Cambridge Centre for Risk Studies

Collaboration with Kivu Consulting Inc

MITIGATING RANSOMWARE RISK: DETERMINING OPTIMAL STRATEGIES FOR BUSINESSES

Centre for **Risk Studies**

UNIVERSITY OF CAMBRIDGE
Judge Business School

KIVU

December 2022

This report is based on original research by the Cambridge Centre for Risk Studies at the University of Cambridge Judge Business School in collaboration with Kivu Consulting Inc.

The following people contributed the research, model development, and writing of this report.

Cambridge Centre for Risk Studies

Jennifer Copic, Cyber Model Lead and Senior Risk Researcher
Gabriele La Malfa, Risk Researcher
Juliane Kriebitzsch, Risk Researcher
Dr Andrew Coburn, Chief Scientist
Professor Daniel Ralph, Academic Director
Tamara Evan, Report Editor and Risk Researcher

Kivu Consulting Inc.

Winston Krone, Chief Research Officer
Stephen Lister, Senior Incident Response Consultant
Terry Mee, Senior Incident Response Consultant
Matthew McCabe, General Counsel & Chief Risk Officer

The Cambridge Centre for Risk Studies greatly appreciates the valuable guidance and support of the following individuals in the making of this report:

Eireann Leverett, Founder and CEO, Concinnity Risks
Suzanne Hopkins-Oldak, Head of Strategic Partnerships, Risilience

Report Reference: Copic, J., Krone, W., La Malfa, G., Kriebitzsch, J., Leverett, E., Coburn, A., Ralph, D., Lister, S., Mee, T., Evan, T., Hopkins-Oldak, S., McCabe, M.; *Mitigating Ransomware Risk: Determining Optimal Strategies for Businesses*; Cambridge Risk Framework series; Centre for Risk Studies; University of Cambridge.

Mitigating Ransomware Risk: Determining Optimal Strategies for Businesses

Contents

1 Executive Summary

The Cambridge Centre for Risk Studies (CCRS) and Kivu Consulting Inc. (Kivu) have combined efforts to pioneer new research to benchmark cost effective responses to cybercrime. This research combines a novel dataset on ransom payment information, company attributes, and effective security controls for remediation to support Chief Information Security Officers (CISOs), Chief Research Officers (CROs), and Risk Managers in assessing and managing the threat of ransomware.

Dataset Characteristics

This paper and the novel dataset it references and describes provide new insights into the significant threat to businesses from ransomware attacks. The dataset provides an aggregate view of 422 attacks carried out against 416 organisations that entered an incident response phase between May 2019 and March 2022. Additional data analysed includes ransomware victims and statistics about ransom demands and payments, country of origin and business sector.

Company Attributes

The most frequently impacted sector in the dataset is Industrials, driven by a large number of events which target capital goods manufacturing firms, professional services firms like lawyers and architects, and transportation, which are all sub-industry groups classed under Industrials in Global Industry Classification Standard (GICS) sector categorisation. The Healthcare and Information Technology sectors round out the top three most attacked sectors in this dataset. Consumer Discretionary and Education complete the top five.

Where a ransomware attack impacted a multinational organisation, the country was determined as the modal geographical location affected by the attack in terms of endpoints, employees or services negatively affected and the company headquarters location. The data shows that 84% of the ransom events occurred in the Americas, while 13% occurred in Europe. Breaking these regions down to the country level, the United States features most frequently in the dataset as a unique attack location, accounting for 80% of all captured ransomware events; the United Kingdom experiences 9%, Canada and Australia experience 2% each.

The majority of attacked organisations in this analysis had only 10 to 1,000 endpoints infected, which supports the conjecture that Small and Medium Sized businesses are the most frequent successful targets of ransomware attacks.

Ransomware Attributes

Examining the 68 ransomware variants featured in the Aggregate Dataset, it is notable that 62% of them have a LeakBlog presence. This means that the threat actors responsible for these attacks may also exfiltrate data as a means to further encourage payment. 49% have a group structure of Ransomware as a Service (RaaS), 47% have a Closed Group structure and just 4% have a Live off the Land Group (LOTL-Group) structure. Further, 94% of the ransomware variants accept negotiation on their pricing. By event frequency the data also shows that the top ransomware variant was Phobos/Dharma, with Sodinokibi/REvil and Conti completing the top three. Another measure is to analyse the total ransom payments per ransomware variant, which yields a different top three: DarkSide, Conti and Egregor. However, sorting by the average per event ransom payment the ranking changes yet again, with ALPHV (BlackCat), ViceSociety and DarkSide in the top three.

Ransom Payments

In 72% of the events in the databases, a ransom was paid. This figure is starkly different to those in other industry reports on the payment of ransoms. This is due to the source of this report's data being a ransom negotiation and recovery firm, which would not have been retained if the victim organisations were able to quickly recover from backups without the need to pay a ransom or even negotiate. Put simply, the Aggregate Dataset captures only incidents in which companies sought professional assistance in responding to attacks.

The dataset captures a total ransom demand of $249.38 million, with a total actual ransom payment of $147.87 million. These ransom demands and payments are heavy tailed as seen in other academic literature.

Ransom Event Analysis

The data demonstrates that quarter four (Q4) is the busiest quarter both in terms of frequency of events and in terms of the number of payments made. As a year, 2020 saw a higher number of attacks than 2021, the only other year with complete data in our dataset. This is likely due to the workplace changes resulting from COVID-19.

Interestingly, Q4 of 2021 shows a unique trend in that there were fewer ransom events which resulted

in payment, yet the total ransom payments that were made account for the second largest quarter in the dataset. This could highlight that ransom payments are getting larger (with an increase in "big game" targets), a theory that has been recently supported by other research.[1]

Control Effectiveness and Savings

The term "control effectiveness" or "security control effectiveness" is not consistently defined in academic or industry literature. For the purposes of this paper, control effectiveness is considered in terms of the security or privacy risk reduction the control can provide for the ransomware threat and not the measure of how effective a control is deployed or implemented. The risk reduction element of control effectiveness is then split into two parts: one which determines controls that would have reduced the likelihood of the event occurring while the other examines the potential ransom payment cost savings.

The latter sections of this report focus on illuminating which controls are best recommended for each company using the CIS Top 20 v7 classification as an indicator, providing a ranking of the most pervasive ransomware in terms of both frequency and attack effectiveness.

Control 8 (Malware Defences) is listed in 51% of the logged cases as one of three controls that would have prevented or mitigated the attack. Control 4 (Controlled Use of Administrative Privileges) (46%) and Control 6 (Maintenance, Monitoring and Analysis of Audit Logs) (43%) complete the top three effective controls from an event frequency standpoint. This combination of three controls was recommended 11% of the time.

Aggregating these results further by grouping the controls into the high-level cyber hygiene categories of Basic, Foundational and Organisational, we can see which grouping is most recommended. The results highlight that the Basic cyber hygiene category needs further review by organisations to aid in event prevention or limit event impact. Interestingly, the Organisational grouping is barely referenced as effective at-risk reduction, potentially because securing IT systems is a more effective at-risk reduction technique than organisational controls, due to the rise in ransomware attacks that rely or incorporate purely technical vectors (such as exploiting zero-day vulnerabilities or the use of previously lost credentials). Organisational controls such as employee training have little impact against such attacks.

The study finds that the controls with the greatest potential cost savings are Control 19 (Incident Response and Management) which has the highest potential cost savings of $333,000, Control 3 (Continuous Vulnerability Management) is the next most cost effective, with a potential savings of $238,000 and Control 6 (Maintenance, Monitoring and Analysis of Audit Logs) with a potential savings of $197,000. The controls with the smallest cost savings potential are Control 1 (Inventory Management of Hardware Assets), Control 14 (Controlled Access Based on the Need to Know) and Control 20 (Penetration Tests and Red Team Exercises), all with a cost savings less than $18,000.

Conclusions

This report's findings provide quantified insights into the potential response of effective controls to ransomware threats and allows organisation an evidence base to support controls prioritisation. CISOs, CROs and risk managers can use this work to start a discussion on their security postures and preparation for evolving attack methods and tactics. In particular, this report proves a strong correlation between certain sets of controls and specific attack vectors, meaning that defences need to be regularly reviewed and revised as attacker groups change their modes for gaining access to networks.

Although the dataset and analysis are novel in the academic space, the researchers recognise that data asymmetry exists within this analysis and thus limits the overall interpretation. The lack of data on cyber risk is a clear challenge for both cyber security professionals and the cyber insurance industry.[2] Swift action is needed to develop a live comprehensive data feed that replicates this analysis to aid in real-time cyber security control investment decision making. The report shares these results in order to provoke discussion and potentially further research and reporting in this area.

[1] (E. Leverett et al. 2022)

[2] (Cremer et al. 2022)

2 Introduction

Ransomware Overview and Trends

Ransomware is a type of malware (malicious software) that has two basic technical goals - to make a system inaccessible and to steal the data it contains. These goals may be combined together in many cases or used alternatively, but the purpose is always to extort a ransom (typically demanded in a cryptocurrency) in exchange for the decryption keys to regain control of the system and/or the return of (or a promise not to publish) the stolen data. In addition to the costs of the ransom demand, organisations may also incur regulatory fines and expenses as a result of an attack, as well as litigation costs following a compromise of confidential data and significant business interruption losses.

The impact of ransomware in cyber risk has grown dramatically in the two years since the onset of the COVID-19 pandemic (2020-2022). Until 2019, losses related to data theft or unauthorized exposure were the biggest driver of cyber insurance claims (more than 50%).[1] Since 2020, the trends have changed and ransomware has become responsible for the highest number of insurance claims (leaping from 13% in 2019 to 54% in 2020).[2] Aon shows an even more dramatic increase in ransom events, with an increase of 548% in ransom event frequency in Q1 2021 compared to Q1 2018, compared to data breach, which is down 52%.[3] This data shows that threat actors have focused their attacks to exploit systems and vulnerabilities enabling remote working during the COVID-19 pandemic.

Trends in the first quarter of 2022 indicate a general decrease in malware attacks compared with Q4 2021. The largest volume of attacks, around 57%, was recorded in Europe, the Middle East and Africa. The remaining 43% is divided between the Americas (22%) and Asia Pacific (21%).[4] Chubb reports that, to date, Professional Services, Technology and Manufacturing were the most targeted sectors in 2022 while the recent Coalition report supports this ranking that the Manufacturing and Industrial sectors are the top targeted sectors, but there has also been a 57% raise in claims from non-profits.[5]

The war in Ukraine has been a significant event for cyber attacks. Prior to the February 2022 invasion, several established threat actors (e.g., Lockbit and Conti) clearly favoured Russia, presumably in order to protect their unofficial safe-haven status within the country. This included openly not targeting Russian organisations and writing malware code that deliberately avoided Russian networks. Since January 2022, some threat actor groups have openly supported Russia (Stormous) or Ukraine (various groups under the Anonymous "collective") and may have been involved in active operations against the other country or supporting entities.[6] Other cyber threat actors have sporadically voiced support for Russia, in some cases leading to factionalism within that threat actor group between pro-Russian and pro-Ukrainian members (e.g. Conti).[7] While previous cyber attacks (2015-2016) against Ukrainian banks, government agencies, and energy organisations (presumably carried out by groups guided or affiliated to the Russian state) had caused extensive damage, after the outbreak of war Ukraine demonstrated preparations for forward defence in cyber space,[8] with counter-offensives of ransomware and Distributed Denial of Service (DDOS) attacks targeting several Russian government agencies.[9]

As the size of ransom demands grew from 2018 to 2020, and threat actors moved from relatively small, fixed price ransom demands to more significant amounts tailored to the perceived sized of a victim, negotiation has become an important aspect of ransomware campaigns. Once the attack has taken place, the victim has a short timeframe in which to respond to a threat actor's demands but may be able to negotiate with the attacker for more time to pay, proof from the attacker that they are able to decrypt the data, or proof data has actually been exfiltrated, as well as a reduction in the size of the ransom demand. Increasingly, threat actors have added to the pressure of the cyber extortion by stealing data prior to launching any encryption of the victim's network. A victim is then pressured to pay a ransom both to recover its system and to prevent the release of sensitive data – a so-called "double extortion" event. As regulatory concerns have led to a trend in victim unwillingness to pay ransoms by 2022, threat actors have evolved to carry out data theft and extortion in ransomware attacks, rather than simply extorting after encryption.

