clearswift

Critical Information Protection & Security

Questions for the Board to ask

January 2016

Table of Contents

Introduction

Board Directors have a number of roles and responsibilities. Asking the right questions of those managing aspects of the business will help ensure risks are discharged properly. There is heightened awareness amongst investors, customers, clients, employees and the public of the risks associated with cyber-security and the protection of digital information.

Through conversations with Board members at other companies, Clearswift has compiled a set of questions that the Board needs to discuss when it comes to information security. This was spurred on by the new EU Data Protection legislation which will come into force in 2016. This guide seeks to enable you, as a Board Director, to have more sophisticated conversations about the benefits of good security. Large scale incidents are thankfully rare, but when they occur they are generally catastrophic. However all cyber security incidents of which there are many always lead to business disruption, many of which could have been avoided.

Kirstin Gillon from the ICAEW IT Faculty comments: "The Board should strongly consider the benefits of strong security and how it can be built into a more positive story. Good security can be built into a brand and potentially add competitive advantage. Effective management of operational risks might reduce capital requirements. Biggest concerns relate to staff behaviour, whether inadvertently falling for scams by clicking on suspect emails, or giving out sensitive information, or maliciously stealing sensitive data such as customer lists."

What is Information?

Information is not just found in documents, it can be in email and content posted to social media or cloud collaboration services. It is found in databases, but probably more importantly, the reports run from databases, which then become more portable, so can be readily emailed or uploaded. In conjunction with the information, there are also the systems where the information can be found. This can be servers in the datacentre or laptops, it can be mobile phones or tablet computers, it can be devices owned by the organization or it could be the employees' own devices, it could be cloud based storage or even on a USB stick.

What is Information Security?

Information Security is the steps that a Company needs to take to ensure that its information assets and systems are protected from internal and/or external threats such as loss, corruption, damage and/or theft.

What responsibility does a Board have to manage Information Security?

There is increased responsibility placed on boards, by virtue of changes such as the revisions by the Financial Reporting Council in September 2014 to the UK Corporate Governance Code. There is a need for a board's corporate strategy to focus on good risk management and an expectation that boards have control of the critical risks to their business. Managing the security of digital content is of paramount importance to companies for several reasons including:

- Retention of competitiveness by protecting its intellectual property;
- Facilitates the exchange of external and internal important information;
- Provides a mechanism for secure financial transactions;
- Maintaining a credible reputation;
- Demonstrates compliance with legal, contractual and regulatory requirements, particularly where required to collect and retain personal information about employees, customers and partners; and
- Provides a mechanism to verify information is authentic, un-damaged and confidentiality maintained.

In the past privacy, data and security questions were most often handled by legal teams or IT departments; now this responsibility is being elevated to boards and there is increasing demand for transparency on related matters. Companies are increasingly being impacted from the fallout of poor security; Sony and Ashley Madison are recent examples where significant damage was caused to both their reputation and finances. Notably Ashley Madison has lost investor confidence after the hack to its information system. Ashley Madison had hoped to raise $200 million by listing its' shares in London this year, 2015. It's reputation as a discreet "dating agency" shattered by a lack of adequate information security!

Are there new information risks?

Yes there are plenty of new risks, some are from cyber-attacks, but many others are the result in changing working practices, legislation and inadvertent conduct by employees. Today, many of the new attacks are based around content, documents in particular to create the attack. This can be as simple as embedded malware in a word document which runs when the document is opened – and infects the user's system before proliferating out to the network. Through to exfiltration of critical information in meta-data in a document (who can forget the last UK election where the federation of small business petition turned out to come from one party's HQ?) as well as inappropriate information being sent to unauthorised individuals.

What is metadata and what risks does it create?

Metadata is the detail available to users that provides more insight into information; for example it will describe where information was created (such as GPS information in photographs or the name of the computer a document was created on) and hence the location of individuals can be tracked. It might provide details about authors, time and date of creation of information too amongst other property based description.

Another class of information is the revision history within a document. This might be obvious if you have 'track changes' switched on, or it might be embedded in the document by default, for example in fast save information. Either way, this can contain sensitive information which can result in a data leak.

Of course one of the new risks is around collaboration, or rather interrupting the flow of information during collaboration. Traditional data loss prevention solutions (DLP) can reduce one set of risks but introduce another.

Legislation and fines

As a member of the Board the last thing you want to deal with is a data breach. These are expensive. Today the maximum fine that the Information Commissioner's Office (ICO) can impose is £250,000, however this will change in 2016 when the next round of EU legislation around Data Protection comes in. At this point the maximum fine will be between 2-5% of global turnover, or €100,000,000. This level of fine could destroy a company, or at least put it into receivership.

