To what extent is the cyber insurance marketplace responsible for the growth of Global ransomware?

Word Count – 4,489

Contents List:

Introduction:

I have chosen to research and write about this topic as a cyber underwriter myself, working for a leading cyber insurance carrier in the City of London, this is a topic pertinent to my own professional development and of a particular interest to me personally as I think about the development of this Global threat. I believe this is an important topic for the cyber insurance marketplace as a whole and a question that needs addressing in the very near future by regulators and Government bodies, I will assess the arguments both for and against the question and present my own thoughts and conclusions along the way. It must be noted that a large proportion of the research undertaken when writing this dissertation has been based online, as access to libraries has been restricted due to Covid -19, every effort has been taken to use credible and scholarly online sources to support my research and conclusions.

The proliferation of the internet across every facet of our day to day lives over the last twenty to thirty years has been remarkable; from the world of work and instant communications, to logistics & supply chains, healthcare & travel, virtually every aspect of every modern business uses the internet. Many modern businesses are in-deed entirely dependent on technology and access to the internet to function. Connected systems allow many business to provide in many cases the entirety of their services, whether this be in the form of cloud computing services or simply access to customers – the internet and consistent and safe access to it is key. It is the growing dependency of almost all businesses to access their systems and remain connected to the internet which means that protecting this access and ensuring system uptime must be the foremost risk consideration for risk managers and commercial insurance buyers around the World. Such universal 'system dependency' and the threat of not being able to access the internet and connected systems has given rise to the cyber insurance market and the risk transfer solutions and incident response capability now available.

In 2018 PriceWaterhouseCoopers, (PWC) released a report stating that, 'the US stand-alone cyber insurance market was estimated to be at $2.5 - $3.5 billion annually, with expectations to grow by another $2 billion over the next three years.'[1] Standalone cyber insurance, has without doubt been one of the fastest growing lines of business in recent years with gross written premiums estimated to have grown around '30% year on year since 2016'[2]. At the same time the coverage has expanded, incident response capability improved and insurers ability to underwrite, model and articulate the risk greatly improved.

In 2016 the Federal Bureau of Investigation, (FBI) released a report stating that incidents of Global ransomware were on the rise, with, 'ransomware attacks not only proliferating, they're becoming more sophisticated.'[3] Fast forward to 2019 and the FBI received over '460,000 complaints and estimated over $3.5 billion in costs across all instances of cyber crime and ransomware'.[4] The FBI statistics show a trebling in costs associated with ransomware since 2016 and a doubling of reported incidents. There is no doubt that as modern businesses have become ever more dependent on technology and connected by every means possible to the internet that the prevalence and cost of ransomware has increased substantially. This essay will attempt to determine to what extent it may be true that cyber insurers are responsible for the growth of ransomware around the World as is often suggested, or was growth of this twenty first century crime inevitable given near universal dependency on connected systems and their prevalence around the World.

<u>The overall growth of the cyber insurance marketplace:</u>

There is no question that the cyber insurance market has grown enormously over the last few years and clearly the frequency and severity of ransomware events has grown alongside it, what is also interesting to note is the corresponding growth in ransom

---

[1] PWC, *Are insurers adequately balancing risk & opportunity? Findings from PwC's global cyber insurance survey,* https://www.pwc.com/us/en/industry/assets/pwc-cyber-insurance-survey.pdf

[2] EY, *2020 Global Insurance Outlook,* https://www.ey.com/Publication/vwLUAssets/Insurance_outlook/$FILE/ey-global-insurance-outlook.pdf

[3] FBI, (29th April 2016), *Incidents of Ransomware on the Rise, Protect Yourself and Your Organization,* https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise

[4] FBI (February 11th 2020), *Internet Crime Complaint Center* 2019 Internet Crime Report, https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2019-internet-crime-report

demands over the last few years and to a lesser extent the types of business and organisations being impacted by ransomware. The growth of both ransom demands and ultimately their timely payment may well point to the increasing role that cyber insurance plays in promulgating this Global threat.

