MILLIMAN WHITE PAPER

Modelling financial losses from a ransomware attack using a causal approach

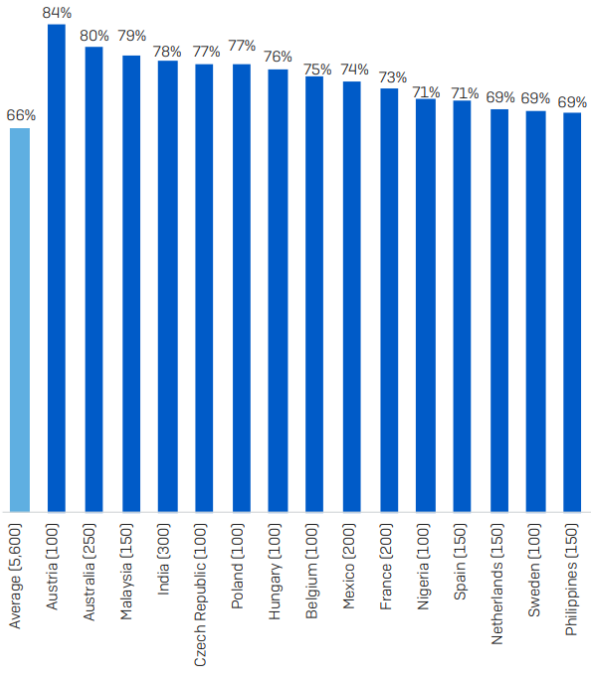
Chris Beck
Alexandre Boumezoued
Yousra Cherkaoui
Eliott Pradat
Blake Fleisher

With ransomware attacks on the rise all over the world, regulators are keeping a close eye on the reimbursement of ransoms by insurers. Given the evolving hacker behaviours and the uncertain nature of ransomware refunds by insurers, modelling the financial losses from a ransomware attack is most comprehensively done using a causal model approach. The modelling framework includes the ransom's reimbursement and the company's IT hygiene. The impact of the latter on the loss distribution is significant.

Ransomware attacks increased by 105% in 2021, targeting financial services firms, cities, universities and hospitals, among others.[1] In 2020, the US Federal Bureau of Investigation (FBI) received nearly 2,500 ransomware complaints, with losses exceeding USD 29 million.[2] The actual number of attacks and losses is expected to be much greater. In France, for instance, the governmental portal dedicated to cyberattack reporting received about 1,700 assistance requests in 2021 due to ransomware attacks, while the official numbers in France were only 260.[3] Ransomware attacks have long been underreported as companies are concerned about the reputational damage that could arise from a breach being made public. Organisations all around the world are concerned with these attacks, as shown in Figure 1.

Even tech companies are not spared. In early 2019, Altran experienced a ransomware attack, while the same happened to Sopra Steria at the end of 2020. In 2021, Toshiba TFIS acknowledged being attacked with DarkSide, the same ransomware that was involved in the attack against Colonial Pipeline.[3]

FIGURE 1: PERCENTAGE OF ORGANISATIONS VICTIMS OF RANSOMWARE [4]



Data sourced from VERIS Community Database

[1] Taylor, A. (17 February 2022). There's a huge surge in hackers holding data for ransom, and experts want everyone to take these steps. Fortune. Retrieved 12 July 2023 from https://fortune.com/2022/02/17/ransomware-attacks-surge-2021-report/#:~:text=Governments%20worldwide%20saw%20a%201%2C885,SonicWall%2C%20an%20internet%20cybersecurity%20company (subscription required).

[2] Congressional Research Service (5 October 2021). Ransomware and Federal Law: Cybercrime and Cybersecurity. Retrieved 12 July 2023 from https://crsreports.congress.gov/product/pdf/R/R46932?msclkid=2dde282ebb5811ecbdd822acab620866.

[3] Rieß-Marchive, Valéry (30 December 2021). France: These cyberattacks marked 2021. LeMagIT. Retrieved 12 July 2023 from https://www.lemagit.fr/actualites/252511499/France-ces-cyberattaques-qui-ont-marque-2021.

[4] Sophos. L'état des ransomwares 2022. Retrieved 12 July 2023 from https://assets.sophos.com/X24WTUEQ/at/5v9fhtkvjhsx3mt46nzspb/sophos-state-of-ransomware-2022-wpfr.pdf.

