Briefing Paper

Cybersecurity Revisited

(See also Cybersecurity November 2013)

October 2016

Introduction

2016 has proved to be a bonanza year for cyber-attacks, but may yet prove to be no more than part of a secular upward trend. It began with a group calling itself *New World Hacking* which claimed responsibility in January for taking down the BBC's global website and Donald Trump's website using the largest ever DDoS attack recorded up to then.

Source: http://thehackernews.com/2016/01/biggest-ddos-attack.html

Then came an attack registered at 620Gbps that hit 'Krebs On Security', the website of security researcher Brian Krebs. The big warning there is that the attack made use of a botnet that captured and orchestrated the attack from 150,000+ compromised Internet-of-Things devices, routers, DVRs and security cameras.[1] The same technique was then used just last week (late September) to take down the French hosting company website OVH.com, in two simultaneous assaults of 799Gbps and 191Gbps, for a total of 990Gbps.[2]

In an all-connected world, cyber-crime is a given, and the cost is inexorably rising. In many cases, but by no means all, it may remain more of a nuisance than an existential threat, but the severity of the attacks is on the rise. Personal inconvenience of being hacked or losing files due to malware is one thing, downing an enterprise website using DDoS as on the scale of the attack on SONY, or stealing IDs and account numbers is quite another, and the thought of cyberwarfare is yet another.

[1] Techradarpro (28 Sept 2016) 'Here's how security cameras drove the world's biggest DDoS attack ever' http://www.techradar.com/news/internet/here-s-how-security-cameras-drove-the-world-s-biggest-ddos-attack-ever-1329480

[2] The Register (27 Sept 2016) '152k cameras in 990Gbps record-breaking dual DDoS' http://www.theregister.co.uk/2016/09/27/152463_hacked_cameras_deliver_990gbps_recordbreaking_dual_ddos/

Personal

Receiving suspicious emails from 'friends' is one way to know they have been hacked. Phishing, Spear Phishing, downloaded malware, directions to a fake website, by now these are well tried and tested methods of petty theft which can, if passwords are revealed, lead on to bigger crimes. But when Dropbox loses 70 million customer passwords and emails[3] followed by the announcement that Yahoo! lost over 500 million, [4] there are grounds for disbelieving professional IT companies are hosting your data safely.

The problem is especially acute in the Yahoo! case, partly because the evidence suggests Yahoo! was *aware* of the hack before Verizon agreed to buy the company for US$4.8 billion – a sum that will likely be renegotiated – but even more so because apparently, Yahoo! was *unaware* until July 2016 that the hack had begun in 2014. Initial claims that the hack was in some way state-sponsored have since been disputed by security firm *InfoArmor*; they suggest the hack was by "Group E", who are believed to have sold the data at least three times on the dark web.[5] A recent study of 383 companies globally for IBM by the *Ponemon Institute*, found that the average cost paid for each data record on the dark web had increased to US$158 from US$154 in 2015.[6]

> According to our research, the average total cost of a data breach for the 383 companies participating in this research increased from $3.79 to $4 million. The average cost paid for each lost or stolen record containing sensitive and confidential information increased from $154 in 2015 to $158 in this year's study.[7]

The sample size is too small to extrapolate, nor was the research company able to adjust for non-respondents who may have had a different profile, but the authors believe "the current sampling frame is biased toward companies with more mature privacy or information security programs."

---

[3] The Telegraph (28 August 2016) 'Dropbox hackers stole 68 million passwords - check if you're affected and how to protect yourself' http://www.telegraph.co.uk/technology/2016/08/31/dropbox-hackers-stole-70-million-passwords-and-email-addresses/

[4] The Financial Times (24 September 2016)'Yahoo faces questions over delay in data breach revelation' https://www.ft.com/content/54ec6bd8-818e-11e6-8e50-8ec15fb462f4

[5] Wall Street Journal (29 September 2016) 'YahooHack Origin Disputed' https://www.pressreader.com/ Wikipedia (accessed 3 October 2016) "The dark web is the World Wide Web content that exists on darknets, overlay networks which use the public Internet but which require specific software, configurations or authorization to access. The dark web forms a small part of the deep web, the part of the Web not indexed by search engines, although sometimes the term "deep web" is mistakenly used to refer specifically to the dark web." The dark web is the secondary market where anything can be for sale.

[6] The report alternates between data record and per capital data loss. The letter term is not used in this Briefing Paper to avoid confusion with per capita national income

[7] IBM and Ponemon Institute (June 2016) '*2016 Cost of Data Breach Study: Global Analysis*' http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN and Infographic at http://www-03.ibm.com/security/infographics/data-breach/

Enterprise

One of the major causes of weakness in the cybersecurity of enterprises lies in legacy systems that have not been updated, sometimes for many years. Furthermore, updating legacy systems can be extremely difficult if they are housed within expensive specialised tools. For example, Windows XP still accounts for around one-third of all desktop operating systems globally, and if it is used in a very costly healthcare MRI scanning machine, upgrading is not an easy option. This is a boon to hackers. Lauri Love, a British hacker who is facing extradition to the US for hacking into Pentagon computers, and who now advocates hacking for the good rather than the bad of an enterprise, makes the point about failure to update security.

> Hacking is mostly a case of persistence, it is not always a case of spectacular ability – just determination to keep looking until you find the one thing that wasn't up to scratch.[8]

An extreme example, but not an uncommon one, was highlighted during the trial in Seattle of Roman Seleznev, son of a Russian Member of Parliament, who was found guilty of hacking into restaurant and retail Point of Sale (PoS) systems between 2009 and 2013 using automated techniques, such as port scanning to identify computers used to process credit cards and connected to the Internet. He then downloaded malware into those computers. His job was made easy by the legacy systems in use.

