Cybersecurity

A brief personal introduction

Slide 1

My name is Athlyn Evans. I am the Head of IT & Data at Creditinfo Malta, I have a first class degree in Computer Sciences and Electrical Engineering and a Master Degree in Information Systems. I have worked in IT for 25 years. For many years I was a freelance IT Consultant who specialised in IT and Data Security. I worked for the UK Ministry of Defence and BAE systems and was responsible for perimeter line security for encrypted communications between defence and government departments, this included areas of conflict. I also worked in the Airline industry to improve security post 911. My last security position was working in the digital film industry in the UK and Hollywood, LA ensuring digital security and digital fingerprinting for large data warehouses used in CGI production.

At the end of this presentation there will be a question and answer session. As this is such a large subject and it is sometimes difficult to translate theory into practice for any organisation, I am hoping that we can perhaps debate some of these issues and how you see the relevance to yourselves.

Slide 2

Why cybersecurity is such a big issue, why the stakes are so high and the answers so difficult.

Today I will address some of these issues and why cybersecurity has become such a hot topic for organisations around the world.

There are two billion people around the world who are online. That's two billion people who are relying on the Internet to be a trusted place to obtain and share information. Some of these two billion are using the Internet to buy real or digital goods, collaborate with business partners, and handle the tasks of everyday life, like paying their bills, online shopping and information research.

There are thousands of people and even organised criminals who buy and sell data stolen from both individuals and organisations.

Many people still worry about the security of their online transactions and whether their privacy is being protected. The endless stream of news stories

about cyber-attacks contributes to these concerns. 2013 saw an enormous rise in Ransom ware where by executing malicious code downloaded via email or as part of a web page, your computer is locked unless you pay the hacker a fee to release your machine.

Slide 3, 4 and 5

Cybersecurity is like a jigsaw and is made up of many pieces and often they seem to conflict with the Internet's fundamental principles. A framework for policymaking is useful when preserving those principles whilst maintaining good security practice.

Slide 6

What is cybersecurity?

If you ask an ordinary user like a friend or neighbour, you'll get one answer— maybe having to do with concerns over their credit card data being stolen or having gone too far in a Facebook posting that could be read by a prospective employer. If you ask parents, they will tell you they worry about what a child might be looking at, or the possibility that the child is the victim of cyberbullying or on the receiving end of "sext" messages.

This is a view of the typical end user, but it’s just one perspective.

For businesses, cybersecurity has other far reaching implications— companies all need to safeguard customer information, protect commercial data, and prevent intrusions and damage to their corporate networks. Yet the business perspective of cybersecurity is far from uniform;

Companies vary widely in their specific needs, expectations, and sophistication there is no ‘one size fits all’ approach.

A small business may not be concerned about the same things that utility companies are concerned about, and a manufacturing industry may not have the same cybersecurity requirements as a financial services companies need. Then there is the government perspective, which has to take into account the concerns of individuals and businesses whilst also dealing with any national security threats that an Internet attack might pose. With many government services and national physical infrastructures increasingly tied to the Internet, the disruptive potential of a cyber attack is now significant.

Governments' approaches to cybersecurity, like industries, aren't always the same. Among other things, they vary with the country's geographic location and economic development.

For example there are differences between developed and developing countries in how they address cybersecurity. Those of us who live in developed countries have become used to inexpensive bandwidth and relatively easy access to security software. Does that mean that developed countries are more secure? In theory at least, it should but in practice the policies and procedures in place are so fragmented there are still many holes in security they may be exploited.

In developing countries the same fragmentation exists but with additional issues related to internet access. Unlimited access for a set fee isn't the norm. Users often pay more as their use goes up, so things like spam imposes costs on people who can least afford it. Neither, in some cases, can they afford to download regular antivirus updates. In places where electricity is unreliable, an attempt to download new software can turn into a costly failure if the power shuts off.

