UKaid
from the British people

KPMG

Queen Mary
University of London

Improving Resilience to Ransomware with Cybersecurity Capacity Building

November 2022

Authors

Maria Bada
Lecturer at QMUL,
Cybersecurity & Cybercrime

E: m.bada@qmul.ac.uk

Maria Bada is a Lecturer at Queen Mary University in London and a KPMG Associate. Her work focuses on cybersecurity capacity building and the human aspects of cybercrime and cybersecurity. She has collaborated with government, law enforcement and private sector organisations to assess national level cybersecurity capacity and develop interventions to enhance resilience. She has also supported National Cyber Security Strategy development for the UK government and governments in Europe, Africa, Asia and Latin America. She is a member of the National Risk Assessment (NRA) Behavioural Science Expert Group in the UK, working on the social and psychological impact of cyber-attacks on members of the public.

Nathan Steuer
Assistant Manager, Cyber Incident Response, KPMG UK

E: nathan.steuer@kpmg.co.uk

Nathan Steuer is a Cybersecurity Consultant at KPMG UK working within the firm's Infrastructure, Government and Healthcare practice. As a member of the Cyber Response Services team, he conducts incident handling procedures including remediation, analysis and recovery from ransomware attacks and other cybersecurity threats. Nathan has led security innovation initiatives for a number of public and private sector clients and has delivered technical security training and awareness campaigns for stakeholders at many experience levels.

Ravi Jayanti
Manager, Cyber Risk & Strategy, KPMG UK

E: ravi.jayanti@kpmg.co.uk

Ravi Jayanti is a Manager in KPMG UK's cybersecurity consulting team with five years' experience in cyber third party risk management, target operating model design, threat and regulatory intelligence reporting, and business resilience. Ravi works with clients across financial services, healthcare and government sectors, and spent one year supporting KPMG International's global cyber innovation strategy. He has contributed to multiple white papers and international working groups on strategic challenges in cyber, and has a specialist knowledge in the interaction of cybersecurity with geopolitics, public policymaking and regulation. He has a keen interest in the role of public-private partnerships in active threat hunting and community defence.

The Advisory Group

An Advisory Group was established to provide technical and strategic expertise to the authors of the paper. The group consisted of the following members:

- **John Ashdown**
(Cyber Senior Manager, KPMG UK)
- **Laura Baldwin**
(Cyber Policy Department, FCDO)
- **Mike Bazett**
(Transformation Director, KPMG UK)
- **David Ferbrache**
(Global Head of Cyber Futures, KPMG International)
- **Jemima Hodkinson**
(Head of International Cybersecurity Programme, FCDO)
- **Richard Krishnan**
(Technology and Cyber Risk Partner, KPMG UK)
- **Christopher Painter**
(President of The Global Forum on Cyber Expertise Foundation)

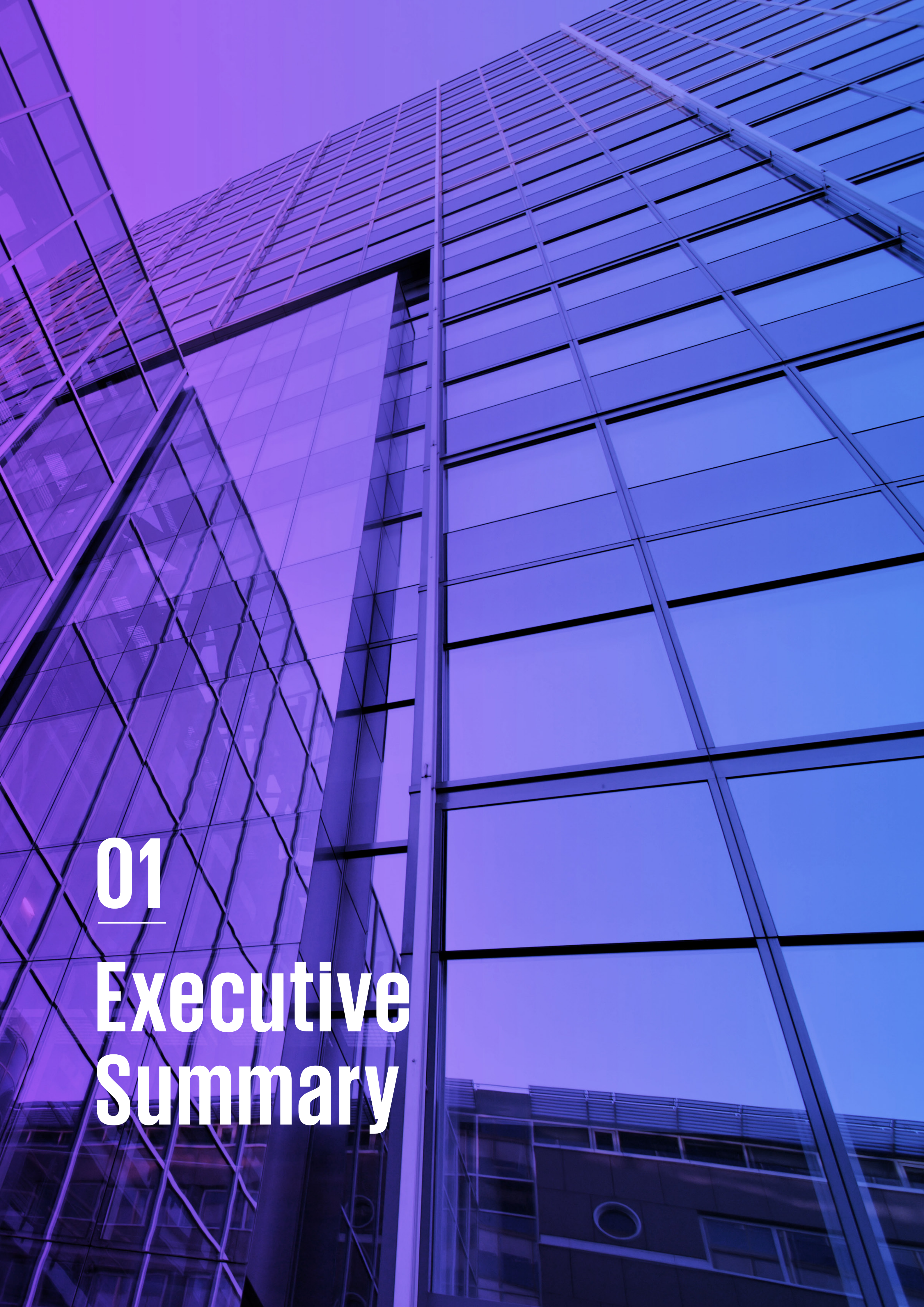
Acknowledgements

The authors give thanks to the following individuals and organisations who supported our research for this paper. Not all views expressed in this paper may reflect the views of the contributors listed below.

- **Alexandra Adina Asgari** (GFCE Secretariat)
- **Anna Collard** (Knowbe4)
- **Adv Jacqueline Fick (**VizStrat Solutions)
- **Dr Brett van Niekerk (**Department of Information Technology Faculty of Accounting & Informatics, Durban University of Technology)
- **Babatunde Okunoye** (Department of Communication and Media Studies, University of Johannesburg South Africa)
- **Susan Potgieter** (SABRIC)
- **Alex Yankovski** (KPMG Ukraine)
- **Gennadii Reznichenko** (KPMG Ukraine)
- **Matthew Roach** (Head of the International Information Integrity Institute (i-4), KPMG UK)
- **Varsha Sewlal**
- **Megan Stifel** (The Institute for Security and Technology)
- **Elizabeth Vish** (The Institute for Security and Technology)

This report was funded by the Foreign, Commonwealth & Development Office (FCDO). However, the views expressed in this publication are those of the author(s), and do not necessarily reflect the opinions, or the official policies, of the FCDO.

Contents



01

Executive Summary

01 Executive Summary

Since its emergence in the 1980s, the internet has driven positive change for individuals, societies, and businesses all over the world. It has empowered the sharing of knowledge, fostered innovation and been a major contributor to economic growth. Over this period however, the internet has also become a fertile ground for criminals to act across borders with greater ease and anonymity than ever before. One class of such activities is 'Ransomware', where a victim's system or data is rendered inaccessible until an attacker's demands are met. Coordinated ransomware threats emerged in the mid-2000s and soon proved to be a profitable business model for attackers. In the decade that followed, targets shifted from individuals to organisations in a bid to extort larger payments. Over this time, the surge in popularity of cryptocurrencies (notably the introduction of Bitcoin in 2008) provided criminals with a means of monetisation which is decentralised and thus difficult to track and address through conventional economic crime mechanisms, making it ideal for the evasion of law enforcement agencies. The tactics, techniques and procedures used by ransomware operators have adapted rapidly and continuously, often faster than the industry can respond.

Following a spate of high-profile attacks against critical national infrastructure, policymakers worldwide are beginning to develop national cybersecurity defence strategies to combat the risks that their citizens, businesses, and infrastructure face. Ransomware attacks continue to be the preferred method of attack for cybercriminals in 2022 and are evolving in response to changing geopolitical and market forces. According to the latest WEF Global Risks Report (2022)[1] there was a 435% increase in such attacks in 2020 alone. Whilst more developed countries are progressing towards sustaining multifaceted approaches to securing their infrastructure, many developing countries still face several fundamental challenges to protecting their businesses and people.

These include:

- Lack of formalised cybersecurity strategies, policies, and regulatory frameworks
- Lack of capacity to enforce policies and regulatory frameworks
- Lack of information security awareness and security culture
- Inadequate standards and maturity models for cybersecurity
- Lack of information security professionals and skills within the public and private sector
- Reliance on imported hardware and software
- Lack of sector-specific R&D programs
- Lack of integration into international partnerships for dealing with cyber incidents[2]

This paper has been produced as part of the UK Foreign, Commonwealth and Development Office's Digital Access Programme (DAP), which aims to catalyse more inclusive, affordable, safe, and secure access for digitally excluded communities. The authors aim to identify specific cybersecurity capacity building activities and mechanisms that policymakers may consider to enhance their organisations' resilience to ransomware attacks and other forms of cybercrime. These focus on developing cybersecurity skills and capacity, defining a regulatory response to ransomware, building effective partnerships for ransomware defence, and developing a community-based resilience architecture.

In support of the paper's aims, the authors reviewed the existing literature and explored a number of recent high-profile case-studies to frame the current state of global ransomware. A series of interviews were held with government officials, academics, and public and private sector security professionals from around the world to capture the wide variation of challenges and opportunities across the international policymaking community. The Digital Access Programme focussed on capacity building within 5 particular partner countries: Brazil, Indonesia, Kenya, Nigeria, and South Africa. Whilst we have produced recommendations for the international policymaking community as a whole, much of our research was conducted with a lens on the 5 DAP partner countries, who are developing economies home to rapidly growing numbers of internet users.

[1] WEF. 2022. The Global Risks Report 2022, 17th Edition. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

[2] https://ictframe.com/cybersecurity-challenges-in-developing-countries/

Overall, nine themes have been identified from our qualitative analysis of the challenges faced in managing ransomware. These are as follows:

- **Governance**
- **Criminal infrastructure**
- **Incident response capacity**
- **Cyber Insurance**
- **Legislation and law enforcement**
- **Trust and collaboration**
- **Certification schemes**
- **Societal impact**
- **Skills and training**

To alleviate these challenges, based on the review of existing literature and analysis of our own research, we have developed:

- Good practice principles that should underly the development of a long-term ransomware policy strategy and inform the decisions of policymakers. These are:
  - The unique vulnerability of ransomware as a threat vector
  - Civilian control of cybersecurity and ransomware resilience policies
  - The mission-critical role of public-private sector partnerships
  - Long term strategies coupled with short-term demonstrable successes
  - A graduated approach to policy implementation and regulatory enforcement
- A set of specific good practice recommendations for policy prescriptions across the five DAP participant countries and similar nations. These policy recommendations are divided into 4 clusters and amount to some 50 specific actions for policymakers to consider (details in Policy Recommendations section).

We have classified these recommendations as either “Formative” (F), “Established”(E) or “Strategic”(S). The classification is issued based on the level of maturity of a developing nation’s cybersecurity strategy one would expect to be in place, prior to the implementation of a policy. The 4 policy clusters are:

Cluster 1 – Build effective partnerships for ransomware defence:

1.1 Establish collaborative modes of working with major technology partners

1.2 Develop incentives to encourage private sector businesses to share cyber threat intelligence (CTI) with peer organisations, suppliers, customers and governments

1.3 Develop a framework for international collaboration and engagement with other national governments and international law enforcement organisations

1.4 Implement a community defence framework to actively disrupt ransomware revenue streams, operating models and infrastructure

Cluster 2 – Develop a community-based resilience architecture:

2.1 Develop a target operating model (TOM) for a national cybersecurity incident response team (CSIRT) and ransomware response policies

2.2 Benchmark key economic sectors to understand weaknesses and single points of failure in critical national infrastructure (CNI)

2.3 Run industry ransomware incident response exercises and resilience tests with CNI sectors and industry and technology partners

Cluster 3 – Strengthen cybersecurity skills and capacity:

3.1 Run consumer- and small-to-medium enterprise (SME)-targeted training and awareness campaigns in ransomware defence and broader cybersecurity hygiene

3.2 Develop a foundational cybersecurity controls framework for minimising ransomware attacks and create a pathway to certification

3.3 Build private, public sector and justice system skillsets in critical ransomware response capabilities to meet skills gaps

3.4 Develop higher education programmes and academic partnerships with universities to enable skills sharing and research

3.5 Attract key cybersecurity skillsets through easing of visa requirements for foreign nationals with desired technical or industry backgrounds

Cluster 4 – Define a regulatory response to ransomware:

4.1 Make regulatory decisions about whether to accept the payment of ransomware ransoms, and the provisions of cyber insurance providers

4.2 Require disclosure of data breaches and cyber attacks resulting from ransomware

4.3 Require a baseline third party assurance regime for the most cyber capable sectors which covers ransomware response capabilities

4.4 Establish regulation and compliance controls on the cryptocurrency market to hamper ransomware operators from monetising their efforts.

During the course of interviews and literature review, it became apparent that whilst ransomware has unique features that differentiate it from other cyber attack vectors, the solutions to ransomware preparedness are shared with multiple other forms of cyber attacks, and that defending against ransomware requires a broad uplift in overall cybersecurity maturity. Thus, whilst we have identified ransomware-specific policy considerations, many recommendations may be applied to improve cybersecurity resilience at a much broader level.

The paper presents a broad range of capacity building considerations, and consequently the reader should evaluate each of the proposed actions within the context of local resource constraints and political considerations. By promoting secure and trusted digital connectivity, policymakers can generate high-skilled jobs, create opportunities for local entrepreneurship and develop partnerships with international businesses to achieve mutual prosperity.

02 Literature Review

02 Literature Review

Ransomware attacks continue to be the preferred method of attack for cybercriminals in 2022 and are rampant among critical infrastructure organisations (Forbes, 2022)[3]. Such attacks present a threat to organisations and individuals worldwide and continue to evolve in response to changing geopolitical and market forces that impact the monetisation model of the criminal operators. According to the latest WEF Global Risks Report (2022)[4] there was a 435% increase in such attacks in 2020 alone. Cybersecurity failure now frequently ranks as a top-five risk in East Asia and the Pacific as well as in Europe, while four countries—Australia, Great Britain, Ireland, and New Zealand— ranked it as their number one risk. As policymakers and law-enforcement begin to mobilise against these threats, the importance of effective regional and international coordination becomes increasingly evident.

In the European Union, the average ransom more than doubled from $80,000 to $170,000 between 2019 and 2020 according to an ENISA Threat Landscape Report[5]. After several high profile and highly publicised ransomware incidents in the region, the report ranked ransomware as the primary threat for 2021. A survey conducted across 30 countries showed that the overall cost of remediating a ransomware attack also vastly increased over this time, from $761,106 in 2020 to $1.85 million in 2021 – more than doubling in the space of a single year.

In Africa, Interpol[6] reported more than 1.5 million ransomware detections in 2020, with Egypt, South Africa, and Tunisia experiencing the highest rates on the continent. The number of detections recorded by Kaspersky in the first half of this year in Kenya amounted to 32.8 million, which was on par with South Africa (at 31.5 million) and nearly double that recorded in Nigeria at 16.7 million.[7] The industries found to be most at risk across these three countries were the public and telecommunications sectors. In the last quarter of 2020 alone, 56.2 million threats were detected by the Communications Authority of Kenya (CA)[8]- a 59.8% increase in cyber threats compared to the previous quarter.

