The Bridewell of knowledge

November 2015

Bridewell Consulting
Security & Risk Assurance Services

- Ongoing update on developments in security and risk assurance
- Promoting discussion between business leaders and security professionals
- Celebrating the value information security brings to business
- Objective perspective on current issues
- Building awareness and understanding
- Dispelling fear

How would you deal with an incident?

Information security breaches are once again headline news. Telecommunication and utility companies have seemingly lost valuable customer data, leaving their customers potentially vulnerable to fraudulent activity. There has also been the UK retailer. Their website leaked customer data even though they were quick to insist this was not a security matter but the result of 'internal issues'. This is perplexing in that the website did not even need to be hacked to expose customer data. The Information Commissioner's Office (ICO) is making enquiries.

In this latest round of security failures it is fair to say that the response from the companies involved did little to inspire confidence. These varied from denying the incidents were consequential, were the result of technical difficulties through to not being able to quantify the extent of the breach.

What went on internally within these companies will most likely never become public. However, what has, is the external communication element of their incident management processes. These could have been far more effective by clear messaging, acknowledging the problem and clearly outlining the steps they were taking to resolve the incident. Comments like we did not actually lose your customer log-on details or playing on semantics by arguing it was not actually a security incident do not inspire confidence and are simply counter-productive.

We live in a world where social media provides people with the opportunity to openly express their dissatisfaction with a company, their customer service. They can even highlight problems with websites before the company concerned becomes aware. Given this, all companies as part of any incident management process, should have a comprehensive communication plan that should not only stand up to scrutiny but also protect the people who matter the most - their customers.

Companies who embrace social media from a promotional and business development perspective must also do so when things go wrong. This leaves the big question as to how would your employer respond to a data loss?

Spam, spam, spam, spam

The canned meat spam (spiced ham) was immortalised in a famous Monty Python sketch which featured a couple trying to order in a cafe populated by Vikings. The couple found the menu contained nothing but spam.

There are a few explanations as to how the term spam became associated with fake (junk or illicit) e-mail messages. One theory is that because spam is jokingly referred to as fake meat it was logical to apply the term to fake e-mails. The second theory is linked to the Monty Python sketch where any attempt at a conversation by the couple using the word Spam resulted in the Vikings singing "Spam, Spam, Spam, Spam Wonderful Spam". The second theory is reinforced by some of the very early spam e-mail messages which were accompanied with the sound file of the Monty Python Viking Spam song.

Spam is a menace for a number of reasons. First, the volume of mail wastes valuable bandwidth and time. It forces people to delete unwanted messages which in turn impacts their productivity. Secondly, spam is a prime mechanism for the transfer of viruses and malware. It is used by criminals to initiate complex frauds providing the foundation of a phishing attack. Finally, there is the matter of cost. Whilst it costs relatively little for a spammer to send thousands of e-mails an hour and bounce the e-mails off third party servers, the cost of receiving and managing the received e-mails is significantly higher.

A recent study concluded that the cost to a small to medium sized business in the UK equated to a loss of more than £34,000 per year. The study analysed employees over a 30 day period noting that each employee on average received 25 unwanted e-mails per day. They concluded the time taken to deal with spam e-mails equated to almost one working day per year per employee.

Apple recently were criticised and classed as spammers for offering all iTunes customers a U2 album. Many customers said they were not U2 fans and they felt the offer was irritating and presumptuous and proved difficult to delete. Personally I would have preferred the Monty Python Sound Track of "Spam, Spam, Spam, Spam Wonderful SPAM".

It is clear that despite the tools we now have for managing and dealing with spam, it is a problem that is not likely to disappear any time soon.

To discuss what Bridewell Consulting can do for you please e-mail bc@bridewellconsulting.com

Bridewell Consulting LLP, Soane Point, 6-8 Market Place,
Reading, Berkshire, RG1 2EG, tel: +44 (0)1189 255 084

www.bridewellconsulting.com

Will my boat be safe in this harbour?

