Cyber Resilience in the Post-COVID World

Maj Gen (Retd) Chip Chapman CB

QUANTUM RESILIENCE

Third Generation working?

QUANTUM
RESILIENCE

National Risk Register
(Assurance matrix)

Impact measurement (T and H series): fatalities, casualties, social disruption, economic disruption, anxiety, outrage.

Training in **Crisis management / programme management scenarios** to reduce volatility of **Consequence management** sackings

Distant horizon scanning leading to **capability development** to reduce and mitigate future risks/vulnerabilities/threats

“Golden 24 hours (or less)” – credibility of the message

The ‘Playbook’: the guide to actions *(your head will know how heavy your ass is when your neck is in the noose!)*

The Contestable Domain of Cyber Space

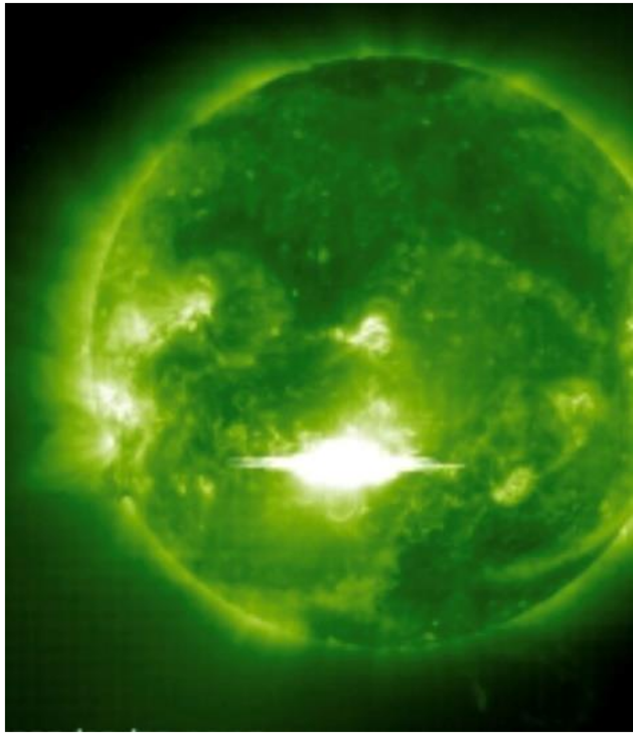
	Generate	Process	Store	Transmit	Consume
Missions					
Users					
Systems					
Networks					
Servers					
Computers					
Devices					
Information					
Data					

This 9x5 grid represents the contestable cyber domain capable of being attacked. All these 45 intersections need to be protected in a truly secure IT environment, and not just networks and transmissions. There is no threat where there is no vulnerability. Cyber is also the future potential attack vector against space-based platforms such as satellites.

AVOID – DETECT – SURVIVE – RECOVER

What’s the question?

Business continuity
how would you operate if the internet stopped for a week/month?



QUANTUM RESILIENCE

The Legal Cyber Environment

What are the threats?

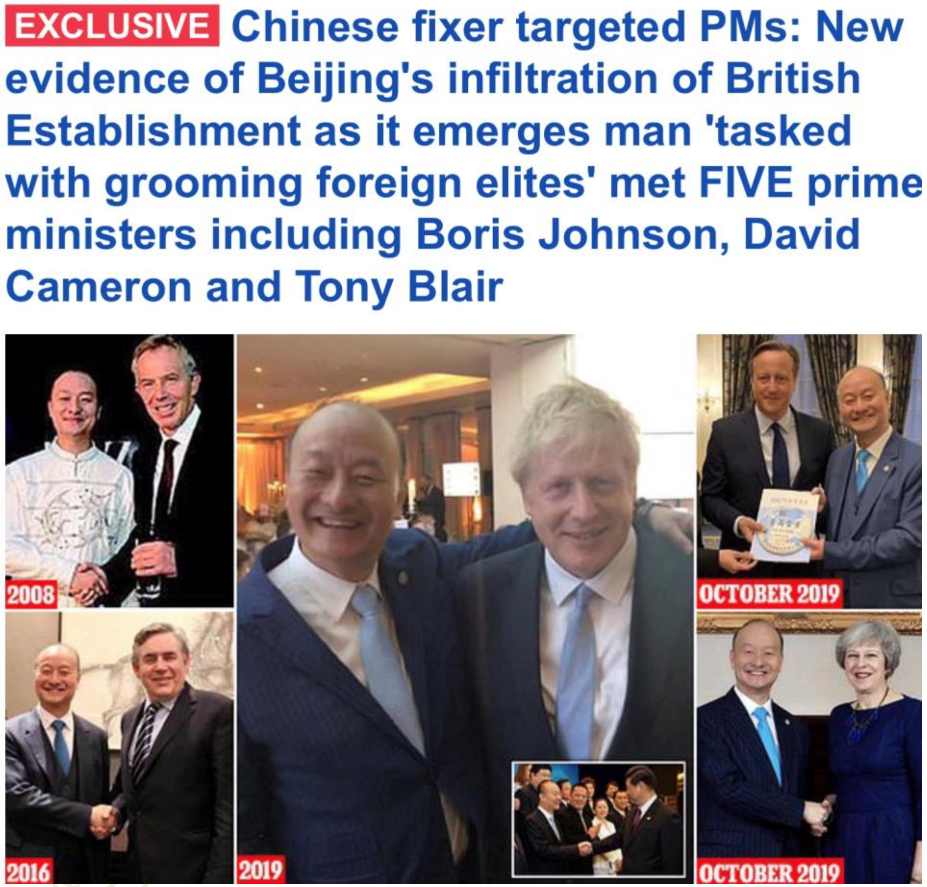
What are the attack types?

