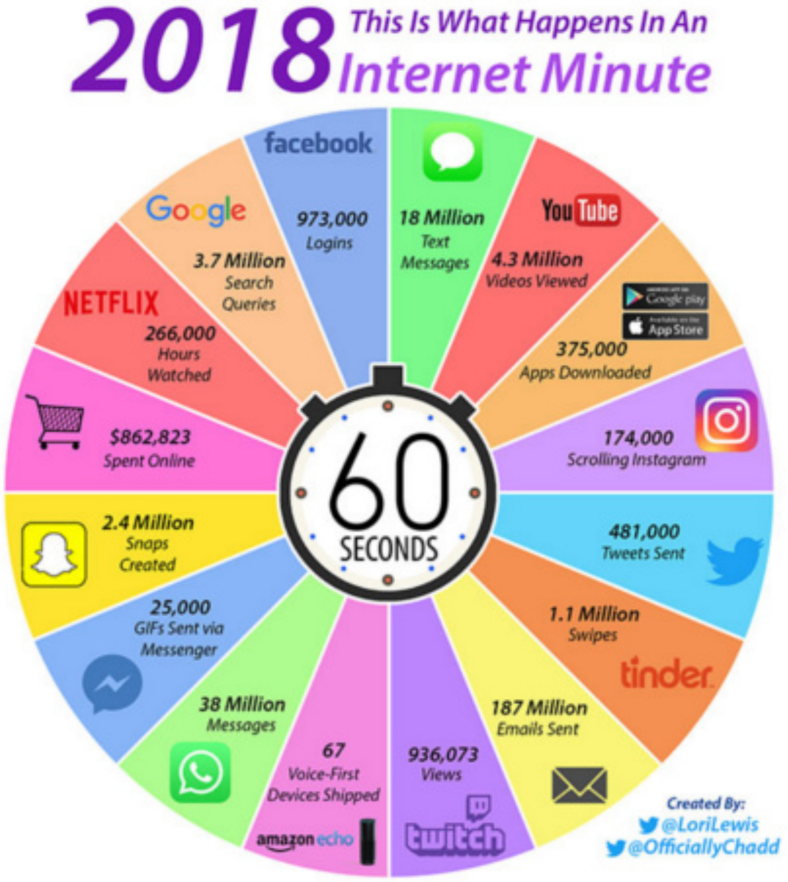
# CYBER SECURITY: 3 THINGS EVERY BOARD SHOULD KNOW

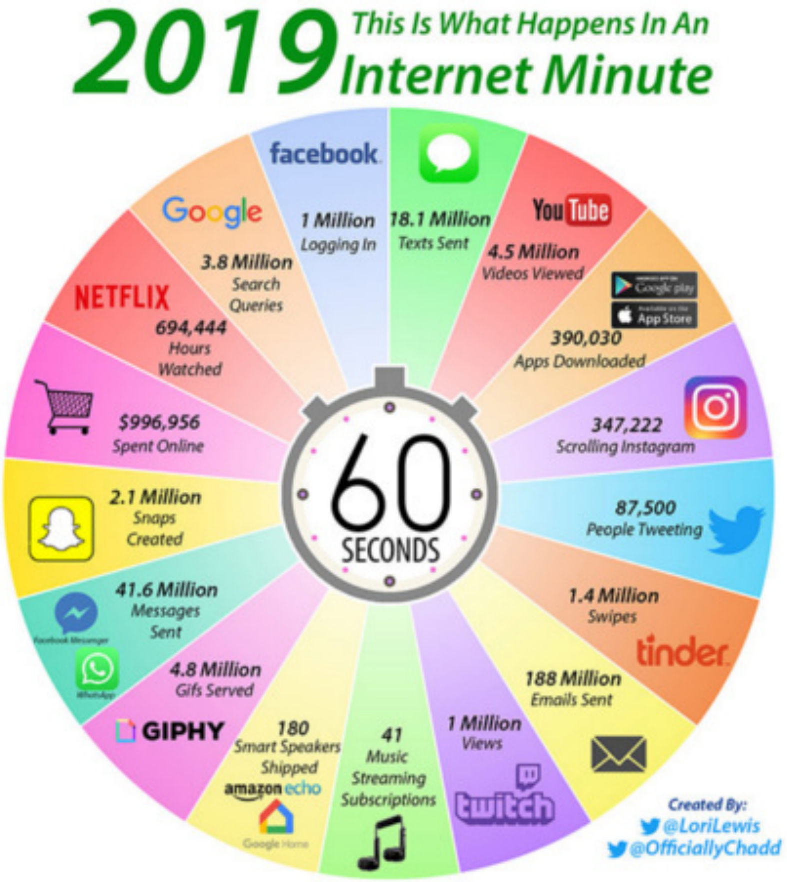
Simon Whittaker

Cyber Security Director - Vertical Structure Ltd

# Prepare, Protect, Persist ®

- **Prepare**
- We help you and your partners to understand how to identify and resolve potential security issues at the earliest stages with hands on 'hack yourself first', threat modelling and GDPR compliance workshops as well as security training for non-technical colleagues.
- **Protect**
- Using automated and manual penetration testing techniques, we provide a comprehensive security report for your Web and mobile applications, including API testing, and networks. The report highlights potential issues and their resolutions.
- **Persist**
- We ensure that your organisation benefits from continual improvements in security levels through information assurance processes, auditing and certification including ISO27001:2013 and Cyber Essentials.





http://www.visualcapitalist.com/internet-minute-2018/

simon.whittaker@verticalstructure.com

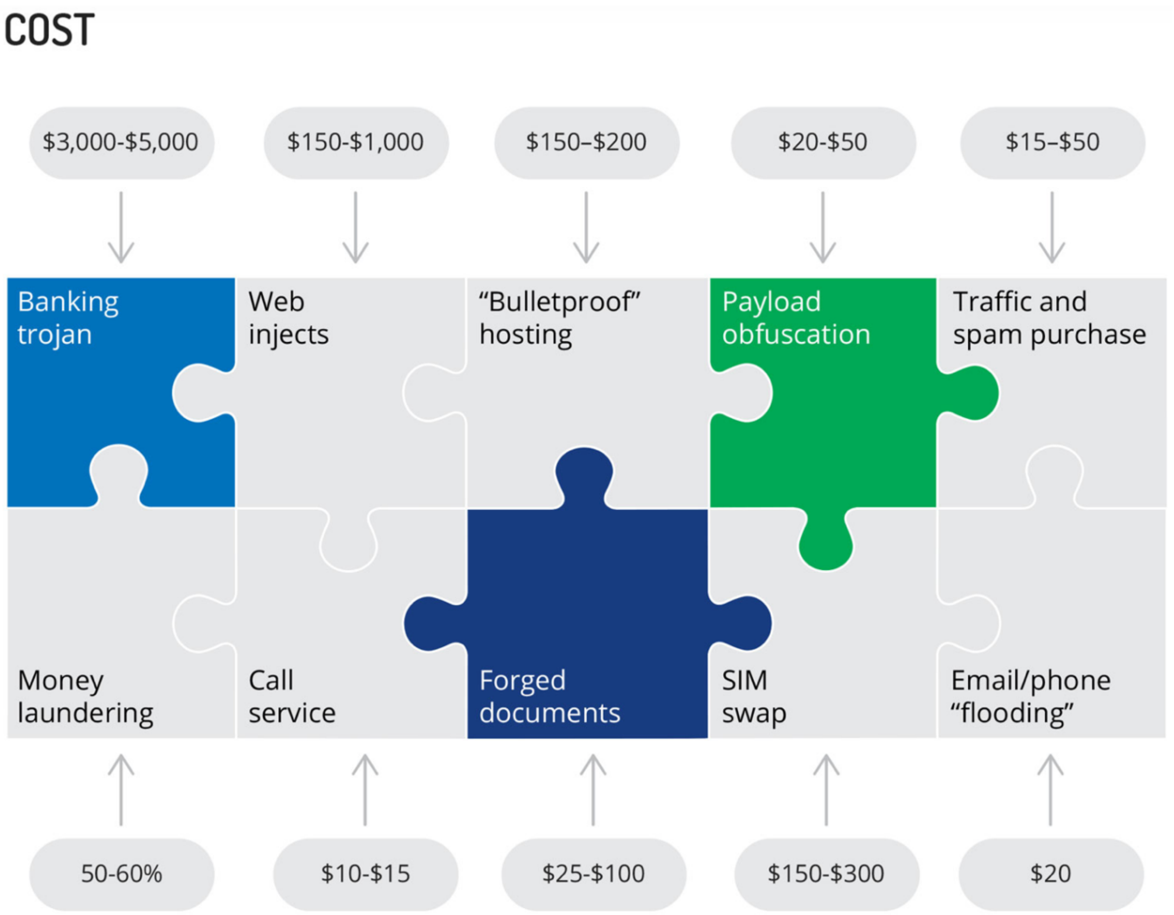
# Security Breaches through the ages

- ‘Target’ stores in November 2013
  - 40 million customer records stolen
- ‘Neiman Marcus’ during 2013
  - Millions affected
- ‘Home Depot’ in September 2014
  - 56 million credit card details stolen
- ‘JPMorgan Chase’ data breach during 2014
  - 76 million households and 7 million small businesses
- ‘Sony Pictures’ hack in November 2014
  - Massive amounts of confidential internal information
- OPM – June 2015
  - Included 5.6 million finger prints

