Cyber Security as a Strategic Concern

Dr Steve Jones
Cyber Security Advisor
Norfolk & Suffolk Constabularies

stephen.jones1@suffolk.police.uk

Overview

- Considering a cyber security strategy
- Planning for **WHEN**, not **IF**
- Summary
- Inputs, resources and tools


“IT WILL NEVER HAPPEN TO US...”
“...I TAKE NO RESPONSIBILITY”

More Famous Last Words?

"Cyber security is IT's responsibility"

"Our cyber security is good"

"We're too small to be of interest to hackers"

Background question for today:

How would your business respond to a cyber-attack?

For instance:
Account Compromise,
Denial of Service,
Ransomware etc.

Why is this important?

23% of businesses overall have a cyber security strategy in place

- In other words, 77% of businesses have no plan!

39% of businesses identified a cyber-attack

- Phishing is the most identified threat vector (83% of identified attacks)
- Key word: “identified”: Actual amount of attacks likely to be far higher

46% of businesses have not acted to identify and mitigate cyber security risks over the past 12 months

Cyber Security Breaches Survey 2022, published by the Department for Digital, Culture, Media and Sport:

https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

Cyber Security Strategy

A high-level plan for how the organisation, its technological assets and data are protected against accidental or malicious loss/damage.

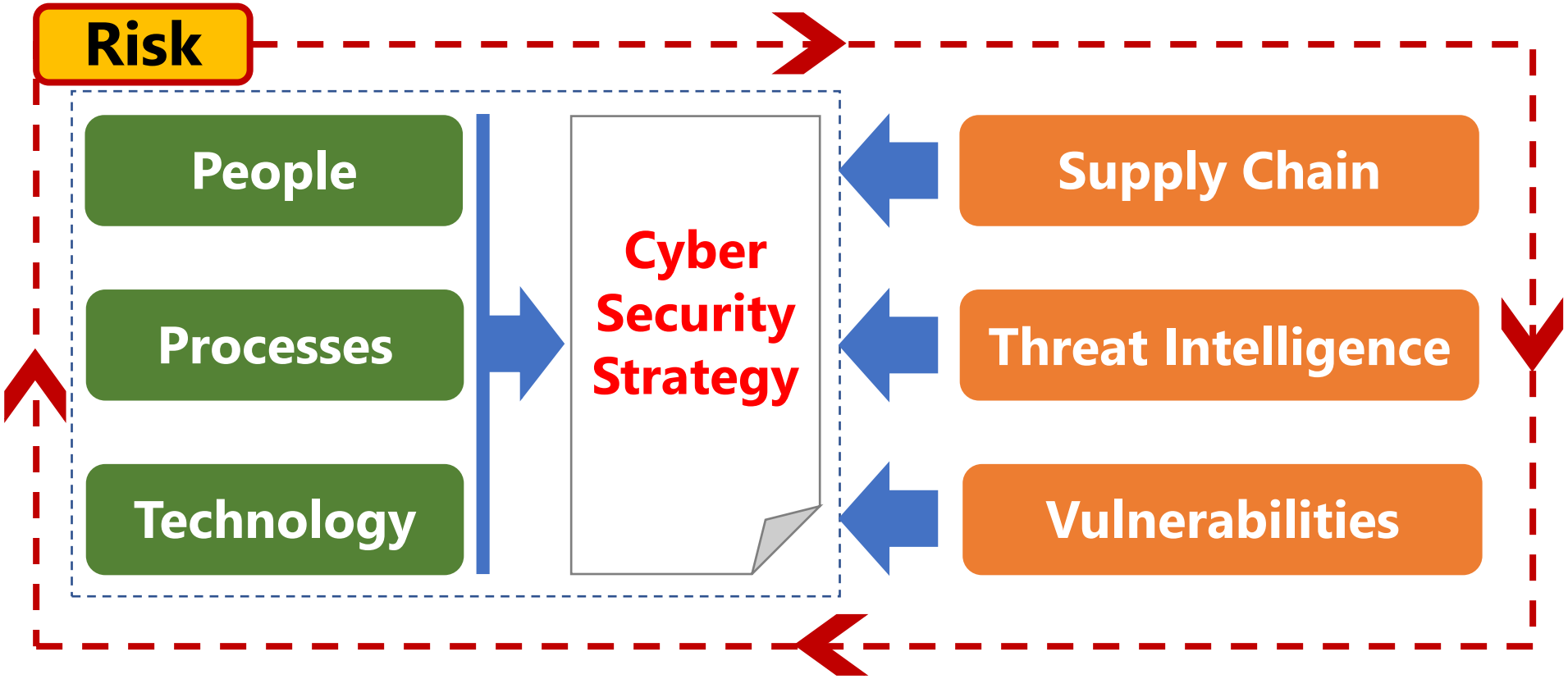
- A ‘living document’, updated and tested regularly
- The foundation for specific incident response plans and playbooks
- Requires senior management and/or board level attention
  - Everyone in the organisation has their part to play though!

Why Have a Cyber Security Strategy?