What needs to be done?

QUANTUM
RESILIENCE

CRIME (You or the ‘insider’ threat)

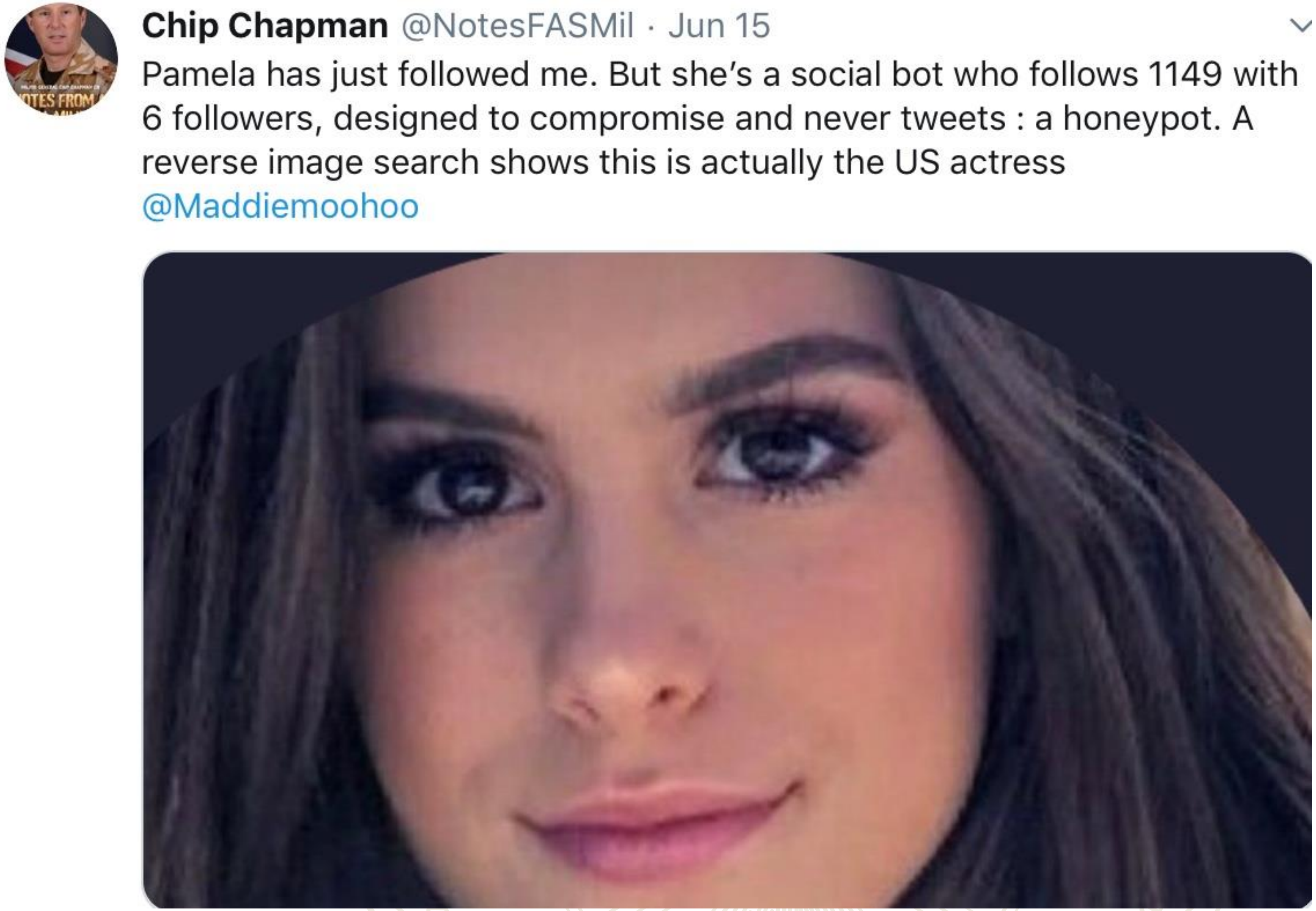
Compromise/
Kompromat
Revenge
Ideology
Money
Ego



