scripted

Volume 5, Issue 2, August 2008

The Internet: Where Did IT All Go Wrong?

Robert Schifreen[*]

Abstract

It is hard to imagine life today without the Internet, and all of the benefits that it brings to our business and personal lives: convenient, cheap and instant communication across time zones and national boundaries; online shopping and banking; document and data exchange without the need to ship media; collaborative working and online entertainment; and free access to more information than previous generations could ever have dreamed of. Rapid progress indeed, for a global information system that didn't exist until the summer of 1991 when the world's first website went online at CERN as a result of work by Tim Berners-Lee. It's also hard to imagine life today without all of problems that the Internet has introduced: phishing attacks, cyber-bullying, data theft on a scale never before imagined, spam, distributed denial-of-service attacks, ransomware, spyware, website defacements, and so on, none of which will disappear any time soon, despite the best efforts of the myriad purveyors of security systems, or the specialist IT crime units that have been set up alongside traditional police forces throughout the world. This analysis assesses the various ways in which the Internet has changed our lives, and the problems that it has brought. It also offers suggestions and advice as to how the effects of those problems can be mitigated in the future.

DOI: 10.2966/scrip.050208.419

[*] IT Security trainer and Web Developer, University of Brighton. Author of "*Defeating The Hacker*" (2006, Wiley).

1. Introduction

Large-scale public online information systems such as the Internet are nothing new. In 1979, Prestel was introduced to the UK as a dial-up network offering information from a variety of commercial, governmental and amateur sources plus email facilities; at its peak it boasted some 90,000 subscribers. France had a similar system in the form of Minitel, introduced as an electronic substitute for printed telephone directories, but which rapidly spread to attract users with a wide range of special interests (many of them sexual, it must be said – always a significant driver in establishing uptake of online systems). Throughout the 1980s, the IT press ran headlines hailing the coming "year of the modem." Interest in online communications continued to grow, but while these systems proved popular with users, they suffered from being insular; subscribers to Telecom Gold and Prestel could not email each other, for example. The emerging computer-savvy teen generation fragmented into those who were committed fans of the online world and those who were not.[1] In this analysis, I assesses the various ways in which the Internet has changed our lives, as well as the problems it has brought. I also offer suggestions and advice as to how the effects of those problems can be mitigated in the future.

2. Enter the Hacker

The online world of the 1980s shared one charactistic with that of today, namely the existence of the hacker. While the technical skills and resources of yesteryear's hackers were high (considering the relative difficulty in obtaining and sharing information compared with today), their motivation may well have been very different. Arguably, hackers of the 1980s were not out to cause damage or disruption, but were driven by curiosity and the wish to be able to defeat the best efforts to keep him out. They guessed passwords – not to steal vast amounts of private information but to test whether they could. Having discovered another new password, they would record it carefully in their notebooks and move on. The thought of using that password for gain or malice rarely crossed their minds.[2] Indeed, 1980s hackers would have had a hard time finding any significant systems to attack; few companies had computer networks, and fewer still were connected to the outside world. Technical magazines aimed at corporate IT personnel regularly published articles entitled "Do you need a LAN?", explaining the benefit of linking together the few deskop computers that they controlled. The year of the network had not yet arrived. The standard medium for storing corporate information was still the neatly filed sheet of paper. Computerised databases did exist, but they were rare and mostly offline on floppy disks. Those that were online were connected to slow telephone modems and

---

[1] This division may have been facilitated by the fact that a quality modem typically cost several hundred pounds, and most people needed at least two because Prestel had its own standard. Users also paid for accounts on various online systems, and the lack of interconnectivity meant having to regularly log into each of them.

[2] I concede that malicious hackers existed, but they were not the norm, and I contend that the approach I describe above was more common.

call charges made them expensive to access (especially from outside the country in which they were based). Those (old) hackers, assuming they could afford the telephone bill, simply stood little chance of stumbing across much data of interest.

3. Rise of the Internet

As the 20th century drew to a close, the Internet was rapidly revolutionising corporate IT. Discrete systems became joined-up, allowing their users to converse with each other. Internal LANs and WANs started to become commonplace, and the server ousted the filing cabinet as the storage medium of choice. Today, the traditional dial-up modem is almost obsolete in the West, with domestic users having super-fast, permanent connections that would have cost thousands of pounds per month just a decade ago. In a survey published in May 2008 to mark Museums and Galleries Month in the UK,[3] the Internet was cited as the second best invention of all time, between the wheel and penicillin. But this electronic global village has brought an explosion in digital crime which few could have imagined. Today's corporate and domestic Internet users deploy ever-growing amounts of new equipment and facilities without pausing to adequately consider, and cater for, the security implications. The remainder of this article examines this situation more detail.

