WHITEPAPER

Ransomware: **Avoid paying a King's ransom for your data.**

Why a thorough understanding of threat, the need for advanced protection and the removal of implicit trust is critical in guarding against ransomware attacks.

Contents

1. Introduction: Fighting back in the golden age of ransomware.

Digital transformation has made business more efficient and revolutionised connectivity. Cloud storage and applications put files and tools online; mobile devices open that access wherever and whenever; big data, and the tools that help make sense of it, reveal new insights; and the ever-growing Internet of Things feeds those databases with a constant stream of precise information.

But every new tool is an avenue through which an attacker could enter a network and deploy ransomware – all while our reliance on digital technologies means ransomware's impact has never been more keenly felt.

Ransomware works. A single attack could net attackers millions of dollars, and cybercrime itself costs organisations $6 trillion per year globally in damages[1]. History shows us that ransomware attacks have caused damage far beyond a financial cost.

The WannaCry ransomware, a worm exploiting a weakness in Microsoft Windows, spread across the globe in 2017 affecting 230,000 computers in 150 countries and severely hindered the work of organisations like Spain's Telefonica and a third of NHS hospital trusts in the UK. Another ransom-based malware, Locky, made more than 50,000 infection attempts in one day in 2016, masquerading as an emailed invoice and crippling many businesses in the US, Canada and France.

Newer ransomware attacks tend to be targeted at specific entities or industries, and they have affected everything from oil pipeline operations and food supplies to Covid research in recent years.

The European Union Agency for Cybersecurity, ENISA, says ransomware "ranks as a prime threat" in the cybersecurity landscape[2]. Ransomware is becoming an increasingly significant problem, and the way we now work means only a robust attitude to physical hardening, security policy and incident response can reduce its impact.

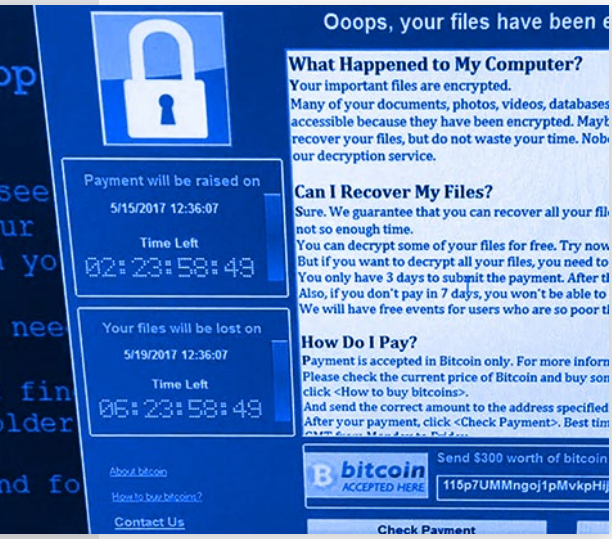
The pandemic caused businesses of all sizes to make rapid changes to their core IT infrastructure in order to support home and hybrid working for remote employees. Businesses now rely on the easy availability of cloud storage, an abundance of online services, and often on third-party applications to create new data management opportunities and offer workers flexible access. Off-the-shelf tools make rolling out remote service provision more straightforward and lessen the load on internal systems.

But what is convenient for IT teams is also convenient for potential attackers.

cybercrime itself costs organisations $6 trillion per year

1. https://www.sdxcentral.com/articles/news/cisco-ceo-cybercrime-damages-hit-6-trillion/2021/05/
2. https://www.enisa.europa.eu/news/enisa-news/hackers-for-hire-drive-the-evolution-of-the-new-enisa-threat-landscape

What is ransomware and what does it do?



Ransomware is a specific kind of malware. Think of it as an evolved computer virus. Installed either on purpose or inadvertently, the goal of ransomware is to sow a particular kind of chaos. Where a virus may corrupt files or render a system inoperable with no real end goal beyond disruption, ransomware is designed to leave systems (apparently) mostly intact – enough that a victim might be convinced to pay a ransom fee to eventually get their system back up and running.

Typically, a ransomware attack spreads through various means, including phishing emails with malicious links or attachments, portable computers, exposure to public Wi-Fi, and Zero-Day vulnerabilities, causing significant disruption. If the ransom is paid, typically by sending cryptocurrency to an anonymous wallet, the criminal agrees to provide the information required to unlock or decrypt the affected data.

But this is by no means guaranteed – the Kansas Heart Hospital, for example, paid a ransom only for its attacker to then demand a second, larger fee[3]– and the keys may take several days to arrive. Even if, instead, the approach is to start afresh and restore from backups, a poorly managed IT setup might mean it could take days or weeks to get back up and running, or that those backups could themselves be affected.

Increasing attack sophistication

Malware authors are flush with more directions of attack – and potential vulnerabilities lurking in a wider range of easily-accessed systems – than ever before. Ransomware spreads through various means, including phishing emails with malicious links or attachments, portable computers, exposure to public Wi-Fi, and Zero-Day vulnerabilities.