- Ashley Madison – July 2015
- Talk Talk – November 2015
- LinkedIn – revealed May 2016
  - 117 million user details
- Dropbox – revealed August 2016
  - 68 million user details
- Yahoo – revealed Dec 2016
  - 1 billion user details...
- Equifax - September 2017
- Butlins – August 2018
- Exactis – June 2018
- British Airways – September 2018

https://www.privacyrights.org/data-breaches

# Cyber Operations Cost

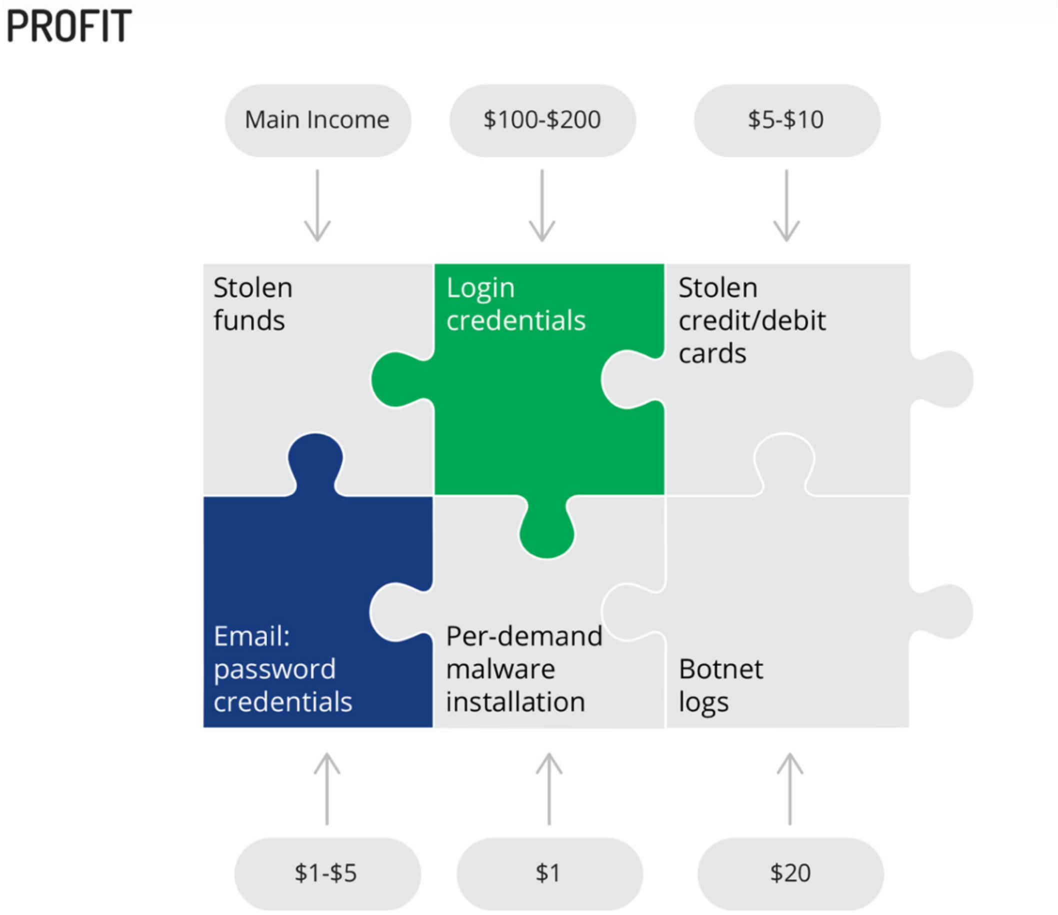


## COST

| | | | | |
|---|---|---|---|---|
| $3,000-$5,000 | $150-$1,000 | $150–$200 | $20-$50 | $15–$50 |
| Banking trojan | Web injects | "Bulletproof" hosting | Payload obfuscation | Traffic and spam purchase |
| Money laundering | Call service | Forged documents | SIM swap | Email/phone "flooding" |
| 50-60% | $10-$15 | $25-$100 | $150-$300 | $20 |

Source: https://www.recordedfuture.com/cyber-operations-cost/

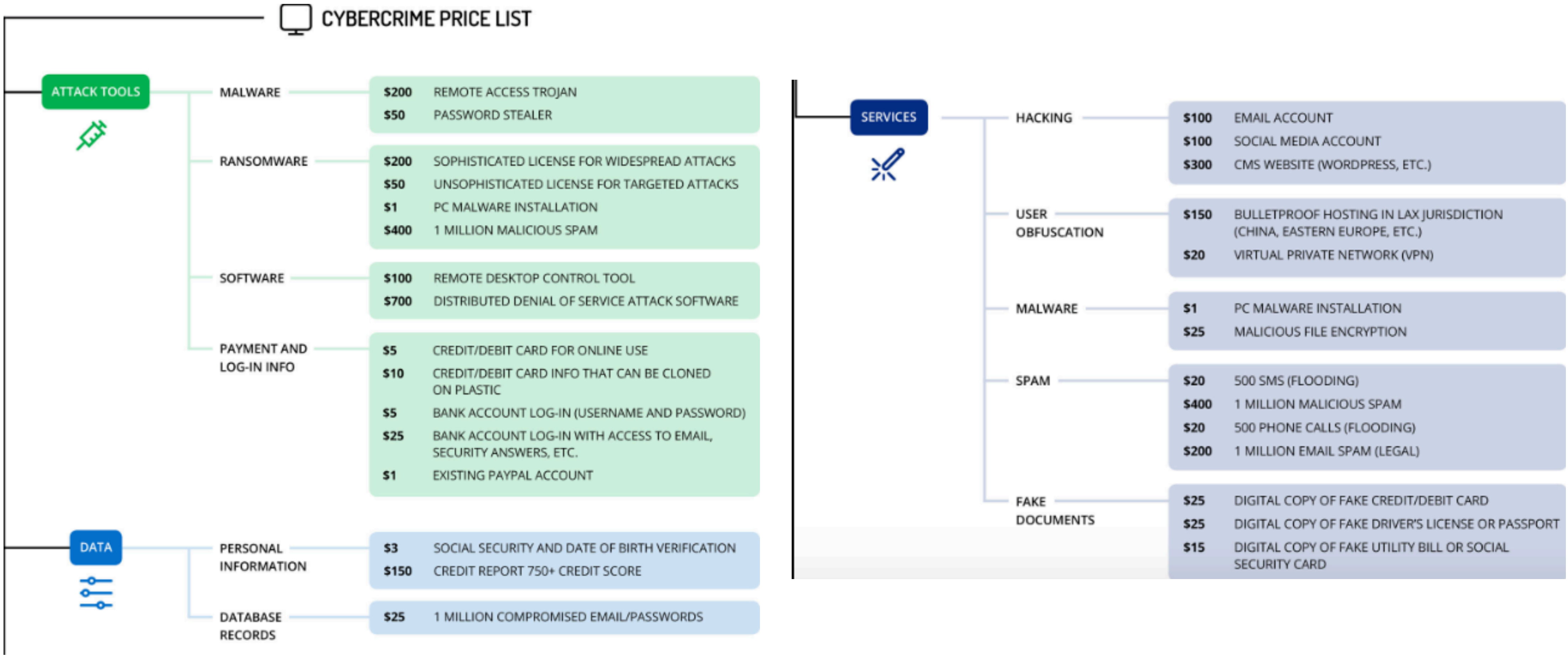
# Cyber Operations Cost


PROFIT
Main Income
$100-$200
$5-$10
Stolen funds
Login credentials
Stolen credit/debit cards
Email: password credentials
Per-demand malware installation
Botnet logs
$1-$5
$1
$20

Source: https://www.recordedfuture.com/cyber-operations-cost/

simon.whittaker@verticalstructure.com

# Cybercrime price list



CYBERCRIME PRICE LIST

| | | | |
|---|---|---|---|
| ATTACK TOOLS | MALWARE | $200 | REMOTE ACCESS TROJAN |
| | | $50 | PASSWORD STEALER |
| | RANSOMWARE | $200 | SOPHISTICATED LICENSE FOR WIDESPREAD ATTACKS |
| | | $50 | UNSOPHISTICATED LICENSE FOR TARGETED ATTACKS |
| | | $1 | PC MALWARE INSTALLATION |
| | | $400 | 1 MILLION MALICIOUS SPAM |
| | SOFTWARE | $100 | REMOTE DESKTOP CONTROL TOOL |
| | | $700 | DISTRIBUTED DENIAL OF SERVICE ATTACK SOFTWARE |
| | PAYMENT AND LOG-IN INFO | $5 | CREDIT/DEBIT CARD FOR ONLINE USE |
| | | $10 | CREDIT/DEBIT CARD INFO THAT CAN BE CLONED ON PLASTIC |
| | | $5 | BANK ACCOUNT LOG-IN (USERNAME AND PASSWORD) |
| | | $25 | BANK ACCOUNT LOG-IN WITH ACCESS TO EMAIL, SECURITY ANSWERS, ETC. |
| | | $1 | EXISTING PAYPAL ACCOUNT |
| DATA | PERSONAL INFORMATION | $3 | SOCIAL SECURITY AND DATE OF BIRTH VERIFICATION |
| | | $150 | CREDIT REPORT 750+ CREDIT SCORE |
| | DATABASE RECORDS | $25 | 1 MILLION COMPROMISED EMAIL/PASSWORDS |
| SERVICES | HACKING | $100 | EMAIL ACCOUNT |
| | | $100 | SOCIAL MEDIA ACCOUNT |
| | | $300 | CMS WEBSITE (WORDPRESS, ETC.) |
| | USER OBFUSCATION | $150 | BULLETPROOF HOSTING IN LAX JURISDICTION (CHINA, EASTERN EUROPE, ETC.) |
| | | $20 | VIRTUAL PRIVATE NETWORK (VPN) |
| | MALWARE | $1 | PC MALWARE INSTALLATION |
| | | $25 | MALICIOUS FILE ENCRYPTION |
| | SPAM | $20 | 500 SMS (FLOODING) |
| | | $400 | 1 MILLION MALICIOUS SPAM |
| | | $20 | 500 PHONE CALLS (FLOODING) |
| | | $200 | 1 MILLION EMAIL SPAM (LEGAL) |
| | FAKE DOCUMENTS | $25 | DIGITAL COPY OF FAKE CREDIT/DEBIT CARD |
| | | $25 | DIGITAL COPY OF FAKE DRIVER'S LICENSE OR PASSPORT |
| | | $15 | DIGITAL COPY OF FAKE UTILITY BILL OR SOCIAL SECURITY CARD |

