



Sports Cyber Webinar

Marsh & CFC Presents

24th August

A business of Marsh McLennan

Presenters



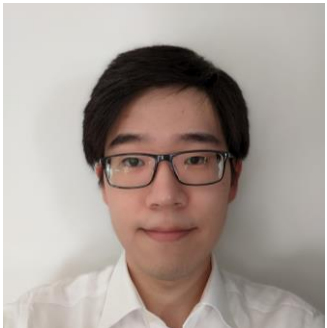
James Mathes

Account Executive – Cyber



Faizal Janif

Head of Cyber Advisory Asia Pacific



Jonathan Lee

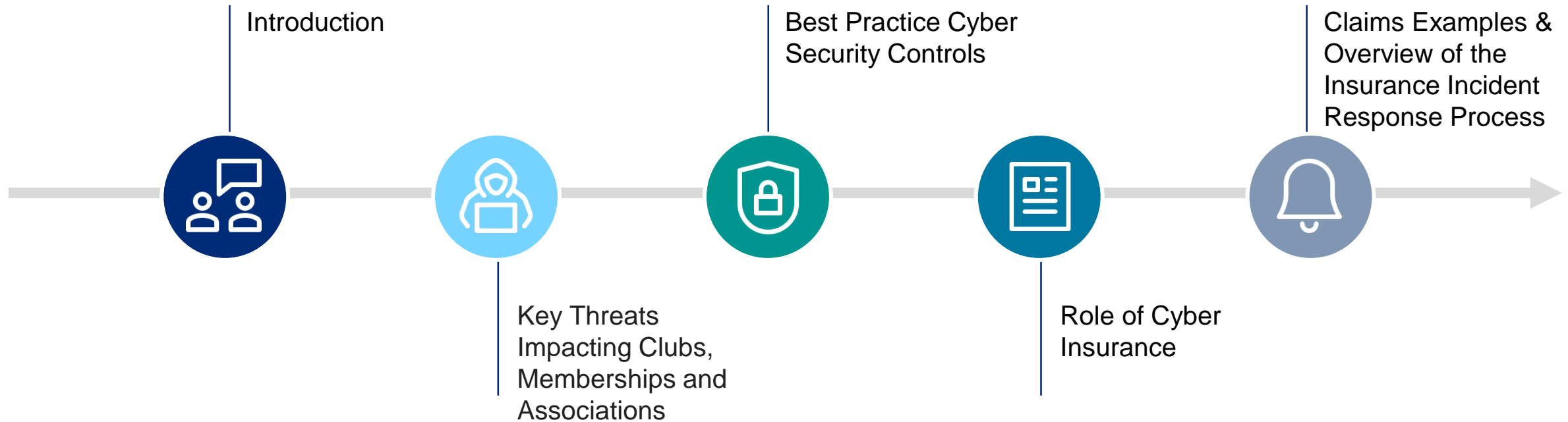
Graduate Broker – Cyber



Harry Hill

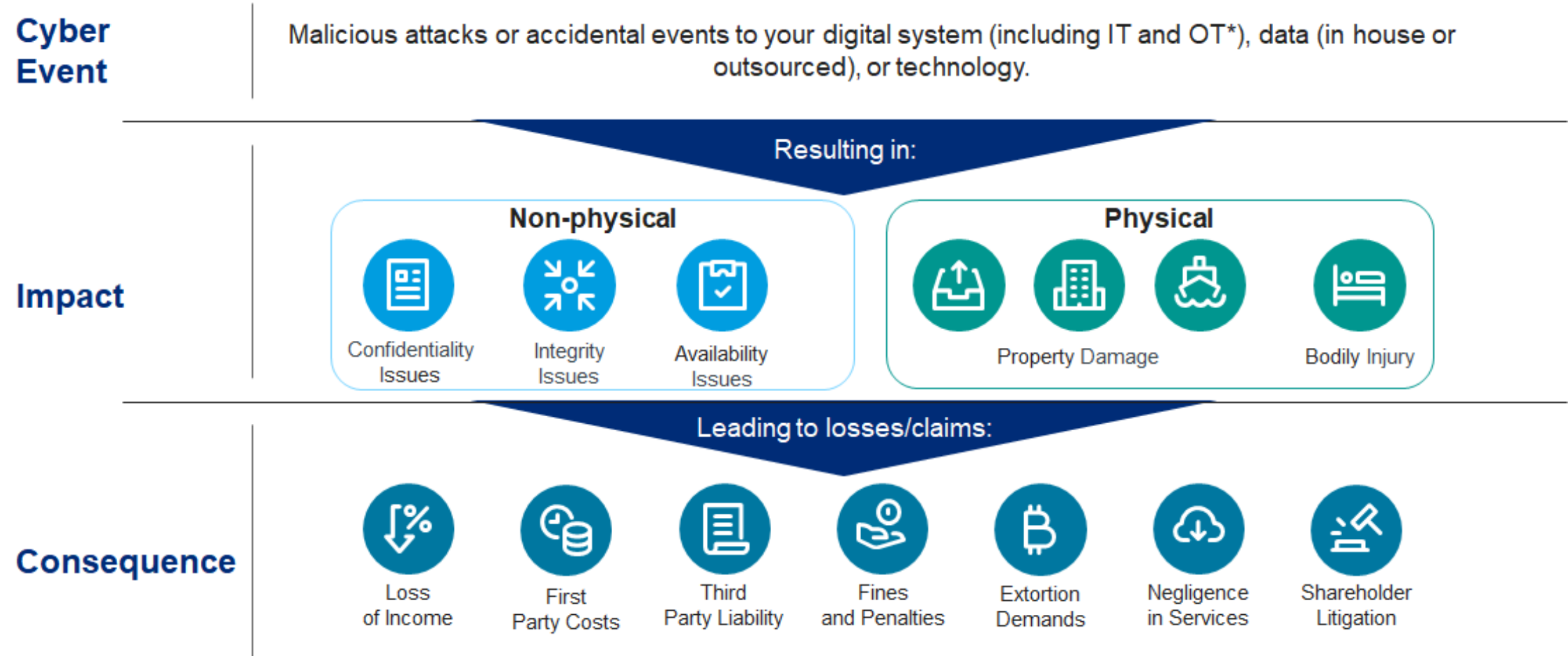
Cyber Development Manager

Agenda/Discussion



Key Threats Impacting Clubs, Memberships and Associations

Cyber Threat Landscape



*Operational technology

Impacts of Cyber Event upon Sports Clubs



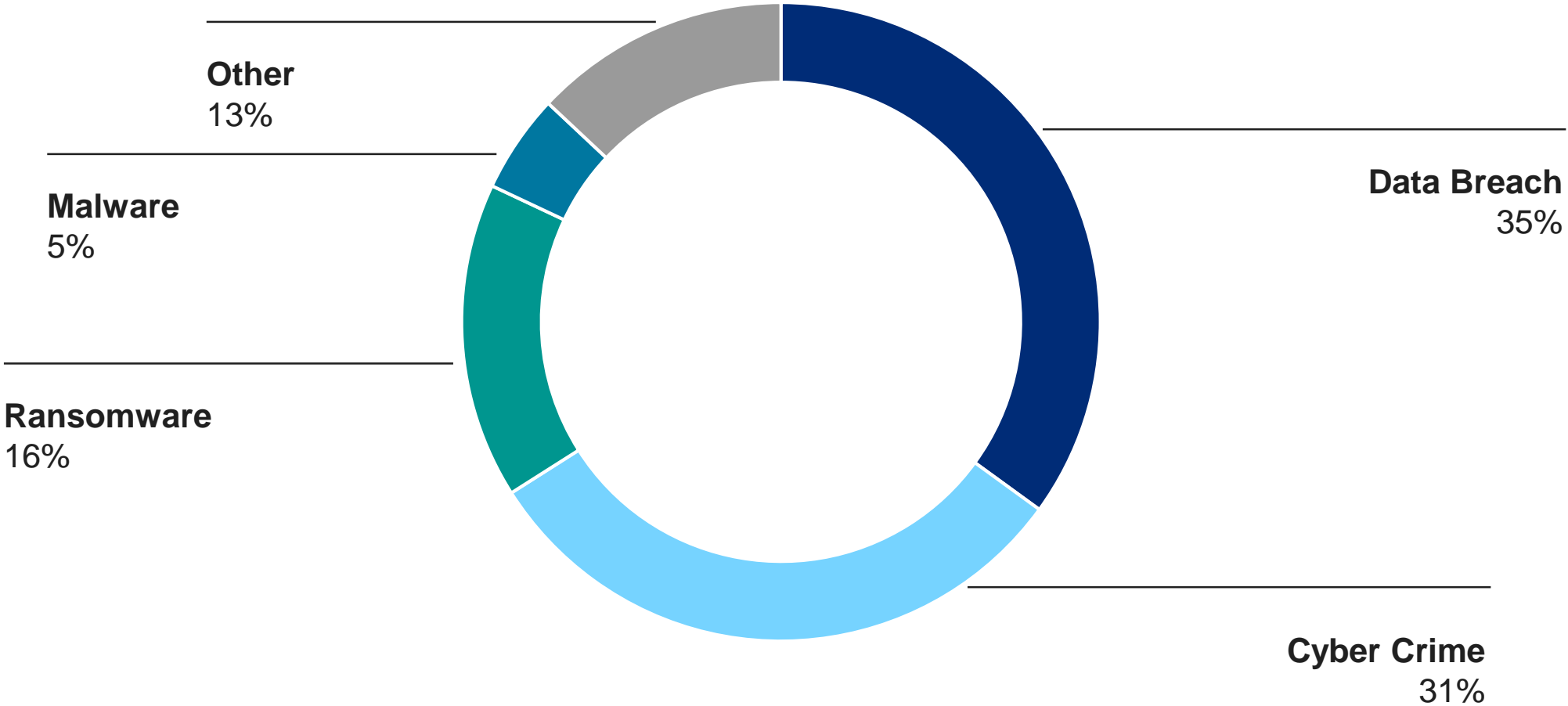
Data Privacy

**Brand Damage /
Reputational Harm**

**System
Interruption**

Key Threats

Clubs, Memberships and Associations



Best Practices – Cyber Security Controls

