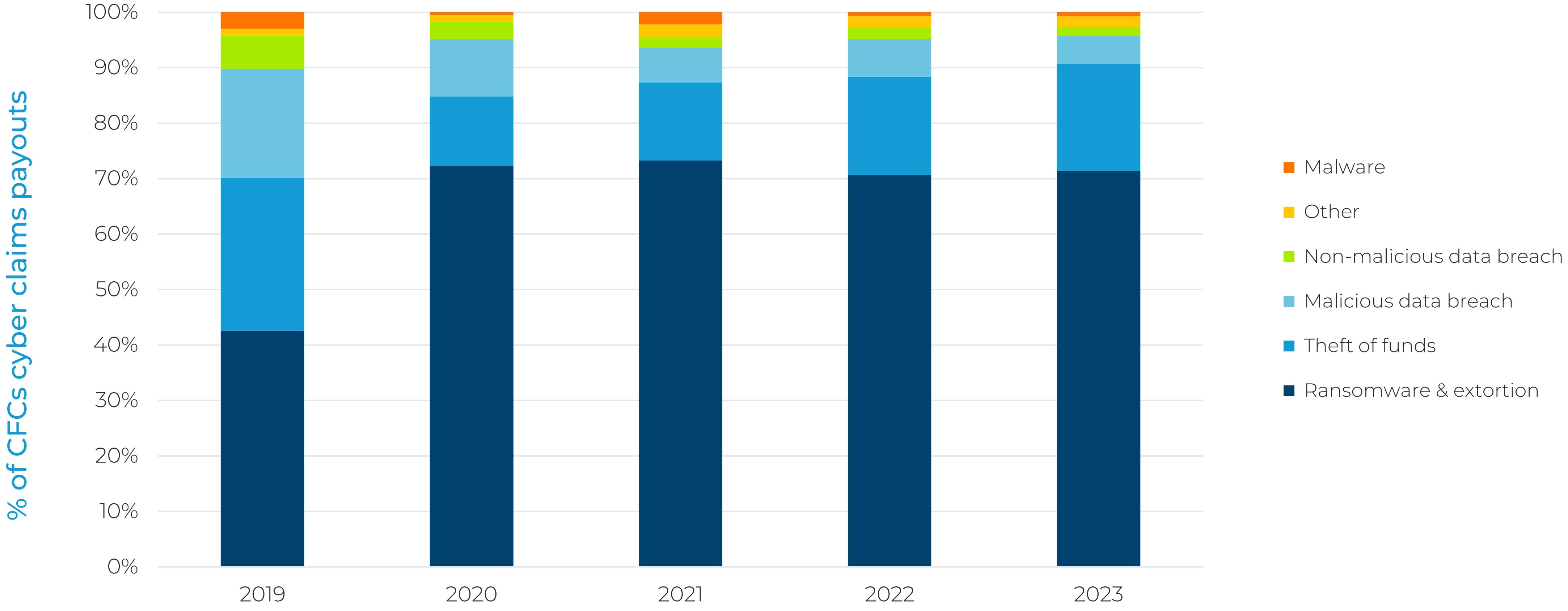
- Ransomware is a common and dangerous type of malware. It works by locking up or encrypting your files so you can no longer access them.
- A ransom, usually in the form of cryptocurrency, is demanded to restore access to the files.
- Traditionally ransomware was spread by email attachments and malicious websites, however it is more common for threat actors to gain access to a businesses systems via remote access services.
- A ransomware event can often lead to a Data Breach.

