Lessons From the Cyber Battle Zone

30th July 2019

ES2

ES2 PEOPLE ES2 KIDS ES2 IR INCIDENT RESPONSE

ES2 Capabilities

ES2
ENTERPRISE SECURITY
ENTERPRISE SOLUTIONS

ES2
MANAGED SERVICES

ES2
ANYTHING CLOUD

ES2
VENDORS

ES2
IR
INCIDENT RESPONSE

ES2 KIDS
By Kids For Kids

ES2 PEOPLE
PERMANENT ■ TEMPORARY ■ CONTRACT

So what's all the fuss about?

February 2017 – Statement from the Australian Privacy and Information Commissioner, Timothy Pilgrim.

Announced the passage of the Privacy Amendment (notifiable Data Breaches) Bill 2016 which establishes a mandatory data breach notification scheme in Australia.

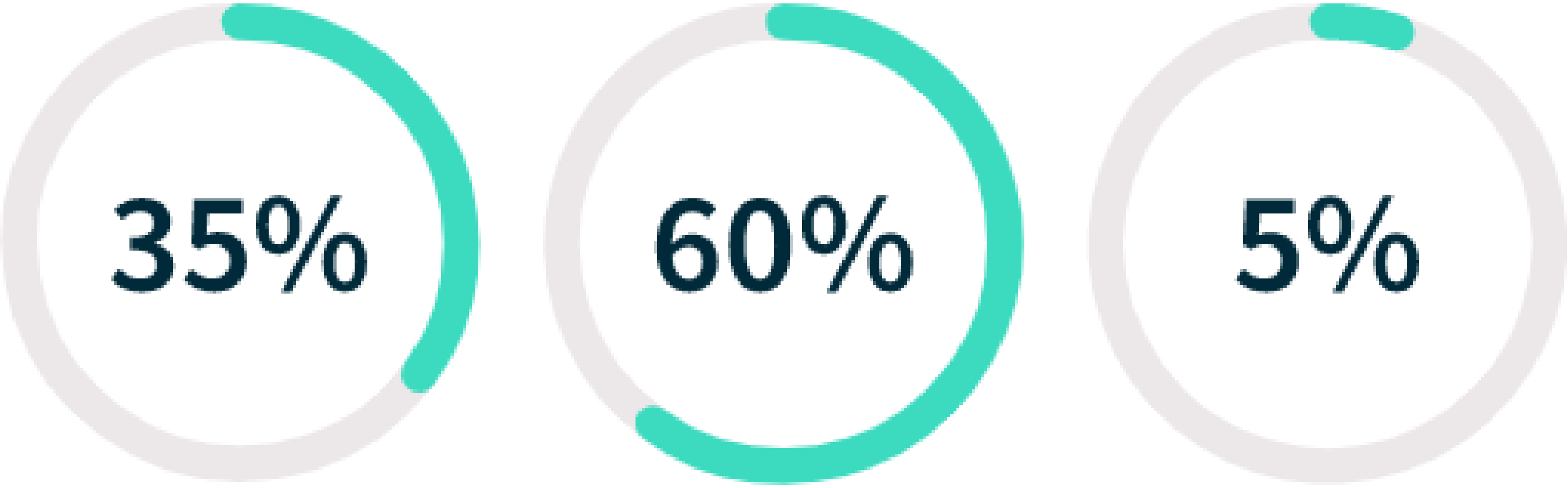
This amendment will require government agencies and businesses covered by the Privacy Act to notify any individuals affected by a data breach that is likely to result in **serious harm** The OAIC will also need to be advised of these breaches and can determine if further action is required. The law also gives the OAIC the ability to direct an agency or business to notify individuals about a **serious breach**

In the meantime, agencies and business should continue to take **reasonable** steps to make sure personal information is held securely – including being equipped with a clear response plan in the event of a data breach.

