STRATEGICGROUP
YOUR TRUSTED IT PARTNER

Aron Robertson
CCO @ Strategic Group

aron.robertson@strategicgroup.net.au

www.linkedin.com/in/aronrobertson/

Anatomy of a Cyber Attack
How Hackers Target Your Business

The Why : Increasing Impact

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC

Annual Cyber Threat Report

2024–2025

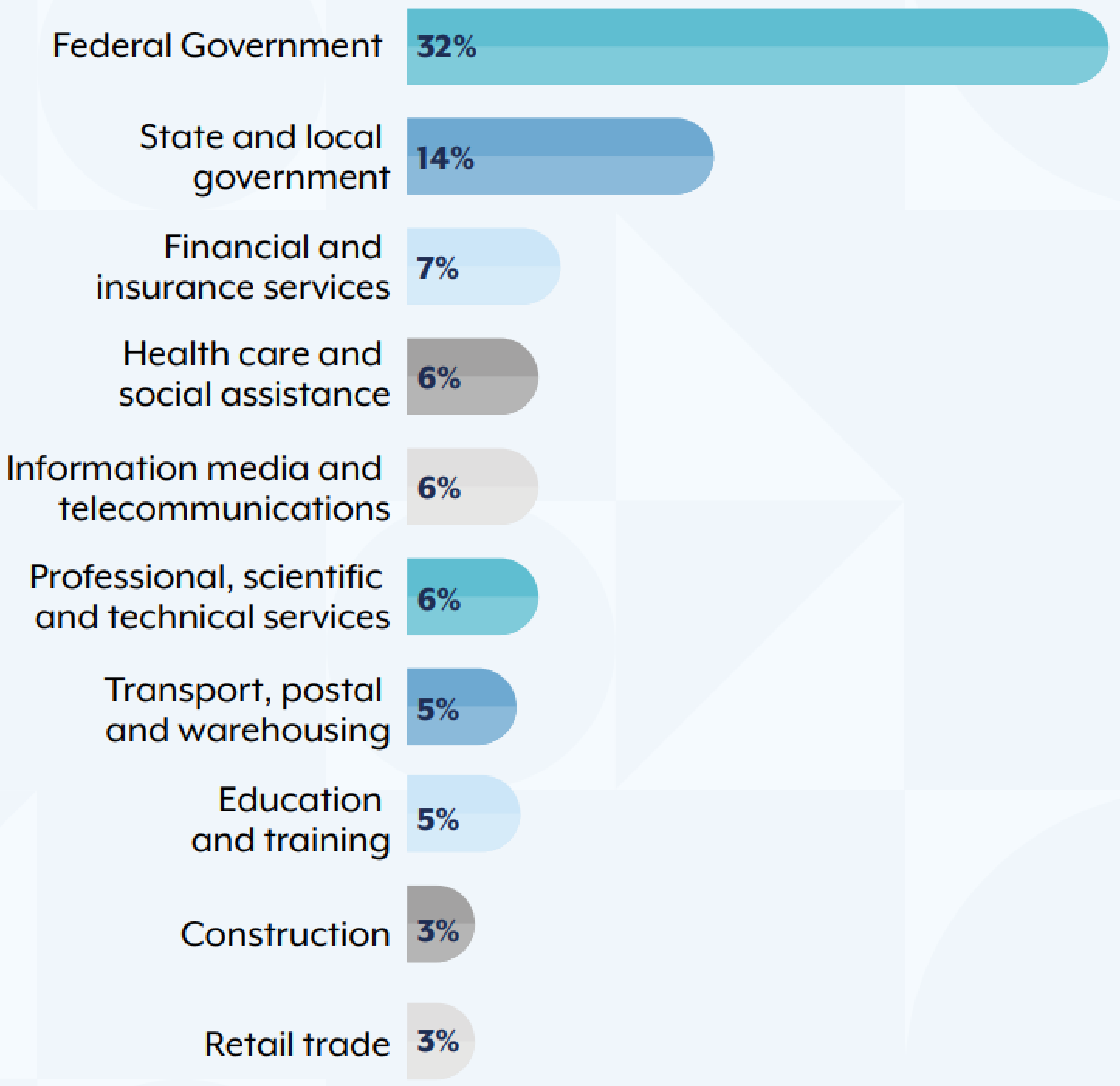
The average self-reported cost per report and business size was:

- small business – **$56,600** (up 14%)
- medium business – **$97,200** (up 55%)
- large business – **$202,700** (up 219%).