Ransomware is a type of malware used by malicious threat actors around the World, with the threat to publish sensitive data or perpetually prevent access to systems. For many business not being able to access their systems or the threat of publishing the sensitive data they hold could have enormous implications. It is not just SME business that face this threat, malicious threat actors are prepared to target any and all types of organisation. In-deed it is often the most public organisations which make for the most lucrative targets, as is highlighted by Riviera Beach City, Florida whose councillors unanimously agreed to pay '$600,000 to regain access to their systems following a ransomware attack in 2019' [5]. This particular instance is a relative anomaly in terms of size, most business, if un-insured for the threat are unlikely to have such cash reserves available to make a ransom payment. Aside from the size of the ransom, what is most interesting is the actual propensity to pay the ransom itself, in this case and many of the thousands of un-reported 'successful' ransomware attacks that have taken place over the last few years. 'In 2017, just 39% of organizations hit by ransomware paid to retrieve their encrypted data. That figure rose to 45% in 2018, then shot up to 58% in 2019'[6]. The question is why would businesses become more willing to pay ransoms over the last two years, after all ransoms aren't getting smaller. It is true that business are more dependent on their systems than ever before, but this doesn't adequately answer why such a larger jump in two years, in my opinion. I believe the growth of ransomware attacks, has led to the growth of and increasing penetration rates of cyber insurance, which has led to the growth of services and sophistication of cyber insurers in being able to efficiently pay ransoms to criminals, which has led to more 'successful ransomware attacks' in a somewhat self-perpetuating circle.

---

5 Forbes.com (June 20th, 2019), Florida City Agrees To Astonishing $600,000 Ransom Payout, https://www.forbes.com/sites/kateoflahertyuk/2019/06/20/florida-city-agrees-to-astonishing-600000-ransom-payout/#3ace51352ac6

6 Infosecurity Group, (1st April, 2020), Ransomware payments on the rise, https://www.infosecurity-magazine.com/news/rise-in-ransomware-payments/

The simple dynamic of more insurance, equates to more ransoms and ransomware isn't true, as is the case with the traditional kidnap and ransom market. However the case is certainly true, I believe that an ever more sophisticated cyber insurance market and the ease and profitability of propagating cyber crime certainly do go hand in hand.

The increasing sophistication of the cyber insurance marketplace:

Almost all true standalone cyber insurance policies will include cover for extortion, being the costs associated with ransom demands following a ransomware attack as well as other costs associated with the cyber event. The propensity and willingness for a business who has bought cyber insurance to pay a ransom regardless of who it is to, in order to restore access to their systems, knowing that the insurers will pay the bulk of the cost must be far greater than for those business who are un-insured against cyber events. It is not only the fact that the event itself is insurable that is attractive, it is the speed and sophistication in which the payments are made and facilitated which is of great importance here too. Most ransomware attacks often have a time sensitivity attached to them, aside from the obvious inability to access systems, ransoms are often coupled with the threat to release or delete sensitive data if payments aren't made within a certain (often tight) timeframe which can have a catastrophic impact on businesses.

Ransom demands of this nature are almost never made in traditional fiat currencies, they are almost always demanded in bitcoins. The relative anonymity of cryptocurrencies and the ability to bypass the traditional banking system makes the use of cryptocurrency wide spread and the de-facto currency for dark web criminality. I will focus on bitcoins and the transaction process specifically, to highlight the point, that the increasing sophistication of the cyber insurance market and its growing ability to seamlessly transact with cyber criminals is one of the key reasons why a case can me made that cyber insurance propagates ransomware. It is the ease of payment to cyber criminals which I believe has really fuelled this issue, in the same way that kidnap and ransom insurance buys you access to extraction and negotiating specialists, cyber insurance buys you access to bitcoins and also negotiating specialists. Most business who don't buy cyber insurance, will not be able to quickly or easily procure the required amounts of cryptocurrencies to facilitate a payment to cyber criminals when demanded to do so, much less be willing or able to negotiate with

the criminals. Business who are insured against these perils, will be able to hand over the handling of the situation in its entirety to cyber insurers and the specialist 3rd party partners they work with. In-deed it is the marketplace of 3rd party partners that work with cyber insurers who really are fuelling the growth of ransom payments. It is these 3rd parties who specialise in being able to access cryptocurrencies with ease, negotiate with the criminals and ultimately work with the criminals to decrypt and restore an insureds systems. It is the cyber insurance proposition that brings all of this together for their clients who suffer these attacks. Cyber insurers and their 3rd party partners have made it easy to transact effectively with these criminals, who in turn know how easy and profitable it is to transact with the insurers and their 3rd parties. Not regarding any other aspects of cyber insurance or cyber criminality, it is clear in my opinion that cyber insurers have certainly helped facilitate and 'grease the wheels' of these types of criminal transactions and make it supremely easy to take place.

