equilibrium risk
security & risk management

Guide to
Cyber Protection

Guide to
Cyber Protection

Introduction

Hello and welcome to our guide to cyber protection. In this guide, when we talk about cyber protection, we are talking about protecting anything that is connected to the internet or is networked. This can include your desktop computers, your laptops and even your operational technology such as machines or robots.

We understand that cyber protection can be very technical, our aim here is to be as untechnical as possible, leaving the technical stuff to our experts!

We have started with the basics of cyber protection in the office environment, and then provided further information about how you can build on the basics and achieve extra resilience.

We have also included a section about Operational Technology (OT). While IT cyber protection is mainly about protecting information, OT mainly deals with protecting machines. A simple distinction is IT is the office, while OT is the factory floor.

Scope

The most effective way of protecting your cyber assets is to carry out a full security analysis to highlight what the problems are, how to deal with them and what to do when things go wrong. This document provides only general guidance on cyber protection.

For more detailed guidance specific to your business, please get in touch.

Basic Guidance for Office

Cyberattacks against your IT devices come in many shapes and sizes, such as phishing attacks, malware or ransomware. But most are basic in nature, carried out by unskilled perpetrators.

Our IT Cyber Protection advice is in the shape of 1 educational control and 8 technical controls. They are designed to guard against the most common cyberattacks.

Following our advice allows you to attract new business with a promise you have cyber security measures in place and to reassure your existing customers that you are working to secure their information against a cyberattack.

3M Buckley Innovation Centre, Firth Street, Huddersfield, West Yorkshire, HD1 3BD
Telephone: 01484 505321 | Enquiries: enquiries@equilibriumrisk.com

Awareness Training

Cyber security awareness training is about training your staff to be aware of the consequences of their actions. By making small changes in the way your employees work, you can greatly increase the safety of your business. To be successful, your training should be iterative with lessons learnt from mistakes made in the training modules.

Firewalls

Acting in the same way as the perimeter fence of your business, all internet traffic should be controlled through a firewall. A firewall effectively creates a buffer zone and can analyse all incoming traffic to find out whether it should be allowed onto your network.

Secure Configuration

Securely configuring your devices ensures they are as secure as possible. When devices are made, the default configuration is for software to be open and as multi-functional as possible. Unfortunately, this can provide opportunities for cyber criminals to exploit. Laptops, phones, tablets and printers are all a target for cyberattacks that need securing.

Access Control

Much like access control in the physical world, controlling who and when someone 'enters' your business is crucial. Moreover, when a member of staff accesses your network, they should have just enough access to software, online services, and information for them to perform their role. Extra permissions should only be given to those that need them.

Malware Protection

Malware protection protects your devices from 'malicious software' such as ransomware and/or viruses. There are various ways in which malware can find its way onto a device, and there are several ways in which we can defend against malware, such as anti- malware software, whitelisting and sandboxing.

Up-to-date Software

Keeping your devices up to date is one of the most important things you can do to improve security. As well as updating features, an update will also fix any security vulnerabilities that have been discovered. Operating systems, programs, apps or phones should all be updated wherever there is an option.

Remote Working

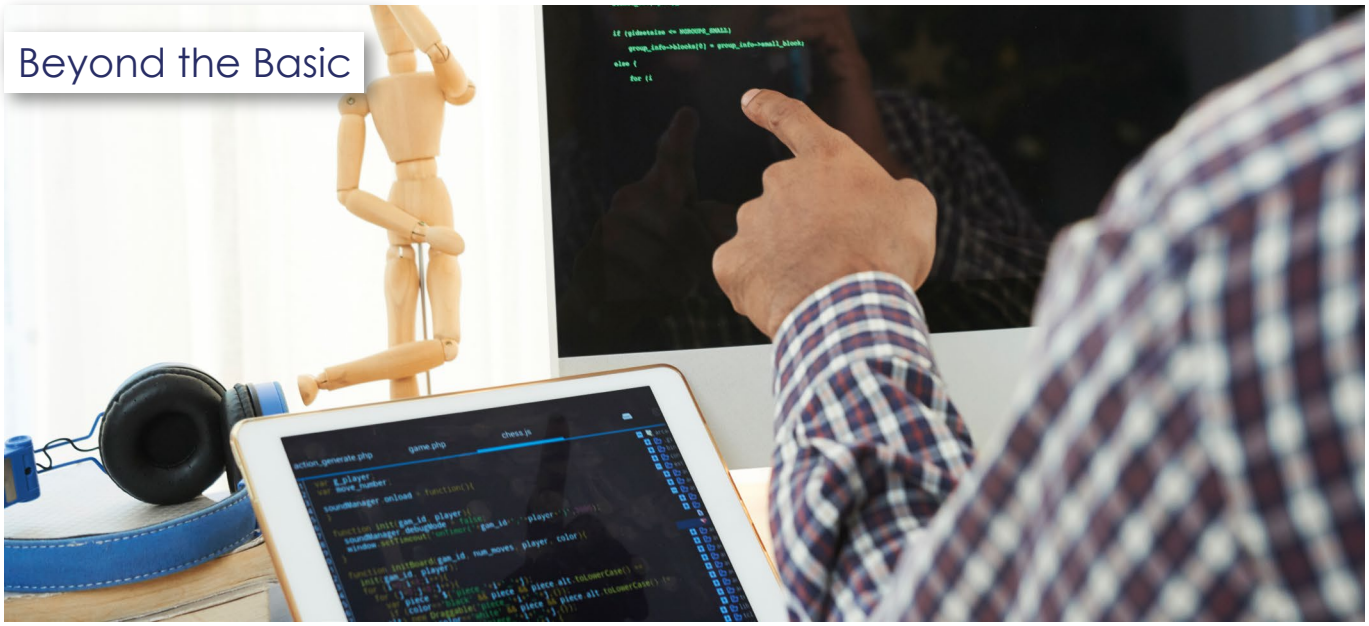
In the modern workplace, more and more staff are working remotely. You should consider how data is protected both in transit and at rest. Develop a way for your staff to work without exposing your business and ensure they stick to it.