Phishing and its many variants are growing in sophistication. Computers and workers are progressively moving away from the office; hybrid working often leads to the use of insecure networks, out-of-policy hardware, or security updates that lag behind – all of which can be exploited. And new tactics are being shared by hackers all the time which makes spotting the signs of phishing incredibly difficult – and it only takes one successful attack to bring down an entire network and put the integrity and privacy of a company's data at risk.

Zero-day attacks moreover, which exploit platform vulnerabilities known only to hackers, are also a possibility and present a real risk. As much as cybersecurity practise has kept pace with known threats, zero-day attacks aren't something that can be prepared for. A backdoor in a VPN or a previously unknown bug in a login process could be all it takes for hackers to bring chaos to a network. The Log4j exploit, which came into focus at the beginning of 2022, enabled hackers to take control of web-facing servers with a simple string of text, and is estimated to have affected over 44% of all corporate networks worldwide[4].

A recent vulnerability of the Zimbra Collaboration Suite resulted in hacks on almost 900 servers[5], and went unknown (and unpatched) for over a month. This is not uncommon. Such attack vectors are often shared between underground networks which aim to develop and launch coordinated hacks before they are more widely known and patched.

affected over 44% of all corporate networks worldwide

3. https://www.extremetech.com/extreme/229162-hospital-pays-ransomware-but-doesnt-get-files-decrypted
4. https://fudosecurity.com/company/blog/impact-of-apache-log4j-vulnerability-and-how-to-stay-safe/#:~:text=Representing%20a%20high%2Drisk%20and,44%20%25%20of%20corporate%20networks%20worldwide.
5. https://www.bleepingcomputer.com/news/security/almost-900-servers-hacked-using-zimbra-zero-day-flaw/

Zero-day exploits are routinely packaged together in tools which help administrators deploy penetration testing to discover vulnerabilities in their networks – but those same tools can allow even those without advanced knowledge to launch attacks.

Ransomware attacks are becoming increasingly more sophisticated and damaging, too. Critical infrastructure is at risk, as 2021's Colonial Pipeline attack proves. Ransomware-as-a-service puts the tools and expertise of hackers in the hands of third parties, which might range from competitor companies to state-sponsored hackers performing geo-political attacks.

ENISA's 2020-2021 threat landscape report[6] states that, "We are observing the golden age of ransomware… and some argue that it has not yet reached the peak of its impact." It is clearly time to develop a robust data management policy before it is too late.

How ransomware infiltrates a network

Phishing

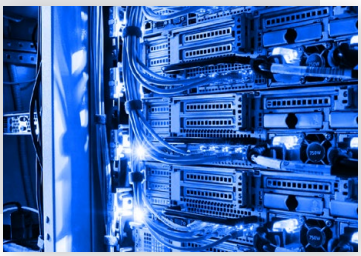
Attackers using phishing attempt to steal user data, including login credentials and credit card numbers, to gain the level of access required to deploy ransomware software. Generally, phishing is performed by a hacker masquerading as a trusted entity – a colleague or supplier – through email, instant message or text message. Advanced forms include spear phishing, which narrows phishing's usually wide net to target known individuals; whaling, which takes aim at the highest-level employees; and vishing, which utilises telephone conversations – a danger as AI-driven deep fakes begin to make voice replication more realistic.

Zero-day attacks

Security vulnerabilities may hide in software and firmware, unknown to their creators or users. If a hacker finds one of these, it's known as a zero-day vulnerability – one for which the developer or vendor has had no notice of the flaw. By definition these cannot be prepared for directly, and their existence may not even be widely known about until long after an attack has occurred.

Portable computers

Access to company hardware can provide hackers with a direct connection to a network. A lost or unattended laptop, an improperly secured encryption module, or a portable drive filled with data could be extremely valuable for an entity wishing to infiltrate internal systems, and the growing prevalence of remote working means this is a growing attack vector.



Insecure networks

Workers operating remotely may attach their hardware to compromised networks. Public Wi-Fi is inherently insecure and can be monitored and investigated by hackers looking for credentials or sensitive information in data streams. Home Wi-Fi may also carry vulnerabilities; a user's own network may be compromised without their knowledge, particularly as it is likely to be home to numerous devices which may not pass corporate compliance standards.

6. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

2. The evolving threat landscape

The threat of cyber-attacks has never been greater. From indiscriminate mass phishing to targeted ransomware attacks on public organisations, private companies and even national infrastructure, cybercrime is growing fast for one key reason: there's serious money to be made.

The vital nature of infrastructure makes it a prime target – the Colonial Pipeline ransomware attack netted its hacker group around US$4.4 million – but corporate ransomware attacks can pay out even more. In March 2021 one US financial firm paid US$40 million[7] to regain control of its network, and recent ransomware attacks have demanded upwards of US$70 million[8].

But it's not only large-scale operations that are lucrative. 46% of those hit with a ransomware attack pay the ransom, at an average of over US$800,000 – in the manufacturing and utilities sector, the average is closer to US$2 million[9]. Ransomware is big business, and it follows that cybercrime has begun to take on a corporate structure of its own.

