A Practical Guide
to
Incident Management

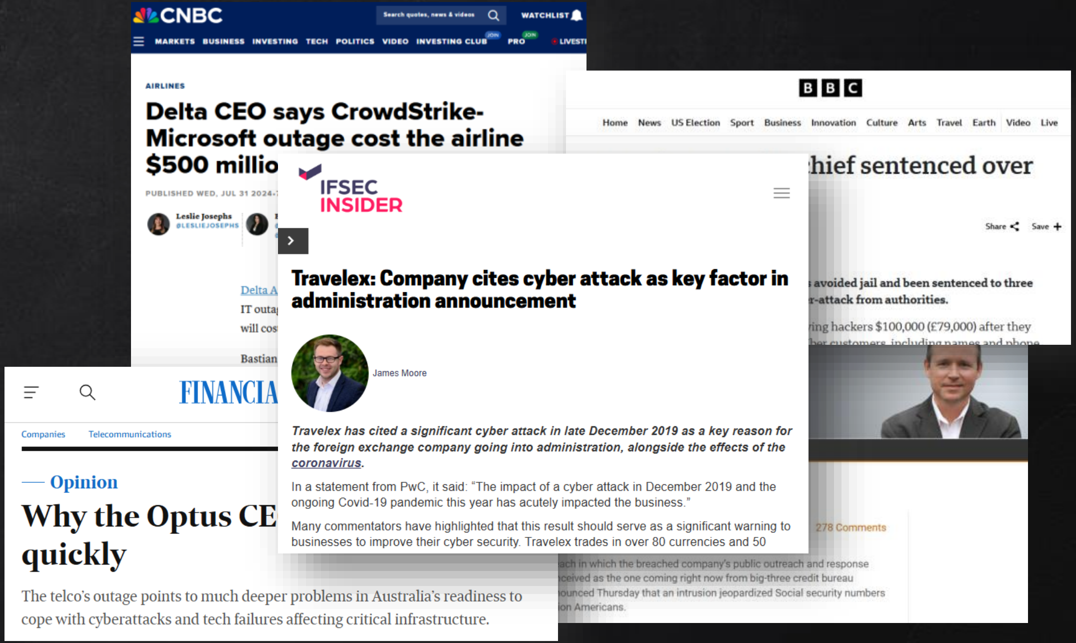
Jon Edney

Head of Cybersecurity and Privacy, Tuatahi Fibre Ltd

CISSP, CIPT, CEH, CIMS

Why should we care?

- Incident Management is easier to get wrong, than it is to get right.
- Your IM preparation, leadership skills and character will be put to the test in front of your most significant stakeholders.
  (Customers, Suppliers, CEO, Board, Shareholders, Regulators, Insurers, Politicians)
- What you do during an incident can directly and dramatically influence the future viability of your business.


CNBC
Search quotes, news & videos
WATCHLIST
MARKETS BUSINESS INVESTING TECH POLITICS VIDEO INVESTING CLUB JOIN PRO JOIN LIVESTI
BBC
Home News US Election Sport Business Innovation Culture Arts Travel Earth Video Live
Share Save
IFSEC INSIDER
FINANCIA
Companies Telecommunications
278 Comments

AIRLINES

Delta CEO says CrowdStrike-Microsoft outage cost the airline $500 millio

PUBLISHED WED, JUL 31 2024·

Leslie Josephs @LESLIEJOSEPHS

Delta A
IT outa
will cos

Bastian

hief sentenced over

s avoided jail and been sentenced to three
r-attack from authorities.

ing hackers $100,000 (£79,000) after they
ber customers, including names and phone

Travelex: Company cites cyber attack as key factor in administration announcement

James Moore

Travelex has cited a significant cyber attack in late December 2019 as a key reason for the foreign exchange company going into administration, alongside the effects of the coronavirus.

In a statement from PwC, it said: "The impact of a cyber attack in December 2019 and the ongoing Covid-19 pandemic this year has acutely impacted the business."