Fines are actually only a small component of any monetary impact from a data breach with additional costs including:

- Reputational damage
- Loss of confidence by stakeholders, regulators, investors, customers, employees, lenders and partners
- Loss of new sales as well as existing clients
- End user financial status monitoring (should credit card details, or bank account details be lost or stolen)
- End user, institutional and personal investor law suits
- Increased audit costs

While the law relating to personal liability, in conjunction with information security, in the EU is different from the that in the US, there is no doubt that no Board member wants to end up in the media explaining an information breach which could have and should have been prevented. Changes to the EU DP legislation means that the spotlight will be on Board members to adequately protect the business from cyber-security threats in a cost-effective manner.

Good information security can create competitive advantage and that begins with understanding. It should not be left to the IT department to protect information, it needs to be driven by the Board.

Questions to Ask

The following questions aim to help company Board members target the key issues the CIO's of every business should be aware of. While some might appear obvious, there will be discrepancies across the Board as to the prioritisation of the information from a corporate perspective. meta-data in a document (who can forget the last UK election where the federation of small business petition turned out to come from one party's HQ?) as well as inappropriate information being sent to unauthorised individuals.

Do you know what the critical information is for this business?

This might be the most obvious question, but it is also the most difficult. Without a proper understanding of the information inside a business it becomes impossible to put together a cost-effective strategy to protect it. There is a difference between 'sensitive' data which is traditionally regulated and 'critical' information which your business runs on. So, while your HR database might be seen as being 'sensitive', it will be next generation product designs and/or bids for contracts which may constitute your critical information.

- Have we defined what our most critical/sensitive client data is?
- How do we define critical information in our business?
- How do we protect that critical information from loss or theft?
- Do we know where it's located (endpoints / databases / archives / etc.)?
- What is the financial/reputational risk if this data was lost/stolen (quantified and by example)?
- How are other people in our industry solving this problem (by example) and what is their experience?
- What are the regulatory / legal obligations regarding our client information?

Where is our critical information and who has access?

Once again, this should be an easy question to answer but it is not. This is not just about information that is held in a database, but can also be the copies of reports which are on laptops, or accessible from table computers and smartphones. It is further complicated with social media and cloud collaboration tools.

- Which types of devices hold our critical information?
- Do we use social media are there controls around its use?
- Do our employees use social media from work devices or network?
- Do we use cloud collaboration tools? Which ones?
- How do we audit and control information being posted to social media / cloud collaboration tools?
- Do 3rd part contractors / partners / consultants have access to our cloud collaboration tools? If so, can we audit their use of our information?

What controls exist to protect our critical information – technologically and operationally?

Good information security practices are not solely based on technology, but need people and policy (or process) in the mix as well.

- How will we classify this information as critical (electronic/human) in each location and how long will this exercise take?
- Are there appropriate information security policies in place? When were they last reviewed and do they cover current business practices, such as social media and cloud based collaboration?
- Is there a technology solution available to capture ALL the potential egress accidentally or maliciously of our client information (including cloud/mobile/bring or choose your own device, aka BYOD or CYOD)?
- Does this solution fit within our existing infrastructure today or is further investment required (on premise or in the cloud)?
- What organisational changes (staff/ training etc.) will we need to undertake in order to make the solution effective and when?
- If there is no knowledge of what our critical information and an appropriate system to protect it, then how long will it take to implement and by whom?
- Which departments will need to be involved and which told about the project?

Who is responsible internally for the protection and security of that critical information?

It is easy to argue that information security is the responsibility of everyone in the organization, however there needs to be Board level sponsorship and a go-to person to make the project a success.

- Who is owns critical information protection (IT/HR/CTO)?
- How will we manage when it stops working for whatever reason?
- Who will/do we get to help us from a consulting/product and ongoing support perspective?
- What do the analyst/forums say about our chosen partners?
- Which departments are protected or which function will we start with?
- What happens if we re-classify some information from/to critical during the project?
- How will we respond if we have a data breach before the project is implemented?

How much do we invest in automated systems to protect critical information?

This is the million dollar question – and it can't be answered unless you understand the information you are trying to protect. It is obviously not worth investing £1m to protect £100 of information. Similarly it's not worth putting all the money into protecting a database when it is laptops which have more critical information and are open to greater risk.

- What will/does a solution cost CapEx / OpEx / TCO and what is the ROI?
- Will the ongoing OpEx decrease over time, or increase?
- Do we have the required skill set to run the solution effectively?
- Will the solution integrate into existing event management and/or operational management systems, e.g. ticketing?

What software do we employ at the gateway to stop the bad stuff coming in and the good stuff going out?

Traditionally gateway solutions for email and the web offer inbound 'hygiene' security functionality to prevent viruses and spam. Next generation adaptive security solutions can also offer advanced threat protection and data loss prevention functionality as well.