ACSC ASD Essential 8

Marsh Advisory Pacific

Executive Summary

Exploitation of the
pandemic
environment

Disruption of essential
services and critical
infrastructure

Ransomware

Rapid exploitation of
security vulnerabilities

Exploitation of Supply
Chain networks

Business email
compromise

Definition of the Controls

What do the Essential 8 controls do



Application Whitelisting

To control the execution of unauthorized software



Configure Macros

To block untrusted macros



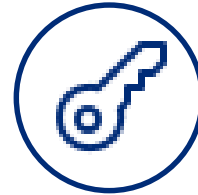
Multi-Factor Authentication

To protect against risky activities



Restrict Admin Permissions

To limit powerful access to systems



Patch Operating Systems

To remediate known security vulnerabilities



Patching Applications

To remediate known security vulnerabilities



Application Hardening

To protect against vulnerable functionalities



Daily Backups

To maintain availability of critical data

The Essential Eight




Mitigation strategies to thwart cyber attacks

Overview




The Australian Cyber Security Centre's (ACSC) Essential 8 risk management framework is a prioritised list of **eight mitigation strategies** (security controls) that organisations can implement to protect their systems **against a range of adversaries**. ACSC considers implementation of the Essential 8 to be the most effective cyber resilience baseline for organisations.

Published in Feb 2017, Australian Signals Directorate (ASD) found that when operating effectively, the **Essential 8 mitigates 85% of targeted cyber-attacks**.

