Editorial: Information Security

Claire Laybats & Luke Tredinnick

This issue of *Business Information Review* takes a focused look at Information Security, and the role of information professionals in securing information systems and processes. Information security is not simply a matter of IT security; it also encompasses legal compliance, governance, and workflow issues. Nevertheless a series of high profile cyber-attacks in recent years have bought the question of information security to greater public attention, and thrown light on our growing dependency on digital technologies. Privacy, data protection, and the misuse of data are now driving the political agenda around information security in some sectors. How did this come to be and why has information security risen up the political and commercial agenda?

The rise of information security

For many, 2015 was the year that information security became global news, with a string of news stories concerning major hacking or data breaches. Yet the current focus on information security issues really begins a little earlier, with the politicization of cyber activism, and it's attention to questions of privacy and civil liberties.

In 2010 the international non-profit journalistic website Wikileaks began publishing a batch of leaked US diplomatic cables. Although Wikileaks had been around for a number of years as a place where whistleblowers could anonymously leak sensitive or classified documents, the publishing of the diplomatic cables marked a significant change in the international profile of the organization. It also marked a change in tactics: Wikileaks working in collaboration with a number of traditional newspapers across the US and Europe to manage the disclosure. Old media and new media were coming together. The scale of the leak was unprecedented; over two hundred and sixty million words of data was involved, and the publication created headlines across the world over successive weeks. This was the largest disclosure of classified government information in history. And it was just the beginning of a new form of political activism relient on our growing dependency on information technology and on the architecture and infrastructure of the information age.

The cablegate affair mirrored a fundamental change in the function, role and scale of information in political and commercial organizations. On the one hand we now gather and maintain vast collections of information like never before across government and business. In the age of big data all information has value. On the other hand these vast swathes of data are subject to rapid and easy manipulation, and sometimes lax oversight. The nature of the digital infrastructure underpinning contemporary society makes it easier to manipulate information at volume. The fact that millions of documents can be carried on a tiny storage device and transmitted globally across high speed data networks makes leaks of the scale of cablegate almost inevitable. Information wants to be free. And that means that political

motivated data leaks now come in gigabytes, rather than pages. There is even a new profession that trades in transforming vast data sets into publically comprehensible stories: data journalism.

The cablegate affair established a pattern that was set to continue. In 2013 the computer professional Edward Snowdan leaked about 9000 documents originating from the US National Security Agency (NSA). The documents not only in themselves highlighted the vulnerability of digital information to disclosure, but also detailed the degree to which security agencies were engaged in systematic surveillance of digital communications globally. This year the disclosure of 11.5 million documents from the Panama based corporate services provider Mossack Fonseca has exposed the details of global finance and led to the resignation of the Icelandic prime minister. In between dozens of smaller political leaks have maintained a constant stream of information emerging from cyber activism.

The high profile cases related above reflect the rise of hacktivism – political activism that comes in the form of hacking and exploiting information systems and communications networks, with a focus on issues around civil liberties, privacy and freedom of speech. Hacktivism is not just a concern for governments, increasingly it is emerging as a tool to attack commercial enterprises. After the cablegate leaks the Anyonymous collective attacked companies who had withdrawn services from the Wikileaks foundation, including Amazon. In July 2015 a politically motivated group compromised and leaked customer account information for Ashley Madison, a website that traded in facilitating extra-marital affairs. The account details subsequently appeared online. The disintermediating effects of the global information network enables this kinds of direct action.

A few months after the Ashley Madison hack, the British telecommunications services provider Talk Talk sustained what it described as “a significant and sustained cyber attack” (BBC, 2015). Customer account details including payment details were compromised in what appeared to be a corporate extortion attack. It later transpired that the account details were not encrypted. This was not hactivism, but another side effect of a global digital economy: cybercrime. In November 2015 ten million account profiles for the VTech educational software company were compromised. The same month, the credit referencing agency Experien was hacked with customer information of up to 15 million customers compromised. Each year there are countless cases of extortion and blackmail based on data breaches, many of which go unreported. Each case creates untold anxiety amongst the organizations’ customer bases and did untold damage to the reputations of the organizations involved.