> In some cases, the victim's security practices were startlingly deficient as well. "In the case of the Broadway Grill, in particular, every credit card number that had been swiped at the restaurant between December 1,2009, and October 22, 2010, (over 32,000 unique credit card numbers) had been saved to a text file that was stored on the business' back of the house computer," the 2014 indictment noted. Seleznev was then accused of placing additional malware on the restaurant's POS to capture subsequent credit card numbers.[9]

Besides lax security that is vulnerable to hackers, there are plenty of cases of data loss due to security glitches rather than malicious attacks, and to human error, such as the fat finger problem. In 2015, "Deutsche Bank mistakenly paid US$6bn (£3.9bn; €5.3bn) to a hedge fund client in the US after a junior trader entered the wrong amount."[10] A report the previous

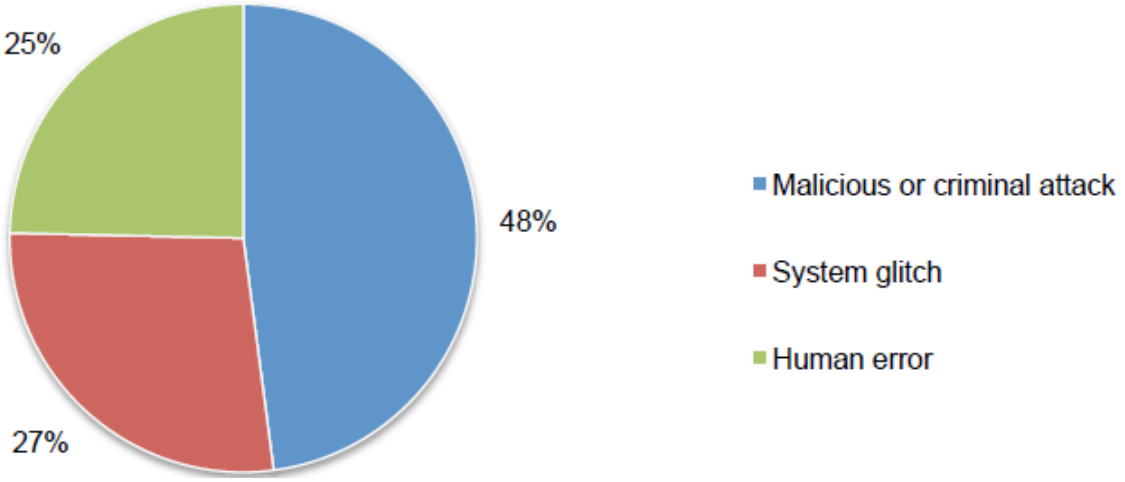
[8] Financial Times 'Cyber Poacher turns gamekeeper' 3 October 2016

[9] Arstechnica (28 Sept 2016) 'Hacker who stole 2.9 million credit card numbers is Russian lawmaker's son' http://arstechnica.com/securi'ty/2016/08/hacker-who-stole-2-9-million-credit-card-numbers-is-russian-lawmakers-son/

[10] International Business Times (20 October 2016) 'Deutsche Bank's $6bn 'fat-finger' error revealed' http://www.ibtimes.co.uk/deutsche-banks-6bn-fat-finger-error-revealed-1524773

year suggested human error is responsible for one in five data loss errors.[11] The IBM/ Ponemon Institute report estimated 25% of data losses were due to human error in their sample, and 27% to system glitches, thus malicious or criminal attacks accounted for under 50%.

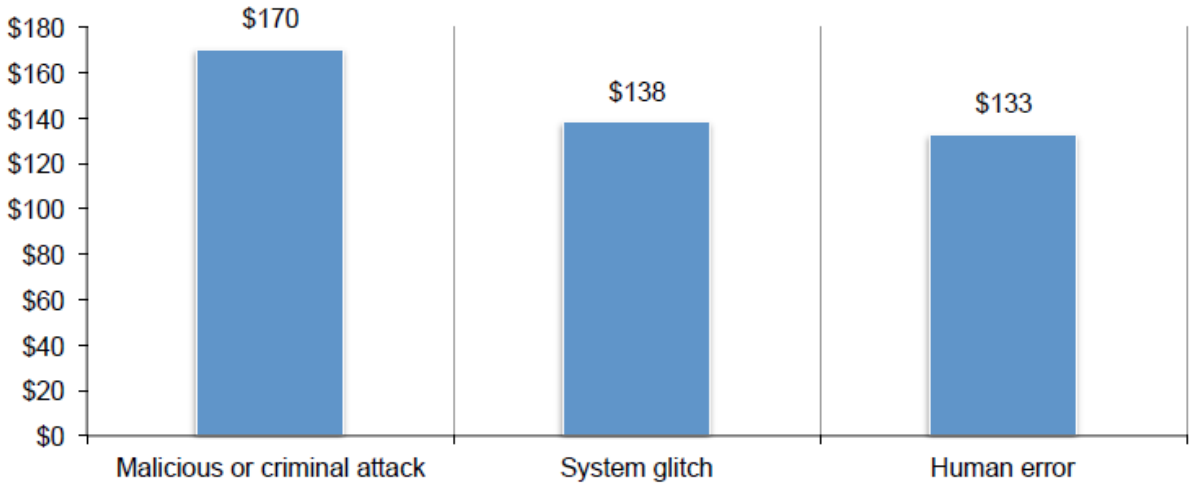
Distribution of the benchmark sample by root cause of the data breach



Source: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

However malicious attacks accounted for the highest cost per data record of the three causes of data loss.