Obligatory stats slides

964

notifications



35%

human error

60%

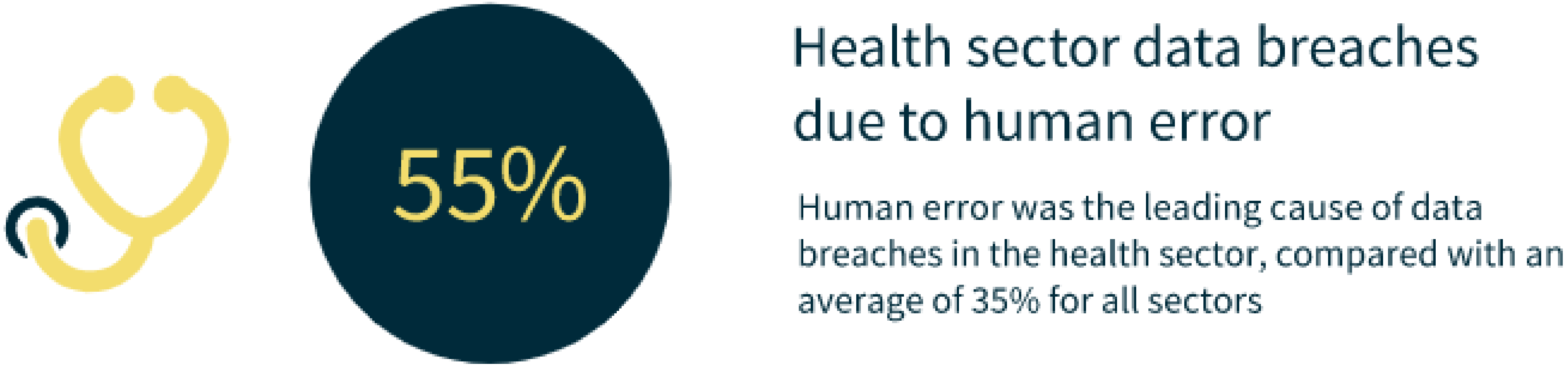
malicious or criminal attacks

5%

system faults

Source – OAIC, 12 Month Insights Report

Obligatory stats slides



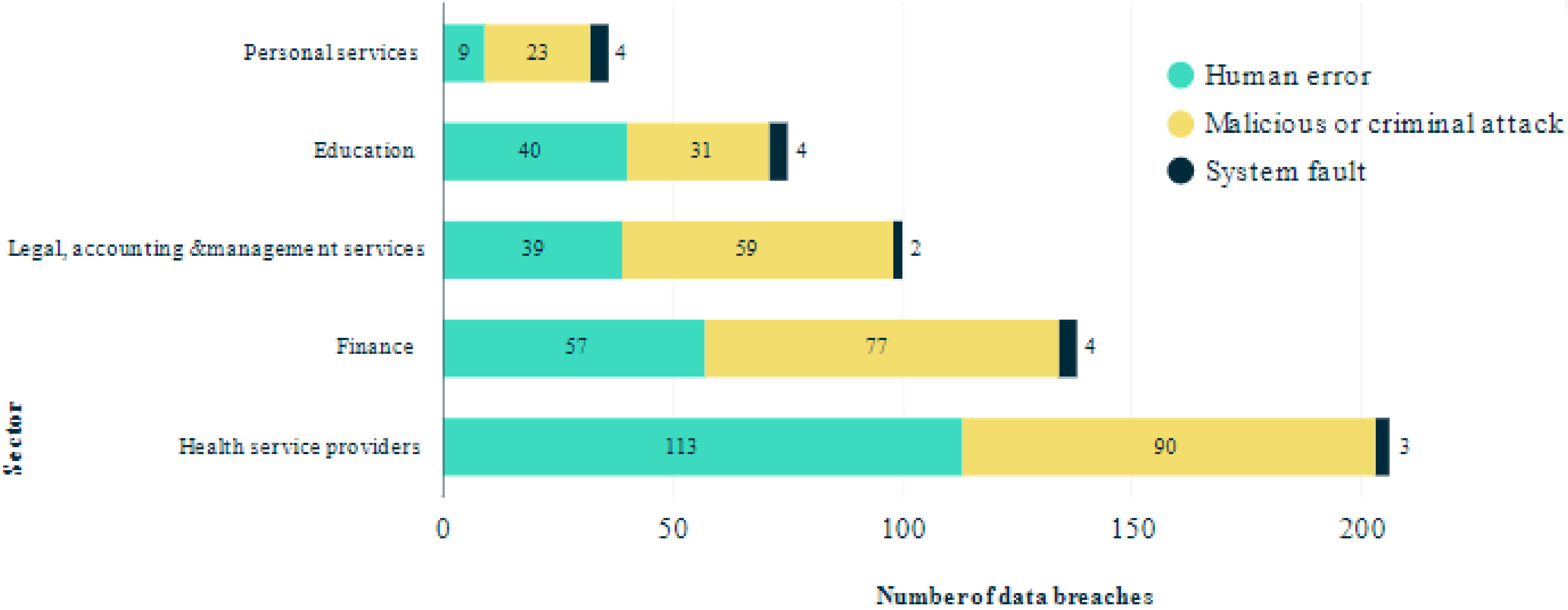
55%

Health sector data breaches due to human error

