# Tackling cybercrime and ransomware head-on: Disrupting criminal networks and protecting organisations

Received (in revised form): 9th November, 2021

**Marja Laitinen**
Digital Crimes Unit Lead, Microsoft EMEA, Finland

Marja Laitinen leads Microsoft's Digital Crimes Unit (DCU) in Europe, Middle East and Africa (EMEA), managing a team of attorneys, investigators, business intelligence analysts and outside counsels across the region. Together with her team she supervises Microsoft's enforcement efforts against organised criminals and other illicit organisations engaged in cybercrime and related illegal activities. Ever since joining Microsoft in 2000, Marja has collaborated extensively with police, prosecutors and other law enforcement officials in EMEA. Before this she worked at Susiluoto Attorneys-At-Law Ltd, a leading Finnish law firm in the field of IPR protection. A Finnish national, Marja is a graduate of the University of Helsinki Law School, and she is currently based in Finland.

Microsoft Digital Crimes Unit (DCU) EMEA
E-mail: marjal@microsoft.com

**Sarah Armstrong-Smith**
Chief Security Advisor, Microsoft EMEA, UK

Sarah Armstrong-Smith is chief security adviser in Microsoft's Cybersecurity Solutions Area. She principally works with strategic and major customers across Europe, to help them evolve their security strategy and capabilities to support digital transformation and cloud adoption. Sarah has a background in business continuity, disaster recovery, data protection and privacy, as well as crisis management. Combining these elements means she operates holistically to understand the cyber security landscape, and how this can be proactively enabled to deliver effective resilience. Sarah has been recognised as one of the most influential women in UK tech and UK cyber security and she regularly contributes to thought leadership and industry publications.

E-mail: sarah.armstrongsmith@microsoft.com

**Abstract** This paper provides a look into the current cybercrime trends, fuelled by the ongoing digital transformation and global pandemic, proliferating across organisations of all sizes and posing high socio-economic risk to critical infrastructure and supply chains. Attackers are capitalising on the technological advances, cloud adoption and hybrid working environments through launching targeted and persistent, human-operated ransomware campaigns. A coordinated and sustained effort is required between governments and the private sector to disrupt criminal infrastructures and global networks that cybercriminals rely on to launch and profit from their attacks. Collaboration and partnerships are also required to support organisations with building necessary cybersecurity capability to prevent, detect and respond to ransomware threats, through adopting zero trust principles and architectures by design and default.

KEYWORDS: cybercrime, ransomware, law enforcement, organised crime, cyberattacks, cyber security protection, zero trust

## INTRODUCTION

This paper focuses on the developments of the cybercrime economy, in particular the growing trend for disruptive and destructive attacks associated with human-operated ransomware, and the steps required to prevent and protect from extortion-based attacks.

The goal is to help organisations and governments understand how cybercriminals continuously shift their attack modes, and to determine the best way to protect and defend against those attacks, utilising a combination of advancements in technology and human intelligence to understand the context of the attack vectors and to refine related processes.

While sharing of intelligence provides insights on the changing attack vectors, most organisations are not equipped to deal with the growing level of attacks in isolation, so a deliberate and targeted approach is required to disrupt the malicious infrastructure and criminal networks. This paper further explores the imperative for public and private sector partnerships, across different jurisdictions, in the critical unification against cybercrime.

## CYBERCRIME TRENDS

In today's digital world, it is relatively easy to be a cybercriminal — just a bit of money and access to the Internet will do. Too much technical expertise is not required, as the dark web has created an industrialised economy with specialisation of skills, products, services and profit models, offering cybercrime-as-a-service. The growing demand for these services has further boosted the cybercrime supply chain, and attackers are increasingly using automation to drive down their costs and expand their scale.[1]

