Why Information Security is Everyone’s Business
Executive Summary

There are several issues that make small and medium enterprises (SMEs) more vulnerable to information security breaches. SME's or Not for Profit Organisations have fewer resources and skills than larger companies, making them especially susceptible to simple commodity Internet-based attacks. Weakness to these simple attacks can then open the door to more sophisticated attacks on the business, all of which may go undetected for some time.

In this whitepaper I am going to discuss the critical steps that can be taken to strengthen your company’s information security. The following 10 stages go through in detail' the key considerations and actions to take in securing your information security.

Neil Douglas
IT Consultancy Director

*DID YOU KNOW?*

£3,230
The amount cyber security breaches cost the average UK small business*

*Cyber Security Breaches Survey 2020

*DID YOU KNOW?*

£5,220
The amount cyber security breaches cost the average UK medium/large business*

*Cyber Security Breaches Survey 2020
Why Information Security is Everyone’s Business

Introduction

While it seems like every other week a large corporation makes the headlines for a data breach, the UK Federation of Small Businesses reported that small businesses received on average 10,000 attacks a day and the North West, South East and West Midlands are the most likely victims of a cyber-attack.

In another report National Cyber Security Alliance found that 60% of hacked small and medium-sized businesses go out of business after six months. As such, the stakes have never been higher, and Information or data must now be viewed as a business asset in the same way buildings, vehicles, staff, equipment and processes are.

What’s the worst that can happen?

With a multitude of valuable data floating around the company’s IT systems, it’s important to understand the threats to that data.

Data is at risk from a whole range of threats, yet many SMEs don’t have a risk assessment or register for their information. Depending on the location of your data – both geographically (such as in public cloud or other offices) and internally (in your buildings), some or all of the threats below may increase the risk of your company losing their data:

- **Malicious Attacks** – external attackers determined to either steal, corrupt or deny access to your data. Attackers may range in ability depending on their motivation and the value of your data and knowing who your adversaries are likely to be is essential in providing adequate protection.

- **Insider Attacks** – malicious attacks from disgruntled employees or the theft of data to sell / take to a competitor

- **Accidental Loss** – due to misconfiguration of the security controls or infrastructure – this is particularly a concern in public cloud where security may be assumed to be the cloud providers responsibility, when in fact the onus is on the customer to secure the application.

- **Human Error** – accidental loss due to unintentional disclosure or deletion – it’s not uncommon to see information incorrectly released as part of a tender process or for a user to accidentally wipe an entire folder of important data

- **Data loss** due to storing data in less well-protected cloud providers often in countries outside of the UK. If a cloud provider goes into liquidation your data could be lost when the service contracts covering the cloud providers services and hardware are terminated.

- **Attackers** who target your supply chain to either disrupt your business or attack it directly.

- **Fire or Flood** resulting in loss of key information assets – both threats can be devastating for a business, especially with increased regularity because of climate change

- **Natural disasters** such as earthquake & volcanic activity (both unlikely in the UK but may affect companies with regional offices overseas)

* UK Federation of Small Businesses
Strategic planning

Threats to your business information can take many forms. A little planning on how to prevent attacks and how to react afterwards is vital as it’s inevitable you will be breached at some point. Very few organisations (16% of businesses and 11% of charities) have formal cyber security incident management processes in place according to the UK Cyber Securities Breaches Survey in 2019.

When an incident occurs, do you know what data has been lost? Do you have planned response procedures in place including those required to meet the GDPR requirements?

Responding to a breach

Key considerations when responding to a breach include:

- When an incident occurs, do you quickly know what data has been lost? Do you get immediate alerts?
- Does your company have planned response procedures in place, including those required to meet the GDPR requirements?
- Have you got a detailed crisis management plan prepared in advance and regularly updated?
- Do you do annual scenario testing, alongside senior management media training and refresher courses? (If not, you should consider it.)

Information types

The significant increase in computer use in the early 1990s led to businesses replacing many manual processes, one by one, with some form of computer processing and inevitably, this led to the expansion of information stored on their computer systems.