Professionalisation of malware

Prospective hackers, even those without the skill or know-how to create attacks, can now access Ransomware-as-a-Service (RaaS). This offers criminals access to off-the-shelf malware variants, expertise from the cybercrime community, and even databases full of online credentials for a one-off fee, a subscription, or a share in any profits.

Some attackers have even begun offering their victims access to 24/7 support to make paying ransoms (and, theoretically, getting back online) as easy as possible. This level of professionalism is designed as a convincer to businesses: if it's easiest to pay up, move on and get back up and running – and, indeed, if it is cheaper to pay than it would be to suffer an average of 20 days of business downtime[10] - the theory is that a ransom payment could simply be chalked up in the loss column.

Commonly used terms and explanations associated with ransomware attacks:

Crypto

The most commonly thought-of variety of ransomware is based on encryption. This malware targets a single machine or, in some cases, spreads across a network, encrypting and essentially trapping certain kinds of data until a ransom demand is met. This could be, in effect, impenetrable. 2048-bit RSA encryption has yet to be cracked, and would theoretically take the average PC hundreds of millions of years to break; some ransomware uses less-powerful encryption, and some includes inadvertent software flaws which can make recovery straightforward, but modern implementations tend to be more resilient.

7. https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack
8. https://www.theverge.com/2021/7/5/22564054/ransomware-revil-kaseya-coop
9. Sophos State of Ransomware 2022 - https://assets.sophos.com/X24WTUEQ/at/c5234fvn45pvmk5w6nhh4vkh/sophos-state-of-ransomware-2022-infographic.pdf
10. https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/

Locker

Locker ransomware targets a machine's core functions, essentially locking users out. Available interactions may be limited only to a window containing a ransom demand. This kind of malware does not always encrypt sensitive data, sometimes merely locking the user's machine instead, though whichever method it employs it can be highly disruptive and costly in terms of productivity, and may force the purchase of replacement hardware or in some cases cause a complete loss of data.

Extortion

Some ransomware is designed with more malice. Double-extortion ransomware sees attackers taking a copy of sensitive data before encrypting it, demanding a ransom both for the release of the original data and one to prevent its spread. This means even companies with strong backups may fall victim. Triple-extortion ransomware, in which attackers issue demands to affected third parties as well as copying and encrypting data, is a further threat and one which comes with serious reputational damage.

Ransomware-as-a-service (RaaS)

Aping the model of Software-as-a-Service, RaaS is a new trend which sees ransomware authors either licensing their malware to third parties which might not otherwise have the capability to produce their own, or deploying targeted attacks on behalf of a third party for a fee. This means the number of potential attackers has grown, and its newfound ease of use makes ransomware a more attractive option in industrial or international espionage.

Fresh techniques to extort the ransom

If a company is unwilling to pay, ransomware attackers now use ever-more devious techniques. They find and copy data rather than simply encrypting it, threatening to spread secrets to corporate rivals in a practice known as double extortion. Some might even go further and threaten to demand a ransom not only from the attacked company but from affected third parties – triple extortion – which means significant reputational damage as well as financial losses.

Don't think that a ransomware deployment is a simple task. Criminals will work hard to find multiple avenues of infiltration – they will identify hardware and software weaknesses, use phishing to collect personal information and credentials of high-level employees, secretly snoop around networks and storage to identify valuable data, all before deploying a targeted attack with the maximum impact.