Per capita cost for three root causes of the data breach (US$)

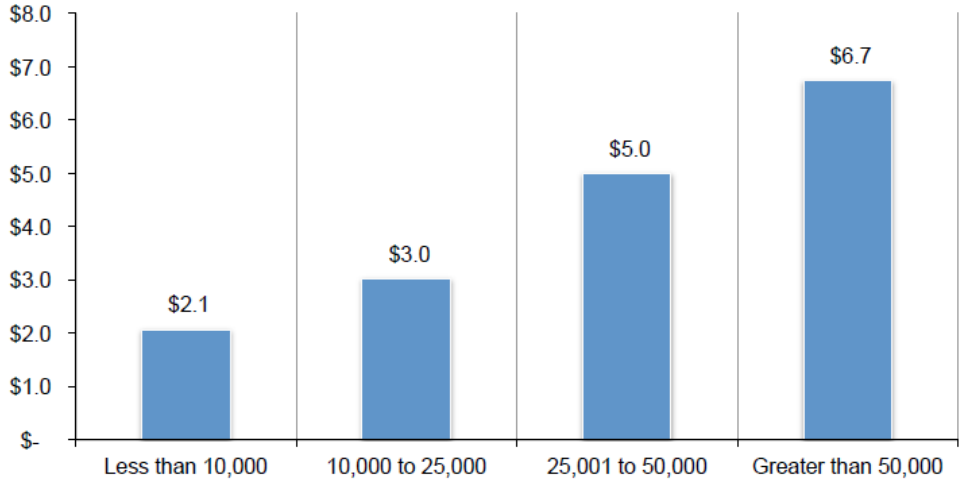


Source: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

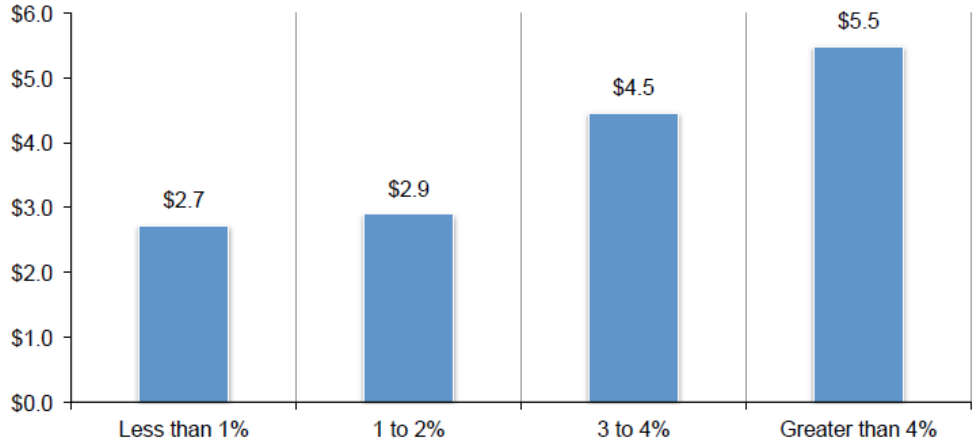
Of the costs that arise from data loss two factors seem to outweigh others. The first is the scale of the loss and the second is the increase in churn rate among customers due to reputational damage.

[11] CloudTech (3 November 2014) 'Beware the fat finger when it comes to cloudy data loss' 'http://www.cloudcomputing-news.net/news/2014/nov/03/beware-fat-finger-when-it-comes-cloudy-data-loss/

Total costs by size of data breach (US$ millions)

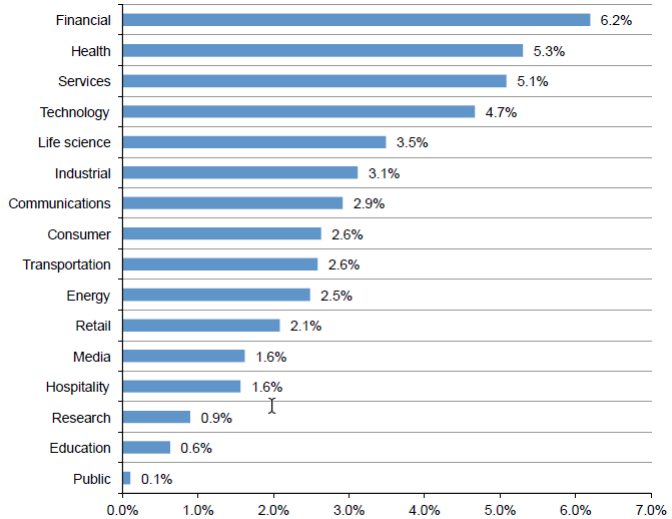


Total costs by abnormal churn rate (US$ millions)



Source: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

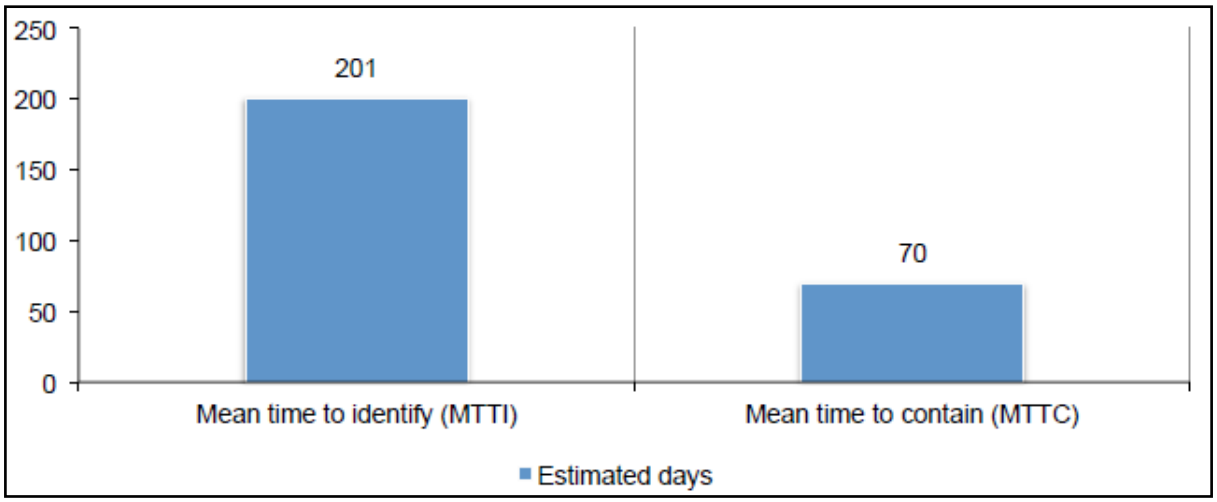
Abnormal churn rates by industry classification of benchmarked companies