Human error was the leading cause of data breaches in the health sector, compared with an average of 35% for all sectors

Source – OAIC, 12 Month Insights Report

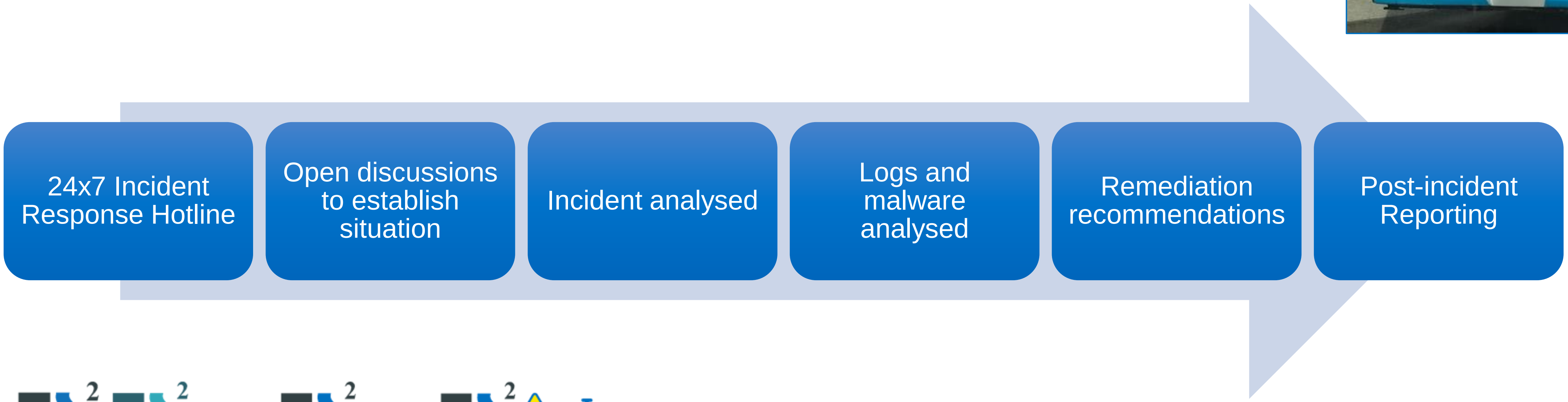
Obligatory stats slides



Source – OAIC, 12 Month Insights Report

ES2 Incident Response Services

1800 373 732
(1800 ES2 SEC)



