Security for SMEs

Securing assets and planning for the future

A White Paper from:

Dale Penn

Security Consultant

Advent IM Ltd

ADVENT IM

Security for SMEs

Securing assets and planning for the future

Dale Penn, Security Consultant – Advent IM Ltd

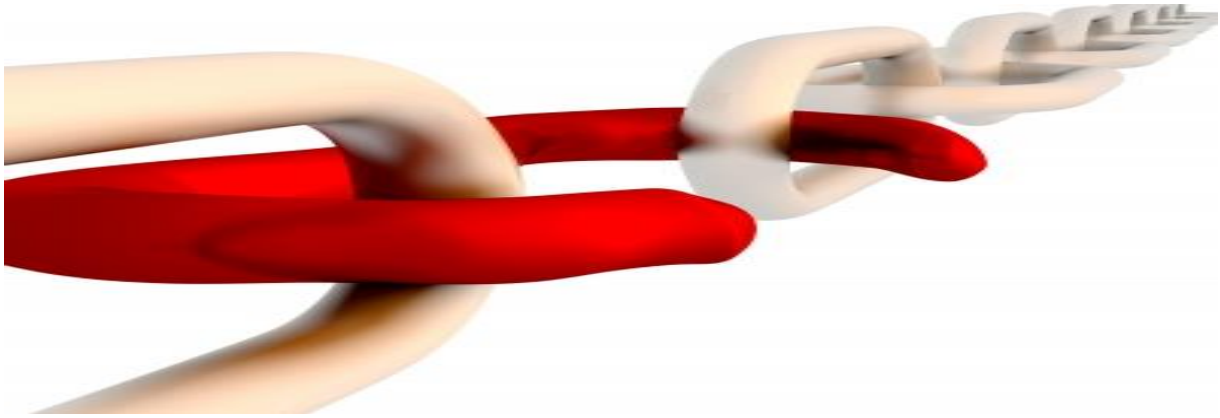
INTRODUCTION

Information is a valuable asset for any organisation. The compromise of the confidentiality, integrity or availability of any piece of information could potentially damage your organisation, be that financial or reputational damage. For example, should a member of your organisation lose/leak personal data to a third party this could lead to a heavy fine from the ICO and negative nationwide press coverage.

Information Security for SME's is always going to be problematic at best due to the simple fact of the restrictions on resources. Security had always been seen as a nice to have rather than a must have. However this is not the case as SME's are facing exactly the same threat landscape as larger enterprises who have more resources to implement costly solutions.

The main obstacle is always going to be, what is the most cost effective implementation that yields the best practical security in line with my organisation's needs?

The correct level of security which is designed around the functional business processes/outputs is essential as security should not be a barrier to operations. Security should be an enabling tool helping business move forward. Hopefully the days of the Security Manager saying "NO" are far behind us.



