Information Security Now – 50

Big Hacks
(Can They Teach Us Anything?)

John Mitchell

When the editor requested an article on big hacks I immediately realised that I had a problem with the definition of ‘big’. Is it the sheer volume of compromised data, or is it the impact it has on an individual; an institution; a nation state; the world? More importantly can they teach us anything for the future? But how is any impact to be measured? Many reporters concentrate on the financial aspects, but I consider that the most important thing is loss of trust. Loss of trust in data processing itself. Perhaps it would be possible to evaluate several hacks to derive a formula to measure their significance? When I was researching for my doctorate in risk management I once created a twenty-seven-element formula to calculate the significance of a risk. The only problem was that I only had hard data for four off those elements, the rest being guestimates, which bought a severe element of doubt to the result. Could it be trusted? With hacking we have the same problem. How accurate are the numbers? Tabloid journalism may be important in alerting the public to a breach, with headlines along the lines of the ‘biggest hack so far’, but is such loose language helpful in measuring actual impact?

In the Beginning

The story of electronic hacking begins almost with the dawn of the electronic age, when in1903 Nevil Maskelyne disrupted a public demonstration of Marconi's purportedly secure wireless telegraphy technology by sending insulting Morse code messages through the auditorium's projector. What has this to do with today’s computing? Well, if you cannot trust the information you receive from a system, then what reliance can you place in the system? So, perhaps one of the most important elements in assessing the significance of a hack is to determine its impact on trust? If I can hack fifty million access credentials and effectively become those people, then trust in anything received from those people is diluted. Conversely, those people will have reduced trust in the institution which allowed their data to be compromised. A word of caution. Volume is not everything and relatively small hacks may have a significant impact on subsequent trust. Making IT good for society is this Institute’s strap line, so anything which undermines trust in IT is likely to be bad for society.

Different Hacks – Same Outcome?

Hacks are emerging as one of the most significant risks facing all enterprises, but there are some who seem to be repeat offenders, mainly because of their visibility. These customer-facing companies receive more attention than companies in other sectors, such as mining, manufacturers and logistics, where the damage to their reputations among consumers and subsequent loss of trust, is unlikely to be as severe. Perhaps this also needs to be built into any equation? The email that arrived in 382,000 BA customers’ email inboxes in the

early hours of Friday 7th September 2018 served up the usual platitudes from companies which have been hacked. "We take the protection of your personal information very seriously. Please accept our deepest apologies for the worry and inconvenience that this criminal activity has caused". This data breach was significant not so much by the number of customers affected, but the potential value of the data stolen. Complete credit card information, including security codes and associated bank account details, together with enough other information to fool the security checks of other accounts. BA put the onus on the affected customers to contact their financial services providers. Also, although BA contacted the impacted customers, they did not send a reassurance message to those who had not been compromised, leaving millions of customers wondering whether their data had been stolen, but they had missed any subsequent warning message. Not the way to restore trust in your operations and the company is also facing a £500 million group action lawsuit. The airline may also receive a fine of up to £897million if regulators find that it has been in breach of GDPR where penalties for serious failings are capped at the greater of four per cent of global turnover, or €20 million. So, another couple of elements to be added to any hacking equation?

A different kind of hack, Wannacry, stole nothing, but demanded money with menaces, along the lines of 'we have encrypted your data and if you want to get it back, then pay us'. This showed that a denial of data attack could be more damaging than a straight-forward denial of service attack, but the result is the same. Loss of trust in data processing.

Insert A lists what many reporters believe as being some of the most significant hacks, since Maskelyne's embarrassment of Fleming in 1903. I stress that these are public domain hacks and exclude those which are classified, and which are often more frightening in their potential impact. The list also suffers from the exclusion of a couple of hacks which, although not large in volume terms, I deem to be very important and which I shall discuss later.

The listed examples indicate that the number of compromised, or stolen user accounts is seen as the most appropriate measure of an important hack. I beg to differ. In some cases, the impact of a single hack on a solitary device may have significant consequences. Also, many of the hacks listed are dwarfed by simple incompetence, such as that displayed by TSBs attempt to upgrade its banking platform. The full cost of this fiasco could spiral to as much as £229 million which would comfortably exceed its last year's pre-tax profits of £163 million and easily outstrip the financial impact of most of the listed hacks.