To pay or not to pay

As institutions around the world succumb to these breaches, they are faced with the age-old question: "to pay, or not to pay." Many companies hold the viewpoint that it is relatively "safe" from a US regulatory standpoint to pay the ransom, provided the bad actor is not part of a foreign terrorist organisation or subject to Treasury Department sanctions. However, as both ransomware attacks and regulation evolve, that may not necessarily be the case.

INSURANCE REIMBURSMENT OF RANSOM PAYMENTS RAISES QUESTIONS

In this context of rising ransomware attacks, insurers paying ransoms are criticised for multiple reasons. In addition to being expensive, cyber covers are accused of fueling ransomware attacks. Many have proposed a government ban on ransom payments, like Michael Daniel, former Special Assistant to President Obama and Cybersecurity Coordinator on the National Security Council, who stated, "We need to break this cycle and deprive the ransomware ecosystem of 'fuel.' [5] Several recommendations not to pay ransoms were issued, not only in the US:

1. In 2019, the FBI released a public announcement urging individuals or organisations not to pay ransoms and instead contact the FBI[6].
2. In his report, "The state of IT security in Germany in 2021", Germany's Federal Office for Information Security issued recommendations for local authorities on how to deal with ransom demands and advised not to pay ransoms but rather encourage prevention.
3. During a French Senate hearing, the National Agency for Computer Systems Security (ANSSI) and the Parquet de Paris (Paris Public Prosecutors' Office) suggested banning ransom payments[7].

INSURERS CAN NOT ADDRESS RANSOMWARE ALONE

US officials declared in 2021 that US and European governments intend to coordinate their efforts to tackle ransomware attacks. This raises questions about the role of insurers in fighting ransomware attacks and, more generally, their role in covering cyber risk due to the underlying insurability question. Major insurance actors[8] argue that the insurance industry alone cannot face the global cyber threats, among which are ransomware attacks.[9] The projections of ransomware attacks for 2022 and beyond are dark. Cybersecurity Ventures predict they will cost USD 10.5 trillion annually by 2025.[10]

Ransomware is malware

Ransomware is a type of malware that encrypts access to files and demands a ransom, in cryptocurrency,[11] in exchange for a decryption key. A significant development in the history of ransomware payments occurred in 2008 when bitcoin arrived.[12] The decentralised virtual money allows peer-to-peer transactions. This helped cybercriminals continue their unlawful activities and get paid for them untraceably. Typically, the modus operandi of ransomware goes through these phases:

1. Finding a target to hit.
2. Blocking access to local information.
3. Issuing a frightening message or ransom note and attempting to extort money.

VICTIMS FACE A DIFFICULT DECISION

A ransomware victim faces a choice between business interruption and using backed-up data to restore the activity or paying the ransom to obtain the decryption key to unlock the damaged files and servers, as well as extra payments to delete the stolen data. In some cases, not only is the targeted organisation required to pay the ransom but also its customers and other business partners. For instance, Vastaamo Finnish psychotherapy clinic experienced this triple extorsion. The clinic's data for 40,000 patients were breached due to a ransomware attack. **The criminals demanded that both the clinic and the patients pay.**

The FBI has been able to recover some of the bitcoin paid to bad actors. For example, the FIB recovered 63.7 of the 75 bitcoin paid in the US pipeline attack.

CYBER INSURANCE CAN REIMBURSE

The decision of weather to pay an ransomware claim is often a very practical financial decision. This it the case with Lake City, FL. Lake City was ransomware with the demand for bitcoin. Lake City held insurance against a potential ransomware attack. The insurance company, Beazley, paid 42 bitcoin to unlock the cities information.[13]

---

[5] Maranon, A. & Wittes, B. (11 August 2021). Ransomware Payments and the Law. Lawfare. Retrieved 12 July 2023, from https://www.lawfareblog.com/ransomware-payments-and-law.

[6] Priebe, J. (9 October 2019). FBI Public Service Announcement on Ransomware https://www.carpedatumlaw.com/2019/10/fbi-public-service-announcement-on-ransomware/.

[7] Adam, L. (7 September 2022). https://www.lemonde.fr/pixels/article/2022/09/07/rancongiciel-l-etat-pret-a-valider-l-indemnisation-des-rancons-par-les-assurances_6140628_4408996.html.

[8] Wolff, J. (12 June 2021). As Ransomware Demands Boom, Insurance Companies Keep Paying Out. Wired. Retrieved 12 July 2023, from https://www.wired.com/story/ransomware-insurance-payments/.

