A global business perspective on fostering ransomware resilience

Introduction

In today's digital landscape, malicious cyber activity targeting individuals, businesses and governments alike is surging, marked by unprecedented scale, frequency, and intricacy. With over 350,000 new malware variants emerging daily[1], hostile cyber actors have an expansive arsenal of offensive cyber capabilities at their disposal. Particularly, the prevalence of ransomware attacks has reached new heights, aggravated by a disruptive model known as Ransomware-as-a-Service (RaaS). Under RaaS, sophisticated cyber criminals make ransomware tools readily available off-the-shelf to individuals or groups at minimal costs, effectively eroding the barriers to entry into this profitable criminal domain. As a result, the landscape of ransomware attacks has grown in both complexity and frequency, magnifying the potential destructiveness of these attacks, as even inexperienced perpetrators gain access to highly sophisticated tools.

With attackers increasingly targeting a wide variety of organisations, including governments, ransomware attacks are a rising topic on policy agendas worldwide. Recognising that companies are not only the target of attacks, but also at the forefront of detecting threats and creating innovative approaches to resilience and response, it is vital that the public and private sectors work together to respond to this escalating issue.

This paper explores the evolving landscape of ransomware attacks and their expanding footprint on society and global economy. It describes the proactive measures taken by businesses to fortify resilience against ransomware, drawing examples from the diverse cross-sectoral and global membership of the International Chamber of Commerce (ICC). It also highlights the pressing need for collective action, emphasising the importance of international cooperation, information sharing, and collective multistakeholder efforts to combat the multifaceted nature of preventing, detecting, and responding to ransomware threats. This paper illustrates ICC's commitment to

[1] International Chamber of Commerce, Cybersecurity Issue Brief 1: Government action on cybersecurity (2021)
[2] ICC Endorses Accra Call for Cyber Resilient Development at the Global Conference on Cyber Capacity Building (2023)
[3] International Chamber of Commerce, Towards a common implementation framework of the cybersecurity acquis: shared goals for cyber action (2023)

elevating cyber resilience across international and national development agendas[2] through bolstering cybersecurity efforts through an agreed framework of actionable common goals[3].

Current state of play

Ransomware attacks pose a significant threat, with critical infrastructure services, businesses of all sizes, and governments targeted within the growing cyber ecosystem. In recent years, ransomware has evolved significantly, transforming into a well-organised and profitable activity with substantial profit margins. The average ransom size increased from $84,116 in Q4 2019 to $154,108 in Q4 2020[4]. In addition, the disruption to operations from ransomware has cost businesses thousands of dollars in operational losses. Activity levels continued to fluctuate throughout 2022 and into the first months of 2023, largely in concert with directional trends observed in the last two years. In May 2023, 332 ransomware incidents were observed, indicating slightly less than a 13% decrease compared to April 2023[5].

The professionalisation of the cybercrime economy lowers the skill barrier to entry, providing greater access to tools and infrastructure for a wider potential group of criminals. This shift is reflected in the evolution of ransomware to a double extortion model, wherein cybercriminals in addition to encrypting a victim's sensitive data, now exfiltrate it, increasing their leverage and potential harm. Consequently, the threat of ransomware and extortion is rising with attacks targeting governments, businesses, and critical infrastructures. Ransomware victims come from diverse geographical origins, with most prominent organisations affected from Western countries like the US, Canada, and Europe. However, there is an increasing trend of cases in emerging tech hubs, including countries like Brazil and India, reflecting their growing technological infrastructure[6]. Attackers increasingly threaten to disclose sensitive data to encourage ransom payments, with human-operated ransomware[7] being the most prevalent, as one-third of targets are successfully compromised by criminals using this type of attack. Out of those successful attacks, about 5% result in targets being ransomed.[8] Credential phishing schemes, which indiscriminately target all inboxes, are also on the rise, and business email compromise, including invoice fraud, poses a significant cybercrime risk for enterprises. The industrial and engineering sectors have been the most targeted with at least 45 separate incidents in April 2023. The second most-targeted sector, technology, experienced at least 44 separate incidents in May.[9]

The expanding impact of ransomware

As ransomware attacks have become more audacious in scope, their reach and footprint impacts society and businesses alike. These attacks can severely disrupt day-to-day life, such as access to education and organizations' operational capabilities, leading to financial losses for individuals, businesses, and the overall economy. Beyond the financial impact, and reputational risks, ransomware poses a direct threat to people's safety, making the risk more visible worldwide.

Disruption of critical services, such as healthcare and emergency response can trigger direct consequences that extend beyond the immediate incident. The ripple effects of ransomware to everyday life can result in mild inconveniences, such as disruption of public services, to significant psychological consequences, or even potential loss of lives and damage of government security.