Source: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

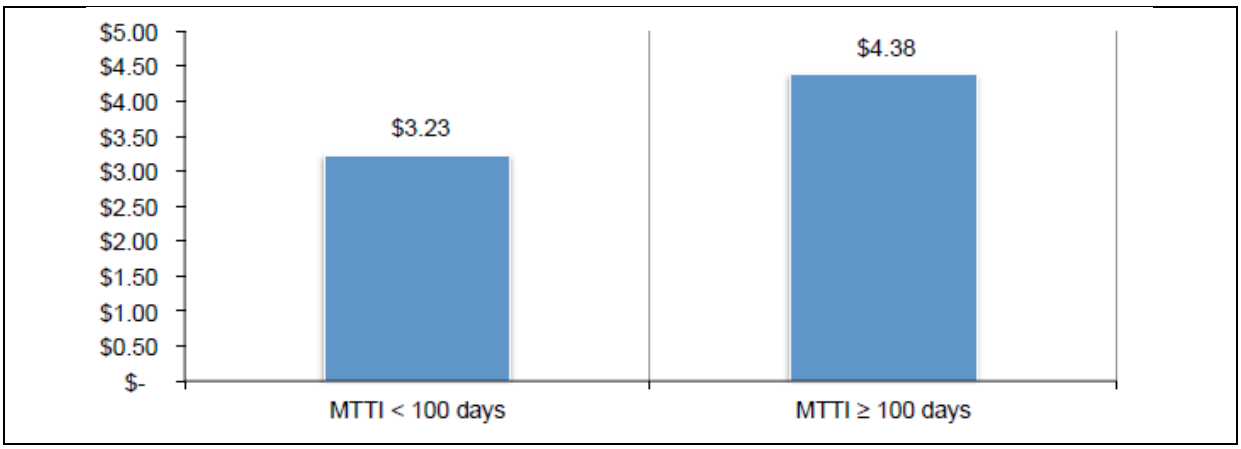
Unsurprisingly, in the sample used, the financial services sector is especially vulnerable to the effects of churn, followed by the health services sector and the service sector in general. Many of these costs will be regarded as the costs of doing business, just like how supermarkets adjust their overall prices to cover the costs of pilfering, but as more businesses move online, for example retailing, they will find they are paying the prices for a loss of reputation. The loss of trust in the safety of credit card or healthcare information will simply destroy some companies. One of the most concerning charts in the IBM/Ponemon Institute report shows the average time it took the sample companies to detect (Mean Time to Identify or MTTI) and to resolve the problems (Mean Time to Contain or MTTC).

Mean time to identify and contain data breach incidents (in days)

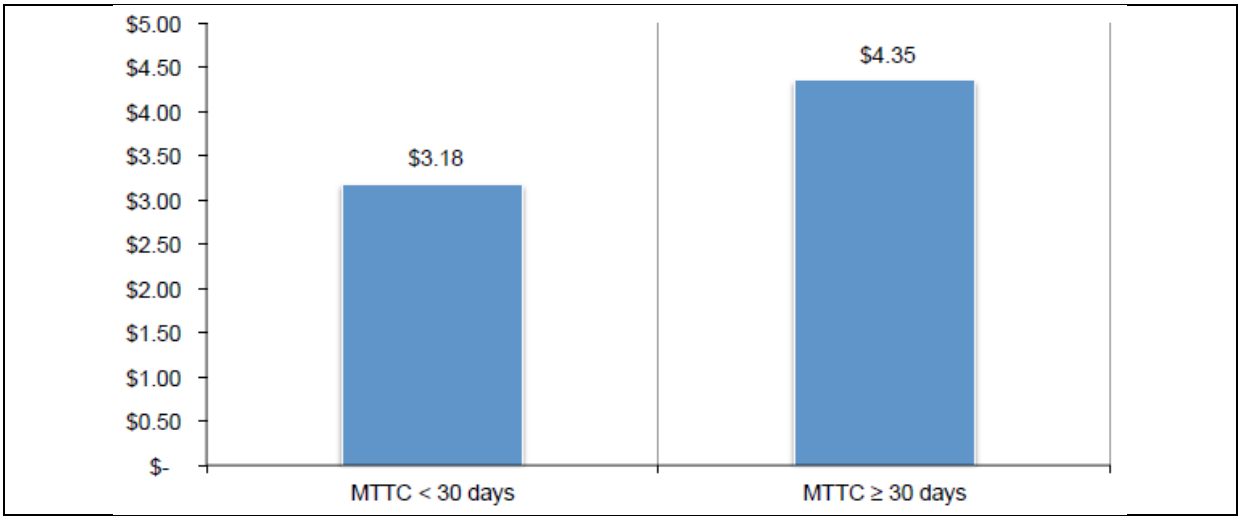


The longer the MTTI and the MTTC the higher the cost per data record lost.

