Shield business performance from the threat of ransomware

Content

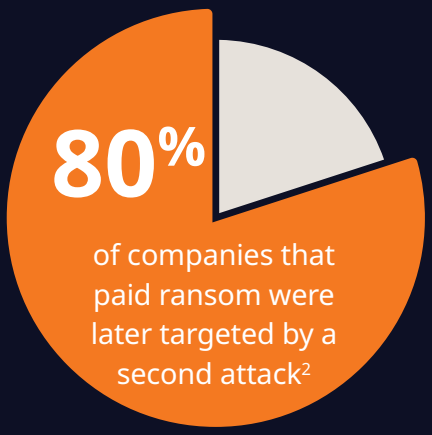
Key takeway:

This paper delves into the growing threat of ransomware. It discusses how organizations can strengthen their defenses before, during and after a ransomware attack. In addition to the evolution of ransomware attacks over time, it covers the impact of ransomware attacks in the digital age, why digital identity is a common ransomware target, and how to build a holistic approach to ransomware protection and recovery.

A weekend in cyber turmoil

Imagine this: It's a regular Friday afternoon in the office. Employees are getting ready for the weekend ahead. Little do they know that a malicious threat is waiting in the digital shadows, ready to wreak havoc. As the clock strikes 5pm, an unsuspecting employee opens an innocuous email from what looks like a trusted vendor. Chaos ensues. A malicious attachment in the email swiftly encrypts critical files across the company's network. Every affected computer screen shows a ransom note demanding a significant sum in exchange for the decryption key that would restore access to the company's files. Failure to comply within 48 hours means loss of private data, regulatory fines, reputational damage, loss of confidence in the C-suite and a negative impact on the company's share values as soon as the markets open on Monday.

The clock also starts ticking on the number of days and hours to report the incident to comply with strict regulations while deciding on the best strategy — to deal or not with the threat actors. Paying a ransom isn't a guarantee that data won't be leaked on the dark web. And, due to payments crossing borders, doing so is increasingly becoming illegal in many countries.



With digital technologies becoming the core of business operations and enterprises becoming data-driven entities, ransomware isn't just a nuisance. It's an existential concern. This is the real threat ransomware presents: Malicious software or malware that prevents an organization from accessing computer files, systems or networks and demands a heavy ransom for their safe return.

And as tech evolves, so does the threat. Enterprises must constantly stay ahead of the curve in not only protecting their critical assets but also being ready to respond to a possible breach in a way that isolates and limits the impact.

A brief history of ransomware

Despite recent infamy due to its destructive impact on business finances, essential services and geopolitical issues, the risk of ransomware itself isn't a new phenomenon. The AIDS Trojan, also known as PC Cyborg, was one of the earliest recorded ransomware attacks, all the way back in 1989. Distributed via floppy disks and encrypted file names on the victim's hard drive, the attacker demanded a payment of $189 be sent to a post office box in Panama.

In 2017, a worldwide ransomware outbreak named WannaCry disrupted thousands of computers in over 150 countries. It attacked the Windows Operating System and encrypted data, demanding a ransom paid in Bitcoin. The interesting fact was that it exploited a vulnerability for which a patch had long existed — even today, many cyberattacks exploit known published vulnerabilities. More recently, in 2023, the file-transferring software MOVEit's zero-day vulnerability was exploited by the CL0P ransomware, targeting large brands across industries and public services and affecting more than 60 million individuals.[3]

Ransomware operators started as isolated groups with malicious intent. It has since evolved into a sophisticated industry. New models, like ransomware as a service (RaaS), equip anyone to launch attacks with ready-to-deploy software tools and generate additional revenue. Some examples include LockBit, Ryuk and DarkSide, which was responsible for the high-profile Colonial Pipeline breach. That attack halted operations and resulted in fuel shortages and the declaration of a state of emergency across 17 U.S. states — apart from the financial costs. According to Cybercrime magazine, the global cost of ransomware is expected to be around $42 billion in 2024 and rise to about $265 billion by 2031.[4]