It’s now commonplace for even small companies to hold all the following types of data:

- Customer Information – names, email addresses, addresses, phone numbers, credit card details, bank details, invoices and order history (often used to market to existing clients)
- Prospects Contact Details – names, addresses, email addresses, phone numbers and opportunity details.
- Employee Information – names, addresses, personal email address, next of kin contact details, pay and salary details, medical details that may impact work and performance details
- Company Data – a wide range of data ranging from internal meeting notes, emails, company databases, product information and pricing, sales data, strategy, intellectual property, trade secrets, tender details and many more.

It’s worth noting that cyber thieves recognise that many small businesses act as conduits into other larger businesses. So, a breach of your company’s systems could leave you liable for breaches of your business partners’ systems, with potential impact on your reputation and future business opportunities.

* UK Cyber Securities Breaches Survey (2019)
Storage of data

You must therefore always know where all your data is stored, and have listed every device or service that holds company data. This information should be readily to hand and definitely in your crisis manual.

Information Value

It’s common for businesses to have no idea of the value of their data, even though there are businesses where nearly the whole company’s value comes from data – Facebook and Google to name two.

As a business, it’s important to understand that information or data is an important asset. Some commentators are now describing data as the world’s most valuable resource, instead of oil (according to the Economist)

All assets have value, and information is no different. What makes information different though, is that it has serious value not only to your company, but to others.

The value in an asset doesn’t just cover the purchase cost of that asset, it also covers:

- Costs to acquire or develop the information
- Costs to maintain or develop the asset
- Productivity loss if the information isn’t available
- Liability issues if the information is compromised
- The value of the information to internal stakeholders or an adversary
- Potential reputation damage from a loss

Not all information in the business has the same value, so it’s important to prioritise the protection of data that is most valuable (for the reasons outlined above).

The UK Cyber Securities Breaches Survey in 2019 reported that 58% of businesses hold personal information about customers electronically.

* UK Cyber Securities Breaches Survey (2019)
**Data Retention**

Many SMEs also have no formal data retention policy or processes in place. This means that the longer the business has been operating, the more information it will hold.

Storing unnecessary information leads to the following:

- Increased infrastructure costs, through larger storage and backup space requirements.
- Higher operational costs, if using public cloud services on a pay as you use basis.
- Lost productivity, searching for current data.
- Increased time spent dealing with Freedom of Information Request or Subject Access Request.
- Increased risk of regulatory fines, if data is lost that should no longer have been kept.

There are, of course, valid reasons for keeping certain types of data, but it’s important to understand what data should be kept, what data should be archived, and what should be deleted.

Article 5(e) of the GDPR states personal data shall be kept for no longer than is necessary for the purposes for which it is being processed. Organisations must, therefore, ensure personal data is securely disposed of when no longer needed. This will reduce the risk that it will become inaccurate, out of date or irrelevant.

This is linked to having processes in place to respond to “data access requests”, particularly ones asking you to prove that all their data has been removed.

**Regulatory**

In addition to the above, many UK regulations have some form of information protection requirements. Regulations can be split into industry-specific and non-specific regulations.

Nearly all UK businesses will be impacted by the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA).

The DPA mandates “all data controllers and data processors to apply technical and organisational measures to protect their data”. Penalties for non-compliance are severe, and we’re now starting to see those fines filter through from the UK Information Commissioner’s Office (ICO).

While the DPA concerns itself with the protection of personal data, the Payment Card Industry Data Security Standard (PCI-DSS) exists to protect the processing of credit card data. Non-compliance can not only lead to fines, but also the withdrawal of credit and debit card facilities, which your business may depend on.

In addition to the above, businesses may also be required to comply with industry-specific regulatory bodies such as:

- Advertising Standards Authority (ASA)
- Financial Conduct Authority (FCA)
- Care Quality Commission / Care Inspectorate
- Architects Registration Board
- Pensions Regulator
- General Medical Council / General Dental Council
Why Information Security is Everyone’s Business

**GDPR impact**

Despite GDPR compliance requiring organisations to make changes to their information security policies, by formalising their data protection management processes, GDPR remains an area where continual improvement is needed.

**Just 30% of private companies and 36% of charities have made changes to their information security practises as a result of GDPR according to The UK Cyber Securities Breaches Survey in 2019.**

However, Article 32 of GDPR requires that organisations implement “appropriate technical and organisational measures” to manage risks and secure data, hence, companies must ask themselves if they have fully considered their GDPR obligations.

**Cyber attack**

There are several reasons a client might realise that their information security isn’t up to scratch. Unfortunately, the first of those is where the client suffers downtime or data loss as the result of a cyber-attack.