---

[4] Lumen, Part 1: What Is Ransomware And How It Evolved (2021)
[5] Ericsson, CrowdStrike Falcon Intelligence Elite Ransomware Digest (2023)
[6] Telefónica Tech, Next Defense Cyber Threat Intelligence Improving Resilience (2023)
[7] A term describing threats driven by humans who make decisions at every stage of the attacks. Microsoft, Digital Defense Report: Illuminating the threat landscape and empowering a digital defense (2022)
[8] Microsoft, Digital Defense Report: Illuminating the threat landscape and empowering a digital defense (2022)
[9] Ericsson, CrowdStrike Falcon Intelligence Elite Ransomware Digest (2023)

The repercussions of ransomware attacks also extend to data loss and privacy concerns, and legal and regulatory implications that erode trust in digital systems and services. This loss of trust can keep people from engaging in the digital world, creating a sense of unease and disengagement with information services. National security risks associated with attacks on critical infrastructure and essential services cannot be underestimated. The interconnected nature of critical infrastructure or essential services, encompassing sectors such as energy, transportation, health, and national security amplifies the ripple effects of such attacks, with governments classifying ransomware as a threat to national security, public safety and economic prosperity.[10] Collective action in response to those risks is paramount, and necessitates international cooperation. To effectively combat this increasingly serious problem, robust cybersecurity measures and global safeguards must be put in place.

How is business improving resilience against attacks

In response to the threat of ransomware, the private sector bolsters resilience and recovery by adopting comprehensive security measures, including developing incident response plans, maintaining robust asset inventories, implementing strong data backups, and ensuring up-to-date systems with the latest security patches. Cybersecurity training also comes into play as a crucial component, giving employees the necessary knowledge on best practices, aiming at building a strong security posture of systems and services from the inside out. Below we offer a few illustrative examples:

Telefónica doubles as a first-tier managed security service provider and as a key telecoms and digital provider. As a security service provider, Telefónica sets out counter-ransomware tools and strategies that help organisations mitigate, prevent and recover effectively from such incidents[11]. This includes adding cyberdefence capabilities to customers' processes, technologies and operations through the Telefónica Digital Operation Centre[12] (DOC), as well as the development of detailed Incident Response Plans (IRP), with procedures for incident response strategies and a dedicated Incidence Response Team (IRT) where needed. As a telecoms and digital provider, Telefónica applies security by design across its processes in all business lines and geographies, develops state of the art cyberintelligence capabilities, leverages on its scale and positioning to increase its resiliency and builds on its networks and systems.

Lumen provides expert guidance[13] to bolster the resilience of businesses against ransomware threats, focusing on education and policy enforcement, securing endpoints, implementing back-end security, patching software and managing data.

Microsoft relies on innovative technical and legal strategies and public and private partnerships to deter attackers and make attacks less likely to succeed.[14] Following industry guidelines, such as the National Institute of Standards and Technology's published framework for managing the risks of ransomware (NIST.IT.8374), Microsoft established a set of requirements for Optimal Ransomware Resiliency State (ORRS), ensuring that their internal systems withstand ransomware threats.

In addition, Microsoft's Digital Crimes Unit (DCU)[15], established in 2008, plays a pivotal role in combatting cybercrime, leveraging its unique insights into online criminal networks to support law enforcement with criminal referrals. It disrupts cybercriminal infrastructure through civil legal actions and technical measures to increase the cost of cybercrime operations. Recognising the collaborative nature of the fight against cybercrime, the DCU collaborates extensively with Microsoft's security teams, law enforcement, security firms, researchers, NGOs, and customers,

---

[10] The White House, National Cybersecurity Strategy (2023)
[11] Telefónica Tech, Next Defense Cyber Threat Intelligence Improving Resilience (2023)
[12] Telefónica Tech, About the Digital Operations Center
[13] Lumen, Part 2: How To Prevent Ransomware Like A Pro (2021)
[14] Microsoft, Digital Defense Report 2022: The importance of cybersecurity hygiene (2022)
[15] Microsoft, On the Issues, Digital Crimes Unit: Leading the fight against cybercrime (2022)

magnifying its impact. The DCU also shares insights to aid victim remediation, support educational initiatives, and develop technical countermeasures that bolster the security of Microsoft's products and services.