<u>The importance of the cyber insurance marketplace:</u>

It should not be underestimated however, the importance of being able to deliver these services, for a relatively nascent line of insurance the speed at which the cyber insurance market must adapt to keep up with an ever changing and perennially sophisticated criminal opponent is astonishing. It must be pointed out that ransomware in itself is not a new concept, 'crypto-virology and the concept of ransomware has been around since, the first widespread adoption of the internet itself during the mid 1990s'[7]. It is firmly my opinion that ransomware would exist regardless of whether there was insurance available to protect against it. In-deed since the mid 1990's the world of work has been transformed immeasurably by technology, as I have mentioned most modern business are entirely dependent on the internet and its availability to function. Extortion in itself is a concept as old as time, we are merely seeing the growth of 21st century extortion and the reaction from risk taking underwriters to be able to protect their clients against it.

[7] Cacm.org, (July 2017), Cryptovirology: The Birth, Neglect, and Explosion of Ransomware, https://cacm.acm.org/magazines/2017/7/218875-cryptovirology/fulltext

Recent Global ransomware 'outbreaks' such as the Wannacry event impacting the 'NHS amongst other entities around the World in 2017'[8] shows how widescale and potentially damaging cyber events can be. In fact 'The Economist' stated in 2017 that, 'data and not oil was now the most valuable resource in the World'[9]. It stands to reason therefore that there would be a sophisticated and widely adopted cyber insurance marketplace, in-deed the threat of a cyber event being perpetrated against a modern business is now, 'fifteen times more likely than that business suffering a theft or fire' according to a report authored by the insurer Hiscox and distributed by the Insurance Insider[10]. Therefore whilst there is a correlation between the propensity to pay a ransom and deliver a 'successful' attack for the criminals, this is a very real and very potent threat faced by business around the World and on a daily basis. The fact that the cyber insurance market is able to facilitate payments and restore a business to full functionality means that thousands of business are saved from the threat of losing their most valuable resource. The alternative proposition of not having the cyber insurance marketplace available or leaving your most valuable resource un-insured is un-thinkable. Whilst the correlation between making ransom payments and the growth of ransomware is clear, the cyber insurance market is also responsible for keeping affected businesses in business and there is little evidence to suggest that without the cyber insurance marketplace ransomware or extortion would disappear. In-deed the recent coronavirus outbreak has shown how much more reliant modern businesses are on technology than they may even have considered previously, and this is unlikely to change.

Penetration of cyber insurance remains low:

Whilst the arguments for cyber insurance being a major contributing factor for the growth of Global ransomware attacks are clear, I will now examine the reasons why twenty first century criminality and the growth of ransomware may well be happening independently of the cyber insurance market and certainly is not limited to growing in line

[8] BBC News, (13th May 2017), Massive ransomware infection hits computers in 99 countries, https://www.bbc.co.uk/news/technology-39901382

[9] The Economist, (6th May 2017), The world's most valuable resource is no longer oil, but data, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[10] Hiscox Cyber Readiness Report, (22nd June 2020), One in six firms pays up ransoms to hackers, finds survey, https://www.insider.co.uk/news/one-six-firms-pays-up-22230266

with the insurance market. Despite the plethora of journalism written over the last five years or so about the potential growth of the cyber insurance market; whilst growth has been strong overall, gross written premium and overall penetration rates remain relatively low. By comparison to the Global property and casualty market, which accounts for '$1.6 trillion in premium',[11]as we've discussed already the nascent cyber insurance market is still only $3.5 billion in premium. In-deed Airmic (the Association of Insurance and Risk Managers in Industry and Commerce) reported recently that 'cyber and IT related risks have emerged as the top concerns for members', 'with 43% of respondents stating cyber-risk as their top concern.'[12] Clearly the risk of ransomware exists and clearly risk managers are aware of the threat their businesses face. It is interesting therefore that the size of the cyber insurance market alone would show us there is very little correlation to be drawn between the size of the cyber insurance marketplace and the growth of ransomware, clearly the growth of ransomware is happening independently and being driven by a multitude of factors and not the growth of cyber insurance alone.