4. The Need for Speed

The data communication speeds available to even the smallest businesses today are staggering, compared with just a few years ago. The best-performing modems operated at 56,000 bits per second (bps), although first-generation online systems ran at just 300 bps. Today's broadband can theoretically run at 8 million bps, some 140 times faster than the best of the old-breed modems. Even if the "up to 8 meg" service only hits 30% of its headline speed, that is still 8000 times faster than a 300 bps modem. This allows much faster access to web pages, audio content and on-demand movies, but it also means that hackers can scan networks by the thousand in search of vulnerabilities, and quickly download any confidential information that they happen to enounter. High-speed communications, coupled with the ever-growing ability of modern hackers to exploit such technology, has resulted in ever wider scope for attacks. A Distributed Denial of Service (DDoS) attack against a web site can disable it without the need to know any secret usernames and passwords. Instead, the power of a few hundred broadband-connected computers is harnessed to flood the site with legitimate requests in order to overwhelm it. In such DDoS attacks the victim site may face, each second, the amount of traffic that it would normally experience in a month.

5. Modern Hackers and the Internet

Today's electronic miscreants and cyber-vandals have access to millions of interconnected systems, all of whose virtual door handles they can rattle day and night at incredible speeds for a fixed monthly fee. They can hide behind anonymising web proxies, or operate via a Wi-Fi link from the nearest coffee shop or bar that offers free

---

[3] 'Museums Key To Preservation Of Ideas Says MGM Survey' available at: http://www.mgm.org.uk/press/ART57533.htm.

wireless access. No longer do hackers need to put in countless hours of obsessive research to learn the art of upsetting computers. A couple of words typed into a search engine will lead to the necessary tools for decrypting scrambled wireless network traffic, cracking Windows passwords, creating a virus or a botnet, and plenty more besides – including a free program for Windows that automatically fires some 1500 ready-made hacking queries at Google. Search engines such as Google can lead hackers straight to confidential data without any real hacking at all, simply by helping them to locate private information that has inadvertently been placed on publicly-accessible web servers by people who should have known better.

It is easy to assert that there is no legitimate need for programs that aid hackers, and that the distribution and possession of such tools should be criminalised. That is certainly the view of many governments, including that of the UK.[4] However, the IT security industry is quick to point out that not all hackers are so-called "Black Hats" (i.e. those who hack to cause deliberate damage); there are also many "White Hats" around who indulge in hacker-like activity for the public good.[5] These include researchers looking for vulnerabilities in existing systems or to test new ones, law enforcement agencies who need to access protected data found on the laptops of terrorist suspects or paedophiles, and even the humble help desk operative who is asked to recover a protected spreadsheet for which the Marketing Director has forgotten the password during the long Christmas break.

Who are these "hackers", "crackers", "virus-writers", "spammers", "phishers", and why do they want to attack your network?[6] For many, hacking was once a method of studying and a fun way to impress friends (and girls, occasionally), but in recent years, as networks have begun to hold information that is much more valuable, those who still indulge in the practice are less interested in boosting their ego or showing off and more interested in compiling money.[7] DDoS are less likely to be a college student wanting to learn whether it's possible; they're more often the result of a company refusing to give in to a blackmail threat. Phishing attacks aren't a harmless bit of fun to see how many people fall for the trick – those who do get taken in will find their bank accounts emptied in just a few minutes, with the proceeds often ending up funding drug cartels and organised crime.

The IT security industry is forever playing catch-up, trying to beat the hackers at their own game. But they will never win. The criminal fraternity is always one step ahead. The security industry will never be anything but reactive, and that includes corporate IT security personnel who have to spend much of their time fire-fighting with the result that they rarely have the resources to look to the future.

---

[4] P Sommer "Criminalising hacking tools" (2006) *Digital Investigation* 3, 68.

[5] C C Palmer "Ethical Hacking" (2001) 40 *IBM Systems Journal* 3, available at: http://www.research.ibm.com/journal/sj/403/palmer.html.

[6] ***Hacker:*** an individual who seeks to access or investigate computer systems for curiosity or education. ***Cracker:*** also termed *malicious hacker*, one who access computer systems for illicit gain or to cause damage. ***Virus Writer:*** a creator of computer viruses; with the advent of virus-writing kits, little actual programming skill may be needed to become a *script kiddie*. ***Spammer:*** someone who sends mass unsolicited commercial email in the hope of garnering sales. ***Phisher:*** a hacker who sends email seeking to lure victims to fake websites that capture information such as bank account details.