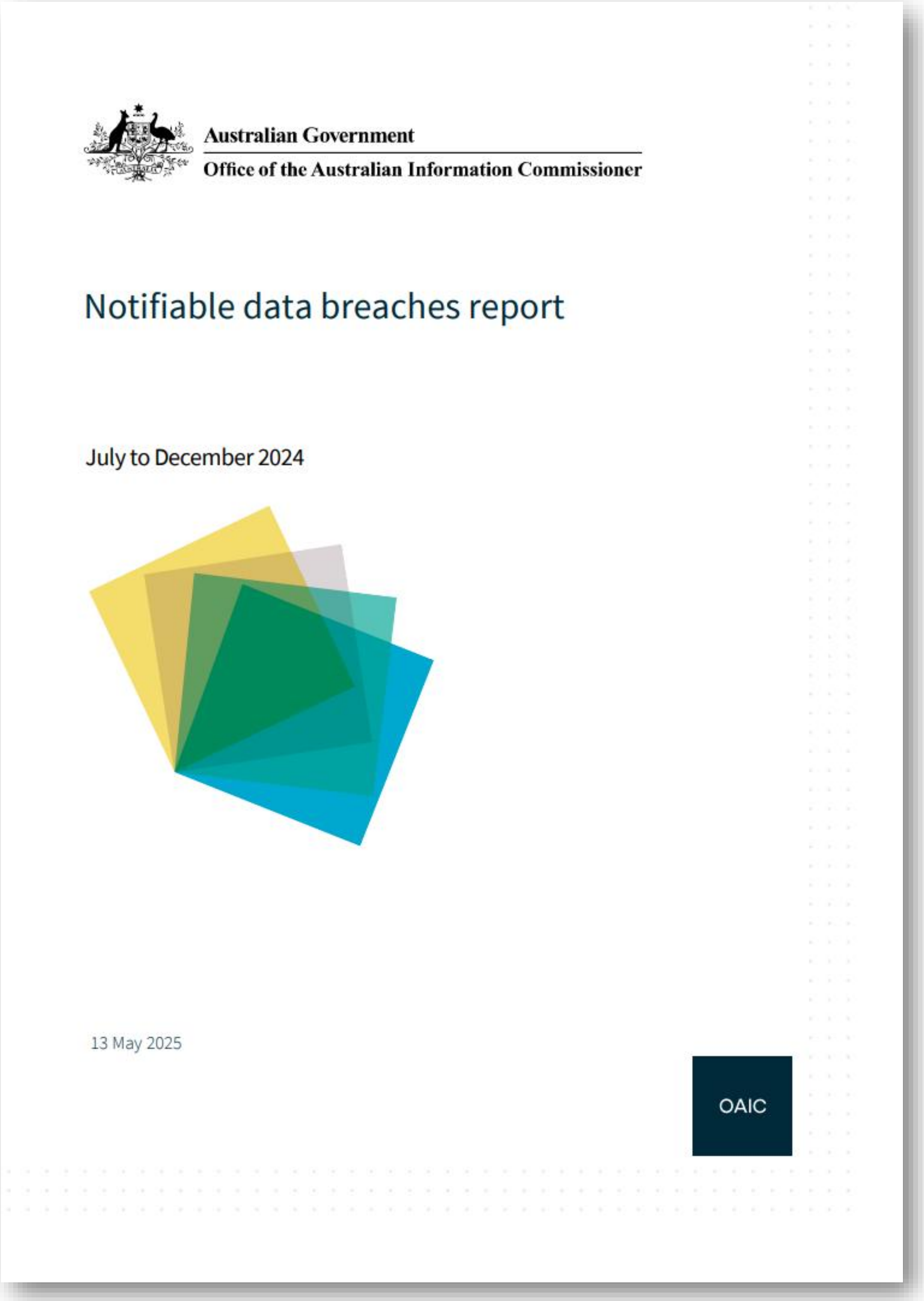
The top **cybercrimes** reported by **businesses** were:

- email compromise resulting in no financial loss **(19%)**
- business email compromise fraud resulting in financial loss **(15%)**
- identity fraud **(11%)**.