MTTI and Total Average Cost (US$ millions)

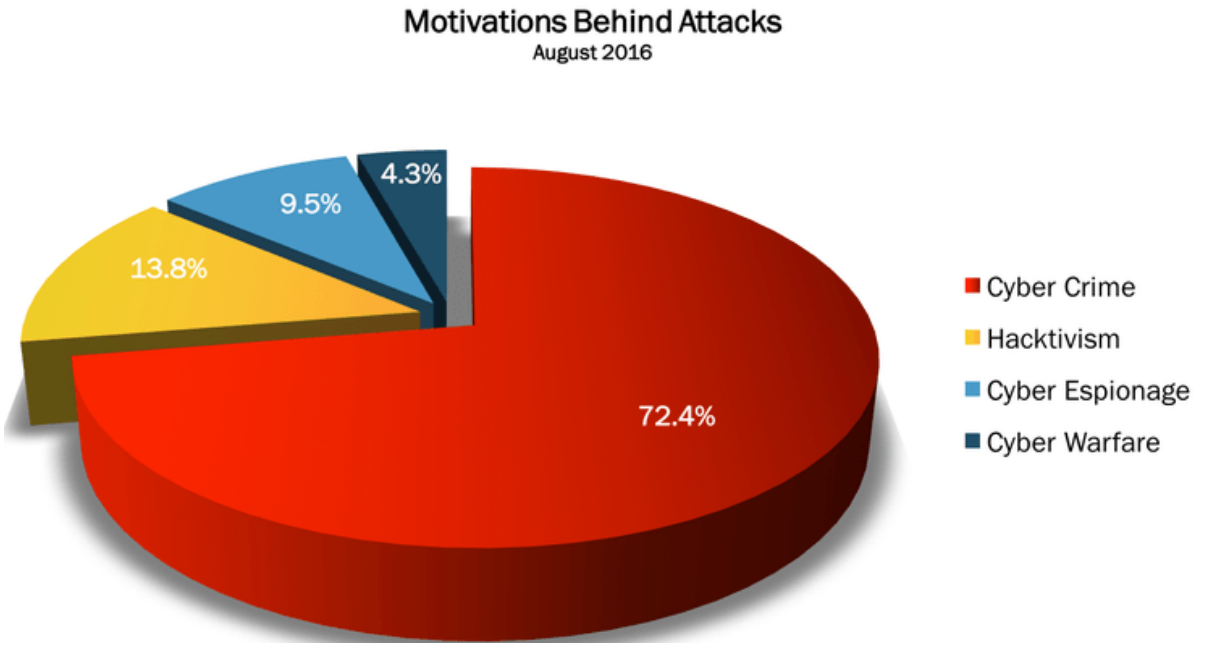


MTTC and Total Average Cost (US$ millions)