Australia cyber claims breakdown



**CFC cyber claims data from January – December 2023*

Ransomware remains a **top threat**



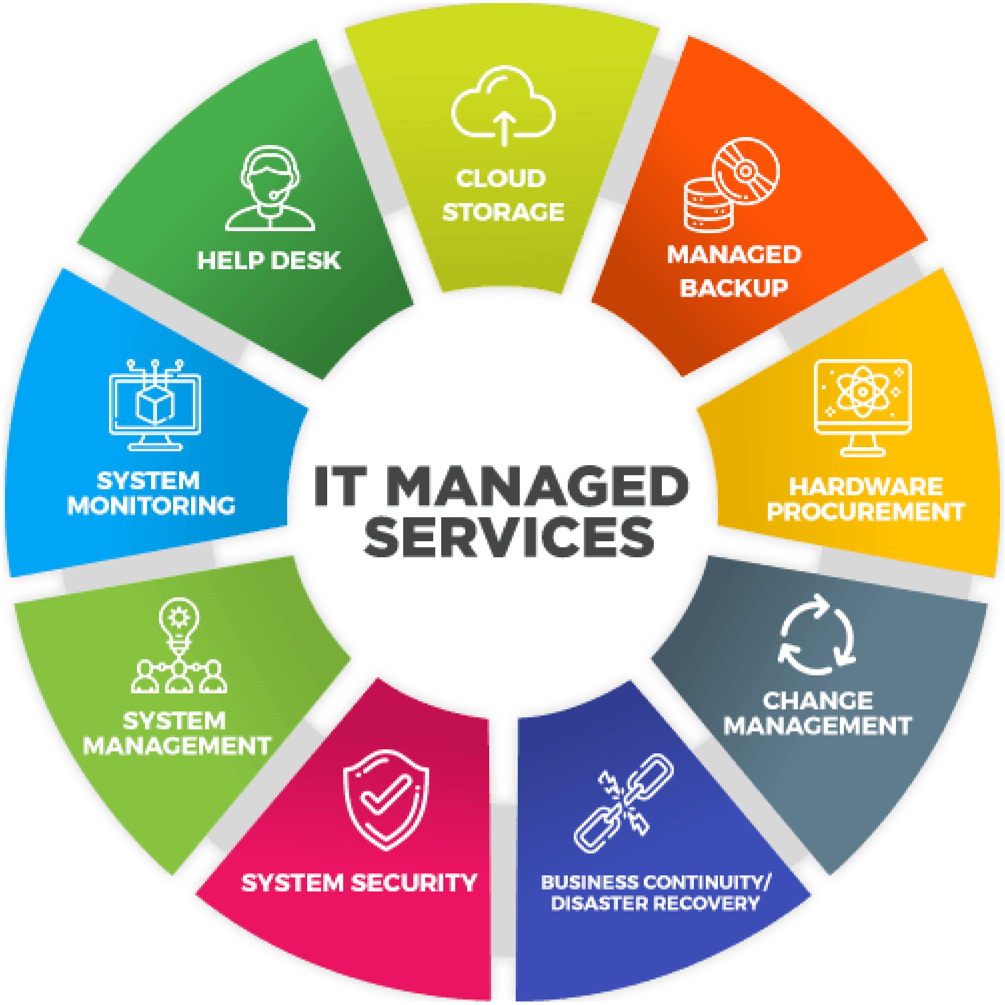
**CFC annual cyber claims data from January – December*

Emerging Cyber Threats

Vendor Supply Chain

Cyber criminals are entrepreneurial and are always looking for ways to get a bigger pay day for their efforts.

As a result, **cyber criminals are looking up and down the supply chain** looking for weaknesses they can leverage.

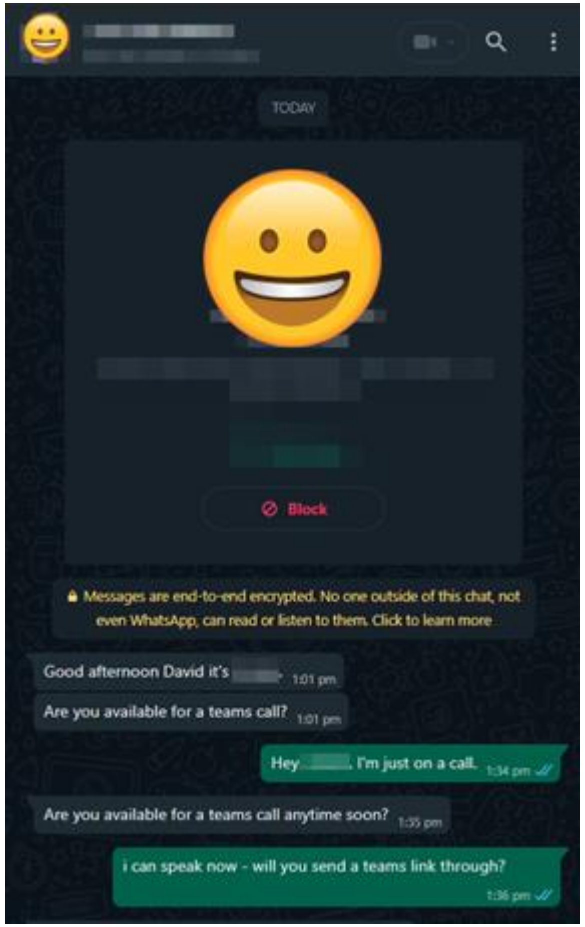


Emerging Cyber Threats

Artificial Intelligence

Threat actors are using free software to create semi-realistic videos of senior executives to **enhance the success of their social engineering scams**.