[1] (Ralph 2019)

[2] (BitSight Technologies 2021)

[3] (AON 2022)

[4] (WatchGuard Technologies 2022)

[5] (Chubb 2022; Coalition 2022)

[6] (Vail 2022)

[7] Ibid.

[8] (Naimisha 2022)

[9] (Nast 2022)

There is a wide range of reasons victim organisations may choose to pay a ransom, including:

- Deficient or non-existent data backups which will delay the recovery process or make a full recovery commercially impossible;
- Threat actors may target senior executives, boards, or key partners and stakeholders to enact greatest impact on the decision-making processes of organisations;
- The threat of publication of confidential data concerning employees, customers and consumers (with resulting regulatory and litigation costs) may outweigh the perceived reputational damage to the victim of being publicly known to have paid a ransom;
- Estimated business interruption costs on the organisation may make it less costly to pay the ransom then experience the duration of outage to manually rebuild or reset systems from backups;
- The encryption and locking of vital systems may make it impossible for an organisation to adequately estimate the damage and potential losses, making paying a ransom seem the only verifiable costed option. This is exacerbated when victim organisations have not undertaken sufficient data mapping prior to an attack;
- Availability of reimbursement for ransom payment from cyber insurance and the perceived difficulty in proving business interruption losses, especially for mid-cap organisations.

Cyber Security Controls

To defend themselves against potential attacks, organisations implement various strategies and protocols to make systems resistant to ransomware attacks. These strategies and protocols are called cyber security controls, or mitigations. Several different classifications for controls exist, such as the 20 controls listed in the Center for Internet Security (CIS) Top 20 Controls v7 (known as CIS v7), National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, and MITRE ATT&CK Mitigations.[10] The controls are related to systems protection, data protection, information systems management, and troubleshooting operations due to an attack.

Control Effectiveness Definition

A review of the existing literature on cyber security controls provides an extensive review of defender techniques, considering both prevention and response to attacks, with some academic experiments also reporting on the effectiveness of these techniques, or controls.[11] Yet, the term "control effectiveness" or "security control effectiveness" is not consistently defined in academic or industry literature. NIST even proposes competing definitions within its own glossary, one focusing on the correct implementation or deployment of a given control and the other combining the first definition with the idea of risk reduction.[12] For the purposes of this paper, control effectiveness is considered in terms of the security or privacy risk reduction the control can provide for the ransomware threat and not the measure of how effective a control is deployed or implemented. The risk reduction element of control effectiveness is then split into two parts: one which determines controls that would have reduced the likelihood of the event occurring while the other examines the potential ransom payment cost savings.

To date, an academic study with real world event data in terms of the ransom demand, payment, effective control strategies and company attributes has not been identified. Incident responders play a critical role in attack management and ransom negotiation and thus have access to rich data on these variables. The Cambridge Centre for Risk Studies and Kivu formed a partnership in early 2021 to address this gap in cyber research.

The paper provides statistics for ransom attacks that were able to at least partially penetrate or compromise relevant networks and thus trigger the use of ransomware negotiation and recovery services. These events are then connected to those CIS v7 controls that were identified as most likely to have prevented and/or limited the impact of the specific event. This connection of an individual ransom event back to the top three preventative controls was completed by incident response analysts with direct experience of the event. Controls classification according to CIS v7 are listed in the Appendix of this report.

This research began in early 2021 and thus prior to the release of the CIS Top 18 Controls v8 (CIS v8). Therefore, this report uses CIS v7 in the analysis of the dataset, but references are noted where relevant controls might map to CIS v8.

[10] (Center for Internet Security 2021; NIST Joint Task Force Interagency Working Group 2020; MITRE ATT&CK 2021)

[11] (Beaman et al. 2021; Oz et al. 2022)

[12] (NIST and Computer and Security Resource Center 2022a; 2022b)

Breakout Box – CIS v7 Control 19

CIS v7 Control 19 covers Incident Response and Management. The main definition of this control reads:

"*Protect the organisation's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.*"[1]

The following describes the security subcategories that each company should implement to be ready to respond promptly to an attack:

- Having a detailed response plan and assigning duties to individuals regarding problem solving
- Having an efficient management and detailed reporting phase
- Publish reports on anomalies
- Conduct test and planning sessions and create incident scoring and prioritisation schemes

[1] (Center for Internet Security 2021)

Breakout Box – Key Ransomware Events

Costa Rica, 2022 – In April and May 2022, a series of attacks by Conti and Hive were carried out against 30 different Costa Rican government agencies, such as the Ministry of Finance and the Ministry of Labor and Social Security. The government was forced to shut down key systems and declare a state of emergency, labelling the attack an act of terrorism with the newly elected President Chaves Robles quoted as saying "We're at war and this is not an exaggeration."[1] Recovery took almost two months, with many in the private sector impacted as well.

Irish Health Service Executive (HSE), 2021 – In May 2021, ransomware was executed after months of unnoticed reconnaissance by the ransomware gang Conti within the network. The ransomware encrypted 80% of systems and forced medical staff to switch to pen and paper, creating numerous errors and delaying appointment and procedures.[2] The threat actors had exfiltrated 700GBs of data which included personal health information (PHI).[3] Interestingly, Conti posted a decryption key days into the lockout, which allowed for a quicker recovery. Full recovery was not achieved, however, until September 2021, 4 months after the ransomware had been executed.

Apache Log4j Library, 2021 – A zero-day vulnerability (meaning that cyber threat actors exploited this vulnerability before security specialists even knew about it in the wild) in an open-source Java logging utility, log4j, was discovered and "estimated to be present in over 100 million instances globally."[4] It allows for remote code execution (RCE), permitting threat actors to steal data, execute malware or take control of vulnerable machines. This event is a significant example of an imbedded risk to digital supply chains.

Colonial Pipeline, 2021 – A high profile ransomware and data breach attack on Colonial Pipeline caused a six-day disruption in the US Northeast, resulting in gas shortages. Impact was limited, however, due to the company paying DarkSide, the hacking group responsible for the attack, $4.4 million in ransom. Research by BitSight shows that "62% of the largest US Oil and Energy companies are at heightened risk of ransomware attack."[5]

SolarWinds, 2020 – Notable for the exploitation of SolarWinds software, threat actors implanted malicious code in the tech firm's offerings which then spread to its customers, including US government offices.

[1] (Associated Press 2022)

[2] (Corera 2021)

[3] (US Department of Health and Human Services 2022)

[4] (Center for Internet Security 2022)

[5] (Olcott 2021)

3 Dataset Analyses and Insights

Dataset Characteristics

The dataset used in this paper was compiled by Kivu, a cyber security company that intervenes in the event of a ransomware attack to aid in incident response and remediation. Once victim attribute information was assigned at the company level, the data was anonymised for reporting purposes. There are two overlapping datasets used for this analysis. One is a collection of ransom events that resulted in a payment (called Ransom Payment Dataset) and the other is a set of events with effective control strategies identified (called Effective Controls Dataset).

Ransom Payment Dataset

The Ransom Payment Dataset reports 303 ransom attacks against 300 different organisations between May 2019 and Jan 2022.[13] The data included dates of payments, the relevant ransomware variants, the original ransom demand and actual payments made (both in USD and BTC). There were 370 individual ransom payments made for the 303 unique ransom attacks, which includes test payments and payments made to separate cryptocurrency wallets.

Effective Controls Dataset

The Effective Controls Dataset contains 183 unique ransom attacks on 180 organisations between January 2021 and March 2022. For each of these attacks, incident responders who were directly involved in the negotiations or remediation process assigned the top three CIS v7 controls that would have prevented or limited the loss. (CIS Top 20 v7, see Appendix for list and definitions). It is worth nothing that no ranking was done when assigning the top three and thus the three assigned controls are treated equally in the analysis.

Aggregate Dataset

There are a total of 422 unique ransom events operating on 416 individual organisations, with 64 records listing both ransom payment and effective controls. Analysis on ransom payments and ransomware variants is carried out on the entire Ransom Payment Dataset, while analysis on effective controls is applied to the entire Effective Controls Dataset, unless otherwise noted.

[13] Some organisations in the dataset were attacked more than once during the 1.5-year analysis window.

Company Attributes

Sector

The GICS sector classification along with two additional sectors is used throughout to classify all the victim organisations in the Aggregate Dataset. [14]

- *Education sector* – to account for university, colleges, museums both private/public and for-profit/not-for-profit, as well as local primary and secondary school districts[15]
- *Government sector* – to account for local municipal authorities/services and public sector bodies

Sectors were classified using Standard and Poor's (S&P) Capital IQ and desktop research, in a few cases reverting back to the incident response analyst when data was limited. Below (Figure 1), the count of unique events as opposed to the count of unique victim organisations is presented, as some organisations in the dataset were impacted by multiple ransom attacks over the analysis time frame.

The most frequently impacted sector in the dataset is Industrials, driven by a large number of events which target capital goods manufacturing firms, professional services firms like lawyers and architects, and transportation, which are all sub-industry groups classed under Industrials in GICS sector categorisation. The Healthcare and Information Technology sectors round out the top three most attacked sectors in this dataset. Consumer Discretionary and Education complete the top five.

Country and Regions

The country where ransomware attacks occur was captured using data from Kivu, with missing data populated by S&P Capital IQ and desktop research for the Aggregate Dataset. Where a ransomware attack impacted a multinational organisation, the country was determined as the mode geographical location affected by the attack in terms of endpoints, employees or services negatively affected and the company headquarters location.

20 countries are represented in the combined dataset with 80% of system infections recorded

[14] (S&P Global 2018)

[15] The Education Services category within Cons Discretionary sub-industry of GICS was not used in order separate results for education from other consumer-focused industries. Further, this category in GICS considers for-profit institutions while this data is more focused on not-for-profit educational centres.

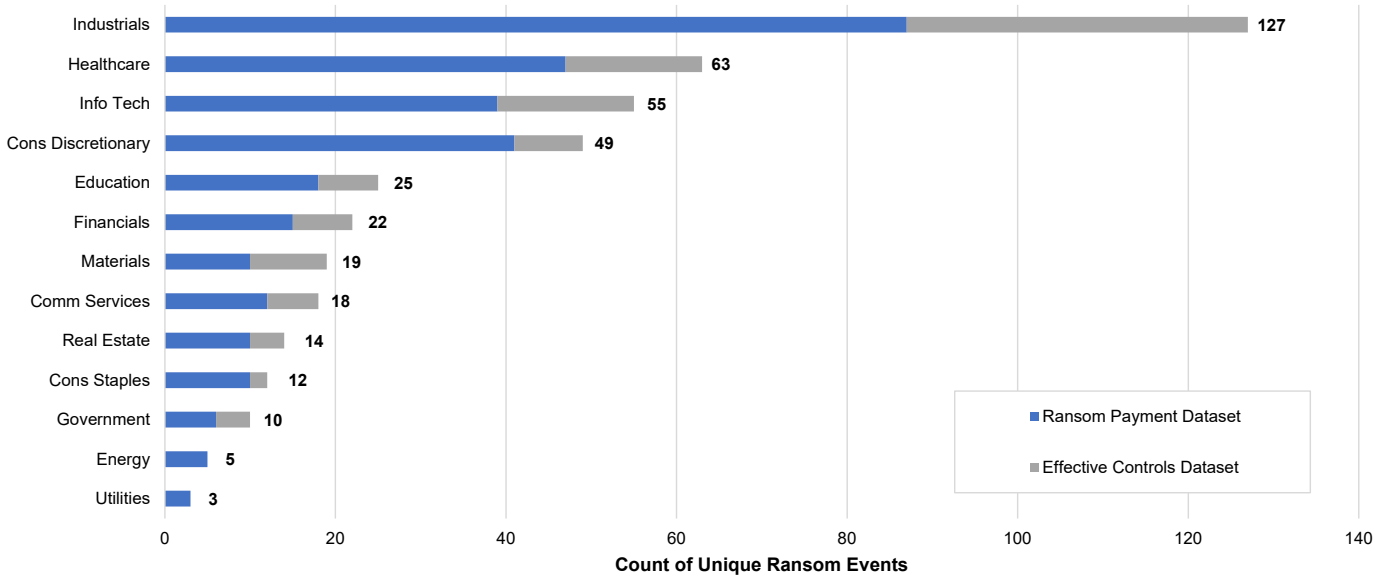


Figure 1: Sectors frequency per dataset (Source: Cambridge Centre for Risk Studies).

taking place in the United States. Using the UN Statistics Division's regional definitions shows that 84% of the ransom events occurred in the Americas, while 13% occurred in Europe.[16] Breaking these regions down to the country level, the United States features most frequently in the dataset, accounting for 80% of all captured ransomware events; the United Kingdom experiences 9%, Canada and Australia experience 2% each.

