Using a Security Standard to get started on Cyber Security

Paul Rolison ACA

Director – Cyber Strategies Ltd

CYBER STRATEGIES

Develop • Protect • Maintain

Why consider a security standard?

- Provides a structured approach
- No need to reinvent the wheel
- Framework to measure internal and external actions
- Options to have Third Party and independent assessments
- Starting point = Cyber Essentials

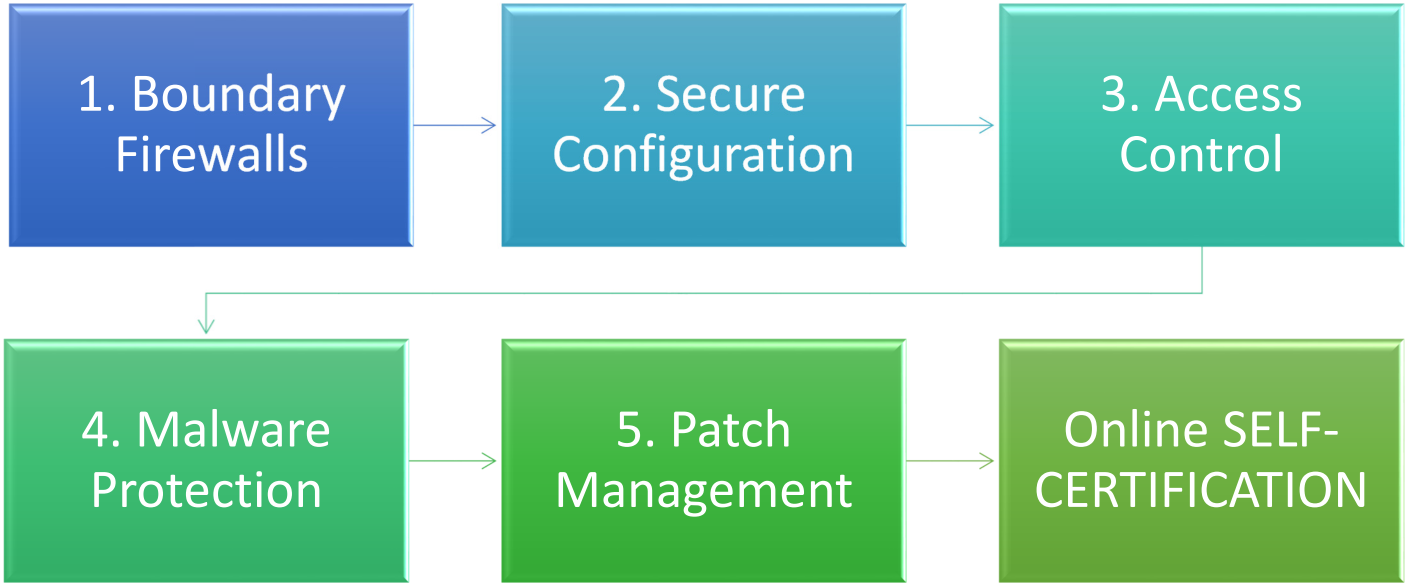
Cyber Essentials & Cyber Essentials Plus

- Background
  - Launch by Government June 2014 (Chartered Accountants Hall)
  - Response to a lack of Security Standards for all organisational sizes
  - “Essentials” as the requirements are seen as a minimum position
  - Designed to be financially and technically accessible by all
  - Two levels – Basic and Plus
- Regulatory approach
  - Owned by HM Government and strategically managed by National Cyber Security Centre (NCSC)
  - Administered by a single Cyber Essentials Partner – IASME
  - Delivered by a number of Certification Bodies appointed by IASME

CYBER STRATEGIES
Develop • Protect • Maintain

Cyber Essentials Basic process

Aim to prevent Internet borne (Cyber) attacks on data
5 disciplines around infrastructure configuration



