BUSINESS LECTURE TWO

Dr Henry Pearson

Cyber Security and Privacy - Threats and Opportunities.

Introduction

Henry started his talk by confessing that he was definitely not a marketer, as he had been occupied with IT and related technologies for all of his career. Henry is ideally suited to make sense of current developments in cyber security and data privacy. He spent 25 years in senior appointments at Detica plc before its sale to BAe Systems to become their Applied Intelligence Division, a leading supplier of cyber security products and services to governments and commerce. He has provided extensive advice on cyber security to the UK MOD with hands-on experience of handling major cyber and privacy incidents and now fulfils a number of roles for the UK National Cyber Security Centre.

PART ONE - CYBER SECURITY

The Costs and Other Impacts of Cyber Attacks

Henry began by pointing out that data security should be the concern of everyone in the business including the marketing department. Successful cyber attacks not only cause companies financial damage. The Impact on the reputation of the victim's brand and on its enterprise value or share price (if quoted) can also be severe.

The costs associated with cyber attacks are escalating rapidly. The anti-virus firm McAfee estimates them at $600 billion annually,

(0.8% of the global GDP), while Forbes is forecasting 6$ trillion per year on average through 2021. Many major incidents have collectively cost their victims up to $1billion, and even single company costs can be in the range of $10 million to $100 million. and sometimes more.

The total compensation for victims of the Wannacry worm was capped by insurers at $4 billion. Similarly the total amount of the damage caused by the NotPetya virus was estimated at around $1.2 billion. As an example of single company costs, in 2013 Target (the US retailer) lost the data for over 40 million credit cards as well as personal data for over 70 million customers. In addition to a $18.7 million payout to customers, the total cost to the company was estimated at $291million.

However, the costs incurred because of a cyber attack is only one part of the problem. The fallout from the loss of personal data creates just as many serious issues.

For instance Yahoo, suffered 3 major breaches affecting the data of around 2 billion accounts. As a result its sale price to Verizon was reduced by $4 billion, reflecting a major decrease in enterprise value.

Talktalk, the mobile phone company, lost the data for 150,000 users. As a result tens of thousands of customers went to other suppliers. The impact of this was far more serious that the £400,000 fine by imposed by the Information Commissioner and the £60M cost directly incurred in making good the damage caused by the attack.

Preventing Cyber Attacks - The Technology

Henry was asked whether cyber intrusions are inevitable. His reply was “yes”, but he went on to say that this did not mean companies should give up and live in fear. 80-90% of cyber attacks could be prevented by relative simple and cheap measures. He gave the following pieces of advice, simple to implement and important not just for business for all of us as home users as well:

1. Always apply patches and updates to your operating system and other software as soon as they become available.

2. Make sure your firewall is turned on.

3. Install an appropriate anti-virus program.

Just to show how important these issues are, and how often they are neglected, Henry pointed out that when Target suffered its attack it had installed a sophisticated anti-malware system at a cost of $1.6 million. This would have protected its system, indeed it detected the malware on a number of occasions and could have removed it automatically but this feature was turned off at the time as the company's security staff did not trust the system and ignored its alerts. Similarly there was a patch available for many versions of the Microsoft Windows operating system used by the NHS which would have prevented the problems caused by the Wannacry worm for some Health Trusts, but the patch had not been applied in many cases.

Preventing Cyber attacks - Government's Role

For larger systems there are of course other necessary measures to ensure they are properly configured to provide security. In this area government is currently taking a very active role. The National Security Strategy (2015) identified cyber attacks as a tier one National Security threat. The new National Cyber Security Strategy published in November 2016 is supported by £1.9 billion transformative investment, almost double the amount invested in the previous five years.

[To read the full text click HERE]

As part of the strategy, the National Cyber Security Centre has now been created, as part of GCHQ, to be the single point of advice to the UK government on cyber security, providing world class incident management capabilities. It is particularly concerned with the creation of technical defences at scale: supporting industry to

develop Active Cyber Defence capabilities to automatically tackle phishing, block malicious domains and IP addresses, and disrupt malware attacks.