Threat actors are also using AI to **write better scam emails and even malicious software like ransomware**.



[redacted]

TODAY

[redacted]

⊘ Block

🔒 Messages are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Click to learn more

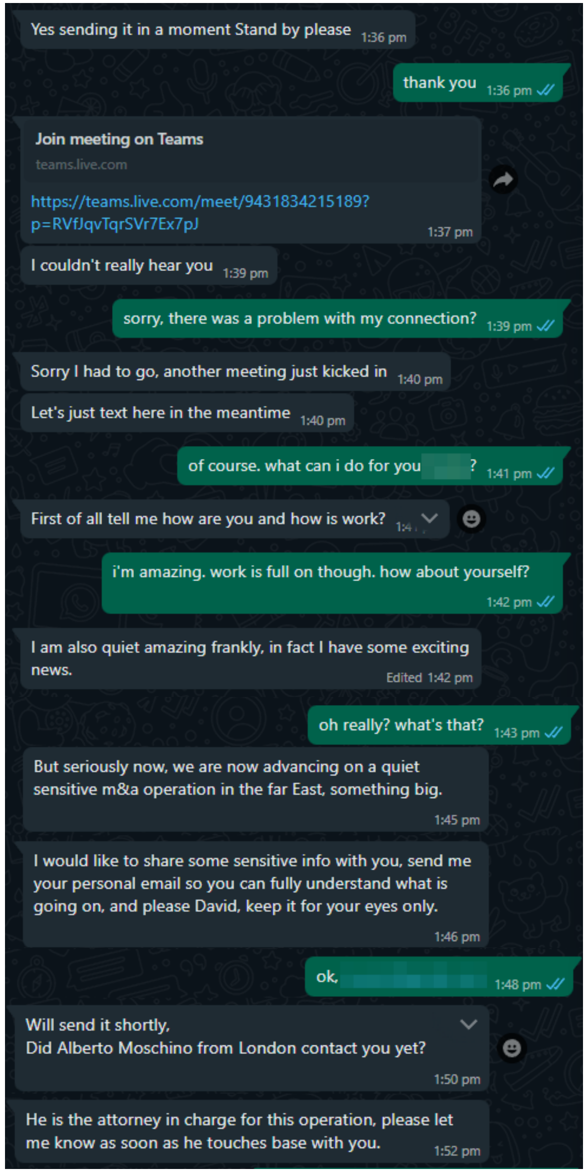
Good afternoon David it's [redacted] 1:01 pm

Are you available for a teams call? 1:01 pm

Hey [redacted]. I'm just on a call. 1:34 pm

Are you available for a teams call anytime soon? 1:35 pm

i can speak now - will you send a teams link through? 1:36 pm



Yes sending it in a moment Stand by please 1:36 pm

thank you 1:36 pm

Join meeting on Teams
teams.live.com
https://teams.live.com/meet/9431834215189?p=RVfJqvTqrSVr7Ex7pJ 1:37 pm

I couldn't really hear you 1:39 pm

sorry, there was a problem with my connection? 1:39 pm

Sorry I had to go, another meeting just kicked in 1:40 pm

Let's just text here in the meantime 1:40 pm

of course. what can i do for you [redacted]? 1:41 pm

First of all tell me how are you and how is work? 1:4

i'm amazing. work is full on though. how about yourself? 1:42 pm

I am also quiet amazing frankly, in fact I have some exciting news. Edited 1:42 pm

oh really? what's that? 1:43 pm

But seriously now, we are now advancing on a quiet sensitive m&a operation in the far East, something big. 1:45 pm

I would like to share some sensitive info with you, send me your personal email so you can fully understand what is going on, and please David, keep it for your eyes only. 1:46 pm

ok, [redacted] 1:48 pm

Will send it shortly,
Did Alberto Moschino from London contact you yet? 1:50 pm

He is the attorney in charge for this operation, please let me know as soon as he touches base with you. 1:52 pm

How does CFC **proactively protect** our customers?

Proactive Monitoring

From the moment a business binds a cyber policy,
CFC starts working to protect them against cyber-attacks.