If the kinds of incidents described above seem to be becoming more and more common in the twenty-first century, that is because they are. They testify to a fundamental change in the global information and communications infrastructure. Information itself has become more integral to every part of our lives. Individuals, business and governments now generate vastly more information each day than even in the relatively recent past. All commercial operations are now to some degree in the business of managing, manipulating and selling information in one form or

another. In a very real sense information is value in the digital economy. But information has also become a kind of currency; we exchange information about our interests and identity in order to access services online. If information has greater value, then it becomes more susceptible to criminal or political intervention.

But despite appearances, there has not been a sudden explosion in the volume of cybercrime and cyber activism, or indeed a sudden rise in the importance of information security. While it has become over recent years matter of widespread public concern and media interest, the problem of information security has been with us for over thirty years, and growing steadily throughout that time. Indeed, the origins of hacking, cyber activism and cybercrime in the hobbyist computing subculture the 1970s still has a significant bearing on how the issue is framed in contemporary culture, and out responses to it. Therefore it is worth briefly exploring what this relationship is.

The beginnings of cybercrime

Cybercrime in Britain has a definitive beginning. In 1984 a young computer hacker who went by the pseudonym of *Triludan the Warrior* was messing around with a modem and home computer. He already had a *Prestel* account of his own, but that didn't stop him typing a string of 2s at the log-in prompt of the system. To his surprise, the username was accepted. Triludan sat back from the keyboard. If someone had chosen such a basic string of characters for a username, he thought, perhaps they had applied the same approach to the password. After a few attempts he was in with *1234*. Without really trying he had gained full access to a test account owned by a British Telecom employee. It was almost as if British Telecom wasn't taking security seriously at all. He later recalled: "I came across a Prestel test ID by accident – I was testing a modem and just typed random numbers, basically" (Cited by Leyden, 2015). That accident was the beginning of what became one of the most important hacking cases in British legal history.

Prestel was then still a relatively new videotex system; it had been developed by British Telecom in the late 1970s and by the mid nineteen eighties had almost one hundred thousand subscribers. Most users accessed Prestel via a dumb terminal connected to a television set, but it could also be accessed via computer and modem. This was the dawn of consumer online systems, and the very latest addition to Prestel was Mailbox, a service that allowed subscribers to send electronic messages to one another.

Triludan's test account gave access to information on Prestel that ordinary users could not see – information about the organization of the Prestel system, and also a list of telephone numbers for development computers. He shared this with friend and journalist, Stephen Gold, and together the two hackers found a way to gain root access to the main Prestel service. They could now change, delete, or read any of the pages on Prestel. They could access and send messages from every user mailbox. To prove what they had done, they left a message on the Duke of Edinburgh's Mailbox,

and after trying to warn British Telecom directly, they contacted the press. Stephen Gold and a now unmasked Robert Schifreen were arrested shortly after.

By the early 1980s hacking was beginning to garner increasing public awareness. Just a year before the Prestel Hack, the film *WarGames* (1983) had highlighted the potential dangers of hacking with typical Hollywood overstatement, as a youthful Matthew Broderick graduated from altering high school grades to bringing the world to the brink of nuclear war. The same year, the *414s*, a group of teenage hackers in Wisconsin, were identified after having accessed government computers and banks. In Europe, the recently formed *Chaos Computer Club* was already beginning to attract mainstream attention, and by 1985 would become known around the world for transferring 134,000 DMs in a hack of a precursor to online baking systems. Public attitudes towards cybercrime had been primed by this kind of coverage, and by the strange, unfathomable nature of the emerging online world. Cyberspace – coined by William Gibson the same year as the Prestel hack – was an alluring but unfamiliar place for most. Many of the stereotypes we still associate with hacking and cybercrime – the brilliant but socially awkward and isolated teenager working from their bedroom in the middle of the night- were forged during this period. British public opinion was primed for a major information security scandal, and the Prestel hack came at precisely the right time.