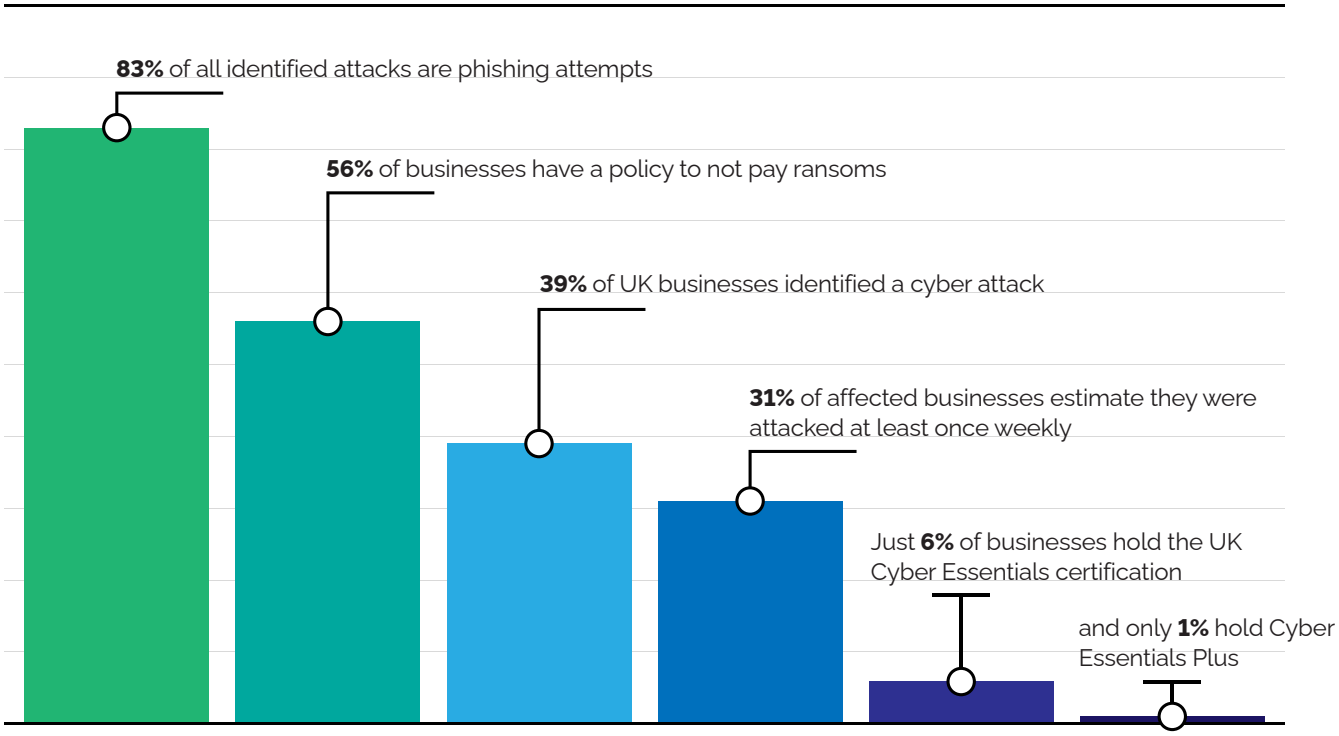
A heavier security burden

The techniques hackers use to carry out such reconnaissance have also improved markedly in recent years. Hackers use private servers and networks to test for zero-day vulnerabilities, usually targeting the most widely used software platforms or device firmware. This isn't always a manual process: researchers on either side of the moral divide often develop bespoke tools to scan for vulnerabilities, often finding hundreds in a sweep. Bug bounties can be a tempting tool to encourage hackers to use their skills for good, but the potential rewards of a ransomware attack often outweigh these.

Automation is not only valuable in bug discovery. Spear phishing, the practice of crafting targeted phishing attacks on individuals by aping high-level employees, can now be automated via AI to produce communications so authentic that they generate conversion rates of up to 80%[11]. AI can be, and has been, used to emulate the voice of CEOs[12], making phone-based phishing (known as vishing) truly effective. And as the power of AI grows, such deep fakes will infiltrate video calls too.

The threat landscape may be broadening, but it is not new. Companies know of the danger of cyber attacks, and regulators do too. Gartner predicts that by 2025 60% of organisations will use cybersecurity risk as a primary factor in determining whether they'll be willing to do business with a third party[13]. One incident could jeopardise the reputation of any company, large or small – and the potential for such incidents is only growing.

Cyber attack stats: 2021-2022



Source: UK Cyber Breaches Survey 2022[14]

11. https://www.scmagazine.com/analysis/phishing/ai-as-a-service-tools-craft-spear-phishing-emails-with-minimal-human-input
12. https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402
13. https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio
14. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

3. Cloud and the limitation of liability

It's fair to say that the workplace has changed, perhaps forever. Even before Covid-19, many businesses were exploring hybrid and remote working; since then, over half of employees work remotely once a week[15], and 74% of professionals expect remote work to become standard[16]. Returning to the office full time may never truly be an option: 97% of employees appear to be happy with the status quo,[17] wanting to avoid returning to the office full time.

For all the opportunities this opens for flexibility and improved quality of life, the rise in remote working provides many more opportunities for data to be compromised. The FBI reported a 300% rise in cyber incidents over the first wave of lockdowns[18] – businesses were forced to move to large-scale cloud provision quickly, speeding the adoption of digital technologies in internal operations by three to four years[19] in a matter of months.

It was a time of immense pressure for IT departments. Loopholes were missed, software and processes were not properly vetted – and, all of a sudden, new applications and platforms became a huge target. While the severity of the risk means cybersecurity attitudes have now mostly caught up, a remotely operating workforce that is increasing in size remains a weak point.