HOW AND WHAT TO IMPLEMENT

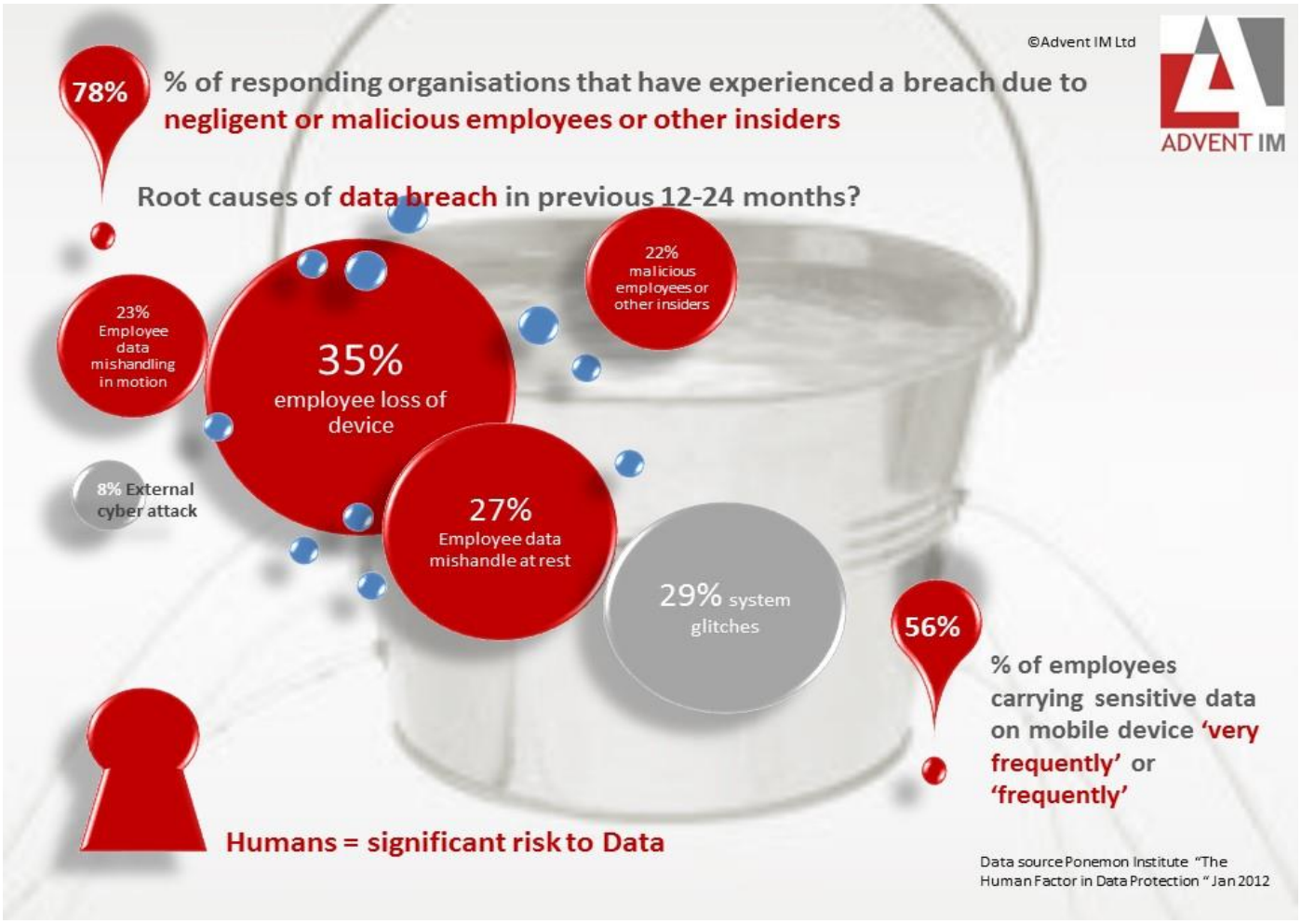
Governance

First and foremost, information security had to be driven by top management.

> SUN TZU "Leadership causes people to follow their superiors willingly: therefore, following them in life and death the people will not betray them"

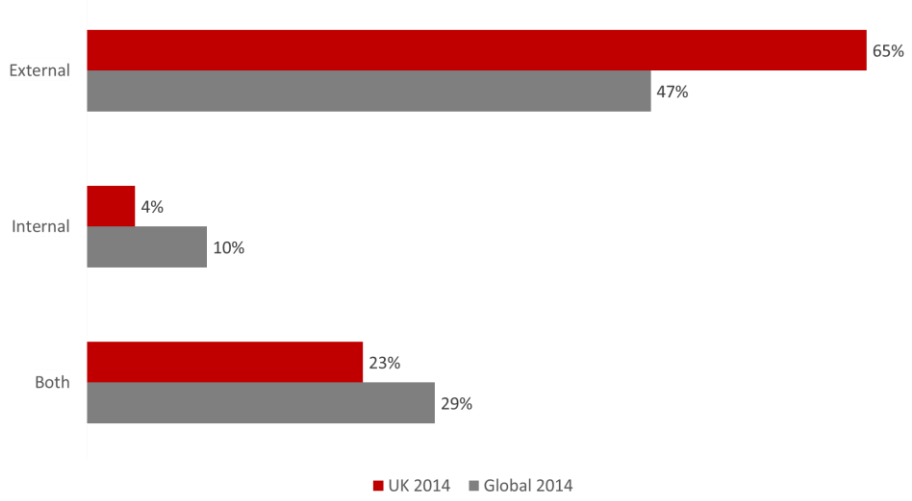
Senior Management top down support is imperative to a successful implementation of an information security strategy. Senior managers are in a position to provide both the downward direction required to implement and enforce policy which is instrumental in ensuring information security becomes part of the organisations culture.