> **In Africa, Interpol reported more than 1.5 million ransomware detections in 2020, with Egypt, South Africa, and Tunisia experiencing the highest rates on the continent.**

Among ASEAN countries, there were a reported 2.7 million ransomware detections during the first three quarters of 2020[9]. Among the ten member countries, Indonesia suffered the most with 1.3 million counts, accounting for almost half of all detections in the region. During the COVID-19 pandemic, critical health service infrastructure such as hospitals in Indonesia and Thailand were especially targeted. It is thought that criminals believed they were more likely to receive pay-outs from these already overwhelmed public institutions.

In South America, more than half of all cyber attacks on the continent were targeting users or infrastructure located in Brazil, where the number of internet users has grown continuously, from 40% of the population in 2010 to 81% in 2020[10]. Brazil suffered a large number of ransomware attacks in 2021[11,12], with manufacturing being the most targeted sector, making up 20% of the recorded attacks[13]. This is consistent with a trending effort amongst cybercriminals to find a vantage point in the critical role manufacturing organisations plays in global supply chains to pressure victims into pay ransoms. A recent study[14] found that 40% of the Brazilian firms chose to pay a ransom after being attacked and those that did only managed to retrieve about 55% of the impacted data.

[3] Forbes (2022). Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know. https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=5e343ee77864

[4] WEF. 2022. The Global Risks Report 2022, 17th Edition. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

[5] ENISA Threat Landscape Report 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

[6] Interpol. 2021. African Cyber threat assessment report.

[7] https://thefintechtimes.com/over-81-million-cyber-attacks-in-kenya-south-africa-and-nigeria-in-h121/

[8] https://www.standardmedia.co.ke/business/article/2001418222/ransomware-the-new-threat-to-kenyan-businesses

[9] Interpol. 2021. Asean Cyberthreat Assessment.https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia

[10] ITU. Percentage of individuals using the Internet. https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2022/July/PercentIndividualsUsingInternet.xlsx

[11] https://www.gov.br/governodigital/pt-br/sisp/guia-do-gestor/documentos/sessoes-tematicas-do-sisp-2021/sic-guia-api.pdf/view

[12] https://tiinside.com.br/18/02/2022/brasil-sofreu-mais-de-33-milhoes-de-tentativas-de-ransomware-em-2021/

[13] https://www.zdnet.com/article/manufacturing-is-the-most-targeted-sector-by-ransomware-in-brazil/

[14] Sophos. (2022). The State of Ransomware 2022. https://www.sophos.com/en-us/whitepaper/state-of-ransomware

Advanced and developing economies

Technology and the advent of borderless information has brought unprecedented new opportunity for the acceleration of social and economic growth. However, whilst more developed countries are progressing towards sustaining multifaceted approaches to securing their infrastructure, many developing countries still face a number of fundamental challenges to protecting their businesses and people. These include:

- **Lack of formalised cybersecurity strategies, policies, and regulatory frameworks**
- **Lack of capacity to enforce policies and regulatory frameworks**
- **Lack of information security awareness and security culture**
- **Inadequate standards and maturity models for cybersecurity**
- **Lack of information security professionals and skills within the public and private sector**
- **Reliance on imported hardware and software**
- **Lack of sector-specific R&D programs**
- **Lack of integration into international partnerships for dealing with cyber incidents**[15]

These challenges comprise the spectrum of technology, people, strategy and legal considerations which policymakers must balance as they seek to promote growth in the cyber domain while managing affiliated risks. As discussed by Świątkowska (2020)[16], digitalisation of developing countries often outpaces the establishment and implementation of robust security controls and governance frameworks. Cybercriminals take advantage of this gap to target digital infrastructure and its users in developing counties. Lacking formal security budgets, skills and technology, organisations in developing countries may make an easier target than those operating in more developed states.

Ransomware case studies

Presented below are three recent case-studies of ransomware attacks targeting critical national infrastructure (CNI). These incidents were selected as they resulted in major impact to organisations and citizens of the affected countries, including theft of personal data and disruption to national services. The case studies are:

01 **The two sequential attacks on Costa Rican government institutions in late 2022**

02 **The attack on the US Colonial Pipeline in mid-2021**

03 **The attack on the Irish Health Services Executive (HSE) in mid-2021**

These attacks evidence the disruptive nature and nationwide ramifications of ransomware. In the following section, high-level details of the incidents are discussed along with some lessons learned for policy-makers to consider.

[15] https://ictframe.com/cybersecurity-challenges-in-developing-countries/

[16] Świątkowska, J. (2020) Tackling cybercrime to unleash developing countries' digital potential. Pathways for Prosperity Commission Background Paper Series; no. 33. Oxford, United Kingdom.

Case study	Costa Rican government ransomware attacks (2022)	Irish HSE ransomware attack (2021)	Colonial Pipeline ransomware attack (2021)
Date(s)	First wave of attacks: April 16th – May 4th Second wave: May 31st – June 27th	Initial compromise: March 18th – May 12th Payload execution: May 14th – May 21st	May 7th – May 12th 2021
Target	Government ministries, local and national civil service administrations, universities, research institutes, hospitals	Irish Health Service Executive (HSE)	Colonial Pipeline
Perpetrators	Conti ransomware group (first wave); Hive ransomware group (second wave)	Wizard Spider (Trickbot) cybercrime group (using Conti ransomware)	Unconfirmed but likely to be the Darkside ransomware group
Technology impact	Disabling of systems used by citizens for managing local and international tax, takeover of government websites Healthcare data breached; key hospital systems impacted Approximately 700 GB of data breached from several government and civil services	Services at 41 major hospitals disrupted: cancellation of outpatient, radiology, and routine check-up appointments COVID-19 testing referral scheme taken offline; reliance on walk-in centres	Unavailability of key control systems used to regulate flow through the 5,500-mile pipeline; subsequent shut down of pipeline operations 100 GB of data stolen
Wider impact and aftermath	A total of $15 million in ransom demands between both attacks Declaration of emergency issued alongside major protests over the non-payment of civil salaries Operational losses totalling $30 million per day for international trade and tax revenue Thousands of hospital appointments missed	Data of up to 520 patients published online, including special category medical data IT recovery and remediation costs likely to exceed 100 million EUR Staff burnt out and delays in payment of travel and subsistence claims	Temporary spike in fuel price to over $3 per gallon; panic buying of fuel following days of pipeline shutdown, and resulting shortages across many states in the south and the eastern seaboard Ransom of $4.4 million (75 BTC) paid
Recovery	Key financial services restored from June 24th onwards	Decryption key received on May 21st; approximately half of servers and applications restored by June 14th; nearly all servers / apps recovered by 21st September	Pipeline operations restarted May 12th Ransom of $2.3 million (63 BTC) recovered; DarkSide RaaS operator pressured to shutdown following pressure from law enforcement

Key considerations and lessons learned:

Case study	Costa Rican government ransomware attacks (2022)	Irish HSE ransomware attack (2021)	Colonial Pipeline ransomware attack (2021)
Technical controls	Initial VPN access was gained via compromised credentials, stolen via an **undetected piece of malware.** The attack exploited **a flat network architecture** to gain access to an admin network share, enabling privilege escalation[17]. **Back-ups had been encrypted,** per a post by Conti themselves, on their own forum.	**Detective controls** were not in place. The anti-virus product in use was running with **malware signatures that were out of date** by over a year, and there was **no effective patching programme** in place for endpoint or network devices.	A compromised password led to the initial VPN access; **basic cyber hygiene controls** over compromised credentials were not effective.
Cyber governance	Other ransomware groups will recognise an **already compromised organisation** as a target and exploit it. Organisations should be prepared for sequential attacks.	**Central, executive oversight** of cybersecurity controls was not in place. Support provided under existing **retainer services and managed services was not sufficient** to manage the attack; further private sector support was required.	A decision was made to **pay the ransom** given the criticality of the pipeline's operations. The legal permission to make payments may be useful, but may also **encourage ransomware operators to target jurisdictions** with cultures that allow it.
Public policy / diplomatic view	**Rewards for information leading to the apprehension of cyber criminals** may be useful to policy initiatives; a $10 million reward was offered by the US State Department.[18] **Private sector support** from Microsoft, as well as the **governments of Spain, Israel, and the United States,** enabled forensic and recovery efforts.[19]	Initial engagement with Irish NCSC, Interpol and the Garda National Cybercrime Bureau **enabled quick access** to an IR service provider. **Engagement with the judicial system** enabled the HSE to secure a High Court injunction preventing the selling or publishing of data stolen from its security systems.[20]	Traceability inherent in blockchain technologies underlying the payment **enabled some of the ransom to be recovered.** The DarkSide ransomware group were forced to shut down, reporting **"massive pressure"** from US law enforcement agencies, indicating the value in active defence efforts. [21]

[17] https://www.bleepingcomputer.com/news/security/how-conti-ransomware-hacked-and-encrypted-the-costa-rican-government/

[18] https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/

[19] https://www.reuters.com/world/americas/costa-ricas-alvarado-says-cyberattacks-seek-destabilize-country-government-2022-04-21/

[20] https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

[21] https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html

Country case study – Ukraine’s strategy for ransomware preparedness

Having faced a series of major ransomware attacks on their critical infrastructure since 2015, Ukraine’s national response presents several important lessons for bolstering security capabilities, strategy, and governance. In the build-up and immediate aftermath of the 2022 Russian invasion of Ukraine, cyber attacks were expected to be used heavily as instruments of hybrid warfare. However, it was reported that the rate of successful attacks has been significantly lower than expected[22], with some citing the success of ransomware preparedness efforts over the previous 7 years, as well as support from international partners, as the reason for Ukraine’s improved management of cyber attacks.

From interviews with regional subject matter experts, the authors analysed Ukrainian efforts to harden their infrastructure against these ransomware attacks. Whilst Ukraine experienced many successes in this space, they also encountered a wide range of challenges, which present lessons learned that DAP partner countries may incorporate into their policies.

[22] https://www.ft.com/content/1315165d-3986-4671-972f-c1ce04104560

Discussion identified the following as some of the key lessons learned throughout their transformation efforts, extracted from both their successes and challenges:

Challenge: Lack of skills hampered progress in both private and public sector firms.

It is important to build trust and engagement by identifying value that can be delivered in the short-term while more strategic long-term change is undertaken.

Look for solutions and opportunities that can be implemented within the constraints of the current infrastructure, skill sets and workforces. This way immediate enhancements can be delivered incrementally.

Using existing applications in conjunction with middleware technology such as Application Programming Interfaces (APIs) can enable interoperability without the wholesale change of moving to complex alternative solutions.

A key start point for change is ensuring knowing what you have, where you have it and what state it is in, is critical for taking informed decisions.

Challenge: Public mistrust of government bodies can dampen capacity building efforts.

Efforts to create a legislative strategy for cybersecurity were hampered by mistrust of government bodies. A great deal of legislation was opposed on the basis that the expansion of central government powers would result in violation of free speech protections and individual privacy. A public communications campaign, as well as effective safeguards against misuse of expanded cybersecurity powers, should be in place as part of any legislative strategy. Legislative efforts should be fronted by civilian authorities who are functionally independent of military or intelligence bodies.

Challenge: Some well-intentioned programmes can be corrupted.

A certification scheme set up by Ukraine's cybersecurity agency, with the aim of improving the general standard of cybersecurity controls, was commonly believed to be corrupted. The certification would reportedly be issued for bribes, or else is issued to organisations with ties to the government. The establishment of independent oversight agencies and suitable penalties for corruption efforts is critical to safeguarding trust in key capacity building schemes.

Success: The private sector should be considered an equal partner.

Ukraine's cybersecurity strategy sought to improve relationships between the public and private sectors. As per the reporting of the Atlantic Council, private sector organisations were not considered equal partners and regulation limited their ability to participate in intelligence sharing and response efforts. The establishment of the CERT-UA (Ukraine's government CERT) and the CyS-CERT (the private sector analogue) began to address these challenges and significantly improved trust and coordination efforts. Among the most effective programmes established was one which saw the sharing of government threat intelligence with major cybersecurity service providers, who in exchange for the intelligence provided support efforts to track down cybercriminals.

Success: Utilise international partnerships for access to technology and response capabilities.

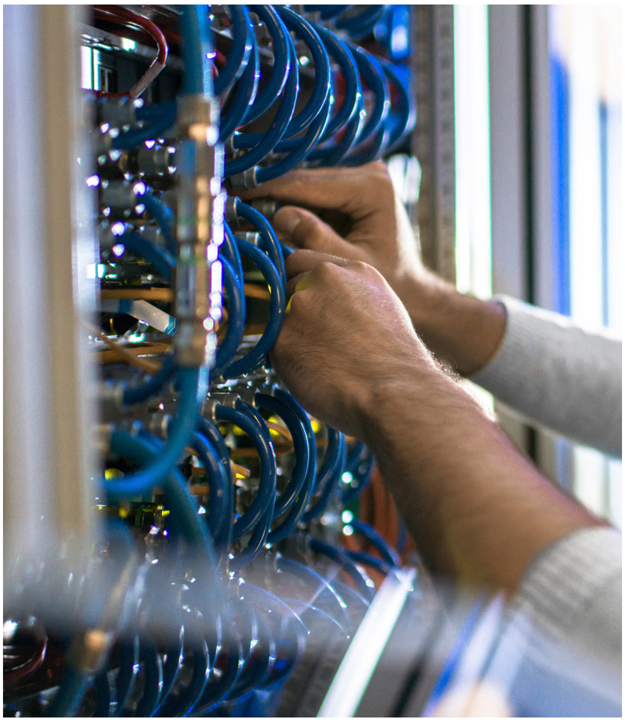
Ukraine utilised partnerships with NATO, EU and USAID programmes to access to at least $10 million worth of investment prior to the Russian invasion to bolster cybersecurity defences around critical national infrastructure (CNI), with significantly more provided following accession to NATO's Cooperative Cyber Defence Centre of Excellence (CCDCoE).

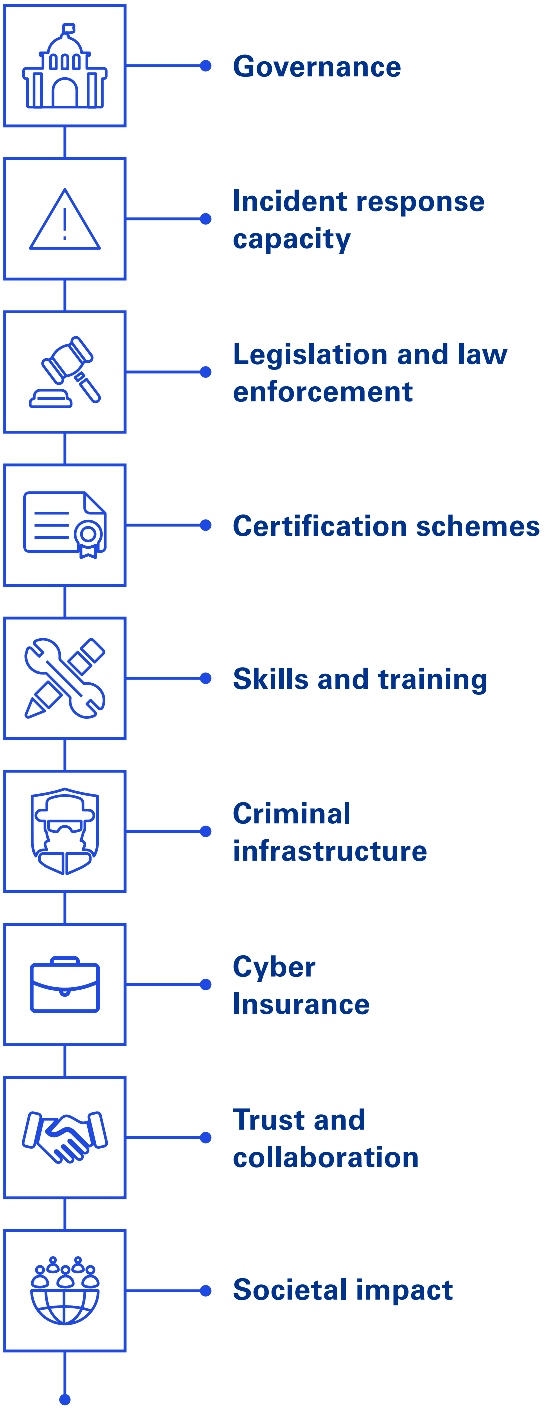
03 Analysis

03 Analysis

Thematic analysis was conducted on the qualitative data collected from interviews and literature to identify frequent challenges and improvement opportunities for organisations and policymakers around the globe. We adopted a blended approach (a mix of deductive and inductive) to analyse interview data. The inductive approach is based on 'open coding' meaning that the categories or themes are freely created by the researcher, while the deductive content analysis requires the prior existence of a theory to underpin the classification process. The analysis performed aims to provide a baseline view of these challenges and opportunities as well as to support conclusions and recommendations. Excerpts that did not fit into themes were further analysed to highlight additional issues that stakeholders might have raised during the interviews or to inform our understanding on the various topics around ransomware.