There are other important differences in emerging economies. People access the Internet through wireless services, and Internet users in these countries are much more likely to get on the Internet at a cybercafé or community access points like libraries. These methods of access are extremely important for people who might otherwise never be able to get online.

But these methods of connecting have certain risks. Cybercafes can be especially problematic, because of the possibility that private information will be available to other users who sit down a few minutes later at the same computer. In Uganda, criminals took advantage of this, methodically recording online banking transactions made at cybercafés.

For all of these reasons, a developing country is likely to have a different set of priorities when it comes to the Internet, than a developed nation.

While developed countries may be most focused on securing advanced computing infrastructure or funding cybersecurity R&D, a developing nation may well be more concerned with developing the technical and policy capacity to deal with online fraud.

Slide 7

Many countries lack the basic legislative frameworks to address cybercrime, particularly when the crime may not even originate in their countries. This makes cybercrime a particularly attractive criminal activity as legal legislators continuously play catch up with technology.

Which of these concerns should be the priority when it comes to our cybersecurity efforts and cybersecurity policy in general? For that matter, how do the diverse concerns of governments match up against the security needs of individuals and businesses? I'm not sure there is a definitive answer to that question. They all have legitimate interests, and in many cases, the interests, though specific to them, are also intertwined with other organisations and other legislation (data protection act, computer misuse act, telegraphy act etc.)

That doesn't mean we should throw up our arms in frustration and say it is an impossible issue to address effectively. It just means we have to think in a global sense and not restrict our view to just our internal corporate systems and data. We live in a connected world so we must consider the wider implications of this.

Any framework for tackling cybersecurity needs to work back from an understanding of the different ways in which the Internet is valuable to its users of both the internet in general and our own corporate systems and data

To everyone, the Internet has value as a communications tool and as an engine of economic growth. It also has value as an enabler of social and even political change.

Slide 8

What are the main fears?

It is key to security to understand how your users, both internal and external use and access your data.

The main fear of any organisation is loss of data. Where this was once simply an issue of failure of hardware or software leading to data loss this has grown into a complex network of issues. For example

1. Data loss due to hardware/software failure – should be mitigated by robust backups and clear disaster recovery plans.
2. Data loss due to data leakage – this may be something as simple as smart devices or laptops being lost or stolen – devices should be at least password protected, ideally data should be encrypted
3. Insecure data transmission – email is the most common method of leak. Email is inherently insecure and corporate and private data should never be sent by email, unless encrypted
4. Access control – Users should only ever have access to data they need to perform their role. Access to data should be controlled by a robust access policy including restricting users access to write or amend data
5. Mobile access to data – has become a way of life for many road warriors. Access should be via VPN to corporate networks from anywhere that is outside the office network. This is particularly important when using public wifi access points.
6. Educate users – Users need to understand why access personal emails via work machines circumvents corporate security. Why accessing social media and other websites may pose a security risk.
7. Central control of machines via Active Directory and robust policies preventing the downloading and installation of software is a basic security requirement from IT security and data protection policy perspective.

Slide 9

User education and organisation culture is the most important issue in data security. This is not a technical issue and should not be the sole remit of the IT Department. This is a management issue where IT are only part of the solution.

1. HR needs to ensure that Computer usage policies are in place and signed by every member of staff, from top to bottom
2. Staff need to understand and be educated that the hardware and data they use does not belong to them, it is all owned by the company

3. All staff need to understand that regardless of their position in the company, security and access policies apply to all
4. Staff should be educated to understand that by their individual actions they may pose a risk to the organisation
5. Policies should be in place regarding new starters, leavers, access to data, computer mis-use, remote access policy, authorised software, non-authorised software etc., etc.
6. Data retention and security policies should be reviewed and signed off by management at least annually.

Slide 10

Why is this important? Isn't this all a bit of a drama? Some real world examples (I have removed the names of organisations involved to protect the guilty)

Example A

Company A spent $15,000 on an email protection software to scan all corporate email for Trojan and Viruses. All corporate email was scanned before entry to the company mail server. Logs showed that with a user base of 1200 users over 100,000 viruses were stopped at the gateway every day. The company was happy or complacent, depending how you look at it for six months.