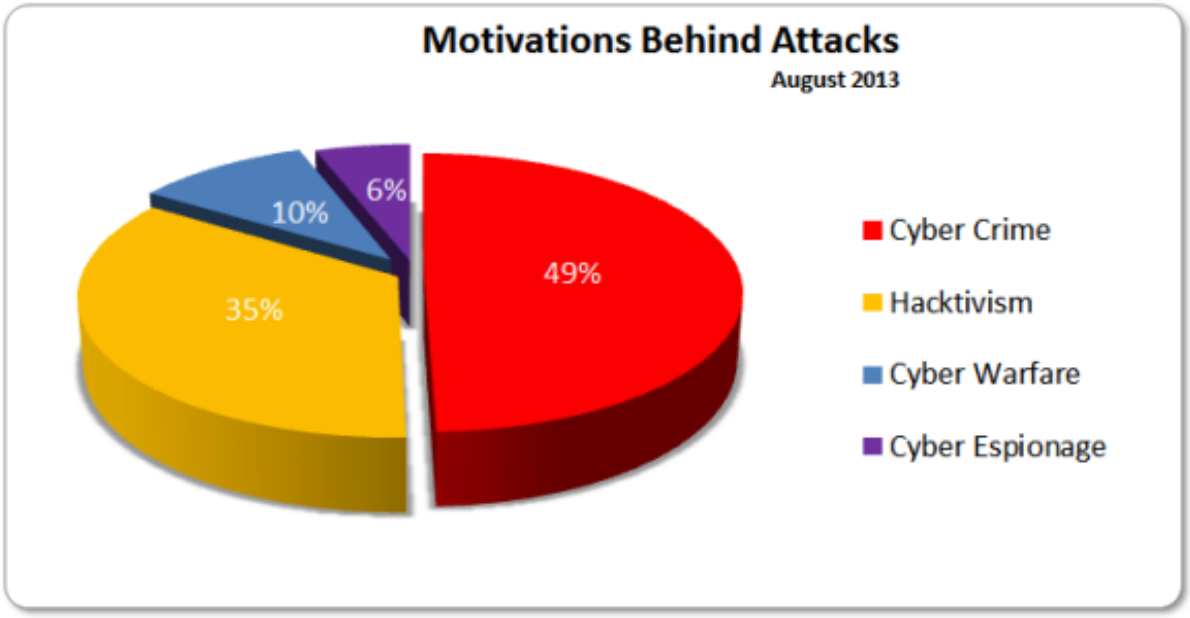


Source: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

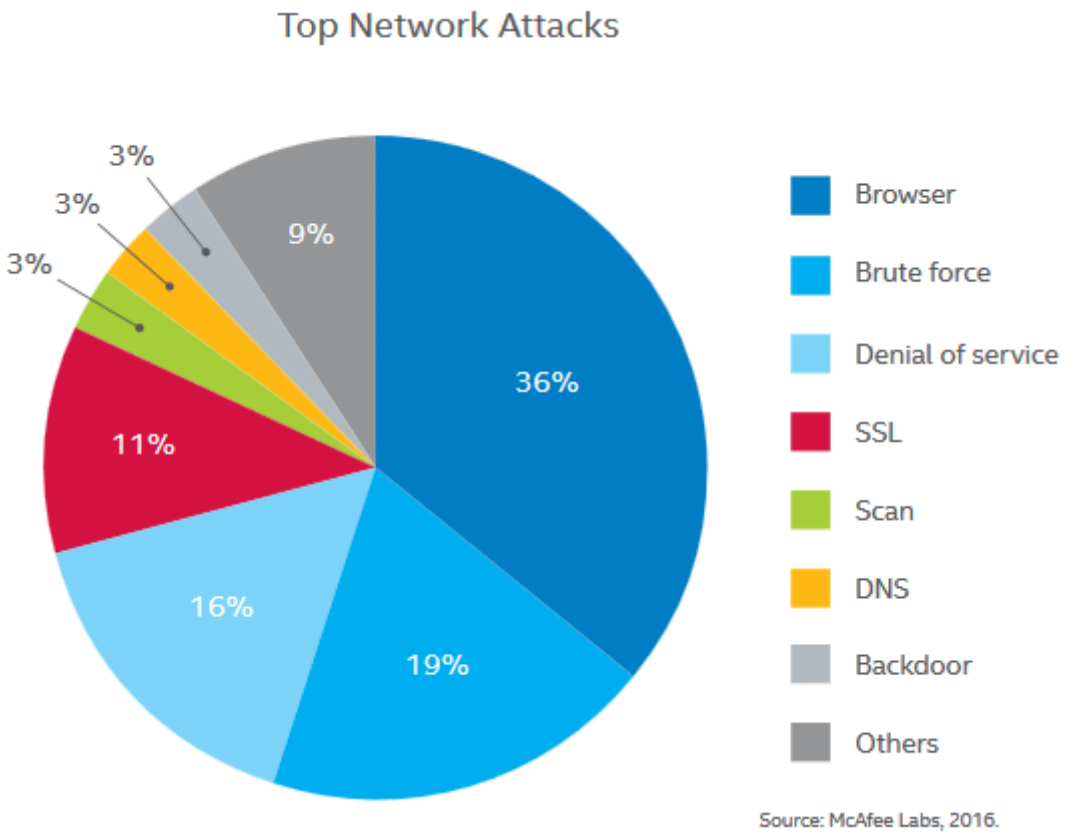
The Cybersecurity November 2013 Briefing Paper carried estimates by Hackmageddon of the motives driving malicious hacks. Below we see that by 2016, cybercrime has jumped from under 50% to over 70% of the recorded attacks. And somewhat alarmingly, cyber espionage has increased from 6% to 9.5% and cyber warfare has decreased from 10% to 4.3%, respectively. Hactivism, active as it is, is now squeezed down to under 14% from 35%.



Source: http://hackmageddon.com/category/security/cyber-attacks-statistics/

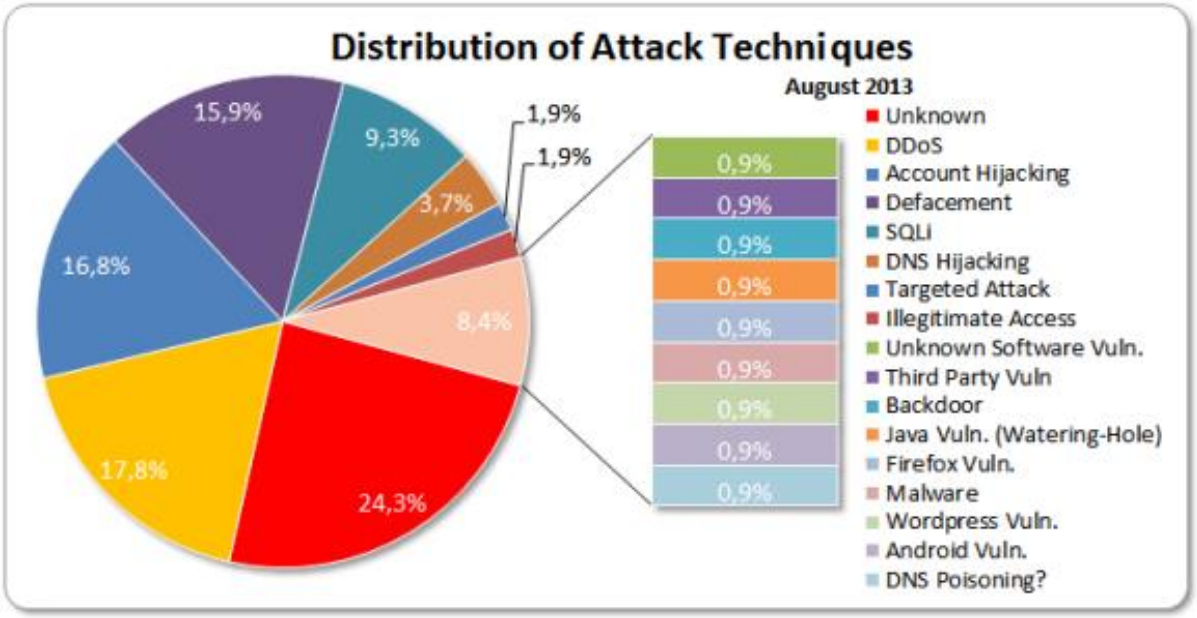


Hackmageddon does not provide comparable data for the destruction of attack techniques for 2016, but a McAfee Labs *Threats Report* does.[12]



Source: http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2016.pdf

[12] McAfee Labs *Threats Report* March 2016 http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2016.pdf