The majority of ransomware is propagated through innocent user interactions such as clicking on a malicious link on a phishing email or inadvertently visiting a compromised website. Virtually all ransomware events, especially the vast majority of ransomware events that impact the traditional SME cyber insured are opportunistic and disseminated through indiscriminate means. It is actually very rare that malicious threat actors specifically target victims. I believe it is this important dynamic that also points to the growth of ransomware being totally separate to the growth of the cyber insurance marketplace. In-deed the growth, proliferation and likelihood of being impacted by ransomware is so indiscriminate, absolutely no correlation can be made between the likelihood of being impacted compared to having bought a cyber insurance policy. There is no way for malicious threat actors to know which businesses are buying cyber insurance or not in the first instance and the indiscriminate nature of ransomware attacks shows this cannot be an important factor for hackers when determining their attacks. In the same vein it is the indiscriminate nature of these attacks, the ease with which these attacks can take place and the un-imaginably large

[11] McKinsey & Company, (April 20200, State of property & casualty insurance 2020, https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/state%20of%20property%20and%20casualty%20insurance%202020/state-of-property-and-casualty-insurance-2020.ashx

[12] Airmic, (11th June, 2020), Cyber-risks moves to the forefront of risk manager concerns, https://www.airmic.com/news/press/cyber-risk-moves-forefront-risk-manager-concerns-airmic-member-survey

amount of potential targets that can be hit in any one go that is fuelling the growth of ransomware, not the insurance which protects businesses against the attacks.

Ransomware as a service:

Similar to my above argument, I believe another key reason for the growth of ransomware independent from the growth of the cyber insurance market, is quite simply the ease of being able to launch a ransomware attack. The vast and anonymised profits and most importantly, as I mentioned above the virtually infinite number of potential targets open to a malicious threat actor. Examining some of these points individually will help to show why the growth of ransomware continues to be so large over the past few years. Ransomware is software, like any type of software that one can typically buy from a licensed vendor for a specific purpose. In-deed the same concept applies to ransomware, which can be bought and sold relatively freely over the dark web. RaaS (Ransomware as a service) not to be confused with SaaS (Software as a service) is not a new thing, however the threat it poses has become more vicious and harmful. 'This model is so enticing to some cyber criminals that you can see the RaaS provider's advertisements on the dark web'[13] The availability of this malicious software to be bought and sold as easily as any other type of retail product on the web, means anyone can become a cyber criminal if they so wanted. The anonymity of the dark web, and payment processing also makes this an extremely attractive proposition from those willing to sell the software, to those willing to perform the attacks. The possibility of an insurer paying the ransom must play little on the minds of these criminals.

The concept of anonymity that is afforded by not only the dark web, but by the use of cryptocurrencies in fuelling this type of crime has also hugely advanced this burgeoning twenty first century criminality. In-deed without the anonymity of the dark web and availability of non-fiat and de-centralised currencies, ransomware and certainly ransomware as a service could not work as concept. Anonymity and de-centralised crypto-currencies are likely to be of much greater importance to the growth of ransomware in itself than the

[13] Tripwire.com, (May 16th 2018), Ransomware-as-a-service (RaaS): how it works, https://www.tripwire.com/state-of-security/security-data-protection/ransomware-service-raas-works/

growth of the cyber insurance marketplace could ever be. Crypto-currencies and their phenomenal growth in popularity and use over the last few years has certainly fuelled cyber crime and ransomware in a much more meaningful way than insurers have. However as I mentioned previously the cyber insurance market place must take some credit for being able to successfully navigate this murky world with ever increasing sophistication, as a service to those facing the criminal threat. Going hand in hand with the anonymity, and the vast potential for profit making is also the growing number of people with the necessary skills to become cyber criminals. The widespread adoption of the World Wide Web around the world means that any one with access can take part in this criminal venture with anonymity. The unequal Global distribution of jobs means that in some parts of the World the easiest and most profitable means of criminality are cyber related. In-deed the 2017 WannaCry ransomware attack that impacted the UK's NHS was believed to have originated from North Korea, a country cut-off and heavily sanctioned by the International community, where the availability of young, highly talented and highly motivated cyber criminals is high[14]. There is no doubt that all of these factors coming together in unison have helped develop and propel the growth of ransomware collectively over the last few years, in a much more meaningful way than simply the growth of the cyber insurance marketplace has done.