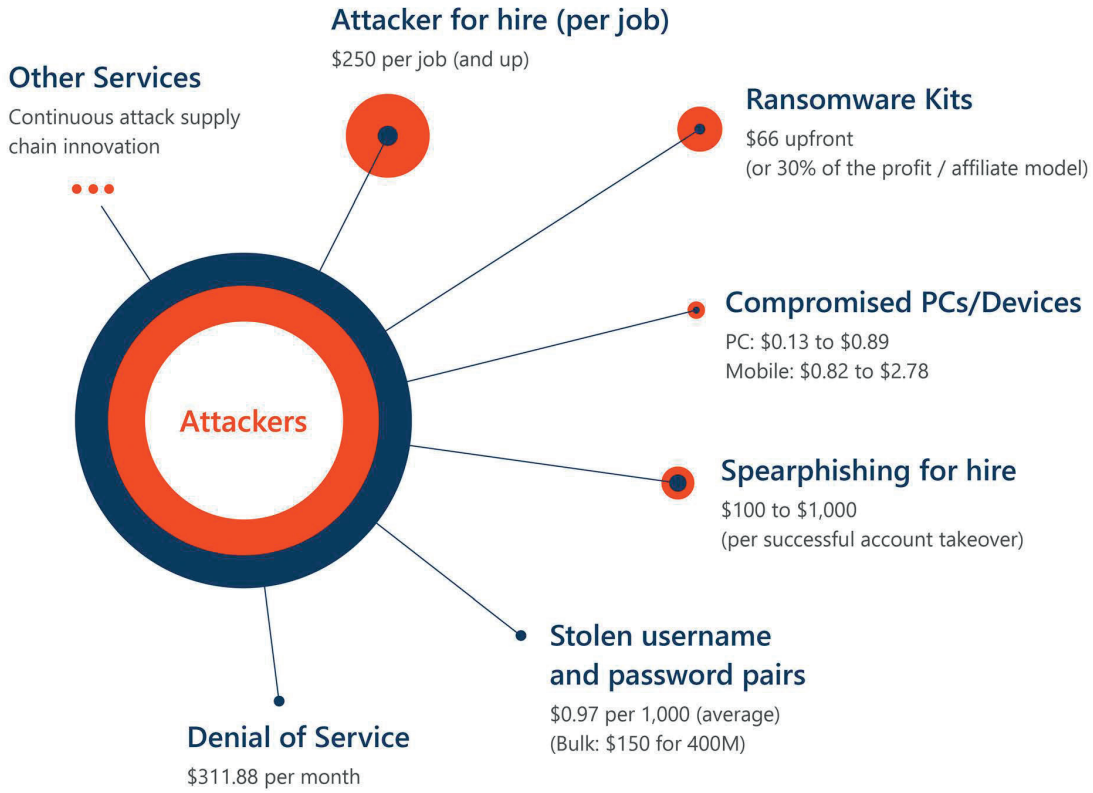


**Figure 1:** Average prices of cybercrime services for sale
Source: Microsoft Digital Defense Report[1]

The easy-to-access attack tools, combined with the global pandemic, switch to hybrid workforce and erosion of the corporate network perimeter, have opened new doors for cybercriminals and cyberattacks have escalated. The level of supply chain and ransomware attacks has especially spiked, calling for an urgent need for the public and private sectors to come together to equip organisations of all sizes with the ability to protect themselves, and to take effective action to disrupt and deter these growing threats.

In addition to frequency, the severity of attacks has increased over the past year. Examples include supply chain attacks such as HAVEX and SolarWinds and 0-day industrial control systems (ICS) malware such as Triton and Industroyer. To make themselves harder to detect, criminals are relying on standard administrator tools that blend in with legitimate day-to-day activities.[2]

Cybercrime poses a massive threat to national security, as cybercriminals are utilising these resources and targeting all sectors for financial gain, political or other notorious purposes (see Figure 1). This has led governments worldwide to make combatting cybercrime a priority and seek out private sector assistance.

## EVOLUTION OF RANSOMWARE MODELS

The utilisation of malware and ransomware in cybercrime is nothing new — indeed, ransomware itself has been prevalent for many years — but what is perhaps surprising is the pace of evolution and the changing models (see Figure 2).

Ransomware initially started as a high-volume, low-yield commodity attack that predominantly utilised pre-packaged malware, with little human intervention required. The initial focus of attack was individuals, aimed at encrypting hard drives on a single PC.

Over the last ten years, there has been a shift in tactics, to have more focus on human-operated attacks, with more emphasis on organisations, as witnessed by the (Not)Petya and WannaCry attacks in 2017. This ranges from small companies up to multinational enterprises and government institutions.

Ransomware has become a favoured attack vector for organised crime networks, with the resources and capability to launch an attack on a similar scope and scale to that seen in nation-state attacks, often operating across jurisdictions to avoid detection and capture. This is marked by 'persistence and patience' to not only infiltrate networks,

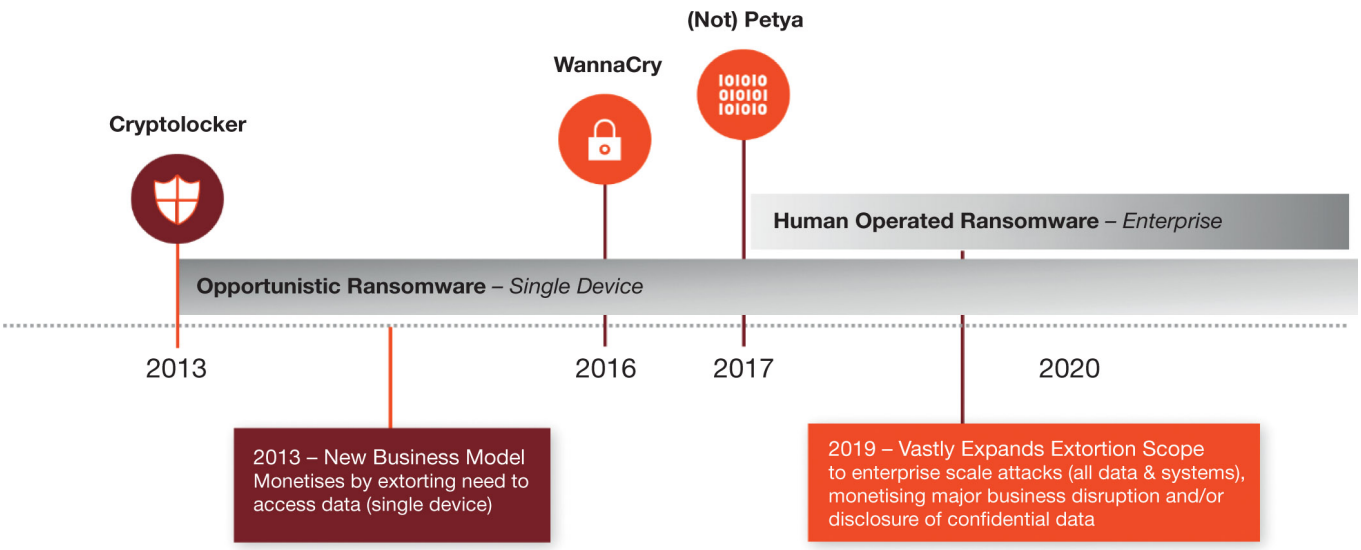


**Figure 2:** Evolution of ransomware models
Source: Microsoft

but to take time to perform detailed reconnaissance of their target, to learn the infrastructure, and to learn the defences.

According to Sophos,[3] while the number of organisations being hit by ransomware has dropped and fewer organisations have suffered data encryption, the financial impact of this crime has more than doubled, increasing from US$761,000 in 2020 to US$1.85m in 2021. The sophistication and complexity of targeted supply chain and ransomware attacks have increased,[4] elevating the urgency of public and private sectors to work together to equip all organisations with the ability to act against these threats.

The ability to ransom an entire network can be achieved within 45 minutes;[5] however, it is the events leading up to the attack that require the most scrutiny.

The entry point continues to be crude in some respects. The attackers still favour the 'tried and tested' methods to gain initial entry to the network through credential harvesting, pre-coded malware, or taking advantage of misconfigured or unpatched servers. Attackers may also utilise a password spray to see whether compromised credentials bought on the dark web are still active, or whether they have been reused across other accounts.