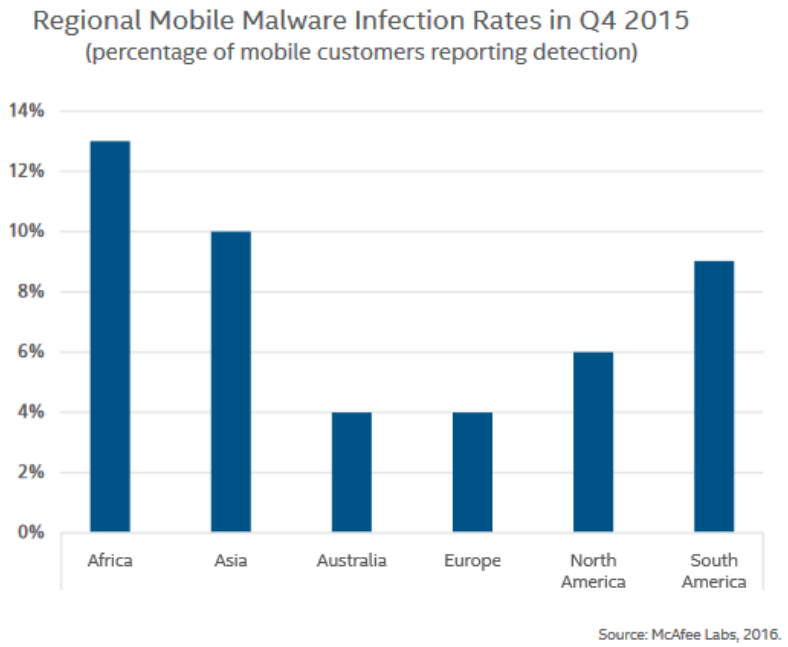


Source: Cybersecurity November 2013

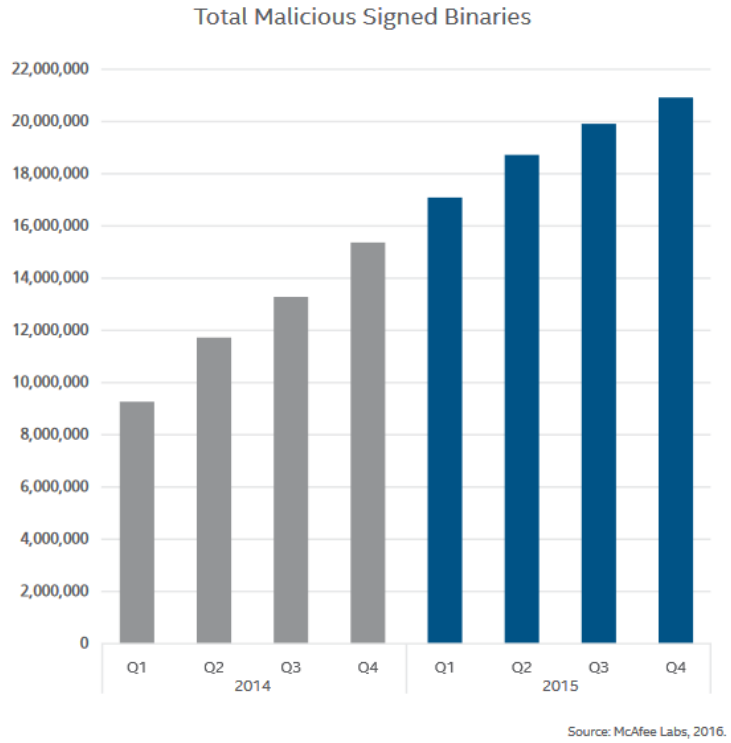
Given the humongous nature of recent DDoS attacks (see above) it is interesting to note this does not necessarily mean that the incidence of DDoS is on the increase, but the severity certainly is. For instance, Akamai's State of the internet Security report for Q2 2016 found that DDoS had increased by 129% over Q2 2015, but by only 9% over Q1 2016. However, the means by which DDoS attacks are launched have widened in recent years. The use of bots to take over DNS (Domain Name System) servers now includes NTP (Network Time Protocol). NTP "is a distributed network clock time synchronization protocol that is used to synchronize computer clock times in a network of computers and runs over port 123 UDP. *NTP is one of those set-it-and-forget-it protocols that is configured once and most network administrators don't worry about it after that. Unfortunately, that means it is also not a service that is upgraded often,* leaving it vulnerable to these reflection attacks."[13] See above Lauri Love's comments on parts of the system that are not up to scratch.

Since the advent of smartphones, mobile communications have become an intricate part of doing business, from m-banking to m-commerce to BYOD at work to the use of smart devices in the services sector, etc. In consequence, the use of malware to access data and intercept passwords has grown significantly. The Internet-of-Things will bring about exponential growth in this sector. The McAfee Report shows the regional distribution of malware infections on mobile devices. In Asia it has climbed to 10%.

[13] The Hacker News (2 January 2014) 'Abusing NTP to launch massive Reflection DDoS Attacks' http://thehackernews.com/2014/01/Network-Time-Protocol-Reflection-DDoS-Attack-Tool.html



A relatively new phenomenon is the rise of binary infections, one of which embeds itself into the phones operating system and the other sends out false messages, for example, to switch money between accounts without the customer being aware. The bar chart from McAfee shows the number of binary malware grew between the start of 2014 to the end of 2015 from under 10 million to over 20 million globally. This is the new frontier of both the Wild West and the Wild East.



Source: http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2016.pdf

Ransomware, where data is encrypted by the unauthorized intruder, is another major trend. In the UK, it is "increasing 259% in the last five months alone" according to one security analyst.[14] 23 out of 58 universities in Britain have been victims of ransomware, while 28 National Health Service Trusts (NHTs) admitted being victims, only 1 claimed not to have been, and 31 declined to comment on the grounds of patient records confidentiality.[15] Ransomware now comes in easily managed packages, ready to install. Many of the ransoms are for small sums of money, tempting vulnerable small businesses in particular to pay to have their encrypted data unencrypted.

State

State players are involved in espionage and cyber-warfare, and the innovations and techniques are breaking all norms. On the defensive side of the picture are issues such as protection of a nation's critical infrastructure, to law enforcement against child abuse and online hate, to terrorism and protection of national security systems. On the offensive side are espionage and cyber warfare. It goes without saying that all states with the cyber-capability will use it to some degree, and those without it try to achieve it.

It is in the nature of politics that citizens of any nation learn more about the antics of competing nations than they do of their own. The control of information even, especially in a cyber age remains vital to the power of the powerful. Citizens of the West know more about the espionage and cyber warfare of China and Russia than they do of their own governments, and vice-versa. At the state level this is all about state-craft. For example, after the US and Chinese governments came to an arrangement to haul back on cyber-attacks, the *Wall Street Journal* reported that "Hackers operating out of China were linked to between 50 and 70 incidents that the cybersecurity firm Fire-Eye Inc. was investigating on a monthly basis in 2013 and the early part of 2014.... Starting October 2015, however, this tally dropped below 10 incidents and hasn't recovered..." (*Wall Street Journal*, 'Chinese Hacking Activity Appears to Be Declining' 22 June 2016).