Twenty first century crime:

My final argument against the fact that the cyber insurance market place is responsible for the growth of ransomware is the fact that, cyber crime generally and ransomware being a major aspect of it is surging, whilst traditional forms of crime area decreasing. Whilst the World has become more technologically advanced, so have enterprising criminals. There is a direct correlation to be drawn between the decreasing frequencies of traditional bank robberies and the growth of ransomware and cyber criminality. Even back in 2013, Cable News Network (CNN) reported that, 'bank robbers don't rob banks anymore, they don't need guns, and they don't wear masks. Instead they hide behind their computer screens and cover their digital tracks'[15]. Its safe to say that we

[14] BBC.com (16th June 2017), NHS cyber-attack was 'launched from North Korea', https://www.bbc.co.uk/news/technology-40297493
[15] CNN.com, (July 9th 2020), Cyberattacks are the bank robberies of the future, https://money.cnn.com/2013/07/09/technology/security/cybercrime-bank-robberies/

are now in that future World. The prevalence of technology has allowed the darker elements of human nature to come to the fore in the shape of cyber criminals, who's livelihoods are now safer, more anonymised and more profitable than their traditional criminal counterparts.

It would be unfair I believe to draw a parallel between the growth of the cyber insurance market and the growth of cyber crime in general, its seems inevitable to me that the growth of cyber crime and ransomware would have happened as traditional forms of crime become more and more unattractive. Conversely, I believe the cyber insurance market place actually plays a crucial role in helping to combat this type of crime and ransomware. In a similar vein to traditional crime insurers being able to require their insured's physical premises to invest in the best alarms and physical security, cyber insurers are able to work with their insureds to ensure the best computer and network security to combat the threat of ransomware. The cyber insurance marketplace is well placed as a nascent market to be able to develop into providing comprehensive risk management services and incident response capabilities, in-deed the very best cyber insurers at the moment are focussing their efforts on this front. Whilst non-traditional crime continues to grow, and I believe there is no reversing this trend, it is up to the cyber insurers and their marketplace to be able to provide the effective means to combat against this growth and at the same time provide a meaningful risk transfer solution to their clients. The role of the cyber insurance marketplace in helping to slowdown the growth of cyber criminals is huge and I believe this is where the cyber insurance marketplace will really be able to show its value. It is clear in my mind that the growth of non-traditional crime and ransomware in particular are inevitable and will continue to grow as the World becomes ever more connected and the means to propagate this type of crime becomes ever easier and more profitable and the developing cyber insurance marketplace is a consequence of this new World.

Conclusion:

I have endeavoured to present a balanced set of arguments to the question of whether cyber insurance is responsible for the growth of ransomware, I believe the cyber insurance marketplace is still relatively nascent though. Whilst conclusions can be made at

this early stage, it must be remembered that this is a fast changing and ultra modern concept and the cyber insurance marketplace is largely playing catchup to this Global threat. There is no doubt in my mind after carefully considering the arguments for and against that ransomware as a concept would have emerged regardless of whether the cyber insurance marketplace existed, the fact that the threat has risen over the last few years, is largely down to the greed and success of the first wave of cyber criminals, more than the fact that an insurance policy now exists to help business impacted by this threat.

I believe the concept of cyber insurers creating efficiencies around payment of ransoms, creating relationships with cyber criminals and ultimately facilitating the payment of ransoms has helped make ransomware even more successful and profitable and is likely to have fuelled its success in part. I do believe this raises another important question about the willingness of cyber insurers to pay criminals though. The payment of ransoms to anonymous criminals is a very dangerous precedent and one which needs careful consideration from regulatory bodies and in-deed respective Government bodies. As I have shown there is evidence to show that ransoms are getting larger and cyber insurers are getting better at paying them, which is a very dangerous concept if left un-checked and likely not a sustainable model for insurers or in-deed the business community to pursue.