Passive scans – The CTA team develop passive scans to run against the CFC portfolio for known vulnerabilities to identify at risk systems and services.

Identified 10k+ insureds with active vulnerabilities

Continuous scans – Those passive scans that have a high correlation with claims are rolled into a continuous scanning program that helps underwriters with risk selection.

Detected 10k+ RDP and 600 active malware instances

Deep scans – A subset of vulnerabilities are not possible to detect without more direct interaction with the target environment, and subsequently the CTA team uses our Response mobile app to gain consent to enable Deep Scanning.

Only performed on clients who give consent

cfc

Cyber Threat **Analysis**

Tuning out the noise to provide actionable intelligence

Threat Intelligence – The CTA team draws upon a wide range of threat intelligence partnerships including; government agencies, private sector experts, and our own proprietary data feeds in order to tackle systemic vulnerabilities.

100+ threat intelligence feeds monitored

Claims Intelligence – In collaboration with actuaries, the CTA team correlate the gathered threat intelligence with cyber claims data to remove the noise and create actionable claims intelligence.

Automatically correlates against 2,500+ cyber claims

Dissemination – Leveraging the Response mobile app, the CTA team push out alerts directly into the hands of policyholders.

Alerts pushed out directly to policyholders via app

cfc

How we **prevent** cyber attacks

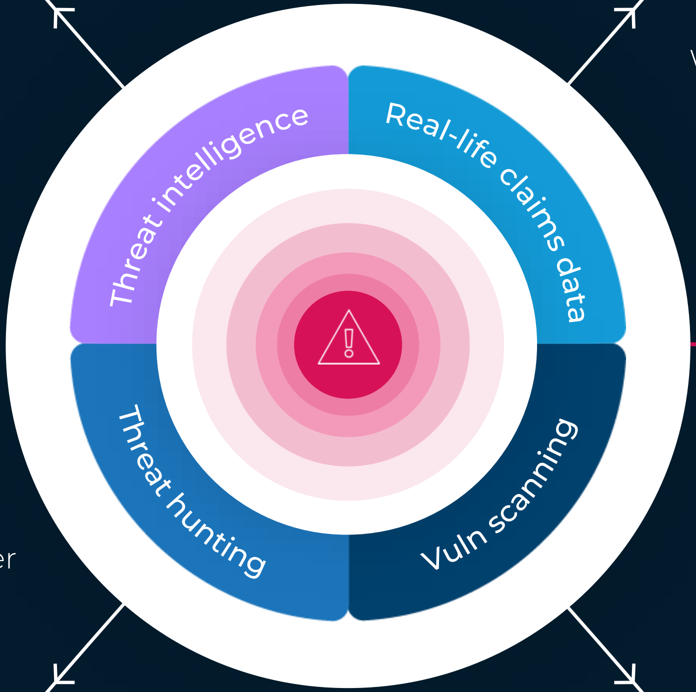
From the moment a customer takes out a CFC cyber policy, we start working around the clock to protect them against cyber attacks.

Threat intelligence

We partner with government and private threat intelligence organisations to identify and analyse information about cyber threats targeting our insureds.

Threat hunting

We search for signs of malicious activities, unauthorised access , or other indicators of compromise that go beyond traditional security measures.

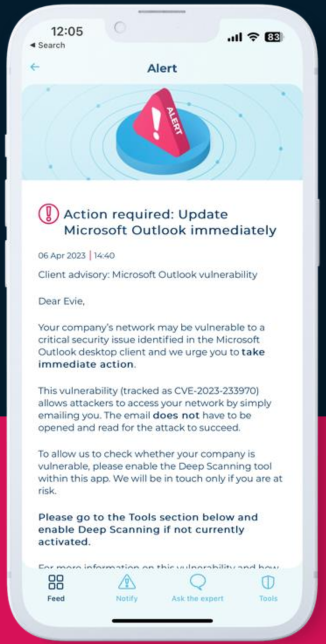


Real-life claims data

We use our own proprietary claims data to help identify attack trends and potential threats.

Vulnerability scanning

We actively scan insureds for known vulnerabilities and cyber risks that have a high correlation to claims.



Action required: Update Microsoft Outlook immediately

06 Apr 2023 | 14:40

Client advisory: Microsoft Outlook vulnerability

Dear Evie,

Your company's network may be vulnerable to a critical security issue identified in the Microsoft Outlook desktop client and we urge you to **take immediate action**.