EXCLUSIVE Chinese fixer targeted PMs: New evidence of Beijing's infiltration of British Establishment as it emerges man 'tasked with grooming foreign elites' met FIVE prime ministers including Boris Johnson, David Cameron and Tony Blair

2008
2016
2019
OCTOBER 2019
OCTOBER 2019

QUANTUM
RESILIENCE



Chip Chapman @NotesFASMil · Jun 15

Pamela has just followed me. But she's a social bot who follows 1149 with 6 followers, designed to compromise and never tweets : a honeypot. A reverse image search shows this is actually the US actress @Maddiemoohoo

Madison Shipman

Hackers

Hecklers

What does the current ‘battle damage assessment/big data analytics tell us?

Cyber crime during COVID

Company responses

Home and corporate networks

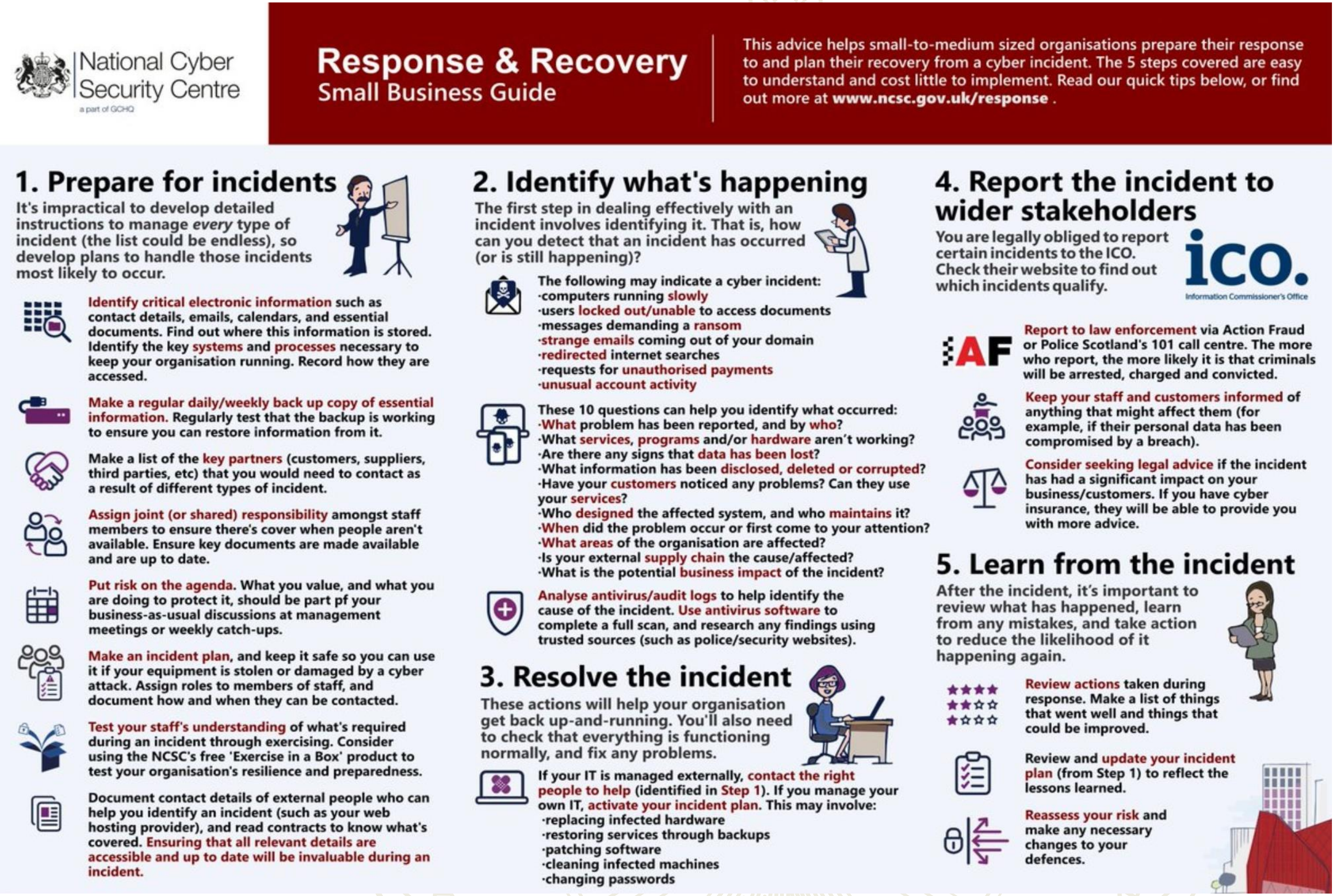
QUANTUM
RESILIENCE

Crisis and Consequence management for the future

Distant horizon scanning – what plans are required?

Preventing a cyber CAR crash (cyber active resilience)

Scenario exercising your responses during disruptive challenges



National Cyber Security Centre
a part of GCHQ

Response & Recovery
Small Business Guide

This advice helps small-to-medium sized organisations prepare their response to and plan their recovery from a cyber incident. The 5 steps covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/response** .

1. Prepare for incidents

It's impractical to develop detailed instructions to manage *every* type of incident (the list could be endless), so develop plans to handle those incidents most likely to occur.

Identify critical electronic information such as contact details, emails, calendars, and essential documents. Find out where this information is stored. Identify the key **systems** and **processes** necessary to keep your organisation running. Record how they are accessed.

Make a regular daily/weekly back up copy of essential information. Regularly test that the backup is working to ensure you can restore information from it.

Make a list of the **key partners** (customers, suppliers, third parties, etc) that you would need to contact as a result of different types of incident.

Assign joint (or shared) responsibility amongst staff members to ensure there's cover when people aren't available. Ensure key documents are made available and are up to date.