[9] Cerulus, L. & De Goujard, C. (22 June 2021). EU, US launch initiative against ransomware. Politico. Retrieved 12 July 2023 from https://www.politico.eu/article/eu-us-launch-ransomware-cooperation-group/.

[10] Morgan, S. (10 December 2022). Top 10 Cybersecurity Predictions and Statistics for 2023. Cybercrime Magazine. Retrieved 12 July 2023 from https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/.

[11] Glover, C. (13 September 2021). Are ransomware and cryptocurrencies intrinsically linked? Tech Monitor. Retrieved 12 July 2023 from https://techmonitor.ai/technology/cybersecurity/ransomware-and-cryptocurrencies.

[12] Pope, J. (2016). Ransomware: Minimizing the risks. Innovations in clinical neuroscience, vol. 13, no 11-12, p. 37.

[13] Dudley, R. (2019). The extortion economy: How insurance companies are fueling a rise in ransomware attacks. Pro Publica.

HACKERS DO NOT ALWAYS LIVE UP TO THEIR PROMISES

According to the Sophos State of Ransomware 2021 Report**,** 8% of victim organisations have never received a working decryption key after payment. And even if the right key is received, victims may not be able to restore everything completely, as the average of data recovered is 65%.[14]

Changes in regulation

RANSOMWARE DOUBLE EXTORTION COULD TRIGGER CFAA

Historically, the law has had a difficult time keeping pace with rapidly evolving cybercrimes like ransomware. Ransomware has been prosecuted by current laws such as the Computer Fraud and Abuse Act (CFAA) and the Economic Espionage Act (EEA). Both laws are quite old, enacted in 1986 and 1996, respectively. The CFAA makes it a crime to transmit in interstate or foreign commerce a demand for money or anything else of value "in relation to damage to a protected computer, where such damage was caused to facilitate the extortion."[15] A common trend in ransomware attacks is double extortion—where the bad actor threatens to disclose data exfiltrated if the victim refuses to pay the ransom. Threatening to disclose information if the ransom is not paid could trigger aspects of the CFAA, particularly if there are threats to obtain information through unauthorised access to a protected computer and/ or threats to disclose information already obtained through unauthorised access into a protected computer. In contrast to the CFAA, the EEA authorises criminal penalties for theft of trade secrets, including intangible "financial, business, scientific, technical, economic, or engineering information."[16]

REAL CHALLENGES WHEN THE ATTACK IS PERPETRATED FROM ANOTHER COUNTRY

Although ransomware can be prosecuted by way of these laws, there are significant practical concerns in investigating and prosecuting cybercrimes when the attack originates from another country. Sovereign nations have their own legal systems. While some countries have extradition treaties with the United States, the bad actor is often located in places like Russia, China, North Korea and Iran, where there is no extradition treaty with the United States. Recent research suggests that 74% of ransomware revenue goes to Russia-linked hackers.[17] Cyberattacks are also famous for the attribution problem. It is very difficult to attribute an attack to a particular bad actor, and there are varying degrees or standards of attribution. Countries that are home to ransomware criminals, and are often believed to collaborate with them, have plausible deniability by claiming the level of attribution is insufficient.

NO PROHIBITION ON PAYING RANSOM UNLESS IT FUNDS TERRORISM

When it comes to firms and institutions paying the ransom, there are no specific prohibitions. However, as mentioned earlier, it is a crime to knowingly provide currency or other property to entities designated by the US Secretary of State as foreign terrorist organisations or listed on the Office of Foreign Assets Control's Designated Nationals and Blocked Persons List. This is similar to ransoms in other crimes such as kidnapping. In 2015, the US Department of Justice clarified that it "has never used the material support statute to prosecute a hostage's family or friends for paying a ransom for the safe return of their loved one."[18]

Laws for ransomware have initially focused on reporting and pay particular attention to the financial services and banking sectors. Work is being done to protect personally identifiable information (PII) and to track the movement of currency to other bad acts. In July 2021, the US Department of Justice seized USD 2.3 million in cryptocurrency paid to the ransomware group DarkSide. Deputy Attorney General Lisa O. Monaco, for the US Department of Justice, stated, "Ransom payments are the fuel that propels the digital extortion engine, and today's announcement demonstrates that the United States will use all available tools to make these attacks more costly and less profitable for criminal enterprises. We will continue to target the entire ransomware ecosystem to disrupt and deter these attacks."[19]