Top 10 reporting sectors from incidents reported to ASD's ACSC



The Why : Increasing Impact



Australian Government
Office of the Australian Information Commissioner

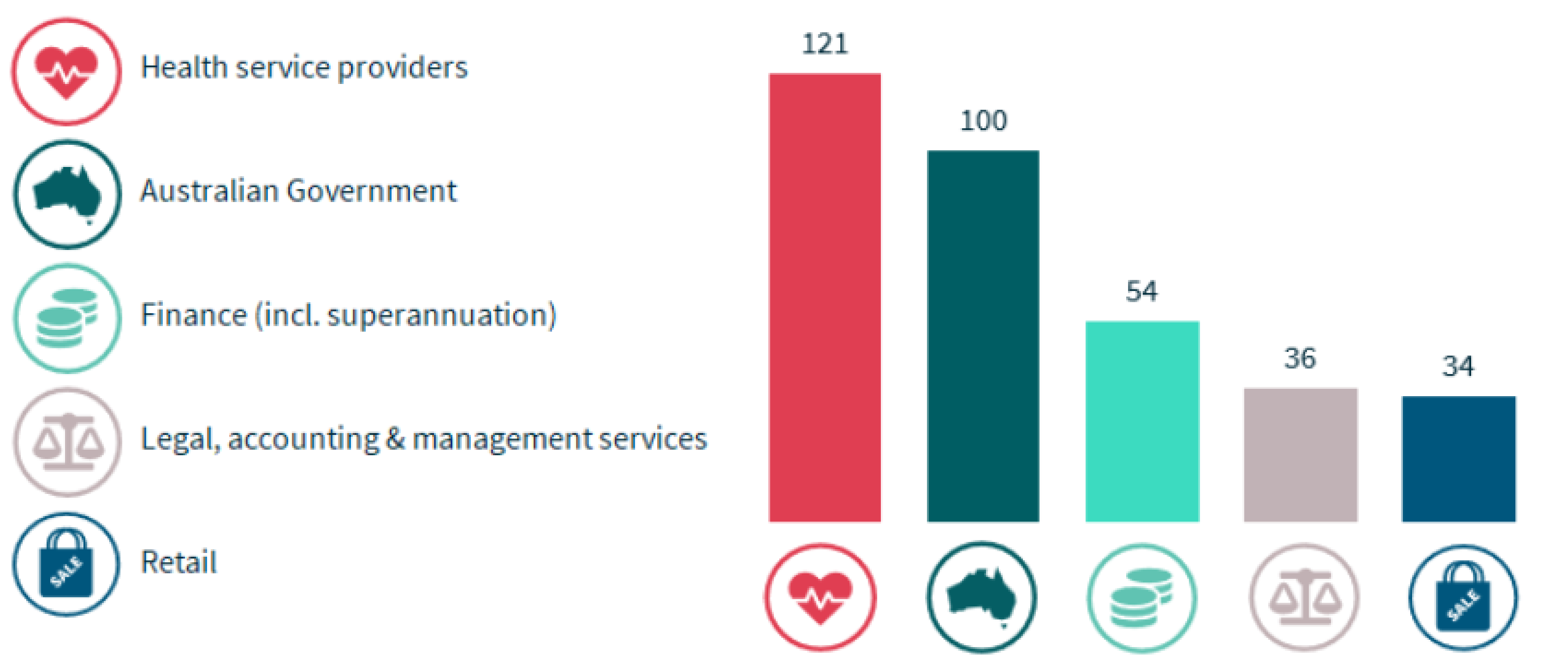
Notifiable data breaches report

July to December 2024

13 May 2025

OAIC

Top 5 sectors to notify data breaches



Malicious or criminal attack

404 ▲

Up 17% from 346

Human error

170 ▲

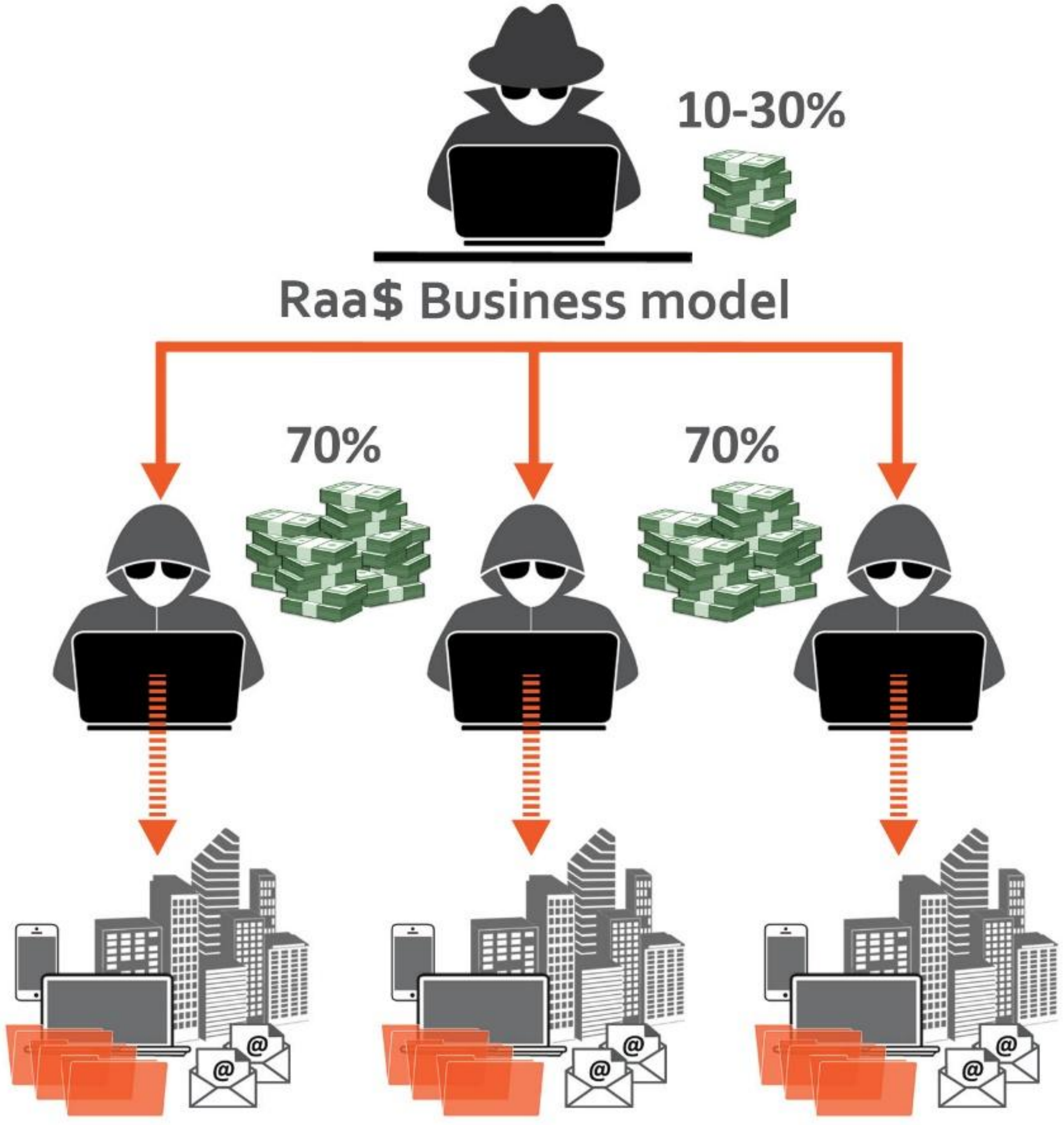
Up 10% from 155

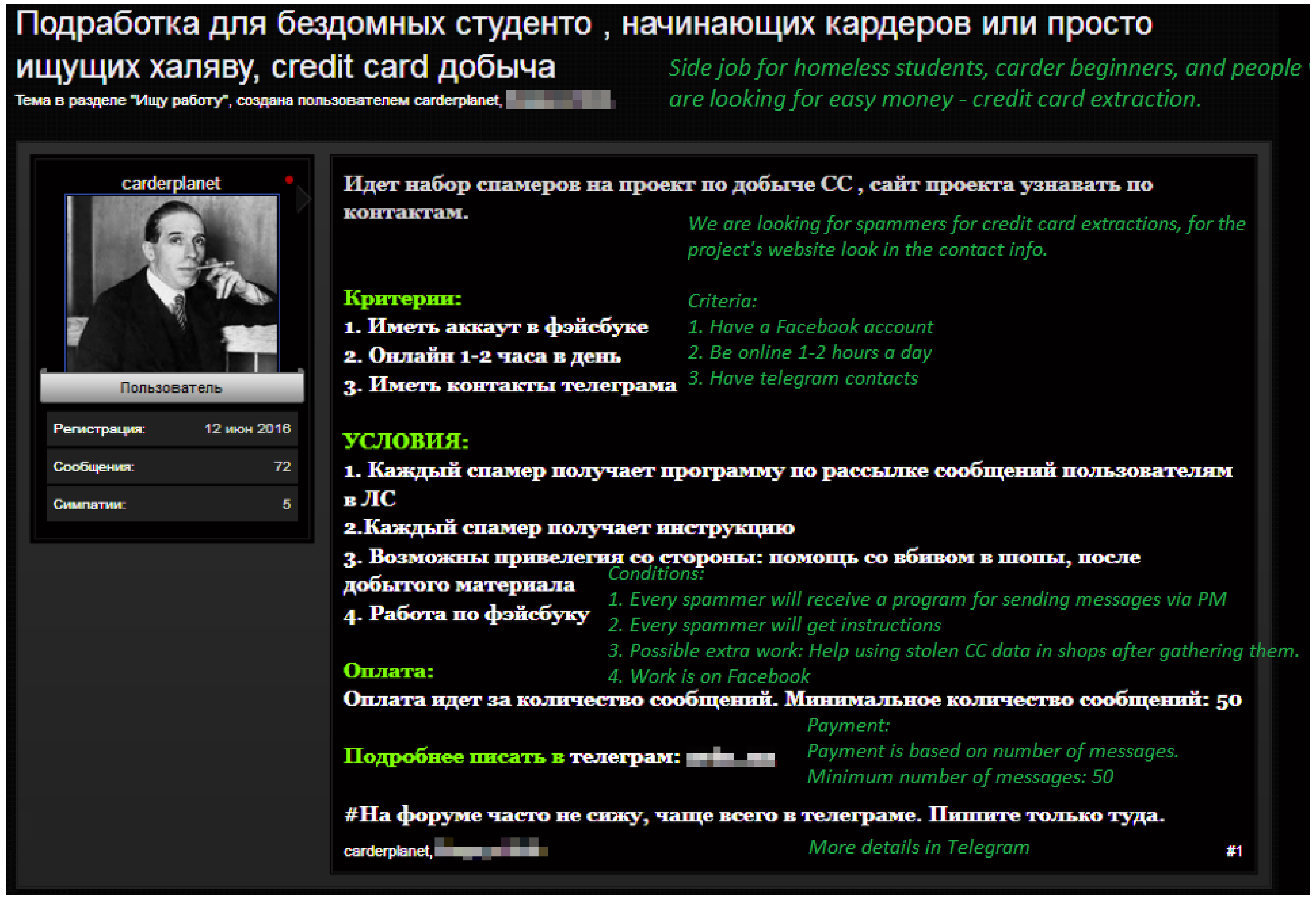
System fault

12 ▼

Down 29% from 17

The Criminal Ecosystem





Подработка для бездомных студенто , начинающих кардеров или просто ищущих халяву, credit card добыча

Side job for homeless students, carder beginners, and people
are looking for easy money - credit card extraction.

Тема в разделе "Ищу работу", создана пользователем carderplanet, [redacted]

carderplanet

Пользователь

Регистрация: 12 июн 2016

Сообщения: 72

Симпатии: 5

Идет набор спамеров на проект по добыче СС , сайт проекта узнавать по контактам.