Perhaps the network was breached by a Ransomware virus that encrypted all the data it could access, or an executive’s email address was breached and used to make fraudulent payment requests costing the business thousands. If you were lucky, that realisation came through your own due diligence or because of a failed tender, where information security was high on the requirements and it made you review your security policies.

It is precisely because of this fear of a breach, that some large companies are mandating that their suppliers must have a minimum security solution in place, such as Cyber Essentials Plus and without it, you will not be able to get on their tender list.

**Beginning your journey**

Regardless of how a company gets to this point, it can often seem daunting to know where to start with so many standards on the market and so many areas to consider. This whitepaper helps you to get started on the journey.

**First and foremost**

If you are planning on a new or improved information security improvement programme, you are going to need board-level sponsorship as early as possible in the process. Your board must understand the value of data that the business holds, and more importantly, they must want to stop it falling into the wrong hands.

Board sponsorship brings accountability and an agreed budget – both of which are crucial in your programme. Unfortunately, getting board-level buy-in is going to be much easier to get, if you’ve just suffered a cyber-attack, especially one where you have a regulatory investigation to deal with, or where the company has suffered financial losses, either through the loss of hard currency, or major clients. Don’t put yourself in this position – it is crucial to plan ahead.

* UK Cyber Securities Breaches Survey (2019)
Information Security Checklist

Where do you start?

So, your organisation needs to improve their information security, but where do you start? Companies should consider the following factors when planning an information security improvement programme.

Any checklist should include the following actions:

**Step 1 - Assemble your team**

Any improvement programme is going to take resources and time – and you are unlikely to be able to complete it, without help from the rest of the business and/or an experienced cyber consultant.

You’ll want to assemble a team of experienced people, involving:
- Senior Management
- Department Heads – HR, Sales, Operations/Production, Finance etc.
- Information Security / Data Protection experts (possibly a third party for many SMEs).

Once your team is assembled, briefed and understand that this is a board-level initiative that you will report on, you can get cracking.

**Step 2 – Manage your assets**

The next step is to try to understand what you need to protect. You cannot protect what you don’t know exists. Companies will likely have data spread across many systems – both on-premise, in the cloud and even possibly on employees’ own devices. Your multi-departmental team comes into its own here – this team knows every aspect of your business and more importantly knows the critical processes that keep it working.

They will know:
- Where your data resides
- What systems they use to access that data
- Where the data comes from and who you share it with
- How and where their team’s work.

This data feeds into two critical documents:
- **Physical Asset Register** – a document containing every physical device where you store data – servers, PCs, laptops, tablets, mobile phones
- **Information Asset Register** – similar to the physical asset register, it lists every information asset you hold – from physical devices, cloud services, databases, file shares etc. If you hold company data on it, it should appear in this register.

Crucially, the data and device owner should be listed along with the types of data stored and whether it is currently encrypted or not.

Classifying data allows you to:
- Determine the security controls to be applied later in the process that should be used to protect the data
- Prioritise the data that needs to be protected sooner rather than later.
- Determine who should have access to the data and how that data should be accessed.

**TOP TIP**

You should always consider where you are going to get the information security expertise from - whether it is in-house and/or via a third-party consultant.

**TOP TIP**

With a comprehensive list of information assets, you can now classify the data according to its value – to both the business and any third party, should it fall in the wrong hands.
Why Information Security is Everyone’s Business

Information Security Checklist cont.

Step 3 - Decide on your compliance requirements

There are many regulatory compliance standards that you must meet, as well as industry and company-specific standards that you may be required to meet, as well as optional best practices frameworks that will help you achieve that compliance.

Your board will make the decision on what standards to meet; however, GDPR will undoubtedly be on that list, with PCI-DSS, a requirement if you take credit card payments in any form.

Standards such as Cyber Essentials, IASME, NCSC 10 Steps, ISO 27001 and NIST are generally optional, although they may be required in some industries or to win certain contracts.

Step 4 – Assess the threat, vulnerabilities and risks

These three areas are often confused, so we’ll start with a definition for each:

Threats – Threats are sources of danger to an asset. A threat may or may not be realised. Threats fall into different categories, but some common threats are hackers, malicious employees, viruses, hardware failure, power loss, fire and flood.

