StewartBrown
Integrity + Quality + Clarity

Speaker: Stuart Hutcheon

(Partner - StewartBrown)

Cyber Crime & IT Fraud

Could your aged care service survive if it lost $5,000? $50,000? Or $1 million overnight?

StewartBrown
Integrity + Quality + Clarity

Contents and Outline

- Overview
- History
- Categories of Cyber Crime
- Types of Cyber Crime
- Prevention and Cyber Security
- Current Case Studies

Overview

The 5 most cyber attacked industries

1. **Healthcare**
2. Manufacturing
3. Financial Services
4. Government
5. Transportation

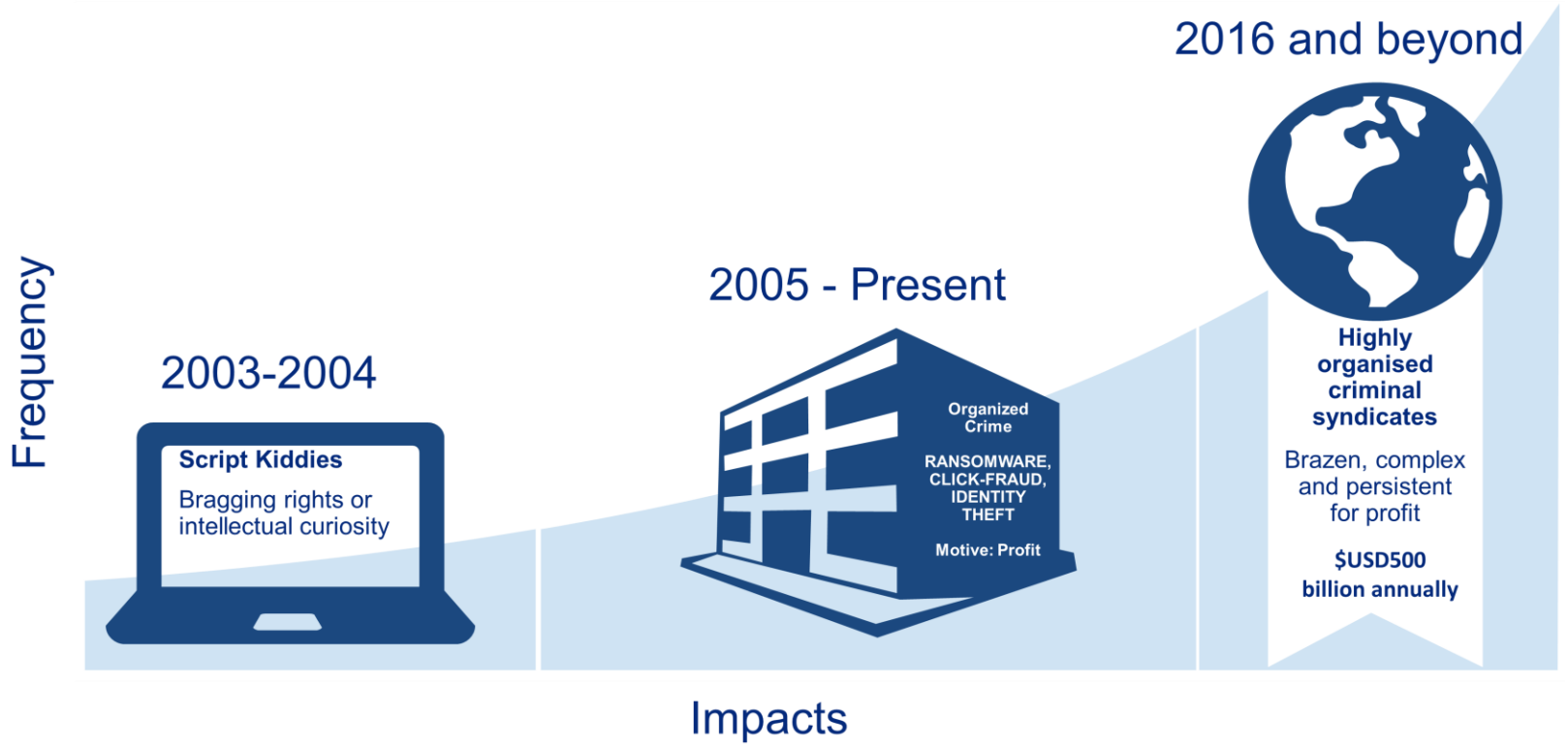
"Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the ***speed, convenience and anonymity of the Internet*** *to commit a diverse range of criminal activities that know no borders, either physical or virtual"* – Interpol

1. **The Computer as a weapon**
   - Using a computer to commit real world crime
   - Cyber terrorism and credit card fraud.