REGULATORY ONGOING DISCUSSIONS ON RANSOMWARE REIMBURSEMENT BY INSURERS

The regulatory entities have been engaged in an active debate on the ransomware reimbursements by insurers. During a French Senate hearing, the ANSSI and the Parquet de Paris criticised cyber insurers for being too willing to pay ransoms. They suggest that the reason why France is more often a victim of ransomware cyberattacks is because the French pay easily. [20] According to the Hiscox Cyber Readiness Report in 2021, France is in the top three of countries that pay ransom demands (in 19% of ransomwares attacks), behind the

[14] Cook, S. (14 June 2023). 2018-2022 ransomware statistics and facts. Comparitech. Retrieved 12 July 2023 from https://www.comparitech.com/antivirus/ransomware-statistics/.

[15] Congressional Research Service (5 October 2021), op cit.

[16] Ibid.

[17] Tidy, J. (14 February 2022). 74% of ransomware revenue goes to Russia-linked hackers. BBC. Retrieved 12 July 2023 from https://www.bbc.com/news/technology-60378009#:~:text=New%20analysis%20suggests%20that%2074,it%20is%20harbouring%20cyber%2Dcriminals.

[18] Congressional Research Service (5 October 2021), op cit.

[19] US Department of Justice (7 June 2021). Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists DarkSide. Press release. Retrieved 12 July 2023 from https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

[20] Chicheportiche, O. (5 June 2021). Why Insurers Might Stop Covering Business Ransomware Risk. BFM Business. Retrieved 12 July 2023 from https://www.bfmtv.com/economie/entreprises/pourquoi-les-assureurs-pourraient-arreter-de-couvrir-le-risque-des-rancongiciels-subis-par-les-entreprises_AN-202105060007.html.

US (21%) and Germany (21%).[21] According to the ANSSI, some victims prefer to pay a few million in ransomware rather than tens of millions in data loss covered by their insurance policies. In response to this hearing, AXA France suspended its ransomware reimbursement coverage.[22] A few months later, Generali France made a similar decision by stating that insurers should stay out of ransomware insurance following a parliamentary report by deputy Valéria Faure-Muntian of LREM that recommends banning insurers from paying ransoms.[23] However, in February 2022, the Legal High Committee for Financial Markets of Paris (HCJP) issued a report on this matter. According to the committee, a ban on ransom payments would penalise certain companies or public institutions that are victims of cybercriminals. They could find themselves in great financial difficulty because they could not cover all or part of their losses.[24]

Ultimately the French government relied on this recommendation and issued a bill, tabled on March 2023 in the National Assembly, authorising this payment if the victim company files a complaint within 72 hours, paving the way to the end of ransomware suspensions made recently by some major insurers.

It is unclear, however, how long ransomware payments will be permitted in the US. Many have proposed a government ban on ransom payments.[25] Michael Daniel, former Special Assistant to President Obama and Cybersecurity Coordinator on the National Security Council, stated, "We need to break this cycle and deprive the ransomware ecosystem of 'fuel.' A payment ban would take some burden off organisations, by removing payment as a legal possibility. As a result, well designed prohibitions would provide targeted organisations with leverage to push back against their attackers. Such prohibitions should not be implemented immediately, in fact, such bans should only be put in place after governments have established effective victim-support mechanisms. Payment prohibitions should be part of a broad-based campaign to improve prevention, deterrence, disruption, and response." Some disagree with a ban. According to Jen Ellis, Rapid7 community and public affairs vice-president, "In the world we do live in, banning payments would almost certainly result in a pretty horrific game of 'chicken,' whereby criminals would shift all their focus towards organisations which are least likely to be able to deal with downtime—for example hospitals, water-treatment plants, energy providers, and schools." [26]

As regulations concerning ransomware continue to develop and evolve, paying the ransom in ransomware attacks is likely to become complicated and possibly even illegal. Companies and institutions should consider how regulations may change when assessing the risk posed by ransomware.