However it must not be forgotten that in this nascent market, cyber insurers are simply providing the service they have offered to their clients, this is no different to kidnap and ransom insurance or in-deed traditional crime insurance. It is too easy to suggest that cyber insurers themselves are responsible for the growth of ransomware and cyber crime, I believe that the cyber insurance market place actually has a much more important and meaningful role to play in helping combat the threat of ransomware and cyber crime. Cyber insurers are uniquely placed to be able to gather huge amounts of data relating to their insureds, much of this information is readily available and I believe the best cyber insurers ought to be providing pro-active risk management services to their clients to help prevent the spread of ransomware, rather than simply indemnify the client when they're impacted. At the same time I believe law enforcement agencies and Government bodies need to find a way to be able to regulate the dark web marketplace that truly enables this crime. The relatively anonymous nature of this crime and the vast profits that can quickly be made

means that this type of crime will continue to surge and the cyber insurance marketplace will continue to grow as result.

It is the un-checked movement of legitimate funds into the hands of anonymous criminals that must be stopped to be able to bring a slowdown of ransomware and cyber-crime, whilst insurers are certainly responsible for helping to facilitate these payments, this is not the sole contributing factor to the growth of ransomware. In my opinion the cyber insurance market place provides a valuable service and means to effectively combat the growth of ransomware, that so far no Government or Law enforcement agency has been able to legislate against. I believe the growth or the cyber insurance marketplace will actually be predicated on its continued ability to prevent the growth of ransomware and I believe this is an exciting industry to be involved in, particularly in helping to define the future trajectory of the cyber insurance marketplace and how effectively we as insurers can combat this crime.

Bibliography:

1. PWC, *Are insurers adequately balancing risk & opportunity? Findings from PwC's global cyber insurance survey,* https://www.pwc.com/us/en/industry/assets/pwc-cyber-insurance-survey.pdf (website)

2. EY, *2020 Global Insurance Outlook,* https://www.ey.com/Publication/vwLUAssets/Insurance_outlook/$FILE/ey-global-insurance-outlook.pdf (website)

3. FBI, (29th April 2016), *Incidents of Ransomware on the Rise, Protect Yourself and Your Organization,* https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise (website)

4. FBI (February 11th 2020), *Internet Crime Complaint Center* 2019 Internet Crime Report, https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2019-internet-crime-report (website)

5. *Forbes.com (June 20th, 2019), Florida City Agrees To Astonishing $600,000 Ransom Payout,* https://www.forbes.com/sites/kateoflahertyuk/2019/06/20/florida-city-agrees-to-astonishing-600000-ransom-payout/#3ace51352ac6 (website)

6. *Infosecurity Group, (1st April, 2020), Ransomware payments on the rise, https://www.infosecurity-magazine.com/news/rise-in-ransomware-payments/* (website)

7. Cacm.org, (July 2017), Cryptovirology: The Birth, Neglect, and Explosion of Ransomware, https://cacm.acm.org/magazines/2017/7/218875-cryptovirology/fulltext (website)

8. BBC News, (13th May 2017), Massive ransomware infection hits computers in 99 countries, https://www.bbc.co.uk/news/technology-39901382 (website)

9. The Economist, (6th May 2017), The world's most valuable resource is no longer oil, but data, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (website)

10. Hiscox Cyber Readiness Report, (22nd June 2020), One in six firms pays up ransoms to hackers, finds survey, https://www.insider.co.uk/news/one-six-firms-pays-up-22230266 (website)

11. McKinsey & Company, (April 20200, State of property & casualty insurance 2020, https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/state%20of%20property%20and%20casualty%20insurance%202020/state-of-property-and-casualty-insurance-2020.ashx (website)

12. Airmic, (11th June, 2020), Cyber-risks moves to the forefront of risk manager concerns, https://www.airmic.com/news/press/cyber-risk-moves-forefront-risk-manager-concerns-airmic-member-survey (website)

13. Tripwire.com, (May 16th 2018), Ransomware-as-a-service (RaaS): how it works, https://www.tripwire.com/state-of-security/security-data-protection/ransomware-service-raas-works/ (website)

14. BBC.com (16th June 2017), NHS cyber-attack was 'launched from North Korea', https://www.bbc.co.uk/news/technology-40297493 (website)

15. CNN.com, (July 9th 2020), Cyberattacks are the bank robberies of the future, https://money.cnn.com/2013/07/09/technology/security/cybercrime-bank-robberies/ (website)