Source: https://www.recordedfuture.com/cyber-operations-cost/

Simon.whittaker@verticalstructure.com

# ”Hackers” – the stock image

# The reality

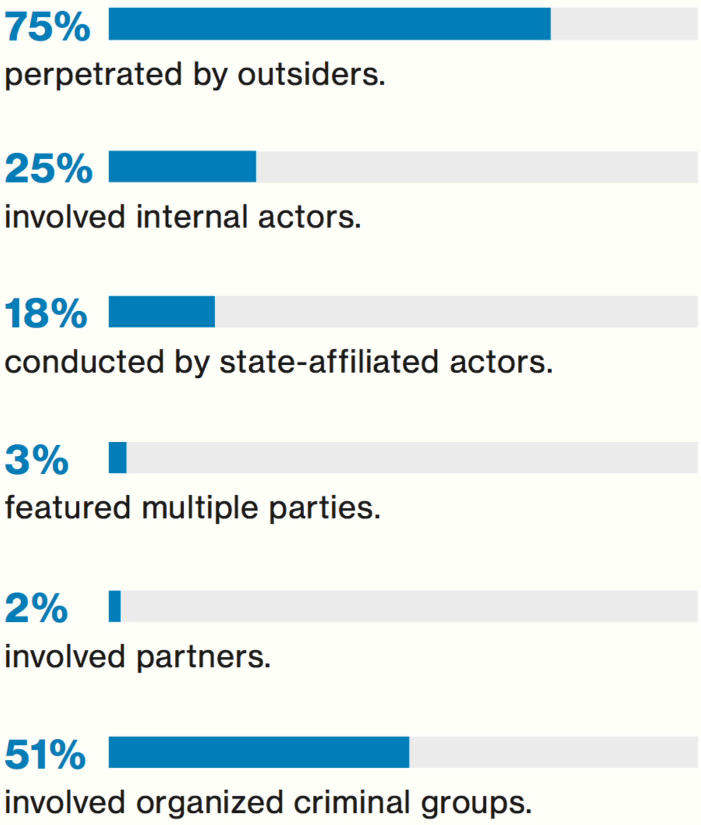
- *"It's time to think differently about cyber risk – ditching the talk of hackers – and recognising that our businesses are being targeted by ruthless criminal entrepreneurs with business plans and extensive resources – intent on fraud, extortion or theft of hard won intellectual property."*

- Paul Taylor, UK Head of Cyber Security, KPMG
  - http://bit.ly/takingTheOffensive

COLLEGIUM BOSTONIENSE
FUND. MDCCCLXIII
RELIGIONI ET
BONIS ARTIBUS
IHS
αἰ ἐν
ἀριστ εύειν

DEPARTMENT OF STATE
UNITED STATES OF AMERICA
E PLURIBUS UNUM

## Who’s behind the breaches?



**75%** perpetrated by outsiders.

**25%** involved internal actors.

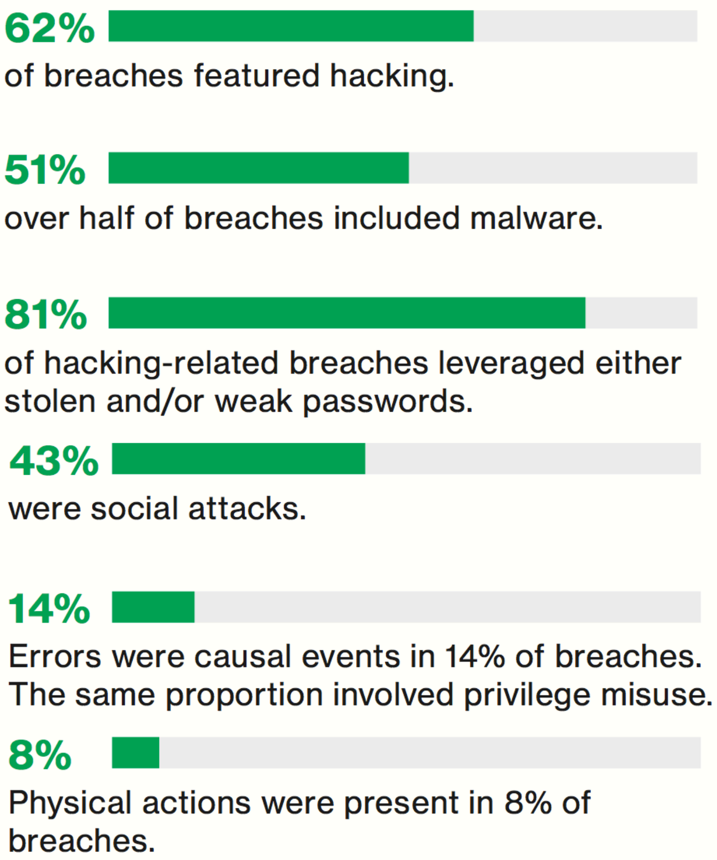
**18%** conducted by state-affiliated actors.

**3%** featured multiple parties.

**2%** involved partners.

**51%** involved organized criminal groups.

## What tactics do they use?



**62%** of breaches featured hacking.

**51%** over half of breaches included malware.

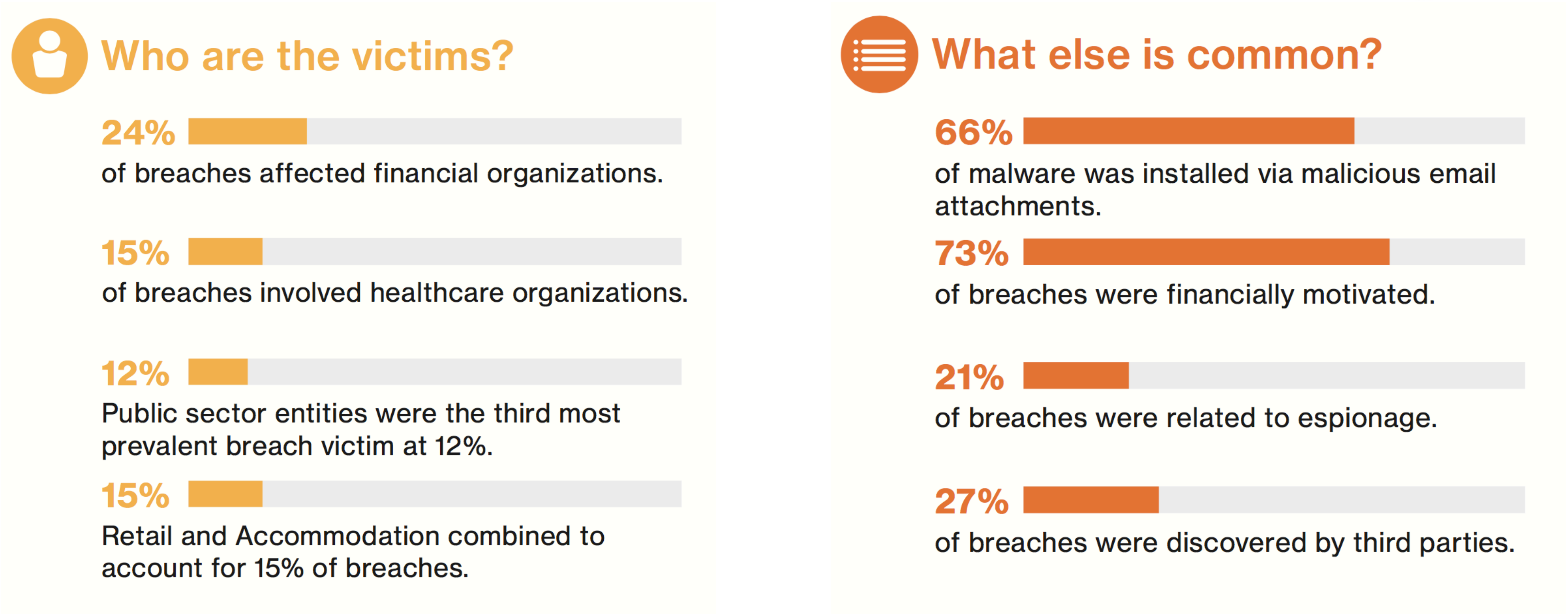
**81%** of hacking-related breaches leveraged either stolen and/or weak passwords.