Another year is almost over and there is still no sign of the new EU data protective directive. However, there have been some significant developments including the recent European court ruling in response to the validity of US Safe Harbour rules. This has left many US companies facing the headache of how to manage client data outside of the EU.

Safe Harbour was the name given to a policy agreement established between the US and the EU in November 2000. It regulates the way US companies export and handle the personal data of European citizens while adhering to the stringent requirements for the transfer of personal data outside of the EU.

The Safe Harbour agreement established a framework as a compromise solution between US and EU privacy procedures. All European member countries were subject to the agreement which allowed data transfers without the authority of individual countries. US companies that did not join Safe Harbour had to obtain authorisation separately from each European country. In simple terms the agreement regarded US companies as an extension of the European Economic Area (EEA) implying they were trusted to safely transfer personal data. Safe Harbour was designed as a "streamlined and cost-effective" way for US companies to get data from Europe without breaking its data privacy rules.

As a result of the Snowden revelations a European privacy campaigner, alleging the US Government gained access to data relating to European citizens from US technology companies, asked the Irish Data Protection Commission to audit what material Facebook might be passing on. Initially he was rebuffed, being told it was all covered by Safe Harbour. However, the campaigner took the matter to the European Court of justice. They ruled that the Safe Harbour agreement did not eliminate the need for local privacy watchdogs to check US companies were taking adequate data protection measures. This effectively invalidated the Safe Harbour agreement.

Whilst the implications of the ruling will be played out over the coming months, the implications are clear. There are currently some 4000 companies relying on Safe Harbour who will have to reconsider their data flow architectures and look at alternatives for approving data transfers. This will include EU model contract clauses and Binding Corporate Rules (BCRs) even though these can involve lengthy approval process by European regulators.

As a result of the ruling the Irish Data Protection Commission has at least agreed to investigate allegations that Facebook was making personal data available to US intelligence agencies.

And finally... Bridewell Consulting at the ISC2 Congress 2015

Formed in 1989 (ISC)2 has a global membership of over 110,000 certified professionals across 160 countries. Their vision is simple, to inspire a safe and secure cyber world.

(ISC)2 is the largest not-for-profit membership body of certified cyber, information, software and infrastructure security professionals. A number of Bridewell consultants are members of(ISC)2 and carry their industry recognised certifications. including the Certified Information Systems Security Professional (CISSP), - Certified Cloud Security Professional (CCSP) and Certified Secure Software Lifecycle Professional (CSSLP), to name a few.

Bridewell Consulting has been working closely with (ISC)2 members to establish a new (ISC)2 Chapter in the Thames Valley. It was launched successfully in October 2014 with the inaugural meeting in Reading in February of this year. Bridewell has also been invited to speak at (ISC)2 Secure Events in Dublin and Rotterdam.

The (ISC)2 Security Congress EMEA was held in Munich in October. The event was well attended with close to 300 delegates from across the EMEA region. There were a number of highlights with excellent talks ranging from "How I hacked my Home", "The Cyberpsycology of Information Security" and the "Myths in Biometrics". Bridewell Consulting attended the event and were delighted to present on the challenges of Big Data and Security.

What makes this event different from other security conferences is that it is attended by a diverse mix of professionals such as lawyers, developers, risk managers and CISOs who carry (ISC)2 certifications. This mix makes for engaging debates and discussions. The event was a great success and it is one we would recommend to both security and non-security professionals to attend in 2016.

Bridewell Consulting will be hosting an (ISC)2 Thames Valley Chapter social and networking evening in Reading on the 3rd of December with the next public meeting planned for 11th February 2016.

For more information on this and the (ISC)2 Thames Valley chapter please contact bc@bridewellconsulting.com

INFORMATION SECURITY & ASSURANCE
CLAS Consulting, ISO27001 Advisory and PCI Compliance

CYBER SECURITY
Security Operations, Security Architecture and Network Security

INFORMATION & TECHNOLOGY RISK
Risk Management, Risk Assessment and Risk Treatment

SECURITY TESTING
Application and Infrastructure Penetration Testing

DATA PRIVACY
Data Protection Consulting and Audits