The Managing director or similar is ultimately accountable for the security of information within your organisation. However, it should be further recognised that responsibility also rests with every staff member, and an effective IA Governance Framework detailing roles and responsibilities assists in reinforcing this message. This in turn will also ensure that appropriate governance arrangements are in place to provide ownership and accountability by all staff for the security of the organisation and its information.

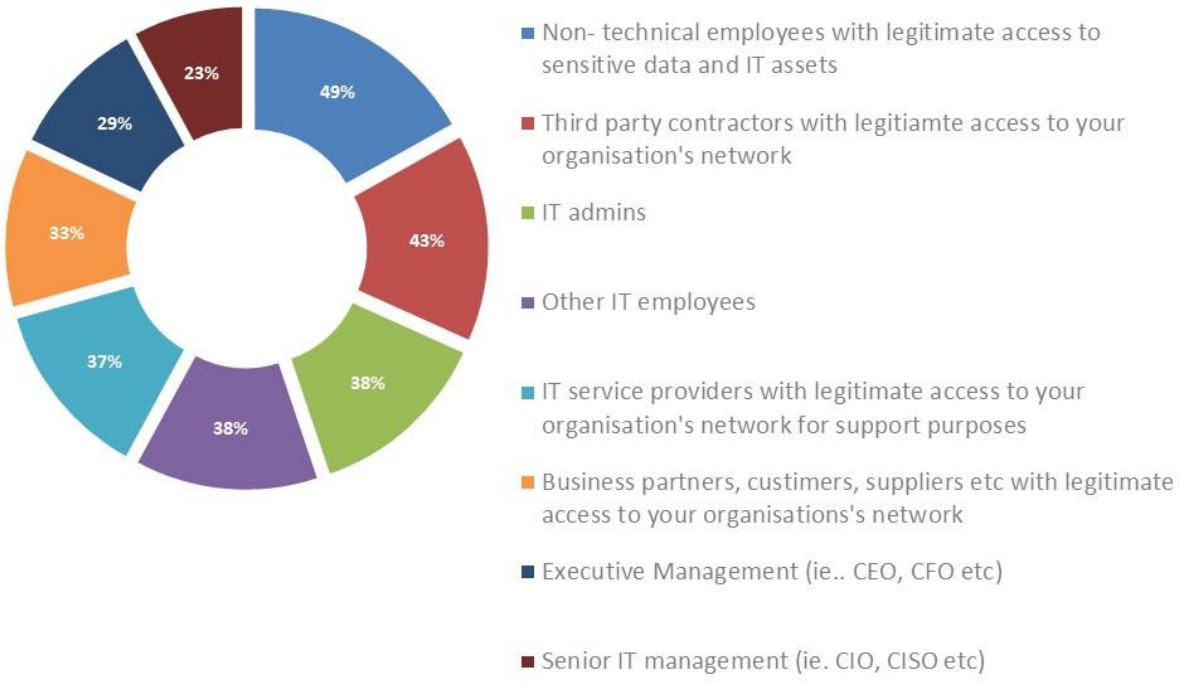


These findings seem to be in direct opposition to the *perception* of where threat comes from. The UK shows an over-index in this perception.

PwC 2014: perception of cybercrime is largely external



Vormetric Insider Threat Report 2014:
Insider groups posing highest level of threat



Layered Approach to Information Security

The benefits of operating a layered approach to information security cannot be understated. Business after business report breach after breach due to human error! And why? Because organisations are overinvesting in expensive technical solutions and not focusing on a holistic layered approach that cover

people, policies and procedures. This in my opinion is as, if no more important, then finding the correct technical solution.