Preventing Cyber Attacks - Management's Role

Henry then concluded the discussion on cyber security by emphasising two basic points. First, the whole of the C-Suite must be engaged in and committed to cyber security. This is not just a task for the CIO of CSIO (Chief Information Security Officer). Second the prevailing culture for efficient cyber security is to recognise this is not simply a problem of negligent users. Hackers have now become so sophisticated anyone can be caught out. .

Managing the Consequences of a Cyber Attack

Henry next moved to give some advice as to how to manage the consequences of a cyber attack. He made the point that how a company reacts when it is attacked can materially affect the business outcome. The basic principle is open, honest and timely announcements of the problem and the steps being taken to deal with it. He cited LinkedIn (which lost 117 million passwords and email addresses) Adobe and MumsNet as examples of such communication. Of course the cost to remedy the problem was still incurred but reputational damage was minimised, On the other hand both Yahoo and Ashley Madison suffered significant reputational damage by trying to ignore the problem and hoping it would go away.

It is essential to have a crisis management plan prepared in advance, so that it can be implemented quickly whenever necessary. Such a plan needs to address all stakeholders, but particularly customers or clients affected by the attack, employees and investors or shareholders, as well as keeping the general public informed if a public service provider is involved.

The CMO and Cyber Security

Finally Henry turned to consider the particular duties of the CMO in the field of cyber security, which he described as follows:

- Help identify key stakeholders
- Understand brand specific risks
- Engage in Business Continuity Plans
- Oversee the design and implementation of the Crisis Management Plan.

In order to discharge his responsibilities, the CMO needs to work wth all members of the C–Suite, and particularly to form a close relationship with the CIO or CSIO. Asking the following questions is a good way to start:

- What significant incidents have we had?
- What was our response?
- What was our most significant near miss?
- How was it discovered?
- How can marketing help with our cyber security initiatives?
- What are our priorities during a cyber attack?
- How is the performance of security team evaluated?
- Do you have relationships with / or take advice from government or industry bodies?
- Do you talk to your to supply chain partners, vendors or other partners?
- What is our plan to communicate internally and externally to key stakeholders?
- Have you lined-up expert support if a significant cyber attack impacts?

- Have you, or have you considered, evaluating the company against Cyber Essentials? [***For more information click:*** HERE]
- Have you looked at and briefed the Board on “10 Steps to Cyber Security”? [***For more information click***: HERE]
- Is the Directive (on security of) Networks and Information Systems (NIS) relevant to us? [***For more information click:*** HERE]

PART TWO - DATA PROTECTION AND PRIVACY

Data Security and Privacy Are Connected Issues

Henry then turned to consider data protection and privacy. He made the point that the question of privacy is intimately bound up with cyber security. Loss of data automatically involves loss of privacy for those affected.

Misuse of Personal Data a Bigger Issue

However, privacy of data is also concerned with fears that data holders may misuse or improperly disclose the data they hold on their customers. There is a high level of distrust with the larger data processing companies such as Google and Facebook, particularly in the light of the recent problems with Cambridge Analytics. The implementation of the General Data Protection Regulation (GDPR) is of course intended to deal with these issues

The Implementation GDPR a Positive Opportunity

The implementation of GDPR will require many companies to re-confirm the permissions and preferences of their customers and potential customers whose data they hold. Henry made the point that this can be done in a positive manner, reinforcing the image of the brand as one that cares about customers data.

The CMO and GDPR

Thus the CMO must play a pivotal role in dealing with the way the business reacts to GDPR. He should be concerned that the following matters have been dealt with, either through the marketing department or that of the CIO or the Chief Security Information Officer (CSIO):

- Audit of data holdings
- Confirmation that data encryption has been implemented, where needed
- Re-confirmation of contact preferences from customers
- Audit of the methods used by the business to gather and record customer permissions
- Audit of contracts with, and oversight of, third-parties who handle personal data collected by the business.