24x7 Incident Response Hotline

Open discussions to establish situation

Incident analysed

Logs and malware analysed

Remediation recommendations

Post-incident Reporting

ES2 Experience

Man in the Middle

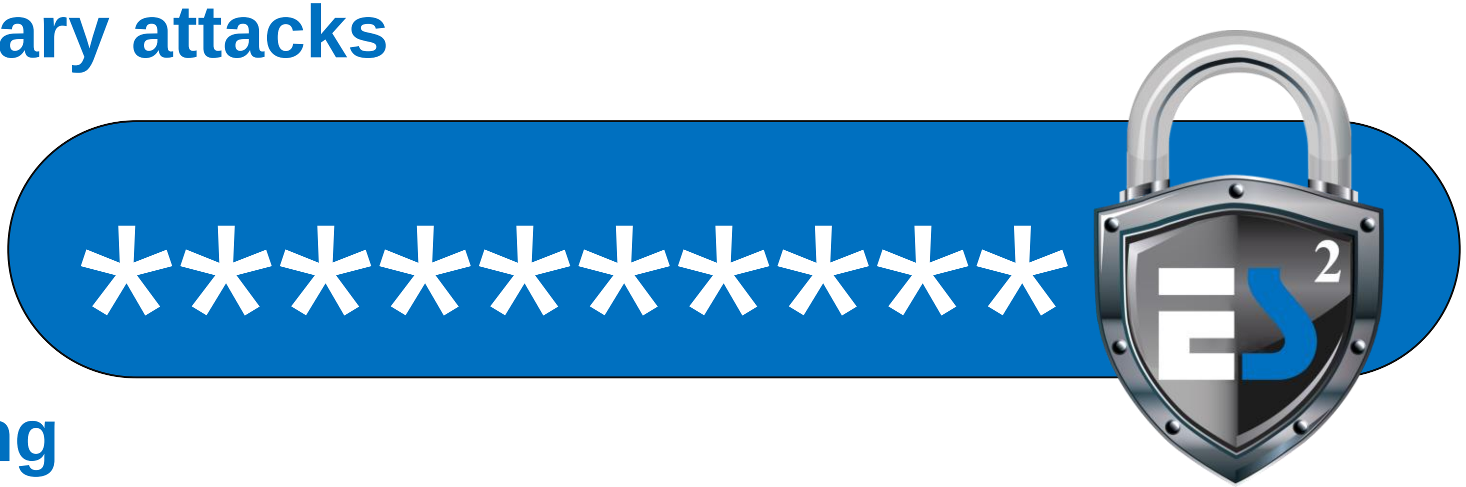
Bruteforce/Dictionary attacks

Phishing

Vishing

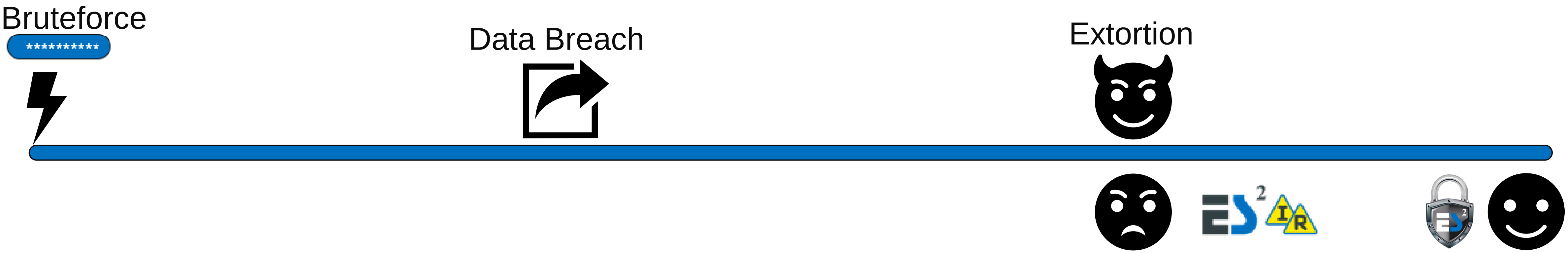
Password Guessing

Poor password management



Incident Scenario 1

Attacker Activity