Small, But Perfectly Formed

In the 1990s a legitimate hacking group within the US military took control of a warship's weapons' control systems and were able to control the targeting of its weapons. The same group then manipulated the flight programme of a fighter squadron. They were able to direct the fighters to a non-existent refuelling tanker which showed their ability to 'splash' a squadron of aircraft without firing a shot, or even being in the vicinity. A new form of warfare, cyber-warfare, had been created.

In 2016 hackers took control of the engine management system of a Jeep and proved that they could drive it off the road. This single hack has cast doubts on trust that can be placed in driverless cars.

The Bangladesh central bank hack only involved 35 transactions and yet the perpetrators took just over $100 million and it could have been as much as $1 billion, but for a simple spelling error.

These hacks did not involve large numbers of transactions, but along with the Stuxnet hack, the potential consequences are so huge as to put them high on the list of significant hacks. From a learning perspective it becomes obvious that sheer volume is not necessarily the thing that makes a hack significant. Also, these hacks were external, but what about the threat from inside the organisation, or from trusted partners? I will deal with this aspect later.

Cyber Warfare Hacks

Nation states are probing for weaknesses in their opponent's national infrastructure as part of an undeclared cyber war. In 2013 it was widely reported that the British secret service has tapped into at least 14 undersea cables passing through Cyprus using passive optical splitters which enabled GCHQ to daily intercept tens of millions of e-mails, SMS messages and phone calls. This hack is significant on a pure volume basis alone, but even more so when one considers the range of data intercepted and the use to which it can be put. On the other side, the Russian GRU has been linked to a series of cyber-attacks around the world. The United States charged 12 GRU agents with involvement in the hacking of Democratic Party national committee emails before the 2016 presidential election. This may have been a relatively small hack on a volume basis, but the subsequent leaking of selected emails badly damaged Hilary Clinton's attempt to become President of the USA, so on an impact basis this hack was monumental. Recent reports indicate that the Moscow's GRU spy network has also conducted a series of attacks on the UK's energy networks, telecommunication systems and media groups. Last year the boss of the National Cyber Security Centre (NCSC), revealed that since his organisation was established in October 2016, it had seen Russia repeatedly target vital British infrastructure. Staff at the NCSC had responded to more than 600 "significant incidents" between 2016 and 2017.

Trusted Parties

Genuine errors made by insiders, such as clicking on dangerous email links, poor password management, sharing passwords, losing equipment, etc., occur daily. I once sat next to someone on an aircraft and simply by looking over their shoulder I was able to obtain the system security log-ins for a major oil company, plus enough other information to conduct a phishing attack on their company. Negligence of the highest order, but not deliberately malicious. However, what about the malevolent side? In 2016 IBM's Cyber Security Intelligence Index found that 60 per cent of all attacks were carried out by insiders, three-quarters of which involved malicious intent. Research by Willis Towers Watson in 2017 also showed that 66 per cent of cyber breaches were down to employee negligence, or malicious acts. This highlights the weaknesses of people within the organisational control mechanisms. This means that any up-to-date threat assessment should have insiders high on the list. This includes the suppliers and contractors to which we give authorised

access to our systems and data. We trust them to do their job and hope that they will behave. But trust is not a control and privileged users often have access to sensitive data, have knowledge of the system architecture, configuration and tools and can cover their tracks. See **Insert B** for an example of this.

Faith v Trust

Volume isn't everything and incompetence may be more damaging than malicious intent. Trusted staff, or third-parties may be more dangerous to us than external attacks. Any attempt to measure the significance of a hack must not only evaluate the number of records stolen, or accounts compromised, but also the indirect cost of the hack and what it may point to for the future. A single hack on a solitary car is not in itself of great importance, but its potential impact on trust in autonomous vehicles may well rate it as one of the most significant hacks of recent times. Likewise, the Stuxnet worm may only have affected a single installation, but its ability to alter the mechanical behaviour of an engineering system puts trust in autonomous manufacturing systems in doubt. If we cannot trust our vehicles, or our manufacturing, or our financial systems, or the news that we receive, then what reliance can we place on data processing as being good for society? Faith is defined as belief without proof. As an IT auditor I believe that trust comes from belief in the reliability of a system to protect my data and always produce the correct result. If the system is compromised, then trust is also compromised. So, perhaps what I should be looking for is an equation which measures trust, of which a hack is just another element to be considered when evaluating the confidentiality, integrity, availability and compliance aspects of a system.