Before implementation of mitigation strategy, a quick checklist to perform following activities

-  **Identify which system require protection** (i.e. which systems store, process or communicate sensitive information or other information with a high availability requirement)
-  **Identify what level of protection is required** (e.g. nation-states, cyber criminals or malicious insiders)
-  **Identify targets most likely to target systems** (i.e. selecting mitigation strategies to implement based on the risks to business activities from specific adversaries)

The following updates are made to the Essential 8 by ACSC in July 2021

-  Moving the implementation of controls to a **risk-based approach**. Where implementation of controls is not possible (for example legacy systems), have adequate risk management processes
-  **Implementation of mitigation strategies as a package**, rather than evaluating each individual control for its level of maturity
-  **Redefining the number of maturity levels and what they represent** for control

SOURCE: Australia Cyber Government Site, Secondary Articles

The Role of Cyber Insurance

Why is Cyber Insurance important?

Cyber insurance responds to claims made by victims of a cyber incident. These include:



Incident Response Services

Immediate 24/7 access to incident response services following an actual or suspected cyber event



Extortion Payments

Ransom payments* and access to specialist ransom negotiators

**where it is legal for insurers to pay a ransom*



Business Interruption

Loss of profit related to business interruption following a cyber incident attack



Restoration Costs

Costs to repair and restore IT systems and data



Third Party Liability Cover

Defence and Liability Costs incurred for damage to others, caused by an insured



Cyber Crime

Funds Transfer Fraud; Social engineering and Phishing

CFC Cyber Presentation

Marsh Sports Clubs

CFC - Harry Hill
24th August 2022



Innovative insurance



CFC is a specialist insurance provider, pioneer in emerging risk and market leader in cyber. Our global insurance platform uses cutting-edge technology and data science to deliver smarter, faster underwriting and protect customers from today's most critical business risks.



Innovator of
the Year

Reactions London
Market Awards 2020



Broker Partner of
the Year

British Insurance
Awards 2020



5 star Excellence
Award

Insurance Business UK
2020



100k+

Customers



90+

Customer
countries



\$800m+

Premium



500+

Employees



1999

Founded



5

Global
offices

We love Australia!



CFC has been trading in Australia for over 15 years and handles tens of thousands of submissions each year from Australian businesses. We pride ourselves on our services levels - responding to over 90% of new business enquiries in 24-hours or less.