Remote working presents increased risk

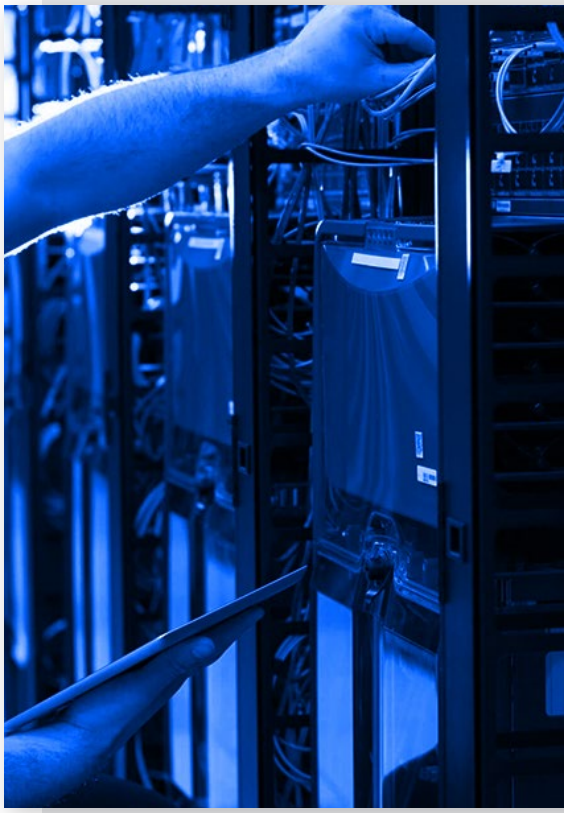
Workers now move around more often. Laptops move in and out of the office regularly, and many employees prefer to work in coffee shops or cafes than at home. It's not unusual to hear about laptops being left in the open or lost on public transport; TfL says an average of two laptops are left on the London Underground every day[20]. Even in the workplace, an employee may not have a permanent desk and may be lulled into the confidence of leaving their hardware unattended wherever they may be sitting.

Without proper controls, loose hardware movement presents attackers with an opportunity to infiltrate systems; shoulder-surfing a password, listening in on a compromised Wi-Fi network or stealing a critical laptop or USB drive and becoming privy to sensitive information. Employees must be made aware of their role in data security and strict usage policies must be implemented and adhered to by all parties. But the data itself must also be secured whether online, in transit, or at rest.

The FBI reported a 300% rise in cyber incidents

15. https://review42.com/resources/remote-work-statistics/
16. https://www.forbes.com/sites/ashiraprossack1/2021/02/10/5-statistics-employers-need-to-know-about-the-remote-workforce/?sh=4194b5f3655d
17. https://review42.com/resources/remote-work-statistics/
18. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2021.pdf (p19)
19. https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever
20. https://www.information-age.com/two-laptops-left-tube-every-day-reveals-transport-london-123461389/

Multi-factor authorisation is important to protect even compromised credentials – though hackers have begun to build clever systems which can sit in the middle of SMS authentication. A physical encryption module helps to reduce data loss due to human error but doesn't stop it happening – particularly if that encryption module is also compromised or stolen, or if the employee leaves the company with it in their possession. It is therefore essential that local storage is encrypted, ideally at the hardware level, and made tamper-proof to prevent malicious action resulting in a loss of valuable company data.

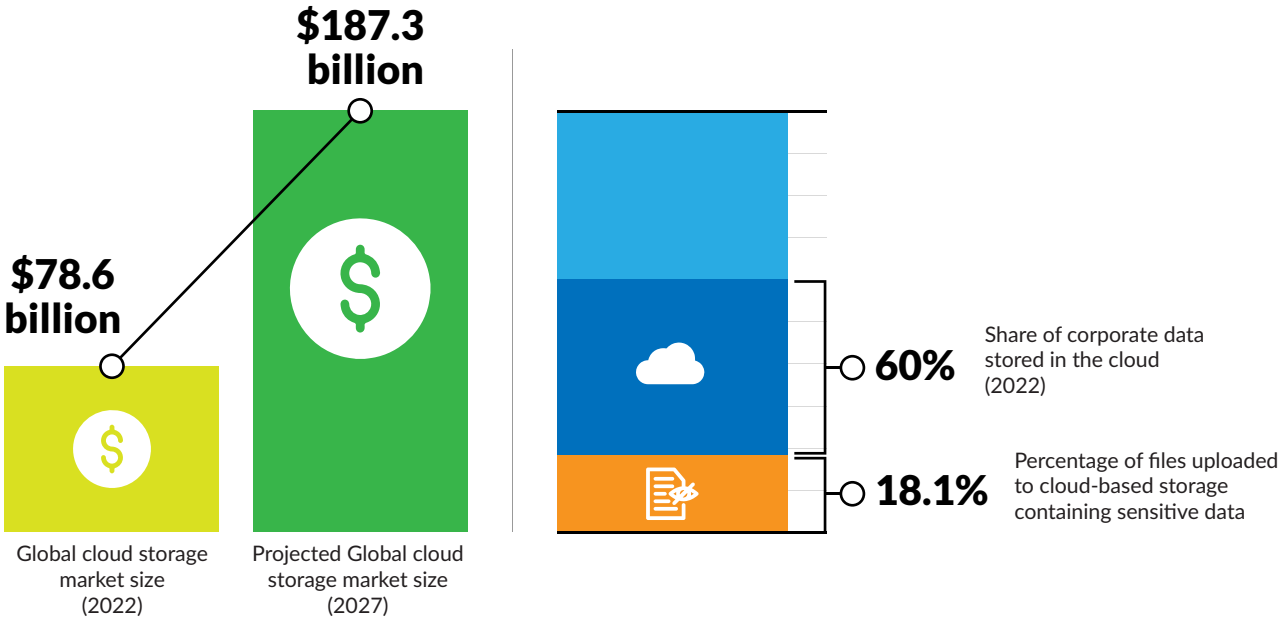


Cloud compromises

The move out of the office has necessarily meant a new reliance on cloud storage. This is understandable and, in some cases, vital – but it's also a concern. Using cloud storage usually means trusting data to a third-party data centre. Data centres are just as vulnerable to cyber attack as local networks, perhaps more so, and a fire or disaster at a data centre could cause significant disruption to business storage.