China is interesting in this regard because while hacking activities in Asia Pacific are ramping up due to its contested claims on the South China Sea, domestically it seems to be welcoming the participation of international software vendors and cloud service providers in its cybersecurity policy development.[16] Microsoft, Intel, Cisco and IBM are among those invited to attend the Technical Committee 260. In a parallel development, Microsoft and Huawei have joined forces in a "buyers guide" to allay fears that foreign IT poses threats to

[14] The Guardian (3 August 2016) 'Ransomware threat on the rise as 'almost 40% of businesses attacked' https://www.theguardian.com/technology/2016/aug/03/ransomware-threat-on-the-rise-as-40-of-businesses-attacked

[15] Information Age (24 August 2016) 'Ransomware on the rise' http://www.information-age.com/ransomware-on-the-rise-123462256/

[16] Wall Street Journal (26 August 2016) 'China Sets New Tone in Drafting Cybersecurity Rules' http://www.wsj.com/articles/china-moves-to-ease-foreign-concerns-on-cybersecurity-controls-1472132575

cybersecurity.[17] The challenge they face is scepticism that the intelligence agencies of both countries could pass up an opportunity to install spyware into each other's communications networks.

If China's strong card is patience, Russia's lies in chess. Keeping the other side guessing, and shaping their perceptions (rightly or falsely) is known as 'reflective control' which might be best thought of as a stratagem in game theory. It often involves 'false flagging' by using non-state proxy agents. In its confrontation with the government of the Ukraine, it is widely believed that Russia took down the power grid on 23 December 2015. One security expert suggests the operation probably involved a combination of cybercriminals and the state rather than just the state.[18] But most intriguing is the use of Regin malware, reportedly widely used by both Russia and the USA to hack into telecom network, hotel systems and businesses. It is generally assumed Russia used this to hack into the Democratic National Committee in July 2016. On the US side, it was reported that the US-Israel invented malware Stuxnet was used to destroy maybe up to one-fifth of Iran's nuclear centrifuges. According to Kaspersky Labs, this zero-day attack had all the hallmarks of the Equation Group which has close ties with the US National Security Agency. To round off this narrative worthy of the author John le Carré, a shadowy group calling itself The Shadow Boxers in August 2016 announced on Twitter that it would auction off a US$500 million a treasure trove of cyber weapons which were reportedly developed by the Equation Group. Russian spies? Sending a message? The name Shadow Boxers seems highly appropriate.[19]

If there is solace in any of this, it just might just be that cyberwarfare will be less *totally* destructive than nuclear-thermal warfare. But maybe not if you happen to be on a dialysis machine at the time.

Singapore

In more ways than one Singapore is the exemplary state when it comes to cybersecurity. A Cyber Security Agency (CSA)[20] has been established at the highest level, as part of the Prime Minister's Office and managed by the Ministry of Communications and Information. Its remit covers overseeing cyber security strategy, education and outreach, and industry development. The CSA is a precursor of a Cyber Security Act to be introduced in 2017 which broadly will cover protection of critical information infrastructure, and to manage and

[17] Wall Street Journal (13 September 2016) 'Microsoft, Huawei Join in Cybersecurity Message' http://www.wsj.com/articles/microsoft-huawei-join-in-cybersecurity-message-1473757469

[18] Wired (3 March 2016) 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid' https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[19] Financial Times (20 August 2016) 'Cyber espionage: A new cold war?' https://www.ft.com/content/d63c5b3a-65ff-11e6-a08a-c7ac04ef00aa; Wikipedia (accessed 3 October 2016) *Stuxnet* https://en.wikipedia.org/wiki/Stuxnet; New York Tines (16 February 2016) 'U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict'http://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html

[20] Cyber Security Agency https://www.csa.gov.sg/

report and raise standards of cybersecurity providers.[21] In 2014 a National Cybersecurity R&D Laboratory at the National University of Singapore (NUS) was announced to undertake cybersecurity research and development in collaboration with industry or international partners. Private sector vendors are working closely with government and universities to establish research labs as cybersecurity is seen as a growth sector.

And yet, Singapore is pursuing the vision of a Smart Nation with the Internet-of-Things and a heterogeneous network (HetNet) providing universal connectivity on-the-go. As seen above, the Internet-of-Things can so easily become the Internet-of-Thieves. The key weakness of the Internet-of-Things is that manufacturers, for obvious commercial reasons, design the equipment to be plug-and-play, so the equipment is marketed with factory-setting passwords. There is nothing to edge households towards encrypting their webcams or to use complex passwords. A smart nation could become a place for smart cyber criminals using bots to controls hundreds of thousands Internet-of-Things with ease.

But Singapore has decided upon one sensible step forward. To disconnect the working devices of civil servants from the Internet. It sounds draconian, but the reality is that *anything* connected to the Internet is vulnerable. This does not imply that everyone should disconnect. Driving a car is a risk, but one we all take. For most purposes, the losses of being unconnected would quickly outweigh the gains. What is required to reduce risk is awareness and a change in behaviour, taking sensible precautions, such as having back-ups and anti-malware software installed. But to have a dual system, one that is connected and one that is not is a sensible solution for very high value assets. A connected system can download the required materials, have them scanned for bugs, and once sanitized they can be fed into the secure unconnected system. A similar reverse process can also take place. It sounds laborious and there will be an administrative cost, no question about that. The solution is not perfect. To hermetically seal off one system entirely will prove a challenge. But if the value of the assets being protected is sufficiently high, then it's a price to be paid. How wide ranging those assets will prove to be will be the policy challenge. But that is the world of cybersecurity we are living in.

[21] Channel New Asia (11 April 2016) 'New Cybersecurity Act to be tabled in 2017: Yaacob Ibrahim' http://www.channelnewsasia.com/news/singapore/new-cybersecurity-act-to/2685052.html