7,000+

customers

\$75m+

premium

Top

cyber provider

15+

underwriters



Proud sponsors of

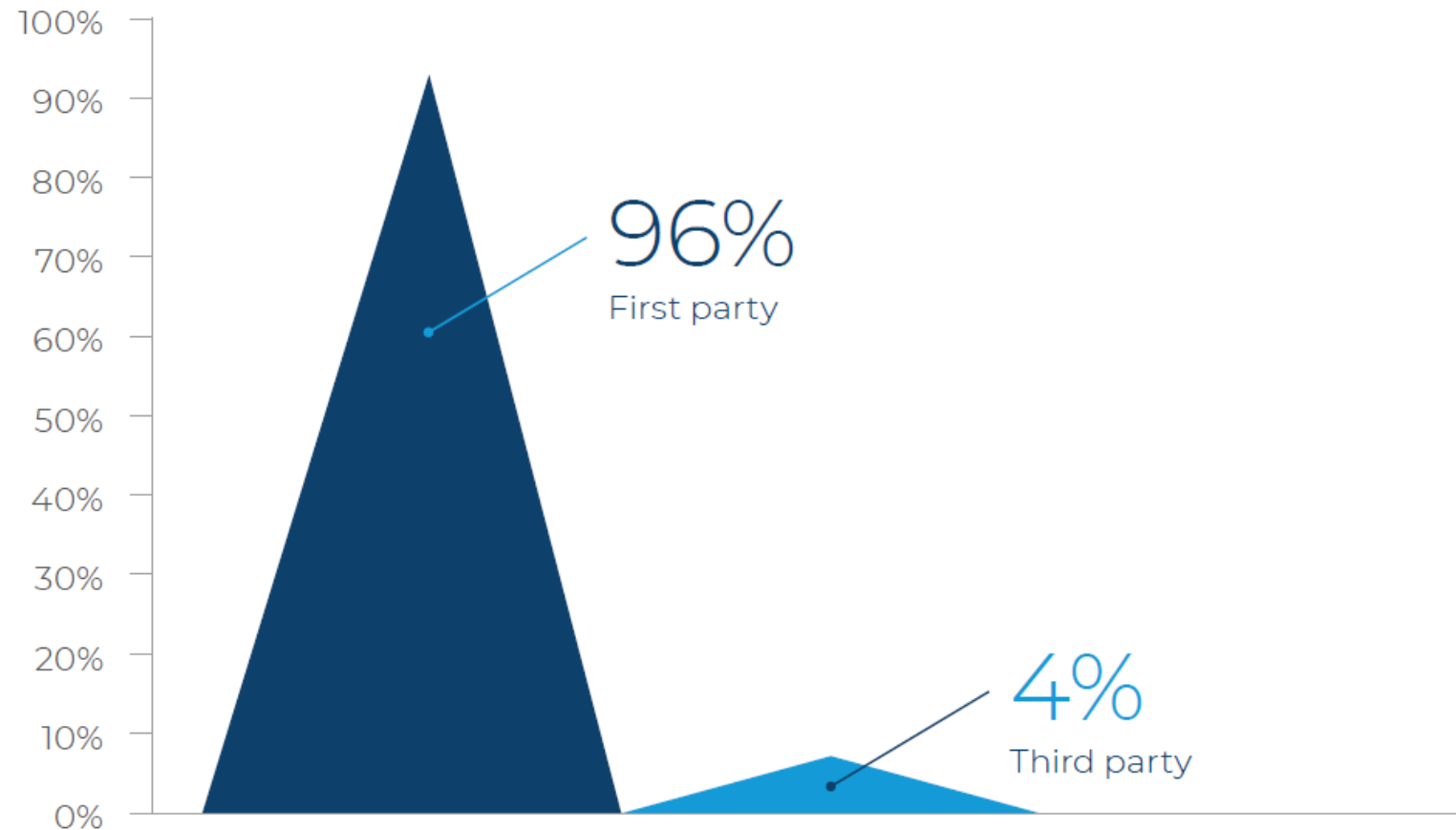




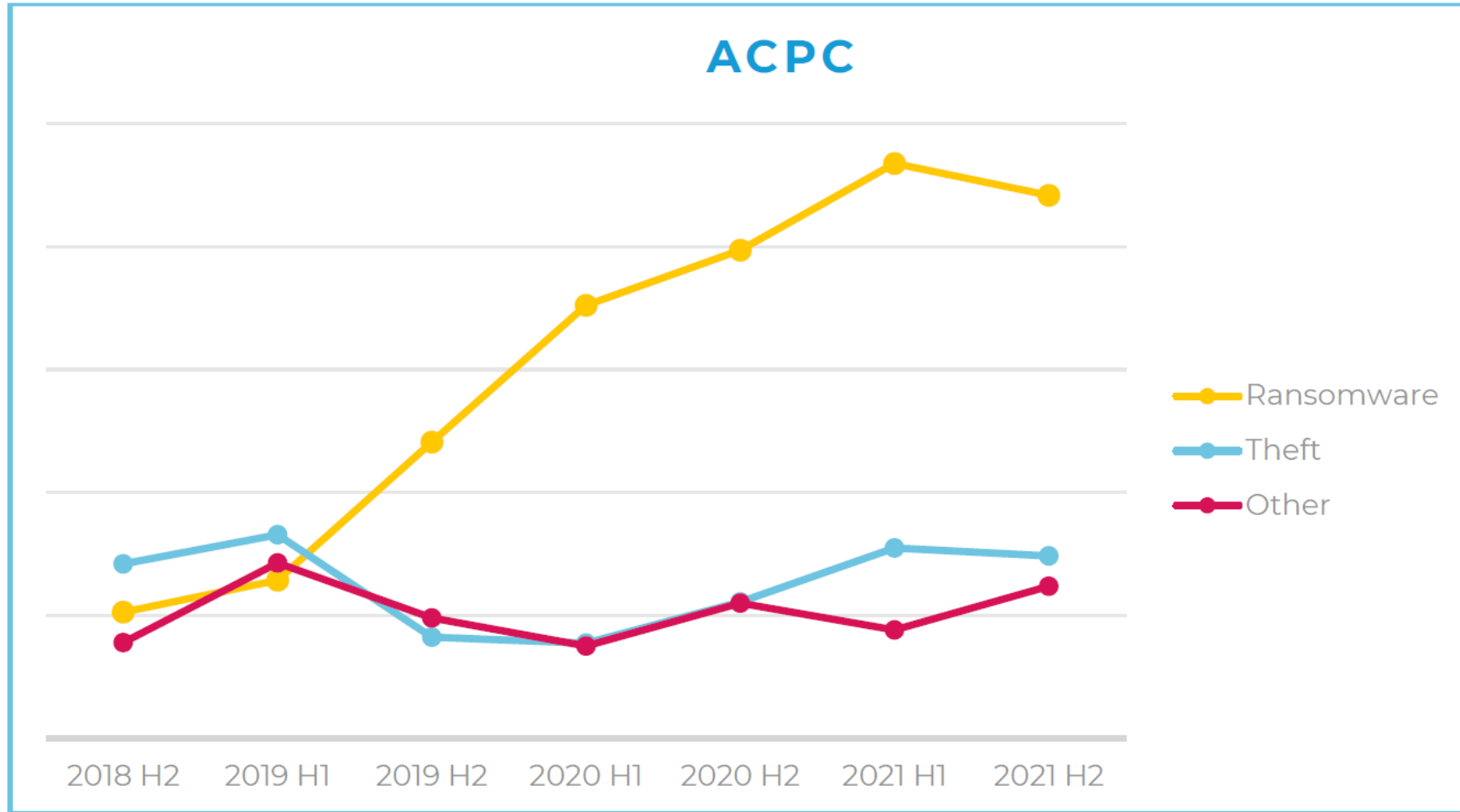
Cyber Risk in 2022

Evolution of cyber claims

First party v third party claims



Severity of losses have dramatically increased...



Case Study:

How Ransomware impacted a Football Club

60,000 members

Ransomware event was caused by an open RDP Port leading to the encryption of their POS server.

No direct financial loss to the insured – they were able to rebuild their POS server.

However, forensic analysis found a significant amount of personal data was stored on this server – including Credit Card info.

Breach counsel advised the client that they insured should notify the OAIC and the individuals directly affected.

Total costs of the incident - \$244,753





Transferring your risk: The Cyber Product

Core covers

1. Incident
response

2. Cybercrime
(theft of funds)

3. System
damage & BI

CFC Response

The team, technology and intelligence that support our customers before, during and after a cyber event.

CFC Response has proactively prevented over a thousand cyber attacks and handled over 3,500 cyber events in the last two years. Our award-winning team of more than 100 cyber incident specialists around the world serve 60,000+ businesses across 65 countries.



Claims Product
Solution of the Year

Insurance Times Claims
Excellence Awards 2021



Cyber Claims Team
of the Year

Insurance Insider Cyber
Rankings 2020

100+ cyber specialists

2,000+ incidents a year

20+ years

Industry's leading
cyber incident
response app

Team



Technology



Intelligence



Prevention at your fingertips



An integral part of our cyber policy, our award-winning mobile app, Response, gives policyholders access to a range of proactive cybersecurity tools and services.

- Get real-time threat intelligence, delivered to your phone
- Activate free risk management and cyber security tools
- Access our cyber security experts for advice at any time
- Instantly notify us of cyber incidents



Best Customer App

Insurance Times Tech & Innovation Awards 2021



Insurer Claims Innovation

Insurance Post Claims and Fraud Awards 2021

Questions?