Local backups, therefore, are imperative, as is protecting anything stored in the cloud in the right way. Encryption is vital, of course. In the event of a breach, data should be stored in a form which cannot be exploited by criminals – but the requirement for encryption cannot be dependent on any cloud storage provider. Server-side encryption stores encryption keys in the cloud, making them accessible to hackers and potentially by phishers; moving the decryption to a secure hardware module, inaccessible except in person, makes for a key storage solution without the same vulnerabilities.

Growth of the cloud



Sources:

- *https://www.researchandmarkets.com/reports/5145033/cloud-storage-market-by-component-solutions-and*
- *https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/*
- *https://www.mcafee.com/blogs/enterprise/cloud-security/12-must-know-statistics-on-cloud-usage-in-the-enterprise/*

4. The human factor

Hackers have many avenues through which they could make an attack. They might look to compromise physical hardware. The rise of hybrid working has led them to target vulnerabilities in VPNs and exposed ports on protocols like RDP. Alternatively, or in addition, they might attempt to infiltrate the supply chain, introducing compromised components and software into an organisation undetected.

But these methods are difficult to achieve, particularly at scale. While small- and mid-sized businesses are still very much targets, hackers are now attempting to catch the largest prizes. The easiest way to infiltrate a system with ransomware is to target the weakest link in the chain: the human element.

The 2021 iStorage backup survey highlighted that users already have a strong idea of the importance of cyber security, with 88% of those surveyed stating that their employers could do more to implement tighter cyber security practices. That's data which comes from employees, not the CEO or CTO. Users know they have their part to play – but their role in data security needs to be enforced through proper governance, a sharp and evolving compliance policy and, most importantly, by ensuring that everyone understands why continuing vigilance is so important.

The rise of social engineering

Social engineering is core to cybercrime, and it may be today's primary method of infiltration: 94% of cyber attacks begin with a phishing email. Confidence tricks – subject lines ranging from a threat of an imminent password change to updates on holiday or Covid policies – are used to convince a user to click through. An attacker with insider knowledge (or one which has done a lot of research) might tailor their tactics to address a known event or pain point. If a particular employee has been targeted, or a certain executive researched, attackers might use specific information to target employees with pinpoint accuracy.

SoSafe's Human Risk Review 2022 shows that hybrid working models pose not just a physical risk but a logical one. Amongst the most successful phishing subject lines in 2021 were 'Important: CORONAVIRUS update' and variants of 'You must complete the following task'. Many attacks play on the recipient's confidence by piggybacking on other current events, but those which play on positive emotions like flattery and trust are most effective.

The multi-layered nature of modern attacks means phishers are also becoming more creative with their disguises. They may have gained access to a known service provider, using it to help stop bogus emails from being flagged by automated systems. Similarly, they may host their websites on domains which look authentic but aren't – a recent practice sees hackers replacing certain characters in URLs with Unicode alternatives which look identical. Some might also take advantage of zero-day vulnerabilities to produce authentic-looking communications which completely bypass network security, which is the reason platforms like Microsoft Exchange Server are some of the most commonly targeted and exploited by hackers.

94% of cyber attacks begin with a phishing email

A phishing attack isn't always easy to spot, particularly for busy individuals or those without a certain level of computer savvy. Critically, phishing attacks are often successful - two out of three users open phishing emails, and almost a third will click links or attachments within. Over half of those will then enter details into, for example, a fake login screen[21].

Human hardware

As the workforce moves in greater numbers to home and hybrid working, the number of threat vectors has naturally increased. Even usually astute employees may be more relaxed while at home and lower their guard. They may even be unaware of the additional risks their home network could introduce, from insecure Wi-Fi to unpatched smart devices. Even in the workplace, the rapid expansion of the Internet of Things (IoT) places many more connected devices on the same networks as vital machines. Many IoT devices may host critical vulnerabilities or out-of-date security patches, leaving them open to potential zero-day attacks.

22.3 billion devices are expected to be IoT linked by 2024,[22] any one of which could act as an entrance point to an improperly secured network. Employees may also be tempted to save work on insecure cloud services or use personal devices and mobile phones because their work tools are less comfortable or user-friendly.

Employee knowledge of cyber threats

- **77%** do not understand the term '***ransomware***'
- **70%** do not understand the term '***malware***'
- **65%** admit to having lost data
- **99%** state that data loss or theft is of concern

Source: iStorage backup survey 2021

21. SoSafe Human Risk Review 2022, p44
22. https://www.consilium.europa.eu/en/policies/cybersecurity/

5. Regulation and trusted supply chains

The expansion of cybercrime from comparatively small-scale attacks to inter-sector, international and professional disruption means its increased impact has been mirrored by growing concern from governments and regulators. Much of a business's data security strategy must now be driven by regulatory demand – and it is an internal responsibility to ensure it is met.