However it was not immediately clear what offence Schiffreen and Gold had committed. The UK did not have dedicated laws against cybercrime at this time, and while successful prosecutions had been bought in the United States by charging hackers with theft of minute quantities of electricity from the systems they penetrated, it was thought that a counterfeiting charge might be more successful. The case hinged on whether the username and password used by Schrifreen and Gold constituted a counterfeited instrument. While they were initially found guilty, eventually on appeal they were acquitted with the law lords criticizing the "procrustean" attempts to bring the forgery act to bear on a computer crime.

What followed in the wake of R v. Schifreen & Gold (1988) was a scramble to introduce legislation to protect against the emerging threats of hacking and computer crime. Largely influenced by popular stereotypes and public misconceptions rather than real threats, the first Computer Misuse Act (1990) cast its net fairly wide with vague and ambiguous wording throughout. It did not, for example, define computer. It did not define a computer program. It did not define data. Despite this potentially wide reach only a handful of successful prosecutions have been bought. As a recent ONS discussion paper (2014) reveals, there is a massive discrepancy between the perception of risk, and the number of offences that have been committed.

Thirty years later, the R. V Gold & Schifreen seems rather quaint. Hacking, information security, and cybercrime are no longer the preserve of lone hackers working from their bedrooms. Not only Prestel, but the whole culture of online bulletin board systems accessed via direct dial-up connections has gone by the wayside. Yet the issue of cybercrime and information security has not gone away. Indeed, over the last few years it has come to haunt the tech industry. And the way

in which we think about cybercrime and information security is still influenced by idea of the brilliant hacker working in isolation to penetrate distant and arcane information systems.

The legacy of the Prestel hack endures in our attitudes towards information security, cybercrime, and risk, and endures in the computing misuse legislation in force in the UK. In some sense information security is still most commonly framed as an *external threat* emanating from some nefarious source, rather than as a matter of internal risk management. The coverage of more recent high profile hacking cases and information security breaches re-enforces this idea of an external threat. But in many ways, the major problems that are created by out increased dependency on information are not the external threats to which it is subjected, but the internal processes by which it is managed.

What is Information Security?

At first glance, information security seems like a fairly straightforward and uncomplicated concept – a matter of technically securing information systems and data against unwanted intruders, malicious software, and unwanted use, and maintaining the fitness for purpose of information in order to minimize institutional risk. However, information security is more than just a matter of IT security. It is more than simply maintaining firewalls, anti-malware software, and secure passwords. The security of information poses innumerable risks for businesses in the contemporary world: the risk of falling foul of the information law; the risk of significant reputation damage through data breaches and leaks; the risk of not being able to conduct business owing to catastrophic failure of information systems, and the risk of becoming subject to sustained political action aimed at disrupting commercial operations.

Most definitions of information security encompass a number of different issues in relation to information and data management: confidentiality; integrity and availability. Confidentiality relates to limiting the availability of information to unauthorized individuals or entities – essentially preventing information falling into the hands of those we would like to prevent accessing it. Integrity on the other hand relates to maintaining the accuracy and completeness of the information collection over its life cycle including managing and auditing modifications to the data or data collection. Availability is a matter of insuring the information is available to the processes in which it is required, and that the security controls and processes are fit for purpose.

We of course inevitably associate information security with digital information because so much of the information on which contemporary commercial practice currently depends is digital in nature. However, unlike IT security, information security does not necessarily or exclusively relate to digital information.