This vulnerability (tracked as CVE-2023-233970) allows attackers to access your network by simply emailing you. The email **does not** have to be opened and read for the attack to succeed.

To allow us to check whether your company is vulnerable, please enable the Deep Scanning tool within this app. We will be in touch only if you are at risk.

Please go to the Tools section below and enable Deep Scanning if not currently activated.

For more information on this vulnerability and how

Real-time, actionable threat alerts

Using our **Response app**, we alert our insureds to threats targeting their business & help them mitigate the risk.

Single-click enabled cyber security tools

★★★★★

Excellence in Risk Management

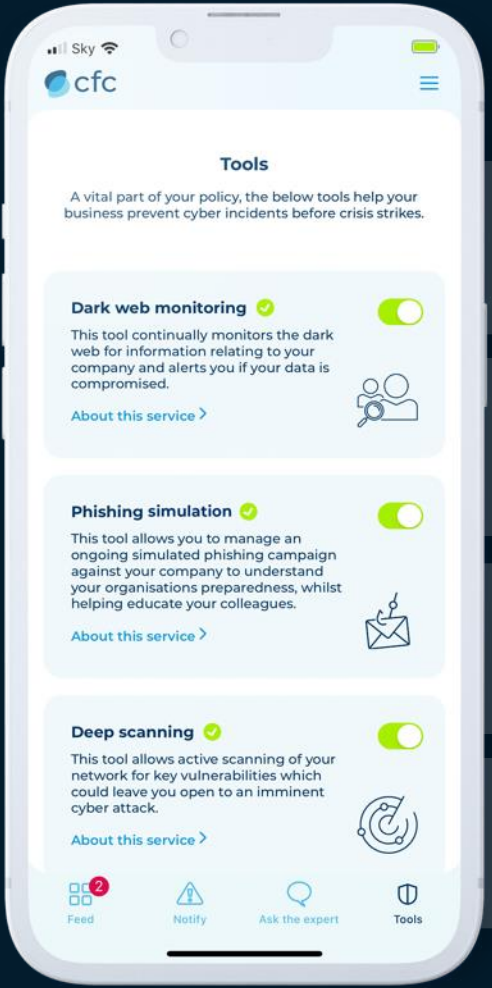
Insurance Times Awards 2022

40,000+ Response app users are benefitting from these free tools that would normally costs thousands.

Try it today!

Download via App Store or Google Play or scan the QR code

Demo policy number:
DEMOCFC000



Sky

cfc

Tools

A vital part of your policy, the below tools help your business prevent cyber incidents before crisis strikes.

Dark web monitoring ✓

This tool continually monitors the dark web for information relating to your company and alerts you if your data is compromised.

About this service >

Phishing simulation ✓

This tool allows you to manage an ongoing simulated phishing campaign against your company to understand your organisations preparedness, whilst helping educate your colleagues.

About this service >

Deep scanning ✓

This tool allows active scanning of your network for key vulnerabilities which could leave you open to an imminent cyber attack.

About this service >

Dark web monitoring

Ensures customers credentials aren't in the wrong hands

Phishing simulation

Improve awareness and response to phishing emails and social engineering

Deep scanning

Identify potential threats and vulnerabilities within an insureds network

'Ask the expert'

Access our global cyber security team for expert technical support

How does CFC Response **help our customers?**

Largest in-house incident response team

★★★★★

Cyber Safety & Loss Control Team of the Year

Zywave Cyber Risk Awards 2024

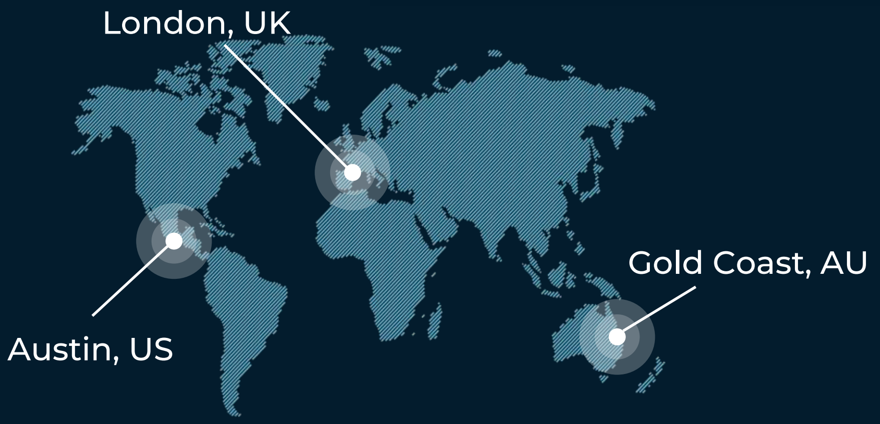
CFC Response successfully prevents and remediates thousands of cyber events for our customers each year.

