ProtectUK

Cyber security

Original publication date
02/11/2020

1. Introduction

Many organisations rely on computer systems to carry out business or nationally critical functions and employ digital technologies to manage safety, security and engineering systems. As a result, businesses can become vulnerable to threats that undermine their confidentiality, integrity or accessibility. The consequences of such incidents can be significant to organisations, leading to loss of reputation, damage to assets, regulatory fines or result in physical injury.

In order to understand the cyber risk to business, a Cyber Risk Assessment should be conducted. This will help to make sure that the approach to cyber security is proportionate. While there is no specific format for this, it should be based on the Risk Management processes detailed below.

Risk assessing is a continuous, on-going process which you will need to revisit as your business changes and/or threats evolve.

Cyber Security Checklist



2. Assessing the risk

The following three step process will help you identify:

- the digital technologies and systems which are most important to your business
- who might attack them
- how they might be vulnerable

This information will allow you to narrow down what you must protect.

Step 1: Impact

What are you trying to avoid?

Your approach to cyber risk management should be driven by the impacts you are trying to avoid. Start by identifying the systems, data and technologies on which your business relies. The type of questions you might want to ask are:

- is there technology that must be available for the business to function? For example, payment systems or access controls.

- do physical security systems rely on digital technology? How are they protected?
- is personal or financial data being processed? If so, what if this data is lost, stolen or unavailable?
- are third-party systems relied upon? If so, which systems are central to your business?

If you take a systematic approach, you should be able to produce a prioritised list. You then need to consider the impact of these systems being compromised or becoming unavailable. This basic understanding of what you care about and why it's important, will help you identify what you must protect.

For further information:

National Cyber Security Centre's (NCSC) Risk Management guidance

Step 2: Threats

What type of attacks can you expect?

A 'threat' is the individual, group or circumstance, which could cause a given impact or incident to occur.

It can be challenging to develop an accurate assessment of the threat to your business without undertaking an appropriate analysis.

However, the following will help you develop a baseline threat picture:

- **Commodity attacks**: All organisations and events, regardless of profile and size, are at risk from commodity attacks that exploit basic vulnerabilities using readily available hacking tools and techniques. Mass phishing emails are one example of such an attack.
- **Targeted attacks**: Some businesses will be targeted by cyber criminals who, for example, intend to steal financial or personal information, e.g. spear phishing. See How Cyber Attacks Work for further information about targeted attacks
- **Methodology**: Most attacks are preventable and use well-known techniques. The NCSC Cyber Threat to UK Business and Fortnightly Threat Reports will help understand the latest trends
- **Insider threat**: Not all threats are external. It is essential that internal threats are incorporated into your assessment. See the NSCS's - Reducing data exfiltration by malicious insiders for further information

- **Learn from experience**: Has your business or similar businesses previously experienced cyber-attacks? How could those attacks have been prevented?

With some research, you should be able to develop a baseline threat assessment. For example, you may decide that your business is unlikely to be deliberately targeted, therefore commodity attacks exploiting basic vulnerabilities are the main threat.

Alternatively, you may discover that businesses of similar profile have been targeted by organised crime groups, therefore the threat is heightened and specific defensive measures are required.

It should be noted that most targeted attacks still use basic techniques, such as phishing emails, to enable attacks.

Step 3: Vulnerabilities

How secure are the computers, networks and systems you rely upon?

The final stage of the process is identifying your vulnerabilities. A ‘vulnerability’ is a weakness that would enable an impact to be realised, either deliberately, or by accident.

You should start by overlaying your critical systems (see ‘Impact’, above), with the expected capabilities of any attackers (see ‘Threats’, above).

Next, focus on establishing whether the security controls for each critical system are appropriate for the threat. Remember, most cyber attacks are preventable if basic controls are in place.

NCSC ‘Common Cyber Attacks: Reducing the Impact’.



Systems supplied by third parties

Identify who is supplying your critical systems and establish a clear picture of each supplier's cyber security posture.

A good starting point is to ask whether your suppliers hold any existing security certifications (e.g. Cyber Essentials, Cyber Essentials Plus, ISO 27001). Holding a certification indicates that the supplier has a proactive approach to cyber security.

If suppliers do not hold any certifications, you will need to invest time to understand more about their security posture. From an IT infrastructure perspective, you may wish to use the Cyber Essentials themes as discussion points, these include:

- firewalls
- secure configuration
- user access control
- malware protection
- patch management

For providers of online services, you may wish to focus your discussion on the common web application security issues. The Open Web Application Security Project (OWASP) Top 10 is a good starting point.

There are other sources of useful information relating to systems supplied by third parties:

- specifically for Video Surveillance Systems (CCTV), the Surveillance Camera Commissioner operates the Secure by Default self-certification scheme
- for more complex physical security systems, NPSA (formerly CPNI) has developed the CAPSS (Cyber Assurance of Physical Security Systems)
- the NCSC Mobile Device Guidance offers advice on the purchase and use of different operating systems, biometrics and advice to the end user

If any of your suppliers are unable to meet your security expectations, you should update your Risk Register and consider mitigations. The NCSC Supply Chain Security collection offers detailed advice on how to manage supply chain risk.

3. Use NCSC guidance

Beyond the advice signposted above, the NCSC website has a collection of guidance suitable for organisations of all sizes. Included within this guidance is a Board Toolkit, which provides resources designed to encourage essential cyber security discussions between the board and their technical experts.

For further information, please go to the NCSC 10 Steps to Cyber Security

KEYWORDS
CYBER SECURITY
THREAT
ATTACK METHODOLOGY
CCTV
ACCESS CONTROL
PALS GUIDANCE
PUBLICLY ACCESSIBLE LOCATIONS