A growing threat

Cyber security is an increasing threat to organisations. We look at cyber risk trends and emerging perils and explain how they can be mitigated.

The key to effective security is to have a layered approach, combining a number of different tools and techniques – if one layer fails then others are in place to catch the threat.

The protection legislation could lead to your business incurring a fine – up to £50,000 in serious cases. For many, however, particularly larger and more well known businesses, the reputational damage could be much worse – not only can you be negatively impacted by a loss of data or a system attack, but also by being unable to demonstrate that you are taking steps to meet best practice.

Risk cannot be totally eliminated but it is extremely important to be able to demonstrate that you have done everything reasonably practicable to ensure it is an acceptable level.

The following are basic measures that you can put in place to prevent security breaches or limit the damage if they do occur:

Step A: Assess the risk to your business. Before you can establish what level of security is right for your organisation, you will need to know the personal data you hold and assess the associated risks. You should consider what personal data you collect, store, use and dispose of personal data.

Step B: Document your policies and procedures to clearly state how you will manage data security and cyber risks. Defining your policies and written procedures provides clear direction and guidance to your staff and allows you to perform regular checks that they are being followed. It also provides a baseline for continual review to evaluate improvement.

Step C: Consider how valuable, sensitive or confidential the information is and what damage or cost impacts for individuals if there was a security breach. This enables your decisions and management of controls to be risk informed and ensure that you are prioritising what is most critical and important to control. This includes stakeholders such as investors and insurers.

By taking a clear view of the risks, you can begin to choose the security measures that are appropriate for your circumstances. The aim is to create physical and/or administrative controls to reduce the impact of a breach to an acceptable level. You need to ensure that the likelihood and severity of any undesired event is minimised, but also that monitoring and the effective if it does happen. Effective management of crises critically depends it will help foster trust arrangements – tested and ready – covering not only the technical measures that are effectively and efficiently with customers and the media so that you are informed and in full control of the situation.
Take the time to review what personal data you currently have and the means of protection you have in place. Make sure you are compliant with any industry guidance, legal requirements or contractual obligations. Document the controls you have in place and identify where you need to make improvements.

If your system is a few years old, you should review the controls compliance and that they are effective, and make adjustments where necessary. Consider the risks for each... covers personnel competence and have training materials so that everyone knows their data protection responsibilities.

Keep your systems up to date:

● Software needs to be regularly scanned to identify any vulnerabilities which can then be addressed. Review copies of the security assessments of your IT providers and if appropriate, visit the premises of your IT provider to make sure they are as you would expect.

● You also purchase hardware, software used to disrupt... attacks, then attackers can use these to access your network, and even upload or download malicious files. You may be able to prevent breaches happening before they become uploaded to your systems without the approval of the appropriate national professional bodies.

● The system must be designed to prevent or detect threats and make sure they are kept up to date. You should not allow any unauthorised software or data to be uploaded to your systems without the approval and control of competent persons.

Intrusion defence: You need to be able to prevent breaches happening before they penetrate deep into your network, for example by using a well-configured firewall and real-time detection software to alert you to threats and attacks. The sooner you know you have an attack, the more quickly you can respond to the situation. Intrusion may originate from within your organisation as well as outside of it.

Access controls: Restrict access to your system to users and sources you trust. Each user must have their own username and password. A brute force password attack... limit the number of failed login attempts and put into effect proper password changes.

Segmentation: You can prevent or limit the severity of data breaches by separating... compromise, the attacker will not have direct access to your central data store.

Documented management system:

A formal documented management system, including policies and procedures, will enable you to make sure you address the risks in a consistent manner and clearly communicate to your employees what is expected of them. Well-written documents should integrate well with your business processes. Compliance with the management system and its effectiveness should be continually monitored, reviewed and, if necessary, amended to ensure that it remains fit for purpose.

Device hardening: Remove unused software and services from your devices. Older versions of some widespread software have well documented security vulnerabilities. If you don’t use it, then it is much easier to remove it than try to keep it up to date.

Make sure you have changed any default passwords used by software or hardware – these are well known by attacks. Secure your data on the move: You need to ensure that an equivalent level of security is in place.

In order to protect personal data on devices being used away from the office as well as within it.

Many data breaches arise from... You should also consider the security implications of apps you might send by email or post. You can take steps to reduce the effects of the threat by ensuring that personal data is either not on the device in the first place or that it has been appropriately secured so that it cannot be accessed.

Keep your systems up to date: Computer equipment and software needs regular maintenance and updates to ensure it is running smoothly and to fix any security vulnerabilities. Security software such as anti-malware protection should be in place in order to continue to provide adequate protection against evolving threats.

Do your customers, suppliers, outsourcing and procurement: Many small businesses outsource some or all of their IT requirements to a third party. This is to what some or all of their IT requirements are not being handled correctly. You need to ensure that the standards of your suppliers are equal to your own. You should maintain a list of approved suppliers with appropriate evidence demonstrating their competence and integrity.

More information:

● UK Government developed Cyber Essentials Scheme
● MSS 1000-2014 Management System Specification (Chartered Quality Institute, see Insight April 2016)
● ISO/IEC 27001:2013 – Information security management systems
● Industry sector trade bodies
● Relevant national professional bodies.

Download this Practical Guide at www.isrm.org/info-hub

Cyber Security

● Step E: Begin putting the measures in place. The risks will not reduce until you implement the risk control arrangements and your staff understand them and fully comply. You also need to continually monitor what you have implemented to ensure it is effective and remains so as situations change.

Data security and cyber risk mitigation measures

There is no single product that will provide a total guarantee of security for your business. The key to effective security is to have a layered approach, combining a number of different tools and techniques. If one layer fails, then others are in place to catch the threat.

Physical security: equipment containing personal data could be stolen or damaged in a break-in. You should ensure that your employees at all levels need to be aware of their roles and responsibilities and made accountable.

Employee awareness and training:

In order to ensure that personal data is either not on the device in the first place or that it has been appropriately secured so that it cannot be accessed.

Keep your systems up to date: Computer equipment and software needs regular maintenance and updates to ensure it is running smoothly and to fix any security vulnerabilities. Security software such as anti-malware protection should be in place in order to continue to provide adequate protection against evolving threats.

Do your customers, suppliers, outsourcing and procurement: Many small businesses outsource some or all of their IT requirements to a third party. This is to what some or all of their IT requirements are not being handled correctly. You need to ensure that the standards of your suppliers are equal to your own. You should maintain a list of approved suppliers with appropriate evidence demonstrating their competence and integrity.

More information:

● UK Government developed Cyber Essentials Scheme
● MSS 1000-2014 Management System Specification (Chartered Quality Institute, see Insight April 2016)
● ISO/IEC 27001:2013 – Information security management systems
● Industry sector trade bodies
● Relevant national professional bodies.

Download this Practical Guide at www.isrm.org/info-hub