Information Risk Management (IRM)

Good risk management enables an SME to be able to make risk based decisions with confidence. However, information risk is quite often forgotten about or not well managed. In my opinion IRM is the most important tool for SME's as this is the method by which an SME can identify what risks there are to their information and select appropriate controls to mitigate that risk to an acceptable level. Risk management not only means the mitigation of perceived risk it also means taking considered risks where the risk may outweigh potential loss.

Properly Identifying threats and vulnerabilities is vital in effectively capturing the risks to any organisations information assets. It is my belief that this process can sometimes underemphasise the threat from the human element of your own organisation, be it malevolent or unintentional. Below are some data shot which highlight this point.

It is vitally important that any IRM is supported by upper management and endorsed via policies, procedures and processes and the appropriate roles and responsibilities are well defined. This will assist in an organisation wide buy in and ensure that the process for implementing the IRM are understood, recorded and repeatable.
When implementing and IRM In my opinion it is important to know your information assets and it is often of benefit to compile and information asset inventory. The inventory would work hand in hand with an information classification policy and assist in appropriately grading each of your information assets.
From here, whichever IRM methodology you use, a calculation would take place involving the threats and vulnerabilities to your assets along with the likelihood of exploitation and the impact should this happen.
This is where IRM really shows its benefit as its output is a measurable statistic which informs you of the level of risk you have against any of you information assets. This then enables you too appropriately and cost effectively implement Information security controls aligned with you risk appetite and not implement expensive blanket control measures like larger organisations.

Policies, Procedures and Standards

Policy writing can be a daunting task, and one for which many are not overly enthused. However, Policies and Procedures are an integral part of any information security program. Not only do they provide direction and accountability, many specific policy elements are a requirement of specific laws, regulations, and/or standards.
Policies are vital for the correct implementation of Information security as this is managements chance to formalise their SME's approach and ensure it is aligned with current business strategy. At high level an SME should have implemented an information security policy which includes a definition of information security along with the objectives and principles to guide all information security activities. It should also assign the general and specific information security responsibilities to appropriate, defined roles. A high level information security policy must also include a process for handling deviations and exceptions.
At low level there should be a suite of information security policies which are broken down into specific topic i.e. Information Handling and Protective Monitoring. These are used to implement the information security controls you have deemed necessary to introduce to mitigate any risks that have been identified.

Education, Education, Education

Education in my opinion is one of the least resource heavy and most beneficial of all information security controls when part of a layered approach. When staff understand the value of information security and the steps to take to safe guard your SME's information you will find that that your workforce's entire approach and attitudes changes and becomes embedded within your organisations culture.
It is important that staff are taught:

- The importance of protecting data and systems
- How to identify confidential/personal data
- Acceptable use of the SME's assets
- The published information security policies and procedures
- Security incident response
- How to avoid common attacks i.e. Phishing

Incident Management

Another important process in a layered information security strategy is incident management. This is another control which does not need heavy technical investment but is instrumental in ensuring that when information incidents do occur they are properly managed.
By this I not only mean that the incident is identified and resolved. What I mean is that there are the proper processes in place for the organisation to not only identify incidents but near "misses" as well. And that these events are properly recorded and reviewed to ensure the appropriate corrective action is taken to avoid further occurrences in the future.
There should be a detailed procedure in place which identifies the roles and responsibilities for all employees. The main objectives of Incident management are:

- Minimise business losses and subsequent liabilities to the company.
- Minimise the possible impact of the incident in terms of information leakage, corruption and system disruption, etc.
- Ensure that the response is systematic and efficient and that there is prompt recovery for the compromised system.
- Ensure that the required resources are available to deal with incidents, including manpower, technology, etc.
- Ensure that all responsible parties have a clear understanding regarding the tasks they need to perform during an incident by following predefined procedures.
- Ensure that all response activities are recognised and coordinated.
- Prevent further attacks and damage; and deal with related legal issues.