Put risk on the agenda. What you value, and what you are doing to protect it, should be part pf your business-as-usual discussions at management meetings or weekly catch-ups.

Make an incident plan, and keep it safe so you can use it if your equipment is stolen or damaged by a cyber attack. Assign roles to members of staff, and document how and when they can be contacted.

Test your staff's understanding of what's required during an incident through exercising. Consider using the NCSC's free 'Exercise in a Box' product to test your organisation's resilience and preparedness.

Document contact details of external people who can help you identify an incident (such as your web hosting provider), and read contracts to know what's covered. **Ensuring that all relevant details are accessible and up to date will be invaluable during an incident.**

2. Identify what's happening

The first step in dealing effectively with an incident involves identifying it. That is, how can you detect that an incident has occurred (or is still happening)?

The following may indicate a cyber incident:
- ·computers running **slowly**
- ·users **locked out/unable** to access documents
- ·messages demanding a **ransom**
- ·**strange emails** coming out of your domain
- ·**redirected** internet searches
- ·requests for **unauthorised payments**
- ·**unusual account activity**

These 10 questions can help you identify what occurred:
- ·**What** problem has been reported, and by **who**?
- ·What **services, programs** and/or **hardware** aren't working?
- ·Are there any signs that **data has been lost**?
- ·What information has been **disclosed, deleted or corrupted**?
- ·Have your **customers** noticed any problems? Can they use your **services**?
- ·Who **designed** the affected system, and who **maintains** it?
- ·**When** did the problem occur or first come to your attention?
- ·**What areas** of the organisation are affected?
- ·Is your external **supply chain** the cause/affected?
- ·What is the potential **business impact** of the incident?

Analyse antivirus/audit logs to help identify the cause of the incident. **Use antivirus software** to complete a full scan, and research any findings using trusted sources (such as police/security websites).

3. Resolve the incident

These actions will help your organisation get back up-and-running. You'll also need to check that everything is functioning normally, and fix any problems.