The technological components of information security are relatively well understood. Firewalls monitor, block and filter traffic on networks. Anti virus, anti spyware, and

anti malware software scans programmes and data for malicious content. Strong encryption secures data, data transfer and communications against eavesdropping and accidental leaks. Access management, version management, and audit logs help maintain the integrity of information systems. These components are the high walls, locks, security gates, and the barred windows of information security, interrupting the free flow of information in order to ensure its control. But it is a mistake to think of information security as a matter or erecting fences, barricading entrances, and choosing the most secure locks. Security is not something that is *applied* to information systems and processes after the fact, it is something that must be built in from the beginning.

Building information security into information management processes is a matter of understanding the nature of the threats involved. There is a tendency to exaggerate the external threats to information and data – the danger of hackers, political hacktivists, and various forms of malware - and to underestimate the internal threats – the disgruntled or careless employee. Information security threats can be broken down into a number of different kinds:

- The intentional consequences of intentional actions, e.g. hacking, denial of service (DoS) attacks, malicious software, spyware, industrial espionage, and deliberate data theft, leaks or breaches.

- The unintentional consequences of intentional actions, e.g. accidentally or carelessly deleted information, accidentally or carelessly disclosed information, unintentional breeches of confidentiality, unintentional data leaks.

- The unintentional consequences of unintentional actions, e.g. accidental loss of data, accidental destruction of data.

In many ways the first of these are easiest to predict, and easiest to protect against. The intentional consequences of intentional actions describes the kinds of malicious actions and software that draw most coverage: hacking; malware and data theft. These risks are relatively easy to articulate: the known unknowns of the information security world, the events we can anticipate and prepare for. Far harder to predict are the unintentional consequences of intended or unintended actions: the critical emails that are deleted rather than archived; the information shared with a mailing list rather than an individual; the briefcase accidentally left on the train containing a batch of client files. We can write policy to prevent employees installing their own software and hold them accountable if they do; we can train them to understand the risks from malware and spyware involved in this. There is no policy than can prevent someone from losing a USB storage device or pressing reply-all on a group email – the policy and training implications of these unintentional and unpredictable events need to focus on minimizing the potential impact of these risks.

Information security is a matter of understanding and managing risk, and not eliminating threats. When every functional computing device is also a networked computing device, there is no such thing as an absolutely secure information system.

Just as important as maintaining the confidentiality of information is maintaining the fitness for purpose of both information and the processes into which it is slotted, and this inevitable involves risk. More secure systems bring about their own kinds of risks for organizations, the very real trade of between security and the free flow of information need to be weighed every day.

Almost without exception the real information security weak-spots in any system or process are not technological vulnerabilities but human operators. Humans have a habit of behaving in unpredictable and sometimes inexplicable ways. Hackers have a name for exploiting the human problem in information security. It is called social engineering. Social engineering is the process of tricking someone into disclosing passwords, access details, or confidential information often by masquerading as someone who is or should be entitled to access. As the infamous hacker and subsequently cyber security specialist Kevin Mitnik observes, it is often easier to trick someone into allowing you access to a system, than to bother hacking it:

> "For the social engineer, it is the easiest way to reach his goal. Why should an attacker spend hours trying to break in when he can do it instead with a simple phone call?" (Simon & Mitnick , 2003).

People behave in ways that they shouldn't and that they know they shouldn't because often it is more convenient, more polite, or just normal practice. They use simple or predictable passwords; the use the same passwords on multiple systems; they write down their passwords; they share their log in details with colleagues; they respond helpfully to inquiries; they leave systems logged-in; they take home files on memory sticks; they use the same email for personal and professional purposes. We all know these things are a problem. And yet we all almost certainly indulge in some of these bad information security habits at some point. So ubiquitous are they that it becomes almost irresponsible to ignore them.

The fact that humans are the real weak spot in many information security processes highlight that information security should not be considered primarily as a technological issue. The technology has altered the scale and intensity of communication and information practices, but the underlying principles of human socialization remain the same. Information security is at its heart a problem with people, and their messy, unpredictable, organic nature. The way to address information security is to understand how information slots into the work processes within an organization, and where the vulnerabilities lie.