In ransomware-as-a-service (RaaS) attacks, developers typically create the ransomware and payment site and affiliates are recruited to attack businesses and encrypt their devices. One of the most notorious ransomware operators, REvil, who were attributed to the Kaseya supply chain ransomware attack,[6] deposited US$1m in bitcoin on a Russian-speaking hacker forum to prove to potential affiliates that they mean business.[7]

For example, as shown in Figure 3, a threat actor may develop and deploy malware that gives one threat actor access to a certain category, whereas a different threat actor may merely deploy malware. Attackers can purchase malware and access to specific networks and target industries. This is effectively a crime syndicate where each member gets paid for managing a particular task.

Once an attacker has gained initial entry, the ability to encrypt systems or exfiltrate data requires administrative access to networks and servers to enable them to perform tasks. Often this requires the attacker to move laterally through the target's network, elevating privileges utilising scripts or further malware to achieve their objective. For this to be effective and go undetected by the organisation requires a degree of stealth and attacker expertise. In some cases, attackers have spent years undetected in the network and although dwell time has dropped over time, detection of attacker presence remains one of industry's weak points.

While the will and motivation of attackers varies, the prominent factor in cybercrime tends to be financial gain. When considered against the backdrop of a global pandemic, however, there is a willingness and desire

| RANSOMWARE TAXONOMY | |
|---|---|
| **Primary role** | **Description** |
| Develops | Writes the malware |
| Deploys | Sends phishing e-mails, deploys ransomware |
| Provides access | Malware that loads other malware or a group that sells access-as-a-service |
| Manages/operates | Leadership of a group (such as MAZE cartel membership) and/or function that provides coordination (such as managing or operating a central extortion leak site) |
| Publicly reported connection | A publicly reported connection exists |

**Figure 3:** Ransomware taxonomy
Source: Microsoft[8]

to move beyond disrupting IT services to disrupt or destroy the critical infrastructure by accessing and sabotaging operational networks and industrial control systems, leading to substantial socio-economic impact.

The reasons could be numerous. There is a higher potential for larger ransoms to be paid to get back control of services or to prevent an industrial-scale accident. Attacks are also increasingly politically motivated.

The trend is perhaps also indicative of the cloud computing age. As organisations are being driven to digitally transform their business to deliver operational efficiencies, increase competitive advantage and foster innovation, the attackers' ability to infiltrate the operational technology (OT) and Internet of Things (IoT) environments brings higher potential for industrial-scale sabotage or accidents.

While it is widely accepted that encrypting systems and exfiltrating data without being detected requires a good working knowledge of technical infrastructure and cyber security protocols, the same cannot necessarily be said of legacy or operational environments that may be running bespoke or niche services. The attackers' ability to encrypt, remove or change parameters in an operational network can cause a devastating impact, which could lead to loss of supply or loss of life, whether the attacker intended to or not.

According to Microsoft data,[9] the top three targeted sectors between June and July 2021 were consumer/retail, insurance/financial and manufacturing /agriculture (see Figure 4). And despite continued promises not to attack hospitals or healthcare companies during a pandemic, healthcare remains in the top-five sectors victimised by human-operated ransomware.

In September 2020, the first recorded death attributed to a cyberattack[11] was reported in Germany. Police launched a 'negligent homicide' investigation after

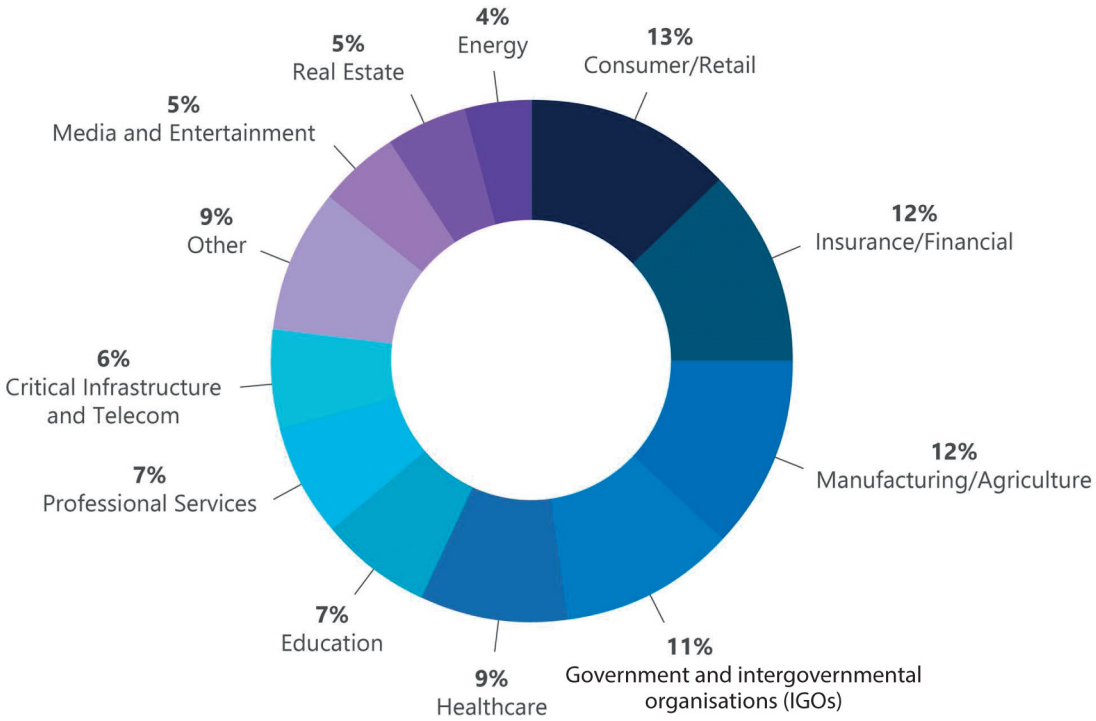


**Figure 4:** Microsoft DART ransomware engagements by industry (June–July 2021)
Source: Microsoft[10]

ransomware disrupted emergency care at Düsseldorf University Hospital. The female patient was scheduled to undergo critical care at the hospital when the attack disabled systems. She was transferred to a hospital 19 miles away, where she subsequently died. While the police investigation eventually concluded that the attack was not to blame for the patient's death,[12] most cyber experts agree that it is only a matter of time before an attack against hospitals or other front-line services causes such a tragedy.