The reasons for ransomware's popularity among cybercriminals are clear:

- Deploys easily, for quick financial returns and lucrative cyber-insurance payouts
- Covers a broader range of threat vectors
- Starts up easily, with subscription-based payment models lowering entry barriers
- Remains difficult to trace once the ransom is paid in cryptocurrency to international actors

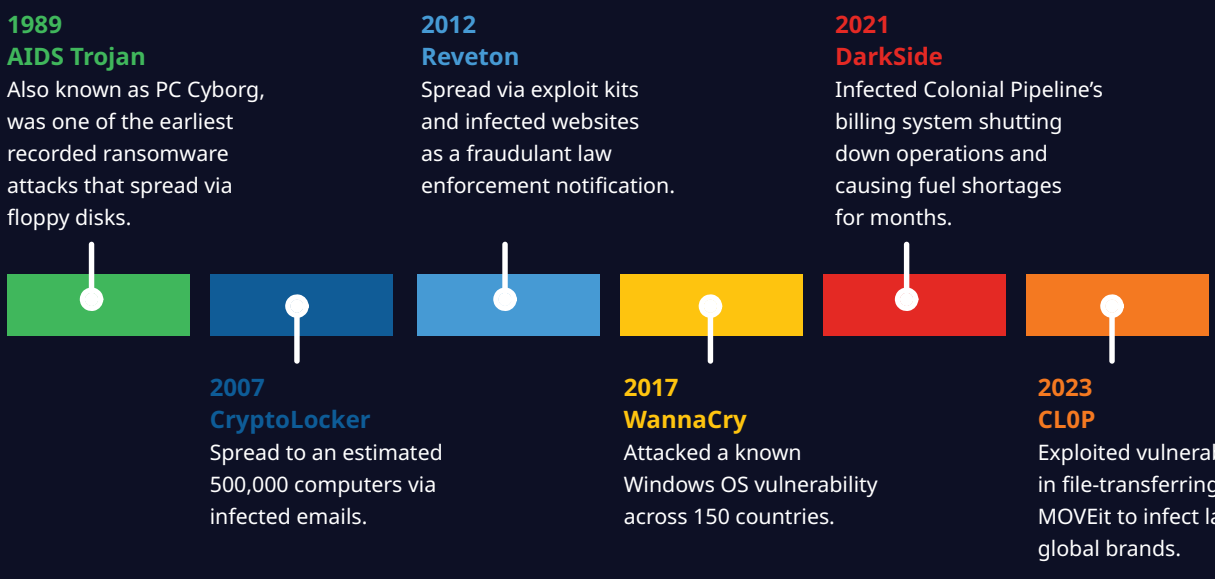


Figure 1: The evolving nature of ransomware attacks over time

Evolving with the times

Over the past decade, ransomware has evolved in tandem with the digital landscape, the emergence of hybrid work environments and, more recently, advancements in connected devices and artificial intelligence (AI).

Digital landscape: Today, digital is ubiquitous. But the interconnectivity of devices, networks and systems has also offered ransomware operators a broader attack surface and impact radius. As businesses transition to cloud-based services, edge computing and IoT, ransomware operators are adapting to the new digital landscape. They're targeting not only traditional on-premises vulnerabilities but also robust cloud- and web-based infrastructures.

Hybrid/remote workplace: The shift to hybrid work environments has unveiled new security complexities as traditional corporate perimeters have vanished. This change makes it challenging for organizations to secure every entry point effectively. Recent studies have found that remote working increased ransomware and social engineering risk by 53%.[5]

Impact of AI: Ransomware operators are already using AI for targeted attacks. They analyze criteria, such as economic value, security gaps and data sensitivity, to identify victims more efficiently. While AI has enhanced threat detection in cybersecurity, ransomware has countered these improvements by leveraging AI to evade detection and refine tactics. The advent of generative AI might pose an even bigger threat. GenAI gives bad actors the tools to make ransomware that adapts and learns from its encounters with defensive mechanisms. The result could be attacks that are more complex and difficult to trace.