Size

For the records in the Effective Controls Dataset, a proxy is used for the company size compared to the number of infected endpoints. Small and Medium sized organisations are most targeted by ransom attacks, with one report suggesting that 70% of the attacks in 2021 targeted organisations with less than 500 employees and another report suggesting that small organisations (with an annual revenue of less than $25 million) were 119% more likely to have an insurance claim relating to the Microsoft Exchange vulnerability.[17] The majority of attacked organisations in this analysis had only 10 to 1,000 endpoints infected, which could support the targeting of Small and Medium Sized businesses. The limitation of this analysis is that the dataset tracked the number of endpoints potentially or verifiably infected and not the entire corporate endpoint structure. Thus, a ransomware attack limited to a division or department of a larger organisation will, for this study, reflect the number of endpoints actually affected and not the size of the organisation as a whole.

[16] (United Nations Statistics Division 2022)

[17] (McLaughlin 2022; Coalition 2022)

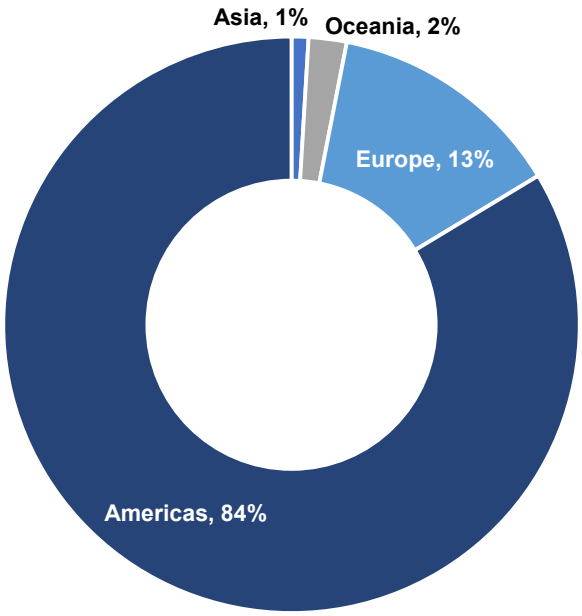


Figure 2: Region frequencies (Source: Cambridge Centre for Risk Studies).

Ransom Payments

The Aggregate Dataset has a total ransom demand of $249.38 million, with a total actual ransom payment of $147.87 million. For the Aggregate Dataset, there are 370 individual ransom payments made for the 303 unique ransom attacks, which includes test payments and payments made to separate Bitcoin wallets. The difference between the average and median is caused by outlier demands and payments. There are a handful of very low ransom demands by lone cyber extortionists in the data, along with small ransom payments made for "proof of life" or to show good faith in negotiations.

Table 1: Controls Subset Data Frequencies by Endpoint Tier (Source: Cambridge Centre for Risk Studies).

Organisation Infected Endpoint Tier	Controls Records by Tier
Tier 1: Up to 10 endpoints	6%
Tier 2: Up to 100 endpoints	52%
Tier 3: Up to 1,000 endpoints	39%
Tier 4: Over to 1,000 endpoints	3%

Table 2: Ransom Demand and Payment Statistics (Source: Cambridge Centre for Risk Studies).

Dataset Characteristics	Initial Demand	Ransom Paid
Count of Unique Ransom Events	93	303
Average	$2,681,500	$488,016
Median	$300,000	$90,937
Total	$249,379,482	$147,868,894

In 72% of the events in the databases, a ransom was paid. This figure is starkly different to those in other industry reports on the payment of ransoms. This is due to the source of this report's data being a ransom negotiation and recovery firm, which would not have been retained if the victim organisations were able to quickly recover from backups without the need to pay a ransom or even negotiate. Further, some victims only ever made a "proof of life" payment, but this is still counted as paid in the dataset. Verizon's 2022 DBIR reviewed ransom incidents and found that 60% of attacks didn't result in payment, leading them to liken ransomware to a lottery.[18]

Timeline of Ransom Events and Payments

The data demonstrates that quarter four (Q4) is the busiest quarter both in terms of frequency of events and in terms of the number of payments made. As a year, 2020 saw a higher number of attacks than 2021, the only other year with complete data in our dataset. This is likely due to the workplace changes resulting from COVID-19.

Interestingly, Q4 of 2021 shows a unique trend in that there were fewer ransom events which resulted in payment, yet the total ransom payments that were made account for the second largest quarter in the dataset. This could highlight that ransom payments are getting larger, a theory that has been recently supported by other research.[19]

[18] (Version 2022)

[19] (E. Leverett et al. 2022)

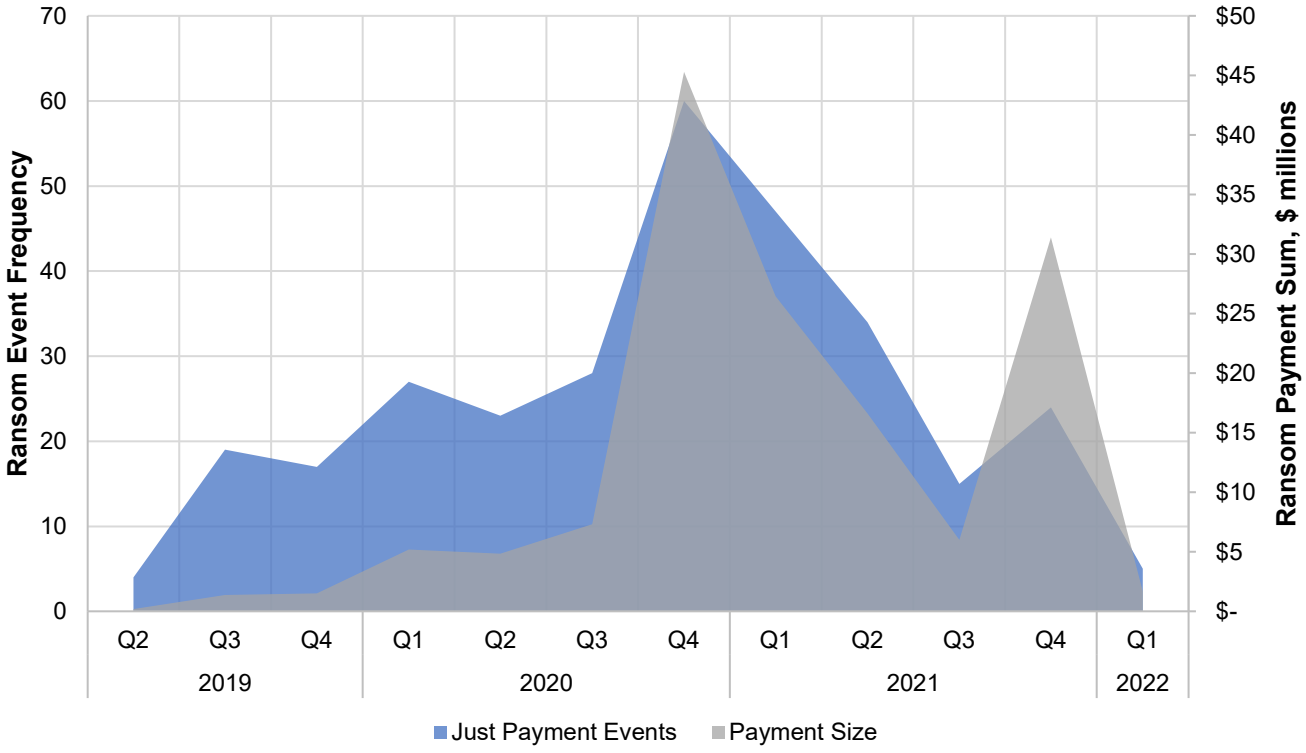


Figure 3: Ransom Event Frequency and Payment Size over Time (Source: Cambridge Centre for Risk Studies).[20]

[20] For ransom payments data only, does not include events where ransoms were not paid

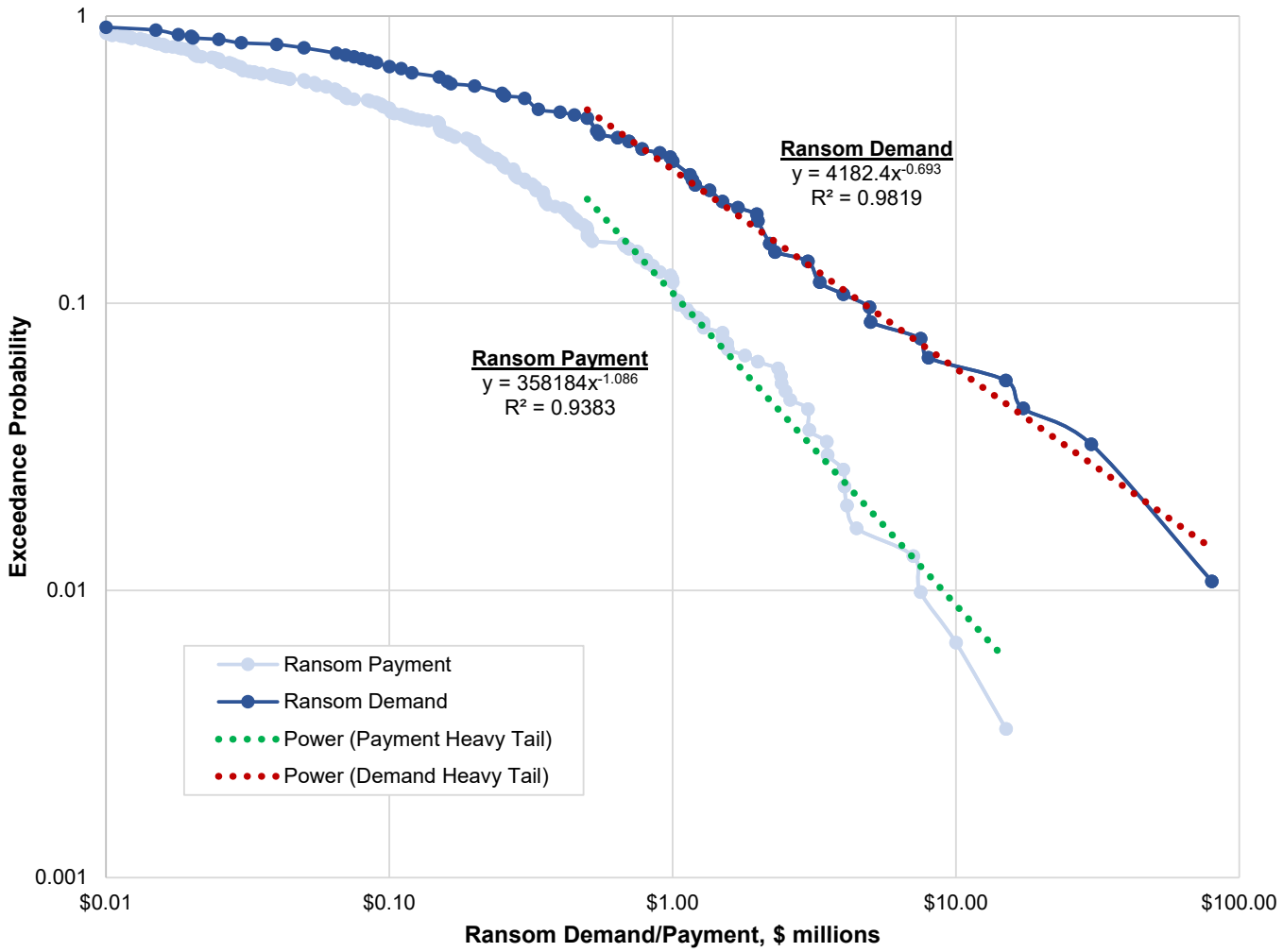


Figure 4: Exceedance probability curve for ransom demands and payments (Source: Cambridge Centre for Risk Studies).