RANSOMWARE ANALYTICS FROM PUBLIC DATABASE

Scarce public data

Due to the sensitive nature of ransomware payments, statistics on these payments are scattered, if available. Data provided in the past five years by security firms (Sophos, 2020; Purplesec, 2020; Coveware, 2020), insurers (Coalition, 2020; NetDiligence, 2019) and law enforcement (FBI Internet Crime Complaint Center, 2019) indicates that the frequency of ransomware attacks has increased, the requested ransom amounts have exploded and the business interruption costs have also increased.[27] This same trend can be found in public data such as the Vocabulary for Event Recording and Information Sharing (VERIS) Community Database.

Veris community database

The VERIS Community Database is an open source database.[28] It aims to collect cybersecurity incidents in a common framework using the VERIS vocabulary, a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner. It helps organisations collect useful incident-related information and share that information with others. It was launched in 2010 by Verizon, an American wireless network operator.

Incidents in VERIS

Out of 9,046 cyber incidents in VERIS from 2013 to 2021, 851 involved a malware. Of these, a little more than one-third, 33.49%, are ransomware. Ransomware starts to appear in VERIS in 2013. They increase overall until 2020 and 2021, when there are more ransomware attacks than other malware attacks, as we can see in Figure 4.

[21] Hiscox. Hiscox Cyber Readiness Report 2021: Don't Let Cyber Be a Game of Chance. Retrieved 12 July 2023 from https://www.hiscox.co.uk/sites/default/files/documents/2021-04/21486-Hiscox-Cyber-Readiness-Report-2021-UK.pdf.

[22] GNT Media (13 May 2021). Ransomware: AXA stops covering ransom payments in France. Retrieved 12 July 2023 from https://www.generation-nt.com/ransomware-remboursement-rancon-axa-france-rancongiciel-actualite-1988068.html.

[23] Robert, L. (3 February 2022). Generali France annonce qu'il va cesser de rembourser les rançons des entreprises victimes de rançongiciels. Comstar. Retrieved 12 July 2023 from https://www.channelnews.fr/generali-france-annonce-quil-va-cesser-de-rembourser-les-rancons-des-entreprises-victimes-de-rancongiciels-110486.

[24] Haut Comite Juridique de la Place financiere de Paris (28 January 2022). Rapport Sur L'Assurabilite des Risques Cyber. Retrieved 12 July 2023 from https://www.banque-france.fr/sites/default/files/rapport_45_f.pdf.

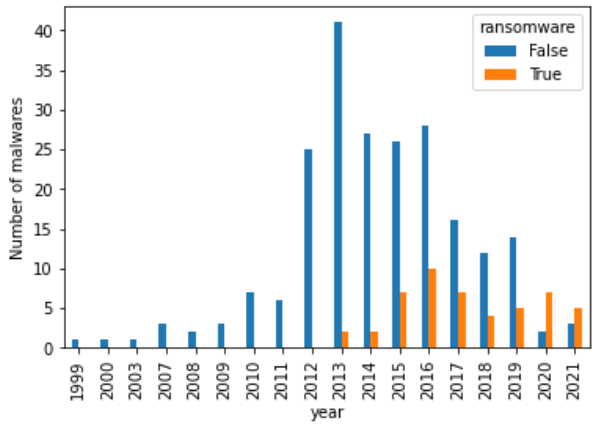
[25] Maranon, A. & Wittes, B. (11 August 2021), Lawfare, op cit.

[26] Tidy, J. (20 May 2021). Ransomware: Should paying hacker ransoms be illegal? BBC. Retrieved 12 July 2023 from https://www.bbc.com/news/technology-57173096.

[27] Balasubramanian, A. (2021). Insurance Against Ransomware. Available at SSRN 3846111.

[28] VERIS. The VERIS Community Database (VCDB). Retrieved 12 July 2023 from http://veriscommunity.net/vcdb.html.

FIGURE 4: MALWARE IN VERIS BY YEAR



Data sourced from VERIS Community Database

MOST INCIDENTS ARE REPORTED IN THE US

The US is by far the most active country in this database. Among the 285 reported incidents, 218 are found in this US, 18 in Canada and 14 in England. The remaining 35 attacks are shared among the 18 remaining countries in the database. France for instance has reported only four ransomware attacks. The listed countries are shown on the map in Figure 5.