If your IT is managed externally, **contact the right people to help** (identified in **Step 1**). If you manage your own IT, **activate your incident plan.** This may involve:
- ·replacing infected hardware
- ·restoring services through backups
- ·patching software
- ·cleaning infected machines
- ·changing passwords

4. Report the incident to wider stakeholders

You are legally obliged to report certain incidents to the ICO. Check their website to find out which incidents qualify.

ico.
Information Commissioner's Office

AF

Report to law enforcement via Action Fraud or Police Scotland's 101 call centre. The more who report, the more likely it is that criminals will be arrested, charged and convicted.

Keep your staff and customers informed of anything that might affect them (for example, if their personal data has been compromised by a breach).

Consider seeking legal advice if the incident has had a significant impact on your business/customers. If you have cyber insurance, they will be able to provide you with more advice.

5. Learn from the incident

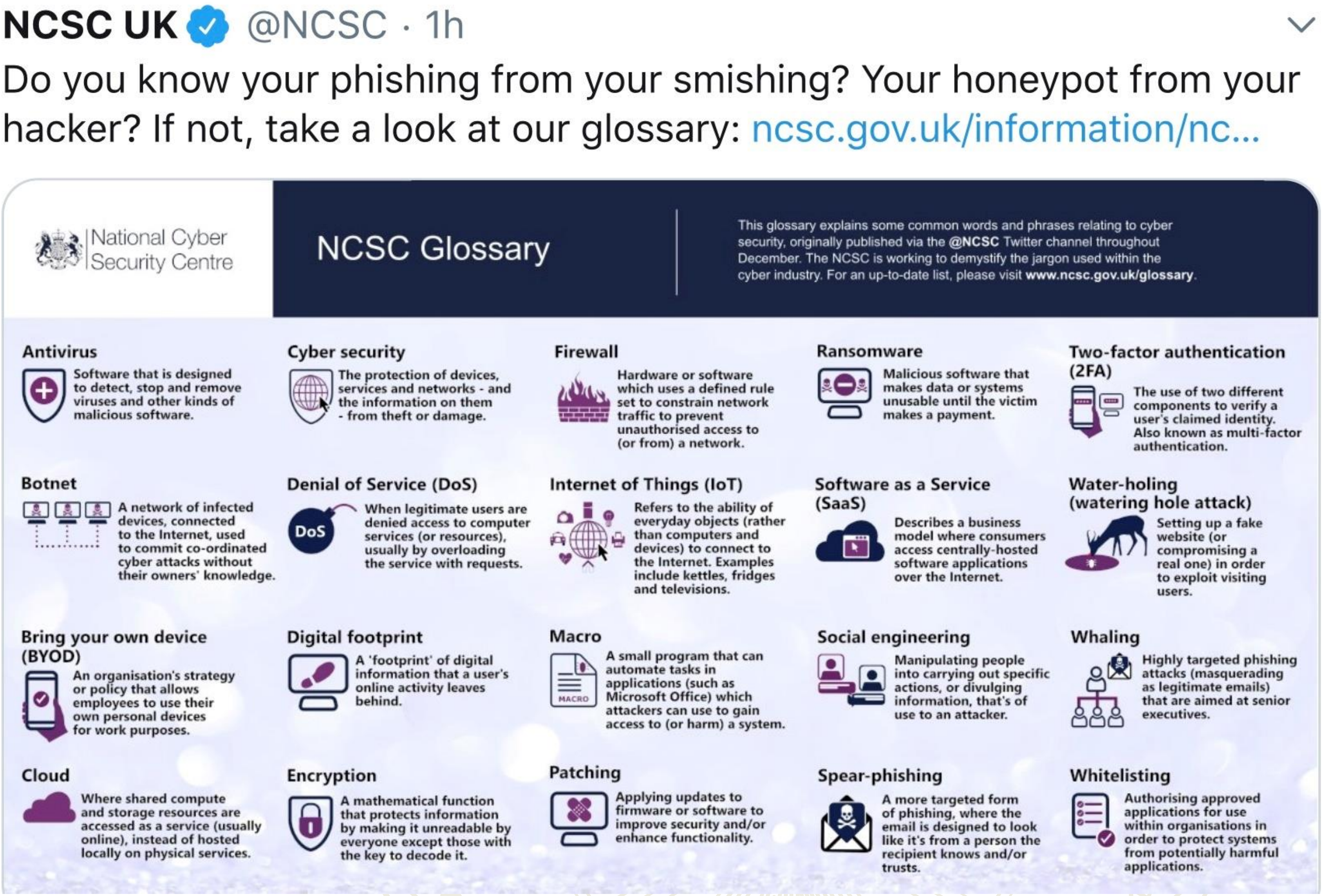
After the incident, it's important to review what has happened, learn from any mistakes, and take action to reduce the likelihood of it happening again.