24/7 follow-the-sun approach

<15 min technical response time

2,500+ cyber events handled each year

140+ security experts



Preventing cyber attacks

Using insights from threat intelligence feeds, the dark web, network scanning and our own real-life claims data, CFC Response identifies potential threats and alerts vulnerable customers before the worst happens.

Responding to cyber attacks

Available 24/7, our global team of cyber incident responders work quickly to triage incidents, contain threats, and repair networks, minimising the impact to our customers and getting them back online quickly.

The Aussie team

Our local team comprises of:

- **Largest dedicated in-house incident response team in Australia** with 40+ people based on the Gold Coast.
- Dedicated **digital forensics & incident response specialists**, with experience handling all types and sizes of cyber attacks.
- Dedicated **cyber security team**, focusing on providing cyber risk advisory and proactive cyber security services for the SMB and SME market.
- **Software development team** who work on innovative solutions to help our clients be better protected and respond to cyber incidents faster.

cfc

How we **remediate** cyber attacks

ACSC Australian **Cyber Security** Centre | NETWORK PARTNER

GIAC CERTIFIED GCIH INCIDENT HANDLER · GIAC CERTIFIED GCFE FORENSIC EXAMINER · GIAC CERTIFIED GCFA FORENSIC ANALYST · CISSP

Technical expertise and real-world experience can make the difference between suffering a catastrophic loss or getting back online quickly.

1

Notify

Available 24/7, the fastest way to notify CFC of a cyber incident is **through our mobile app, Response** or the 24x7 incident response telephone hotline.

2

Triage

A **technical incident responder will be in touch within 15 minutes** to assess the situation and identify the necessary resources to address the incident.

3

Contain

Our **expert, in-house team** of cyber security engineers, forensic specialists and threat analysts work to contain and remediate the incident. We'll also engage third-party specialists to help with activities like reputation management and breach notification.

4

Recover

Once the issue is contained, our team works around the clock to rebuild systems, reconstitute data and get the business **back online** as soon as possible.

Response app

Quickest and most direct way to speak with us

24x7 Hotline

Australia: 1800 803 202

Online

Notify a claim at cfc.com/claims

cfc

Ransomware sanctions process

We cooperate with OFSI and law enforcement.

0

Sanctions inputs

- Payment address
- Variant
- Demand email

1

Direct match

- Global sanctions lists
- Know your transactions

2

Prior Association

- Historic payments
- Historic addresses
- Historic sanctions

3

Contextual Match

- Known associations
- Known sanctions

4

RPRA Report

- Very high (certain)
- High (likely)
- Medium (potential)
- Low (unlikely)