INSERT A

Significant Hacks

British Airways – 2018
Three hundred and eighty thousand payment details stolen, together with enough personal information to fool security checks on other systems.

Superdrug – 2018
Twenty-thousand customer details stolen. The pharmacy advised thousands of its online customers to change their passwords after hackers attempted to blackmail the chain.

Facebook – 2018
Not a hack in the accepted sense, but Facebook allowed a third-party, Cambridge Analytica, to harvest details of 87 million users for political purposes.

Cosmos Bank - 2018
Fake credit cards were then used to force ATMs around the world to dispense cash worth about $13m (£10m) until they were empty.

Equifax - 2017
Cybercriminals penetrated Equifax and stole the personal data of 145 million people.

Yahoo - 2017
Parent company Verizon announced that every one of Yahoo's 3 billion accounts were hacked in 2013.

NSA Hacking Tools - 2017
In April, a group called the Shadow Brokers leaked a suite of hacking tools widely believed to belong to the National Security Agency.

WannaCry - 2017
WannaCry, which spanned more than 150 countries, leveraged some of the leaked NSA tools. The ransomware targeted businesses running outdated Windows software and locked down computer systems. More than 300,000 machines were hit across numerous industries, including health care and car companies.

NotPetya - 2017
The computer virus NotPetya targeted Ukrainian businesses using compromised tax software. The malware spread to major global businesses.

Bad Rabbit - 2017
Another major ransomware campaign infiltrated computers by posing as an Adobe Flash installer on news and media websites that hackers had compromised. Once the ransomware infected a machine, it scanned the network for shared folders with common names and attempted to steal user credentials to access other computers.

Voter Records - 2017
In June, a security researcher discovered almost 200 million voter records exposed online after a GOP data firm misconfigured a security setting in its Amazon cloud storage service.

Uber - 2016
Hackers stole the data of 57 million Uber customers, and the company paid them $100,000 to cover it up. The breach wasn't made public until 2017.

LinkedIn – 2016
164 million accounts compromised in a slow-motion breach that took four years to discover. The reason this is a significant hack is because of how long it took for the company to understand how badly they had been hacked.

FBI – 2016
A 15-year-old hacked the FBI and released detailed information about every undercover FBI officer in America.

Bangladesh Central Bank – 2016
Instructions to fraudulently withdraw US$ 1 billion from the account of the central bank of Bangladesh, at the Federal Reserve Bank of New York were issued via the SWIFT network. Five transactions, worth $101 million were successful, although $38 million has since been recovered. Federal Reserve Bank of New York blocked the remaining thirty transactions, amounting to $850 million.

Adult Friend Finder – 2016
More than 412 million user accounts. The FriendFinder Network, which included casual hook-up and adult content websites was breached. The hackers collected 20 years of data on six databases which included names, email addresses and passwords.

Anthem Health Care – 2015
Seventy-eight million users. The second-largest health insurer in the United States had its databases compromised through a covert attack that spanned weeks. The company claimed that no medical information was stolen, only contact information and Social Security numbers.

Ashley Madison - 2015
The hacker group Impact Team broke into the Avid Life Media servers and copied the personal data of 37 million Ashley Madison users. The hackers then incrementally released this information to the world through various websites.

U.S. Office of Personnel Management - 2015
Certainly, the largest espionage coup of all time, unknown hackers obtained detailed records of every employee and consultant of the U.S. government for the past 50 years, including all top-secret cleared employees.

Home Depot – 2014
Over 50 million credit card details were stolen by exploiting a password from one of its stores' vendors.

eBay - 2014:
145 million online shoppers had their password-protected data compromised. This hack is particularly memorable because it was public and because eBay was painted as weak on security because of the company's slow and lack-lustre public response.