Distribution of Ransom Payments

Leverett et al (2020) shows that ransom payments have heavy tails.[21] In this paper, the researchers fitted power law distributions to Bitcoin payment data between 2013-2019 with alpha values between 2.35 and 1.98. One caveat of their analysis was that the data included both organisation and individual user payments, which they attempted to account for by looking at only payments over $10,000. Our dataset is strictly organisations as opposed to a combination of individuals and organisations as was seem in the Leverett et al analysis, yet we still set the same lower threshold to remove any outlier payments.[22] Following this model, a power law was fit to the report's dataset of ransom demand and payment achieving an alpha of 0.693 to 1.086, respectively. This finding confirms that the distributions of ransom payments and even demands can be fitted with power laws and do indeed have very heavy tails. Further, this chart shows the value of negotiating amounts, as the exceedance probability curve has shifted greatly in terms of likelihood.

Ransomware Attributes

As part of the incident response data collection, Kivu has documented the ransomware name and/or variant in the ransom payment dataset. In the database under analysis, 68 variants of ransomware used for attacks are recorded, across a total of 303 unique ransom attacks. Ransomware variants have different characteristics just as different ransomware gangs have different strategies to achieve their goals.

Ransom Group Structure

In the analysis that follows, the various ransomware variants are grouped into higher level categories to reflect different ransom characteristic structures: RaaS, Closed Group and LOTL-Group. The definitions of these groupings are as follows:

- *RaaS* - Ransomware as a Service (RaaS) refers to a group known to have its own polymorphic

[21] (É. Leverett et al. 2020)

[22] 4 data points were removed for this analysis as we set our threshold to events with ransom payments larger than $10,000.

malware capabilities and also known to rent/sell that capability to other threat actors. Typically, this is done on a ransom share basis, but sometimes it is done for a flat fee.

- *Closed Group* - This category refers to a group who is known to create their own ransomware tooling but does not rent/sell that capability to others. They tend to work in small close-knit groups.
- *LOTL-Group* - Live off the Land group is a special categorisation for groups that do not use custom-made encryptors or reconnaissance tools, but instead use tools that can be found on common OS deployments. For example, groups who use BitLocker to encrypt computers, instead of their own bespoke software and tools.
- *Lone Actor* – This category refers to individual threat actors that are not affiliated with any group and unknown groups.

Ransom Pricing

The data note whether there is a way to contact the ransomware group as either Negotiated versus Non-Negotiated. If the ransom variant is marked as Negotiated, it has been identified that the ransom note states ways to contact the threat actors, for example, by chat, TOR onion site, or email. If there is no way of contacting the group recorded in the ransom note (for example DeadBolt), then the group is defined as Non-Negotiated ransoms. This refers to the group's general strategy of ransom collection, rather than specific incidents. For example, if DeadBolt negotiated a single ransom in the future, this categorisation would not change until a campaign where it embeds contact details into the ransom note had been observed. This is a relevant categorisation for historical analysis as past ransom notes have been reviewed for this categorisation.

LeakBlog Presence

The data also record whether the ransomware variant is connected to so-called "leak blogs", which are known sites that announce leaks like "conti.news".

This is typically indicative that the threat actor is using "double extortion" as a means to increase pressure on the victim to pay. This field is a boolean value, so either true or false.

Top Ransomware in Dataset by Frequency

Looking at all the 68 ransomware variants within the Aggregate Dataset, it can be seen that 62% of them have a LeakBlog presence. 49% have a group structure of RaaS, 47% have a Closed Group structure and just 4% have a LOTL-Group structure. Further, 94% of the ransomware variants accept negotiation on their pricing.

Table 3 shows the ransomware attributes of the top 15 ransomware variants by frequency according to our dataset, accounting for 68% of the events.[23] Within the top 15, 80% of the ransomware groups have a LeakBlog presence while all the top 15 ransomware variants by frequency have negotiable pricing, with the exception of those threat actors identified as Lone Actors. In the latter case, the size of demands and any willingness

[23] Lone Actors are included in the top 15 count as it is interesting to see how prevalent they are within the dataset, representing 3% of the total Aggregate Dataset.

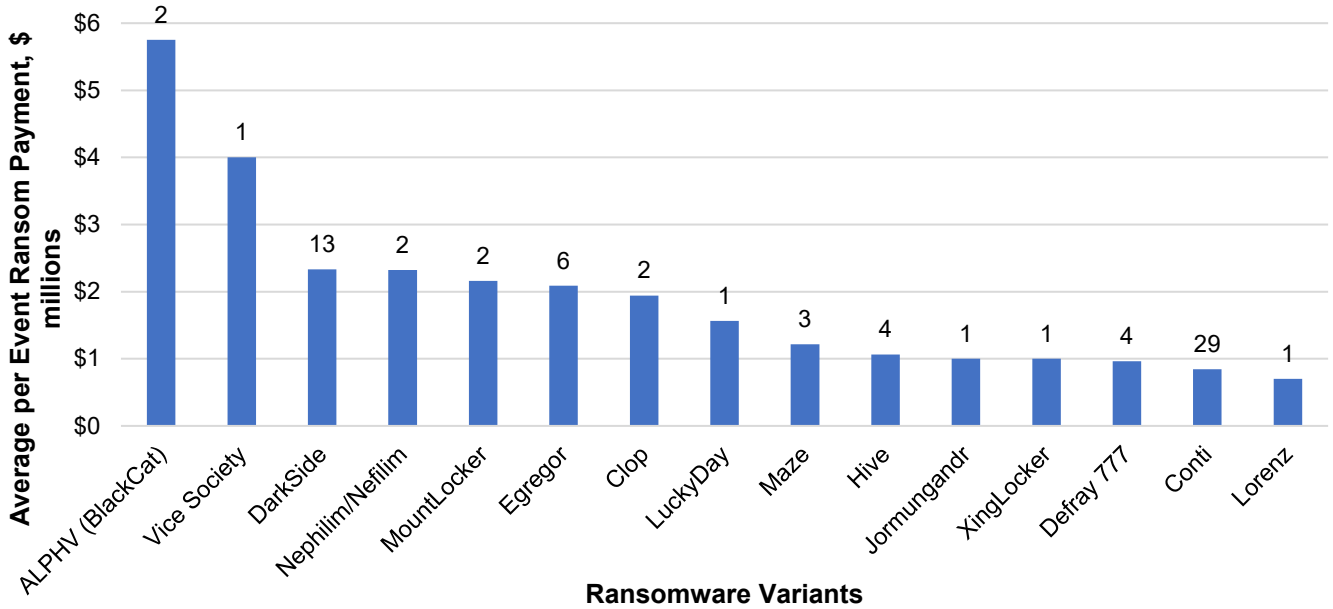


Figure 5: Average per event ransom payments for the top 15 variants with count of events (Source: Cambridge Centre for Risk Studies).

Table 3: Ransomware characteristics for top 15 most frequented ransomware variants (Source: Cambridge Centre for Risk Studies).

Rank	Top 15 Ransomware Variants	Count of Unique Ransom Events	LeakBlog Presence	Pricing Negotiation	Group Structure
1	Phobos/Dharma	41	FALSE	Negotiated	RAAS
2	Sodinokibi/REvil	31	TRUE	Negotiated	RAAS
3	Conti	29	TRUE	Negotiated	RAAS
4	Netwalker	16	TRUE	Negotiated	RAAS
5	DarkSide	13	TRUE	Negotiated	RAAS
6	Lone attacker – not known group	13	n/a	n/a	LONE ACTOR
7	Mamba	11	FALSE	Negotiated	LOTL-GROUP
8	LockBit	10	TRUE	Negotiated	RAAS
9	Ryuk	9	TRUE	Negotiated	RAAS
10	Snatch	9	TRUE	Negotiated	RAAS
11	Egregor	6	TRUE	Negotiated	RAAS
12	PYSA	6	TRUE	Negotiated	RAAS
13	Avaddon	5	TRUE	Negotiated	RAAS
14	Suncrypt	4	TRUE	Negotiated	RAAS
15	Hive	4	TRUE	Negotiated	RAAS

to negotiate have varied on a case-by-case basis, making it difficult to work out pricing strategies. Of the top 15 ransomware variants identified in the dataset, RaaS groups are 87%, Lone Actors 7%, and LOTL-Groups make-up 7%, which has seen a raise in the months following our analysis.

Ransomware vs Payments

In the previous section it was shown that the top ransomware variant was Phobos/Dharma by frequency. Another measure is to look at the total ransom payments per ransomware variants, which yields a top three of DarkSide, Conti and Egregor. Figure 6 shows the attributes of the top 10 ransomware variants that did the most extortionate damage ($ millions) per event, with the data label representing the count of events according to our database. It is clear from the figure that the correspondence between frequency (number of attacks) and the average ransom payment collected is not always respected. For example, ALPHV (BlackCat) with a frequency of 2, collected more money than Hive which has a frequency of 4. More specifically, ALPHV (BlackCat) collects on average $5.75 million per event, while Conti, who has a large number of events in the dataset, collect on average $0.85 million per event. This is in line with the reference literature, with the Coalition report suggesting the average ransom demand ranges from $3.5 to $0.6 million per event in the first half of 2022.[24]

[24] (Coalition 2022)

4 Cybersecurity Control Effectiveness and Cost Savings

Many organisations at the time of a ransomware attack do not know which assets may be at risk, how to protect them, or how to resolve the situation without suffering damage from business interruption or further extortion such as data exfiltration. This dataset is derived from first-hand experience of ransomware attacks on organisations assisted in the ransom negotiation and recovery phase, which makes it unique in the literature.

As previously discussed in the introduction, this paper defines the control effectiveness as the security or privacy risk reduction the control can provide for the ransomware threat. The risk reduction of the control effectiveness is then analysed in two parts: one which looks at controls that would have reduced the likelihood of the event occurring while the other examines the potential ransom payment cost savings.

Control Effectiveness

Control Frequency

Looking at the 183 records in the Effective Controls dataset, Control 8 (Malware Defences) is listed in 51% of the cases as one of three controls that could have prevented or mitigated the attack.

Control 4 (Controlled Use of Administrative Privileges) (46%) and Control 6 (Maintenance, Monitoring and Analysis of Audit Logs) (43%) complete the top three most effective controls. These controls are particularly good at blocking or limiting the impact of larger, more sophisticated attacks where the threat actor performs reconnaissance within the victim's network and incidents in which data is exfiltrated.

The least effective controls in terms of frequency are Control 18 (Application Software Security), Control 19 (Incident Response and Management), and Control 15 (Wireless Access Control), with the latter not listed as an effective control for any of the events. However, these observations are based on the specific Effective Controls Dataset in this study and the potential value of Application Software Security and Incident Response Controls in other circumstances is discussed below.