Penalties for non-compliance can be damaging. In the case of the European General Data Protection Regulation (GDPR), a serious data breach may be met with a fine of 20 million euros or 4% of a company's annual turnover[23]. Breaching more than one set of international regulations may mean multiple fines and penalties.

The fact that ransomware has significantly changed tack in recent years, shifting from a strategy of restricting access to data to one of cloning and potentially distributing it, makes such attacks far more impactful in terms of regulations. Under GDPR, the company is deemed liable for a breach in all but extreme cases; an individual is only deemed responsible for a breach if they have made it intentionally. This means if data leaks from an employee's machine due to an external attack like a ransomware infection, personal liability falls instead to data protection officers, managing directors and the executive board.

Regulations are not only put in place to punish – they're there to protect

Updated regulations

Regulations are not only put in place to punish – they're there to protect. The acceleration of digitalisation during the pandemic – and the subsequent rise in ransomware attacks and other malware – has not gone unnoticed by regulators.

In May 2022 the European Council and European Parliament reached provisional agreement on a revised Network Information Security directive (NIS2) which aims to standardise and embed a baseline of cybersecurity standards across EU member states. It calls for reporting of cybersecurity incidents within 24 hours, improved levels of information exchange between essential and important entities, and a centralised hub for cyber crisis management amongst many other guidelines.

The White House, while not directly issuing regulations, has suggested that US business leaders immediately convene to review their corporate security posture[24]; the UK's National Cyber Security Strategy[25] has outlined five pillars of improvement before 2025, which include measures to begin a consultation on NIS regulations, strengthen the regulatory framework, and propose improvements to corporate resilience reporting.

It is likely that worldwide regulatory frameworks will continue to evolve alongside the increasing risk of cybercrime, but not every region is as stringent as the EU – meaning strategy when dealing with supply chains and outside factors must reflect their potential adherence to a different set of rules.

23. https://gdpr.eu/fines/
24. https://www.whitehouse.gov/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf
25. https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

Zero Trust

The Zero Trust model builds a security framework which requires all users, assets and resources to be continuously validated. In effect, Zero Trust removes an organisation's defences from its internal perimeter and puts the security focus on every entity it interacts with. A Zero Trust Architecture (ZTA) grants no implicit trust to any asset; while the term is commonly applied to networks and digital users, ZTA is particularly relevant in data protection and end-to-end security for hybrid or remote workers, and its principles can equally be applied to supply chains.

Business networks have grown beyond the protection of a simple firewall or set of in-office policies, and monitoring of supply chains is now paramount: every connected device, every firmware update, every third-party platform or tool must clearly demonstrate its security credentials, particularly as liability for data breaches is highly unlikely to be passed on to those third parties. We cannot know when a zero-day attack might occur, but ZTA – properly applied – can minimise the impact of any new threat.

Business networks have grown beyond the protection of a simple firewall

In brief: White House guidelines to protect against ransomware

Implement five best practices

- Multifactor authentication, endpoint detection and response, encryption and a skilled, empowered security team significantly reduce the risk of a successful attack

Backup

- Backing up data, system images and configurations, regularly testing them and keeping backups offline enables systems to be restored in case of attack or disaster

Update and patch systems promptly

- Use a risk-based strategy to inform your patch management system – including operating systems, applications and firmware

Test your incident response plan

- Testing allows teams to discover gaps and flaws in incident response – and to know exactly what impact an incident might cause

Check your security team's work

- Employ third-party penetration testing services to test the security and rigidity of your defences

Segment your networks

- Split operations from business functions, and limit access between such functions to enable them to be isolated in the case of an incident

6. A new security framework

As we have learned, regulations are tightening, the punishment for data breaches is becoming harsher, and ransomware may only be at the beginning of its golden age. Ransomware as a concept cannot be stopped – the worldwide focus must be on ensuring it cannot make an impact. There is no wiggle room left: every organisation, large and small, must develop the most robust security framework possible, particularly in an age where use of cloud storage is growing and the number of network-connected devices is exploding.

Every employee must be critically aware of that policy and the reasons behind it, to establish a core culture of cyber hygiene and resilience. Technical training and education are a vital part of a complex picture to ensure a base level of understanding and compliance; however hardened one's network policy might be, security starts and ends with humans.

Hardware security

Hardware must, of course, be another critical facet to solve the cyber security conundrum. Every organisation must strengthen its security posture top-to-bottom. It must develop a rigorous and well-vetted program of firmware and software updates to ensure every known vulnerability is addressed immediately.