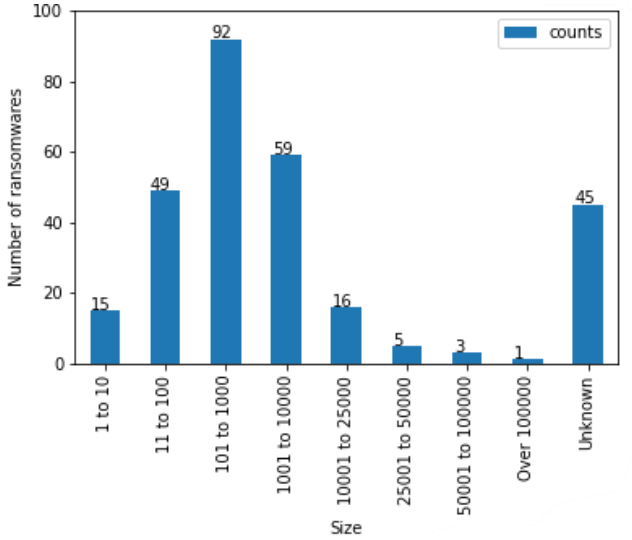
FIGURE 5: COUNTRIES REPORTING RANSOMWARE ATTACKS

Data sourced from VERIS Community Database

SMALL BUSINESSES SEEM TO BE MORE TARGETED

All companies are targeted regardless of size, but the VERIS data shows those with 101 to 1,000 employees, followed by the ones with 1,001 to 10,000, have experienced more ransomware attacks compared to businesses of other sizes.

FIGURE 6: VERIS-REPORTED RANSOMWARE BY SIZE

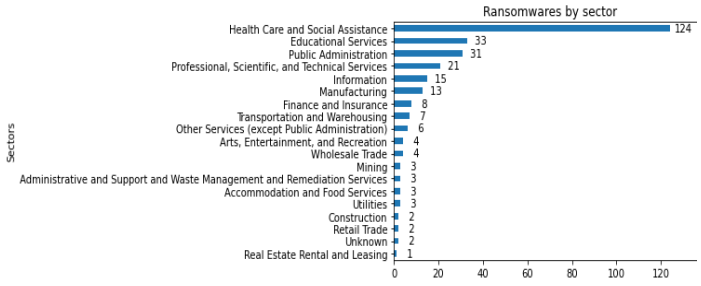


Data sourced from VERIS Community Database

HEALTHCARE SERVICES ARE THE MOST TARGETED SECTOR

Healthcare services are one of the most targeted sectors, followed by educational services and public administration, as we can see in Figure 7.

FIGURE 7: VERIS-REPORTED RANSOMWARE BY SECTOR

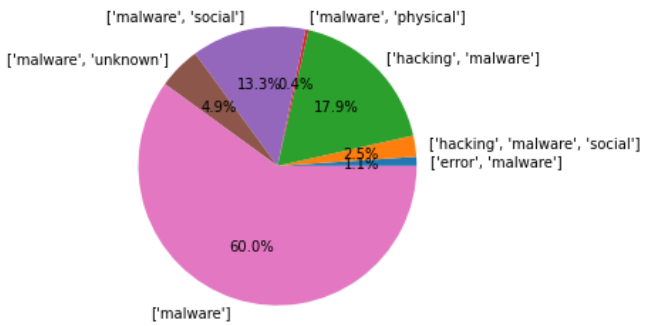


Data sourced from VERIS Community Database

RANSOMWARE IS NOT ALWAYS STANDALONE

In 60% of the observed attacks in the VERIS database, the ransomware attack is standalone: it is not accompanied by another type of attack. The remaining 40% of attacks are accompanied by another type of action: hacking in 17.9% of cases (stolen credentials, vulnerabilities exploitation, buffer overflow etc.), social in 13.3% of cases (phishing, extortion), errors and physical problems in less than 2% of attacks (publishing error, misconfiguration, malfunction).

FIGURE 8: ACTIONS INVOLVED IN CYBERATTACK



Data sourced from VERIS Community Database

As ransomware attacks grew in the last few years, a comparable increase can be noted in the VERIS Community Database This growth mainly concerns 2020 and 2021 in VERIS as ransomware becomes the first malware hackers use. The double and triple data extortion techniques are also observed. Ransomware attacks are not always standalone. The modelling later described does not use the VERIS Community Database as it is a history-free approach. The VERIS Community Database, as all public databases, suffers from underreporting issues. However, the trends observed in official statistics are found in this database.