Organisations should consider implementing those controls and defences which combine the 3-4 controls classed as most important by this report. This strategy would allow those organisations to review and rebalance their defensive postures in near real-time as attack vectors change. Aggregating these

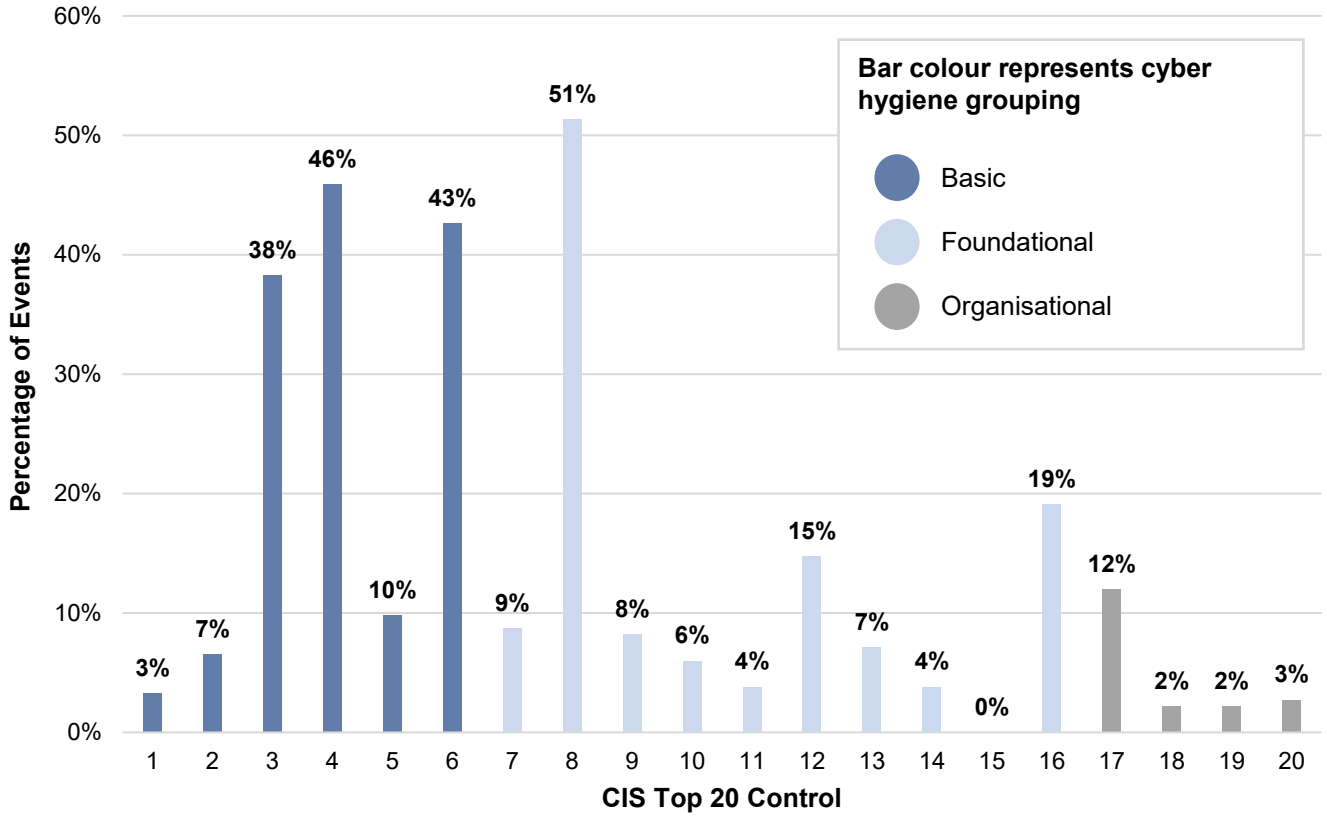


Figure 6: Chart of Control Effectiveness in Reducing Ransomware Risk (Source: Cambridge Centre for Risk Studies).

results further by grouping the controls into the high-level cyber hygiene categories of Basic, Foundational and Organisational, groupings of best-recommended mitigations begin to emerge.

The Basic category of Controls 1 to 6 represents the essential information technology (IT) related controls that organisations need to implement in order to protect themselves against cyber attacks. Foundational is the next step up in terms of risk maturity of IT systems and covers Controls 7 to 16. Finally, the Organisational grouping covers controls 17 to 20, are controls that are implemented at the organisational level and not at the IT system level.

The results demonstrate that the Basic cyber hygiene category needs further review by organisations to aid in event prevention or evenT limit impact. Interesting, the Organisational grouping is barely referenced at all in effective at-risk reduction, potentially because securing IT systems is more effective at-risk reduction than the introduction broad organisational reforms.

Table 4: CIS Cyber Hygiene Grouping by Control Effectiveness Frequency (Source: Cambridge Centre for Risk Studies).

CIS Cyber Hygiene Grouping	Frequency of Controls
Basic	53%
Foundational	43%
Organisational	7%

Incident Response Analyst Observations on Frequency

The following observations from the incident responders on control selection methods used during this study add some explanations to this report's findings.

Controls 1 (Inventory and Control of Hardware Assets) and Control 2 (Inventory and Control of Software Assets) - Hardware and software inventory management are important for determining what IT an organisation has, how it should protect it, and assess its vulnerability. The incident responders who collected this data typically had little visibility on this and the assumption was made for the purposes of this study that some form of inventory had been carried out in assessing the security posture of the organisation.

Control 4 (Controlled Use of Administrative Privileges) and Control 6 (Maintenance, Monitoring and Analysis of Audit Logs) – It is not always possible to determine the initial point of entry into an organisation's network. Even if the weak point can be traced to stolen credentials, it is possible that these were obtained by the attacker from an independent source and thus protecting against phishing or other means of obtaining credentials might not have been a useful control in every case. In the absence of knowing exactly how the threat actors first gained entry, Kivu's analysts looked to secondary controls (e.g. 4 & 6) which might have prevented or identified any unauthorized spread within the network.

Control 8 (Malware Defences) – This malware control gets the highest approval. However, several ransomware attacks either don't use malware at all or employ malware that runs in memory and would not be stopped by standard malware controls. One explanation for the high 51% finding for Control 8 is that it maps in CIS Top 18 v8 to Control 13, which includes EDR protection. This type of continuous monitoring and scanning wasn't given its own control in CIS Top 20 v7. See Breakout Box for further details.

Control 10 (Data Recovery Capabilities) – The relatively low value given to data recovery in this study (6%) is largely due to the nature of the dataset. In many of the cases under study, data recovery systems existed but were bypassed or destroyed by the threat actors, or were irrelevant in the case of data exfiltration where the extortion

Table 5: Top three control combinations (Source: Cambridge Centre for Risk Studies).

Combination Rank	Controls in Combination	Frequency in Dataset
1	• **Control 4 (Controlled Use of Administrative Privileges)** • **Control 6 (Maintenance, Monitoring and Analysis of Audit Logs** • **Control 8 (Malware Defences)**	11%
2	• **Control 3 (Continuous Vulnerability Management)** • **Control 4 (Controlled Use of Administrative Privileges)** • **Control 6 (Maintenance, Monitoring and Analysis of Audit Logs)**	9%
3	• **Control 3 (Continuous Vulnerability Management)** • **Control 4 (Controlled Use of Administrative Privileges)** • **Control 8 (Malware Defences)**	5%

Breakout Box – Control 8 (Malware Defences)

The observation that Control 8 (Malware Defences) would have prevented or limited the ransom event does not imply that organisations are not already aware of the significance of malware defences, but that inadequate deployment and lack of mature implementations lead to cyber complacency.

Conclusions around Control 8 ought to be caveated. In the last 5 years, there has been a rise in security tools that, while ostensibly relevant under Control 8, actually offer a variety of defences arguably best befitting other CIS v7 controls. For example, Endpoint Detection and Response (EDR) systems now often include vulnerability identification and remediation resources to supplement their anti-malware capabilities, and vulnerability scanning tools may now also perform asset discovery and asset inventory review.

This evolution in control systems can also be seen in the progression of the CIS taxonomy itself. The new CIS v8 controls taxonomy, released in May 2021, now includes a specific control on EDR (Control 13) while still having a control focused on Malware Defences (now notated as Control 10). Given the overlap of CIS v7 and v8 during the period of this study, the reference to CIS v7's Control 8 (Malware Defences) should be considered to include the correct use of EDR as a highly valuable tool in defending against many ransomware variants. The diagram below illustrates potential risk maturity levels for CIS v7 Control 8 (Malware Defences) using the sub-controls from the new CIS v8 taxonomy.

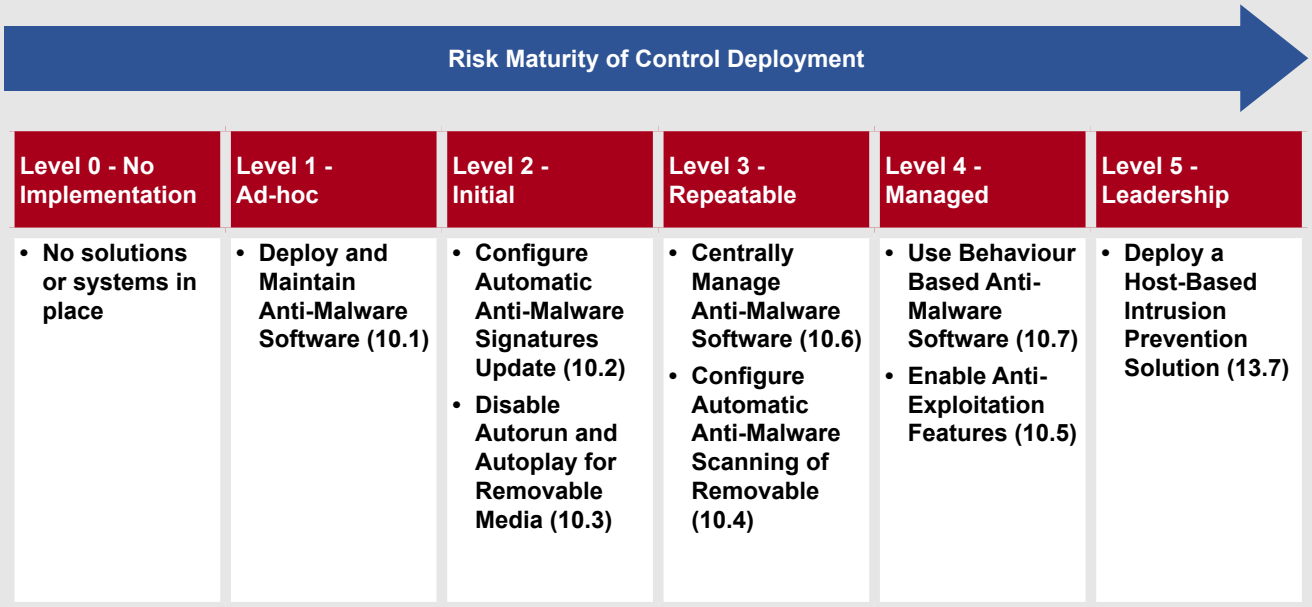


Figure 7: Control 8 (Malware Defences) risk maturity level descriptions, using sub-controls from CIS v8 (Source: Cambridge Centre for Risk Studies).

While there are very few ransomware incidents, particularly highly sophisticated "Big Game" attacks, which don't use any malware to gain access, the strong presence of malware (and thus the popularity of the Control) is a reflection of attack vectors used by many threat actors, especially those skilled in RaaS and other basic tools. Put simply, the availability of third-party malware lowers the skill required to engage in cyber crime and therefore makes it a more widely available option for would-be cyber criminals. Recognizing this in the risk model, the presence of any form of malware control will always be valuable as all organisations connected to the internet are highly likely to face a malware-based cyber threat at some point in their lifespan.

included the threat of publication, rather than a system lockout. It is conceded that with deeper factual analysis, unavailable to Kivu, large loss mitigation might have been achieved in some cases of solely encryption by better implementation of Control 10.