We are looking for spammers for credit card extractions, for the project's website look in the contact info.

Критерии:
1. Иметь аккаут в фэйсбуке
2. Онлайн 1-2 часа в день
3. Иметь контакты телеграма

Criteria:
1. Have a Facebook account
2. Be online 1-2 hours a day
3. Have telegram contacts

УСЛОВИЯ:
1. Каждый спамер получает программу по рассылке сообщений пользователям в ЛС
2.Каждый спамер получает инструкцию
3. Возможны привелегия со стороны: помощь со вбивом в шопы, после добытого материала
4. Работа по фэйсбуку

Conditions:
1. Every spammer will receive a program for sending messages via PM
2. Every spammer will get instructions
3. Possible extra work: Help using stolen CC data in shops after gathering them.
4. Work is on Facebook

Оплата:
Оплата идет за количество сообщений. Минимальное количество сообщений: 50

Payment:
Payment is based on number of messages.
Minimum number of messages: 50

Подробнее писать в телеграм: [redacted]

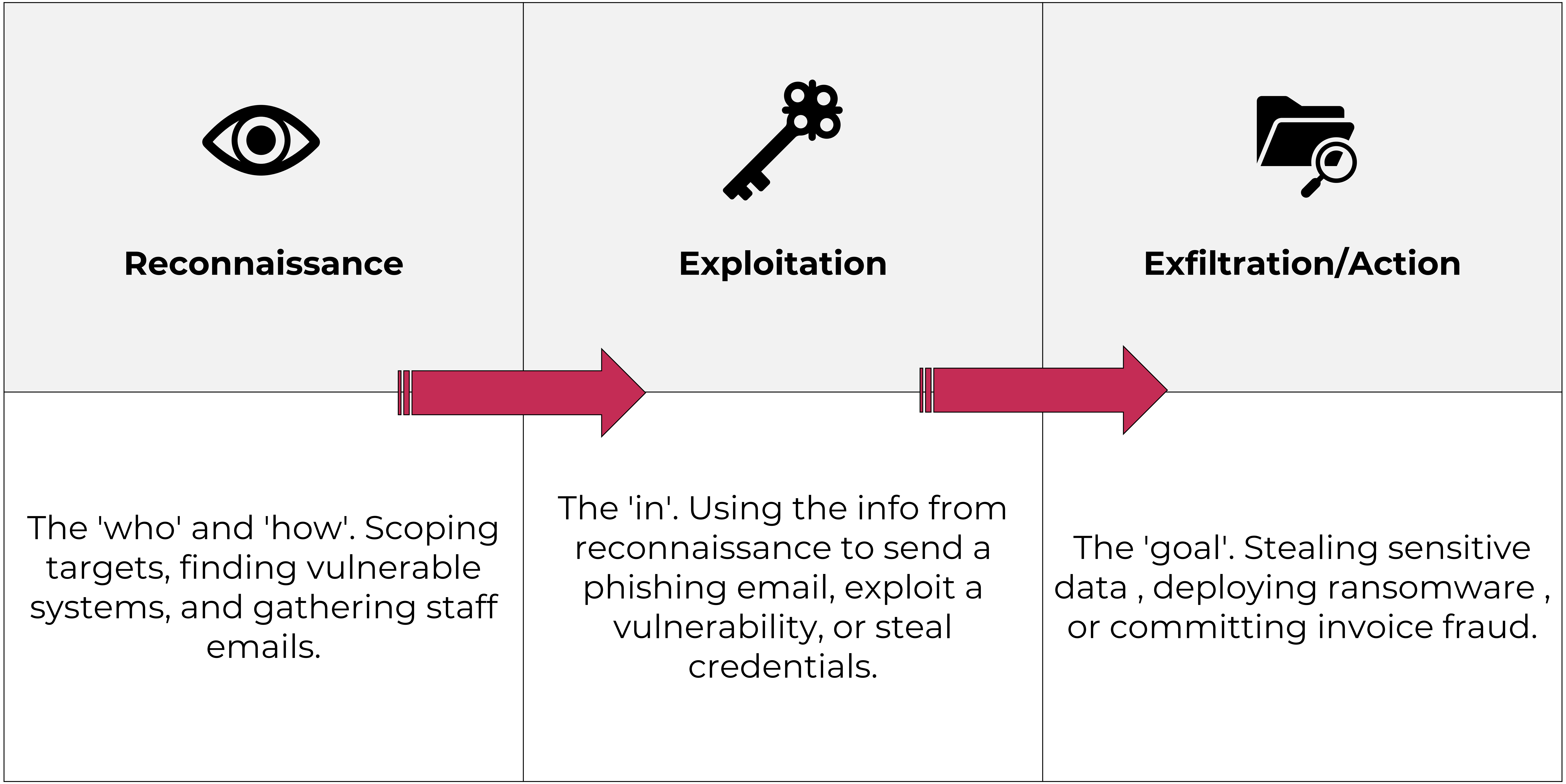
#На форуме часто не сижу, чаще всего в телеграме. Пишите только туда.