Overall, nine themes are identified from our qualitative analysis. These are as follows:





Governance

Incident response capacity

Legislation and law enforcement

Certification schemes

Skills and training

Criminal infrastructure

Cyber Insurance

Trust and collaboration

Societal impact

Governance

The development of an effective governance model with mechanisms for coordination is a significant component of national and organisational resilience. Governance encompasses the system by which an organisation is controlled and operates, and the mechanisms by which it, and its people, are held to account. Ethics, risk management, compliance and administration are all elements of governance. At a national level, drafting a strategy, budget acquisition, risk identification, information sharing, and workforce education are all part of a comprehensive governance plan. International frameworks such as the ISO and NIST standards help agencies and organisations to better manage their risk. These frameworks require a continual risk-based improvement process which enables businesses to identify risks, implement controls appropriate to the risk and monitor the performance of these controls. Organisations should also consider the use of security benchmarks to adoption of security best practices. One of the most comprehensive, the benchmarks developed by the Center for Internet Security[23] are a set of globally recognized and consensus-driven best practices to help security practitioners implement and manage their cybersecurity defences for over 25 different vendor products.

Good governance streamlines the flow of security-related information throughout an organisation. It enables identification of the security decisions that need to be made, the people who should make them and the data required for them to do so. A robust governance model will define roles and responsibilities, identify the individuals responsible for making security decisions and ensure that feedback is provided to the decision-makers on the impact of their choices. In the context of a ransomware attack, such an approach would require designation of accountability for certain planning and response actions: a) the incident response chain of command; b) key internal and third-party points of contact; c) crisis team formation; d) internal and public communications; and e) legal and reporting responsibilities.

[23] https://www.cisecurity.org/cis-benchmarks/

Executive Summary
Literature Review
Analysis
Policy Recommendations
Conclusion

Incident Response Capacity

According to interviewees, a crucial requirement of national level resilience is incident response capacity. Many of the stakeholders who participated in this study highlighted the lack of capacity, skills, and peoplepower within CSIRT teams. Often the lack of personnel hinders or delays the response to incidents, leading to the need to prioritise incidents over each other.

A further challenge for responders was the lack of well-defined target operating models (TOM)- particularly in the case of national cybersecurity incident response teams (CSIRTs). Lack of well-defined processes can result in uncertainty regarding the mandate of security teams to act which can considerably slow down incident response efforts. In one European national healthcare system analysed, the central CSIRT/SOC had limited visibility of IT infrastructure in the hospitals it was responsible for as the IT was managed independently by the hospitals. Many of these 'arms-length' healthcare trusts had directly contracted vendors of medical technology, limiting the CSIRTs control over third-party and supplier risk within the national system. In some cases, these contracts even contained confidentiality agreements preventing the suppliers from sharing incident details with the CSIRT during live incidents.

Table-top exercises were also mentioned by a number of participants as an effective approach to national preparedness for cybersecurity incidents. Regularly exercising national crisis management scenarios with cybersecurity components and testing emergency communication systems for cyber resilience is a way of identifying potential gaps in the ability of a nation or organisation to respond to attacks. A ransomware table-top exercise begins with a specific ransomware attack scenario, describing the details of the attack, and how the organisation should react, step by step. Each organisation's approach to ransomware will vary based on factors such as the technology stack, services and data impacted[24]. Additionally, skills and resources available, processes documented, and legal jurisdiction are likely to influence the range of cyber incident scenarios that an organisation or country is likely to face. A private sector Manager in Africa stated: "[There is a] lack of practising basic safeguards, usually due to resistance to culture shift relating to ways of working and underestimating the value of simulation exercises".

As part of the DAP programme of work, incident response simulations were conducted involving private organisations alongside national and sector wide CSIRTs. One takeaway from these exercises was the importance of building incident response capacity at an organisation level before cross-sector exercising. The simulation of wide-scale attacks was of limited usefulness where there were no roles and responsibilities defined and no legal mandate for response. Without these, the CSIRT was not empowered to take the lead in coordinating a response. It was found that organisations from the private sector and sector wide CSIRTs were very receptive to the tabletop exercises and understood the value they could provide. Perhaps because of their lack of mandate, the engagement was not always matched by public sector and government CSIRTs who proved more resistant to participating.

Information sharing of threat intelligence, vulnerability information and operational good practices between private, public, and international stakeholders is important. Information sharing is best coordinated from a central body with the mandate to collect and disseminate information between national and sub-national levels through clear mechanisms which protect the confidentiality of participants. Trust maintained in this central body is essential to the continued sharing of information at organisational, national, and international levels.

> **One takeaway from these exercises was the importance of building incident response capacity at an organisation level before cross-sector exercising.**

[24] Bada, M. (2022). RISCS Ransomware Workshop: Industry Perspectives. https://www.riscs.org.uk/wp-content/uploads/2022/09/Ransomware-Workshop-V3.pdf

Legislation and law enforcement

The EU's General Data Protection Regulation (GDPR) came into force in May 2018 and was designed to give EU data subjects control with regards to how their data is processed, stored, or transmitted. A 2019 UK Government report found that the regulation had encouraged and compelled some organisations to engage formally with cybersecurity for the first time, and others to strengthen their existing policies and processes[25]. The report suggests that data protection and breach reporting regulation can be a key driver to businesses taking the first steps in cybersecurity. GDPR was quickly followed elsewhere by similar legislation including Brazil's General Personal Data Protection Law (LGPD) and the California Consumer Privacy Act (CCPA). To address the rising cybercrime rates in Africa, the African Union Convention on Cybersecurity and Personal Data Protection (a treaty that is also known as the Malabo Convention) was drafted in 2014. To this date however, only 14 out of the 54 countries in Africa have signed this treaty, and only eight had ratified the treaty at the end of 2020[26].

While some broader regulations apply to the handling of ransomware incidents, security experts are expecting to see more legislation focussing on ransomware negotiation and payments. A 2021 Gartner[27] report estimated that by 2025, an estimated 30% of nation states are expected to legislate ransomware reporting and payment activities. Such changes in the regulatory landscape could provide governments with greater control and visibility over the flow of data and payments from ransomware attacks, however this benefit will only be realised if policymakers can simultaneously develop a framework to effectively promote and enforce the legislation.

> **The report suggests that data protection and breach reporting regulation can be a key driver to businesses taking the first steps in cybersecurity.**

Such a framework would facilitate policymakers to:

- **Coordinate the changes effectively across government and the public sector.**
- **Provide training and support private sector businesses to comply with new legislation.**
- **Provide a straightforward and responsive channel for the reporting of data breaches.**
- **Provision the cybersecurity and digital forensics skills required to support with investigation of reported incidents.**
- **Take enforcement actions against organisations that are not compliant.**

Our research found that whilst many developing economies do have data protection and cybersecurity legislation in place, there was frequently little evidence of effective enforcement. Private sector organisations were often seen to take a 'wait-and-see' attitude - waiting to see the actual ramifications of non-compliance rather than undergoing the required transformation to achieve compliance. With governments lacking the skills, budget, and political will to seek out such behaviour, there is often little incentive for organisations to do otherwise. Such disconnect between legislation and enforcement greatly reduces the practical effectiveness of implemented policies, leading to under-reporting of incidents and a breakdown of communication between businesses and law-enforcement.

The benefits of a holistic approach to cybersecurity policymaking are evident in the case of Singapore. In 2015, the Cybersecurity Agency (CSA) was formed to develop a national strategy to tackle cyber threats. The strategy was aimed at coordinating public and private sector efforts to protect critical infrastructure

[25] RSM 2020 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/906691/Impact_of_GDPR_on_cyber_security_outcomes.pdf

[26] African Union https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[27] Gartner. 2021. The Top 8 Cybersecurity Predictions for 2021-2022. https://www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022

from cyber threats. The strategy also placed a strong focus on growing cybersecurity talent, working collaboratively with the private sector to raise public awareness of the importance of cybersecurity issues. Further strengthening private sector buy-in to the national strategy, the Cybersecurity Act of 2018 established the CSA as the central node of an information sharing network across the public and private sector to support the prevention, detection, and investigation of incidents. With the confidentiality of incident details formally protected by the CSA and support on hand for those who disclose their incidents, the act has established greater trust between private and public sectors.

Certification Schemes

Government-backed cyber certification schemes are designed to standardise a baseline level of trust between organisations, their partners, and clients. These schemes typically consist of a comprehensive set of rules, technical requirements, standards, and evaluation procedures applying to an organisation's products, services, or processes. By obtaining such certifications, businesses are able to:

- Develop a clearer picture of their IT infrastructure and security posture
- Reassure existing customers and partners that their data is protected
- Attract new business by demonstrating the security measures in place
- Obtain government contracts which pre-require certification
- Manage third-party risks more effectively

Previous research suggests that the digitalisation of developing countries often outpaces the establishment and implementation of robust security controls and governance frameworks[28]. Our observations were consistent with the literature, finding that that the creation and adoption of certification schemes was indeed more common in developed countries with greater overall levels of cyber maturity. Evidence suggests that such schemes have a positive impact on security awareness within certified organisations and can be key drivers of customer and investor confidence. A recent study commissioned by the National Cybersecurity Centre (NCSC) into the UK Cyber Essentials assurance scheme found that certified organisations were more likely than non-certified counterparts to be[29]:

- **Aware of the risks posed by cyber attacks (including at a senior level)**
- **Confident that they are protected from these attacks**
- **Implementing security controls, including steps beyond those required for certification**
- **Experience positive impacts on customer and investor confidence**

Third party assurance regimes for mature industries can be used by regulators to drive adoption of newly defined control frameworks and accelerate the benefits of standardisation. For regulators and cybersecurity agencies concerned over ecosystem-wide resilience against ransomware, third-party assurance regimes can foster improved cooperation between organisations and their suppliers, helping to build coherent incident response processes and streamline active defence efforts. They can also generate valuable information on industry supply chains, which can help identify critical third parties and single points of failure.

[28] Świątkowska, J. (2020) Tackling cybercrime to unleash developing countries' digital potential. Pathways for Prosperity Commission Background Paper Series; no. 33. Oxford, United Kingdom.

[29] https://www.ncsc.gov.uk/information/setting-baseline-ce-prior-to-iasme

Skills and training

Our research found that a shortage of cybersecurity skills was consistently identified by stakeholders as one of the major challenges to improving resilience to ransomware attacks. Whilst skills shortages were reported in both the public and private sector, some business areas were much better resourced than others. Industries such as financial services and manufacturing have seen large amounts of investment in response to tightening regulations and the skyrocketing costs of breaches. Consequently, these organisations are better resourced than those in the public sector, where people and technology budgets are likely to be more constrained and face greater scrutiny. In one African country studied, a large financial services provider was found to employ several hundred security engineers nationally, while full-time staff of the national CIRT team numbered less than 5.

The skills gap appears to be accentuated within developing economies where there are fewer trained security professionals and often high rates of skilled workers seeking opportunities overseas. A study conducted by KnowBe4[30] on cybersecurity skills in South Africa found that the roles which organisations most struggled to fill were cloud security professionals, SOC/IR analysts, and risk/compliance professionals, all which presented a hiring challenge for more than 50% of surveyed businesses.
A comparable 2022 study conducted by the UK Department of Digital, Culture, Media, and Sport found that incident management/digital analysis (26% of surveyed businesses), security architecture (24%) and security testing (24%) made up the three biggest skills gaps for UK firms[31]. In addition to the shortage of technical security skills, research indicates that senior management often lack an understanding of cybersecurity issues, leading to a potential knowledge deficit among policymakers and c-suite executives tasked with overseeing these issues. Within even mature organisations, there is often no comprehensive generalist cyber training pathway for individuals moving into decision-making positions. One individual from the public higher-education sector in an African country surveyed stated that 'Policymakers … do not fully understand the intricacies of information/cybersecurity, and the laws take very long to put in place, so they are effectively outdated by the time they are introduced'. In 2021, 9 in every 10 African businesses[32] were found to operate without adequate consideration of cybersecurity standards. If the continent continues to draw investment without making strides in its cybersecurity measures, its rapidly growing base of potential victims will draw increasing numbers of cyber attacks. Such attacks can greatly affect the confidence of investors and potential business partners and could ultimately hamper economic growth.

Another aspect of this skills shortage is the lack of security awareness amongst the general working population. A 2020 study by Deloitte found that 90% of all cyber attacks begin with a phishing email to an unexpecting victim, thus staff security training and exercising is increasingly central to a broad programme of organisational cyber resilience[33]. Interviews revealed that security awareness trainings offered to staff were often seen as 'box-ticking exercises', failing to engage the workforce in a meaningful or informative way. Organisations should instead develop incentives to encourage their workforce to engage with the content more proactively. At present, security awareness programmes are typically offered at an organisational rather than societal level. Policymakers may consider launching national programmes on TV, radio, and social media to raise wider awareness of cybersecurity issues within the population. Similarly, cyber awareness training could be included as part of the higher education curriculum to ensure those entering the workforce have a basic level of security literacy and behaviours.

Multiple interviewees noted awareness raising as a critical facet of ransomware preparedness, given how often phishing and social engineering act as initial points of entry or compromise. Improving cyber hygiene also reduces general likelihood of falling victim to a number of cyber attacks and scams. One UK banking sector organisation's CISO, in reference to the classical "three lines of defence" model deployed to facilitate corporate governance, described a well-trained staff body as the "zeroth line of defence" against cyber attacks. The security leader noted the exceptional force-multiplying risk reduction effect of training and awareness as a boundary security control rather than an internal one.

[30] http://www.securitysa.com/16343r

[31] Ipsos report (publishing.service.gov.uk)

[32] Interpol https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf

[33] 91% of all cyber attacks begin with a phishing email to an unexpected victim | Deloitte Malaysia | Risk Advisory | Press releases

Criminal Infrastructure

Following several high-profile ransomware incidents targeting critical national infrastructure, governments around the world are seeking to disrupt ransomware infrastructure and operating models. This presents a major challenge to individual sovereign states, as much of the infrastructure used by ransomware operators consists of international networks which are resilient to localised takedowns. Moreover, the emergence of cryptocurrencies in the past two decades has provided criminals with a decentralised means of monetisation which is challenging for law enforcement to track and address through conventional economic crime mechanisms. Ransomware criminals can obscure their transactions through cryptocurrency "mixing services," mixing legitimate traffic with illicit ransomware funds thereby muddying the public ledger. Between 2019 and 2020, there was a four-fold rise in the total cryptocurrency value received by ransomware addresses- totalling more than $400m USD in 2020. Little to none of this value was recovered by law-enforcement, and with few barriers to entry and little risk of prosecution, this proliferation shows no signs of slowing down.

Many of those interviewed believed that the use of cryptocurrencies was under-regulated by policymakers and that cryptocurrency should be controlled with comparable compliance protocols, background investigations and KYC checks as those in the fiat currency space. Whilst there have been some attempts to regulate cryptocurrency (e.g. The March 2022 Executive Order- 'Ensuring Responsible Development of Digital Assets' or New York State's 'BitLicensing scheme'), much of the existing regulation aims to define the place of virtual currencies in the existing financial ecosystem rather than actually legislating the underlying cryptocurrency technologies[34]. The criminal operating model is most vulnerable at the point where operators attempt to convert their cryptocurrency to traditional earnings. Regulators must therefore pay close attention to crypto exchanges, where this transfer of value is likely to happen. In 2021, the US Treasury Department's Office of Foreign Asset Control (OFAC) sanctioned the Czech crypto exchange 'Suex' over allegations that it facilitated bitcoin transactions for ransomware actors[35]. This sets a new precedent for policymakers, presenting a way to deter cyber criminals by obstructing their financial enablers.