The scope and scale of attacks, and the ferocity of change in tactics, makes it increasingly difficult for organisations to manage. There is often an explicit understanding of the inherent risk by boards, but organisations are either ill-equipped or do not have the resources and technology to be able to act with required urgency. Investments quickly become obsolete and organisations are increasingly dependent on third-party vendors to provide additional support to bolster capacity.

The interconnected supply chain has also given way to further infiltration through this trusted network. This level of exploitation shows an increasingly sophisticated trend in attack with the aim of derailing the confidence of the public and private sectors and the safety of citizens.

Following the DarkSide US Colonial Pipeline attack in May 2021, researchers discovered a new phishing campaign designed to spread ransomware by capitalising on the interest that had been generated by the attack.[13] E-mails were spoofed to appear as if sent from the recipient's help desk. Recipients were instructed to click on a malicious link to download a critical 'ransomware system update' to protect their organisation from the same fate as Colonial Pipeline.

This proliferation of coordinated attacks across critical infrastructure and the digital supply chain indicates that cybercrime and ransomware models will continue to evolve at scale. Most organisations and government entities are not equipped to deal with this type of attack in isolation, and it requires a deliberate and targeted approach to disrupt the malicious infrastructure and organised crime networks that enable the attackers to operate and hide in plain sight.

The Canadian Centre for Cybersecurity[14] indicates that 'ransomware will continue to be directed at large enterprises and critical infrastructure providers'. While ransomware will continue to target small and medium-sized organisations, the growing trend is 'big game hunting ransomware' attacks against larger organisations that cannot sustain an outage of their digital systems.

## DISRUPTING MALICIOUS INFRASTRUCTURES

Disruption of cybercrime aims at taking away the resources criminals rely on in launching their attack — to remove, or at least interrupt, the criminals' ability to carry out their malicious acts as well as reduce the number of victims and the profitability of the crime.

We have described how cybercrime has over time turned into a well-organised business that is carried out in in several different stages and by many different individuals or groups, being responsible for their separate, distinct tasks. While this compartmentalisation has further complicated cybercrime investigations, the advantage is that by managing to prevent or stop one phase of the crime, we can also have an impact on other phases. There is no need to go after all cybercriminals working in coordination, but set focus to ensure that one phase of the criminal scheme cannot be completed, which will also disrupt other phases and reduce the number of victims.

Most disruptions are carried out by cutting access to the online services that the criminals use — or, more correctly phrased, abuse — to commit their crime. Cybercriminals need Internet connection, Internet protocol (IP) address space, domain

names, servers including virtual private servers, voice over IP (VoIP) telephony, e-mail and merchant accounts and, depending on the specific crime phase or criminal task they are responsible for, the service they rely most on is their 'Achilles' heel' in completing the crime.

Most online service providers' terms of service allow them to terminate their services if the customer is abusing the service to commit a crime. Service providers are also generally not interested in criminals using their services, as dealing with number of related customer complaints or law enforcement requests can easily render especially smaller, lower-margin service providers' services unprofitable. Subsequently, our experience is that the vast majority of online service providers take prompt action when a complaint is logged with them for abuse originating from their network or services, and quite often they will not only shut down the specific service but also all other services used by the same customer.

### E-commerce directive and Internet intermediary liability

In situations when voluntary disruption efforts fail, the European Union's (EU) seminal e-commerce directive[15] provides the legal framework for defining the liability of Internet intermediaries, such as hosting providers. According to the directive, upon gaining knowledge of illegal activity or content, to avoid being held liable, a hosting provider must take prompt action to stop the activity. Moreover, subsequent legal practice has established that hosting providers must not only stop the illegal activity but also take the necessary steps to prevent the illegal activity continuing or infringing content being placed back online after the initial takedown or disruption. The advantage of the e-commerce directive is that it enables any concerned party to notify a hosting provider and trigger disruption; this can be a computer emergency response team (CERT) but also, for example, the IT department of a company.

The e-commerce directive gives a powerful incentive for EU hosting providers to act promptly upon receiving a notification of illegal activity, but its impact is not limited to the member states. This EU directive is frequently used as a model legislation on Internet intermediary liability also in countries beyond the EU's borders and, for example, the UK has maintained its provisions after Brexit through the Trade and Cooperation Agreement with the EU. In addition, in most countries law enforcement authorities have, under national laws, the prosecutorial authority to order a person or an entity to abstain from specific acts to prevent irreparable harm. For this reason, public–private partnerships and cooperation with law enforcement is of fundamental importance in effectively disrupting digital crimes.

### Microsoft Digital Crimes Unit (DCU)

To protect customers against rapidly growing digital crimes, Microsoft created the Digital Crimes Unit (DCU)[16] in 2008 and five years later, in 2013, the Microsoft Cybercrime Center was opened in Redmond, WA to facilitate the functional showcasing of DCU's innovative work in this field. DCU's international, cross-disciplinarian team consists of technical, legal and business experts who investigate online criminal networks and file criminal referrals and civil actions throughout the world, with the core mission of deterring and disrupting cybercrime. DCU applies machine learning (ML) clustering techniques in investigations to spot patterns and more accurately detect, target and disrupt criminal activities.

DCU has established strong partnerships with national and international law enforcement, security organisations, researchers, non-governmental organisations (NGOs) and customers in an effort to

dismantle criminal networks, disrupt fraudulent payments, assist with victim remediation and support education campaigns. To further expand its scope, DCU also shares evidence from its investigations with trusted partners, as well as with internal Microsoft security teams, to support the development of technical countermeasures and strengthen the security and safety of Microsoft's products and services. In addition, DCU uses its voice and expertise to inform cybercrime legislation to advance the fight against cybercrime.

While DCU's criminal referrals complement law enforcement's efforts directed to identifying and prosecuting cybercriminals, DCU's biggest opportunity to disrupt both financially and politically motivated, nation-state-supported cybercrime is through filing civil actions and seeking collaboration from internal and external partners to dismantle the technical infrastructure criminals use to target their victims.