[7] "McAfee North America Criminology Report: Organized crime and the Internet 2007" available at: http://us.mcafee.com/en-us/local/html/identity_theft/NAVirtualCriminologyReport07.pdf.

But these problems aren't solely the result of the cyber criminals that roam the Internet. While today's situation is undoubtedly partly caused by those criminals, blame must also be laid at the door of the legitimate consumers and businesses who have jumped on one or more of the new technology bandwagons with nary a thought as to the implications. The IT industry works unceasingly to get us all hooked on new technology, and not hard enough on making that technology secure or helping us to use it properly. It recommends high-tech products such as broadband routers or SAN storage solutions to home users, but rarely makes any effective effort to offer support or training. So when the home SAN goes down and loses every photograph, DVD and music track, it's the technology that gets the blame.[8] We fall in love with the features and benefits, but are woefully unprepared for the risks.

In the 2008 Information Security Breaches survey, published by BERR (formerly the UK's Department of Trade and Industry),[9] 84% of the large organisations that responded claimed that they were "heavily dependent" on their IT systems. Yet far too many companies deploy new technology without giving sufficient thought as to how they will cope when it doesn't work properly.

6. Recent Incidents and Risks

In May 2008, a hacker in Chile accessed personal data on about 6 million citizens which was then posted on a public web site.[10] In the same month, Spain arrested two "prolific" teenage hackers for allegedly disrupting government websites in the US, Asia and Latin America.[11] Just a couple of days later, it was reported that cyber criminals had started to attack an entirely new area of Internet connectivity, namely VoIP telephone calls.[12]

It is important to note, however, that not all online mishaps are the result of deliberate action. A Conservative candidate in a UK by-election inadvertently sent an email to a journalist containing the party's entire database for the constituency, listing the names and voting intentions of 8000 people.[13] This came shortly after Virgin Trains triggered an improper mailing list, accidentally requesting the company of thousands of commuters at a prestigious golf event, rather than just a dozen of its best customers.[14]

Previously, in what is thought to be the worst example of accidental data loss, the UK government lost two CDs containing personal information on 25 million citizens who were claiming child benefit.[15] While most media commentators blamed Her

---

[8] Similarly, it is the technology that will get blamed when an innocent man is convicted of accessing child porn web sites, because his router shipped with encryption turned off by default and so passers-by were able to easily access his Internet connection.

[9] http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html

[10] 'Hacker leaks 6m Chileans' records' available at: http://news.bbc.co.uk/1/hi/world/americas/7395295.stm.

[11] 'Spain arrests 'prolific' hackers' available at: http://news.bbc.co.uk/1/hi/world/europe/7406260.stm.

[12] 'Identity fraud hits net telephony' available at: http://news.bbc.co.uk/1/hi/technology/7398676.stm.

[13] 'Inquiry into Tory e-mail blunder' available at: http://news.bbc.co.uk/1/hi/uk_politics/7413826.stm.

[14] 'Virgin 'sorry' for day out invite' available at: http://news.bbc.co.uk/1/hi/business/7390263.stm.

[15] 'Discs loss 'entirely avoidable'' available at: http://news.bbc.co.uk/1/hi/uk_politics/7472814.stm.

Majesty's Revenue and Customs for not having encrypted the data, there are more significant lessons to be learned (eg: around access control and limitation). It is impossible to fathom why any user of the system was permitted to dump these records to CD ROM, regardless of whether the information was encrypted. Such a facility should never even have been implemented.

The development of online databases, especially by government agencies, shows no sign of slowing down. For example, the NHS is currently developing one of the world's largest systems, allowing tens of thousands of health practitioners access to tens of millions of patient records.[16] Merely deciding who should be able to see what is a nightmare. Actually implementing and policing it will be worse. Similarly, the British government recently suggested allowing the intelligence services to bring together records of citizens' phone calls and emails into one database that could easily be searched and analysed for patterns.[17] The havoc which could be wrought by any unauthorised access to, or modification of, the data within either of these systems can only be imagined.