2. **The Computer as a target**
   - Using a computer to attack another computer
   - Forms of Hacking, Dos attack, virus/ worm attacks

History

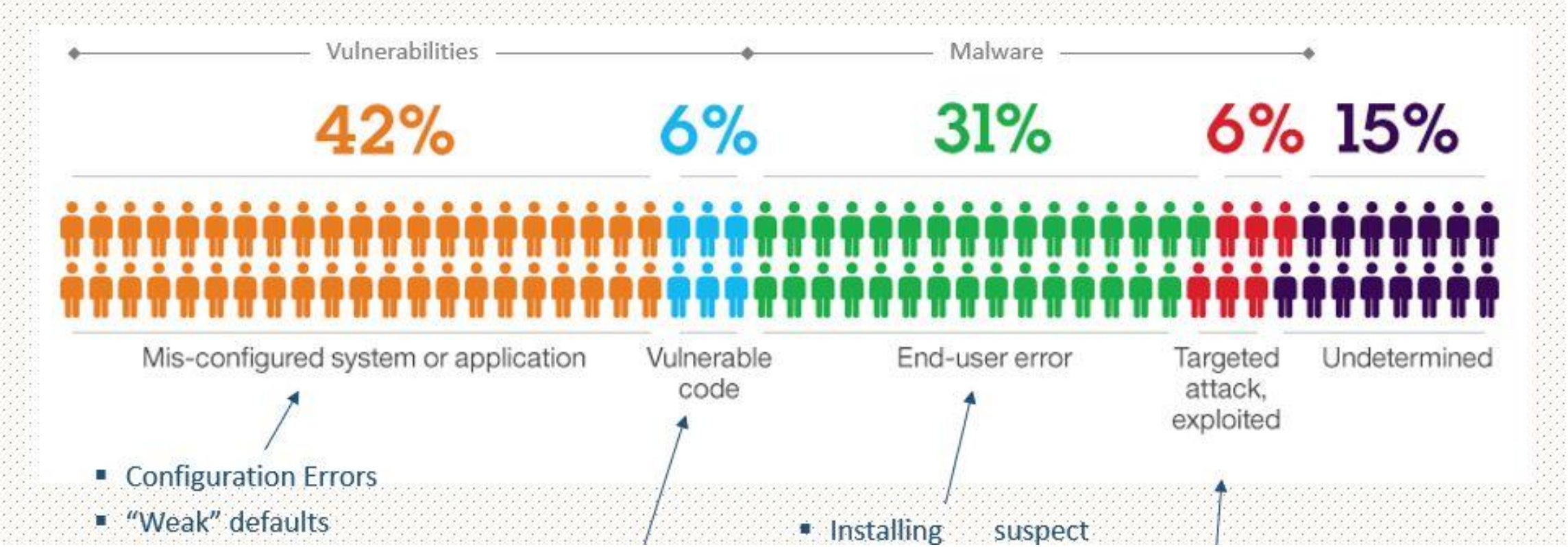
- **1820** - First recorded cybercrime
- **1978** - The first spam e-mail
- **1982** - The first virus was installed on an Apple computer