Generally, businesses recommend the following tools and good practices to prevent ransomware attacks:

- Maintaining an effective inventory of assets and robust perimeter surveillance with vulnerability management tools.[16]
- Regularly backing up important data, stored in a properly protected system.[17]
- Establishing security privilege policies to restrict unnecessary user access, while keeping systems up to date with the latest security patches.[18]
- Conducting cybersecurity trainings to educate employees, performing regular security audits to test mechanisms and minimising external exposure to the internal networks.[19] Artificial Intelligence (AI) can also be used to augment human cyber defense skills, and expedite the time to detect and respod to ransomware attacks.[20]
- Leveraging the benefits of public cloud's hyper-scalability and robust cybersecurity features.[21]
- Utilising Endpoint Detection and Response (EDR) systems, including multifactor authentication for publicly exposed assets.[22]
- Implementing advanced cross-layer detection and response solutions on all platforms.[23]
- Employing up-to-date antivirus signatures.[24]
- Configuring firewalls at the application level.[25]
- Paying attention to vulnerabilities in backup and storage appliances, VPN software, and gateways.[26]
- Patching software to address vulnerabilities for both server and client applications.[27]
- Applying zero trust principles across network architecture.[28]

How is business detecting and responding to ransomware attacks

As ransomware poses a substantial threat to businesses and society, it requires a multifaceted response. It starts with an early detection phase to identify the threat, leading to immediate incident response activation. For example, most recently, Telefónica tackled a public administration attack in coordination with their team through this approach. The local administration notified the Spanish Data Protection Agency, and containment measures, such as shutting down external communications, were enacted. Following the detection and investigation of the entry vector, a progressive recovery plan was established. On a different occasion, in a small retail SME affected by RansomHouse ransomware, forensic analysis uncovered the vulnerability exploited by the attacker. This prompted containment measures, leading to the restoration of backups, investigation, and safe recovery with enhanced security measures. This included conservative network security policies to ensure that the telemetry of the IT infrastructure was

[16] Telefónica Tech, Next Defense Cyber Threat Intelligence Improving Resilience (2023)
[17] Id.
[18] Id.
[19] Lumen, Part 2: How To Prevent Ransomware Like A Pro (2021)
[20] Microsoft, Digital Defense Report (2023)
[21] Id.
[22] Lumen, Part 2: How To Prevent Ransomware Like A Pro (2021)
[23] Telefónica Tech, Next Defense Cyber Threat Intelligence Improving Resilience (2023)
[24] Id.
[25] Id.
[26] Lumen, Part 2: How To Prevent Ransomware Like A Pro (2021)
[27] Id.
[28] Id.

ready and the organization could minimise the time-to-action in the unwanted event of reinfection or any other incident occurring[29].

Effective action lies in a combination of technical measures, investigative capabilities, international cooperation, and voluntary public-private partnership.. . Examples of measures include:

- **Advanced security tools:** Implementing technical protection, such as locking down endpoint USB access with group policies and implementing appropriate endpoint protection software are highlighted as key anti-ransomware measures by Lumen[30]. In other cases, disabling some local endpoint functions is also referenced as a useful hardening measure, as well as closing Remote Desktop Protocol (RDP) ports on machines that don't use them.[31] A wealth of available threat detection and mitigation tools provide robust remediation capabilities to organisations, specifically addressing the risks and challenges posed by ransomware.
- **Cyber threat intelligence:** Another aspect of cybersecurity hygiene is monitoring of ransomware trends. Microsoft's Threat Intelligence Center (MSTIC)[32] monitors ransomware groups and threat actors. Leveraging 43 trillion signals daily, Microsoft integrates insights into its services, enhancing customer protection.
- **Domain seizures:** A common strategy involves the seizure of command and control (C2) servers and domains used by ransomware operators. This proactive approach disrupts the botnets' ability to operate effectively. Microsoft, for instance, granted temporary ownership of domains used by the Waledac botnet's servers.[33]
- **Investigation and remediation:** Telefónica deploys forensic investigation to analyse the whole *modus operandi* employed by the attacker, assess the vulnerabilities that performed the initial access, and identify whether the cybercriminal accessed sensitive information, specifically pertaining to personal data.[34] Microsoft's Detection and Response Team (DART) globally assists customers, preventing and mitigating attacks. Notable examples include support during ransomware incidents in Albania[35] and Poland.[36]

Collaborative Measures

In the face of potential operational disruptions and financial burdens, businesses are increasingly turning to partnerships and cooperative initiatives as a cornerstone of their ransomware defense. These alliances unite industry players, law enforcement, international organizations and the private sector, presenting a united front against this constantly evolving cyber threat.