1. Boundary Firewalls

2. Secure Configuration

3. Access Control

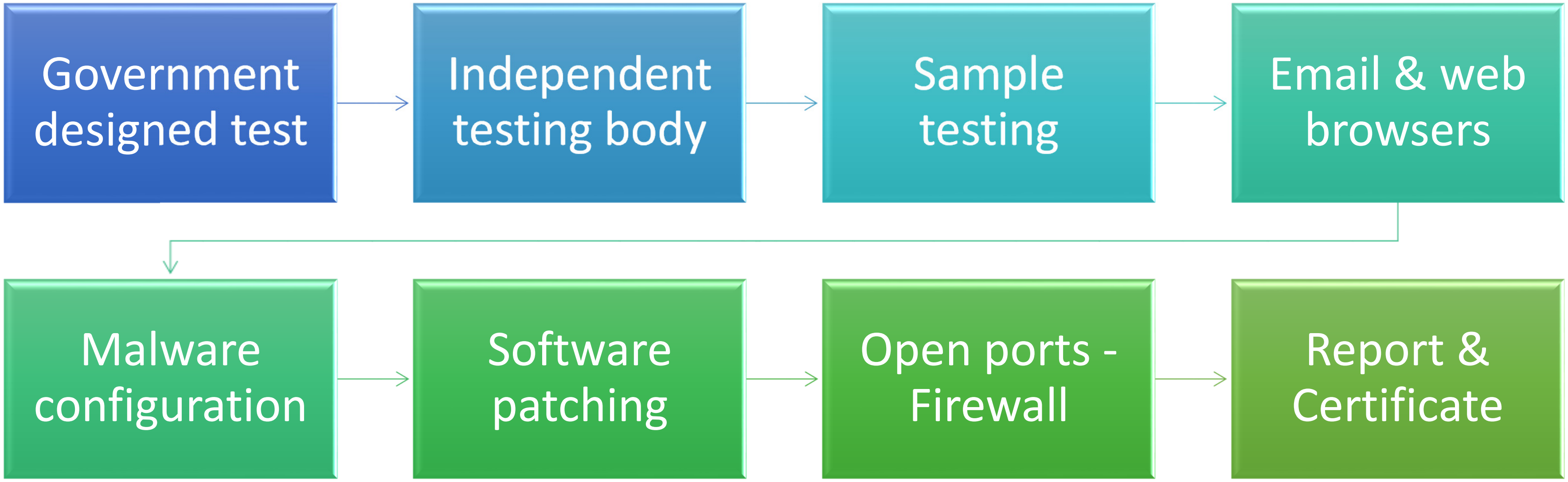
4. Malware Protection

5. Patch Management

Online SELF-CERTIFICATION

CYBER STRATEGIES
Develop • Protect • Maintain

Cyber Essentials Plus process



Government designed test

Independent testing body

Sample testing

Email & web browsers

Malware configuration

Software patching

Open ports - Firewall

Report & Certificate

CYBER STRATEGIES
Develop • Protect • Maintain

Boundary Firewalls

Purpose

To prevent external access via Public IP address

Basic requirement

Configure hardware or software firewalls with only open ports required & with appropriate passwords

In reality

Open ports are not known and have not been reviewed since installation

Older devices still have default username and passwords

Firmware is not up to date

Takeaway actions

Document Internet boundaries

Confirm configuration settings and firmware

CYBER STRATEGIES
Develop • Protect • Maintain

Secure Configuration

Purpose

To prevent weaknesses in configurations from being exploited

Basic requirements

Ensure manufacturer defaults are reviewed and removed where not required, e.g. software installed; default users; and auto-run

Password policy deployed

In reality

“Bloatware” has not been removed and creates vulnerabilities

Users configured with Administrative rights

Inadequate password policy application

Takeaway actions

Remove unnecessary software

Review password policy

Remove Administrative rights

CYBER STRATEGIES
Develop • Protect • Maintain

Access Control

Purpose

To prevent unauthorised access via user accounts

Basic requirements

Only named user accounts used

Access to necessary data only

Administrative rights controlled

Leaver accounts actioned

In reality

Generic accounts used, e.g. reception

Little thought to data segregation and access

Users have day to day account with admin rights

Leaver accounts remain in use

Takeaway actions

Create a list of all users, necessary rights and access permissions

Compare the list to actual settings

CYBER STRATEGIES
Develop • Protect • Maintain

Malware Protection

Purpose

To prevent successful Malware attacks (predominantly via email and web downloads)

Basic requirement

Installation of auto updating anti-malware (anti-virus) software on all devices

Integrate AV with email clients and all web browsers

Daily scanning

In reality

Lack of common AV installed

No organisation wide dashboard

Mobile devices out of date

Browser extension not installed

Takeaway actions

Use one AV solution across all devices

Check integration with email and ALL browsers

Check “Last seen dates” if organisation dashboard available

CYBER STRATEGIES

Develop • Protect • Maintain

Patch Management

Purpose

To prevent known vulnerabilities from being exploited

Basic requirement

Timely installation of security patches, updates and upgrades

In reality

Biggest issue

Lack of processes and management

Reliance on Auto updating

Servers often missed

Unused software missed

Takeaway actions

A comprehensive inventory is required

Proactive patch management required

Remove unused/unnecessary software

CYBER STRATEGIES
Develop • Protect • Maintain

Summary & why start with Cyber Essentials

- Cyber Essentials provides a defined list of requirements
- No need to reinvent the wheel
- Can be delegated to internal or external IT team
- Can be independently assessed
- Can be the start to a more developed security system
- Can prevent around 80-90% of current threats - GCHQ

CYBER STRATEGIES
Develop • Protect • Maintain