More details in Telegram

carderplanet, [redacted]

#1

The Lifecycle of a Cyber Attack



Reconnaissance	Exploitation	Exfiltration/Action
The 'who' and 'how'. Scoping targets, finding vulnerable systems, and gathering staff emails.	The 'in'. Using the info from reconnaissance to send a phishing email, exploit a vulnerability, or steal credentials.	The 'goal'. Stealing sensitive data , deploying ransomware , or committing invoice fraud.

Case Study 1: Business Email Compromise (BEC)

Scenario	Learnings
An attacker, posing as a trusted client, emails a last-minute request to change bank details for an invoice. The firm pays the new, fraudulent account.	The client's funds are lost, and the firm is held accountable. **Always verbally confirm** financial changes using a known, trusted phone number.

Case Study 2: The Insider Threat (Unintentional)

Scenario	Learnings
An employee clicks a malicious link, installing malware. For 3 months, the malware silently exports company emails. This stolen data is then used to create highly convincing new attacks on clients.	One click can lead to a long-term, undetected breach. This gave attackers valuable intelligence to make future scams look legitimate.

Case Study 3: The Identity Threat

Scenario	Learnings
An attacker (**who already has a stolen password**) triggers a login at 5.00 PM on a Friday. This initiatives the MFA "Approve Login" push notifications. The employee, annoyed by the alerts, hits 'Approve' just to make it stop.	The attacker is now in. **MFA is not a silver bullet**; it can be defeated by social engineering or "MFA Fatigue." Always **Deny** unexpected login requests and report them to IT immediately.

Case Study 4: The Rasonmware Threat

Scenario	Learnings
An employee opens a malicious email attachment, launching a ransomware attack. Within an hour, all company servers and critical files are encrypted. A demand for $50,000 in Bitcoin is left.	The business is instantly non-operational. This shows why you need two things: **Cyber Insurance** to cover extortion costs and **offline, tested backups** to restore data without paying.

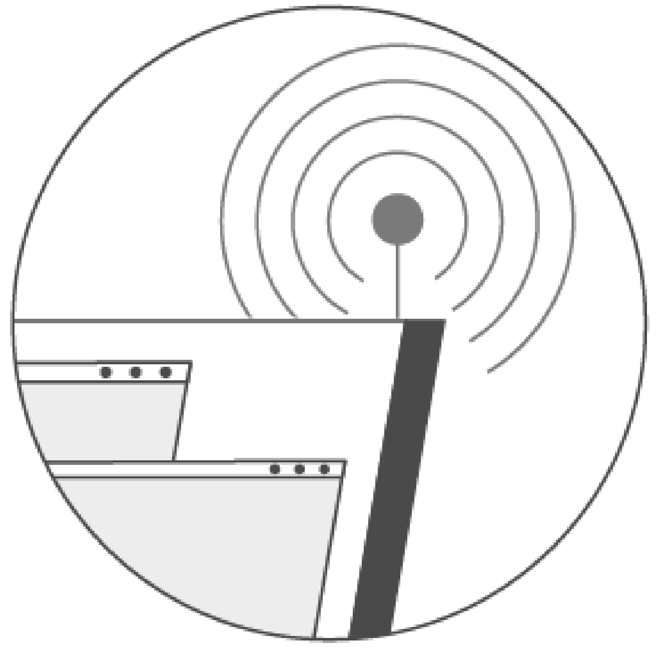
Cyber Resilience Tactics

Multifactor Authentication (MFA)

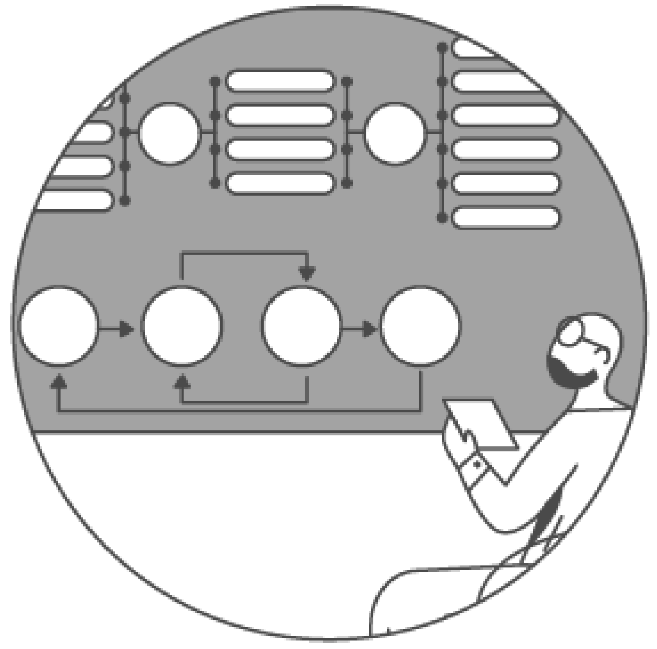
Virtual Private Network (VPN)