Today's determined hacker or opportunistic thief can readily steal large amounts of information from a system to which he has physical access. Portable storage devices such as USB drives or external hard disks, not to mention digital cameras and MP3 players, allow criminals and legitimate users to carry large amounts of data in a small space. While a USB pen drive is an incredibly handy device, companies are becoming aware that they also allow dishonest employees or unguarded visitors to quickly copy large amounts of data from an unprotected workstation. With 8GB pen drives (holding the equivalent of 5700 of the old-style 1.44MB floppy disks) now selling for around £10, the problem is unlikely to go away soon. Conversely, external hard drives are now readily available in capacities up to 1 TB. At 20 KB per page, such a drive can store a pile of paper 30 miles high.

Broadband has led to a large increase in the number of companies that use the technology to allow staff to work from home. In the aforementioned BERR survey, 54% of large companies who responded said that they allow remote access to their systems. Yet, in my experience, few companies have adequately considered the security implications of allowing their network to expand beyond their walls into the homes of dozens or hundreds of employees, many of whom will have PCs that are regularly used for non-business purposes. A virus on a home computer could allow unfettered access to the entire corporate network.

Today's technology also means that employees can easily travel with a local copy of their entire corporate computing environment in the form of a laptop, smartphone or PDA. Previously, a thief who witnessed an employee locking a laptop in the boot of his car would have forced open the boot and steal the computer. Nowadays, technology makes the thief's life much more easy. He simply strolls around the car park in search of BlueTooth signals emanating from hibernating laptops and then decides whether to steal the computer or just the data (by connecting to it remotely and siphoning off information).

---

[16] 'NHS e-records programme launched' available at: http://news.bbc.co.uk/1/hi/health/7130627.stm.

[17] 'Phone calls database considered' available at: http://news.bbc.co.uk/1/hi/uk/7409593.stm.

The BERR survey reveals that 42% of large companies currently use some form of wireless networking, yet 34% still rely solely on WEP encryption even though a few seconds with a search engine will produce abundant advice on how to crack it. Equally, 71% of companies claim to have changed the default SSID of their wireless network, presumably unaware that this offers no increase in security whatsoever. The ease with which wireless networking can be installed means that it is all too easy for staff to add wireless access points to their office without the knowledge or permission of the IT department. If these WAPs are not correctly configured, they open the entire corporate network to all passers-by. Network managers of my acquaintance who have taken the trouble to scan their systems for unauthorised WAPs have invariably been shocked by the results.

Arguably the greatest problem with Windows Vista is that its friendly user interface hides what is actually an extremely complex product. Before Windows XP Microsoft's PC operating systems were clearly divided into two camps, with Windows 2000 targeted at commercial users while PC enthusiasts made do with Windows 95 and 98. Although the OS has now converged into a single product for both home and business use, Microsoft has failed to impress upon home users just how important it is to configure and maintain their PC correctly. In the business arena, such tasks require the services of experienced and trained staff. Home users who buy into the technology but fail to understand its complexity rapidly fall prey to the cyber criminals. The situation is not helped by both Windows XP and Vista creating administrator-level accounts by default, giving complete power both to the novice user and any virus or Trojan which finds an inroad into the PC.

While security providers continue to urge corporate customers to spend an ever-growing amount on security products and services, the irony is that much of this expenditure is actually unnecessary. The Security Breaches survey reveals that large companies now spend 7% of their IT budget on security, up from 2% in 2002. Yet much of the computer misuse which takes place within the corporate arena stems not from the lack of security products but the lack of staff security awareness. Only 40% of large companies currently provide ongoing security awareness training, and hackers are aware of this; no firewall will prevent an employee falling for a phishing scam or disposing of an unwanted PC without first wiping the hard disk.

The Internet makes it all too easy to set up an online shop, and many companies have been tempted to do so despite their lack of experience in operating online or selling securely. Although many security weaknesses can be avoided by purchasing a ready-made software package to create e-shops, some of these products have significant shortcomings which can be exploited by hackers, not all of which are initially obvious to those who purchase them. For example, at least one package sends out emails to customers containing the URL from which they can download their invoice. This URL contains the serial number of the order, which can be changed to view full details of any previous order by any customer. Not only does this allow hackers to effectively access the entire database of previous orders (including customer names and addresses), it also provides invaluable information to competitors.

Not all websites are designed to offer online sales; the majority are simply online brochures, and these have become the must-have items in the digital world. According to the security breaches survey, 93% of large companies have a web site. But while a web site is easy for authorised staff to update, it is just as easy for hackers to deface if they can exploit bugs in the system or manage to guess a password. In the

past few years, many companies, as well as many of the world's major political parties, have suffered at the hands of web site defacers.