Bruteforce

****

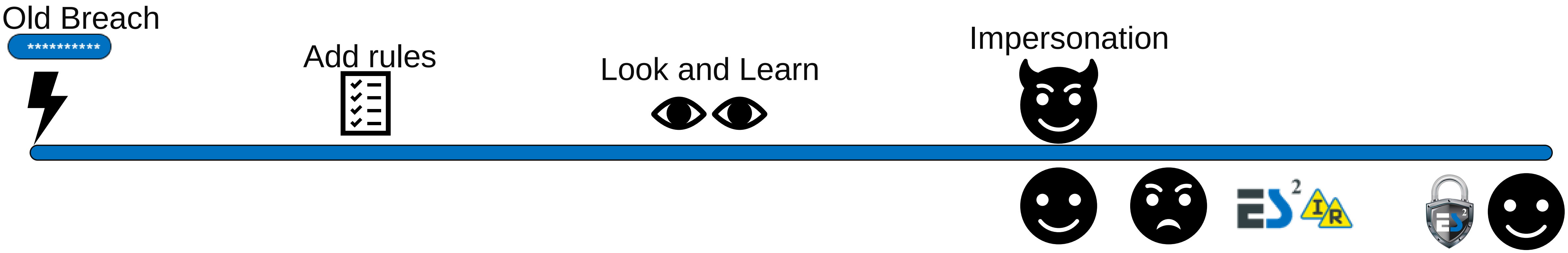
Data Breach

Extortion

Victim Activity

Incident Scenario 2

Attacker Activity



Old Breach

★★★★★★★★★★

Add rules

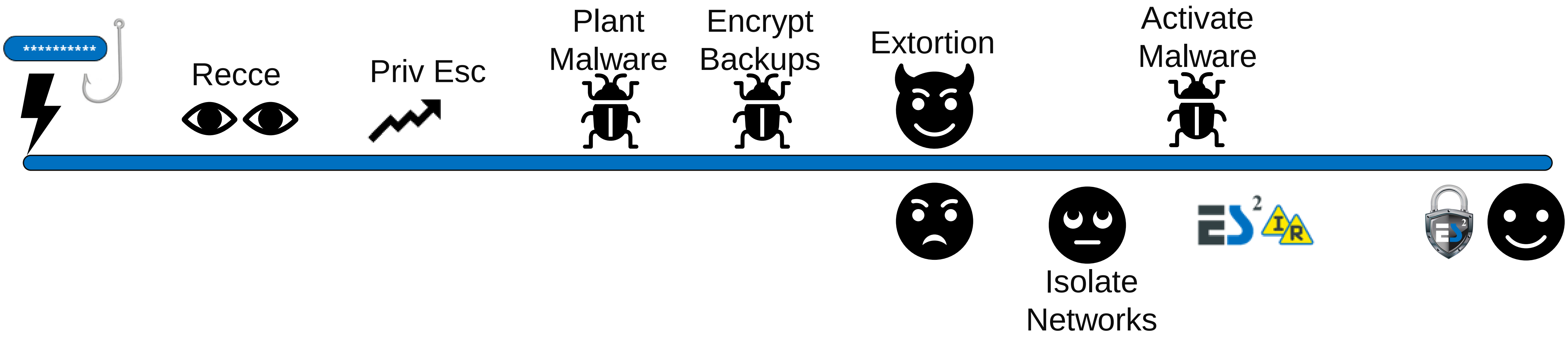
Look and Learn

Impersonation

Victim Activity

Incident Scenario 3

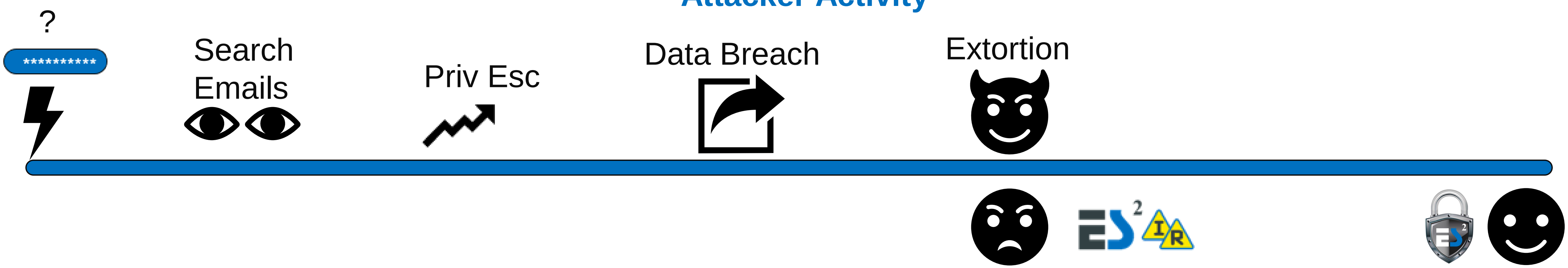
Attacker Activity



Victim Activity

Incident Scenario 4

Attacker Activity



?