Regulation will continue to lag behind the rapid change in technology, but the existing legal framework provides a workable basis and tools to initiate civil actions and disrupt the technical capability of cybercriminals to launch attacks and inflict harm. DCU frequently invokes different legal statutes to disable or gain control over the identified cybercrime infrastructure, to either disrupt or take down the physical or logical communication structures, as well as to seize physical devices, computers and servers used to launch attacks.

## Botnet and ransomware disruptions

Microsoft DCU's 23 global botnet operations, pursued since 2010 in cooperation with law enforcement and different industry partners, have demonstrated the power of combining legal and technical measures in eliminating both domain and IP address-based malicious infrastructures.

Especially concerned by the ransomware capabilities added to Trickbot malware close to the US presidential elections, in October 2020 Microsoft DCU and its partners moved forward with legal action in the US and reached out to hosting providers and telecom operators around the world to disable the IP-based command-and control (C2) servers and IoT devices criminals used to operate the Trickbot botnet's criminal infrastructure.[17] While the criminals have continued their efforts to replace the disconnected servers and the disruption efforts continue, finding their critical infrastructure under attack has shifted Trickbot operators' focus from initiating new attacks to setting up new infrastructure, and they have been forced to turn elsewhere for operational help. Moreover, at the end of October 2021, US law enforcement reported the arrest of a person believed to have been one of the Trickbot programmers, a 38-year-old Russian national taken into custody in South Korea and brought to the United States following an extradition request.[18]

The digital infrastructure that criminals rely on to launch ransomware attacks is rather consistent, and the same infrastructure is often used for multiple campaigns. In essence, only a location to publicise the stolen data and a communication channel with the victims to negotiate the ransom are needed. To make ransomware less profitable and more difficult to deploy, DCU is focused on disrupting the digital infrastructure and payment systems that enable these attacks. Disruptions are carried out by removing websites, servers or e-mail accounts that enable the criminal actor to negotiate the ransom or publicly disclose the victim's sensitive data. In this DCU effectively partners with law enforcement, one example of which is the recent disruption of the payment system of the cybercriminals that attacked Colonial Pipeline.[19]

Because both payment distribution systems and intermediaries supporting the money flow range across international

borders, the pursuing of effective payment disruption requires a global strategy. Regardless of where ransomware is deployed, bad actors typically demand payment via cryptocurrency, and regardless of the transparency that blockchain technology offers, the cryptowallet owners remain pseudonymous. Still, to enjoy the proceeds of their crime, the criminal must append the blockchain with a transaction and find a way to cash out. In result, the best opportunity for private and public sector stakeholders to effectively identify and disrupt weak points in this process is to join forces in international collaboration.

## PREVENTION AND PROTECTION FROM RANSOMWARE

Despite efforts to disrupt the malicious infrastructure used by cybercriminals, the business model for ransomware has effectively evolved into an intelligence operation: attackers perform research on their target victim to identify an optimal ransom demand. Once a threat actor infiltrates a network, they may exfiltrate and study financial documents and insurance policies. They may also understand the penalties associated with local breach laws. After they have collected and analysed this intelligence, the attacker will identify an 'appropriate' ransom.

While there is much debate about whether organisations should pay extortion fees, the aim of this paper is not to debate the legalities and morality behind funding organised crime, but to provide organisations with options to prevent and recover from ransomware or other types of cyberattack. Regardless, it is important to keep in mind that paying a ransom does not guarantee the unlocking of files and restoration of operations, nor prevent possible future attacks.

The only safe way to deal with a ransomware attack is to take measures to prevent, reduce, or slow down the probability of an attack and to have proactive measures that enable fast recovery should the attacker prevail (see Figure 5). This recommended three-step approach to ransomware protection[20] is predicated on priority actions and core architecture decisions that organisations can take to counteract most attacks, irrespective of the technologies deployed. This is embodied around the principles of zero trust. While organisations differ on the description and concept of zero trust, at its core is a mindset shift that assumes compromise, and the notion that nothing should be trusted unless it has been explicitly verified and authenticated, whether it originates from inside or outside the organisation.

### Step 1: Prepare a recovery plan

When an attack happens, transparency is key for knowledge and intelligence gathering.

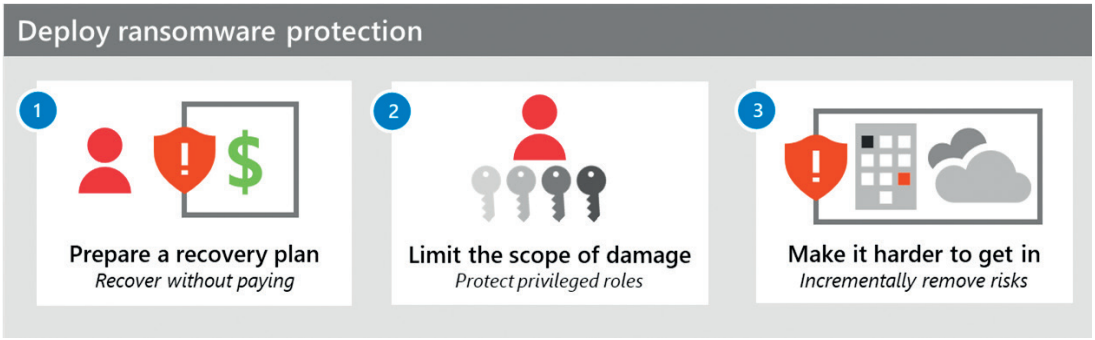


**Figure 5:** How to protect your organisation from ransomware
Source: Microsoft[21]

Following the LockerGogo ransomware attack against the Norwegian Energy supplier Norsk Hydro in 2019,[22,23] the management team publicly declared they would not pay a ransom, then took proactive and decisive action to disseminate information through multiple communication challenges as events unfolded, even taking the unusual step of holding public daily webcasts to answer questions. Despite the overall cost estimated to be more than US$71m, investors reacted positively to the way the company responded to the attack.

The way in which an organisation responds to an attack is often just as important as the attack itself, hence why preparation and exercising of the incident response plan is paramount, not least because attacks can happen at any time.