Remote Desktop Protocol (RDP)

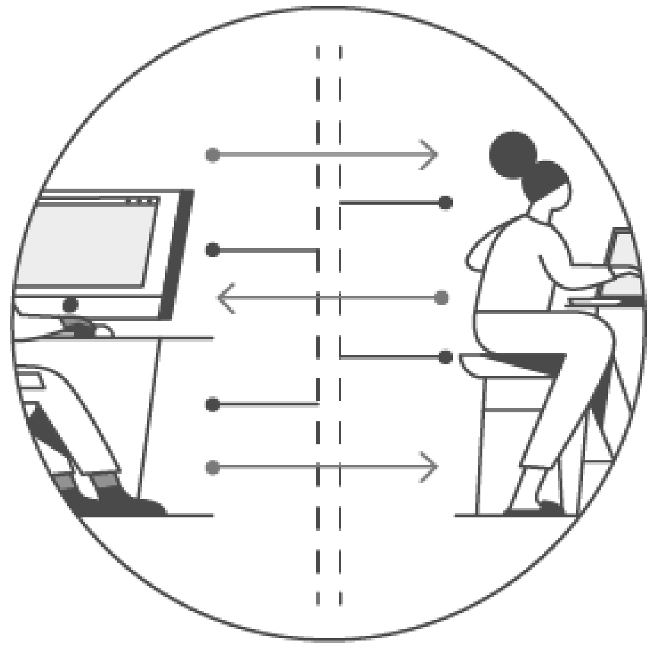
Endpoint Detection and Response (EDR)



Incident Response Planning



Infrastructure and Segmentation



Backups

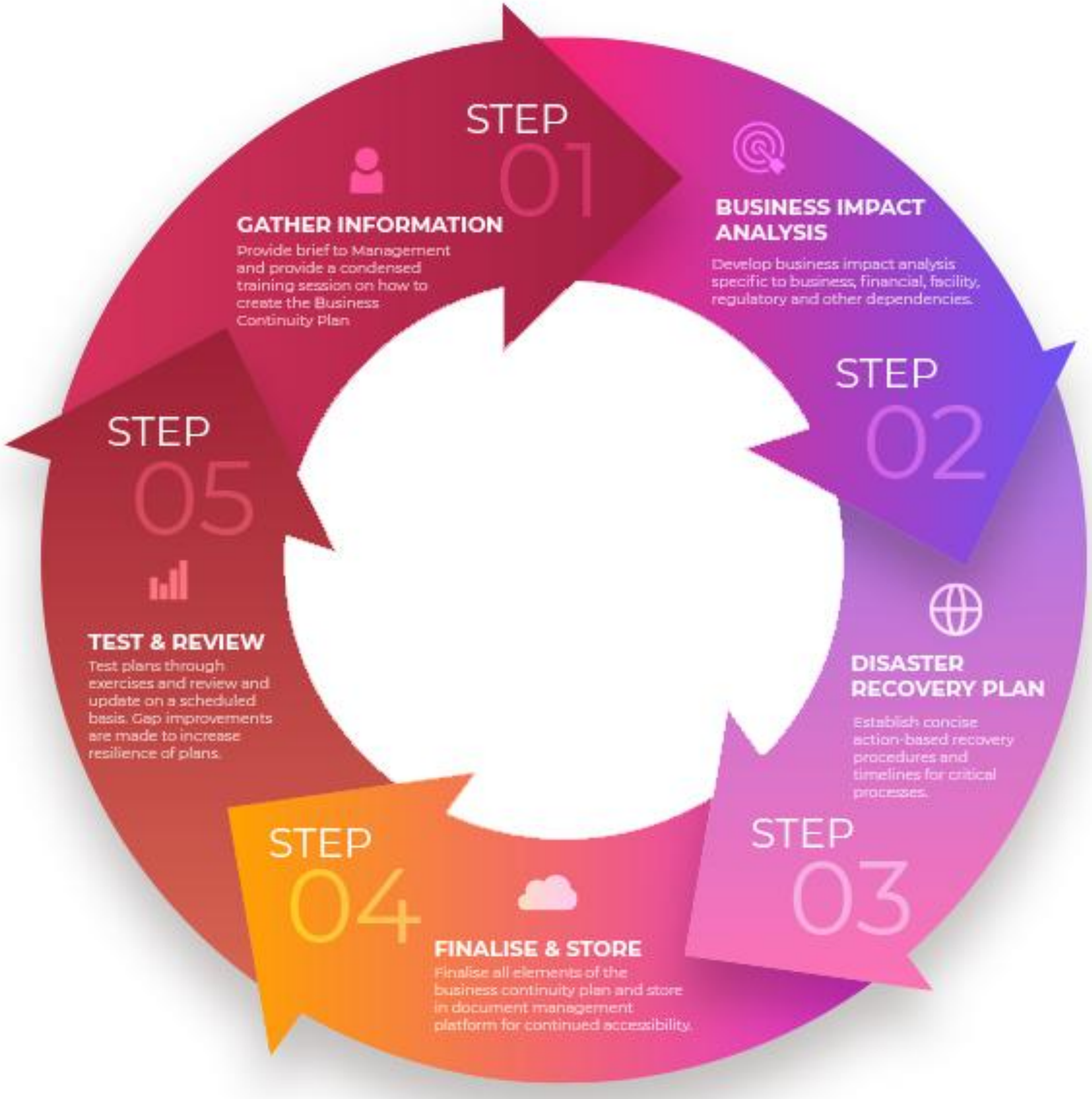
Access Control

Security Culture Training

Email Hygiene

Business Continuity Planning

STRATEGICGROUP
YOUR TRUSTED IT PARTNER



STEP 01

GATHER INFORMATION

Provide brief to Management and provide a condensed training session on how to create the Business Continuity Plan

BUSINESS IMPACT ANALYSIS

Develop business impact analysis specific to business, financial, facility, regulatory and other dependencies.

STEP 02

DISASTER RECOVERY PLAN

Establish concise action-based recovery procedures and timelines for critical processes.