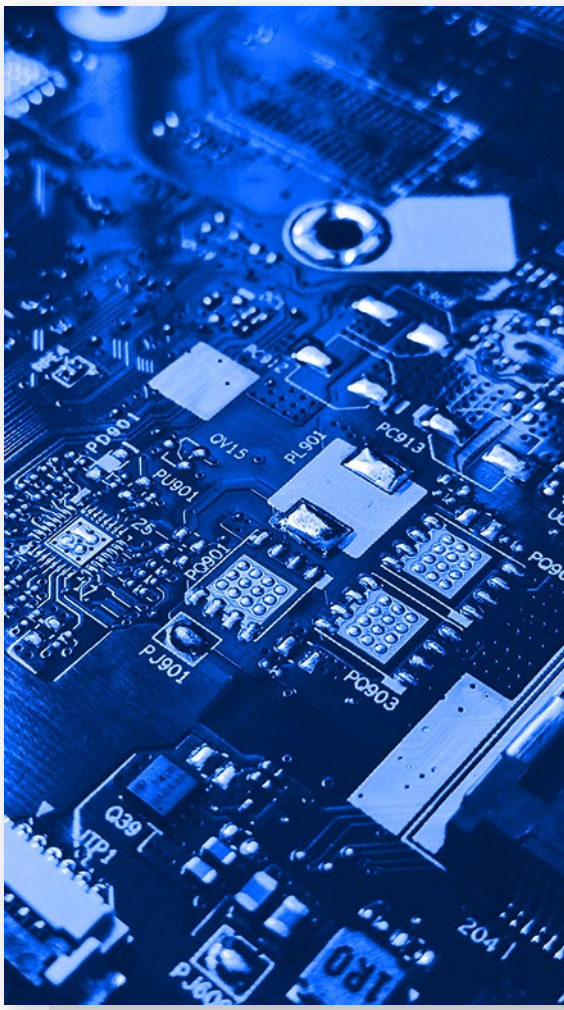
The potential for zero-day attacks must be foremost in administrators' minds, leading to a comprehensive and strict policy of hardware control which reduces the potential for rogue elements to introduce new attack vectors both on premises, through cloud vendors, and when workers access resources from home. Companies must ensure that policies meet new regulations and government guidelines even before they're ratified, and that businesses they work with also comply

Building every policy on the basis of Zero Trust may introduce small hurdles for user connectivity and inter-business communications, but it equally makes implementing a slick and effective security policy smoother. Reducing and streamlining the number of third-party tools can vastly decrease the complexity of managing those tools – an IT administrator with one control panel will be more effective than one bouncing between many.

Data first

Whatever an organisation's policies, integrity of data must come first. It is data which ransomware locks, steals and spreads. Maliciously encrypted data means the incredible costs of downtime, and loose data results in falling foul of regulatory guidelines. Neither is an outcome any business needs.

Companies must ensure that policies meet new regulations and government guidelines



Organisations must be the guardians of their own data because data centres are as vulnerable to attack and disaster as any other entity. While using cloud storage may be an inevitable part of an increasingly remote workforce, a secure backup and data control policy is vital in order to rebound from a ransomware attack quickly. Backups must be secure, thorough and regular, stored in triplicate online, offline, and on devices completely independent of the location and network.

Empowering IT administrators with full control and the necessary hardware does not have to be difficult. iStorage's datAshur BT USB flash drive is FIPS 140-2 Level 3 certified and encrypts data in real time, unlocking via biometric authentication over a FIPS compliant encrypted Bluetooth channel and comes with optional full remote administration tools from a single, easy-to-understand console.

Furthermore, iStorage's diskAshur PRO² and DT² drives are certified to FIPS 140-2 Level 3, NCSC CPA, NLNCSA BSPA & NATO Restricted standards, using 256-bit AES-XTS hardware encryption to seamlessly lock down large amounts of backed up data. And the cloudAshur hardware security module can ensure that any time employees interact with data in the cloud, store data locally, or even share sensitive data over email, it is encrypted to both address security vulnerabilities associated with the cloud and to comply with all relevant data protection regulations. Remote management ensures that access is restricted to only those that need it – if an employee leaves, their cloudAshur module can be disabled by an administrator.

iStorage's unique combination of products gives data the ultimate in protection. Data stored on external drives is fully air gapped; any infiltration of a network or zero-day exploit cannot reach data which is not physically attached. Networks or computers locked down through ransomware are a problem, but physical separation of key data ensures downtime can be kept to an absolute minimum. And while device management can often be difficult, aligning everything along a simple path of remote management ensures sticking to your organisation's policies and complying with regulations is as easy as it can be.

About iStorage

iStorage is the trusted global leader of award-winning, PIN authenticated, hardware encrypted portable data storage & cloud encryption devices.

iStorage offers the most innovative range of products to securely encrypt, store and protect data to military standards; safeguarding valuable and sensitive data to ensure compliance with stringent regulations and directives such as GDPR, HIPAA, SOX, NRC, GLB and DHS Initiatives.

Today, iStorage products are used by government, military, multinational corporations as well as consumers in over 50 countries, with the mantra that encryption is an essential commodity required by all.

Learn more at https://istorage-uk.com