**43%** were social attacks.

**14%** Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

**8%** Physical actions were present in 8% of breaches.

http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/



## Who are the victims?

24%

of breaches affected financial organizations.

15%

of breaches involved healthcare organizations.

12%

Public sector entities were the third most prevalent breach victim at 12%.

15%

Retail and Accommodation combined to account for 15% of breaches.

## What else is common?

66%

of malware was installed via malicious email attachments.

73%

of breaches were financially motivated.

21%

of breaches were related to espionage.

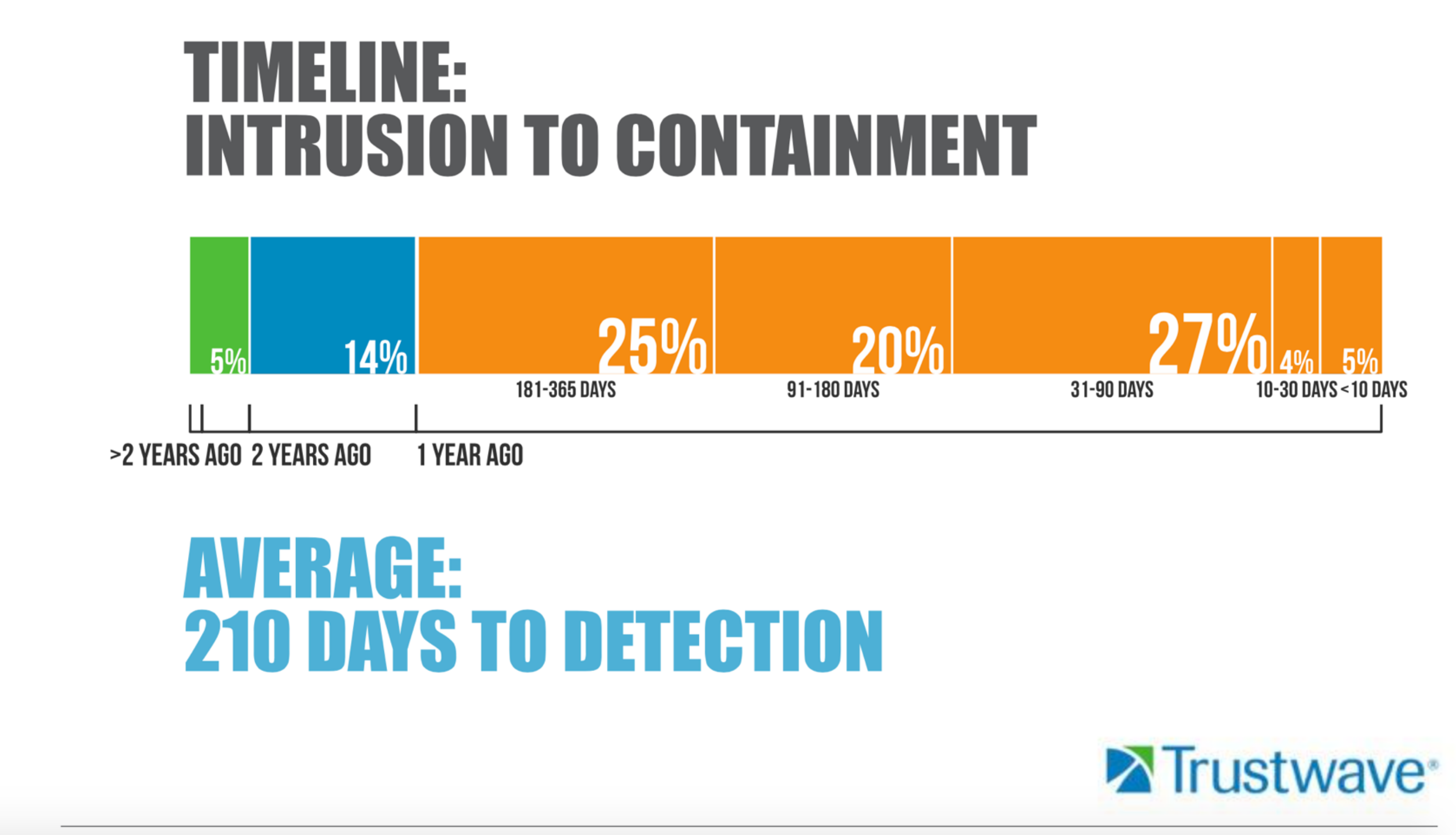
27%

of breaches were discovered by third parties.

http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Simon.whittaker@verticalstructure.com

# Businesses Slow to Detect



## TIMELINE:
## INTRUSION TO CONTAINMENT

## AVERAGE:
## 210 DAYS TO DETECTION

https://www.sans.org/summit-archives/file/summit-archive-1493740625.pdf

# The Governance Jigsaw – The Essential Trustee (CC3)

Ensure your charity is carrying out its purposes for the public benefit

Comply with your charity's governing document and the law

Act in your charity's best interests

Manage your charity's resources responsibly

Act with reasonable care and skill

Ensure your charity is accountable

It's about knowing:

- what your charity can and can't do within its purposes
- how your charity is fulfilling its purposes and benefiting the public
- what difference your charity is really making

It's about being:

- familiar with your governing document
- up to date with filing accounts, returns and any changes to your charity's registration details
- aware of other laws that apply to your charity

It's not about being:

- an expert - but you do need to take reasonable steps to find out

It's about:

- making balanced, informed decisions
- recognising & dealing with conflicts of interest
- ensuring trustee benefits are allowed
- being prepared to question and challenge
- accepting majority decisions

It's not about:

- preserving the charity for its own sake
- serving personal interests

It's about:

- managing risks, protecting assets (reputation) and people
- getting the resources your charity needs
- having and following appropriate controls and procedures
- dealing with land and buildings
- responsibility for, and to staff and volunteers

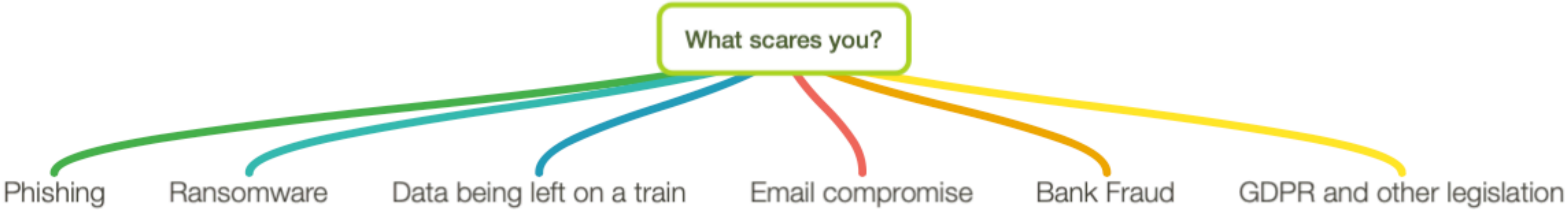
It's about:

- using your skills and experience
- deciding when you need advice
- preparing for meetings
- getting the information you need (financial, management)
- being prepared in case something does go wrong

It's about:

- meeting legal accounting and reporting requirements
- being able to show that your charity complies with the law and is effective
- being accountable to members and others with an interest in the charity
- ensuring that staff and volunteers are accountable to the board
- welcoming accountability as an opportunity not a burden

# What makes an organisation nervous?



What scares you?

Phishing

Ransomware

Data being left on a train

Email compromise

Bank Fraud

GDPR and other legislation

# Some Findings

- UK charities hold funds, personal, financial and commercial data and other information that is of interest or monetary value to a range of cyber criminals and other groups.
- The type and amount of information held varies according an individual charity’s size, objectives, structure and contacts.
- Charities are subject to the same cyber vulnerabilities as other organisations and businesses that conduct financial transactions, and rely on electronically held data or information to conduct day-to-day operations.
- Thirty charities interviewed for a recent government-commissioned report had collectively experienced a range of cyber breaches in the last two years including viruses, phishing emails, ransomware attacks, identity theft, website takedowns and variants of online financial fraud.
- The breaches resulted in loss of funds, data and website control. Although based on a very small dataset, the findings suggest that malicious cyber activity against the charity sector is varied and enduring.

https://www.ncsc.gov.uk/files/Cyber%20threat%20assessment%20-%20UK%20charity%20sector.pdf