Vulnerabilities – Vulnerabilities are weaknesses in a process, application, operating system, security control or programme that allows a threat or threat agent to exploit that weakness to gain unauthorized access to data, change the data or make it unavailable.

Risks – Risks are events or conditions that could have an undesirable outcome for the company. A risk is a potential for loss, damage or destruction of an information system due to the result of a threat exploiting a vulnerability.

From the outset, the board should have a documented risk appetite and a rating system for risk. That’s unlikely to be the case except where a company has gone through something like ISO 27001. The team plays an important role in identifying threats and vulnerabilities and the impact that those will have should they be realised.

Risk can be measured in two ways:

Your team plays an important role in identifying threats and vulnerabilities and the impact that those will have should they be realised. Risk can be measured in two ways:

• Quantitative Risk Analysis - where the output is a financial cost – for example, a quantitative risk analysis may determine that the single loss expectancy of an information system is £100,000. How that figure is calculated isn’t important for this document, but it is important to ensure the cost of the control doesn’t exceed this figure.

• Qualitative Risk Analysis - is a much more common method for an SME to use to assess risk. This typically uses a risk matrix to determine risk value based on the probability of a risk occurring versus the impact on the company should it occur. A qualitative risk analysis is subjective and is opinion based – hence, it’s a good idea to involve several people in determining the risk. As an example, the risk of a virus encrypting all your data from an infected email attachment could be as high as 100% However, there is a 100% probability you will lose access to all your data unless some form of controls are put in place to mitigate the risk. After introducing a risk minimisation solution, using multiple security controls, this risk may drop to say 20% - a figure the board may or may not find acceptable.
Information Security Checklist cont.

The output from this stage will likely be a risk assessment that contains a value or a grade for every risk. The risk assessment should list at a high level the existing controls used to mitigate any risks but the ultimate aim of the risk assessment, is to determine whether to accept, transfer, mitigate or avoid the risk, and the accountability for this sits directly with your board. Their choices are:

- **Accept the Risk** – Typically used where the risk of an event happening is low – i.e. the impact will be minimal, even if it does happen and you can deal with it if it does. Risk Acceptance must always be documented – particularly the reasons why the risk was accepted.

- **Transfer the Risk** – The most common reason to transfer risk is the use of insurance – you transfer the risk of the event occurring to the insurance company who will pay out if it does. But make sure you have read the “small print” to ensure you are covered!

- **Risk Avoidance** – Changing your plans to avoid the risk. For example, if January is your busiest month where you can’t afford any unplanned systems downtime, you may implement a change freeze or patch freeze on systems to avoid the threat of an unstable patch preventing systems from functioning correctly.

- **Risk Mitigation** – This is the most common form of risk management action – you perform an action or implement controls to reduce the risk to an acceptable level.

**Step 5 - Decide on your compliance requirements**

At this stage, you are now aware of the risks to your data and which ones you need to prioritise. That’s going to take some time, and you need to give some thought to what happens if a serious security incident happens.

Consider your responses to the most likely threats and document who will do what and when. Nobody expects your plans to be 100% correct, first, second or even third time – so you need to practice your response to certain events and update your plans after each event.

Having a documented incident management plan ensures that if the worst happens, you have a starting point for dealing with it, informing the right people and ensuring you contain the incident as best you can. In any crisis, your actions during the first hour are crucial. You should not be spending that time searching for your MD’s out of hours telephone number!

**Step 6 - Business Continuity and Disaster Recovery Plans (BCDR)**

The most serious incidents may stop your critical business functions from taking place. This is a serious situation and every hour that goes by, reduces the chances of your business survival.

Creation of BCDR plans ensures that when this happens, you have plans in place to keep people safe, get your business functional again for the most critical processes and ensures you have a process for returning to normal, once the situation allows.

Types of events that may require you to invoke a DR plan include fire, flood, ransomware attack, critical hardware failure and loss of key sites through power or Internet connectivity loss.
Information Security Checklist cont.

Step 7 - Consider third party access

In many businesses, third party suppliers have access to your systems – whether that’s an IT support or application support vendor, external consultants or contractors. These third parties can introduce security weaknesses and may not be as secure as you need them to be.