Review actions taken during response. Make a list of things that went well and things that could be improved.

Review and **update your incident plan** (from Step 1) to reflect the lessons learned.

Reassess your risk and make any necessary changes to your defences.

QUANTUM
RESILIENCE



NCSC UK @NCSC · 1h

Do you know your phishing from your smishing? Your honeypot from your hacker? If not, take a look at our glossary: ncsc.gov.uk/information/nc...

National Cyber Security Centre

NCSC Glossary

This glossary explains some common words and phrases relating to cyber security, originally published via the **@NCSC** Twitter channel throughout December. The NCSC is working to demystify the jargon used within the cyber industry. For an up-to-date list, please visit **www.ncsc.gov.uk/glossary**.

Antivirus
Software that is designed to detect, stop and remove viruses and other kinds of malicious software.

Botnet
A network of infected devices, connected to the Internet, used to commit co-ordinated cyber attacks without their owners' knowledge.

Bring your own device (BYOD)
An organisation's strategy or policy that allows employees to use their own personal devices for work purposes.

Cloud
Where shared compute and storage resources are accessed as a service (usually online), instead of hosted locally on physical services.

Cyber security
The protection of devices, services and networks - and the information on them - from theft or damage.

Denial of Service (DoS)
When legitimate users are denied access to computer services (or resources), usually by overloading the service with requests.

Digital footprint
A 'footprint' of digital information that a user's online activity leaves behind.

Encryption
A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.

Firewall
Hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorised access to (or from) a network.

Internet of Things (IoT)
Refers to the ability of everyday objects (rather than computers and devices) to connect to the Internet. Examples include kettles, fridges and televisions.

Macro
A small program that can automate tasks in applications (such as Microsoft Office) which attackers can use to gain access to (or harm) a system.

Patching
Applying updates to firmware or software to improve security and/or enhance functionality.

Ransomware
Malicious software that makes data or systems unusable until the victim makes a payment.

Software as a Service (SaaS)
Describes a business model where consumers access centrally-hosted software applications over the Internet.

Social engineering
Manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker.

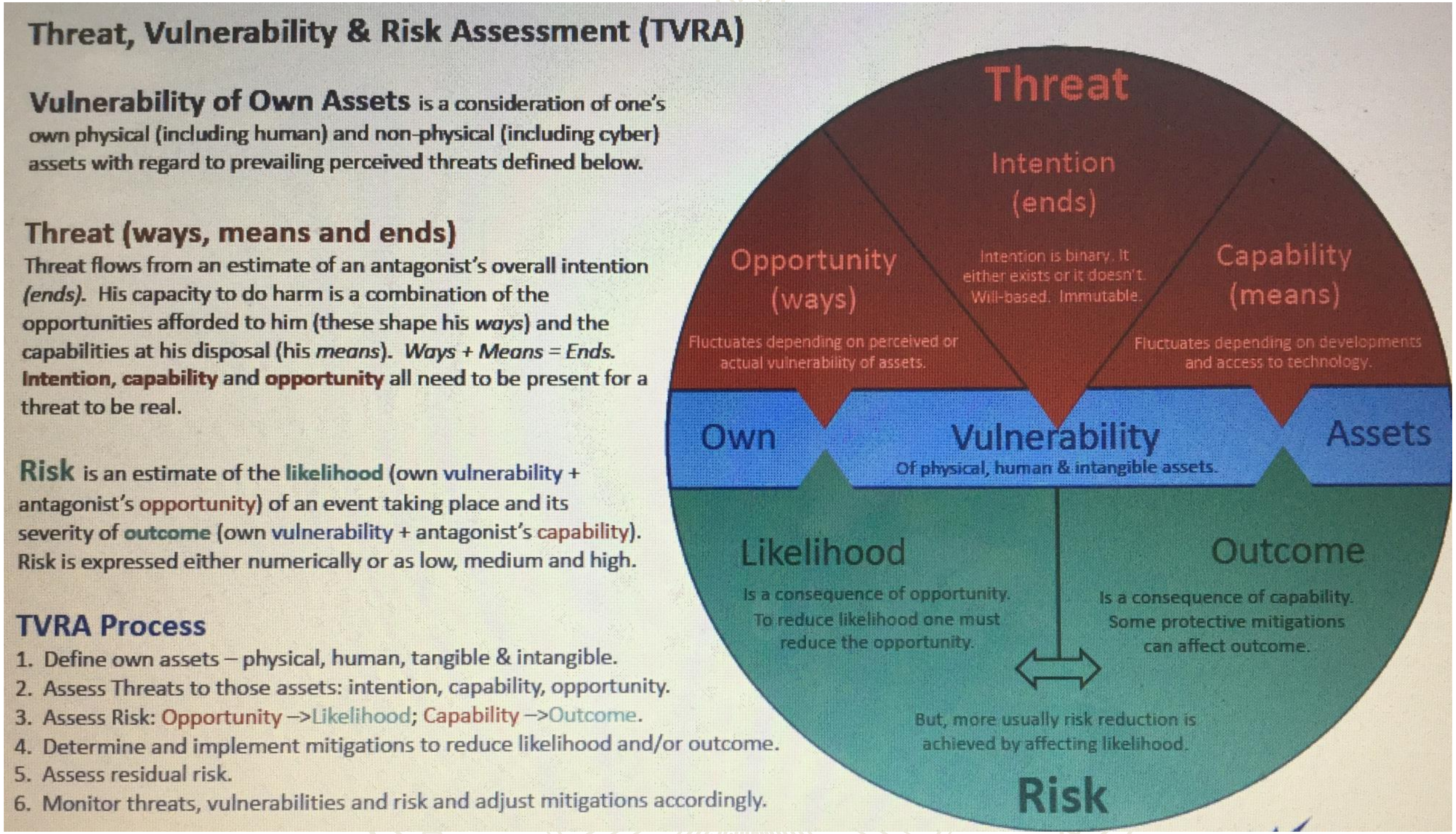
Spear-phishing
A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.