- It's Proactive!
  - Prevention is the best defence
- Underpins any response plans the organisation has to:
  - Enable business continuity and recovery
  - Disrupt a detected cyber-attack in progress
  - Contain a breach and limit damage
- Cybercrime is a long term and increasing threat

Developing a Cyber Security Strategy

- Consider cyber risk from inside and outside of the organisation
- Inform and refine strategy using reputable and reliable external feeds



External Feeds

CSP

THE EASTERN CYBER RESILIENCE CENTRE

Cyber East

CVE®

Planning for WHEN not IF

- Take the position of **When**, not **IF**, a cyber security incident will occur

- Cyberspace is not limited by geographic boundaries
  - Cyber criminals operate all over the world
  - Organised cyber criminal groups may operate over several continents
  - Law enforcement challenges

Hostile Cyber Actors

Hackers

Includes:
- *Cyber Criminals*
- *Hacktivists*
- *Terrorists*

Nation States

Insiders

Incident Response Plan

The starting point in responding to a cyber security incident

Should Include:

- Key contacts
- Process and criteria for decisions and escalation
- Response process covering incident lifecycle
- At least one conference number
  - Always available for urgent incident calls
- Guidance on relevant legal and regulatory obligations

Can Be Enhanced by:

- Simple checklists for ease and convenience
- Methods to document and track an incident
- Technical guidance on:
  - Incident analysis and containment,
  - Remediation and recovery
- Playbooks and guidance for specific types of incident

Derived from official NCSC Incident Management guidance at:
https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes

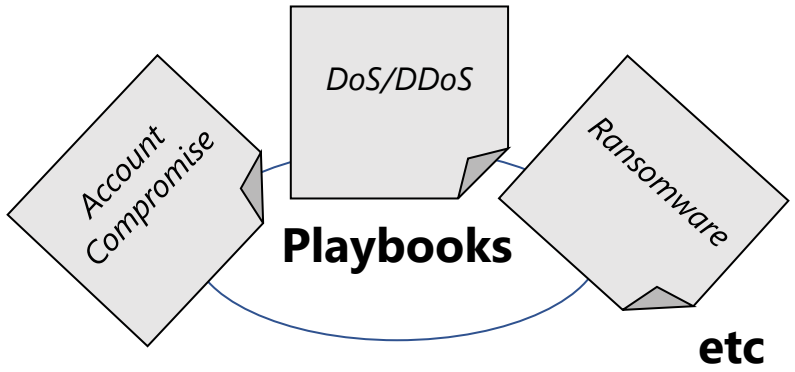
Cyber Incident Response Playbook

A detailed response plan, typically focused on a specific type of incident e.g. Account Compromise, Denial of Service and Ransomware etc.

- Immediate and simple response instructions
  - Covers the first hours of responding to the incident
  - Key contacts and stakeholders with clearly defined and delegated response tasks
  - Facilitate rapid response

- Detailed guidance and action points
  - Identification and triage
  - Containment and prevention of further impact
  - Remediation and recovery

- Outline steps to capture and retain evidence



Testing and Refinement

- The cyber landscape is constantly changing and your strategy and response needs to change with it
  - Threats
  - Vulnerabilities

- Strategies, response plans and playbooks need to be tested!
  - Ensure they are fit for purpose

NCSC Exercise in a Box

https://www.ncsc.gov.uk/information/exercise-in-a-box


JUST CLAIM ON THE CYBER INSURANCE...
...DON'T NEED TO DO ANYTHING ELSE

Cyber Insurance

Cyber insurance can be part of a robust cyber security strategy and response plan…

…but NOT a substitute!

- Always check cyber insurance policy details carefully
  - Implemented strategy and response plans may be required to claim
  - Are there any cover limitations?

CYBER ESSENTIALS

https://www.ncsc.gov.uk/cyberessentials

Summary

- Plan for **WHEN**, not **IF**, a cyber security incident occurs
- Implementing a cyber security strategy is a continuous undertaking
  - Continuously test and refine it
  - Consider the cyber risk from both inside and outside of the organisation
  - Requires senior management / board level attention
  - Inform your strategy with information from reliable and reputable sources
    - E.g. CiSP, ECRC, Cyber East, CVE etc.
    - Do not underestimate the value of networking
- A cyber security strategy underpins the business' response to incidents

Inputs, Resources and Tools

- **NCSC 10 Steps to Cyber Security**
  https://www.ncsc.gov.uk/collection/10-steps
- **Cyber Security Information Sharing Partnership (CiSP)**
  https://www.ncsc.gov.uk/section/keep-up-to-date/cisp
- **Eastern Cyber Resilience Centre**
  https://www.ecrcentre.co.uk
- **Cyber East**
  https://www.cybereast.co.uk
- **Local Police Forces**

  https://www.norfolk.police.uk/advice/cybercrime

  https://www.suffolk.police.uk/advice/cybercrime
- **NCSC Active Cyber Defence**
  https://www.ncsc.gov.uk/section/active-cyber-defence/introduction
- **NCSC Cyber Aware**
  https://www.ncsc.gov.uk/cyberaware/home
- **NCSC Exercise in a Box**
  https://www.ncsc.gov.uk/information/exercise-in-a-box
- **Police CyberAlarm**
  https://www.cyberalarm.police.uk
- **CVE**
  https://www.cve.org

"It will never happen to us"

How will you respond when it happens?

"Cyber security is IT's responsibility"

Everyone has their part to play!

"Our cyber security is good"

Your cyber security can always be improved!

"We're too small to be of interest to hackers"

Cybercriminals do not care!

Thank You!

I welcome questions and further discussion in the networking time later

I appreciate any feedback at:
https://nscyber.com/BusinessFeedback

If you are a victim of cybercrime, please report this to the Police via. Action Fraud:

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040
https://www.actionfraud.police.uk