Modelling

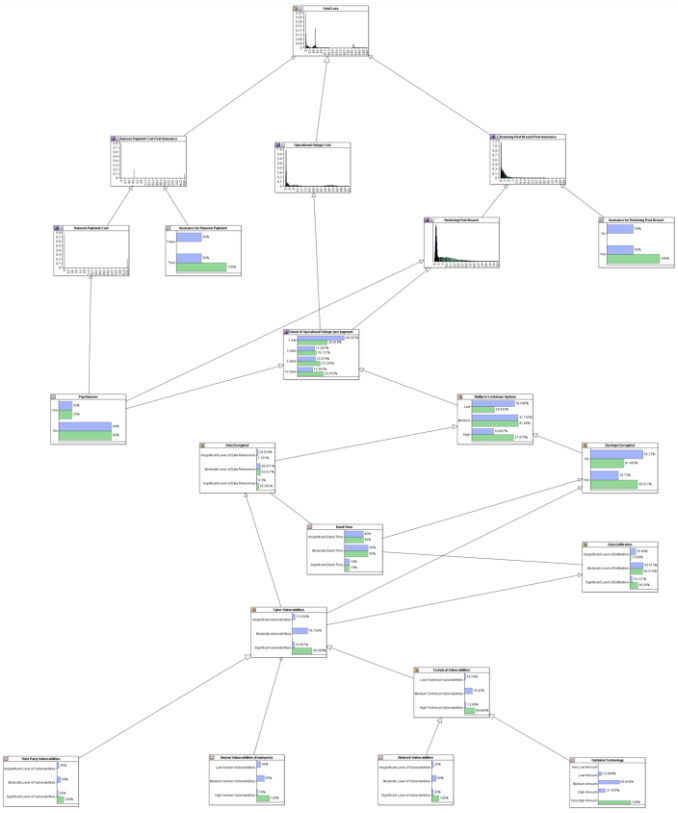
SELECTION OF A SET OF SCENARIOS

With new types of ransomware on the rise, innovative controls and possible legal and regulatory changes on the way, the risk posed by ransomware is constantly evolving. What may be the state of the world today may be completely different one month later. Causal modelling is an approach that can account for these changes and test different scenarios.

Unlike other methods, causal models incorporate expert insights without forcing the data to represent a financial loss curve directly. Causal modelling uses a Bayesian network to probabilistically express how different events interact with each other to create different outcomes. Experts are asked investigatory questions to uncover the paths a risk will take as it manifests. By situating unprecedented events in context, experts provide better estimates for the impact of a ransomware attack and build up a logical explanation of how outcomes can be derived.

To illustrate how different states and events interact with each other in a ransomware attack, we have included an example of a ransomware model in Figure 9.

FIGURE 9: RANSOMWARE MODEL



Source: Milliman-created ransomware model using AgenaRisk

Each box in the model represents the relationships within the process, control or action accounted for by the model. The model shows how an organisation's human vulnerabilities, network vulnerabilities, outdated technology and third-party vulnerabilities flow into situations where a bad actor can encrypt or exfiltrate sensitive data on a corporate system. The model then shows the outcomes of such events and calculates the operational outage cost, restoring post-breach cost as well as the cost of the actual ransom payment, if it is paid.

SIMULATION AND TESTING

In the ransomware model provided, the 25th percentile to the 75th percentile of the loss distribution ranges from approximately $883,000 to $4.47 million. If all controls were to stop working and were set to their worst state, the 25th percentile to the 75th percentile of the loss distribution would range from approximately $8.96 million to $31.72 million.

One of the great advantages of causal modelling is its flexibility. If the state of a node changes, for instance if the firm made significant software and hardware updates, then the outdated technology node can be toggled to reflect that it is in a better state and the model will update to account for this.

This flexibility also provides the ability to test different risk decisions. As mentioned earlier, one of the greatest concerns is whether to pay the ransom. This can impact a firm's decision on whether to pay the ransom.