# Range of Criminals

Simon.whittaker@verticalstructure.com

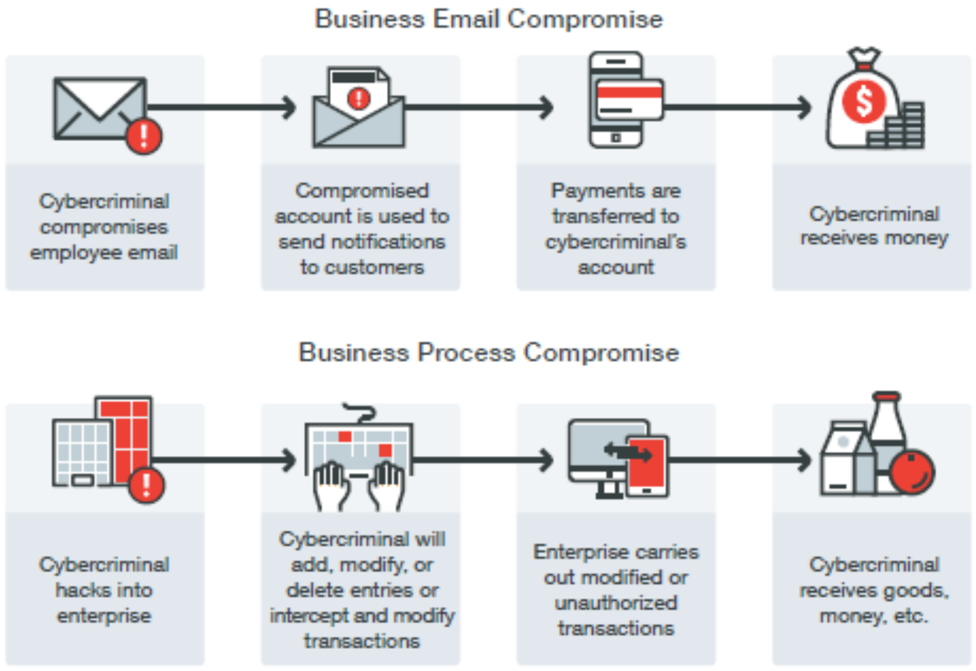
# A Trusting Sector

simon.whittaker@verticalstructure.com

# Business Email Compromise

simon.whittaker@verticalstructure.com

# What is Business Email Compromise



Business Email Compromise

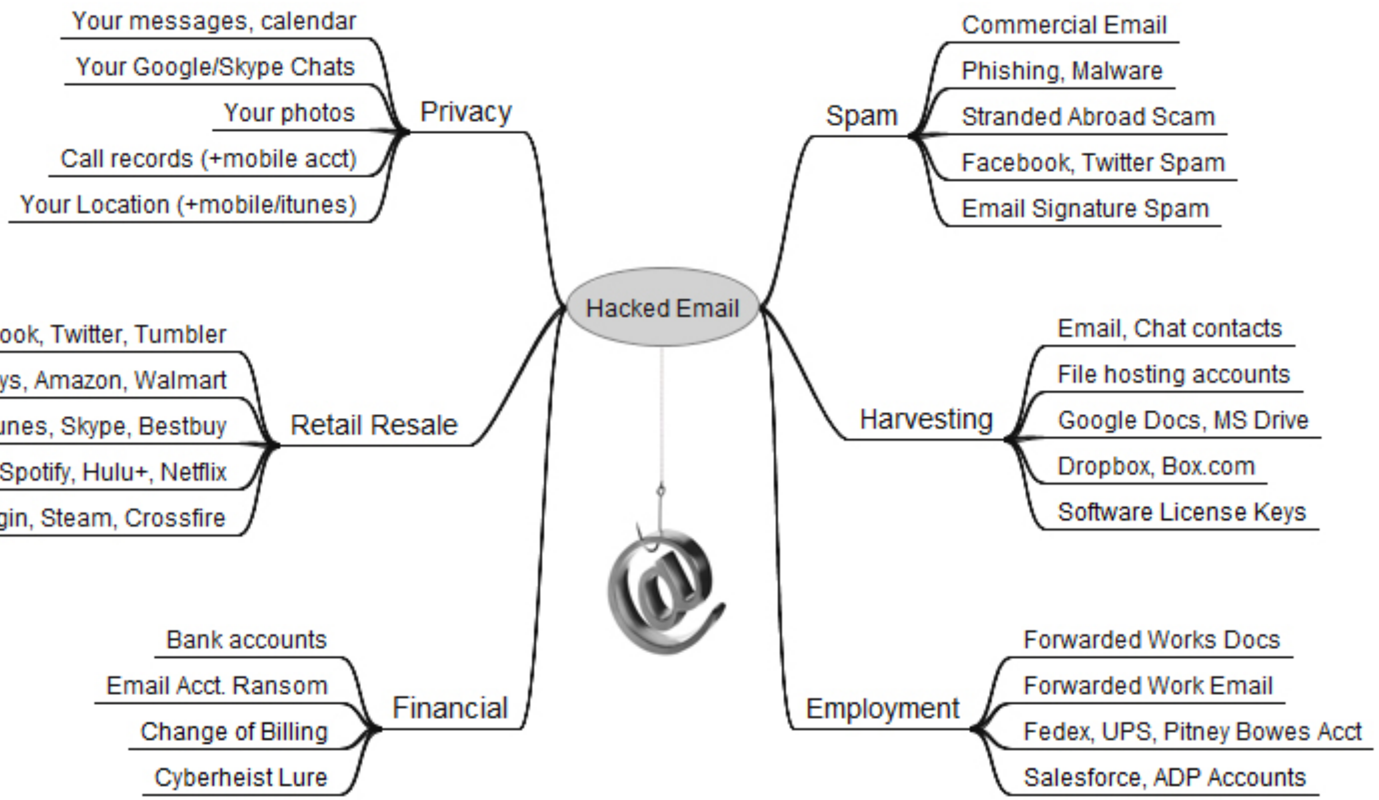
Cybercriminal compromises employee email → Compromised account is used to send notifications to customers → Payments are transferred to cybercriminal's account → Cybercriminal receives money

Business Process Compromise

Cybercriminal hacks into enterprise → Cybercriminal will add, modify, or delete entries or intercept and modify transactions → Enterprise carries out modified or unauthorized transactions → Cybercriminal receives goods, money, etc.

*BEC versus BPC attacks*

# The value of a compromised email address



https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/

# Suppliers

# The Assessment

National Cyber Security Centre

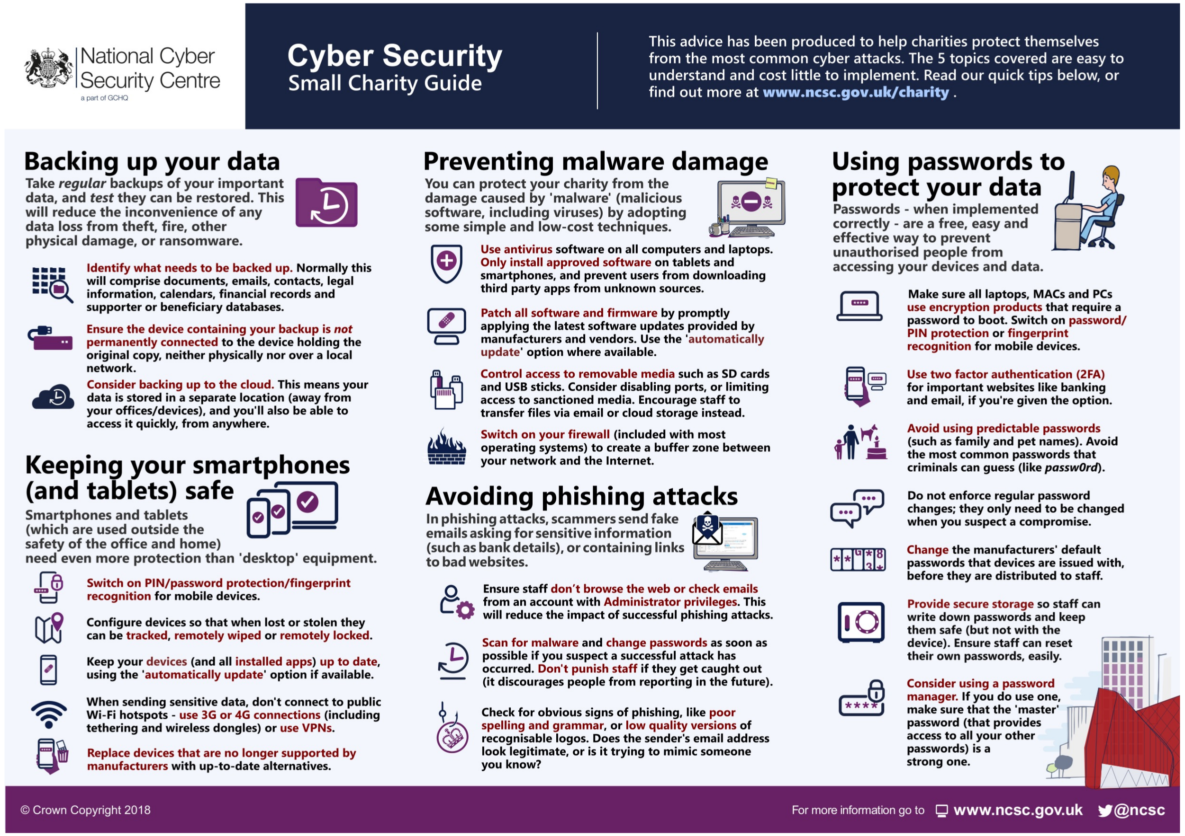
a part of GCHQ

**Cyber threat assessment:**

**UK charity sector**

February 2018

https://www.ncsc.gov.uk/files/Cyber%20threat%20assessment%20-%20UK%20charity%20sector.pdf



National Cyber Security Centre
a part of GCHQ

# Cyber Security
Small Charity Guide

This advice has been produced to help charities protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/charity** .

## Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

Identify what needs to be backed up. Normally this will comprise documents, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases.

Ensure the device containing your backup is *not* permanently connected to the device holding the original copy, neither physically nor over a local network.

Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

## Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

Switch on PIN/password protection/fingerprint recognition for mobile devices.

Configure devices so that when lost or stolen they can be tracked, remotely wiped or remotely locked.

Keep your devices (and all installed apps) up to date, using the 'automatically update' option if available.

When sending sensitive data, don't connect to public Wi-Fi hotspots - use 3G or 4G connections (including tethering and wireless dongles) or use VPNs.

Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

## Preventing malware damage

You can protect your charity from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

Use antivirus software on all computers and laptops. Only install approved software on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.

Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the 'automatically update' option where available.

Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.

Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

## Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

Ensure staff don't browse the web or check emails from an account with Administrator privileges. This will reduce the impact of successful phishing attacks.

Scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred. Don't punish staff if they get caught out (it discourages people from reporting in the future).

Check for obvious signs of phishing, like poor spelling and grammar, or low quality versions of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

## Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

Make sure all laptops, MACs and PCs use encryption products that require a password to boot. Switch on password/PIN protection or fingerprint recognition for mobile devices.

Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.

Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).

Do not enforce regular password changes; they only need to be changed when you suspect a compromise.

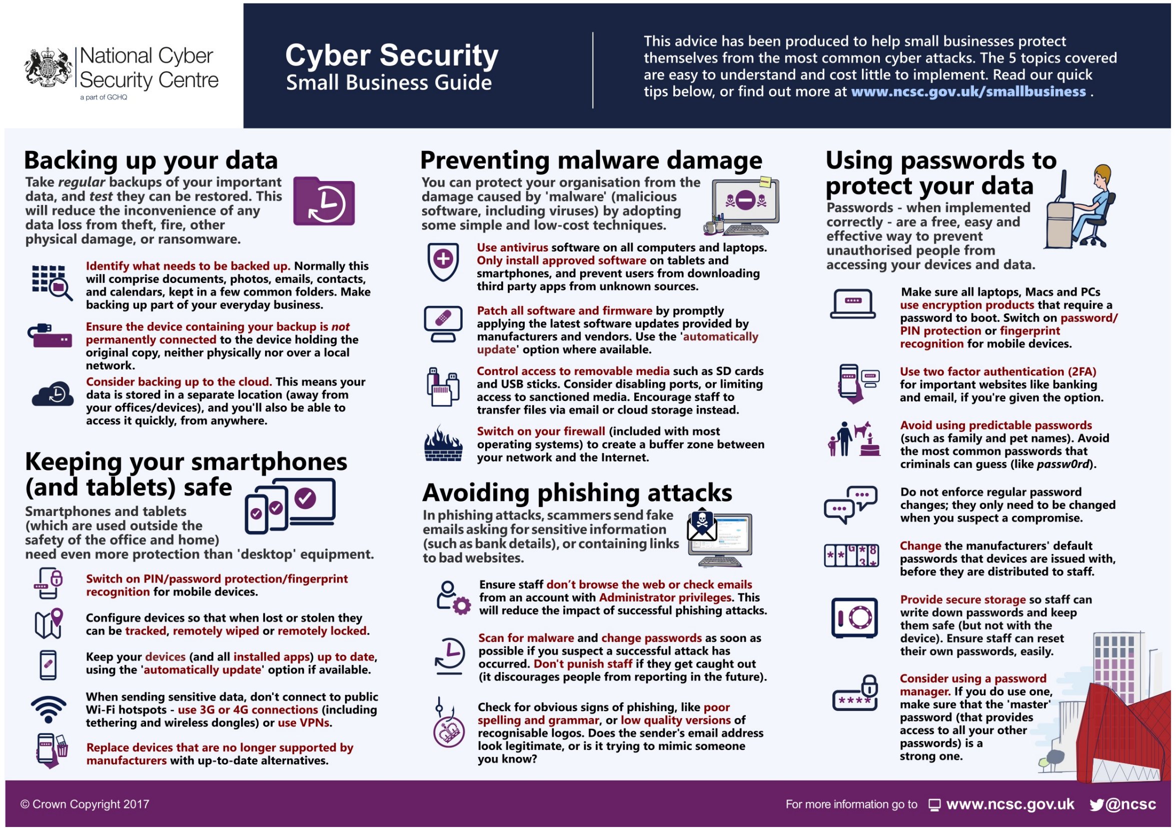
Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.

Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.

Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

For more information go to www.ncsc.gov.uk @ncsc

https://www.ncsc.gov.uk/collection/charity



National Cyber Security Centre
a part of GCHQ

# Cyber Security
Small Business Guide

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/smallbusiness** .

## Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

**Identify what needs to be backed up.** Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.

**Ensure the device containing your backup is *not* permanently connected** to the device holding the original copy, neither physically nor over a local network.

**Consider backing up to the cloud.** This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

## Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

**Switch on PIN/password protection/fingerprint recognition** for mobile devices.

Configure devices so that when lost or stolen they can be **tracked**, **remotely wiped** or **remotely locked**.

Keep your **devices** (and all **installed apps**) **up to date**, using the '**automatically update**' option if available.

When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.

**Replace devices that are no longer supported by manufacturers** with up-to-date alternatives.

## Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

**Use antivirus** software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.

**Patch all software and firmware** by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.

**Control access to removable media** such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.

**Switch on your firewall** (included with most operating systems) to create a buffer zone between your network and the Internet.

## Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.

**Scan for malware** and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).

Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

## Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

Make sure all laptops, Macs and PCs **use encryption products** that require a password to boot. Switch on **password/PIN protection** or **fingerprint recognition** for mobile devices.

**Use two factor authentication (2FA)** for important websites like banking and email, if you're given the option.

**Avoid using predictable passwords** (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).

Do not enforce regular password changes; they only need to be changed when you suspect a compromise.

**Change** the manufacturers' default passwords that devices are issued with, before they are distributed to staff.

**Provide secure storage** so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.

**Consider using a password manager.** If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

For more information go to www.ncsc.gov.uk @ncsc

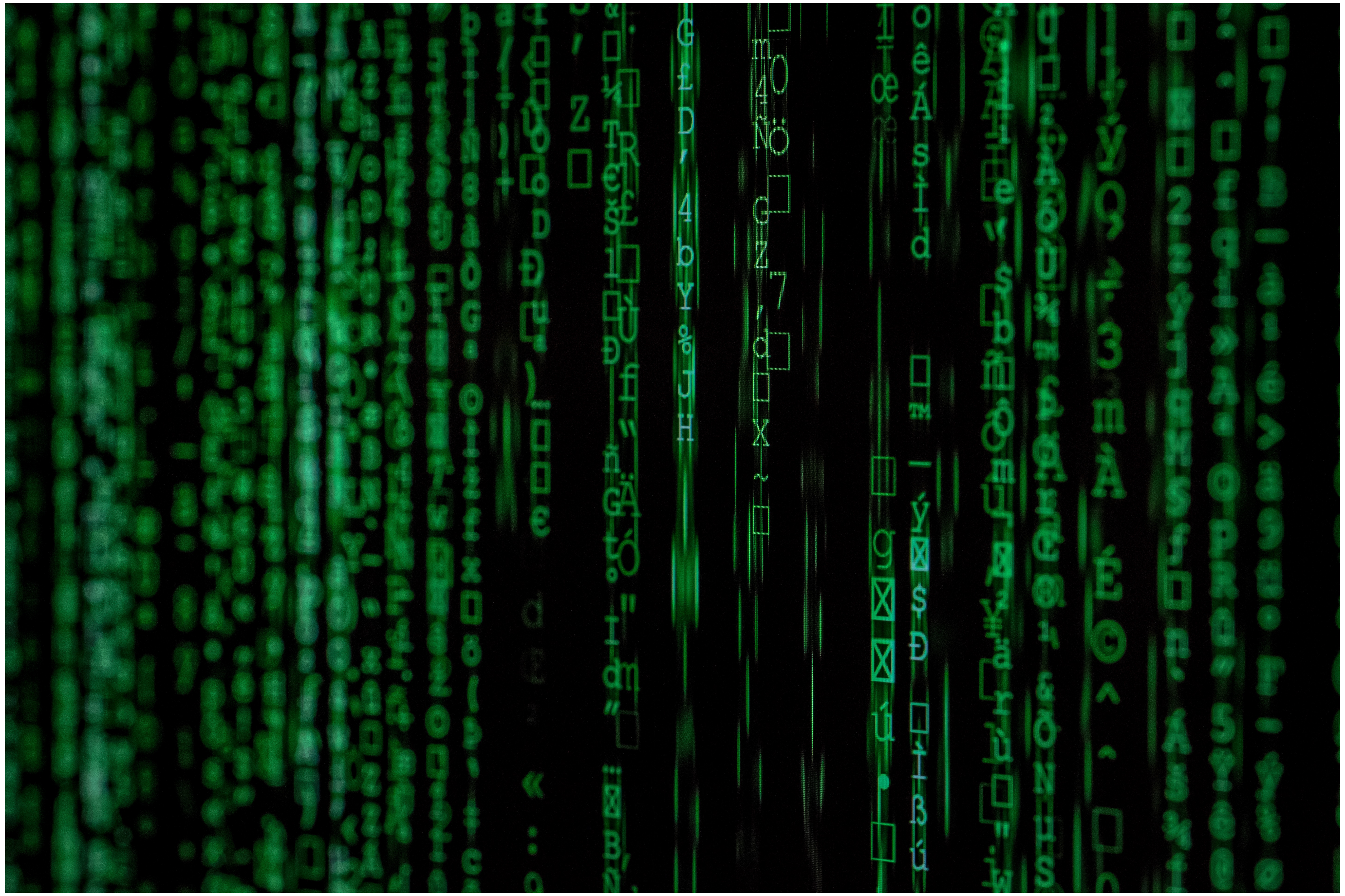
https://www.ncsc.gov.uk/collection/small-business-guide