Two-factor authentication (2FA)
The use of two different components to verify a user's claimed identity. Also known as multi-factor authentication.

Water-holing (watering hole attack)
Setting up a fake website (or compromising a real one) in order to exploit visiting users.

Whaling
Highly targeted phishing attacks (masquerading as legitimate emails) that are aimed at senior executives.

Whitelisting
Authorising approved applications for use within organisations in order to protect systems from potentially harmful applications.



Threat, Vulnerability & Risk Assessment (TVRA)

Vulnerability of Own Assets is a consideration of one's own physical (including human) and non-physical (including cyber) assets with regard to prevailing perceived threats defined below.

Threat (ways, means and ends)

Threat flows from an estimate of an antagonist's overall intention *(ends)*. His capacity to do harm is a combination of the opportunities afforded to him (these shape his *ways*) and the capabilities at his disposal (his *means*). *Ways + Means = Ends.* **Intention**, **capability** and **opportunity** all need to be present for a threat to be real.

Risk is an estimate of the **likelihood** (own **vulnerability** + antagonist's **opportunity**) of an event taking place and its severity of **outcome** (own **vulnerability** + antagonist's **capability**). Risk is expressed either numerically or as low, medium and high.

TVRA Process

1. Define own assets – physical, human, tangible & intangible.
2. Assess Threats to those assets: intention, capability, opportunity.
3. Assess Risk: Opportunity –>Likelihood; Capability –>Outcome.
4. Determine and implement mitigations to reduce likelihood and/or outcome.
5. Assess residual risk.
6. Monitor threats, vulnerabilities and risk and adjust mitigations accordingly.

Threat

Intention (ends)

Intention is binary. It either exists or it doesn't. Will-based. Immutable.

Opportunity (ways)

Fluctuates depending on perceived or actual vulnerability of assets.

Capability (means)

Fluctuates depending on developments and access to technology.

Own Vulnerability Assets

Of physical, human & intangible assets.