Despite being able to access the web from home at broadband speeds, most people still expect Internet access from their office. According to the BERR survey, virus infections, once the major cause of concern for IT security personnel, are now cited by only 6% of respondents as being the most disruptive type of security incident encountered; top, at 50%, are worries about staff misusing the Internet at work. Not only does this cause massive waste of time and money, it also provides a handy way for dishonest employees to smuggle confidential information out of the company. Despite this, 84% of large companies who responded to the survey said that they did not scan outgoing email in order to look for private data.

But of all the security problems that the Web has caused, threats to the online banking industry are by far the most serious. Criminal hackers have realised that raiding online bank accounts is relatively easy compared to staging armed robberies, the chances of being caught are much lower, and, if one is caught, the penalties are less. Phishing attacks are becoming more sophisticated by the week. Poorly-spelled emails are now giving way to professionally-produced messages which attempt to install complex keystroke loggers and other Trojans. Banks realise that computer hackers could spell the end for their business, not just through theft of money but also through loss of goodwill. Financial institutions are therefore now beginning to roll out hardware access tokens, despite the enormous cost implications. Although they can scarcely afford to deploy this technology, they have reluctantly realised that they cannot afford not to.

7. We CAN Make it Better

Although much of today's spending on IT security is unnecessary, there are two areas where the right products can literally save the company and its reputation. One is to ensure that adequate backups are taken frequently and tested regularly. The other is the correct use of encryption to ensure that confidential data which escapes from the company premises cannot be accessed by unauthorised users. Encryption is most important on devices such as USB memory sticks, and also on laptops and other portable computers, which are most commonly subject to theft. However, although strong encryption is built into Windows in the form of the Encrypting File System (EFS), there are fatal flaws in its implementation which often lead to problems when PCs are replaced and the encrypted backup cannot be restored onto the new hardware.

The computer firewall is a relatively modern invention, necessitated by the Internet but still notoriously difficult to configure correctly and securely. Lack of firewall security often allows inquisitive hackers to access inadequately-protected IP surveillance cameras, which are proving popular in many homes and workplaces. Being able to view your premises over the Internet from anywhere in the world is very appealing, but not configuring your firewall correctly will allow everyone to do the same. As IP cameras start to take watch over not just car parks but school halls, swimming pools, server rooms and other private places, those who install them must be aware that unprotected cameras can quickly be located by hackers through a simple Web search.

The Science and Technology Committee of the House of Lords recently issued a report into the state of Internet security in the UK. The report was based on some 700

pages of evidence and ideas, much of which made very good business sense.[18] For example, it was suggested that a policy of mandatory reporting be introduced to ensure that police were aware of any major corporate hacking. It was also suggested that computer vendors be legally obliged to provide computers which were inherently secure, and configured to automatically install security patches. The report criticised the decision to disband the National High Tech Crime Unit and merge it into the Serious Organized Crime Agency, as well as the decision to force consumers to report online banking security breaches to their bank rather than the police, which leaves no single point of reference as to the severity of the problem. Unfortunately, the government has so far accepted none of its recommendations.

8. Conclusion

Computer crime is not going away. It will continue to evolve and advance, alongside our continued use of the Internet to operate our daily lives. Data supermarkets already exist, where hackers trade personal information for $3.00 a throw. Gambling sites, one of the latest industry sectors to have moved online, are the target of attempts by hackers to blackmail them into handing over money in order to prevent a serious system crash. Meanwhile, as more children and pensioners discover the joys of the Internet, these two groups face increased levels of targeting by criminals across the world.

Cyber criminals will evolve,[19] and so must we. There is a growing need for vigilance by all of us, and greater awareness of the dangers that the Internet poses. In the corporate world, excellent advice comes in the form of BS 7799 and its international counterpart,[20] yet the BERR survey reveals that only 54% of large companies are actually aware of its existence and only 11% have implemented its recommendations. The same survey finds that 9% of large companies still store all their critical backups on-site, which will result in total loss of all backed-up data in the event of a major fire or other catastrophe.

No longer is effective IT security down to purchasing and installing security products. The greatest improvement in security can actually be brought about by being more aware of the risks, and by educating others to be similarly concerned. Despite what it says on the box of most security products, it is impossible to buy peace of mind. Security, it is said, is an attitude rather than a product. Never were truer words spoken.

---

[18] House of Lords Science and Technology Committee, 5th Report of Session 2006–07 'Personal Internet Security.'

[19] In the decades to come, we can expect hackers (terrorists or even governments) to attempt to disrupt major infrastructure systems such as power supplies and financial industries by penetrating critical computer systems, and thus future warfare may also transform.

[20] ISO/IEC 27002.