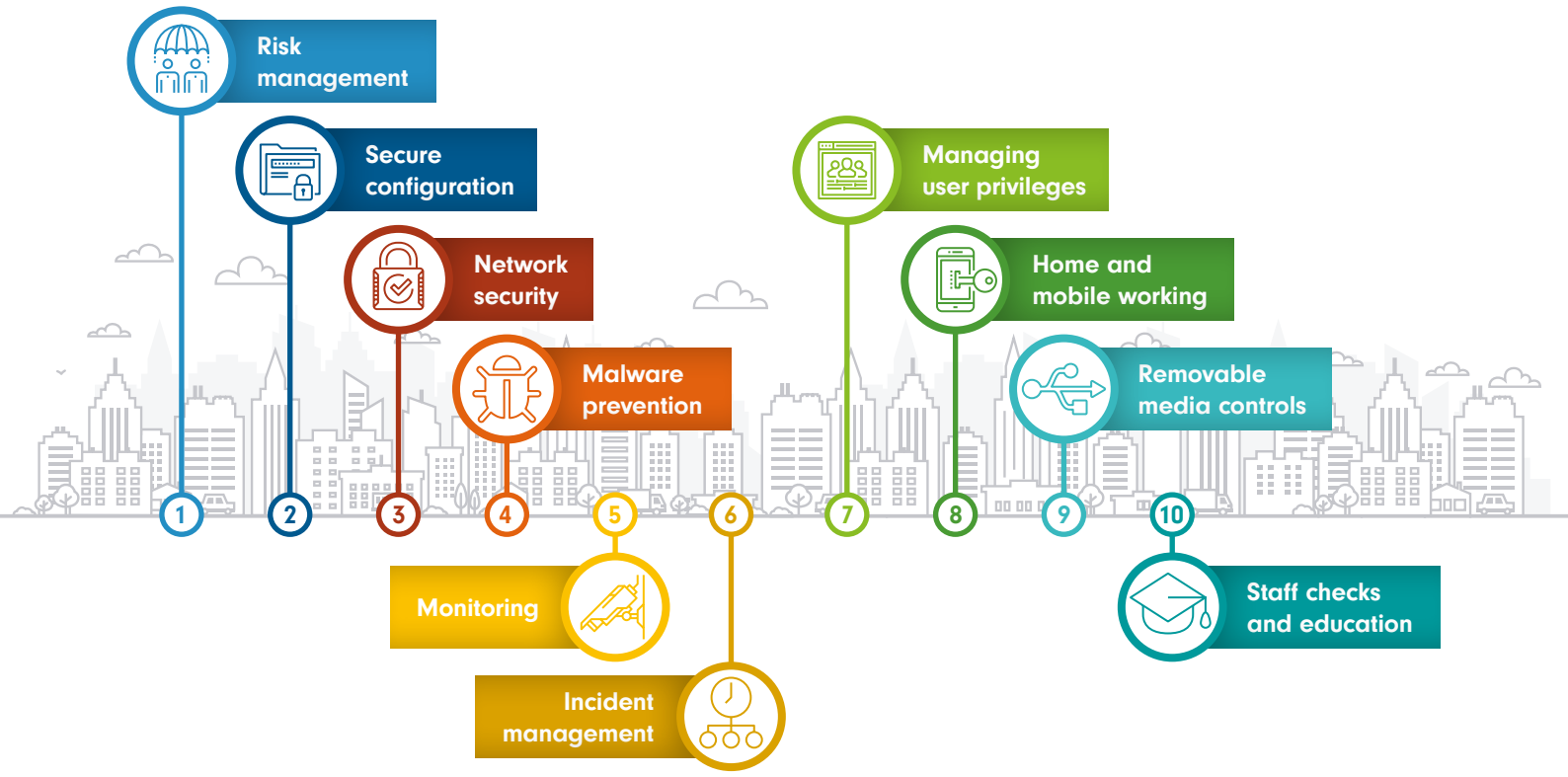
10 steps to protect your business from a cyber attack

According to the National Cyber Security Centre (NCSC), there were 796 cyber attacks between October 2016 and the end of 2017[1]. The NCSC expects attacks to increase and has specifically identified financial services as a targeted sector. Despite this serious threat, only 6% of advisers say that cyber security is one of their top three business challenges[2].

Cyber security's core function is to protect the services you offer to clients from theft or damage and preventing unauthorised access to their personal data. This involves safeguarding your systems and the devices your employees use, such as computers, laptops, tablets and smartphones, from attack. Protecting your business from cyber risks can seem daunting but there are effective and affordable ways to reduce your firm's exposure to the more common types of attack. The following recommendations are based on the National Cyber Security Centre's 10 Steps to Cyber Security and can reinforce the protection your business already has in place.

1. Source: https://www.ncsc.gov.uk/cyberthreat
2. Source: FundsNetwork Business challenges facing financial advisers report, February 2019

What's covered...



FundsNetwork

Fidelity INTERNATIONAL

Set up your risk management regime

Establishing an effective governance structure to determine your firm's risk appetite is key to identifying potential threats and managing responses. You rely on technology, systems and information to run your business. It is therefore essential that you apply a similar level of rigour to assessing the risks to your technology, systems and information as you would to other business risks, such as regulatory, financial or operational risks.