Likelihood

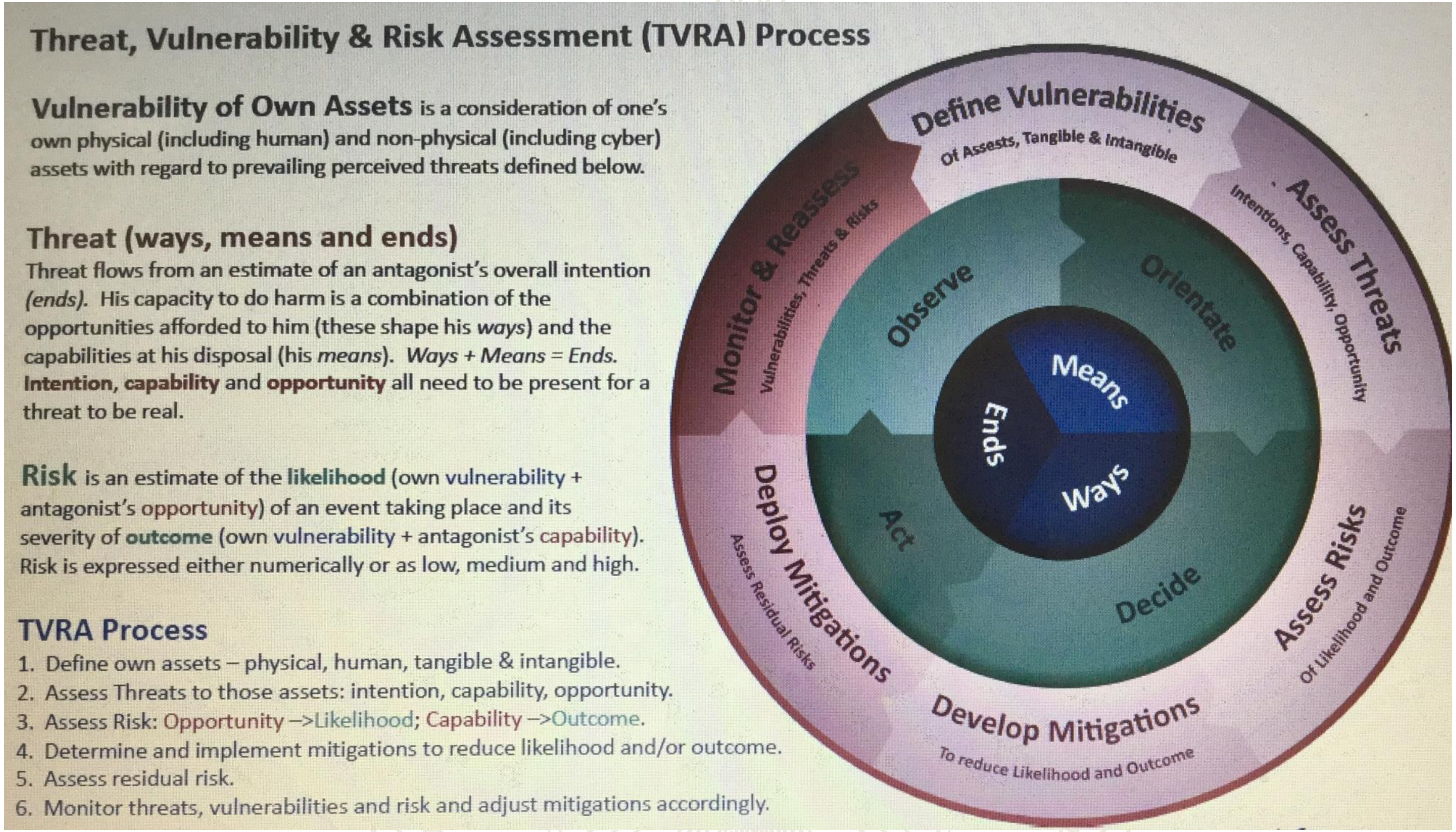
Is a consequence of opportunity. To reduce likelihood one must reduce the opportunity.

Outcome

Is a consequence of capability. Some protective mitigations can affect outcome.

But, more usually risk reduction is achieved by affecting likelihood.

Risk



Threat, Vulnerability & Risk Assessment (TVRA) Process

Vulnerability of Own Assets is a consideration of one's own physical (including human) and non-physical (including cyber) assets with regard to prevailing perceived threats defined below.

Threat (ways, means and ends)

Threat flows from an estimate of an antagonist's overall intention *(ends).* His capacity to do harm is a combination of the opportunities afforded to him (these shape his *ways*) and the capabilities at his disposal (his *means*). *Ways + Means = Ends.* **Intention**, **capability** and **opportunity** all need to be present for a threat to be real.

Risk is an estimate of the **likelihood** (own vulnerability + antagonist's opportunity) of an event taking place and its severity of **outcome** (own vulnerability + antagonist's capability). Risk is expressed either numerically or as low, medium and high.

TVRA Process

1. Define own assets – physical, human, tangible & intangible.
2. Assess Threats to those assets: intention, capability, opportunity.
3. Assess Risk: Opportunity –>Likelihood; Capability –>Outcome.
4. Determine and implement mitigations to reduce likelihood and/or outcome.
5. Assess residual risk.
6. Monitor threats, vulnerabilities and risk and adjust mitigations accordingly.