****

Search Emails

Priv Esc

Data Breach

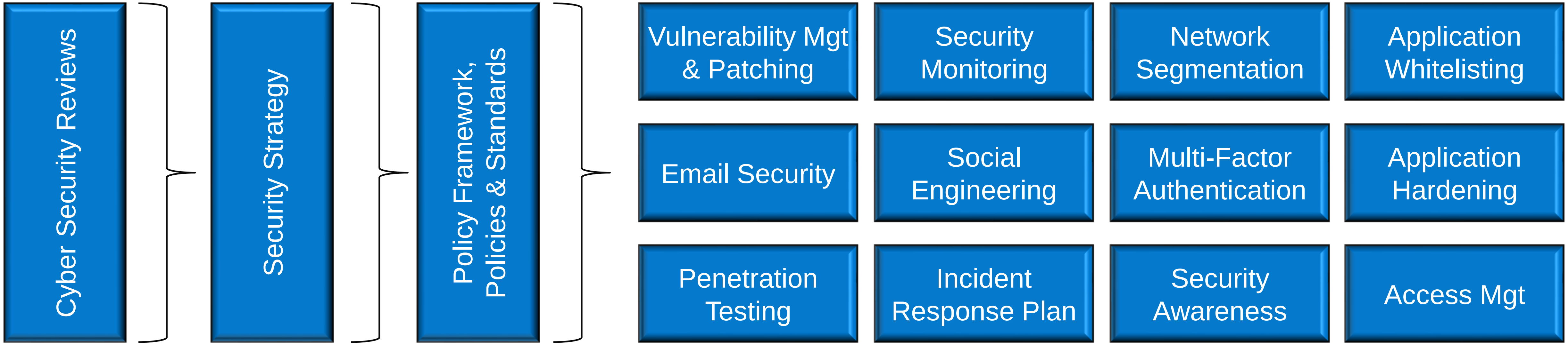
Extortion

Victim Activity

Lessons Learnt

- Maintaining a minimum of 90 days worth of resilient System and/or Data Backups will reduce the impact of a Cyber Attack.
- Implementing Multi-Factor Authentication to avoid Account takeovers and Impersonation attacks.
- Enable Centralised Logging and Alarms to prevent tampering and assist in investigations
- Restricting Outbound Internet Access from Privilege Users and Business Servers makes it harder for Threat Actors to exfiltrate data and download additional tools.
- Start monitoring the Dark Web for exposed Corporate Accounts and company data to provide faster response times.