Removable Media Controls

Controlling the use of removable media in your business will have a big impact on the security of your business. Limit the types of media your staff can use and create a policy that scans all media for malware before importing onto your business network.

Vulnerability Scanning

A vulnerability scan will inspect your network for potential points of exploit. You should expect a vulnerability scan to detect and classify system weakness in your computers, networks and communications equipment. They should also assess the effectiveness of any countermeasures you deploy. Because of the nature of technology, vulnerability scans should be automated or conducted on a regular basis.



Putting these controls in place will put you and your organisation on the path for better cyber security. However, more organised criminals will be better prepared, so you need to be able to detect when your defences are being breached. Where there is a heightened level of risk, we recommend implementing additional protection.

Penetration Testing

Penetration testing, or pentesting, is a simulated attack on your computers or cyber assets. There are many different types of test, but they should be used to reinforce your security posture. Much like an audit, a pentest should provide assurance that your organisation's current security management processes are enough.

Monitoring

There are two different types of cyber security monitoring, network monitoring and endpoint monitoring. But the aim is the same: to give you the earliest warning possible that something is not right. Effective monitoring should continuously monitor all systems and networks, analysing logs for unusual activity that could indicate an attack.

Incident Management

The basic concept of an incident management plan is to stop a malicious act from adversely effecting your business as quickly as possible. Your incident management plan should detail immediate actions, how to escalate a response and post incident actions. The aim is to get your business back operating normally as quickly and efficiently as possible.

Guidance for the factory floor

Cyber-attacks on critical and industrial infrastructure are on the rise, impacting operational reliability and business risk across all industries, including utilities, manufacturing, and oil & gas. Threats to operational technology (OT), the hardware and software dedicated to monitoring and controlling physical devices such as valves, pumps, machines and robots, can disrupt operations. It can negatively impact productivity, causing ecological damage & compromising human safety.

To achieve more robust protection for cyber assets, you should base your security on the security in depth principle. This implies that each layer of defence becomes a delay and if any single layer should fail the threat will be contained by the subsequent layer. The protection measures below overlap each other- where the weaknesses of one layer is overlapped by the strengths of the next.

Separate Networks

Following a detailed network map, you should separate your networks based on their major function. For example, you could divide a network into enterprise, plant, process, and field zones. Each conduit between each zone should be carefully identified.

Perimeter Protection

Once each conduit has been identified, they should be properly protected. An important part of this step includes securing remote access.

Network Segmentation

Within your networks, you should then divide them into smaller zones based on location or function. The perimeter of each of these segments should then be protected. A different Security Level can be assigned to each segment (see table below).

Device Hardening

To reduce the likelihood of a network element being compromised, you should add features to each of your devices that will improve their ability to withstand a cyberattack. This should prevent a hacker accessing your network.

Monitor & Update

As with IT Cyber Protection, you should monitor your networks to detect any potential threats. You should also ensure that all software/ firmware remains up to date with the latest patches. This will address any known vulnerabilities and add security features.
Based on the IEC 62443 standards, our services help you bring your cyber protection to one of the four levels.

Security Level	Target	Skills	Motivation	Means	Resources
1	Casual or coincidental actions	No attack skills	Mistakes	Non-intentional	Individual
2	Cybercrime, hacker	Generic	Low	Simple	Isolated individual
3	Hacktivist, terrorist	ICS specific	Moderate	Sophisticated	Hacker group
4	National state	ICS specific	High	Sophisticated	Multi-Disciplinary

Summary

I hope you have found this document of use. Remember, the most effective way of protecting your data or networked assets is to carry out a full security analysis to highlight what the problems are, how to deal with them and what to do when things go wrong. This document provides only general guidance on cyber protection. If you would like to discuss ways we can help build an effective and balanced security plan, then please get in touch.

3M Buckley Innovation Centre, Firth Street, Huddersfield, West Yorkshire, HD1 3BD
Telephone: 01484 505321 | Enquiries: enquiries@equilibriumrisk.com