Cyber Security Benchmark

Making A Start, Taking Control

Taking control of your Cyber-Security begins with awareness. Awareness means knowing where you are vulnerable, knowing why, and knowing how serious those vulnerabilities are so that you can prioritise fixing them. In the long term, awareness means knowing what changes to make to your organisation, your skills, and your working practices, to ensure you are less vulnerable in the future than you have been in the past. Awareness is that first step into the virtuous cycle of information security risk management. 360is will get you started with better information security risk management by giving you that initial awareness.

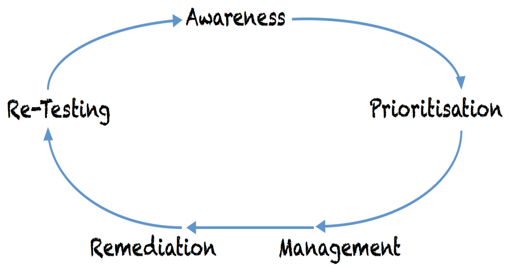

Figure 1. Information Security Virtuous Cycle

What Is The Cyber Security Benchmark?

Our Cyber Security Benchmark will make you aware of the prevalence and seriousness of vulnerability to Cyber-attack of your Internet-facing infrastructure by providing you with answers in a straightforward 1-page report.

- The number of security vulnerabilities in the network
- The seriousness of those vulnerabilities
- How your organisation compares with its peers
- What working practices should be improved
- A security consultant’s observations on this snapshot

Physical, Virtual, Cloud, Service, it's all the same to the hacker. It's infrastructure whether you own it, rent it, or share it with a thousand other organisations. Whether it's on your site or in someone else datacentre, any security weakness in it means your users, your data, and your business is at risk. Sometimes just one significant vulnerability is all it takes to destroy your reputation, your customers trust, and your business. Strong Information Security requires a firm foundation. Infrastructure is that foundation. Take control of your risk.

Using The Cyber Security Benchmark

Exactly how you use this information and what you do with it within your organisation is up to you. Here are some suggestions from our work with existing clients:

- Use it to justify a penetration test or vulnerability assessment, safe in the knowledge that there are enough weaknesses to make the exercise worthwhile
- Use it to judge how well your existing security products are configured and working (or not)
- Use it to judge how well your staff are coping with the challenge of keeping the perimeter secure
- Use it to judge how well your security partner or service provider is at doing their job

60% of cyber-attacks are purely optimistic, you are attacked because you are vulnerable.

25% of attacks are focused industrial espionage, data theft, or financial crime.

70% of investigated data breaches are at companies with less than 100 employees.

£35K to £65K is the average cost of a data breach to a small UK firm.

5 minutes is all it takes to get in touch with us about improving your IT security.

Restrictions & Limitations

This report is provided free of charge to those with the authority to grant permission to survey the network. There is no catch. However you should be aware that:

- This is not a full penetration test or vulnerability assessment and it is not a substitute for one
- While accurate and evidence-based, the report is only a brief summary
- The focus is on awareness, rather than the range of remediation activity

Once you are aware of the size and scale of your organisations vulnerabilities, you can take the next step in investigating, mitigating, and managing them.

@Three_Sixty_IS
360is Ltd
info@360is.com

Three Sixty Information Security Ltd (360is Ltd) is a UK owned and operated Cyber Security professional services provider established in 2002 with offices in Cambridge & London. This document and the 360is logo are Copyright 360is Ltd 2016. Cyber Essentials is a trademark of the Secretary of State for Foreign and Commonwealth Affairs.

Cyber Security Benchmark

360

Scope

Infrastructure	☒	External	☒
Application	□	Internal	□
Wireless	□	Endpoint	□

Network Address/Mask 193.159.228.32 / 28
Exclusions
URLs ____________________

Methodology

A black-box security assessment of hosts associated with the infrastructure, conducted without credentials or trust. Identifying devices and vulnerabilities, given a hacker's eye view. An attempt to circumvent perimeter security to access and exploit systems using non-disruptive means.

Authority

Guy Muller, IT Director, BVOE
Wednesday, 26 October 2016

Severity

#	Vulnerability	Rating
1	Microsoft Schannel Vulnerability	CRITICAL
2	Microsoft IIS HTTP.SYS Vulnerability	HIGH
3	SSL Heartbleed Vulnerability	HIGH
4	SSL Certificate Invalid	MEDIUM
5	PHP <4.4.1 Multiple Vulnerabilities	MEDIUM

Figure 3. Ranking, top 5 of 20 detected vulnerabilities

Ratings above are based upon your network, the role and importance of your systems, and the value of the data stored on or processed by them. Where a given vulnerability is present on multiple systems and those systems are of differing value (e.g. production and test systems) the higher rating is listed. For this reason vulnerabilities may be rated higher or lower here than in generic vulnerability databases that do not take account of asset value.

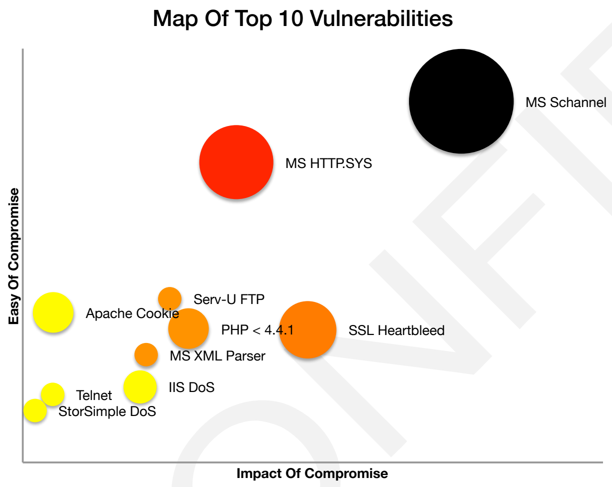

Figure 2. Mapping, top 10 of 20 detected vulnerabilities

Unsupported OS/Application for which no further security updates are being produced.

Unpatched, vulnerable Operating System or application detected.

Incorrect, insecure, out-dated, or ill-advised deployed configuration detected.

Unprotected/unfiltered network service(s) exposed to the Internet.

Ill-advised, bad, or faulty network design detected.

Figure 4. Top 5 of 5 implied organisational weaknesses

Consultant's Comments

Firewall rules were in place but some exposed services were found and some of those services were vulnerable either in their configuration or lack of patches/updates. At least 1 unsupported or unmaintained system was detected. The configuration of encryption services upon which a high level of trust is placed could be improved. These services are a target for hackers, advice changes frequently and patches are released often. You may wish to retain a subject matter expert to deploy SSL/HTTPS and to keep it secure. There did not appear to be any discernable DMZ configured for what would normally be restricted, semi-public services.
Overall these results would place BVOE in the bottom 20% of their peer group, with a score of D.

@Three_Sixty_IS
360is Ltd
info@360is.com

Three Sixty Information Security Ltd (360is Ltd) is a UK owned and operated Cyber Security professional services provider established in 2002 with offices in Cambridge & London. This document and the 360is logo are Copyright 360is Ltd 2016. Cyber Essentials is a trademark of the Secretary of State for Foreign and Commonwealth Affairs.

CYBER ESSENTIALS