One recent development of the ransomware operating model has been the creation of a subscription-based service that enables affiliates to use already-developed ransomware tools to execute attacks and collect a percentage of each ransom payment secured. The model, known as Ransomware-as-a-Service (RaaS), reflects the adoption of the Software-as-a-Service delivery paradigm which has become widespread across the technology sector in recent years. Previously, the ransomware business had a high barrier to entry due to the technical expertise required to develop effective malware. Under the RaaS model however, users need not be skilled or experienced but rather only proficient in use of the tool. The model has therefore empowered even the most novice criminals to execute sophisticated attacks, with more businesses being targeted as a result. RaaS also gives cybercriminals increased resiliency to imposed sanctions. High-profile ransomware groups can pivot from one ransomware service to another, making attribution of attacks far more difficult than it was when each group used a unique strain. This increases the groups chances of receiving ransom payments after sanctioning. A high-profile example of this behaviour was reported by Mandiant[36] with regard to ransomware group Evil Corp sanctioned by OFAC in December 2019. When the sanction was imposed, the group used a strain of ransomware known as 'WastedLocker', however has since switched to Hades and more recently have begun to use Lockbit. A prominent strain of RaaS malware, Lockbit is used by several different threat groups so has allowed Evil Corp to blend in with other unsanctioned affiliates and increase their chances of receiving payment.

Another trend which emerged from the interviews was the need for increased coordination efforts to target criminal infrastructure. As many ransomware groups operate on globally distributed infrastructure, governments operating in isolation will lack the visibility and reach necessary to facilitate effective takedown action and prosecution. Consequently, policymakers should consider engaging in formal partnerships and collaboration efforts in order to expand their visibility of threats and sphere of influence beyond the country's immediate borders. By partnering with the private sector, policymakers can resource the skills and capacity which might not be available to the public sector alone. Such partnerships

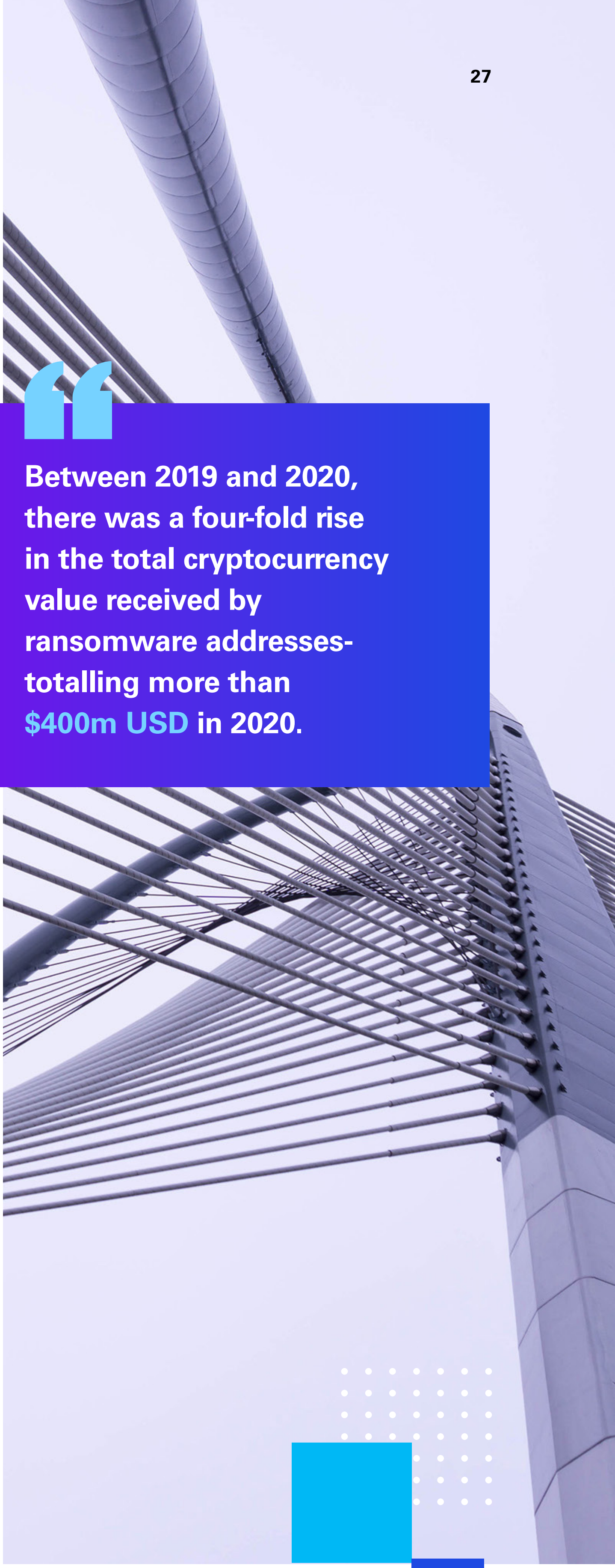
[34] https://securityandtechnology.org/blog/crypto-and-web3-anticipating-security-and-regulatory-challenges/

[35] https://www.coindesk.com/policy/2021/09/28/crypto-regulation-ransomware-and-ofacs-rise/

[36] https://www.mandiant.com/resources/blog/unc2165-shifts-to-evade-sanctions

can be a valuable source of threat intelligence and may also be relied upon to support efforts to take down criminal infrastructure. Interviews revealed that many existing public-private partnerships had not been formally established and questions regarding trust and mutual-benefit to the involved parties remained. Interviews also pointed to the effectiveness of international bodies such as Interpol and Europol in disseminating information and coordinating action against ransomware operators. It is evident that international collaboration has a crucial role to play in tackling ransomware threats, but the challenge for policymakers and diplomats is that of achieving the necessary consensus to actually coordinate action between countries. One manager of a Professional Services enterprise in Africa stated: "International standards and co-operation could be beneficial for insights and a wider view of potential cases and how such cases are dealt with, however sovereignty of countries and the decisions they would need to make should also be respected".

Efforts to take down ransomware infrastructure have had notable effects on ransomware operators, who have adapted their business models and target selection based on a need to avoid the attention of law enforcement. As well as filtering for organisations in sectors with typically low cybersecurity maturity and cash reserves sufficient to pay a ransom, ransomware operators have also become wary of targeting organisations in critical infrastructure sectors, on whom attacks are likely to draw the resources of law enforcement, intelligence agencies and government bodies. In some cases, RaaS operators have even offered decryption keys where their ransomware has been deployed on some sectors. Examples like this, outlined in the case studies, underscore the importance of cohesive, visible trust relationships between organisations and law enforcement, which even when potentially under-resourced can act as an effective deterrent to ransomware operators.



"Between 2019 and 2020, there was a four-fold rise in the total cryptocurrency value received by ransomware addresses- totalling more than $400m USD in 2020.

Cyber Insurance

The cyber insurance market plays a significant role in ransomware operation. Cyber insurance policies often include specific coverages for ransomware, including for business interruption losses, data restoration costs, incident response costs, and ransom payment. It is often argued that the support insurance companies provide encourages attackers, as victims may be more likely to pay if their costs are covered[37]. In fact, attackers have been known to target companies specifically because they have insurance. One major ransomware group REvil even claimed to target the insurers themselves in a bid to identify their customer base and focus their future efforts on these insured businesses[38].

A financial services CEO in Africa mentioned that "The biggest challenge for organisations to be resilient to ransomware is the 'Ability to lower cyber insurance premiums". Research has shown that cyber insurance can be a major incentive for businesses to manage societal cyber risk. Current shortcomings of the industry however mean that its contribution to improving security practices is more limited than policymakers and businesses might hope [39]. Activity such as developing security standards for underwriting, promoting data sharing and creating new collaborations between insurers and law enforcement agencies could further the role which insurance plays in reducing cyber harms to society [40].

NCSC [41] have provided guidance regarding cyber insurance and the government is working with the private sector on sharing more robust cyber risk impact information. The Ransomware Task Force[42] proposes that accelerating the cyber insurance market's maturity, solvency, and expertise will enhance its role in supporting comprehensive public and private action against ransomware. For example, more mature insurance providers would require that their clients adhere to strong baseline security practices which would reduce the disruption caused by a ransomware attack. Insurers can play a more positive role both in driving adoption of better cyber hygiene, and in providing an important safety net for victims of attacks. To do so, the cyber insurance market must be innovative and adaptive to emerging risks, standards, and practices, seeking to address the full scope of cyber harm.

> **The biggest challenge for organisations to be resilient to ransomware is the 'ability to lower cyber insurance premiums'**

[37] Dudley, Renee. "The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks," https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks

[38] https://www.washingtonpost.com/technology/2021/06/17/ransomware-axa-insurance-attacks/

[39] RUSI Occasional paper (2021). Cyber insurance and the cybersecurity challenge: https://rusi.org/explore-our-research/publications/occasional-papers/cyber-insurance-and-cyber-security-challenge

[40] Reuters, 2022. Analysis: Russian ransomware attacks on Ukraine muted by leaks, insurance woes | Reuters

[41] NCSC Cyber insurance guidance: https://www.ncsc.gov.uk/guidance/cyber-insurance-guidance

[42] Ransomware Taskforce (2021). Combating Ransomware. A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force. https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf

Trust and collaboration

Sectorial collaboration

Strong public-private partnerships are a cornerstone of an effective and long-term national cybersecurity strategy. Over the years, the private sector has been forced to evolve in response to the growing scope, scale, and complexity of cybercrime. Today, public sector organisations (many of which are vulnerable due to outdated and legacy systems) must also face up to these threats if they are to effectively protect the critical data and infrastructure which they are responsible for. Amidst a constantly evolving threat landscape targeting both the public and private sectors alike, it is logical that the two work collaboratively to defend the nation's strategic and business interests.

Public-private partnerships have been shown to greatly strengthen the efforts of law enforcement and judicial authorities in disrupting and investigating cyber threats. In 2020, Microsoft took action to disrupt the Trickbot botnet, one of the world's most infamous and prolific distributors of ransomware at the time. After obtaining a US court order approving the action, the multinational technology corporation executed a takedown of the botnet's infrastructure in partnership with telecommunications providers around the world. In total, 94% of the botnet's command and control servers were brought offline. Although Trickbot ultimately survived the takedown attempt, these events set an important legal precedent and demonstrated the significant role which private sector partners can play in disrupting cyber-criminal threats.

Discussions however revealed a number of commonly observed challenges to achieving effective two-way collaboration and information sharing. A lack of mechanisms for collaboration between the public and private sectors was seen to diminish national levels of cyber resilience. Internal fragmentation within government resulted in a lack of clarity on proper incident handling and reporting protocols, leading to reduced confidence and engagement with the public sector. Public-private trust is strongly linked to cultural norms and historical associations, both which can play a big role in the effectiveness of modern-day collaborations. One academic in Latin America spoke about the mistrust between public and private sectors in one country due to the recently complex military history of this state, and the role of the military and intelligence community in shaping cyber policy for largely national defence purposes.

Participants suggested that the "private sector incident responders should be supporting national CIRT delivery", especially in countries with reduced skills and capacity. In regard to notifying the public sector of security incidents, one private sector risk consulting manager in the UK claimed there was a "lack of confidence and reluctance to engage [with the public sector] due to embarrassment of lack of preparedness". Discussion pointed to the importance of mutual benefit in sustaining public-private partnerships. For example, private businesses are much more likely to notify government agencies of cyber breaches if they can expect to receive threat intelligence and law enforcement support in return.

Governments can demonstrate their commitment to building these partnerships by establishing schemes committed to continued trust and relationship building. Examples of such initiatives in the UK are 'NCSC for Startups'[43], bringing together innovative startups with NCSC technical expertise to solve some of the UK's most important cyber challenges, and 'i100[44] Industry 100 (i100)', established to facilitate close collaboration with the best and most diverse minds in UK industry.

> **Private sector incident responders should be supporting national CIRT delivery**

[43] https://www.ncsc.gov.uk/section/ncsc-for-startups/overview

[44] https://www.ncsc.gov.uk/section/industry-100/about

International collaboration

International collaboration emerged as a key driver of national cyber resilience, with many respondents seeing the lack of cross-border collaboration as a limiting factor in their country's ability to handle ransomware threats. The 2014 African Union Convention on Cybersecurity and Personal Data Protection had been ratified by only 8 of 54 countries in the union by the end of 2020[45]. One academic from the African region stated "The challenge is establishing effective collaboration at an international level, but this still relies on individual countries to implement. Given what I have seen in many cyber diplomacy and international working groups, sometimes getting sufficient agreement at international level is difficult as many nations are not necessarily able to implement". For international partnerships to sustain, diplomatic outcomes must be underpinned by capacity building exercises to ensure that policymakers can implement and enforce evolving policy. The Budapest Convention was established to promote these important mechanisms of cooperation; however, many countries have not yet joined. Consequently, the UN is preparing a new international convention on countering the use of information and communications technologies for criminal purposes[46]. This convention will not remove the obligation placed on national level policymakers to implement the controls proposed, but could provide a framework for doing so.

Discussions confirmed that international organisations such as Interpol and Europol play a crucial role in facilitating global cyber-crime control and improving the reach and decisiveness of law enforcement operations against criminal activity. One such example in 2021 saw authorities from France, Netherlands, Norway, Ukraine, USA, and Switzerland (with the help of Europol and Eurojust) act against a globally active group of cybercriminals operating LockerGoga and MegaCortex ransomware[47]. This operation was carried out by the European Multidisciplinary Platform Against Criminal Threats (EMPACT)[48] initiative which aims to improve cross-border cooperation by building trust and familiarity between partnering countries. A total of 12 individuals responsible for coordinating ransomware attacks against critical infrastructure were targeted as a result of the operation.

One example of effective collaboration, the Ransomware Taskforce (RTF)[49] is a cross-sector, international organisation aiming to tackle ransomware threats by disrupting threat actors and equipping organisations to prepare and respond if they are targeted. The taskforce unites key stakeholders from across industry, government, and civil society with the objective of finding new methods of countering the international ransomware threat. Facilitated by the White House National Security Council, another international collaboration committed to building collective resilience to ransomware attacks is the Counter Ransomware Initiative. Bringing together 30 countries and the European Union, the initiative seeks to disrupt ransomware operations, pursue the responsible actors, counter the illicit finance that underpins the ecosystem, and work with the private sector to defend against attacks[50].

[45] African Union https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[46] https://edps.europa.eu/press-publications/press-news/press-releases/2022/new-united-nations-convention-cybercrime_en

[47] https://www.eurojust.europa.eu/news/12-targeted-involvement-ransomware-attacks-against-critical-infrastructure

[48] https://www.eurojust.europa.eu/empact

[49] NCSC. 2021. Ransomware Taskforce (RTF) announce framework to combat ransomware. https://www.ncsc.gov.uk/blog-post/ransomware-taskforce-rtf-announce-framework-to-combat-ransomware

[50] https://www.state.gov/briefings-foreign-press-centers/update-on-the-international-counter-ransomware-initiative

Societal Impact

Many participants in the study were aware of the commercial impacts of ransomware, however a few discussed secondary consequences such as the social, political, or psychological effects of an attack. For example, one think Tank Digital Policy Advisor in Latin America claimed: "Attacks on consumer retail and travel organisations delivered a social impact which people notice". Some of the impacts of ransomware attacks are discussed below:

Reputational impact

Cyber attacks can result in reputational damage to the victim organisation if details of the incident become publicly known. In some cases, this is the direct goal of an attack (as in the case of online defamation), but it can also be a cascading effect of other forms of harm, such as data breaches or ransomware[51]. Knowledge of an attack may lead to customers, partners and staff losing confidence in the ability of the organisation to provide a secure and robust service which could in turn lead to lost present and future business. The reputational impact of ransomware is one of the most feared consequences of an attack and attackers often use this to their advantage, threatening to leak stolen data to the public if a ransom is not paid.

Financial impact

The financial implications of a ransomware attack can be severe. The 2022 IBM 'Cost of a data breach' report found the global average total cost of a data breach to be staggering $4.35M. The cost of an attack will vary with a number of factors: including the costs of operational disruption, recovery efforts, forensic investigation, and the ransom (if paid). Organisations with insurance may be able to recover some of these losses, however, may incur longer term costs due to increased future premiums. The overall cost of disruption is minimised by taking regular offline or cloud-based back-ups, allowing for critical business functions to be restored in the event of data loss or corruption.

Social impact

Although more challenging to quantify, attacks can also have considerable impact to the physical and psychological wellbeing of victims. The 2021 ransomware attack on the Irish Health Service Executive disrupted services at 41 hospitals and resulted in the cancellation of outpatient and radiology appointments across the entire system. Many routine check-up appointments had to be cancelled, including cancer screenings, maternity check-ups, and stroke services. Data of up to 520 patients was leaked online, including sensitive special category medical data. These outcomes were likely to cause significant physical and psychological stress to those affected.