Encryption algorithms: Cybercriminals use smart encryption algorithms that make it more challenging for organizations to decrypt files without paying a ransom. Some modern ransomware not only encrypts data but also exfiltrates crucial information, leading to data breaches. These malicious actors employ a spectrum of encryption algorithms to fortify their malware, including the following:

- Swift and autonomous symmetric ciphers
- Asymmetric ciphers that rely on public-private key pairs
- Hybrid or combinations of multiple encryption techniques to add complexity
- Double-encryption tactics to intensify the complexity of the recovery challenge

Phishing tactics: The most common yet effective tactic for ransomware attacks is phishing emails to gain initial access. Ransomware groups use personalized and convincing methods to trick individuals within organizations. Today, about 1.2% of all emails sent are malicious, which translates to 3.4 billion phishing emails daily.[6]

Figure 2: Different types of phishing threats

Why should organizations be worried?

Ransomware attacks are becoming more complex and frequent. Globally, ransomware affected more than 72% of businesses in 2023.[7] It poses a serious threat to brand value, operations, productivity, economic health, market value and reputation.

Decline in market value: Aside from financial implications, one of the biggest concerns for enterprises facing ransomware attacks is eroded market value and the resulting drop in shareholder confidence. Recent reports show that businesses suffer an average decline of 7.5% in stock value after a ransomware attack, with a mean market capital loss of $5.4 billion.[8]

Expense of downtime: A cyberattack not only incurs a financial cost for data recovery but also leads to prolonged system downtime, which hurts business. A data breach forces operations to halt and redirect all efforts to containing the breach and recovering from the attack. Downtime following an attack may cost nearly 50 times more than the ransom.[9]

Repercussions for CISOs: Chief information security officers, or CISOs, usually pay the price for being responsible for the safety of the organization's sensitive data. The legal pressure to combat and prevent ransomware threats is relentless. In 2016, Uber's former CISO was found guilty of not only hiding the data breach from the U.S. Federal Trade Commission (FTC) but a felony, after Uber admitted to paying $100,000 to cybercriminals.[10] In another example, the U.S. Securities and Exchange Commission (SEC) brought fraud and internal control failure charges against the CISO of SolarWinds following the SUNBURST (also known as Nobelium) attack.[11]

Business shutdown: Enterprises are sensitive to increasingly robust cyberattacks that exploit their sensitive data. As recently as 2019, an Arkansas-based telemarketing firm had to ask its 300 employees to find new jobs after IT recovery efforts were unsuccessful following a ransomware attack.[12]

Regulatory emphasis: In the U.S., the latest rules focus on the growing importance of reporting ransomware cases instantly. Regulatory bodies, such as the FTC and the Office of Foreign Assets Control (OFAC), strictly prohibit businesses from paying ransom to bad actors.

Ransomware's new game: Targeting identity for cyber reward

In the past, cybercriminals primarily directed their ransomware attacks at servers, applications or on-premises employees. In today's hybrid world, however, digital identities control access to everything. This has led to ransomware gangs specifically targeting digital identities and then quickly gaining access to other systems, applications and sensitive data within the organization. It's no surprise that nine out of 10 cyberattacks targeted Microsoft Active Directory, which is the core identity system for most organizations.[13]

Cyberattacks targeting identity systems include the following:

- **Phishing attacks:** Cybercriminals breach identity systems by deploying deceptive emails, messages or websites to trick individuals into sharing sensitive data like usernames and passwords.
- **Drive-by downloads:** Hackers develop malicious websites that automatically download and install malware on devices when individuals visit these sites, compromising their identity data.
- **Social engineering:** About 98% of cyberattacks happen due to social engineering.[14] Attackers manipulate individuals into disclosing confidential information willingly by building trust, posing as a trustworthy entity or leveraging psychological tactics to obtain login credentials or other sensitive data.
- **Supply chain threats:** Ransomware actors also target third-party vendors or supply chain providers within an organization. It helps them gain access to the identity systems of their target.
- **Weak authentication:** About 30% of users have experienced cyberthreats due to a weak password.[15] Ransomware often targets weak authentication practices. It forces attacks by systematically trying different password combinations or using credential stuffing by stealing login credentials from other breaches.
- **Outdated technology:** Outdated software with known vulnerabilities offers a free pass to cybercriminals who exploit this code to gain unauthorized access. They navigate through identity systems effortlessly, compromising sensitive information.