# Backups

simon.whittaker@verticalstructure.com

# Mobile device security

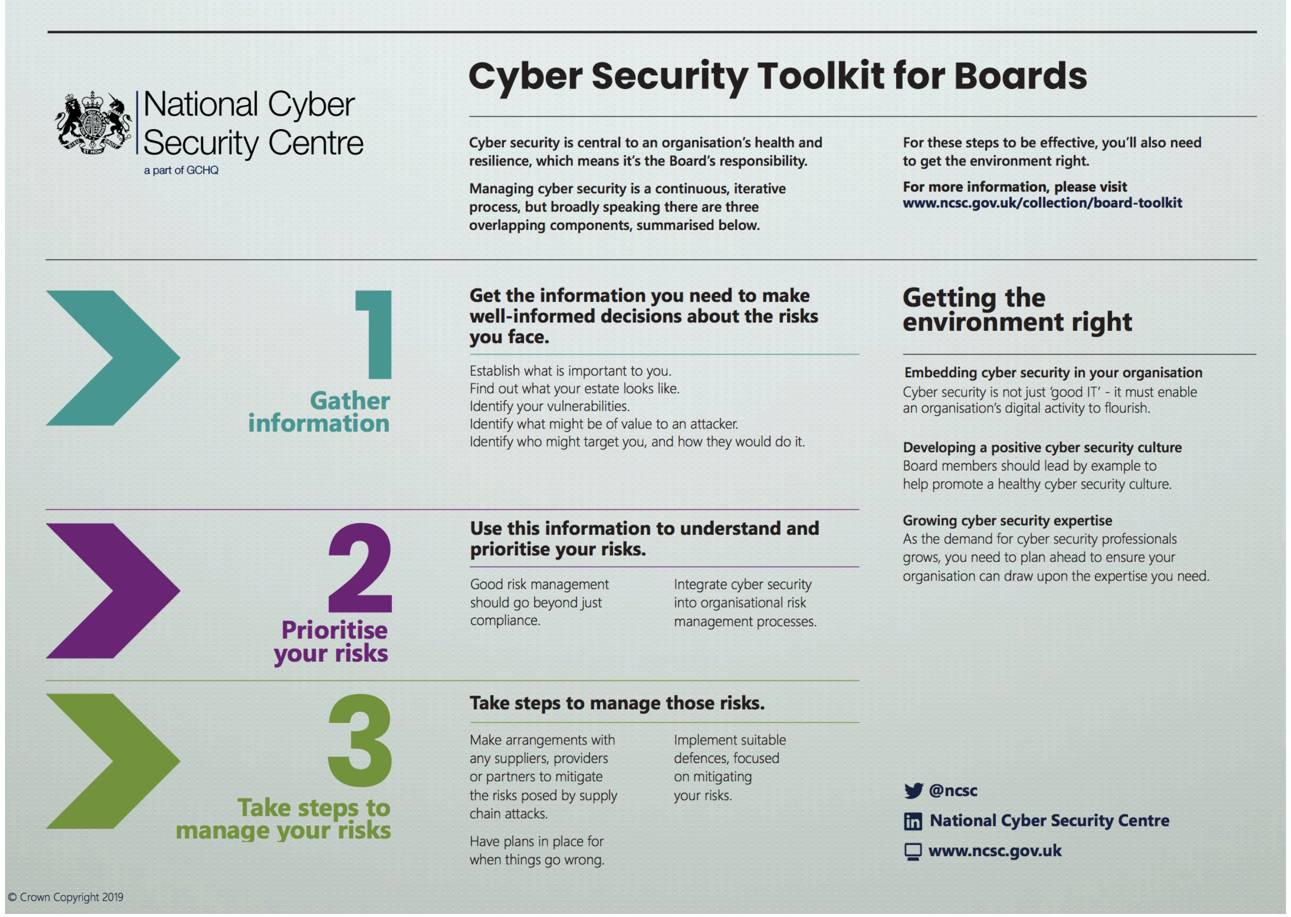
# Ransomware



# Phishing

# Passwords

# Toolkit for boards



National Cyber Security Centre
a part of GCHQ

## Cyber Security Toolkit for Boards

**Cyber security is central to an organisation's health and resilience, which means it's the Board's responsibility.**

**Managing cyber security is a continuous, iterative process, but broadly speaking there are three overlapping components, summarised below.**

**For these steps to be effective, you'll also need to get the environment right.**

**For more information, please visit www.ncsc.gov.uk/collection/board-toolkit**

### 1 Gather information

**Get the information you need to make well-informed decisions about the risks you face.**

Establish what is important to you.
Find out what your estate looks like.
Identify your vulnerabilities.
Identify what might be of value to an attacker.
Identify who might target you, and how they would do it.

### 2 Prioritise your risks

**Use this information to understand and prioritise your risks.**

Good risk management should go beyond just compliance.

Integrate cyber security into organisational risk management processes.

### 3 Take steps to manage your risks

**Take steps to manage those risks.**

Make arrangements with any suppliers, providers or partners to mitigate the risks posed by supply chain attacks.

Have plans in place for when things go wrong.

Implement suitable defences, focused on mitigating your risks.

### Getting the environment right

**Embedding cyber security in your organisation**
Cyber security is not just 'good IT' - it must enable an organisation's digital activity to flourish.

**Developing a positive cyber security culture**
Board members should lead by example to help promote a healthy cyber security culture.

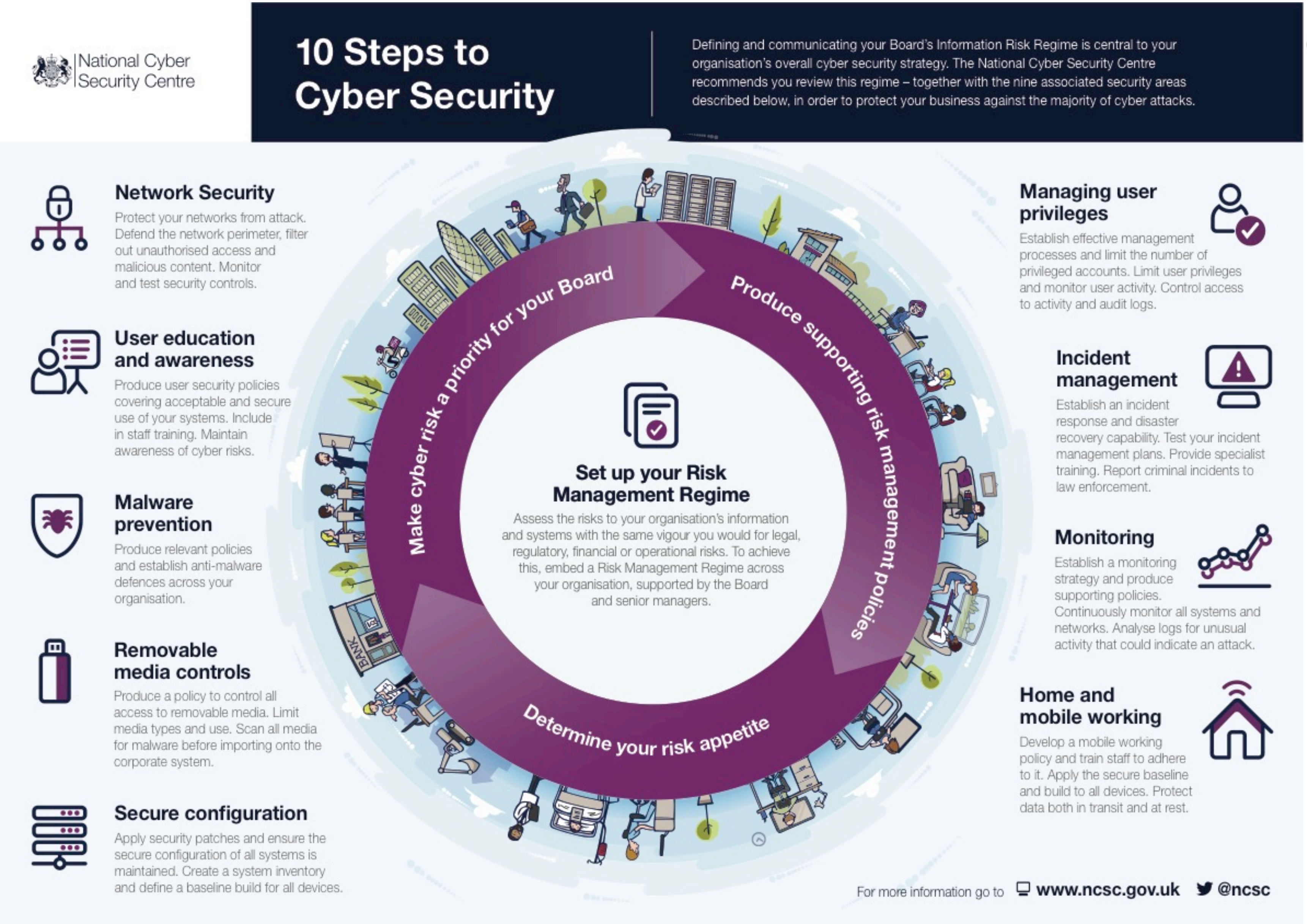
**Growing cyber security expertise**
As the demand for cyber security professionals grows, you need to plan ahead to ensure your organisation can draw upon the expertise you need.

**@ncsc**
**National Cyber Security Centre**
**www.ncsc.gov.uk**

https://www.ncsc.gov.uk/collection/board-toolkit

# Exercise time!

- What is important to your organization?
- Where are the biggest gaps?
- What immediate steps can you take?