- Do our gateway solutions offer Data Loss Prevention (DLP) functionality as well as hygiene functionality?
- Does our DLP solution simply stop and block critical information? Or do they allow continued flow of information having first redacted sensitive and critical information?
- If the DLP solution stops and blocks communication then where does that go for action? Quarantine, IT help desk, back to the employee or to their manager? What is the cost associated with remediation?
- What document metadata information is being leaked in documents? Can you ensure that inappropriate metadata is automatically removed from documents before they leave the organization?
- Do we have technology that allows structural and document sanitisation of the information at the gateway?
- Do we have a gateway which allows the establishment of policies to determine what can pass and what can't? Both based on content and on context (who is sending to whom and how?)
- Do we employ Adaptive DLP software?
- Encryption software is useful to prevent good information leaving the organisation and falling into the wrong hands, however it can also be used to leak information – can we detect improper use of encryption which might be used to exfiltrate information?
- Can we apply encryption policies automatically so email and its attachments uses the appropriate encryption method based on the recipient?

How to stop security tools impacting information flows?

Having the right security tools and process in place is vital to protect critical information but the use of these tools shouldn't impact the business day to day operations. Software available from Clearswift can allow critical information to be redacted seamlessly without impacting business by redacting key details and allowing a flow of information but in a "cleaner/sanitised" form.

Is there new technology that can mitigate the risks?

New technology is being created and brought to market all the time. The latest DLP solutions offer 'Adaptive DLP' (ADLP) and offer rapid risk reduction around critical information protection. ADLP solutions adapt information based on the content and, more importantly, the context of the communication and can automatically remove information that breaks policy to enable secure continuous collaboration. This is not just about information on the way out of an organization, it is also on the way in. Deep Content Inspection is at the heart of the ADLP solution, it can determine whether active-content should be removed on the way in, or if meta-data (and revision history) should be removed on the way out. It can discover a credit card number in an email attachment and remove it, but leave the rest of the communication untouched.

ADLP is designed to help protect an organization's critical information and keep business flowing. This can be through email or across the web with a cloud collaboration platform. ADLP can also be used inside the organization, preventing critical information leaks between departments, for example from finance to other areas of the business with results at quarter end. Today, there is a realisation that 'open' sharing of all information creates risk that can be easily mitigated and while access control can be readily applies to files on a server, email enables anything to be sent to anybody inside the organization. ADLP can help enforce a 'really, really, need to know' policy.

What can be done to demonstrate risks discharged?

Board members need to understand the company's threat profile, controls and processes from relevant company representatives such as security officers and lawyers. Those with operational responsibility, such as Security Officers or Heads of IT should be given a voice at the board and cyber-risks should be regularly reviewed. There are always requests for additional budget, when it comes to security, the cost of not doing something needs to be taken into account. The Information Commissioner's Office (ICO) is constantly upping the expected levels of security that should be deployed from both a process and technology perspectives. Keeping an eye on recent enforcement notices is a good indicator as to what is now 'the norm'.
A section on the management of cyber-risks in the annual report along with the use of information security specific technology should help to boost investor confidence, this is becoming standard in the USA, where they also declare breaches on critical information as well as sensitive information which is protected by direct legislation.

How can this be implemented?

Clearswift Limited can assist companies understand their Information Security risk profile by providing services to help identify the organization's critical information, the risks associated with it and how to protect it by using the next generation of Adaptive Data Loss Prevention solutions. These will allow a Board to properly understand the areas of exposure and provides a detailed mitigation strategy to help as part of a corporate risk strategy. Clearswift's solutions can be deployed stand-alone, or in conjunction with other security vendor solutions.

Summary

There is no doubt that information is what differentiates businesses today, it is both their life's blood and the crown jewels. Protecting information has become a Board level discussion because of the impact should it fall into the wrong hands either through a cyber-attack, a malicious insider or an inadvertent employee action.

Before a solution can be proposed questions need to be asked which will help clarify the problem and assist in defining the solution. An effective information solution needs to include people and policies with technology to back them up. Adaptive Data Loss Prevention solutions can address next generation information borne threats and support the agile business processes and practices of today.

Clearswift offers Professional Services to help Boards to understand their information and their security requirements. Clearswift also offers award winning Adaptive Data Loss Prevention solutions which rapidly reduce risk and are a cornerstone to any adaptive security environment

clearswift

Clearswift is trusted by organisations globally to protect their critical information, giving them the freedom to securely collaborate and drive business growth. Our unique technology supports a straightforward and 'adaptive' data loss prevention solution, avoiding the risk of business interruption and enabling organisations to have 100% visibility of their critical information 100% of the time.

For more information, please visit **www.clearswift.com**

United Kingdom
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale
Reading, RG7 4SA
UK

Germany
Clearswift GmbH
Im Mediapark 8
Cologne D-50670
Germany

United States
Clearswift Corporation
309 Fellowship Road
Suite 200
Mount Laurel, NJ 08054
UNITED STATES

Japan
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
JAPAN

Australia
Clearswift (Asia/Pacific) Pty Ltd
Level 17
40 Mount Street
North Sydney
New South Wales, 2060
AUSTRALIA