Mt. Gox - 2014
$460 million worth of Bitcoins stolen over the course of three-to-four years.

JPMorgan Chase – 2014
83 million accounts were compromised. Which included 7 million small-business accounts and 76 million personal accounts.

Target Stores – 2013
Credit/debit card information and/or contact information of up to 110 million people compromised. The breach was not discovered for several weeks.

Adobe - 2013
38 million user records. Hackers stole encrypted customer credit card records, plus login data for an undetermined number of user accounts.

Spamhaus – 2013
The largest DDoS attack to date. This DDOS attack was sufficiently large to slow down the entire Internet and completely shut down parts of it for hours at a time.

Global Payments - 2012
110 million credit card details stolen**.** Global Payments is one of the several companies that handle credit card transactions for lenders and vendors.

Sony PlayStation – 2011
77 million users**.** Sony took down its service for several days to patch holes and upgrade their defences.

RSA Security - March 2011
Possibly 40 million employee records stolen by a phishing attack.

VeriSign - 2010
Undisclosed information stolen. Security experts are unanimous in saying that the most troubling thing about the VeriSign breach, or breaches, in which hackers gained access to privileged systems and information, is the way the company handled it. VeriSign never announced the attacks. The incidents did not become public until 2011, and then only through a new SEC-mandated filing.

Stuxnet Worm - 2010
This worm subverted more than half of Iran's 8,800 uranium centrifuges causing them to spin out of control while reporting that they were operating normally.

Conficker Worm – 2008
Still infecting a million computers a Year. While this resilient malware program has not wreaked irrecoverable damage, this program refuses to die. It hides and then copies itself to other machines. This worm continues to open backdoors for future hacker takeovers of the infected machines.

Heartland Payment Systems – 2008
34 million credit cards exposed through SQL injection to install spyware on Heartland's data systems. It wasn't discovered until January 2009, when Visa and MasterCard notified Heartland of suspicious transactions from accounts it had processed.

TJX - 2008
94 million credit cards exposed. There are conflicting accounts about how this happened. One supposes that a group of hackers took advantage of a weak data encryption system and stole credit card data during a wireless transfer between two Marshall's stores. The other has them breaking into the TJX network through in-store kiosks that allowed people to apply for jobs electronically.

Estonia Cyber War - 2007
The Baltic state suffered three weeks of DDoS attacks, which completely crippled its IT infrastructure. The attackers targeted political, government, news outlets, universities, schools and businesses and eventually Estonia's banking infrastructure.

The Melissa Virus – 1999
Twenty percent of the world's computers were infected by a virus masquerading as a Microsoft Word file attachment.

INSERT B

A different kind of hack

Most of the reported hacking relates to unauthorised people obtaining unauthorised access, but there is another more assiduous attack. My American client's central system was provided by a third-party. The contract provided for access by the supplier to my client's machine to maintain the software. Security was provided by a VPN and a log-in process. However, to maintain the software, the supplier required super-user status. The audit motto is 'trust, but verify', so I decided to compare supplier log-ins with the change log. My client did not maintain such a log, but I eventually (and reluctantly on their part), obtained it from the suppler. I established that the supplier was logging into my client's machine at times which bore no relationship to the change log. Out of curiosity I checked for access to my client's financial and payroll systems and established that the supplier was using his enhanced status to access the data on those systems. Was this unauthorised access being sanctioned by the supplier's management, or was it a rogue member of staff? I alerted my client, but what should be done? They needed the third-party software and it had to be maintained which required the enhanced access. We decided on a two phased approach. First, we would disable the user account and only enable it when maintenance was required. Second, we would confine the supplier to a virtual machine containing only their system. Its ancillary software and associated files. We explained to the supplier's management that we were simply upgrading our security processes and they did not raise any objections. Since then I have identified other cases of hacking by trusted third-parties which have been facilitated by the trusting nature of my client. This unauthorised access by authorised people is likely to become more common with the growth of cloud services.

John was awarded the 2017 John Ivinson medal for services to the Institute. He is a previous member of Council and the Risk, Audit and Finance Committee. He is currently Treasurer of the Information Risk Management and Assurance (IRMA) specialist group. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or on +44 (0)7774 145638