- *What*: It is necessary to plan for the worst-case scenario and anticipate that it will happen across any part of the organisation. This needs to extend beyond IT infrastructure to include OT and IoT networks, whether cloud-based, on-premises or hybrid.
- *Why*:
  - *Limit damage for the worst-case scenario*: Restoring services may be disruptive, but it is still more efficient than relying on low-quality attacker-provided decryption tools or the return of assets, assuming that these are even provided;
  - *Limit the financial return for attackers*: If an organisation can restore business operations without paying a ransom, the attack has effectively failed and resulted in zero return on investment for the attacker. Even if attackers have been unsuccessful at encrypting the network or shutting services down, they may still attempt to further extort the organisation through data disclosure or abusing/selling the stolen data and compromised credentials. Organisations should therefore be mindful to secondary attacks and implement a heightened period of detection and preparedness that assumes compromise at any time.
- *How*: Organisations should ensure they:
  - *Discover critical business assets*: Often organisations are unaware of the extent of assets they own, or those that are attached to the Internet. Unpatched and unsupported assets can be used introduce vulnerabilities that can be exploited by attackers. Organisations need to perform regular scans of the network and raise alerts when assets are added or removed. The key is to understand which assets have the most value, or disruptive capability if compromised, and translate this into supporting IT assets (applications, files, servers, etc.);
  - *Information protection*: Review broad write/delete permissions attributed to file shares. Broad is defined as many users having write/delete permissions for business-critical data. Often users have far more permissions than needed as organisations deploy a 'just-in-case' approach for convenience. There is also the need to consider users in positions of authority who have the rights to authorise or override transactions;
  - *Protect and secure backups*: The number of accounts with the ability to access and modify backups should be limited. To safeguard against deliberate malicious erasure or encryption, use offline immutable storage and/or out-of-band steps (multifactor authentication or personal identity number [PIN]) before permitting the activity. All changes to backup and storage regimes should be logged and monitored for compliance;
  - *Test 'recover from zero' scenario*: Business continuity and disaster recovery plans need to rapidly bring critical operations online from zero functionality (all systems down). This needs to extend beyond the cyber security response and consider the end-to-end recovery

between the IT and OT environments to validate cross-team processes and technical procedures. This requires 'enterprise resilience' to anticipate and prepare for large-scale attacks and failures.

### Step 2: Limit the scope of damage

- *What*: Strong privileged identity and access controls are required for any role that has access to or controls changes to business-critical assets and systems. This can extend to developers, IT system administrators, as well as OT and IoT operators;
- *Why*: This slows or blocks attackers from gaining complete access to the key resources and limits the ability to exfiltrate data. Taking away the attacker's ability to utilise privileged accounts as a shortcut to resources lowers the chances that they will be successful in controlling enough of the network or data to demand payment;
- *How*: Implement elevated security and authentication for privileged accounts — tightly protect, closely monitor and rapidly respond to incidents related to these roles;
- *Privileged access strategy*: This is a multi-part strategy with the aim to:
  - Validate the trust of users and devices before allowing access to administrative interfaces, utilising privileged access workstations that are logically separated from the Internet;
  - Protect and monitor identity systems, including directories, identity management and consent configurations;
  - Mitigate lateral traversal through segmentation of access, to prevent a single compromised device from being able to control multiple devices, using local account passwords, service account passwords or other secrets.
- *Detection and response*: This requires rapid and responsive detection and remediation of common attacks on remote desktop protocol (RDP), endpoints, e-mail and identities to limit the attacker's ability to laterally traverse IT and OT environments. The aim is to:
  - Utilise extended detection and response (XDR) to provide high-quality alerts, and automation to minimise manual steps, including monitoring for brute-force attempts like password sprays and automatically blocking known threats and quarantining services that show signs of malware;
  - Monitor for adversaries disabling security tools and clearing event logs, which is indicative of attackers trying to cover their tracks;
  - Have trained security staff to detect and respond to threats using a combination of modern enterprise configuration and investigative and forensic capability, to determine how and when the attackers obtained access to the assets, so that vulnerabilities can be remediated;
  - Practise responding to predefined attack scenarios, to validate the detection and incident response capability. The SANS Institute recommends combining red team (attacker), blue team (defender) and purple team (combination) for the best outcome to yield a higher return on investment and success.[24]

### Step 3. Make it harder to get in

- *What*: Given the evolving tactics of attackers, it may not be possible to prevent an attack in its entirety. The objective then is to slow the attacker down and to provide a higher probability to identify and quickly respond to the attack. The priority is to detect and prevent the initial methods of entry to the network and provide rapid notification and response should unauthenticated access be attempted;
- *Why*: While some attackers exhibit a high degree of persistence, the objective is to reduce the overall mean-time-to-detect

and limit impact, as speed is of the essence when managing complex multi-platform, multi-cloud and distributed environments;

- *How*: Identify and execute quick wins that strengthen security controls to prevent entry and rapidly detect and evict attackers, while implementing a sustained programme that provides longevity in systematically reducing risk, while increasing capability:
  - *Dynamically evaluating risk*: Extortion and sabotage-based attacks should be registered on the corporate risk register as a high-likelihood and high-impact scenario. This requires real-time posture management and a dynamic response to ensure risk-based policy decisions are enabled through automatic blocking and alerting capability. Organisations that rely on static policies and reporting may not be able to react quickly enough to the changing threat profile;
  - *Remote access*: The Federal Bureau of Investigation warn that remote administration tools, such as RDP, have been on the rise since mid/late 2016 with the proliferation of dark markets selling RDP access. 'Malicious cyber actors have developed methods of identifying and exploiting vulnerable RDP sessions over the internet to compromise identities, steal credentials, and ransom other sensitive information.'[25,26] Microsoft has identified that over 70 per cent of human-operated attacks in the previous year originated with RDP brute-force.[27] Security therefore needs to be configured against third-party virtual private network (VPN) solutions and updates on hardware appliances maintained. This needs to be in conjunction with endpoint protection to validate devices trying to obtain remote access;
  - *Endpoints*: Internet-exposed endpoints are a common entry vector for attackers, as they take advantage of vulnerabilities in operating systems. It is therefore critically important to apply security baselines to harden Internet-facing servers, devices and applications, rapidly deploy security updates, and systematically remove or isolate unsupported versions of software. There is often a 'race against time' from a technology vendor releasing a critical update, and the organisation applying it, to prevent attackers exploiting unpatched systems. Over time, a strategy should be deployed that modernises infrastructure by adopting cloud-based technology and service-as-a-software (SaaS) applications to reduce overall risk, as part of the 'shared responsibility model';[28]
  - *E-mail and collaboration tools*: Attackers frequently enter the environment by transferring malicious content through phishing campaigns, aimed at getting users to download malware or to give up credentials. Attack surface reduction rules reduce common attack techniques to prevent executable content from being launched in weaponised attachments or websites. The objective is to detonate in a sandbox environment and automatically block the malicious content. In addition, priority accounts should be flagged for those individuals who may be high-value targets for business e-mail compromise, such as executives or those with privileged access;
  - *Accounts*: Relying on passwords alone cannot prevent most attacks. Enforcing multi-factor authentication (MFA) or passwordless sign-in for all users, administrators and priority accounts has proven to be one of the most effective ways of preventing 99 per cent of compromised credentials from being utilised,[29] especially when supported with biometric authentication. In addition, steps should be taken to identify and block weak and common passwords.