STEP 03

STEP 04

FINALISE & STORE

Finalise all elements of the business continuity plan and store in document management platform for continued accessibility.

STEP 05

TEST & REVIEW

Test plans through exercises and review and update on a scheduled basis. Gap improvements are made to increase resilience of plans.

BUSINESS CONTINUITY: NOW AND INTO THE FUTURE

FUTURE PROOFING YOUR BUSINESS IN AN EVER CHANGING ENVIRONMENT

STRATEGICGROUP
YOUR TRUSTED IT PARTNER

WELCOME

Welcome and thanks for downloading 'Business Continuity: Now and into the future'. This eBook is designed to help you identify why business continuity is important and how you can implement a robust plan in your business.

Recent events such as the spread of COVID-19 have reminded many businesses why it's so important to have a plan in place on how to mitigate risks that arise from things like travel bans and mandatory quarantine procedures.

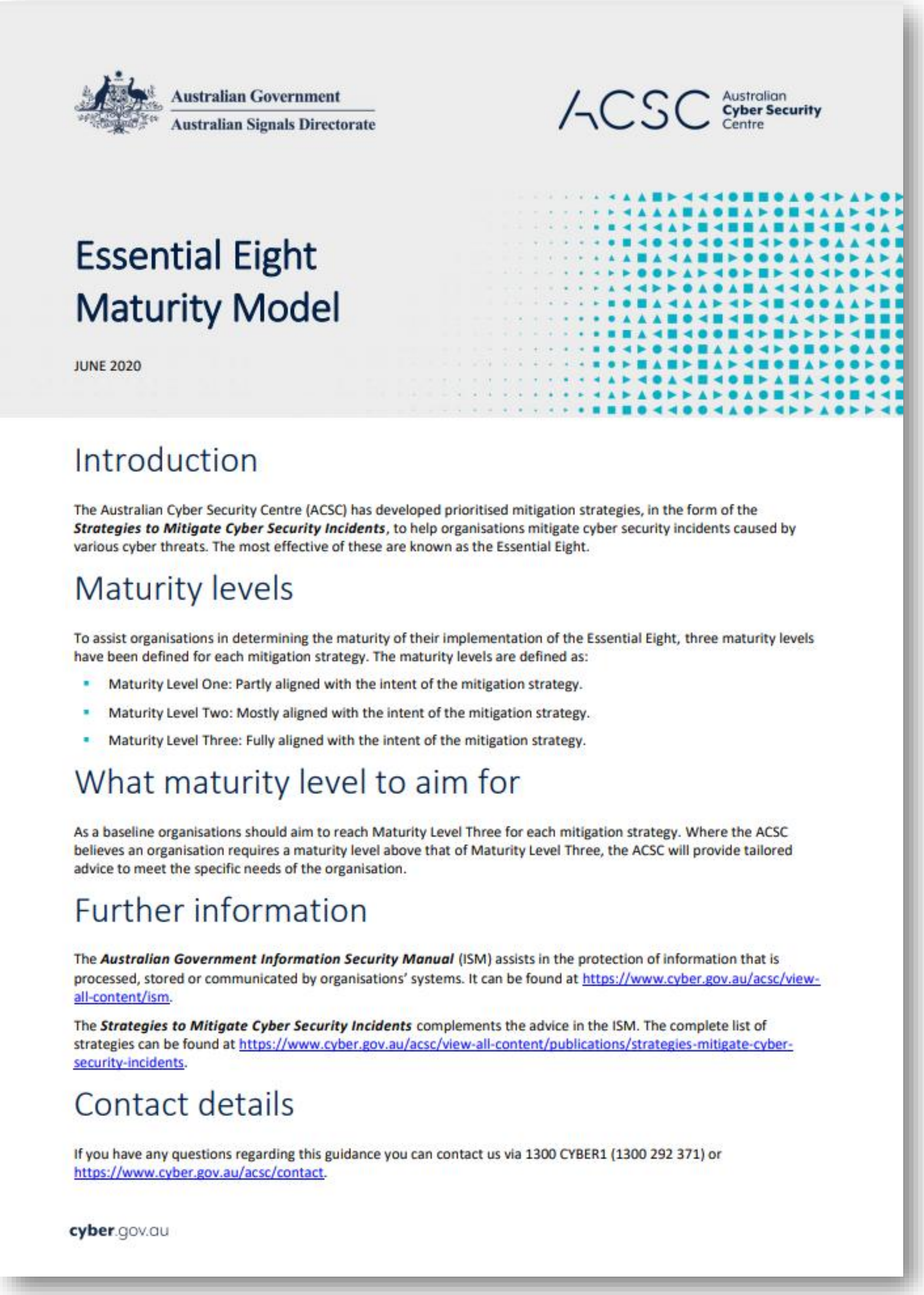
Most disasters don't give advance notice on when they are going to happen, even if there is some warning, events unfold rapidly and can change quickly.

During these events is when a Business Continuity Plan comes into play. An up-to-date, tested plan gives your business the best chance of surviving a disaster. By not having a Business Continuity Plan you are putting considerable risk on your business to not only recover slowly, but perhaps not at all.

Cyber Insurance

First Party Cover	Third Party Cover
• **Crisis Management Expenses** – including notification expenses, legal costs, forensic IT expenses, public relations and credit monitoring expenses. • **Data Recovery Expenses** – costs associated with replacing, restoring and recollecting data. • **Business Interruption Expenses** – loss of business income due to a cyber event. • **Data Extortion Cover** – costs associated with ransomware events.	• **Security & Privacy Liability** – defending claims from third parties, including claim settlements. • **Regulatory Costs** – investigations and resultant fines and penalties issued by regulators. • **Multimedia Liability** – costs associated with copyright and libel/slander type claims.

Governance & Compliance



Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Essential Eight Maturity Model

JUNE 2020

Introduction

The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies, in the form of the ***Strategies to Mitigate Cyber Security Incidents***, to help organisations mitigate cyber security incidents caused by various cyber threats. The most effective of these are known as the Essential Eight.