Types of Cyber Crime

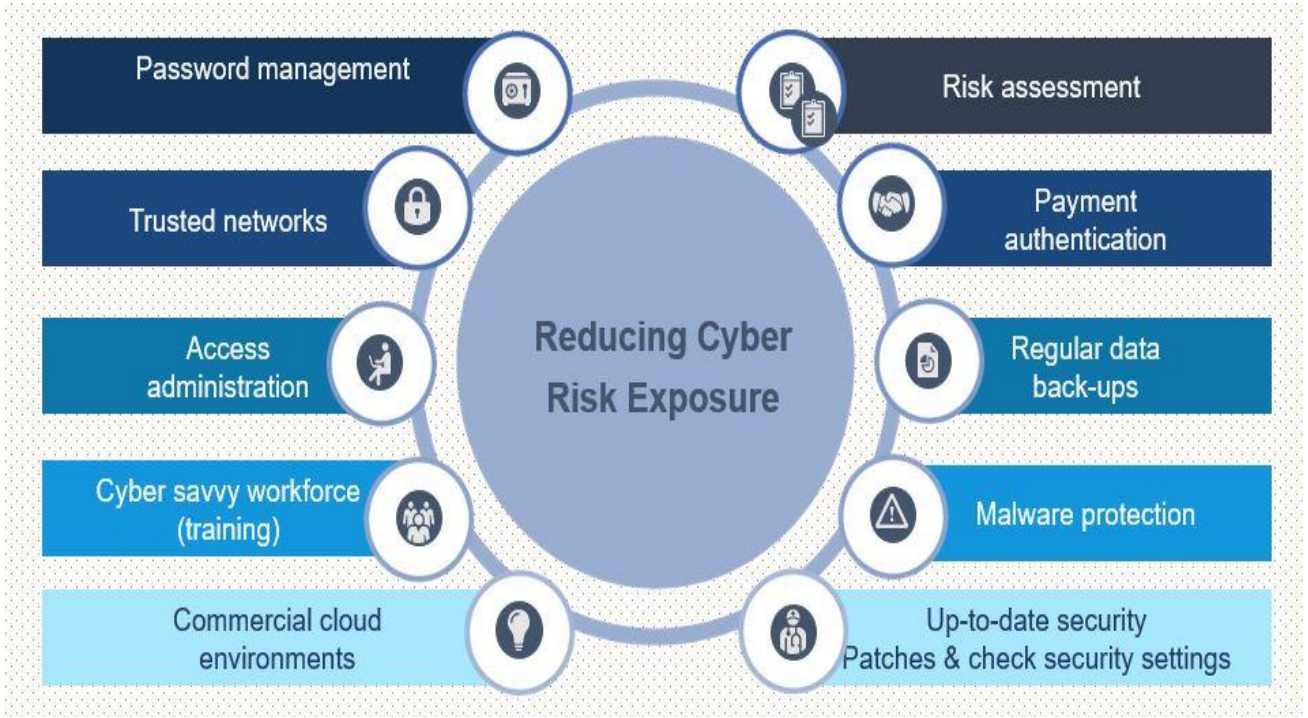
1. **Hacking (credit card)**
2. Denial of Service Attacks
3. **Identity theft**
4. Virus Dissemination
5. **Computer Vandalism**
6. Cyber Terrorism
7. **Online Fraud**
8. Software Piracy
9. Forgery
10. Malicious Code
11. Malware
12. **Phishing**
13. Spam
14. Spoofing
15. Defamation

WHY DO BREACHES OCCUR?



Prevention and Cyber Security

- Firewalls
- Operating system is up-to-date
- Up-to-date anti-virus and anti-spyware
- Use a pop-up advertising blocker
- Use strong passwords
- Secure wireless network
- Reputable websites and mobile applications
- Avoid clicking on unexpected or unfamiliar links



CASE STUDY A

$90k Phishing email – fake CEO

- Finance manager received an email from the ‘CEO’ while the CEO was on leave holidaying in Asia
- The email asked the FM to transfer $90k to an account held with the Bank of China
- There was back and forth between the FM the ‘CEO’ regarding the details of payment
- FM prepared all of the relevant documentation and took this to the CFO for approval for payment. The payment was made

Issue - Email – was very strange and clearly fake

Result - This was a total breakdown of control at a human level, rather than inadequate IT systems.

CASE STUDY B

Client X - Incident 1

- Customer Gmail account was hacked, invoice was sent to a customer for $15k with fraudulent bank details
- The customer paid the $15k to the fraudulent bank account
- Client wore the cost and police are investigating
- **Customer is now transitioning to Microsoft outlook – Being a more secure email provider**

Incident 2

- A supplier email was hacked and the same situation as above occurred in reverse
- The supplier invoice was send to our client for approx. 3K and client paid
- The payment was based off the bank details listed on the invoice (being fraudulent).
- The supplier will wear this cost and our client is not out of pocket
- **A process of checking master supplier bank details has been implemented prior to paying any invoices in order to mitigate this risk**

CASE STUDY C

Client Y:

- Client was processing a refund to a resident for $12k
- During processing through internet banking as hacker watched on remotely
- The internet banking screen was actually a layover (fake) screen and as such the banking details typed in by the finance manager never hit the internet banking site
- The hacker entered different bank details in for the transfer
- They paid the full 12K to an incorrect bank account without knowing
- While the hacker was in their internet banking, he changed the account numbers of saved accounts, including staff super funds and employee bank details
- The bank refunded the money, the account numbers were corrected and an IT review was conducted to identify holes in the IT system

CASE STUDY D

Client Z

- $1million is stolen
- Board members and accountants email hacked
- Changed term deposit instructions
- Bank admitted fault and refunded client

- Purchase cybercrime insurance;
- Engage an IT auditor to review the security of your IT system;
- Educate staff on cybercrime and encourage them to remain vigilant in regard to the risks around emails requesting payment or containing links; and
- Strict use of only official email addresses by all Directors for conducting of entity related business.

Recommendations