Many commentators have highlighted that this result should serve as a significant warning to businesses to improve their cyber security. Travelex trades in over 80 currencies and 50

ach in which the breached company's public outreach and response
ceived as the one coming right now from big-three credit bureau
ounced Thursday that an intrusion jeopardized Social security numbers
ion Americans.

— Opinion

Why the Optus CE
quickly

The telco's outage points to much deeper problems in Australia's readiness to cope with cyberattacks and tech failures affecting critical infrastructure.

1.

Getting in a Pickle

Incident Tiers

Minor
[Business as Usual]

Response is clear and follows a known standard process.

Major
[Multi-Team/Multi-Skill]

A multi-skillset coordinated response is required for which there are no established standard procedures.

Crisis
[All-of-Organisation]

A serious ongoing incident which requires a coordinated company-wide response.

Tips

Risk and Resource

Don’t Over Think!

Playbooks

Playbook

Given to your SOC, IT Support or other “first point of contact”.

Contains step by step containment or remediation steps for common scenarios.

Contents

- Trigger
- Containment/Remediation Steps
- Escalation Trigger & Method

2.

Plans, Plans, Plans

Crisis Management Plan

Crisis Management Plan

Processes an organisation will use to respond to and resolve a major incident.

Contents

- Categorisation/Thresholds for Incidents
- Emergency Facilities, Equipment, Systems
- Communications and Templated Comms
- Key Contacts
- Emergency Delegations & Finance Processes
- Leadership Roles & Responsibilities
- How to Activate

Tips

People

CIMS

All-of-Business

Capability over Seniority

Business Continuity Plan (BCP)

Business Continuity Plan(s)

How the business will continue to deliver its mission/services during a disruption.

Contents

- Critical Functions and Dependencies
- Key Staff and Suppliers
- Alternative Facilities, Equipment, Systems
- Communications Plan

Tips

Business Unit Led

Not Every Team

Disaster Recovery (DR) Plan

IT Outage

Due to a global IT outage we are currently operating on a reduced amount of registers and self checkouts.

We apologise and thank you for your patience.

CROWDSTRIKE

:(

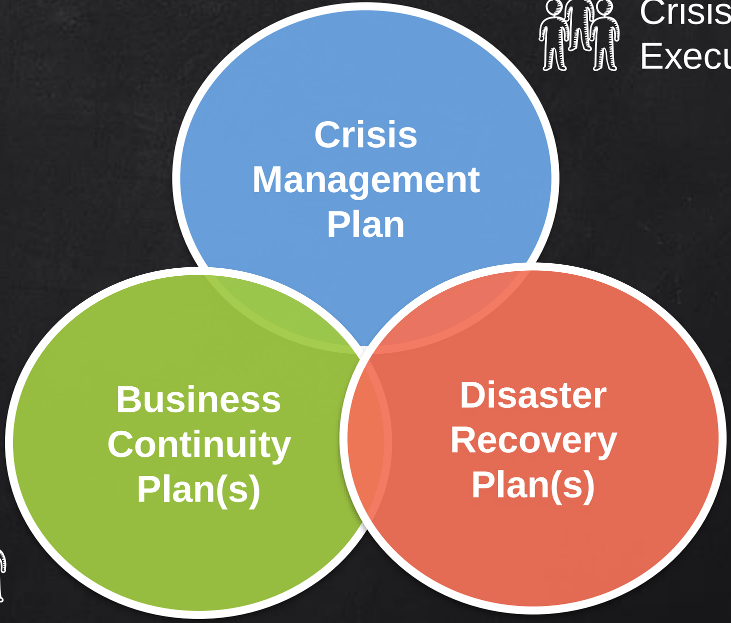
Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

Tips

Not a "For Dummies" Book

Test Assumptions

Key Plans



Crisis Management Plan

Business Continuity Plan(s)

Disaster Recovery Plan(s)

Crisis Management Team/
Executive Leadership Team

Staff and Business
Unit Managers

Technical/OT/IT Team(s)

Your challenge

Take charge of your business with robust, cohesive, and well-rehearsed Incident Management processes you can rely on to navigate any cybersecurity challenge.

thanks!

Any questions?