Maturity levels

To assist organisations in determining the maturity of their implementation of the Essential Eight, three maturity levels have been defined for each mitigation strategy. The maturity levels are defined as:

- Maturity Level One: Partly aligned with the intent of the mitigation strategy.
- Maturity Level Two: Mostly aligned with the intent of the mitigation strategy.
- Maturity Level Three: Fully aligned with the intent of the mitigation strategy.

What maturity level to aim for

As a baseline organisations should aim to reach Maturity Level Three for each mitigation strategy. Where the ACSC believes an organisation requires a maturity level above that of Maturity Level Three, the ACSC will provide tailored advice to meet the specific needs of the organisation.

Further information

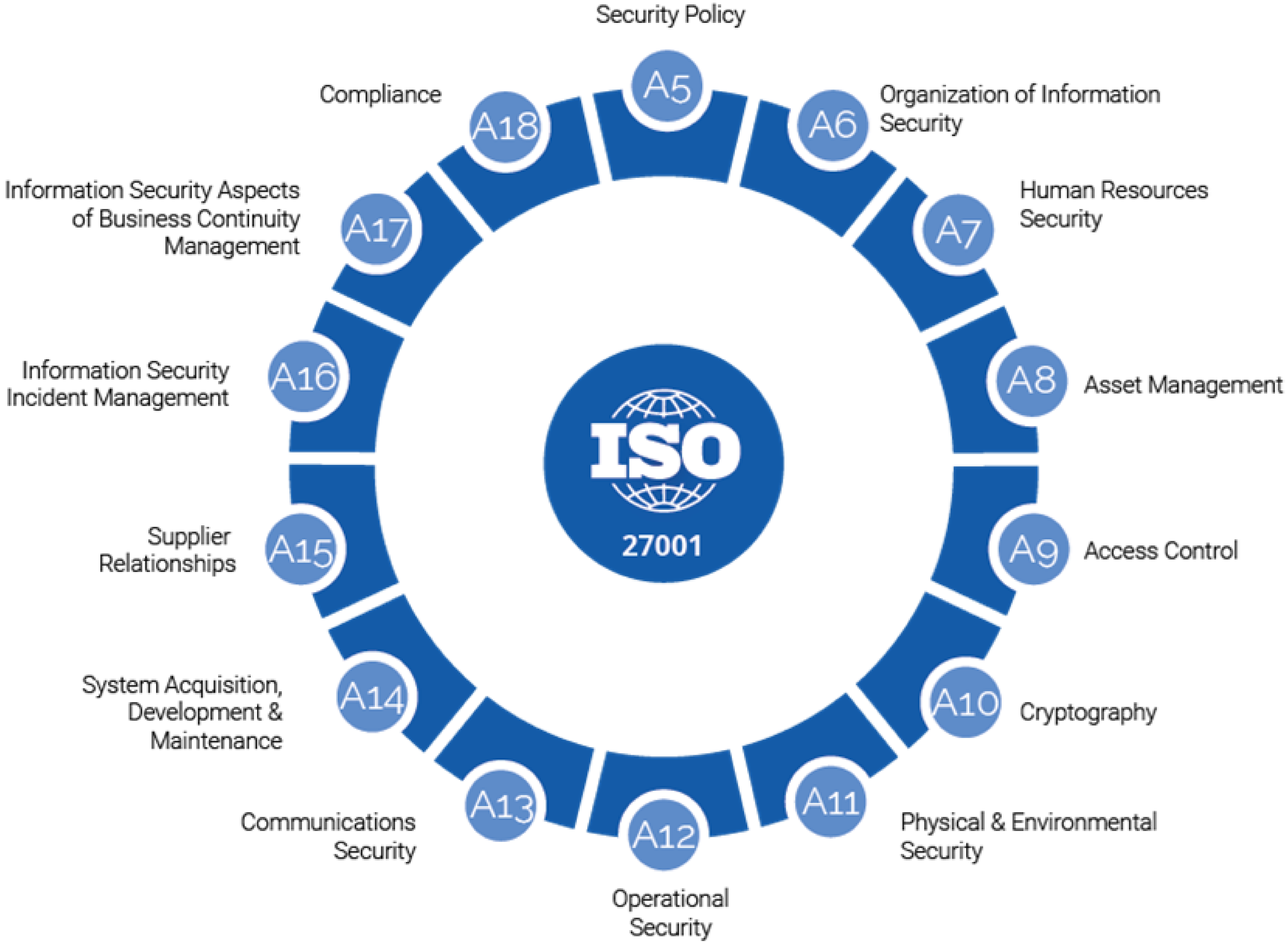
The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/acsc/view-all-content/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents.

Contact details

If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or https://www.cyber.gov.au/acsc/contact.

cyber.gov.au



ISO
27001
A5
Security Policy
A6
Organization of Information Security
A7
Human Resources Security
A8
Asset Management
A9
Access Control
A10
Cryptography
A11
Physical & Environmental Security
A12
Operational Security
A13
Communications Security
A14
System Acquisition, Development & Maintenance
A15
Supplier Relationships
A16
Information Security Incident Management
A17
Information Security Aspects of Business Continuity Management
A18
Compliance

Next Steps: How prepared is your Business ?

A plan is just paper until you test it. We are offering a **hands-on, in-person Incident Response "Fire Drill"** for your leadership and key stakeholders.

The Goal:

Identify your critical gaps, build team muscle memory, and ensure your business can respond effectively to protect your operations, data, and reputation.

What We'll Do:

We will simulate a realistic cyber event and work through the crisis with your team in real-time. Who makes the first call? How do you communicate with staff and clients? When do you engage your insurer? How do you stop the attack from spreading?

Book Your 'Fire Drill' Session:

Visit our page to learn more and register your interest:
https://strategicgroup.net.au/contact/

Open Discussion

Further Reading

STRATEGICGROUP
YOUR TRUSTED IT PARTNER

Evolving Ransomware: Strategies and Insights for Australian Business Resilience

STRATEGICGROUP
YOUR TRUSTED IT PARTNER

Cybersecurity from the breakroom to the boardroom

What is a cyber-aware culture, why it's important, and how to create one.

STRATEGICGROUP
YOUR TRUSTED IT PARTNER

Social Engineering 2.0
Beyond Phishing