Cyber Security Proposed Roadmap



Cyber Security Reviews

Security Strategy

Policy Framework, Policies & Standards

Vulnerability Mgt & Patching

Security Monitoring

Network Segmentation

Application Whitelisting

Email Security

Social Engineering

Multi-Factor Authentication

Application Hardening

Penetration Testing

Incident Response Plan

Security Awareness

Access Mgt

Dark Web

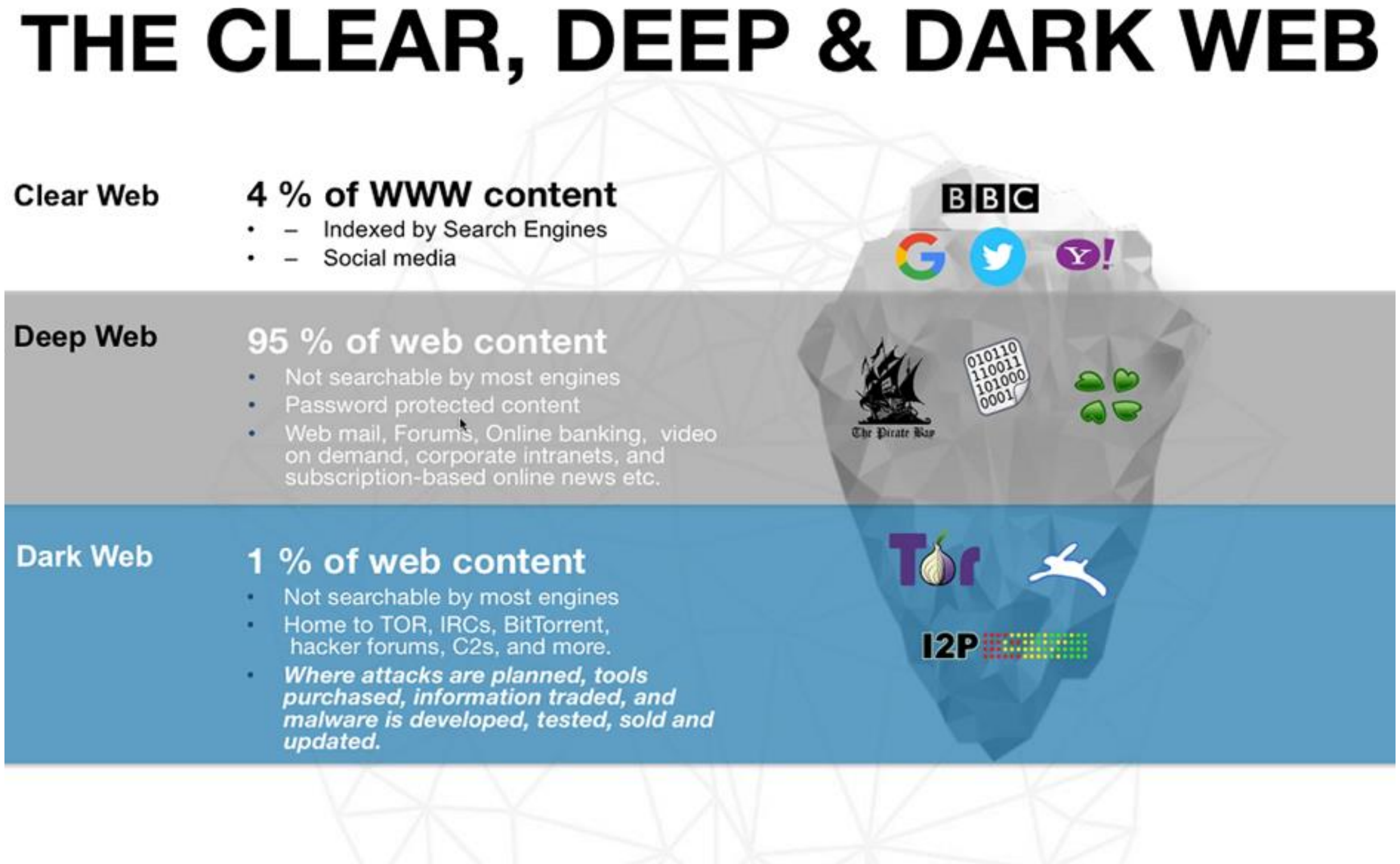
Usernames/Password

Hacked Accounts

Remote Access

Company Data

Privacy Data



THE CLEAR, DEEP & DARK WEB

Clear Web

4 % of WWW content

- – Indexed by Search Engines
- – Social media

Deep Web

95 % of web content

- Not searchable by most engines
- Password protected content
- Web mail, Forums, Online banking, video on demand, corporate intranets, and subscription-based online news etc.

Dark Web

1 % of web content

- Not searchable by most engines
- Home to TOR, IRCs, BitTorrent, hacker forums, C2s, and more.
- ***Where attacks are planned, tools purchased, information traded, and malware is developed, tested, sold and updated.***

Upcoming Cyber Event

THE WORLD'S MOST RESPECTED CYBER SECURITY EXPERT

KEVIN MITNICK LIVE IN PERTH

Kevin Mitnick Live Crown Casino, Perth
10th-11th October 2019 Don't Miss Out!