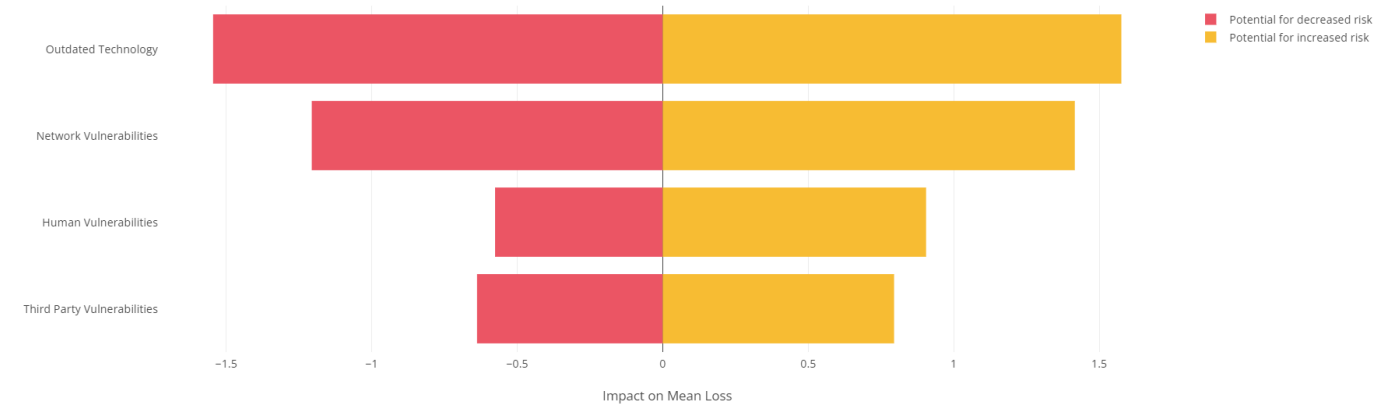
In the model there is a node called "Pay Ransom." If we select "yes," then the model will consider the impact of paying the ransom on the "Extent of Operational Outage" node, the "Restoring Post Breach" node and the "Ransom Payment Cost" node. It will then produce a total loss distribution under the assumption that the ransom is paid. Alternatively, if we select "no," then the model will express the impact of not paying for those three nodes and produce a total loss distribution under the assumption that the ransom is not paid. To better determine the cost of paying the ransom, the model also has a node for whether the insurer covers ransom payments. The model also covers situations where the ransom would be paid a percentage of the time and not paid another percentage of the time.

According to this analysis, under the current, mostly control environment, paying the ransom would increase the expected loss, with the 25th percentile to 75th percentile of the loss distribution ranging from $4.68 million to $6.85 million. This assumes that the insurer would cover part of the ransom payment as well. Alternatively, in the worst-case scenario, when controls are in their poorest states, paying the ransom would reduce the firm's expected loss substantially, with the 25th percentile to 75th percentile of the distribution ranging from $6.03 million to $10.20 million. Thus, according to the model, if the firm's controls are poor, then paying the ransom makes a great deal more sense to reduce potential risk.

The sensitivity analysis in Figure 10 shows the impact of the various drivers in the model on the loss distribution. The greatest potential to reduce risk in the model comes from outdated technology, which would reduce risk such that the 25th percentile to 75th percentile in the most likely current state would be $815,000 to $3.77 million. Having a significant amount of outdated technology also happens to be the greatest driver of increased risk. If the firm stopped updating its technology and all technical assets were considered outdated, then the 25th percentile to the 75th percentile of the loss distribution would increase from $966,000 to $10.78 million.

This type of risk analysis is useful in identifying controls to invest additional resources in, which in this case would be upgrading technology, as well as where not to invest further or perhaps not invest at all. As the firm makes decisions to invest in and improve certain controls, the analysis can be run again to find the next control with the greatest potential to reduce risk.

FIGURE 10: RANSOMWARE MODEL – SENSITIVITY ANALYSIS



Source: Milliman

Concluding remarks

We presented how ransomware attacks are a growing issue that organisations all around the world will have to face. This increasing trend is observed in public databases such as the VERIS Community Database, where ransomware attacks have become the most prevalent malware in 2020 and 2021.

The uncertainty around ransomware reimbursement by insurer regulation and the evolving modus operandi of hackers make a causal approach reasonable to develop. Bayesian networks are used to model an organisation's financial loss. This approach shows that an insurer's reimbursement of a ransom and the state of the IT systems have an impact over the loss distribution.

Milliman

Milliman is among the world's largest providers of actuarial, risk management, and technology solutions. Our consulting and advanced analytics capabilities encompass healthcare, property & casualty insurance, life insurance and financial services, and employee benefits. Founded in 1947, Milliman is an independent firm with offices in major cities around the globe.

milliman.com

CONTACT

Chris Beck
chris.beck@milliman.com

Alexandre Boumezoued
alexandre.boumezoued@milliman.com

Yousra Cherkaoui
yousra.cherkaoui@milliman.com

Eliott Pradat
eliott.pradat@milliman.com