Control Combinations

Given that this report has examined data on the top three controls that would have prevented or limited an attack, the most effective combination of controls can be discerned in an attempt to help focus cyber security budgets. Controls 4, 6 and 8 are the combination this report best recommends, based on the findings. The next best combination is Control 3 (Continuous Vulnerability Management), Control 4 and Control 6.

Incident Response Analyst Observations on Combinations

This grouping of best recommended controls reflects the type of attack vectors most commonly used by threat actors, which can roughly be divided into two groups: trojans and vulnerability attacks.

Trojans are typically delivered by spam, phishing, or by downloads from malicious websites. For example, Conti has used Emotet, delivered by email, which is then used to download Trickbot or Qbot and acquire full control of a network. In these attacks, Control 7 (Email and Web Browser Protections) and Control 17 (Implement a Security Awareness and Training Program) would be useful. However, most of victim organisations in the dataset have adopted these controls to some degree, and it is far from certain that additional focus on those controls would have prevented the attack. Credentials might have been stolen elsewhere and training, even if relevant, may likely not have provided 100% protection. Instead, Kivu's analysts focused on controls that would have stopped the spread, raised the alarm, or mitigated the damage. This explains the identification of Control 4 (Controlled Use of Administrative Privileges), which would have slowed the attack by restricting admin privileges, and Control 6 (Maintenance, Monitoring and Analysis of Audit Logs), which would increase the chance of discovery by monitoring audit logs for suspicious behaviour within the network. While a strict interpretation of Control 8 (Malware Defences) would reduce the value of this control, especially as many threat actors are not using identifiable malware executables, a wider interpretation of Control 8 (and mapping it to Control 13.7 (Deploy a Host-Based Intrusion Prevention Solution) of CIS v8, provides an even broader defence of a network via an EDR system.

A wide range of controls exist to provide best defence against Remote Desktop Protocol (RDP)/Virtual Private Network (VPN)/network vulnerability attacks such as Phobos/Dharma, Darkside, and Snatch. Multi-factor authentication (MFA), while specifically referenced under CIS v8 as Control 6 (Access Control Management), maps to Control 4 (Controlled Use of Administrative Privileges) and to a lesser extent Control 14 (Controlled Access Based on the Need to Know) in CIS v7, used in this study. Control 4 also provides a key benefit of locking down admin privileges which will limit both reconnaissance and spread as threat actors attempt to escalate their original access level. Finally, vulnerability assessment within Control 3 (Continuous Vulnerability Management) can entirely protect the original point of access, while suspicious activity could have been spotted with Control 6 (Maintenance, Monitoring and Analysis of Audit Logs).

The above examples explain the grouping of Controls 3, 4 and 6 for mitigating attacks focused on RDP/VPN/vulnerabilities and LOTL threat actors who use tools leverage average IT infrastructure weaknesses, without needing to introduce new tools via malware.

Cross referencing this with the actual cases in the datasets, Controls 3, 4 and 6 cluster in cases including the Fortinet Zero Day vulnerability and the large number of cases in June 2021 involving vulnerabilities on Exchange Servers where threat actors used web shell attacks to gain access to networks.

By contrast, in cases where the use of Emotet/Qbot (droppers) is identified, e.g. in many of the Conti cases, Kivu's response analysts decision to highlight Control 4, 6 and 8 and bypass Control 10 (data recovery) was likely dictated by attackers using double extortion, threatening to publicise exfiltrated data – thus data recovery, even if successful, would not completely resolve the extortion.

Further, many ransomware groups, including Sodinokibi, Conti and Lockbit, use multiple types of attack vectors, also called techniques, tactics, and procedures (TTPs), so mapping defences to ransomware variants is less important than mapping these to the type(s) of TTPs used by the groups.

Control Frequency by Sector

The frequencies between sectors and CIS controls are shown in Figure 8. This heatmap provides the control number on the x-axis, with the corresponding frequency for sectors along the y-axis.

Agnostic of sector, Controls 3, 4, 6 and 8 are demonstrably and universally effective in reducing risk. The greatest threats in the dataset are, therefore, shown to be more controllable with the implementation of systems against vulnerabilities, administrative privilege controls, monitoring of audit

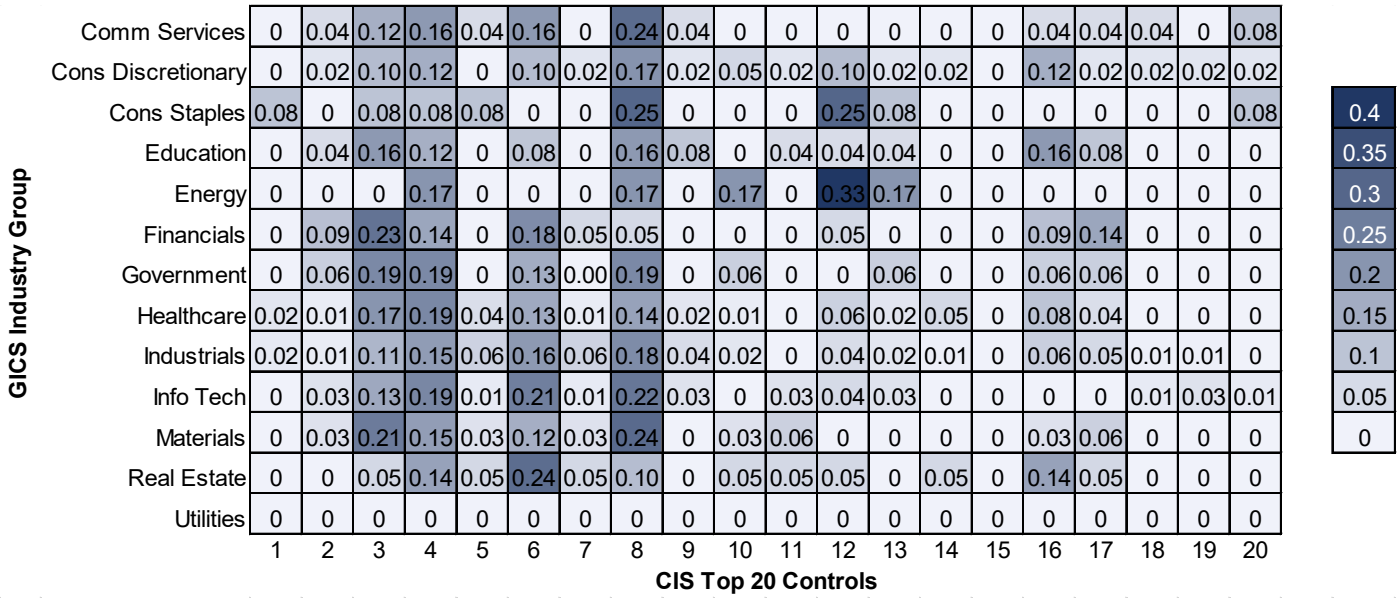


Figure 8: Effective controls versus organisation sector heatmap (Source: Cambridge Centre for Risk Studies).

logs, and strengthening of malware defences. Of these four controls, three sit in the Basic cyber hygiene grouping. Note that the Energy and Consumer Staples sectors register the lowest number of applicable controls and that this is due to the scarcity of samples in the dataset belonging to those sectors.[25]

Interestingly, for the Energy and Consumer Staples sectors Control 12 (Boundary Defence) has the highest frequency, indicating these sectors struggle with proper implementation of air gaps given the age and complexity of IT and OT systems. The Education sector sees a three-way tie between Controls 3, 8 and 16 (Account Monitoring and Control), which can be explained by the vast number of users on their networks. Finally, Healthcare requires improvement in the implementation of Control 4 (Controlled Use of Administrative Privileges). Control 4 in CIS v7 maps to Control 6 in CIS v8 which would indicate that the proper use of MFA is a key defence in these type of attacks.

It is remarkable that Controls 1, 14, 15, 18, 19 and 20 are scarcely present among the different sectors with the later three representing all but one of the Organisational hygiene control grouping. This shows less efficacy of Organisational controls within the context of the dataset.

Incident Response Analyst Observations on Sector Findings

The negative position this report adopts regarding Control 18 (Application Software Security) should be caveated. Poor application security is an indirect cause of almost every security incident where a software vulnerability is exploited and therefore application security is of vital importance across the cyber ecosystem. However, the organisations in the datasets were mainly mid-cap and typically harmed by the lack of application security in third party products, rather than their own lack of application security.

Controls 19 (Incident Response and Management) and Control 20 (Penetration Tests and Red Team Exercises) typically existed and had been implemented to some degree in the victim organisations under study. The problem is that Control 19 and 20 in isolation are not evidenced to prevent the attacks in question. However, it is accepted that had there been no incident response management or plan in place, the situation would have been significantly worse.

Control Cost Savings

The Ransom Payment Dataset and the Effective Controls Dataset were joined on events where both a ransom was paid and effective controls were identified. To examine the potential ransom payment cost savings per control, the three identified controls per event were assigned a third of the value of the ransom paid. Without any ranking between the three assigned controls, this was the best solution. It should be noted that ransom payments are just one of many costs organisations face when hit with a ransomware event. Other costs can include business interruption, incident responses costs, legal fees and so on. This additional event cost data was not collected during the study and thus the ransom payment size is the best proxy for event cost savings with this dataset.

[25] To clarify on the consistency of the samples for each sector, frequencies are reported in Figure 2.

Figure 9 shows the cost effectiveness of implementing each control properly. The x-axis presents the range of potential savings for each control versus the average of the ransom payment in conditions where the control is implemented properly or at higher maturity level. The higher up the x-axis the bubble, the greater the savings potential. The bubble size shows the number of events in the dataset with the plotted average ransom payment size, and thus this acts as a confidence bound on the data, the larger the bubble the more confident we are in the cost effectiveness. The colour represents the classification of the controls by cyber hygiene category.

This figure shows that, in terms of potential cost savings, Control 19 (Incident Response and Management) has the highest potential cost savings of $333k, though this conclusion is drawn from one event observation. Control 19 did not feature in the top ranking when examining frequency of controls per event, but now through the lens of cost savings, it is ranked number one. Control 3 (Continuous Vulnerability Management) is the next most cost effective control in this study, with a potential savings of $238k and with a significant number of observations supporting this assessment. Control 6 (Maintenance, Monitoring and Analysis of Audit Logs) is ranked third in terms of frequency as well as in cost effectiveness, with a potential savings of $197k. Control 8, which was ranked first in terms of frequency, is now ranked twelfth with a cost savings potential of just $87k. Finally, Control 4 (Controlled Use of Administrative Privileges) which was rated second in terms of frequency is now seventh, offering $155k of potential savings.

In terms of the least effective controls, Control 15 (Wireless Access Control) and Control 18 (Application Software Security) are not referenced in this dataset. The controls that make up the bottom four in terms of cost savings potential, all with savings less than $18k are:

- Control 1 (Inventory Management of Hardware Assets)
- Control 14 (Controlled Access Based on the Need to Know)
- Control 20 (Penetration Tests and Red Team Exercises)
- Control 2 (Inventory Management of Software Assets)

Discussion on Control Effectiveness and Cost Savings Findings

Academic literature on control effectiveness is scarce and approaches to the question vary depending on the underlying definition of "control effectiveness". Other definitions tend to focus on the effective implementation/deployment of the control or whether the control contributes "to the reduction of information security or privacy risk" or both.[26] For the purposes of this paper, control effectiveness is considered in terms of the security or privacy risk reduction the control can provide for the ransomware threat and not the measure of how effective a control is deployed or implemented.