Technical Controls

Technical controls cannot appropriately mitigate risk on their own and should be used as a layer of your information security strategy which support the policies and procedures you have developed in response

to the output of your information risk management methodology. However, that said there are some technical solutions available that do bring a lot of value in certain areas i.e. protective monitoring and email filtering. It is the same with ICT as it is with information throughout the whole business. The first step is to conduct a full audit of your system(s) and identify where sensitive data is stored, processed and transmitted. Creating a data flow diagram can be most beneficial as most organisations will secure the network but overlook where the information is in transit and not introduce appropriate controls where information is in motion i.e. USB and email.

Where SME's have developed services on the web it's is very important that public facing applications become a focus of security as these applications could provide a route to the internal network. These applications should receive frequent penetration tests to ensure there are no exploitable vulnerabilities.

Thought should be given to deploying a web application firewall. This would be dictated by how critical availability to the web application was to business operations as an application firewall would defend against attacks that could overwhelm an application or server and leave you vulnerable to attack.

Business Continuity

Business Continuity is another valuable layer of information security strategy and involves you assessing your organisation by carrying out a series of impact assessments on business functions and implementing controls to ensure that those functions are still able to operate should a disaster occur. See ISO 22301 Below.

CURRENT STANDARDS

There are a whole host of standards that you can align your SME to which can be useful in developing information security. However there must be a business need for the organisation to achieve certification. In the main these standards are used to provide assurance to industry. Following is a small description of a few useful standards.

ISO/IEC 27001:2013

ISO/IEC 27001:2013 is the international standard that provides guidelines for the setting up, implementing and managing of an effective Information Security Management System (ISMS). The standard comes in two parts ISO/IEC 27002:2013 (Code of Practice for Information Security Controls) and ISO/IEC 27001:2013 (Information Security Management Systems - Requirements). Part-1 is a standard 'Code of Practice' that provides an organisation with default guidelines on the types of security controls an organisation should implement to safeguard their information assets. Part-2 is the standard 'Specification for Information Security Management Systems' and provides an organisation with the general steps required in establishing a management framework. It is designed to generically encompass the people, the places, the processes and the systems (P3T Controls) within the organisation.

HMG Cyber Essentials Scheme

The purpose of the HMG Cyber Essentials Scheme is to assist UK organisations in defending against the most common forms of cyber threat by deploying a basic level of security controls. These include threats such as denial of service, malicious code and malware, phishing attacks and hacking etc…

The HMG Cyber Essentials Scheme has been developed as part of the UK's National Cyber Security Programme by the Department for Business, Innovation and Skills (BIS), CESG (the UK government's National Technical Authority for Information Assurance) and in close consultation with the Information

Assurance for Small and Medium Enterprises Consortium (IASME) and the British Standards Institute (BSI) and industry. Cyber Essentials is not a standard but rather a set of controls that provide the minimum level of protection against cyber threats. This is a cheap and useful standard for SME's to baseline there cyber security.

PCI DSS

The PCI-DSS has been created by the major credit card companies to protect cardholder data being processed, transmitted or stored by a Merchant and/or the associated Service Provider. The standard is not a legal requirement but a regulatory one, enforceable by the participating credit card companies should a Merchant (or Service Provider to the Merchant) suffer an incident which breaches the security of the cardholder data. A Merchant or Service Provider can be any organisation processing, transmitting or storing data, particularly the 16 digit code that forms the Primary Account Number.

ISO 22301 - Business Continuity Management

ISO 22301 is the international standard for business continuity management, and builds on the success of British Standard BS 25999 and other regional standards. It's designed to protect your business from potential disruption. This includes extreme weather, fire, flood, natural disaster, theft, IT outage, staff illness or terrorist attack. The ISO 22301 management system lets you identify threats relevant to your business and the critical business functions they could impact. And it allows you to put plans in place ahead of time to ensure your business doesn't come to a standstill.

CONCLUSION

In conclusion every SME is going to be different therefore different methods and controls sets are going to be implemented for each SME and there is no one size fits all implementation. However I believe that so long the implementation adheres to the following points you can't go far wrong:

- driven by senior management
- layered holistic approach
- intelligent risk based decisions are made information security is properly adopted into the culture of the organisation

ADVENT IM

www.advent-im.co.uk
0121 559 6699
@Advent_IM
bestpractice@advent-im.co.uk