National Cyber Security Centre

# 10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

### Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

### User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

### Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

### Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

### Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Make cyber risk a priority for your Board

Produce supporting risk management policies

Determine your risk appetite

### Set up your Risk Management Regime

Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

### Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

### Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

### Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

### Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc

simon.whittaker@verticalstructure.com

# Risk Management Regime

simon.whittaker@verticalstructure.com

# Network Security

simon.whittaker@verticalstructure.com

# User Education and Awareness

simon.whittaker@verticalstructure.com

# Malware prevention

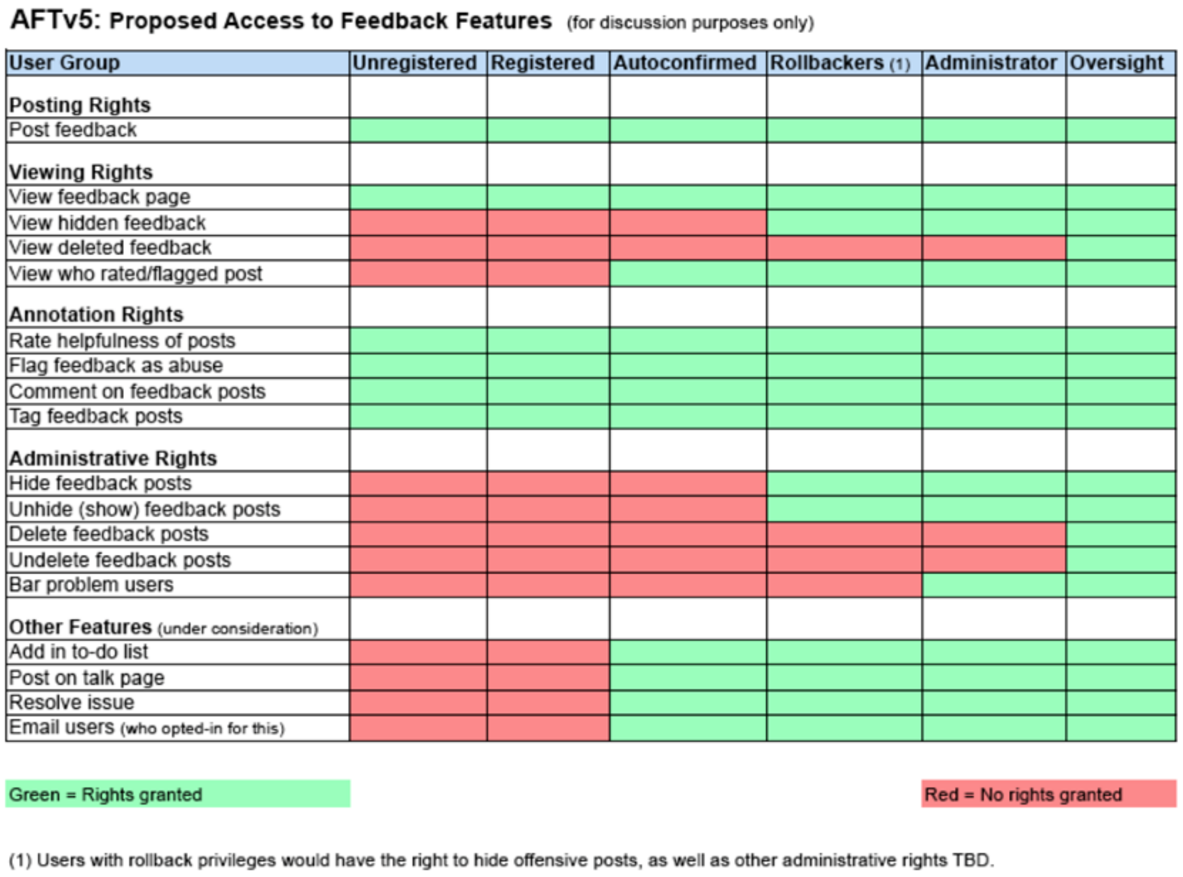
```
<code>file://</code> URL, the "next" a
" role="button">Sign up today</a></p>
```

# Removable Media Controls

simon.whittaker@verticalstructure.com

# Secure Configuration

# Managing User Privileges



**AFTv5: Proposed Access to Feedback Features** (for discussion purposes only)

| User Group | Unregistered | Registered | Autoconfirmed | Rollbackers (1) | Administrator | Oversight |
|---|---|---|---|---|---|---|
| **Posting Rights** | | | | | | |
| Post feedback | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| **Viewing Rights** | | | | | | |
| View feedback page | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| View hidden feedback | 🟥 | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 |
| View deleted feedback | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 |
| View who rated/flagged post | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 |
| **Annotation Rights** | | | | | | |
| Rate helpfulness of posts | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Flag feedback as abuse | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Comment on feedback posts | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Tag feedback posts | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| **Administrative Rights** | | | | | | |
| Hide feedback posts | 🟥 | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 |
| Unhide (show) feedback posts | 🟥 | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 |
| Delete feedback posts | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 |
| Undelete feedback posts | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 |
| Bar problem users | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 | 🟩 |
| **Other Features** (under consideration) | | | | | | |
| Add in to-do list | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 |
| Post on talk page | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 |
| Resolve issue | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 |
| Email users (who opted-in for this) | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 |

🟩 Green = Rights granted

🟥 Red = No rights granted

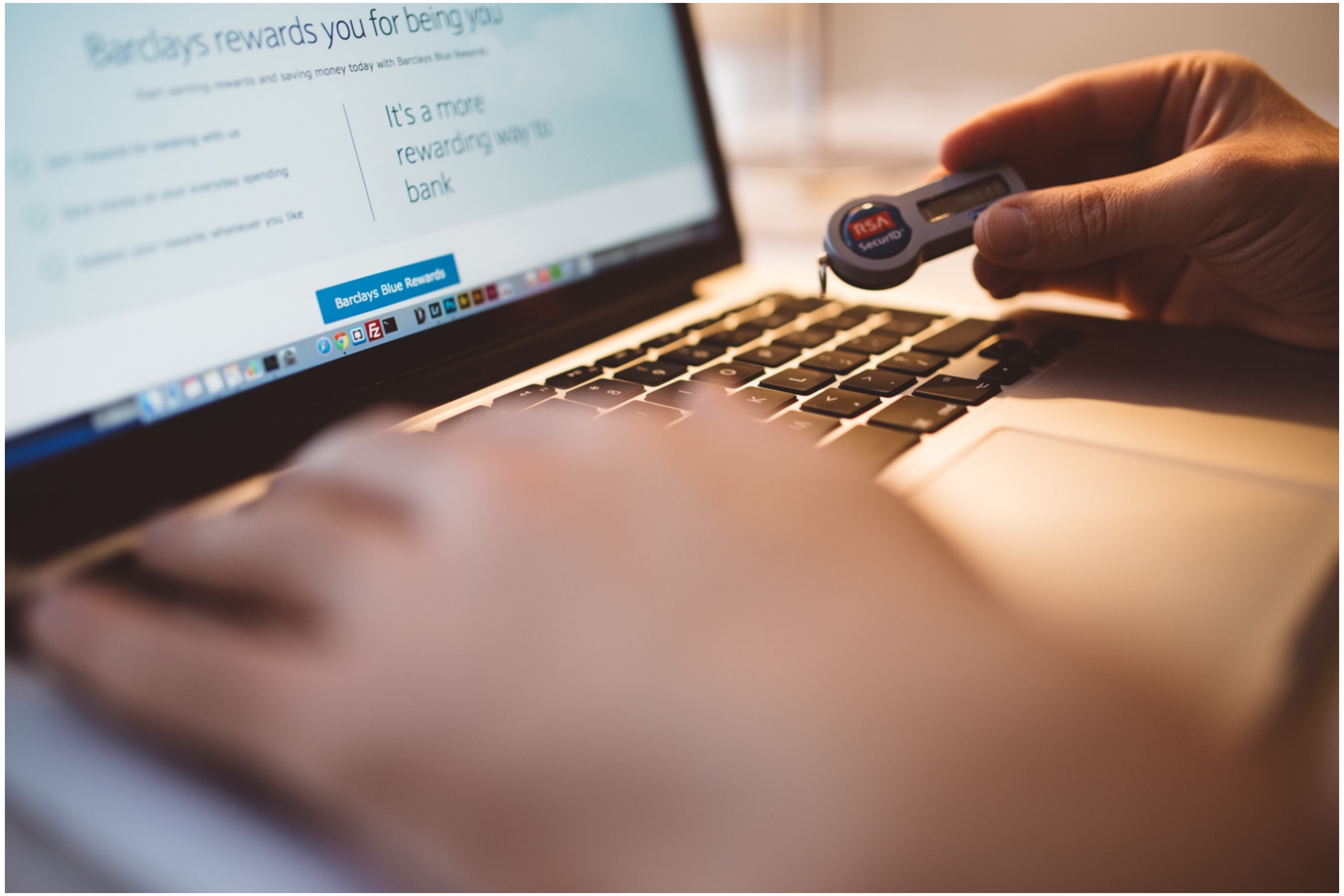
(1) Users with rollback privileges would have the right to hide offensive posts, as well as other administrative rights TBD.

# Incident Management

simon.whittaker@verticalstructure.com

# Monitoring

# Home and Mobile Working


Barclays rewards you for being you
It's a more rewarding way to bank
Barclays Blue Rewards
RSA SecurID

# Questions?

Simon.Whittaker@verticalstructure.com