 Attacks via the supply chain are becoming more common, as it’s often easier to breach the supplier to an organisation, than it is to breach the target itself. That’s why more and more organisations are insisting on minimum security standards are in place, such as Cyber Essentials Plus, before you are even allowed on a tender list.

Step 8 - Implement security controls

With the risks identified, it’s time to implement security controls. These are measures that will reduce or mitigate the risk, based on your board’s risk appetite.

There are three types of controls, all of which combine to reduce the risk to your data:

- Administrative Controls – these are usually your policies, procedures, standards and guidelines around security, including company HR policies and information security policies (including remote working, acceptable use, data protection policies, incident response, disaster recovery, backup policies, third party contracts and vulnerability management policies are some of the administrative controls that can be applied).

- Technical Controls – hardware or software that can be installed. Common ones include anti-virus software, email security software, intrusion prevention systems, backup software, network segmentation, strong authentication via access controls, file and folder permissions, vulnerability management and encryption.

- Physical Controls – controls which put physical barriers in the way to protect data, such as CCTV, fencing, lighting, locks, doors, security guards/dogs etc.

A control can also be a preventative, detective, corrective, deterrent, recovery or compensating control, with many controls falling into more than one category. For example, anti-virus software is a technical preventative, detective and recovery control – in that it aims to prevent virus infection by detecting any viruses which may end up on your system and taking automatic corrective action (quarantining, cleaning or deleting the virus).

Event log monitoring and audit log reviews perform a very important function in identifying suspicious behaviour and needs to be part of every organisation’s security program.

It’s essential not to rely on a single control to reduce your risks. You should practice a policy of defence in depth, to put as many reasonable controls in place as possible to protect your data.

TOP TIP
Remember an attacker will take the path of least resistance to get what they want. Make sure that it isn’t one of your suppliers by ensuring that they are required to meet your security standards, if they have access to sensitive data.

TOP TIP
It is important to consider the cost of the control (both capital and operational costs) and ensure that the cost doesn’t outweigh the value of the data it protects.
Consider penetration testing on a fairly regular basis (at least annually or after a major change) for your most sensitive data.

**TOP TIP**

Pay attention to social engineering techniques and teach users your processes for authenticating a user who appears at your reception desk or on the phone – they may just not be who they claim to be!

Step 9 - User Awareness Training

A very important security control is user awareness training. It’s generally accepted that humans are the weakest part of your security program – they are prone to sickness, mistakes, variations in performance due to workload or tiredness etc.

A good security awareness programme will increase user awareness and make them more vigilant to risks and suspicious behaviour.

Employees need regular awareness training that goes beyond an online video for an hour, once a year, that no-one wants to do! The training should be fun and thought-provoking to maintain levels of engagement and must involve everyone in the company, whether they use a computer or not.

Making non-computer users aware, increases the chances of stopping an attack before it occurs – such as the cleaner noticing someone watching her lock up every night for a week or the warehouse operator noticing sensitive information accidentally discarded in the rubbish.

Step 10 - Perform regular audits

It isn’t good enough to sit back on your laurels – you need to regularly audit your internal systems to ensure your policies and procedures are being followed and being effective.

Then, feed the audit results back into your risk assessment and make continuous improvements to policies and processes to refine security.
Why Information Security is Everyone’s Business

Conclusion and next steps

Companies of all sizes need to implement a security policy that includes control objectives, standards and a procedure. Regardless of the size of the company, an information security programme must be in place to ensure the data is secure and compliant.

The next step is to decide the level of commitment you can withstand. In the UK, Cyber Essentials can be started through a self-assessment questionnaire, whereas Cyber Essentials Plus requires an independent assessment of security controls.

An additional security assessment through a vulnerability scan, uses tools to scan your network for vulnerabilities. This can analyse your entire IT estate, from the inside and outside, the results can then be analysed and actionable steps recommended, which will help you address the security flaws identified.

Whatever the size of your organisation or the nature of your business, cyber security can’t be ignored. But prioritising and embedding cyber security in your operations doesn’t need to be complex or prohibitively expensive, as solutions can be adapted to meet your needs. If in doubt, contact an experienced cyber security consultant. It could be the best investment you make.

If you have any further questions, please contact the author – Neil Douglas, IT Consultancy Director by using the contact details below.

Contact us for an obligation free initial chat about your project or needs

Phone 0330 015 0322
Email info@myitdirector.co.uk
myitdirector.co.uk