National Cyber Security Centre
a part of GCHQ

Guidance

Common Cyber Attacks: Reducing the Impact

Created: 18 Jan 2016
Updated: 07 Oct 2016
Part of: 10 Steps to Cyber Security (/guidance/10-steps-cyber-security)
This white paper explains how basic security controls can protect organisations from the most common cyber attacks.

Common Cyber Attacks: Summary of the White Paper

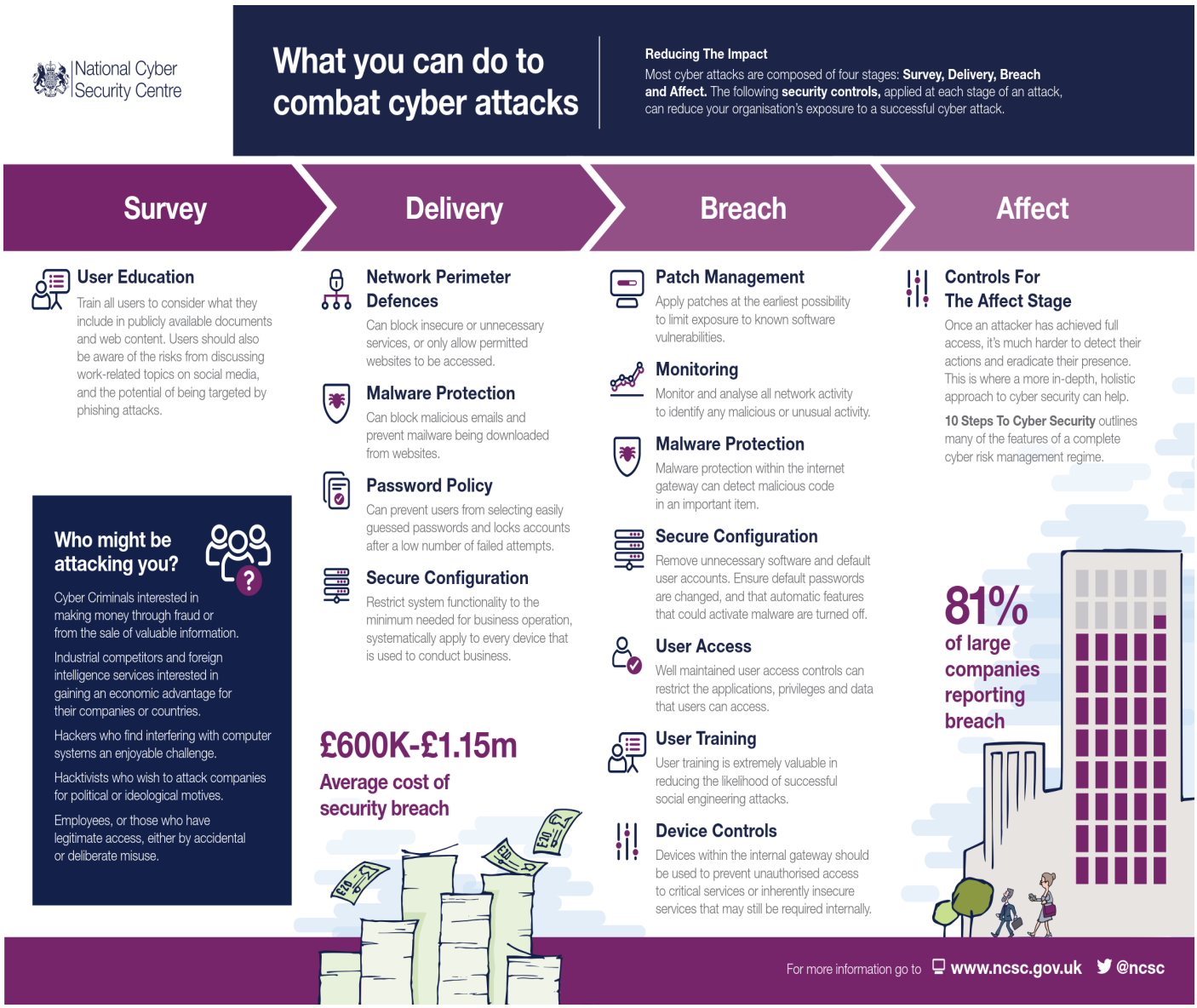
Common Cyber Attacks: Reducing The Impact helps organisations understand what a common cyber attack looks like and explains why all organisations should establish basic security controls and processes, to protect themselves from such attacks. The full version can be downloaded here (PDF)(/file/1477/download?token=3n7aC5e).

It can be read alongside the recently updated 10 Steps to Cyber Security, which offers more comprehensive guidance on the practical steps organisations can take to improve the security of their networks and the information carried on them.

The paper does not provide a comprehensive review of sophisticated or persistent attacks, nor a detailed analysis of how those attacks occurred.

Common cyber attacks at-a-glance

The following infographic summarises the security controls you can apply to reduce your organisation's exposure to a successful cyber attack.



Download the NCSC Common Cyber Attacks Infographic (PDF)(/file/1501/download?token=XQzGHISg)

The threat landscape

Before investing in defences, many organisations often want concrete evidence that they are, or will be targeted, by specific threats. Unfortunately, in cyberspace it is often difficult to provide an accurate assessment of the threats that specific organisations face.

However, every organisation is a potential victim. All organisations have something of value that is worth something to others. If you openly demonstrate weaknesses in your approach to cyber security by failing to do the basics, you will experience some form of cyber attack.

Reducing your exposure to cyber attack

Fortunately, there are effective and affordable ways to reduce your organisation's exposure to the more common types of cyber attack on systems that are exposed to the Internet. The following controls are contained in the Cyber Essentials, together with more information about how to implement them:

- boundary firewalls and internet gateways - establish network perimeter defences, particularly web proxy, web filtering, content checking, and firewall policies to detect and block executable downloads, block access to known malicious domains and prevent users' computers from communicating directly with the Internet
- malware protection - establish and maintain malware defences to detect and respond to known attack code
- patch management - patch known vulnerabilities with the latest version of the software, to prevent attacks which exploit software bugs
- whitelisting and execution control - prevent unknown software from being able to run or install itself, including AutoRun on USB and CD drives
- secure configuration - restrict the functionality of every device, operating system and application to the minimum needed for business to function
- password policy - ensure that an appropriate password policy is in place and followed
- user access control - include limiting normal users' execution permissions and enforcing the principle of least privilege

If your organisation is likely to be targeted by a more technically capable attacker, give yourself greater confidence by putting in place these additional controls set out in the 10 Steps to Cyber Security:

- security monitoring - to identify any unexpected or suspicious activity
- user training education and awareness - staff should understand their role in keeping your organisation secure and report any unusual activity
- security incident management - put plans in place to deal with an attack as an effective response will reduce the impact on your business

Raising your cyber defences

The Internet can be a hostile environment. The threat of attack is ever present as new vulnerabilities are released and commodity tools are produced to exploit them. Doing nothing is no longer an option. Protect your organisation and your reputation by establishing some basic cyber defences to ensure that your name is not added to the growing list of victims.

NCSC Common Cyber Attacks White Paper.pdf
(https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/common_cyber_attacks_ncsc.pdf)

PDF, 725.53KB

This file may not be suitable for users of assistive technology.

NCSC Common Cyber Attacks Infographic.pdf
(https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/NCSC%20Cyber%20Attacks.pdf)

PDF, 275.31KB

This file may not be suitable for users of assistive technology.

Topics

Risk management(/topics/risk-management)
Cyber attacks(/topics/cyber-attacks)

Was this guidance helpful?

We need your feedback to improve this content.

Yes No