Key cognitive issues are relevant to understand how the public are impacted by cyber attacks, including culture, attacker identity, and perceptions of risk[52]. Members of the public are more likely to respond to the effects of a cyber attack than the attack itself[53]. For example, an attack targeting critical infrastructure such as healthcare or electricity and gas would cause heightened worry or anger for the public.

[51] Agrafiotis, I., Bada, M., Cornish, P., Creese, S. Goldsmith, M., Ignatuschtschenko, E., Roberts, T. and Upton, D. M. (2016). Cyber Harm: Concepts, Taxonomy and Measurement - Working Paper 2016-23. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2828646

[52] Bada, Maria and Nurse, Jason R. C. (2019) The Social and Psychological Impact of Cyberattacks. In: Benson, Vladlena and McAlaney, John, eds. Emerging Cyber Threats and Cognitive Vulnerabilities. Academic Press, London, pp. 73-92. ISBN 978-0-12-816203-3. E-ISBN 978-0-12-816594-2. (doi:10.1016/B978-0-12-816203-3.00004-6)

[53] Minei & Matusitz, 2011; Gandhi, Sharma, Mahoney, Sousan, Zhu & Laplante, 2011

Civic impact

Ransomware can compromise both availability and confidentiality of systems and data, posing an operational threat as well as a risk to data. SME interviewees from Ukraine noted the civic impact of ransomware and other cyber attacks when they are deployed against government entities or critical infrastructure, with knowledge or even the rumour of successful cyber attacks able to limit civic participation. Cyber attacks against energy grids or transportation infrastructure created a sense of fear about using public transport, hampering economic participation. Meanwhile, unconfirmed rumours of Russian breaches of voter rolls and military conscription records from the Ukrainian government in March 2022 generated fear that participating in Ukrainian defensive efforts would lead to individual retaliation.

Political impact

"Political cyber harm is a broad concept that encompasses a range of effects on the government, the political system and its processes. It might be observed inter alia through a loss of public influence due to a cyber attack, a disruption of political processes, the exclusion of parties from the political process or deterioration in international relations, and is often accompanied by reputational cyber harm"[54]. State sponsored cyber-weapons are now a very real threat to governments – from espionage (e.g., Russian hacks into the Democratic Party computer system) to targeted attacks on components of national infrastructure (e.g., Estonia DDoS and Stuxnet). In Brazil, public institutions have been heavily targeted by mass data theft and ransomware incidents. There is a growing fear of cyber threats throughout the general population and a recent study found that only 13% of Brazilians consider their data to be very secure[55]. This lack of confidence in the country's digital infrastructure is a challenge which policymakers will look to address as Brazil works towards its aim of joining the OECD.

[54] Agrafiotis, I., Bada, M., Cornish, P., Creese, S. Goldsmith, M., Ignatuschtschenko, E., Roberts, T. and Upton, D. M. (2016). Cyber Harm: Concepts, Taxonomy and Measurement - Working Paper 2016-23. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2828646

[55] https://www.zdnet.com/article/brazilian-insurance-giant-porto-seguro-hit-by-cyberattack/

04

Policy Recommendations

04 Policy Recommendations

Based on the review of existing literature and analysis of our own research, we have developed:

- **Good practice principles that should underly the development of a long-term ransomware policy strategy and inform the decisions of policymakers.**
- **A set of specific good practice recommendations for policy prescriptions across the five DAP participant nations, as well as similar nations.**

Good practice principles for ransomware policy strategy

It is recommended that a ransomware strategy is developed, combining any or all of the specific policy recommendations outlined below based on resource constraints and political considerations, taken together with our guidance. Efforts to tackle ransomware threats should be implemented as part of a wider cybersecurity programme aiming to protect an organisation's data, assets, and services. Although it is the most feared vector of attack, ransomware is most commonly a symptom of broader security gaps which can equally lead to other incident types such as data wiping, keylogging, and phishing attacks. The recommendations provided aim to address these gaps at their root cause rather than alleviating their ransomware-specific symptoms. Consequently, many of these recommendations are not specific to ransomware attacks alone and should be considered by policymakers in the context of their wider cybersecurity agenda.

Based on our research, the authors recommend that any ransomware policy strategy enshrine the following principles:

The unique vulnerability of ransomware as a threat vector

Whilst ransomware can sometimes be deployed for destructive or geopolitical purposes and shares some traits with other modes of attack, it is fundamentally and somewhat uniquely a revenue-driven threat vector. Ransomware groups make the calculation that the pay-off from launching ransomware attacks is greater than the risk and monetary investment of executing them. Whilst some policy recommendations should focus on the uplift of cybersecurity capabilities generally, policymakers should also consider specifically how to disrupt the revenue model of ransomware groups, restrict their options in the way of targets, damage and destroy their infrastructure, and build a community-led defence hostile to their operations. (See Theme 6 for justification)

The mission-critical role of public-private sector partnerships

An effective ransomware policy strategy is infeasible without trust, cooperation and transparency between private sector organisations, government agencies, law enforcement, the judicial system, academia, non-governmental organisations (NGOs) and international partners. All stakeholders make a unique and indispensable contribution to efforts to disrupt the economic model of ransomware threat groups, and improve cybersecurity controls across multiple economic sectors. (See Theme 8 for justification).

Long term strategies coupled with short-term demonstrable successes

Securing long term legislative and executive investment in ransomware policy implementation requires a democratic mandate over an extended period of time. Long term policy strategies should therefore include consideration for how to demonstrate early, up front successes to the public to maintain legislative support and executive branch momentum. (See Theme 1 for justification).

A graduated approach to policy implementation and regulatory enforcement

Given the resources available to many developing economies, highly interventionist policy and regulatory strategies which place a high reporting or implementation burden on organisations are challenging to enforce. Policy strategies should consider approaches which incrementally shift the mechanism for assessing compliance, as well as the penalties for non-compliance, in line with cybersecurity capacity and maturity in key sectors. This may include starting with self-assessment, and shifting to independent assurance and then regulatory audits over time. (See Theme 3 for justification).

Civilian control of cybersecurity and ransomware resilience policies

Cybersecurity and ransomware resilience policies should be developed by a civilian-led independent cybersecurity agency which is: a) Functionally independent of the command structure of either military or intelligence services (and associated agencies or departments); b) Chartered with a mandate which includes the protection of civil liberties and rights to privacy; and c) Supervised by both legislative and judicial oversight bodies answerable to a democratic mandate. (See Theme 1 for justification).

Summary of policy recommendations

A set of policy recommendations are devised with consideration of the above good practice principles. These policy recommendations are divided into 4 policy clusters, and are summarised as follows:

Cluster 1 – Build effective partnerships for ransomware defence

Policies in Cluster 1 are concerned with the establishment of effective working relationships between the government, public sector departments, regulators and cybersecurity agencies, the private sector, major technology partners and international actors, with the aim of enabling a community-based defensive approach to ransomware.

Cluster 2 – Develop a community-based resilience architecture

Policies in Cluster 2 discuss capitalising on and better organising Cluster 1 partnerships by developing a national cybersecurity incident response team (CSIRT) that can coordinate and support response efforts to ransomware, understanding and allocate resources to different sectors based on an understanding of their resilience and cyber maturity, and facilitating cyber incident scenarios to test the response of individual organisations and sector ecosystems and supply chains.

Cluster 3 – Uplift cybersecurity skills and capacity

Policies in Cluster 3 centre around capacity and awareness building activities, including improving general cyber hygiene through public campaigns, the development of a cyber controls framework against which organisations can be certified, development of specific cyber skill sets through train-the-trainer models and higher education partnerships and international collaboration.

Cluster 4 – Define a regulatory response to ransomware

Policies in Cluster 4 focus on the regulatory and legislative response to ransomware, offering recommendations on approaches to regulating ransom payments, cyber insurance provision, and breach disclosure, and considerations on how to implement a third-party assurance regime for mature sectors to improve resilience to ransomware and other cyber attacks.

Detailed policy recommendations

Under the 4 clusters, we have outlined summaries of the 16 key policy recommendations that underly them.

Cluster 1 – Build effective partnerships for ransomware defence:

- **1.1** Establish collaborative modes of working with major technology partners
- **1.2** Develop incentives to encourage private sector businesses to share cyber threat intelligence (CTI) with peer organisations, suppliers, customers, and governments
- **1.3** Develop a framework for international collaboration and engagement with other national governments and international law enforcement organisations
- **1.4** Implement a community defence framework to actively disrupt ransomware revenue streams, operating models, and infrastructure

Cluster 2 – Develop a community-based resilience architecture:

- **2.1** Develop a target operating model (TOM) for a national cybersecurity incident response team (CSIRT) and ransomware response policies
- **2.2** Benchmark key economic sectors to understand weaknesses and single points of failure in critical national infrastructure (CNI)
- **2.3** Run industry ransomware incident response exercises and resilience tests with CNI sectors and industry and technology partners

Cluster 3 – Strengthen cybersecurity skills and capacity:

- **3.1** Run consumer- and small-to-medium enterprise (SME)-targeted training and awareness campaigns in ransomware defence and broader cybersecurity hygiene
- **3.2** Develop a foundational cybersecurity controls framework for minimising ransomware attacks and create a pathway to certification
- **3.3** Build private, public sector and justice system skillsets in critical ransomware response capabilities to meet skills gaps
- **3.4** Develop higher education programmes and academic partnerships with universities to enable skills sharing and research
- **3.5** Attract key cybersecurity skillsets through easing of visa requirements for foreign nationals with desired technical or industry backgrounds

Cluster 4 – Define a regulatory response to ransomware:

- **4.1** Make regulatory decisions about whether to accept the payment of ransomware ransoms, and the provisions of cyber insurance providers
- **4.2** Require disclosure of data breaches and cyber attacks resulting from ransomware
- **4.3** Require a baseline third party assurance regime for the most cyber capable sectors which covers ransomware response capabilities
- **4.4** Establish regulation and compliance controls on the cryptocurrency market to hamper ransomware operators from monetising their efforts.

There are numerous lower-level policies underlying the 16 key policy recommendations outlined above, amounting to some 50 specific actions.

Classification of policy recommendations

We have classified policies as either "Formative" (F), "Established" (E) or "Strategic" (S). The classification is issued based on the level of maturity of a developing nation's cybersecurity strategy one would expect to be in place, prior to the implementation of a policy. The level of maturity is defined per cluster, as below:

Cluster	Cluster 1 - Collaboration / partnerships	Cluster 2 – Resilience / community defence
F Formative	Occasional joint working between private sector firms, major technology partners and government bodies Informal, ad hoc mechanisms of cooperation or intelligence sharing	Basic understanding of maturity of critical national infrastructure sectors Early-stage national cyber incident response team with limited connectivity into private sector
E Established	Transactional working relationships between private sector partners and government bodies in place Mechanisms of intelligence sharing, and collaboration established but with limited follow through to active defensive activity	Reasonable understanding of maturity of CNI sectors based on informal relationships with private sector Operable cyber incident response team with some capacity to effectively respond to incidents
S Strategic	Mutual, trust-based working relationships between public and private sector partners and agencies Effective mechanisms of collaboration and information sharing which inform active defence efforts	Systematic understanding of maturity of CNI sectors Mature incident response team prioritising resources for vulnerable sectors Good relationships with private sector firms with capacity to run major exercises

Cluster	Cluster 3 - Skills / capacity	Cluster 4 - Regulation
F **Formative**	Limited cybersecurity skillsets or awareness among private sector organisations or citizenry / consumers Some, limited opportunities to build skillsets through training / further education; ad hoc programmes in place to improve awareness	Limited regulatory environment with insufficient legislative consensus on approaches to regulating cybersecurity Limited ability to enforce regulatory requirements on private sector
E **Established**	Longer term awareness programmes defined and in place Training / education programmes in place to improve skillsets, including established higher education programmes Guidance from government cyber bodies provided to set basic cybersecurity foundations	Tactical regulations in place with moderate legislative consensus on how to approach cybersecurity regulation Some enforcement capability but reluctance from private sector to comply
S **Strategic**	Strategic, targeted programmes of awareness established alongside higher education and training schemes leveraging partnerships with multiple stakeholders Regular guidance from cybersecurity government bodies focussed on a foundational set of cybersecurity controls	Strategic regulatory environment based on a high-momentum legislative consensus and private sector cooperation Enforcement and compliance monitoring processes; transparent working relations between regulators and private sector

Cluster 1 – Build effective partnerships for ransomware defence

Policy 1.1: Establish collaborative modes of working with major technology partners.

Thematic analysis of the interviews conducted found that strong public-private partnerships were considered by policymakers to be an essential component of a comprehensive national security strategy. Governments should proactively and formally engage with large technology providers on matters of national security to leverage their resources and expertise. By fostering such partnerships, critical national infrastructure organisations would have access to a larger pool of digital forensics, incident response and threat intelligence skills which would increase the sector's resilience to ransomware attacks. In order to facilitate long-term trust and mutual benefit, it is important that a framework for public-private engagement is established in order to manage the associated risks. For example, engagement with multi-national corporations can create diplomatic conflicts of interest where the organisation has existing relationships with other nation states. The framework should also manage corruption risks by implementing independent oversight of contracts awarded.

Policymakers may choose to:

F **Designate cyber agency representatives to partner with major technology partners (i.e., software and hardware vendors, cloud service providers) to develop standard cyber service contracts that can be leveraged by organisations who use their services in CNI sectors. Cyber services may include:**

- Back up and resiliency services.
- Data-at-rest and data-in-transit encryption solutions.
- Managed monitoring and threat hunting services (including for email services).
- Threat intelligence monitoring and dark web scanning services.
- Skills sharing and incident response resource augmentation.
- Training and awareness services.

F **Develop rules of engagement with major technology partners, including consideration of:**

- The need for strictly voluntary engagement with partnership arrangements by organisations in designated CNI sectors.
- Maintenance of separation between technology partners and defence/ intelligence community.
- Consumer and national security safeguards over arrangements whereby data or commercial contracts are exchanged for partnership arrangements.
- Engagement of foreign ministry contacts to gain permission from host government to engage international technology partners.
- Supervision and oversight of partnership arrangements and impact on tendering for other related and non-related government services.

Policy 1.2: Develop incentives to encourage private sector businesses to share cyber threat intelligence (CTI) with peer organisations, suppliers, customers, and civilian-facing government cyber agencies.

Consumption and contextualisation of threat intelligence feeds can enable organisations to detect malicious activity during the early stages of an attack, thwarting the threat actor's final objectives of deploying ransomware or exfiltrating company data. Whilst many commercial feeds are available, governments can play a key facilitating role in the dissemination of threat intelligence by providing a platform for the sharing and curation of threat data. One example of good practice from the UK public sector is the National Cybersecurity Centre's 'Early Warning Service', free to all UK organisations. The service processes a number of UK-focused threat intelligence feeds from trusted public, commercial and closed sources to notify subscribed organisations to potential vulnerabilities, threats, or network abuses against them. The service is fully funded by the NCSC and gives many UK businesses increased confidence in the security of their network. It is a good example of the security benefits experienced by businesses (large and small) when government agencies collaborate effectively with their private sector and international technology partners.

Policymakers may choose to:

F **Establish a public outreach programme to emphasise the benefits of public-private partnerships and information sharing, with a target of attracting input from small-to-medium enterprises and encouraging CNI organisations to join.**

F **Establish forum and platform rules and oversight, which may include consideration of:**

- Independence of the forum from regulatory oversight bodies, intelligence, and defence services to enable transparency among members.
- Code of conduct discouraging or banning presentations by cybersecurity vendors with the aim of selling of solutions and services, to avoid overly-commercialised cultures that de-emphasise information sharing and idea exchange.
- Mechanisms to enable the sharing of incident data anonymously, including details of cryptocurrency-based ransom payments and chat logs with ransomware groups.
- Data quality standards and template data layouts to better organise and automate the analysis of threat intelligence data over time.
- Rules governing the formatting and use of threat intelligence and incident data by other forum members.
- Regularly updating collaboration mechanisms and incentives based on lessons learned and the changing threat landscape.

E **Develop an agency-led government cyber threat intelligence (CTI) sharing forum for private sector partners, along with a data sharing platform to host CTI and indicators of compromise provided by member organisations.**

E **Develop incentives for private sector partners to share cyber threat intelligence. These may include:**

- Financial incentives, including tax incentives for participation.
- Resource and service incentives, e.g. access to cybersecurity services provided by major technology partners, or to government cyber incident response services.
- Regulatory amnesty on data breach fines where ransomware incident log data has been provided for analysis and sharing with other members.
- Access to other organisations' shared threat intelligence data.