[26] NIST and Computer and Security Resource Center 2022a; 2022b

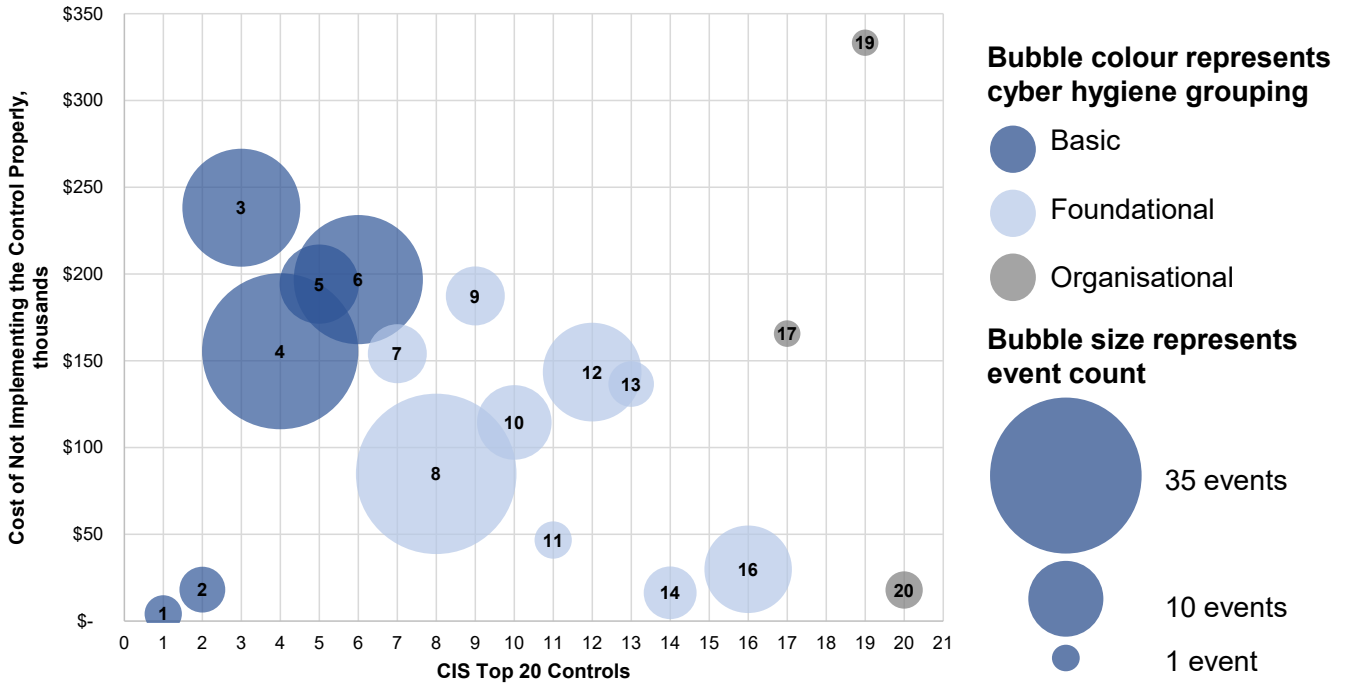


Figure 9: Cost Effectiveness of Implementing Controls Properly (Source: Cambridge Centre for Risk Studies).

Table 6: Survey Results on Deployment and Effectiveness of Controls using CIS v7 (Source: Axon et al. 2021).

Most Deployed	Most Effective

• Control 8 (Malware Defences) was unanimously considered to be deployed "often" or "almost always"
• Followed by these controls which were on average are considered to be deployed "often" and "almost always"
  • Control 12 (Boundary Defence)
  • Control 7 (Email and Web Browser Protections)
  • Control 11 (Secure Configuration for Network Devices, such as Firewalls, Routers and Switches)
	• Control 3 (Continuous Vulnerability Management)
	• Control 4 (Controlled Use of Administrative Privileges)
	• Control 19 (Incident Response and Management)

Least Deployed	**Least Effective**
• Control 3 (Continuous Vulnerability Management) • Control 18 (Application Software Security) • Control 19 (Incident Response and Management)	• No clear result was attested on "least effective" controls

Table 7: Control Combinations with highest effectiveness and cost-effectiveness (Source: Such et al. 2016).

Rank	Control combinations with highest perceived effectiveness
1	Red Team Exercise; Penetration Tests; Dynamic Analysis; Fuzzing
2	Red Team Exercise; Penetration Tests; Vulnerability Scan; Social Engineering
3	Architectural Review; Configuration Review; Penetration Tests; Vulnerability Scan
4	Review of Documented Policies; Procedures and Processes; Architectural Review; Configuration Review; Penetration Tests
Rank	**Control combinations with highest perceived cost-effectiveness**
1	Architectural Review; Configuration Review; Penetration Tests; Vulnerability Scan
2	Review of Documented Policies, Procedures and Processes; Architectural Review; Configuration Review; Penetration Tests
3	Review of Documented Policies, Procedures and Processes; Observation; Social Engineering; Threat Assessment
4	Review of Documented Policies, Procedures and Processes; Architectural Review; Interview; Threat Assessment
5	Architectural Review; Static Analysis; Dynamic Analysis; Fuzzing

Measuring control effectiveness is challenging for several reasons. Firstly, the effectiveness of controls is highly context specific and varies over time.[27] Secondly, controls are interdependent; the control effectiveness of one control depends on the correct deployment of another controls.[28] Common methods to capture perceived control effectiveness are interviews and surveys.

Axon et al. (2021) assesses the perceived effectiveness and frequency of deployment of cybersecurity controls by 30 security practitioners via an online survey and semi-structured interviews.[29] The online survey required the participant to assign effectiveness levels (*very ineffective*, *effective*, *neutral*, *effective*, *very effective*) and frequency of deployment (almost never, rarely, neutral, often, almost always) on a five point Likert scale to CIS v7. Table 6 shows the survey results by deployment frequency and effectiveness. The semi-structured interviews provided deeper understanding of the perception and deployment of the controls.

When comparing these survey findings from Axon et al. (2021) with the data-based findings in this paper, some alignment between the most effective controls can be observed. Both rank Control 19 (Incident Response Management) and Control 3 (Continuous Vulnerability Management) among the top three most effective controls at reducing risk.

Such et al. (2016) assesses the perceived effectiveness and perceived cost of 20 assurance techniques as well as their interdependencies by 153 industry

[27] (Axon et al. 2021)

[28] (Agrafiotis, Ioannis et al. 2016)

[29] (Axon et al. 2021)

stakeholders in an online survey.[30] The controls that were rated most effective were: Red Team Exercise, Penetration Test, Social Engineering, and Architectural Review. The controls with the highest perceived costs were: Source Code Review, Red Team Exercise, Formal Verification and Cryptographic Validation. In addition to individually perceived effectiveness and costs, survey participants were asked to assign each control a first, a second and a third most complimentary control. Based on this collected data, the authors then proceeded to calculate the most effective and most cost-effective control combinations, see Table 7.

It is more difficult to compare this study with Such et al. (2016) as the latter is specifically looking at assurance techniques and not at the wider security landscape, but does feature Vulnerability Scan in its effective control combinations which features in this report's top three. Further, Social Engineering is at the top of Such et al.'s list which relates to Control 17 on Implement a Security Awareness and Training Program which ranks in the middle of the rankings from our analysis, showing less alignment possibly due to the nature of the survey questions. Such et al. (2016) show that Penetration and Red Team Exercises, which aligns with Control 20 in the CIS v7, is highly effective, while this study finds these mitigations least effective both in terms of likelihood reduction and cost savings. While Red Team Exercises and Penetration Tests enable identification of other control deployment/implementation misalignments or gaps prior to security events ever occurring, this control does not directly aid in event risk reduction itself. For example, during a Penetration Test, it might be identified that the organisation needs to improve the implementation of Control 12 (Boundary Defence). When an event occurs, it is Control 12 that prevents or limits the event and not Control 20.

Finally, the recent joint cybersecurity advisory on effective controls to limit initial access done in collaboration with the United States, Canada, New Zealand, Netherlands and United Kingdom governments highlights the need for Control 3, 4, 5, 6, 8 and 16.[31] All of these recommended controls are the top ranked controls from this report's analysis with the exception of Control 5 on Configuration Management.

[30] (Such et al. 2016)

[31] (CISA et al. 2022)

5 Conclusions

This paper has fully explored the insights derived from a unique dataset of ransomware attacks carried out by different threat actors since May 2019. The originality of the dataset is in offering an aggregate of 422 attacks carried out on 416 organisations that entered an incident response phase. This phase consists of identifying the attack, scanning the compromised systems and data, and negotiating (where possible) for ransom. All this emerges in the paper's analysis, which shows:

- Different ransom payment strategies
- Different threat actors at work
- Different sectors/countries affected in terms of frequency
- Different controls identified as effective at reducing the risk or increasing the cost savings

CISOs, CROs and risk managers can use this work to empower and underpin discussions on their security posture and current attack method preparedness. The dataset has mapped out the top three controls that would have been effective according to the incident response analyst directly involved in the case. Internal discussions can focus on optimizing security spend for either,

- event likelihood reduction, or,
- event cost savings, or,
- both.

Event Likelihood Reduction

LLooking at the 183 records in the Effective Controls dataset and looking at the statistics for each control recommended as opposed to the best combination of controls, Control 8 (Malware Defences) prevails in 51% of the events as one of three controls that could have prevented or mitigated the attack, and is thus most effective at reducing the likelihood of the risk. Control 4 (Controlled Use of Administrative Privileges) (46%) and Control 6 (Maintenance, Monitoring and Analysis of Audit Logs) (43%) round out the top three controls for event likelihood reduction. These controls are particularly good at blocking or limiting the impact of larger, more sophisticated attacks where the threat actor carries out reconnaissance within the victim's network and exfiltrates data from the system.

This report also looks at the combination of the three controls recommended for event likelihood reduction and finds that the optimal controls combination is Control 4 (Controlled Use of Administrative Privileges), Control 6 (Maintenance, Monitoring and Analysis of Audit Logs) and Control 8 (Malware Defences), accounting for 11% of the events in the dataset. This implies that Control 4, Control 6 and Control 8 form a very effective barrier against ransomware events when deployed together. The next best combination is Control 3 (Continuous Vulnerability Management), Control 4 and Control 6, accounting for 9% of the dataset.

Event Cost Savings

The study finds that the controls with the greatest potential event cost savings are Control 19 (Incident Response and Management) with the highest potential cost savings of $333k, Control 3 (Continuous Vulnerability Management) is the next most cost effective with a potential savings of $238k and Control 6 (Maintenance, Monitoring and Analysis of Audit Logs) with a potential savings of $197k. The controls with the smallest cost savings potential are Control 1 (Inventory Management of Hardware Assets), Control 14 (Controlled Access Based on the Need to Know) and Control 20 (Penetration Tests and Red Team Exercises), all with a cost savings less than $18k.

Internal discussions should also focus on verification of whether the controls have been deployed correctly and to what level they have been implemented within the organisation. It should also be strongly emphasised that the TTPs used by the threat actors are always changing and evolving, with many ransomware groups using multiple TTPs, so mapping defences to ransomware variants is less important than mapping these to TTPs used by the active groups. There is a strong correlation between certain sets of controls and specific TTPs, meaning that defences need to be regularly reviewed and revised as threat actors change their modes of gaining access to networks. This study provides a view on the effective controls from 2019-2022 data.

While the dataset and analysis are novel in the academic space, data asymmetry exists within this analysis and thus limits the overall interpretation. The lack of data on cyber risk is a clear challenge for both cyber security professionals and the cyber insurance industry.[32] Swift action is needed to develop a live comprehensive data feed that replicates this analysis to aid in real-time cyber security control investment decision making. These results are shared with the reader to provoke discussion and potentially further research in this area.