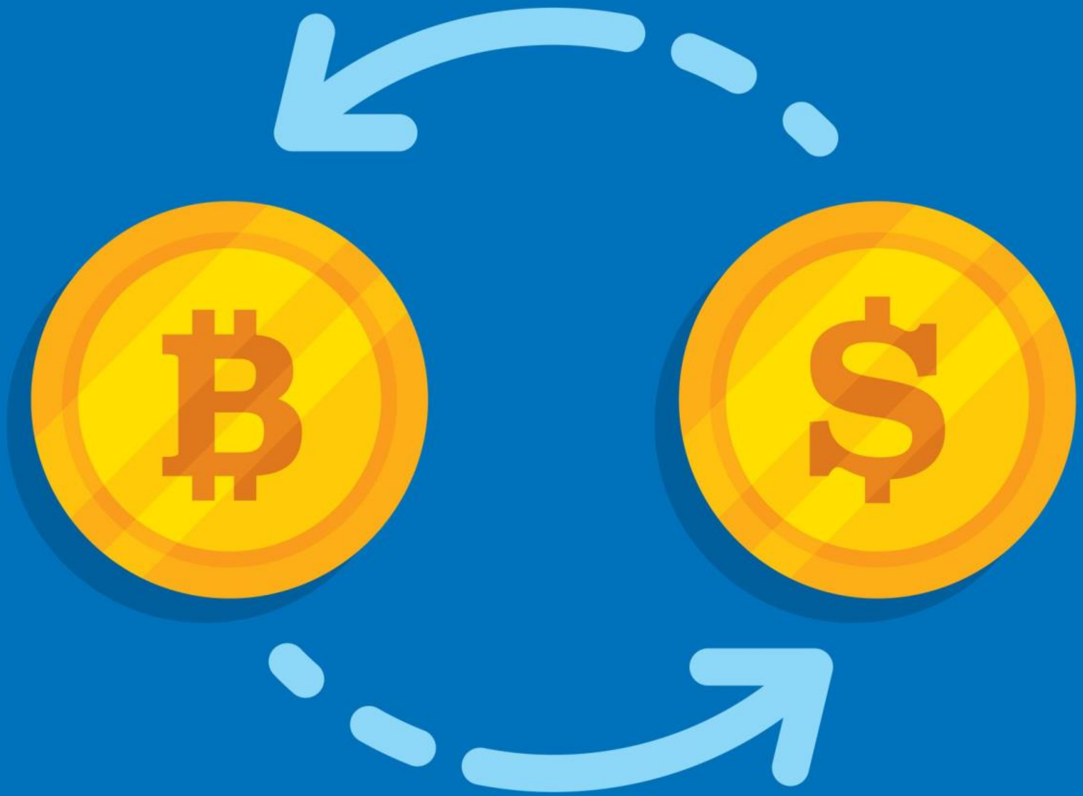
Ransomware: **Negotiation**

- **Requires trained and experienced negotiators.**
- Most people don't understand:
  - You're dealing with a customer service rep.
  - They often need to escalate to a supervisor.
  - They may take a few days off.
  - They may not respond for a while.
  - They won't tolerate abusive language either!
- Negotiations can take as quickly as 2 business days, or as long as several weeks depending on the desired outcome.
- If you are trying to stall them to get ahead of the press or customer retaliation, there is a limit to how long you can drag the process out.
- Like any seller, eventually they will get frustrated and can retaliate if negotiations are not handled properly.

Ransomware: **Payment**

- **Client must pay for cryptocurrency up-front.**
- Delays can occur:
  - Transferring money from bank to crypto-exchange. Usually takes 6-12 hours depending on client’s bank.
  - From negotiator’s crypto wallet to threat actor's wallet. Usually 6-12 hours.
  - Threat actor may delay before confirming they have received payment in full.
- The decryption tool supplied by the threat actor may:
  - Not work properly.
  - May require fixing or support.
  - Can be very slow and labour intensive.
  - May be unable to decrypt large files > 4GB like database, email storage and backups.
- Recovery can take weeks, if not months.

cfc



Free Cyber Security Services

cfc | solis

CFC has partnered with **Solis Security** to provide an **exclusive offer to CFC policy holders.**

Affordable Cyber Security for SME's

You're supported by a global team of cyber security experts for less than the cost of a FTE.

24/7 365 Endpoint Monitoring

Compliment existing internal IT and third-party managed IT services with Solis MDR's 24/7 endpoint threat monitoring backed by our expert team and trusted by CFC.

Reduce Risk & Impact of an Attack

Building upon CFC's proactive external threat detection, Solis' MDR service reduces time an attacker has inside your network, helping to prevent cyber incidents before they cause harm.

Powered by SentinelOne®

Exclusive 60-Day Free Trial

Quickly and easily implement Solis MDR with your existing infrastructure to see it in action.

Simply **email sales.au@solissecurity.com** and provide your CFC cyber insurance policy number to begin!

This offer is exclusively available to CFC cyber insurance policy holders. The free trial is subject to acceptance of the Solis standard terms and conditions, and Solis reserves the right to withdraw this offer at any point without prior notice.

Next Steps

cfc RESPONSE

> Now that you know the value of your CFC cyber insurance policy, how it reacts and the services it offers, what do you do next?

1. Install the CFC Response mobile application and enable “Deep Scanning”
2. Review and update your Incident Response Plan (IRP)
3. Conduct a Cyber Crisis simulation (tabletop exercise) annually
4. Ensure MFA is enabled for all Email and Identity accounts
5. Ensure your EDR security service is monitored 24x7

If you have any questions or would like us to direct you to a partner who can help you develop your cyber security roadmap, email onboarding.au@cfcresponse.com

Questions