E **Assign a central cyber agency resource to curate and manage content uploaded to the platform by members, managing duplicate data and structure information received by members into actionable intelligence.**

Policy 1.3: Develop a framework for international collaboration and engagement with other national governments and international law enforcement organisations.

Cybercriminals operate across borders, often targeting IT infrastructure many thousands of miles away. A problem of international scope, ransomware requires a solution of international proportions. By developing and implementing a strategy for engagement with the international cybersecurity community, domestic organisations can benefit from the intelligence and skills generated by this community. By coordinating with foreign and international law enforcement agencies (e.g. Interpol, Europol), policymakers can build their capacity to target ransomware operators, criminal infrastructure, and monetary proceeds outside of their immediate jurisdiction. In developing this framework, policymakers will need to consider their country's capacity to contribute to this international community and the political will to implement any actions it agrees upon.

One example of effective coordination, the Counter Ransomware Initiative[56] aims to build collective resilience to ransomware, disrupt operations and counter illicit finance that underpins the criminal ecosystem. A part of this initiative, the voluntary International Counter Ransomware Task Force (ICRTF) will facilitate collaboration with members of the initiative and key private sector partners.

Policymakers may choose to:

F **Establish a senior cybersecurity coordination role in the Ministry of Foreign Affairs or Office of the Secretary of State or equivalent, with a mandate to:**

- Engage with allied governance cybersecurity agencies to share intelligence and collaborate over the identification and tracking of international ransomware groups.
- Continue dialogues with other nation states to achieve sustained commitment on capacity build exercises and incident response support.

F **Establish a senior cybersecurity coordination role in the Department of Homeland Security or equivalent, with a mandate to:**

- Attend and contribute to collaboration forums on behalf of the government; these may include major security conferences, the Global Forum on Cyber Expertise, the Global Cybersecurity Alliance, the World Economic Forum's Centre for Cybersecurity and the International Information Integrity Institute (i-4).
- Engage with international law enforcement organisations such as Interpol, on behalf of the government or domestic private sector organisations, to trace cryptocurrency ransomware payments and prosecute ransomware groups.
- Engage with major technology partners based in international jurisdictions and gain support for domestic community defence initiatives.

S **Develop domestic processes for:**

- Develop processes by which information is shared with international law enforcement partners with the aim of supporting multi-jurisdictional prosecutions of ransomware actors.
- Preserving and sharing forensic evidence from domestic ransomware attacks such that they can be used as the evidentiary basis for prosecution in international jurisdictions.
- Cooperating with international law enforcement bodies and legal bodies on tracing and prosecuting domestic ransomware groups attacking international organisations.
- Updating monitoring and response capabilities based on lessons learned.

[56] https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/

Policy 1.4: Implement a community defence framework to actively disrupt ransomware revenue streams, operating models, and infrastructure.

Policymakers should bring together stakeholders from across government and industry in order to disrupt ransomware operations. A community defence framework would bring specialised incident response and digital forensics training to law enforcement and members of the judiciary in order to grant the authorities the expertise required to investigate, attribute, and prosecute cyber criminals operating within their jurisdiction. The framework would also oversee engagement with private sector parties such as ISPs, cloud providers and crypto-exchanges aiming to target ransomware IT infrastructure and revenue streams.

Policymakers may choose to:

F **Designate cyber points of contact in law enforcement agencies to enable sharing of forensic evidence of ransomware attacks by private sector organisations and government bodies, with the aim of gathering actionable intelligence on ransomware groups**

E **Develop an active cyber defence framework owned by the government cybersecurity agency to incentivise market-wide information sharing and active threat hunting by cyber-capable industry players and broader information sharing**

E **Utilise international support and cyber capacity building partnerships to develop and deliver initial training courses to law enforcement professionals and judicial branch stakeholders on:**

- Key cybersecurity and computer network-related concepts which can allow police officers to have productive discussions with organisations who are the victim of ransomware.
- How to give advice on the timely capture of forensic evidence to the victim organisation, including compromise methods, ransom demands and payments.
- How to curate and protect forensic evidence of ransomware attacks and maintain chain of custody, such that they are admissible in a court of law.
- Negotiation tactics with ransomware groups, which can be deployed to lower ransom demands and buy time in which forensic investigation and root cause analysis can be performed.

E **Develop exchange programmes for law enforcement and judicial bodies at regional and international level to enable the transfer of skills and knowledge.**

E **Establish mechanisms by which private sector organisations can seek emergency injunctions on the publishing of breached data leaked by ransomware groups.**

S **Work with cryptocurrency exchange platforms to establish mechanisms of tracing cryptocurrency payments through to ransomware actors' cryptocurrency wallets, and monitoring the exchange of cryptocurrencies into fiat currencies.**

S **Work with technology providers to identify and coordinate takedowns of criminal technology infrastructure that may exist in the country.**

S **Consider the use of offensive cyber tactics to take offline dark web repositories of breached data.**

Cluster 2 – Develop a community-based resilience architecture

Policy 2.1: Develop a target operating model (TOM) for the national cybersecurity incident response team (CSIRT) alongside policies for governing ransomware response.

The establishment of a national CSIRT is an essential step in building cyber capacity within a country. When a ransomware incident occurs, a CSIRT will nationally orchestrate a response by alerting relevant stakeholders, facilitating information exchange, and coordinating actions. To conduct this role effectively, the team must be adequately resourced with a well-defined operating model and mandate for response. Interviews found that national CSIRTs in developing countries are often understaffed and lack the capacity to support the incidents they are alerted to. Consequently, organisations are less likely to notify the national team of ransomware attacks against them. This is in contrast to more mature sectors such as financial services, where industry CSIRTs traditionally have a much larger pool of skills and technology to choose from.

Policymakers may choose to:

F **Establish a governance structure for hierarchy of sector-specific and nationwide cybersecurity incident response teams (CSIRTs), including:**

- Terms of reference for key governance and oversight committees run by the relevant government-led cybersecurity agency.
- An independent oversight mandate to oversee CSIRT operations, make recommendations to uplift process efficiency and effectiveness, allocate budgets and ensure responsible and ethical execution of CSIRT responsibilities.
- Mechanisms of consulting with and evaluating recommendations from both private and public sector organisations who utilise CSIRT services.

F **Establish a resourcing model for the national and sector CSIRTs, which may include:**

- Key roles and responsibilities, interaction models and working hours of CSIRT team resources.
- Secondment of private sector cybersecurity professionals to act as CSIRT leaders, with an aim to alleviate likely resourcing and skills challenges whilst also improving engagement with private sector partners.
- Use of capacity provided by international partners to train CSIRT resources, and also provide train-the-trainer models which build local support capacity.
- Oversight rules for resourcing which minimise the risk of overfamiliarity or undue private sector influence into government cybersecurity policy.

E **Establish key CSIRT operational procedures and processes, including:**

- Playbooks for incident response scenarios, including for ransomware technical response, negotiation, and forensic investigation.
- Communications plans and escalation pathways between CSIRT resources, private and public sector organisations.
- Rules of engagement between the CSIRT and law enforcement or regulatory bodies, on behalf of private or public sector organisations who request support.
- Communications and cooperation linkages between various sector and national CSIRTs, and emergency coordination and response plans for nationwide ransomware attacks targeting critical infrastructure.
- Continuous engagement with private and public sector organisations, threat intelligence sharing forums and major technology partners.
- Processes for the timely production and dissemination of vulnerability / threat advisory notices.

Policy 2.2: Benchmark key economic sectors to understand weaknesses and single points of failure in critical nation infrastructure (CNI).

Policymakers should identify the infrastructure, data, networks, and processes necessary for the country to function. One example of good practice for CNI security is the UK's establishment of a government agency dedicated for this purpose, the Centre for the Protection of National Infrastructure (CPNI). The agency has defined 13 national infrastructure sectors and has designated one or more Lead Government Department(s) responsible for ensuring the security of the critical assets in each sector[57]. Whilst responsibility for the protection of CNI IT from ransomware attacks sits with the National Cyber Security Centre, CPNI works in partnership with the NCSC to deliver advice which considers all aspects of protective security. The CPNI thus ensures a holistic approach to the protection of CNI and established clearer lines of accountability in the event of a ransomware attack or other national security incident.

Policymakers may choose to:

✓

F **Invite voluntary participation from private and public sector organisations in a cybersecurity capacity benchmarking exercise, led by the government cybersecurity agency. The exercise would seek to:**

- Understand the maturity of organisations within the country with regard to key cybersecurity processes, controls, and response capabilities.
- Understand how capabilities vary across different sectors, organisation sizes and structures.
- Find examples of good practice among mature and highly capable organisations which other organisations can replicate and learn from.
- Identify which sectors constitute critical national infrastructure (CNI), and which individual organisations form critical parts or even single points of failure of CNI sector supplier ecosystems.
- Identify which sectors are most vulnerable to major cyber attacks, with the aim of prioritising capacity building efforts and access to CSIRT response services for these sectors.
- Identify which sectors are most likely to be targeted by ransomware groups specifically, considering (1) Organisations' capacity and willingness to make ransom payments; (2) Their ability to prevent and respond to ransomware attacks, and ability to engage support services; and (3) Ransomware groups' potential hesitancy over attacking organisations who are part of critical national infrastructure, given attacks' propensity to trigger a geopolitical, intelligence- or law-enforcement led response. (See Appendix: Who do ransomware groups target?).

[57] Critical National Infrastructure | CPNI

Policy 2.3: Run incident response exercises and resilience tests with CNI sectors and industry partners.

Incident response exercising identifies potential gaps in the ability of an organisation to respond to ransomware attacks and enhances the collective decision-making process of the participating teams and stakeholders. One example of this in practice is ENISA's large-scale and cross-sector cybersecurity exercises[58]. Another demonstration of the positive impact which government agencies can have on their country's resilience, the UK NCSC's exercise-in-a-box is an online too which helps organisations test and practise their response to an attack[59]. This free resource includes guidance for set-up, planning, delivery, and lessons-learned activity for a range of incident types (including ransomware) and does not require expertise to use.

Policymakers may choose to:

E **Enable the CSIRT to conduct sector-specific ransomware incident response exercises and scenario tests with CNI organisations and their partners. As discussed in the analysis section, these exercises are most impactful when the CIRT has a legal mandate for response and organisations have well-defined roles and responsibilities. The exercises should test and document lessons learned against:**

- Technical capability to identify ransomware indicators of compromise, contain lateral movement, isolate infected devices, and restore systems from back up.
- Ability to engage major technology providers, the CSIRT or private incident response service providers in response to an attack, and preserve forensic evidence required for attribution and prosecution.
- Ability to manage communications with affected customers, media, public sector bodies, law enforcement, regulators and security or intelligence agencies as required.
- Ability to manage communications with ransomware groups following an attack.

E **Require the CSIRT to conduct regular sector-wide ransomware attack scenarios, simulating the possibility of a larger scale attack impacting multiple organisations within a sector.**

E **Ensure that lessons learned from ransomware incident response exercises are used to inform the national cybersecurity strategy and crisis management plan.**

[58] https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises

[59] https://www.ncsc.gov.uk/information/exercise-in-a-box

Cluster 3 – Uplift cybersecurity skills and capacity

Policy 3.1: Run consumer- and small-to-medium enterprise (SME)-targeted training and awareness campaigns in ransomware defence and broader cybersecurity hygiene.

Many SMEs lack the resources and skills to necessary for a robust and comprehensive security programme, leaving them exposed and dependent upon third-party support in the event of an incidents. SMEs are however under an increasing pressure to address these security challenges and comply with legislation and good practice standards. In addition to representing a large segment of the economy, SMEs are embedded within key and critical national infrastructure supply chains. Policymakers should consider developing security awareness campaigns targeted at SMEs as well as providing clear guidance on the controls and processes necessary to coordinate an effective response to a ransomware attack.

Policymakers may choose to:

F **Develop a simple cyber hygiene checklist for consumers and small-to-medium enterprises (SMEs), consisting of good practice around:**

- Clicking on phishing links and responding to text scams.
- Use of spam filters and email scanning solutions.
- Downloading suspicious files to their devices.
- Separating work and personal communications devices.
- Using encrypted channels for private communication.
- Secure disposal of confidential waste.
- Use of separate secure passwords and multi-factor authentication.
- Use of VPNs, anti-virus solutions and basic firewall solutions.
- Use of back up services and cloud redundancy, including offline back ups.

F **Develop a communication strategy and multi-media awareness-raising campaign to socialise good practice among the population, with the aim of improving general understanding of cybersecurity best practice principles and limiting the ability of ransomware to spread. Examples of such capacity building initiatives include 'Strengthening Awareness and Trust to Improve National Cybersecurity Governance in Brazil'[60] and the implementation of the UK's 'Get Safe Online' campaign[61] which aimed to provide factual and easy-to-understand information on online safety. Such a strategy can include messaging around:**

- The value of public-private sector partnerships in improving the resilience of the economy and people's livelihoods against ransomware.
- The importance of mutual, community defence against ransomware groups and other cybercrimes.
- Options for how to utilise free or negotiated cybersecurity services provided by major cloud services or major technology partners for the benefit of consumers and SMEs.
- Details of how to contact or request the support of government cybersecurity agencies, industry CSIRTS and industry-specific cybersecurity bodies.

[60] https://cybilportal.org/projects/strengthening-awareness-and-trust-to-improve-national-cybersecurity-governance-in-brazil/

[61] https://www.getsafeonline.org

- Details on the importance of incident reporting and guidance on how to do so.

🟢 **Leverage international support to create a train-the-trainer programme for general cybersecurity awareness, with international cybersecurity SMEs coaching local cyber service providers and businesses on how to provide low-cost training to consumers and SMEs. For example, policymakers should consider the use of ENISA's Good Practice Guide on Training Methodologies[62] aimed at guiding novice and experienced trainers to design and deliver successful security trainings.**

🟡 **Organise cyber awareness and education programmes (including trainers, delivery models and training resources) offering low-cost delivery of cyber awareness training to:**

- School and education systems, targeting students with the aim of encouraging more students to educate themselves on cybersecurity.
- Critical infrastructure sectors with limited resources such as health and social care; and
- Small-to-medium enterprises in any sector (for example NCSC's Small Business Guide: Cyber Security[63]).

E **Provide self-service training materials and cybersecurity awareness videos through website of a civilian-facing government cybersecurity agency, which are updated annually or upon intelligence of specific threats or new ransomware vectors.**

E **Provide guidance on the decision-making processes, roles and responsibilities which need to be predefined in order to respond to a ransomware attack. Examples of good practice include the NCSC's guide on mitigating malware and ransomware attacks[64] and the UK Information Commissioners Office (ICO) guidance on ransomware and data protection compliance[65].**

Policy 3.2: Develop a foundational cybersecurity controls framework for minimising ransomware attacks and create a pathway to certification.

A foundational controls framework would provide organisations with good practice guidance to help them defend against the most common cyber threats. The framework would provide a benchmark against which organisations can self-assess themselves and discover gaps in their security perimeter. This provides the organisation with a clearer picture of their present security posture and would provide reassurance to new and existing customers that their data is protected. Policymakers should consider ways of protecting the integrity of a certification linked to the standard, for example the establishment of an independent oversight body and regular audits of certification quality.

Policymakers may choose to:

✓

F **Adopt and promote security benchmarks for organisations to self-evaluate against best practices. For example, the benchmarks developed by the Center for Internet Security[66]are a set of globally recognized and consensus-driven best practices to help security practitioners implement and manage their cybersecurity defences for over 25 different vendor products.**

F **Develop or build on existing cybersecurity controls frameworks aimed at minimising the likelihood and impact of ransomware attacks and other cyber threat vectors. The framework should be owned by the government cybersecurity agency and be regularly updated, developed with the consultation of a wide range of industry stakeholders and sectors, including but not limited to good practice on:**

[62] https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies

[63] https://www.ncsc.gov.uk/collection/small-business-guide

[64] https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

[65] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ransomware-and-data-protection-compliance/

[66] https://www.cisecurity.org/cis-benchmarks/

Executive Summary
Literature Review
Analysis
Policy Recommendations
Conclusion

- Cybersecurity governance and policies.
- Cybersecurity in internal audit and risk management.
- Third party risk management.
- Training and awareness.
- Security skills and expertise management.
- Human resource risk management, including background screening and insider risk management.
- Consumer and enterprise identity and access management, including authentication, authorisation and privileged access management.
- Physical security and behavioural hygiene.
- Hardware, software and information asset management.
- Secure development lifecycles and application / API security.
- Device configuration and hardening, and vulnerability and patch management.
- Cryptographic key and certificate management, including encryption of data at rest / in transit.
- Cloud security governance.
- Email and web browser security, and malware and anti-virus protection.
- Network resilience and boundary defences, including security of wireless / remote access.
- Security event logging, monitoring and analysis.
- Data and system back up and archiving.
- Security incident and event management, security operations, incident response, penetration testing and red teaming.
- Disaster recovery, business continuity and operational resilience.
- Where applicable: Security of operational / industrial technology solutions, and IoT (hyperconnected) devices.