[32] (Cremer et al. 2022)

6 References

Agrafiotis, Ioannis, Creese, Sadie, Goldsmith, Michael, Jason R. C. Nurse, and Upton, David. 2016. "The Relative Effectiveness of Widely Used Risk Controls and the Real Value of Compliance."

AON. 2022. "Rethinking an organisation's Approach to Risk Management in the New Normal." RIMS and UCLA Extension.

Associated Press. 2022. "Costa Rica, 'under Assault' Is a Troubling Test Case on Ransomware Attacks." NBC News. June 17, 2022. https://www.nbcnews.com/news/latino/costa-rica-assault-troubling-test-case-ransomware-attacks-rcna34083.

Axon, Louise, Arnau Erola, Alastair Janse van Rensburg, Jason R. C. Nurse, Michael Goldsmith, and Sadie Creese. 2021. "Practitioners' Views on Cybersecurity Control Adoption and Effectiveness." In The 16th International Conference on Availability, Reliability and Security, 1–10. Vienna Austria: ACM. https://doi.org/10.1145/3465481.3470038.

Beaman, Craig, Ashley Barkworth, Toluwalope David Akande, Saqib Hakak, and Muhammad Khurram Khan. 2021. "Ransomware: Recent Advances, Analysis, Challenges and Future Research Directions." Computers & Security 111 (December): 102490. https://doi.org/10.1016/j.cose.2021.102490.

BitSight Technologies. 2021. "Ransomware: The Rapidly Evolving Trend." BitSight. 2021. https://info.bitsight.com/ransomware-the-rapidly-evolving-trend.

Center for Internet Security. 2021. "Learn about the CIS ControlsTM." CIS. 2021. https://www.cisecurity.org/controls/v7/.

———. 2022. "Alert: Log4j Zero-Day Vulnerability Response." CIS. January 7, 2022. https://www.cisecurity.org/log4j-zero-day-vulnerability-response/.

Chubb. 2022. "Chubb Cyber Index: Providing Data Driven Insight on Cyber Threat Trends." 2022. https://chubbcyberindex.com.

CIS. 2021. "Learn about the CIS Controls." CIS. 2021. https://www.cisecurity.org/controls/v7/.

CISA, FBI, NSA, CCCS, NCSC-NZ, NCSC-NL, and NSCS-UK. 2022. "Weak Security Controls and Practices Routinely Exploited for Initial Access." https://media.defense.gov/2022/May/17/2002998718/-1/-1/0/CSA_WEAK_SECURITY_CONTROLS_PRACTICES_EXPLOITED_FOR_INITIAL_ACCESS.PDF.

Coalition. 2022. "2022 Mid-Year Update Report on Cyber Claims." 2022. https://info.coalitioninc.com/download-2022-cyber-claims-report-mid-year-update.html.

Corera, Gordon. 2021. "Irish Health Cyber-Attack Could Have Been Even Worse, Report Says." BBC News, December 10, 2021, sec. Technology. https://www.bbc.com/news/technology-59612917.

Cremer, Frank, Barry Sheehan, Michael Fortmann, Arash N. Kia, Martin Mullins, Finbarr Murphy, and Stefan Marterne. 2022. "Cyber Risk and Cybersecurity: A Systematic Review of Data Availability." Geneva Pap Risk Insur Issues Pract. 47 (3): 698–736. https://doi.org/10.1057/s41288-022-00266-6.

Leverett, Eireann, Erin Burns, Bakuei Matsukawa, Vladimir Kropotov, Fyodor Yarochkin, Robert McArdle, and Shingo Matsugaya. 2022. "Ransomware as a Science." In FIRSTCON22. Dublin, Ireland. https://www.first.org/resources/papers/conf2022/FIRST22_RansomwareasaScience_TLP_WHITE_WITHOUT_SOME_SLIDES.pdf.

Leverett, Éireann, Eric Jardine, Erin Burns, Ankit Gangwal, and Dan Geer. 2020. "Averages Don't Characterise the Heavy Tails of Ransoms." In 2020 APWG Symposium on Electronic Crime Research (ECrime), 1–12. https://doi.org/10.1109/eCrime51433.2020.9493256.

McLaughlin, Jenna. 2022. "Ransomware Attacks Are Hitting Small Businesses. These Are Experts' Top Defense Tips." NPR, August 12, 2022, sec. Technology. https://www.npr.org/2022/08/12/1116936751/what-experts-think-companies-should-do-when-ransomware-strikes.

MITRE ATT&CK. 2021. "Mitigations - Enterprise." 2021. https://attack.mitre.org/mitigations/enterprise/.

Naimisha. 2022. "Impact of the Russian-Ukraine Conflict on Cybersecurity." Security Boulevard (blog). May 2, 2022. https://securityboulevard.

com/2022/05/impact-of-the-russian-ukraine-conflict-on-cybersecurity/.

Nast, Condé. 2022. “Russia Is Being Hacked at an Unprecedented Scale.” Wired UK, April 27, 2022. https://www.wired.co.uk/article/russia-hacked-attacks.

NIST, and Computer and Security Resource Center. 2022a. “Control Effectiveness - Glossary.” 2022. https://csrc.nist.gov/glossary/term/control_effectiveness.

———. 2022b. “Security Control Effectiveness - Glossary.” 2022. https://csrc.nist.gov/glossary/term/security_control_effectiveness.

NIST Joint Task Force Interagency Working Group. 2020. “Security and Privacy Controls for Information Systems and organisations.” Revision 5. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5.

NIST SP 800-53 Rev. 5. 2020.

Oz, Harun, Ahmet Aris, Albert Levi, and A. Selcuk Uluagac. 2022. “A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions.” ACM Computing Surveys, January. https://doi.org/10.1145/3514229.

Ralph, Oliver. 2019. “Data Hacks and Big Fines Drive Cyber Insurance Growth.” Financial Times, November 20, 2019.

S&P Global. 2018. “Global Industry Classification Standard.” 2018. https://www.spglobal.com/marketintelligence/en/documents/112727-gics-mapbook_2018_v3_letter_digitalspreads.pdf.

Such, Jose M., Antonios Gouglidis, William Knowles, Gaurav Misra, and Awais Rashid. 2016. “Information Assurance Techniques: Perceived Cost Effectiveness.” Computers & Security 60 (July): 117–33. https://doi.org/10.1016/j.cose.2016.03.009.

United Nations Statistics Division. 2022. “Methodology - Standard Country or Area Codes for Statistical Use (M49).” 2022. https://unstats.un.org/unsd/methodology/m49/.

US Department of Health and Human Services. 2022. “Lessons Learned from the HSE Cyber Attack.” TLP: WHITE, ID# 202202031300. Leadership for IT Security & Privacy Across HHS Cybersecurity Program. Office of Information Security. https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf.

Vail, Emma. 2022. “Russia or Ukraine: Hacking Groups Take Sides.” The Record by Recorded Future (blog). February 25, 2022. https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/.

Version. 2022. “2022 Data Breach Investigations Report.” https://www.verizon.com/business/resources/reports/dbir/.

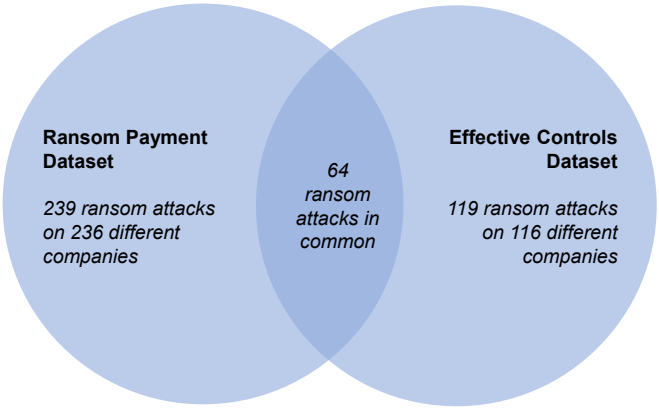
WatchGuard Technologies. 2022. Internet Security Report - Q1 2022. https://www.watchguard.com/wgrd-resource-center/security-report-q1-2022.

7 Appendix

Data Venn Diagram

The following Venn Diagram shows the relationship between the two data sets, one on ransom payment events and the other on effective controls events.

Figure 10: Ransom Payment and Controls Dataset Characteristics (Source: Cambridge Centre for Risk Studies).



Threat Actor Definitions

The report uses "threat actors" as a general definition of an attacker. The term "hackers/gangs" does not clearly articulate the scope other than to mean it's more than one person, which in 99% of attacks, is likely the case anyway. Threat actors are defined either by motivation or expertise, as summarised in Table 8. As observed with North Korea, threat actors can share motivations between political influence and financial theft.

Victim/Target Definitions

The report uses the term "victim" to mean "targeted organisation" as the latter implies that the organisation which suffered the attack was specifically chosen by the threat actor. However, in many cases, the organisation was one of many that had a vulnerability that led to a compromise of its system. In addition, many systems are initially compromised by criminals specialising in gaining access and then selling the compromised credentials through so-called Access Brokers on the Dark Web, with a price determined by the size or nature of the compromised organisation.

CIS v7 Definitions

Table 9 lists the CIS v7 with working control definitions from the CIS documentation.

Table 8: Threat Actor Motivations and Expertise.

Motivations	Expertise
• **Nation-state goals** – push political agenda of recognized nation state with cooperation of that state (e.g. North Korean military, state funded Russian threat actors) • **Financial** – primary goal is making money, even if they favour certain countries (e.g. not attacking Russian companies) • **Political/Social goals** – pushed by groups not aligned/ cooperating with a specific nation state (e.g. hacktivists supporting Ukraine or environmental issues)	• **Advanced Persistent Threats (APTs)** – either funded by nation states or using tools generally only available to nation state actors • **Organised criminal groups** – having ability to use multiple different skill sets/tools, and have the logistics to attack multiple victims over period(s) of time, may be more/less technically proficient • **Hackers** – heavy reliance on technical expertise and technical vulnerabilities • **Individuals** – low to medium technical expertise, not part of a larger criminal gang which can assist with tools/money laundering, includes disgruntled employees

Table 9: CIS Controls, v7 (Source: CIS, 2021).

Control #	Group	CIS Top 20 Security Controls	Definition
1	Basic	Inventory and Control of Hardware Assets	Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
2	Basic	Inventory and Control of Software Assets	Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.
3	Basic	Continuous Vulnerability Management	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.
4	Basic	Controlled Use of Administrative Privileges	The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
5	Basic	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
6	Basic	Maintenance, Monitoring and Analysis of Audit Logs	Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
7	Foundational	Email and Web Browser Protections	Minimize the attack surface and the opportunities for attackers to manipulate human behaviour though their interaction with web browsers and email systems.
8	Foundational	Malware Defences	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defence, data gathering, and corrective action.
9	Foundational	Limitation and Control of Network Ports, Protocols, and Services	Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.
10	Foundational	Data Recovery Capabilities	The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.
11	Foundational	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
12	Foundational	Boundary Defence	Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.
13	Foundational	Data Protection	The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.
14	Foundational	Controlled Access Based on the Need to Know	The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.
15	Foundational	Wireless Access Control	The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.
16	Foundational	Account Monitoring and Control	Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.
17	Organisational	Implement a Security Awareness and Training Program	For all functional roles in the organisation (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defence of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organisational planning, training, and awareness programs.
18	Organisational	Application Software Security	Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.
19	Organisational	Incident Response and Management	Protect the organisation's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.
20	Organisational	Penetration Tests and Red Team Exercises	Test the overall strength of an organisation's defence (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

Cambridge Centre for Risk Studies
Cambridge Judge Business School
University of Cambridge
Trumpington Street
Cambridge
CB2 1AG

T: +44 (0) 1223 768386
F: +44 (0) 1223 339701
enquiries.risk@jbs.cam.ac.uk
www.risk.jbs.cam.ac.uk

Join our LinkedIn group at Cambridge Centre for Risk Studies

Follow us @Risk_Cambridge