10 days before the Christmas break and a SQL Trojan entered the system and took out their main customer system. Everything was restored from backups and was up and running again in 6 hours. 3 days later it was taken out again. Log files showed nothing, there was no intrusion.

What could have been done?

The culprit was traced to a user accessing their Hotmail account and downloading an animated flash Christmas greeting that contained malicious code. The $15,000 investment in email security was breached by a user accessing a webmail account during their lunch break.

By using website filtering or some simple user education this could have been avoided. Downtime cost the company overtime and consultant fees in the region of $12,000.

Example B

MD has laptop stolen from a train. Access to corporate data is compromised as the laptop contains copies of board minutes and discussions of a takeover bid. Email is compromised as email software is able to load all cached emails allowing them to be read off-line. All internal systems are compromised as VPN passwords and web passwords were 'remembered' by the computer.

What could have been done?

Laptop was reported as stolen to the company within 60 minutes. All passwords were changed to prevent access. Nothing could be done about the emails and missing documents. The laptop used a Windows password rather than a Domain Password as the MD didn't like the rules imposed by the domain policy. It is a simple two minute procedure to crack a Windows password, this would leave all data vulnerable. By remembering VPN passwords and web form passwords the laptop is literally an open door to the corporate network. Data should have been encrypted so that even with the loss of the laptop none of the data would be compromised.

All users are vulnerable and regardless of position should abide by security procedures.

Example C – Final Example

A large retail concession chain had access to its stock management system on computers at its concession store within large department stores and airports. The stock price list was amended and a random stock item name was changed to an obscenity. When this was noticed it could not easily be ascertained what data had been amended and therefore the entire database of stock items and prices needed to be restored from backup. As it was not obvious when the data was changed it took time to get back to a clean backup. Also the financials had to be checked to look for anomalies on orders and prices going back to the date when the clean backup was found (22 days)

What could have been done?

Workstations in store should never be left unlocked, some user education would have helped here but on top of this a policy that automatically locks the workstation after a period of non-activity would have also aided security. Most importantly, why did users who only require read access to data have the ability to amend data.

Slide 11

What is basic best practice?

Ensure you have a centrally managed anti-virus software that can track and update machines so that protection is up to date and is auditable.

Ensure email servers have anti-spam provisions. Ideally this should be outside your network to prevent denial of service attacks.

Do not allow users to download and install software. Only authorised software should be used.

Do not allow the use of pirated software as this is a major cause malicious software.

Use complex passwords.

Use Active Directory for control of Windows Machines

Monitor and apply Operating system security updates

Block all unneeded firewall ports and protocols

Be cautious when using social media sites and do not allow the use of apps

Monitor web usage and consider blocking certain sites

Encrypt mobile devices and consider mobile device management options

Document policies and procedures and educate end users.

Slide 12

It is important to instil in the culture of an organisation that we are ALL responsible for security, if in doubt, should I send this information by email, is it safe to install this plugin, can I email this home to work on etc., then ask your manager or data security representative.

Slide 13

Security 10 commandments

1. Security is only as good as its weakest point. Audit security regularly

2. Management are responsible for security not IT, ensure awareness and update management frequently. It should be a regular on management meeting minutes
3. Only allow access to data and equipment that is actually required by a user
4. Document and publish policies covering all aspects of data, retention and usage
5. Use robust complex passwords – All Windows machines should be domain enabled
6. Use Active Directory or Radius service to control access policies
7. Use best practice to centrally control and manage Anti Virus and Anti Spam software
8. Use data encryption for all mobile devices
9. Use firewalls and anti-intrusion devices – test them regularly
10. Ensure ALL users understand how their individual action may affect the entire corporate infrastructure.

Slide 14

Discuss