After risks have been assessed, the next step is embedding a Risk Management Regime across your business, supported by the Board and senior managers. This will help define and communicate your firm's attitude and approach to risk management and help ensure that employees, contractors and suppliers are aware of your firm's risk management boundaries and policies.

1 2 3

Secure configuration

Security should be built in from the ground up. A secure baseline build for all your systems and devices (including hardware and software) is vital as is limiting the ability of staff to change system configurations. In addition, you should remove or disable unnecessary functionality from your systems.

Using supported software and running patching will help fix known vulnerabilities and should be performed on a regular basis. Conducting vulnerability scans, which can be run by automated scanning tools, is also highly recommended.

Network security

The connections from your networks to the internet, and other partner networks, could expose your systems and devices to attack. By creating and implementing simple policies and appropriate responses, you can reduce the chances of these attacks succeeding or causing harm to your business.

You may find it helpful to follow a recognised network design principle to help build appropriate security architecture. Pre-defined standards such as the ISO/IEC 27000-series (also known as the 'ISO 27000 Family of Standards') constitute a set of security standards that provide a globally recognised framework for best-practice information security management. They will assist you in building a robust security framework enabling your business to control and manage inbound and outbound network connections, deploy technical controls to scan for and define malicious content, protect your internal network and monitor and test security controls.

Malware prevention

Any electronic exchange of information, including email, web browsing and removable media, carries with it the risk that malware (malicious software) might be introduced into your systems.

To help mitigate this risk, develop and implement anti-malware policies and standards and ensure they are consistently implemented across your infrastructure. These should include scanning all data for malicious content at the network perimeter, installing firewalls, deploying antivirus and malicious code checking solutions and blocking access to known malicious websites.

Monitoring

System monitoring aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to respond effectively. It also allows you to check that systems are being used appropriately in accordance with organisational policies.

All networks, systems and services should be included in your firm's monitoring strategy. This should ideally include an Intrusion Detection System (IDS) monitoring inbound and outbound network traffic for malicious activity or policy violations. These could be connections from unexpected IP ranges overseas, large data transfers and unauthorised or accidental misuse of systems or data. Critically, it should be able to tie specific users to particular instances of suspicious activity.

4 5 6 7

Incident management

Security incidents will inevitably happen. It's worth remembering that incidents not only can cause harm to your business, they can result in the compromise of sensitive information that could lead to legal or regulatory penalties, and result in reputational damage to your firm.

Establishing effective incident management policies and processes will help improve resilience, support business continuity, improve customer confidence and potentially reduce any negative impact. These processes will typically include establishing data recovery (back up) capabilities, appointing, training and empowering specific employees to make decisions throughout an incident and regular testing of all security-incident management plans (including business continuity and disaster recovery plans).

Managing user privileges

A privilege is the right of a user to perform a particular system-related operation. Managing privileges is made easier by using roles and granting system privileges to those roles – and then granting roles to users. Granting staff unnecessary system privileges or superfluous data access rights can be just as problematic as not allowing a user enough privileges or access. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. These rights should be monitored and reviewed regularly, especially when a user is moving role or leaving the company. Establishing robust user authentication (password) standards is also recommended and access to activity and audit logs should be controlled.

Home and mobile working

Mobile working and remote system access offer great business benefits but come with risks that need to be managed. Establishing risk-based policies and procedures that support mobile working and remote access to systems – by staff as well as service providers – is very good practice.

A secure baseline build and configuration should be applied to all devices. If the user is working remotely, any information exchanged with the corporate network should be appropriately protected, ideally using a Virtual Private Network (VPN). All corporate data should be stored on the corporate network rather than the mobile device and the ability to copy data out, or print files, should be carefully controlled.

Removable media controls

Removable media, such as memory sticks, discs and USB flash drives, provide a common route for the loss of sensitive data and the introduction of malware. Your firm should therefore apply appropriate security controls to using removeable media, including automatically scanning for malware. Other recommended procedures include restricting their use to only necessary functions, encrypting data held on them and actively managing their reuse and disposal. Where used, it is a good idea to make the user accountable for the media's use and safe keeping.

8 9 10

Staff checks and education

Staff have a critical role to play in your firm's security and they should be supported through awareness and education programmes and regular training. A good Information Security programme can deliver security expertise and help to establish a security-conscious culture. All staff (including contractors and third-party users) should be made aware of security policies and understand the disciplinary process for any abuses. A well-designed induction process and regular refresher training is vital to keep up-to-date with the fast-moving environment of cyber security and will help inculcate an incident reporting culture within your firm.

How we protect you and your clients

FundsNetwork understands the importance of keeping your firm's and your clients' information safe and secure. We use proven, industry-recognised security tools and processes to protect against fraud and security breaches and we regularly upgrade this protection in response to advances in security threats.

Fidelity is a member of Cifas, the UK's fraud prevention agency, which works closely with law enforcement partners. Cifas Protective Registration is a fraud protection scheme that helps us protect your clients should they be at risk of fraud.

If you have any concerns about security, please call us as soon as possible on 0800 358 7717.

More advice from the National Cyber Security Centre can be found on ncsc.gov.uk

FundsNetwork

Fidelity™ INTERNATIONAL