Consortia

Coordinated efforts to enhance cybersecurity measures have proven effective, with businesses forming consortia and strategic partnerships among various stakeholders, including cybersecurity experts, law enforcement agencies and government entities to share their resources and effectively combat ransomware attacks. Lumen underlines the importance of third-party expertise in identifying vulnerabilities and addressing risk, through specialist cybersecurity services partners, which for many organisations is difficult to acquire or build in-house[37]. Businesses like Ericsson or Telefónica have joined cybersecurity consortium CONCORDIA[38], aiming to establish an EU-

[29] Telefónica Tech, Next Defense Cyber Threat Intelligence Improving Resilience (2023)
[30] Id.
[31] Id.
[32] Microsoft Threat Intelligence Center (MSTIC): A team focused on identifying, tracking, and collecting intelligence related to the most sophisticated adversaries impacting Microsoft customers, including nation state threats, malware, and phishing. Microsoft, Digital Defense Report 2022: Contributing Teams (2022)
[33] Microsoft, Official Microsoft Blog, Waledac: Undoing the damage of a botnet (2010)
[34] Telefónica Tech, Next Defense Cyber Threat Intelligence Improving Resilience (2023)
[35] Microsoft, Microsoft investigates Iranian attacks against the Albanian government, Microsoft Threat Intelligence (2022)
[36] Microsoft, New "Prestige" ransomware impacts organisations in Ukraine and Poland, Microsoft Threat Intelligence (2023)
[37] Lumen, Part 3: How Ransomware Attacks Are Escalating And What To Do About Them (2021)
[38] Ericsson, Why we're part of CONCORDIA – Europe's largest cybersecurity consortium (2019)

integrated cybersecurity ecosystem. Microsoft has also formed collaborative consortia, such as the Conficker Working Group and the Microsoft Malware Protection Center. These groups partner with various organizations and academics to combat botnets. These consortia focus on close collaboration and operate internationally to defeat ransomware threats. In addition, Telefónica has specialised cybersecurity teams that collaborate with companies of all sizes and sectors in preventing, protecting and managing cybersecurity incidents, including post-incident actions, illustrating the efficiency of collaborative approaches. Finally, Microsoft also partners with industry-specific associations like the Financial Services Information Sharing and Analysis Center (FS-ISAC) to combat ransomware threats targeting their sector. This collaboration involves the identification and tracking of bot infrastructure and generating notifications to internet providers.

Information sharing

Businesses share critical information with internet service providers, governments, law enforcement agencies, and private industry players. This shared intelligence helps remediate malware incidents and prevent the distribution of additional malware. For example, Microsoft has contributed to remediating over 17 million malware victims[39] worldwide through such partnerships.

Telefónica is integrated into the various information-sharing circles established by national authorities and between different private entities, as well as in different countries, to provide all stakeholders with the ability to interact quickly, and react robustly to wide-ranging attacks. For example, Telefónica is a key collaborator in the Spanish National Network of SOCs[40]. The initiative, sponsored by the Spanish Intelligence Agency (CNI)[41] and its cybersecurity-related branch, or National Cryptologic Center (CCN-CERT)[42], focuses on sharing Indicators of Compromise (IOC)[43] and attack patterns among Spanish cybersecurity providers, turning effective information sharing into a catalyst for mitigating and responding to ongoing threats.

Other businesses work closely with law enforcement agencies and international entities. They collaborate with organizations like the FBI, US Marshalls, Dutch law enforcement officials, and Europol's Cybercrime Center to take down ransomware infrastructure. Legal actions are often coordinated across international jurisdictions.

Conclusion

The escalating threat posed by ransomware demands a collective and concerted response. As the accessibility of ransomware tools increases, the cybersecurity landscape becomes more complex meaning there is no one size fits all solution. Businesses, as targets of ransomware attacks, and at the same time, providers of remediation services, cannot bear this burden alone. It is only through collaborative efforts and well-formulated policies that take a whole-of-society approach that the digital ecosystem can protected against the threat of ransomware. Effective action also lies in the implementation of punitive measures against both cybercriminals and nation-state supporters[44].

The International Chamber of Commerce stands ready to support policymakers in meeting this challenge by providing relevant input and evidence to assist the development of policies to secure cyberspace.

[39] Microsoft, Digital Defense Report 2022: The State of Cybercrime (2022)
[40] About the National Network of SOCs (Red Nacional SOC)
[41] About the Spanish Intelligence Agency (Centro Nacional de Inteligencia)
[42] About CCN-CERT (Cenrto Criptologico Nacional)
[43] Microsoft, Indicators of Compromise (IOC) explained
[44] International Chamber of Commerce, Cybersecurity Issue Brief 2: Implementing norms and rules for responsible state behaviour in cyberspace and enhancing cooperation to counter cybercrime (2022)

ABOUT THE INTERNATIONAL CHAMBER OF COMMERCE (ICC)

The International Chamber of Commerce (ICC) is the institutional representative of more than 45 million companies in over 170 countries. ICC's core mission is to make business work for everyone, every day, everywhere. Through a unique mix of advocacy, solutions and standard setting, we promote international trade, responsible business conduct and a global approach to regulation, in addition to providing market-leading dispute resolution services. Our members include many of the world's leading companies, SMEs, business associations and local chambers of commerce.