## PUBLIC–PRIVATE PARTNERSHIPS AND COLLOBORATION

To counter ransomware, a global collaborative effort between the private sector, law enforcement and government is necessary. This requires reducing the profitability of cybercrime, making it more difficult to enter the ransomware market, and supplying victims with effective tools for efficient prevention and remediation.

Unlike physical attacks on sovereign nations, requiring access to land or airspace, attacks on digital infrastructure require neither. Despite attackers being physically located in different countries, they can launch a digital attack from within the victim's own country of operation, and just as easily pull back. This allows attackers to operate with relative ease across jurisdictions and building effective defence requires cooperation and coordination across agencies.

Given the ferocity and persistence of attacks, particularly demonstrated during the global pandemic, world leaders are calling for unification and collaboration against cybercrime, recognising that it requires a joint effort, delivered at scale.

In May 2021, US President Biden issued an executive order[30] on improving the nation's cybersecurity:

> 'Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid.'

In a joint statement following the G7 Summit in July 2021,[31] G7 leaders gave a commitment to fight ransomware, highlighting that:

> 'the international community — both governments and private sector — must work together to ensure that critical infrastructure is resilient against this threat, that malicious cyber activity is investigated and prosecuted, that we bolster our collective cyber defenses, and that States address the criminal activity taking place within their borders […] we call on Russia — to identify, disrupt, and hold to account those within its borders who conduct ransomware attacks, abuse virtual currency to launder ransoms, and other cybercrimes.'[32]

Speaking at the INTERPOL High-Level Forum in July 2021, Secretary General Jürgen Stock called for worldwide police agencies to form a coalition with industry partners to prevent a potential 'ransomware pandemic'.[33] Speaking at the same conference, Tal Goldstein, Centre for Cybersecurity at the World Economic Forum, commented that:

> 'Ransomware is emerging as the "Wild West" equivalent of digital space where anyone, at any point of time, can become a victim. Curbing ransomware demands collective efforts from all to improve cyber hygiene across sectors, to raise cost and risk to cybercriminals through disruptive efforts and to reduce payoff to the criminals.'[34]

## CONCLUSION

Technology is the cornerstone of an advanced society and is incorporated into everything we do. Conversely, cybercriminals seek to exploit any technology that organisations produce: the challenge is determining what form that will take, and how it will affect the supply of interconnected services.

From organised crime to nation-state attacks, these actors are sophisticated criminal enterprises with the resources,

investment and research to deploy complex and persistent attacks against organisations. Increasingly cyberattacks are becoming politically motivated, with a blurring of lines between organised crime and nation states, as attackers move beyond disruption into destruction, with the aim of extracting higher extortion demands.

When considering the digital transformation of their organisation, business leaders need to consider how to manage evolving risk. Resilience is a key success factor when building for reliability, safety, security and longevity. For any new venture or change in business model, it is necessary to consider the threat and opportunity in equal measure.

To uncover shifting attacker techniques and stop them before they can do real damage, organisations need to have visibility across the end-to-end environment, including all interconnections from employees, customers and partners. This ultimately increases the cost and the level of due diligence required, which adds extra burden to organisations. This is not sustainable or cost-effective, and prevents organisations from being able to innovate, especially for small and medium enterprises (SMEs) that lack resource and capability.

More onus is required to help and support the victims of cyberattacks by shifting the focus to the attackers, through closer collaboration between private and public sector, across jurisdictions to disrupt criminal organisations and protect the digital infrastructure they rely upon.

While law enforcement provides effective legal instruments that can be utilised in this regard, there is a time-lag to bring criminals to justice or enact sanctions, by which time the attackers have already fulfilled their objective or moved funds.

While the commitment from G7 and other nations to tackle cybercrime is welcomed, the enactment and enforcement of new legislation and the mechanisms required to implement it invariably take time and the pace of change in technology has invariably moved on.

This is where the role of Big Tech can add value by building security mechanisms and capabilities to actively protect the digital infrastructure, which preserves privacy while making it harder for attackers to exploit. This requires increased collaboration across the public and private sectors and law enforcement that provides the right legal instruments to enable providers to take swift action to thwart attacks and actively share information.

In response to the White House Executive Order in August 2021, the three largest cloud providers, Microsoft, Google and Amazon, along with several other tech providers, announced their commitment to bolster cyber security capability and deliver advanced solutions both in partnership and individually, over the next one to five years.[35] This commitment extends beyond technology and seeks to expand partnerships into education to bridge the skills and knowledge gap.