Information Security and Business Information Review – July 2016

In 1984 while Robert Schrifreen was idly experimenting with the Prestel log in page, Business Information Review had just published its first issue. That issue included coverage of the Prestel service and later the journal covered the ensuing court case (Tagg, 1986). From its birth through its infancy to today, this journal has precisely mirrored the age of information crime and information security in the UK. It is perhaps appropriate then that this issue of the journal is focused in particular on

issues related to information security and governance. By focusing on information security and information governance we hope to highlight not only the importance of the issue in contemporary business and commerce, but also the contribution of the information profession to managing security and risk.

The articles published in this issue of *Business Information Review* all address questions of information security in one form or another. First is Ralph O'Brien's paper *Privacy and Security: the New European Data Protection Regulation and what it means for data breaches.* Ralph is Principle Consultant EU for5 TRUSTe, TRUSTe a leading global Data Privacy Management company. His paper explores the changing regulation around data protection emerging out of the European General Data Protection Regulation (GDPR) and in particular its impact on the management of data breaches.

The GDPR is also discussed in David Haynes' paper, *Social Media, risk and information governance.* David is a regular contributor to *Business Information Review* and visiting lecturer at City University London. His paper address what is often an overlooked area of information work: social media governance. David's paper develops a risk management model of governance that addresses the threats to which social media strategies and outputs give rise. It makes an important case for the risks associated with social media and the importance of incorporating them into information governance processes.

A new contributor to the journal, Nick Wilding is Head of Cyber Resilience at AXELOS Global Best Practice - a joint venture company set up in 2013 and co-owned by the UK Government and Capita plc. Nick is responsible for RESILIA™ Global Best Practice - a portfolio of cyber resilience best practice publications, certified training, all staff awareness learning and leadership engagement tools designed to put the 'human factor' at the centre of your cyber resilience strategy. In his paper - *Cyber resilience: How important is your reputation? How effective are your people* – Nick argues for a move from thinking about cyber security to thinking about cyber resilience, and outlines the guiding principles of cyber awareness learning, training and education.

Finally, Danny Budzak returns to *Business Information Review* with a new paper: Information Security: the people issue. Danny's paper examines the information security issues raised by the involvement of people with information systems. It first sets out the threats to information systems, and the risks associated with information systems, before addressing the mitigation of those threats through managing roles, responsibilities, relationships and training. The paper rounds off for us an exciting issue, and a new venture into themed content than hopefully we shall be developing in the future.

Initiatives and perspectives

Regular readers will know that a key part of each issue of *Business Information Review* are the regular *Initiatives* and *Perspectives* columns, which both round up some of the developments in the business information world. In *Perspectives* Martin White explores recent publications both in the information world and beyond that have relevance for professional practice. This issue he draws attention to research

on data management emerging form the Information School at Sheffield University, research into newspaper archiving practice in the United States, and returns to the issue of information overload amongst other topics. Once again we are also grateful for Alan Fosters continued work in producing *Initiatives.* This issue Alan addresses a range of developments in the areas of digital transformations, data management, value and volume of data, higher education and IT, IM and data skills development, and open data as well as the latest industry news. As ever it is an incredibly comprehensive and useful resource.

References

BBC (2015), Talk Talk Cyber Attack, BBC, available at: http://www.bbc.co.uk/news/uk-34611857 [accessed: 10 May 2016]

Leyden, John (2015), How a hack on Prince Philip's Prestel account led to UK computer law, *The Register,* *http://www.theregister.co.uk/2015/03/26/prestel_hack_anniversary_prince_philip_computer_misuse/* [accessed: 10 May 2016]

ONS (2014), Discussion paper on the coverage of crime statistics, *Office for National Statistics,* available at: http://www.ons.gov.uk [accessed: 10 May 2015]

Simon, W. & Mitnick, K. (2003), The Art of Deception: Controlling the Human Element of Security, London: John Wiley & Sons.

Tagg, Lawrence, (1986), Initiatives, *Business Information Review,* 3 (1): 40 – 46.