F **Establish a mechanism by which organisations can self-assess their cybersecurity controls against the published framework and understand gaps against best practice.**

E **Establish a mechanism by which organisations can achieve certification against the published framework, including:**

- An accreditation body answerable to the government cybersecurity agency, with the ability to accredit suitably skilled organisations to independently assess and certify other organisations against the framework.
- A mechanism of reducing down or setting minimum requirements for certification against the published framework and for the rigour of control attestation, based on:
  - The applicability of controls to an organisation
  - The size and cybersecurity capability of the organisation
  - The criticality of their services and role in critical national infrastructure
- An incentive structure for organisations to achieve certification against the framework, including but not limited to: reduced security due diligence during contract tenders; advertising certification against the framework to customers; access to remedial advice and solutions, and to community defence initiatives.
- An independent oversight body tasked with establishing ethical standards for organisations accredited to certify, conducting regulatory audits of certification quality, and limiting bribery and corruption risk associated with the certification scheme.

Policy 3.3: Build private, public sector and justice system skillsets in critical ransomware response capabilities to meet skills gaps.

In the UK, the annual DCMS study of cybersecurity skills in the UK labour market consistently reveals a lack of basic cyber skills, with the 2022 results indicating that 51% of private sector businesses have a basic skills gap in relation to technical cybersecurity[67]. The cybersecurity workforce shortage is comprised of two elements: a skills gap (those responsible for cybersecurity lacking the appropriate skills) and a skills shortage (a lack of people available to fill positions in cybersecurity). Initiatives such as 'train-the-trainer' programmes upskill domestic cybersecurity professionals, leading to a positive 'trickle-down' effect of cybersecurity skills and awareness to local businesses.

Policymakers may choose to:

F **Develop train-the-trainer programmes to enable international partners to train domestic cybersecurity businesses in upskilling local businesses on key cybersecurity disciplines, and in certifying against published frameworks, with a focus on ransomware controls and response processes.**

E **Establish annual competitions in partnership with major technology providers in which small-to-medium cybersecurity businesses and service provider can compete to develop solutions to technical- or process-level cybersecurity challenges identified by government cybersecurity agencies or industry forums. Incentives for participation and investment may include:**

- Investment and co-development by technology partners in winning solutions
- Access to government cybersecurity support services
- "Preferred provider" status for relevant government contracts for security, subject to appropriate due diligence and certification
- Financial incentives to support solution development
- Exposure to national and international cybersecurity leaders

S **Establish CISO and CEO forums with the aim of:**

- Educating security leaders on how to take advantage of capacity building partnerships and train-the-trainer programmes
- Giving enterprise security leaders a forum through which to engage on key cybersecurity matters, as well as raise requests for new government initiatives and improvement of existing programmes of work

[67] DCMS (2022). Cyber security skills in the UK labour market 2022. https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2022

Policy 3.4: Develop higher education programmes and academic partnerships with universities to enable skills sharing and research.

The international cybersecurity skills gap requires a long-term strategy which embeds cybersecurity skills in the STEM curriculum of schools and universities and makes students aware of the career opportunities available for them in this area. Policymakers should encourage domestic cybersecurity firms to become an agent for change by offering more apprenticeship opportunities to train emerging talent. One example of good practice in this domain is the Ad Hoc Working Group on the European Cybersecurity Skills Framework[68]. The working group develops cybersecurity programmes for higher education and seeks to identify and fund cybersecurity research priorities. The movement of skills between education and the private sector will play a key role in closure of the cybersecurity skills gap.

Policymakers may choose to:

E **Establish a working group composed of higher education institutions, private sector organisations and international partners, tasked with developing a series of higher education programmes in cybersecurity disciplines Development activities may consist of:**

- A gap analysis of the private sector to understand cybersecurity technologies and skillsets, utilising sector benchmarking activities carried out as part of Policy 2.2 to understand priorities for academic qualification pathways.
- Align cybersecurity education programmes with practical problems and challenges of the evolving cybercrime landscape.
- Use of skills and resource provision by international partners to create fast-tracked lectureship and professorship roles in major academic institutions to teach key disciplines, as well as offering options for visiting professors from higher education institutions in international partner countries.
- Establishment of fast-tracked Bachelor and Masters programmes for new students of cybersecurity courses.
- Incentives for students to take on higher education programmes in cybersecurity, including:
  - Engagement as part of courses with major technology partners and private sector partners.
  - Fast-tracked transition programmes that enable transfer from other higher education disciplines into cybersecurity; these may target other disciplines with transferrable or desirable skillsets, such as financial crime or technology.
  - Offers of partially or fully subsidised courses in cybersecurity to incentivise uptake of courses by prospective students.
  - Offers of guaranteed jobs with private sector organisations post-qualification, sponsorship by private sector organisations in exchange for a commitment to employment, or offers of guaranteed year-in-industry placements as part of education programmes.

S **Establish forums for partnerships between private sector organisations and higher education institutions to identify and fund cybersecurity technical research priorities. For example, the European Cybersecurity Industrial, Technology and Research Competence Centre[69] will pool expertise and align development and deployment of cybersecurity technologies. The centre works with industry and the academic community to build a common agenda for cybersecurity investments and research funding.**

[68] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls

[69] https://cybersecurity-centre.europa.eu/index_en

Policy 3.5: Attract key cybersecurity skillsets through easing of visa requirements for foreign nationals with desired technical or industry backgrounds.

As the number of internet users has increased, there has developed a widening digital skills gap and the undersupply of cybersecurity professionals is now estimated to reach more than 3 million worldwide[70]. One challenge for policymakers managing this gap is the migration of skills in and out of the country. A holistic approach must be taken to create a high-skill migration regime that encourages mobility for workers in certain high-skill sectors.

S **Agree eased visa requirements for entry of domestic citizens with desired cybersecurity skillsets or on cybersecurity education schemes into international partner countries, with the aim of enabling them to accrue skills, education, and experience. Eased requirements with international partners should be coupled with strong incentive programmes to return to work or study in local organisations or academic institutions.**

Policymakers may choose to:

F **Ease short-term exit and entry requirements for both private sector cybersecurity personnel and students of higher education cybersecurity courses, with the aim of enabling domestic personnel to attend international conferences and cybersecurity forums, and foreign personnel to attend domestic equivalents.**

E **Ease entry visa requirements for skilled migrants with desired cybersecurity skillsets useful for ransomware management, including technical control disciplines, incident response and recovery processes, and ransom negotiation tactics. Eased entry requirements may be coupled with strong incentive programmes to remain in country, agreed with international partner countries.**

[70] Chandrasekhar, C. and Mee, P. 2021. "Why businesses and governments must fight cyber threats together". World Economic Forum Global Agenda. 3 May 2021. https://www.weforum.org/ agenda/2021/05/ cybersecurity-governments-business/

Cluster 4 – Define a regulatory response to ransomware

Policy 4.1: Make regulatory decisions about whether to accept the payment of ransomware ransoms, and what cyber insurance providers are able to cover.

The regulation of ransom payments is one of the most hotly debated cybersecurity issues among policymakers today. As ransomware attacks have proliferated and victims are paying up to mitigate the damage, there are growing calls to ban ransom payments and prevent insurers from covering them. It follows that if businesses are less likely to pay, the ransomware business model will become less lucrative, disincentivising further attacks. Others however believe this to be an oversimplification, expecting that if ransom payments are banned, attackers will simply turn their focus to public serving organisations such as hospitals, power stations and schools. By targeting these institutions, the criminals may expect the social harm caused by the attacks to apply sufficient pressure to the authorities that the ransom is paid.

Even if ransomware payments were banned, policymakers would face a number of obstacles to enforcing the law. If banning economic behaviours required for survival was completely effective, there would be no illegal drugs trade or black market for human organs[71]. Instead of encouraging businesses to notify regulators and data subjects of a breach, victim organisations may choose to pay a ransom in secret if it represents their best chance of survival. Enforcement of such legislation may therefore reduce the transparency with which businesses handle ransomware attacks and could lead to declining trust between private sector and the regulators. Furthermore, the outlawing of ransom payments would only have the desired societal effect if a blanket ban was imposed, since any sectors exempt from the ban would be heavily targeted. In practice however, prosecution may lack the will to charge executives of CNI organisations such as hospitals and power-stations who have paid a ransom to save lives or to enable local communities to power their homes. A ban could then result in these important public-serving organisations being targeted disproportionally.

At the root of this issue is the misalignment of the victim organisation's priorities with the collective harm caused by ransomware. In many jurisdictions, the choice of ransom payment is a business decision left to the victim organisation. Since the duty of the organisation's leadership is to restore operations and recover data, many will choose to pay the ransom if this the quickest and least expensive way of achieving these aims. The collective public interest is not a priority for the organisation's leadership at this time and therefore they may be incentivised to pay the ransom, even if this leads to further attacks in their industry in the future. Unless policymakers can identify a mechanism to encourage victim organisations to consider the public interest, a zero-tolerance ban on ransom payments will be of limited effect.

[71] https://www.brookings.edu/techstream/should-ransomware-payments-be-banned/

Policymakers may choose to:

E **Make the payment of ransoms demanded by ransomware groups:**

- Completely illegal under threat of punitive measures, with the aim of creating a culture of non-payment across the country such that ransomware groups are deterred from even launching attacks.
- Legal but with compulsory reporting of payments
- Legal only in circumstances where the attack presents an existential threat to the organisation, and where all avenues of containing, responding, and recovering have been exhausted with no reasonable possibility of success.
- Legal under a limited range of circumstances, notably where there is either:
  - A direct and imminent threat to human life arising from the suspension of some services as a result of a ransomware attack, for which there is no manual workaround that can alleviate pressure; or
  - A direct and imminent threat of large scale, catastrophic environmental damage as a result of the suspension of services as a result of a ransomware attack; or
  - A release of data with imminent and large-scale consequences to national security has been threatened, for which it has been possible to guarantee no other copies of the data exist and that the ransoming party does not have ongoing access.

S **Put in place rules to regulate the provision of cyber insurance, considering the mandate for insurers to:**

- Set exclusion criteria for coverage such as the exclusion of geopolitically motivated cyber attacks;
- Exclude coverage of ransomware ransom payments based on legality;
- Provide access to incident response services and incident forensic capabilities;
- Mandate fulfilment of regulatory obligations such as breach disclosure prior to pay out;
- Mandate and conduct audits to verify minimum levels of cybersecurity controls and pre-condition for coverage or else for pay out.

Policy 4.2: Require disclosure of data breaches and cyber attacks resulting from ransomware.

A number of countries and jurisdictions have implemented legislation requiring organisations to report breaches of personal data to a designated supervisory authority. Such a breach could have significant impact to the individuals whose data was affected and the authority ensures that adequate steps are taken by the organisation to protect these individuals. One of the earliest examples, the EU's General Data Protection Regulation (GDPR), came into force in May 2018 and was designed to give EU data subjects control with regards to how their data is processed, stored, or transmitted. It also mandated that data breaches be disclosed to respective EU regulatory bodies within 72 hours of discovery, setting a significant new precedent. GDPR was quickly followed elsewhere by similar legislation including Brazil's General Personal Data Protection Law (LGPD) and the California Consumer Privacy Act (CCPA). In 2022, the US passed the Strengthening American Cybersecurity Act and the Cyber Incident Reporting for Critical Infrastructure Act o which among other requirements, mandated disclosure of breaches within 24 hours. The government of India followed by mandating a 6-hour window for cyber attacks to be reported to the government's cyber emergency response team (CERT-In).

To affect long-term improvements in security culture, legislation must be backed by the political will, skills, and capacity to enforce it. Discussions revealed that whilst many nations do mandate the reporting of ransomware incidents, there was little-to-no evidence of investigation or punitive action in cases of non-compliance. Organisations were often seen to take a relaxed attitude to new cyber legislation, waiting to observe the ramifications of non-compliance rather than proactively investing time and budget to comply with it. Policymakers should therefore accompany such legislation with complementary enforcement capacity building exercises such as the establishment of policing units dedicated to cybercrime and the provision of digital forensics training to these units and their counterparts in the judiciary system. The building of capacity within law enforcement would not only increase policymakers' ability to enforce legislation, but would also encourage organisations to report incidents with the expectation of receiving support with containment, eradication and investigation of the threat.

Policymakers may choose to:

F **Establish voluntary mechanisms of reporting attacks to regulators from non-CNI sectors, with the understanding that timely, voluntary engagement of the CSIRT during response efforts, or at minimum voluntary sharing of information post-response, can be used to alleviate punitive measures or gain access to support services.**

E **Establish regulatory requirements modelled on those of other nations or supranational entities, which require that ransomware attacks (among other major cyber attacks) be disclosed to the government cybersecurity agency within a maximum time period, where:**

- Attacks are conducted on organisations classified as important to critical national infrastructure.
- Attacks involve the loss of personally identifiable information (PII) or special category data (as defined under EU GDPR).
- Attacks resulting in disruption to significant consumer services and business supply chains that make up large parts of the economy.

- A ransom is paid to avoid any of the previous two consequences.

E **Establish punitive measures for failure to report in-scope cyber attacks and data breaches within the maximum time limit. Regulators should consider that:**

- Attack disclosure requirements are in place to improve intelligence gathering efforts over ransomware attacks, improve and better coordinate response efforts, and enable community defence and active threat hunting efforts.
- Punitive measures should not include disbarment from access to CSIRT or government-led threat intelligence sharing services.
- Punitive measures should be commensurate to the level of unwillingness of organisations to provide information and contribute to community defence efforts. The more an organisation engages with collective cyber defence efforts, the lesser the punitive measures can be.

S **Require that all organisations in CNI sectors complete an annual disclosure of the number of cyber attacks they experienced in the previous year which resulted in high priority incident response processes being engaged. Regulators should note that this data is:**

- Not to be shared with law enforcement or regulatory bodies with the intent of ascribing punitive action to the sharing organisations.
- To be used to understand the threats to key sectors and determine where resources and capacity building efforts should be concentrated.

Policy 4.3: Require a baseline third party assurance regime for the most cyber capable sectors which covers ransomware response capabilities.

Third party assurance regimes can be among the most effective mechanisms that cybersecurity regulators have for propagating good practice throughout market ecosystems. In advanced economies, the most critical and cyber-capable sectors (e.g. financial services) are frequently required by regulators to conduct due diligence over their suppliers (third parties) prior to contracting, and sometimes over their supplier's suppliers (fourth parties), screening for issues that could affect their or their customers' privacy, security and resilience. Initial due diligence is often followed up by regular assurance over the length of any supplier contract to monitor their security posture.

As part of third party assurance regimes, contracts can require suppliers to submit to audits by their customers, who assess their security and make recommendations for improvements that reduce the cyber risk to the customer. Implementation of said recommendations is followed up and confirmed over multiple, regular (e.g. annual) ongoing assurance cycles. Assurance regimes can gradually propagate cybersecurity good practice to thousands of suppliers over these assurance cycles by driving incremental improvements in cybersecurity processes and governance. And when suppliers pass good practice requirements on to their suppliers through their own third party assurance cycles, it produces a force-multiplying affect impacting tens of thousands of organisations.

For regulators and cybersecurity agencies concerned over ecosystem-wide resilience against ransomware, assurance regimes can also foster improved cooperation between organisations and their suppliers, helping to coordinate incident response processes and lubricate active defence efforts. They can also generate valuable information on industry supply chains, which can help identify critical third parties and single points of failure.

Even in advanced economies, mandating third party assurance can impose a significant cost and unachievable resource burden on even the most mature and well-resourced organisations. It can also create an audit overhead for popular suppliers who face assurance requirements from multiple customers. For developing economies, strictly limiting this burden is critical to avoiding pushback. Regulators should encourage suppliers in critical sectors to seek independent certification against central control frameworks and push organisations to limit assurance where certification has been achieved. Regulators should also require a light touch assurance regime, minimising resource requirements for the private sector whilst maximising the cooperation, transparency and maturity-building impacts of such regimes.