## References


1. Microsoft (October 2021), 'Digital Defense Report', available at https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report (accessed 24th November, 2021).
2. *Ibid.*, ref. 1.
3. Sophos (April 2021), 'State of Ransomware Report', available at https://news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021/ (accessed 24th November, 2021).
4. *Ibid.*, ref. 1.
5. Microsoft (Septembetr 2020), 'Digital Defense Report', available at https://www.microsoft.com/security/blog/2020/09/29/microsoft-digital-defense-report-2020-cyber-threat-sophistication-rise/ (accessed 24th November, 2021).
6. Varonis (July 2021), 'Revil Ransomware Attack on Kaseya VSA: What you need to know', available at https://www.varonis.com/blog/revil-msp-supply-chain-attack/ (accessed 24th November, 2021).
7. Bleeping Computer (September 2020), 'Revil ransomware deposits $1m in hacker recruitment drive', available at https://www.bleepingcomputer.com/news/security/revil-ransomware-deposits-1-million-in-hacker-recruitment-drive/ (accessed 24th November, 2021).

8. *Ibid*., ref. 1.
9. *Ibid*., ref. 1.
10. *Ibid*., ref. 1.
11. BBC (September 2020), 'Police launch homicide inquiry after German hospital hack', available at https://www.bbc.co.uk/news/technology-54204356 (accessed 24th November, 2021).
12. MIT Technology Review (November 2020), 'Ransomware did not kill a German hospital patient', available at https://www.technologyreview.com/2020/11/12/1012015/ransomware-did-not-kill-a-german-hospital-patient/ (accessed 24th November, 2021).
13. InfoSecurity-Magazine (June 2021), 'Colonial Pipeline incident sparks "Help Desk" Phishing Attacks', available at https://www.infosecurity-magazine.com/news/colonial-pipeline-phishing-attacks (accessed 24th November, 2021).
14. Canada Centre Cyber Security (2020), 'National Cyber Threat Assessment 2020', available at https://www.cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf (accessed 24th November, 2021).
15. Council Directive (EC) 2000/0031 of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2003] OJ L178/1. ELI, available at http://data.europa.eu/eli/dir/2000/31/oj (accessed 24th November, 2021).
16. Microsoft (April 2021), 'Digital Crimes Unit: Leading the fight against cybercrime', available at https://news.microsoft.com/on-the-issues/2021/04/15/how-microsofts-digital-crimes-unit-fights-cybercrime/ (accessed 24th November, 2021); Microsoft (July 2021), 'The growing threat of ransomware' and the testimony given before the House Energy and Commerce Committee's Subcommittee on Oversight & Investigations, https://blogs.microsoft.com/on-the-issues/2021/07/20/the-growing-threat-of-ransomware (accessed 24th November, 2021).
17. Microsoft (October 2020), 'An update on the disruption of Trickbot', available at https://blogs.microsoft.com/on-the-issues/2020/10/20/trickbot-ransomware-disruption-update/ (accessed 24th November, 2021).
18. ITWorld Korea (June 2021), 'FBI seizes $2.3 million in cryptocurrency wallets from Colonial Pipeline ransomware attackers', Tekdeeps.com, available at https://tekdeeps.com/fbi-seizes-2-3-million-in-cryptocurrency-wallets-from-colonial-pipeline-ransomware-attackers/ (accessed 24th November, 2021).
19. The United States Department of Justice, Office of Public Affairs (October 2021), 'Russian National Extradited to United States to Face Charges for Alleged Role in Cybercriminal Organization', available at https://www.justice.gov/opa/pr/russian-national-extradited-united-states-face-charges-alleged-role-cybercriminal (accessed 24th November, 2021).
20. Microsoft (September 2021), 'Rapidly protect against ransomware and extortion', available at https://docs.microsoft.com/en-us/security/compass/protect-against-ransomware (accessed 24th November, 2021).
21. *Ibid*., ref. 20.
22. Dark Reading (March 2019), 'Norsk Hydro: This is how you react to a ransomware breach', available at https://www.darkreading.com/application-security/ransomware/norsk-hydro-this-is-how-you-react-to-a-ransomware-breach/a/d-id/750396 (accessed 24th November, 2021).
23. Microsoft (December 2019), 'Hackers hit Norsk Hydro with ransomware. The company responded with transparency', available at https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/ (accessed 24th November, 2021).
24. SANS Institute (October 2019), 'Red, Blue and Purple Teams: Combining your security capabilities for best outcomes', available at https://www.sans.org/white-papers/39190/ (accessed 24th November, 2021).
25. Federal Bureau of Investigation: Public Service Announcement (September 2018), 'Cyber Actors increasingly exploit the remote desktop protocol to conduct malicious activity', available at https://www.ic3.gov/Media/Y2018/PSA180927 (accessed 24th November, 2021).
26. Avast (October 2018), 'Ransomware attacks via RDP choke SMBs', available at https://blog.avast.com/ransomware-attacks-via-rdp (accessed 24th November, 2021).
27. *Ibid*., ref. 5.
28. Cloud Security Alliance (April 2019), 'The Evolution of cloud computing and the shared responsibility model', available at https://cloudsecurityalliance.org/blog/2021/02/04/the-evolution-of-cloud-computing-and-the-updated-shared-responsibility/ (accessed 24th November, 2021).
29. Microsoft (July 2019), 'Your password doesn't matter', available at https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-password-doesn-t-matter/ba-p/731984 (accessed 24th November, 2021).
30. The White House (May 2021), 'Executive Order on Improving the Nation's Cybersecurity', available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (accessed 24th November, 2021).
31. The White House (June 2021), 'G7 to announce joint actions on forced labor in global supply chains, anti-corruption and ransomware', available at https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/13/fact-sheet-g7-to-announce-joint-actions-on-forced-labor-in-global-supply-chains-anticorruption-and-ransomware/ (accessed 24th November, 2021).
32. G7 Summit Communique (June 2021), 'Our shared agenda for global action to build back better', available at https://www.g7uk.org/wp-content/uploads/2021/06/

Carbis-Bay-G7-Summit-Communique-PDF-430KB-25-pages-5.pdf (accessed 24th November, 2021).
33. Interpol (July 2021), 'Immediate action required to avoid ransomware pandemic', available at https://www.interpol.int/News-and-Events/News/2021/Immediate-action-required-to-avoid-Ransomware-pandemic-INTERPOL (accessed 24th November, 2021).
34. *Ibid.*, ref. 33.
35. The White House (August 2021), 'Biden Administration and Private Sector Leaders announce ambitious initiatives to bolster the nation's cybersecurity', available at https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/ (accessed 24th November, 2021).