Founder - Silvana Macri

STAYCYBERSAFE

01 THE ENTERPRISE FIGHTS BACK

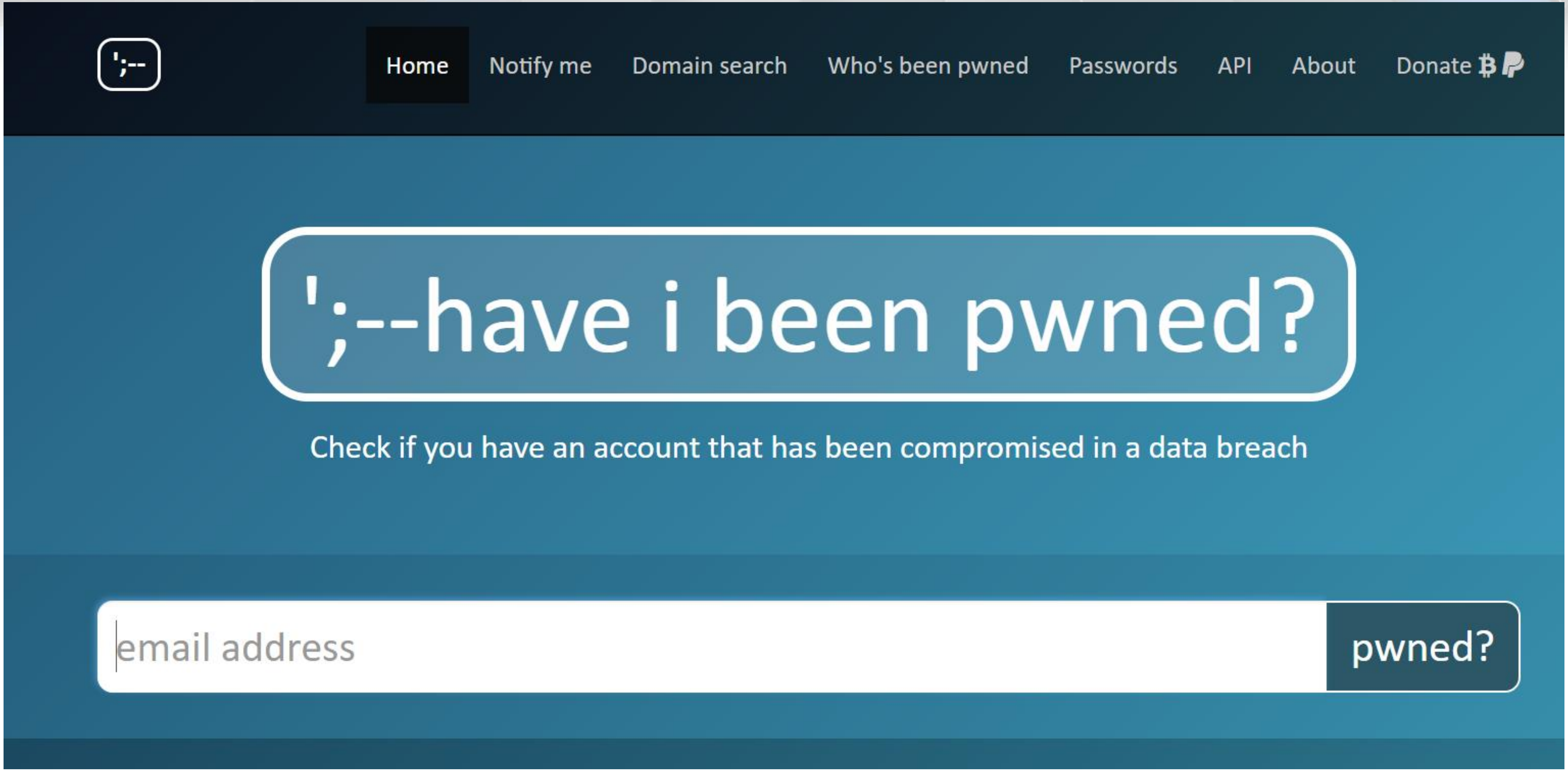
02 FROM BLACK HAT TO WHITE HAT

03 CxO LUNCH

04 2019 WESTERN AUSTRALIAN CYBER SECURITY AWARDS

Book Your Tickets NOW! – wacyberawards.com.au
Tickets Starting from $15 (plus GST/fees)

Have I Been Pwned



Check if you have an account that has been compromised in a data breach

ES2 Kids

By Kids For Kids

ES2 Kids is a Not-for-Profit Foundation that assists in bridging the gap of Cyber Security Awareness for K-12 kids.

ES2 Kids focus is to facilitate Cyber Security Awareness from the Private and Government sectors to K-12 kids (and their parents …)

By Kids For Kids

ES2 Kids Q+A

Steve Simpson, Heidi Drouin & Aidyn Bassett

Thank you

Fred@ES2.com.au

Steve@ES2.com.au

Info@ES2kids.com.au