Policymakers may choose to: ✓

E **Require that organisations in CNI sectors with the highest maturity cybersecurity capabilities, including financial services, telecommunications and pharmaceuticals, to validate the cybersecurity controls of their key suppliers and partner organisations, with the aim of:**

- Asking capable private sector partners take an active role in validating the resilience of their respective sector supply chain ecosystems;
- Propagating cybersecurity best practice principles throughout CNI sector ecosystems through programmes of security reviews and contractual obligations;
- Forcing investment in cybersecurity controls for organisations supplying critical economic sectors, and building maturity, capacity and awareness of cybersecurity challenges.

S **Lay out a controls framework aligned to certification schemes, as well as an operating model for third party assurance, which includes:**

- Risk assessment of suppliers to understand the inherent risk a supplier's specific services pose to an organisation;
- Initial due diligence of cybersecurity best practice prior to engaging a supplier in a contract;
- Contractual obligations over the maintenance of appropriate cybersecurity controls and appropriate and timely notification in the event of a ransomware attack or breach;
- Ongoing assurance throughout the lifetime of the supplier which seeks to continuous validate cybersecurity controls against evolving threat landscapes, regulatory and control frameworks, and changes to the supplier, the client or the services.
- Use of independent certifications against national cybersecurity frameworks in lieu of third party assurance (in order to minimise audit burdens on suppliers).
- Validation of incident response and resilience plans to enable coordination between organisations and their suppliers in the event of major ransomware attacks.

Policy 4.4: Establish regulation and compliance controls on the cryptocurrency market to hamper ransomware operators from monetising their efforts.

Cryptocurrencies are a decentralised form of currency, making them difficult for law enforcement to track and address through conventional economic crime mechanisms. For this reason, ransomware demands are usually made in cryptocurrency- most commonly in bitcoin which accounted for 98% of payments made in the first quarter of 2019[72]. Founded in the aftermath of the 2008 financial crisis, bitcoin represented a decentralised alternative to the state-controlled financial systems which had failed during the crisis. In the past, cryptocurrency advocates have strongly opposed the idea of state-imposed regulation or security controls on the crypto markets. In recent years, however, the industry has suffered from massive levels of fraud and criminal activity and there appears to be growing support for regulation as a means of restoring trust in the crypto markets, with the US and UK establishing regulatory regimes which enforce penalties for non-compliance.

Addressing the cryptocurrency market targets a core component of ransomware modus operandi that it shares with few other cyber crime vectors: The reliance on untraceable payment mechanisms. By bringing greater transparency and accountability to transactions made in cryptocurrency markets, working with international partners to do so, cybersecurity regulators can significantly dampen the revenue model of ransomware operators and make it economically inviable.

Policymakers may choose to:

E **Enforce robust identity verification, anti-money laundering (AML) and know-your-customer (KYC) checks during onboarding and transactions to improve traceability for ransomware payments, money-laundering and other criminal activity. When global cryptocurrency exchange Binance introduced (KYC) verifications, more than 96% of its customer base complied. Such standards should be enforced evenly across different geographic regions to avoid certain locations becoming cybercrime hotspots.**

E **Require exchanges to perform dynamic sanction screening for high-risk individuals, politically exposed persons or those in 'high-risk' countries.**

E **Through cybersecurity representatives in the State or Foreign Affairs department or equivalent, collaborate with international partners to:**

- Coordinate enforcement of aforementioned policies with international partners for non-domiciled exchanges;
- Exchange best practice on governing KYC, AML compliance with international partners;
- Develop training programmes for local resources and discuss shared resourcing models with international partners to improve initial capacity building.

[72] https://www.emsisoft.com/en/blog/33977/is-ransomware-driving-up-the-price-of-bitcoin

05 Conclusion

05 Conclusion

The ransomware challenge facing governments and organisations continues to grow, and researchers warn that "no business or industry is safe". Once thought of solely as an IT risk, the real-world implications of cybercrime have never been clearer in the wake of high-profile attacks on critical national infrastructure such as those on the US Colonial Pipeline or the Irish Health Service Executive. Ransomware attacks can cause major operational disruption to victim organisations and can cost a company millions of dollars in losses between recovery, ransom payments, lost revenue, and regulatory fines. In addition to the immediate operational impact of an attack, ransomware can also have wide-reaching societal ramifications. Disruption of critical infrastructure and theft of personal data can lead to feelings of frustration or helplessness amongst the population or even physical harm. The social harms caused by cybercrime could contribute to political instability and a loss of confidence in those responsible for governing and providing national services.

With a focus on the partner countries of the FCDO Digital Access Programme, our research found that developing economies currently undergoing rapid digitisation will face a high risk of cyber attacks until they establish and implement robust security controls, legislation, and governance frameworks to protect their expanding digital workforce. Thematic analysis of the interviews conducted for this study, revealed several key cyber resilience challenges faced by developing economies, including the development of effective governance, enforcement of legislation, upskilling of the workforce and creation of partnerships. To address these challenges, we proposed a set of good practice principles for policymaking alongside the following four clusters of recommendations designed to support the development of national cybersecurity capacity:

Cluster 1	Build effective partnerships for ransomware defence
Cluster 2	Develop a community-based resilience architecture
Cluster 3	Uplift cybersecurity skills and capacity
Cluster 4	Define a regulatory response to ransomware

Although much of our research was centred around the challenges faced by developing economies, we saw many similarities between nations regardless of their resources or economic status. Factors such as public-private trust and communication, political will and skills shortages emerged as core themes, with each nation having its own unique approach to addressing these policy challenges. These recommendations identify specific cybersecurity capacity building exercises and mechanisms that policymakers may consider to enhance their organisations' resilience to ransomware attacks and other forms of cybercrime. The paper presents a broad range of capacity building considerations, and consequently the reader should evaluate each of the proposed actions within the context of local resource constraints and political considerations. By promoting secure and trusted digital connectivity, policymakers can generate high-skilled jobs, create opportunities for local entrepreneurship and develop partnerships with international businesses to achieve mutual prosperity.

06

Appendices

Methodology

Aim

This research paper will identify specific cybersecurity capacity building activities and mechanisms that policymakers can put in place to enhance their constituent organisations' resilience to ransomware. This work aims to:

a. Provide a baseline view of the capabilities of middle-income countries to prepare for and respond to ransomware attacks.

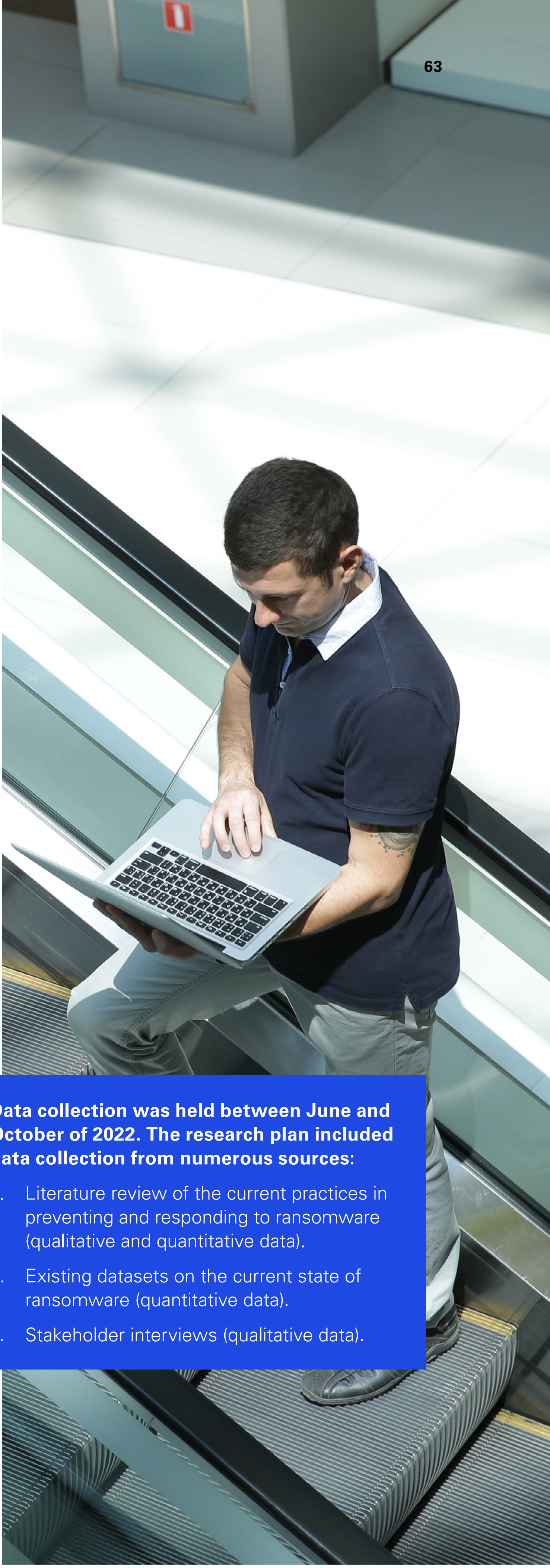
b. Identify existing challenges in advanced and developing economies

c. Identify recommendations and best practises to improve resilience to ransomware attacks.

Data Collection

To support this study's findings, recommendations and conclusions, field data collection was performed with the following aims:

- Exploring the impact of ransomware attacks on CNI and vulnerable groups
- Identifying case studies of ransomware attacks the vulnerabilities exploited and the impact on victims
- Exploring the direct or indirect impact of cybersecurity capacity building in resilience to ransomware
- Identifying recommendations for policy making to enhance resilience.



Data collection was held between June and October of 2022. The research plan included data collection from numerous sources:

a. Literature review of the current practices in preventing and responding to ransomware (qualitative and quantitative data).

b. Existing datasets on the current state of ransomware (quantitative data).

c. Stakeholder interviews (qualitative data).

Participants in this study were invited to participate in an interview. Online interviews lasted around 60 minutes. Prior to their participation, they received an information letter which included the aim of the study, information about the research, as well as confidentiality and anonymity information. The semi-structured interviews targeted both stakeholders tackling cyber-crime at a strategic or policy level (e.g., Legislators, policymakers, academics) and those dealing with cyber threats at an organisational or operational level (e.g., CISOs, Incident Responders, SOC leads). The interview guide (See over the page) used for this study included a number of questions covering topics such as:

- **Challenges for organisations' resilience to ransomware**
- **The impact of policy measures for increasing organisational ransomware resilience and the complexity of implementing these**
- **The potential harms of ransomware attacks**
- **Current technical security gaps**
- **Skills gap in security staff roles**
- **Reporting practises and the involvement of law enforcement**
- **Public-private sector collaborations**
- **International policy making**

Participants

A total of 36 participants took part in this study. Interviews were conducted with representatives from:

- Public sector
- Private sector
- Finance sector
- Academia
- Law enforcement
- Incident Response
- SMEs
- NGOs
- Non-profit organisations

Interviewees were recruited through the networks of KPMG, FCDO and the DAP Programme. Participants from UK, USA, Brazil, South Africa, Kenya, Nigeria, Indonesia and Ukraine were selected based on their professional role as well as their experience with cybersecurity capacity building and the handling and prevention of cyber attacks such as ransomware.

Ethical considerations

Throughout the process of recruiting participants, data collection and analysis, all necessary steps to ensure anonymisation of data was followed. Personal information such as names and contact details were not collected or stored during the interviews.

Interview Guide

01 Can you describe the current state of ransomware resilience within your country?

02 What are the current drivers of your regulation in cyber space?

03 Which sectors do you think are mostly impacted by ransomware attacks currently?

04 What do you perceive as the biggest challenge or gap for organisations to increase their resilience to ransomware?

05 What do you perceive as the biggest challenge or gap for countries to increase their resilience to ransomware?

06 What policy or control have you implemented (or seen to be implemented) which had the biggest positive impact on ransomware resilience?

07 What do you think are the biggest costs to businesses following a ransomware attack?

08 What do you think could be done to prevent ransomware attacks at an international policy making level?

Who do ransomware groups target?

Organisations should fulfill at least 2 out of the 3 criteria listed (ideally 3 out of 3) for ransomware groups to consider them a viable target.

Organisations who are willing and able to pay a large ransom

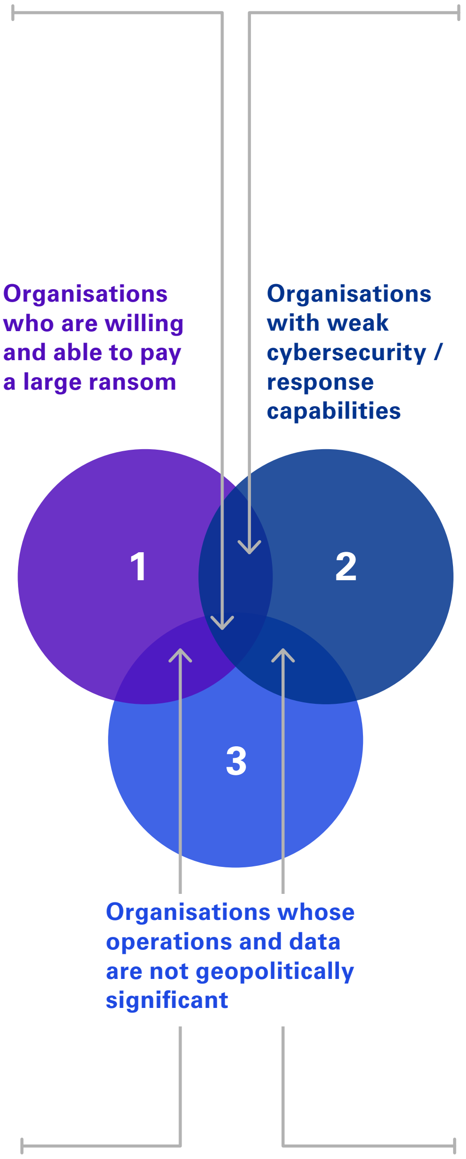
Description: Significant cash flows; controllers of highly regulated data such as PII or special category data whose breach would result in regulatory fines; organisations with operational processes which produce outputs that influence share prices and for which outages are highly visible; organisations with cyber insurance policies covering ransomware payments

Organisations with weak cyber security / response capabilities

Description: Organisations with poor cybersecurity governance; no encryption of data at rest; poor back up and recovery configuration; disorganised response capabilities; undefined communications plans and poor relationships with law enforcement and regulator bodies

Organisations whose operations and data are not geopolitically significant

Description: Organisations who do not play a significant role in critical national infrastructure and for whom outages do not have geopolitical, public health or environmental effects; organisations that hold data with low sensitivity to national security considerations or public services


Organisations who are willing and able to pay a large ransom
Organisations with weak cybersecurity / response capabilities
1
2
3
Organisations whose operations and data are not geopolitically significant

Goldilocks Zone: Feasible, Profitable, Inconsequential

High ransom payments, easily executable, repeatable attacks with high likelihood of payment and limited consequences

Example sectors: Mining, chemicals, medical equipment manufacturing, commodity retailers, food and beverage producers, local government services and councils, higher education, pension schemes, law firms and legal services

Feasible, Profitable but highly Consequential

Reward: High ransom payments based on high value data and operations, and easily executable, repeatable attacks.

Risk: May incur major response from national governments, intelligence agencies and law enforcement, unwanted geopolitical attention.

Example sectors: Renewable and non-renewable energy; electricity generation and provision; gas and water utilities providers, waste and disposal services, aerospace and defence, transportation and major infrastructure, healthcare, telecommunications, national civil service and government bodies

Profitable, Inconsequential but Difficult

Reward: High ransom payments, limited consequences for the attack

Risk: Attacks require major time investment and are hard to execute; failed attacks may leave behind actionable intel on compromise methodologies

Example sectors: Banks and insurers, wealth and asset management, pharmaceuticals, technology hardware and equipment, software and computer services, electronics and electrical equipment

Feasible, Inconsequential but not Profitable

Reward: Easily executable, repeatable attacks with limited consequences and high likelihood of payment.

Risk: Low and occasionally zero ransom pay off depending on value of data accessed and financial resources of target.

Example sectors: Agriculture, household goods and furnishings, travel and leisure services, arts, entertainment and recreation, charities, construction and materials, small-to-medium size enterprises (SMEs), primary and secondary schooling, social care services

UKaid
from the British people

KPMG

Queen Mary
University of London