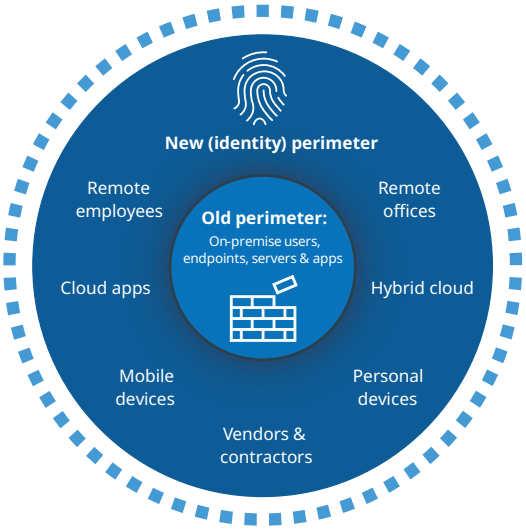


Figure 3: The old on-premises perimeter versus the new digital-identity perimeter

The impact across industries

Not only are ransomware attacks prevalent across industries, but over time, different ransomware groups have also specialized in exploiting vulnerabilities within a specific industry. Depending on the industry, the impact of a ransomware attack on identity systems that leads to a disruption in operations could have a debilitating impact on consumers and society at large.

Healthcare: Healthcare organizations don't always have a mature cybersecurity organization owing to the talent crunch. However, high volumes of patient data make them a prime target for ransomware attacks. These attacks can disrupt critical healthcare services, compromise patient privacy and even risk lives. It's important that healthcare firms partner with cybersecurity experts who can protect their identity infrastructure without adding friction to their customer engagement.

Success story

Swift response to a ransomware attack helps a healthcare provider shield its business from devasting impact

Business needs

- Immediately respond to and restrict the impact of a ransomware attack that originated from a phishing email and spread across most systems
- Recover and upgrade the provider's security posture to shield its Microsoft Active Directory environment, including 130 servers and 25 domain controllers (DC), from future ransomware attacks

Solution

Semperis' experts immediately shut down all risky access and conducted a thorough cleansing of the provider's AD environment.

- Initiate remedial measures like resetting tickets for network access and multiple resets of account passwords
- Identify a DC unimpacted by the ransomware attack to initiate recovery
- Deploy Semperis' Directory Services Protector (DSP) to help the healthcare firm gain an accurate and complete picture of the incident and its AD security stance
- Use the DSP to continue to scan and monitor the IT environment for AD misconfigurations and malicious changes made to AD and to automatically roll back those changes

Outcome

- Limits the damage of a ransomware attack on the AD infrastructure with immediate response and recovery
- Avoids serious reputational and financial impact on business
- Enhances the security posture to continuously monitor and protect the AD environment from the evolving threat of ransomware attacks

Manufacturing: In 2022, the U.S. experienced 250 data breach cases, affecting more than 23.9 million users within the manufacturing industry.[16] The manufacturing sector, with its legacy infrastructure and distributed networks, is often an easy target for identity-based ransomware attacks. Hackers can gain access to valuable intellectual property (IP) and trade secrets, product designs and manufacturing processes. This access causes significant financial losses and damages a company's competitive positioning. Manufacturers must strengthen their IT and operational technology security posture continuously. Doing so protects critical infrastructure against emerging threats and ensures minimum downtime if there is a breach.

Life sciences: The life sciences industry prioritizes investments in cybersecurity. However, it remains a lucrative target for identity-based ransomware attacks considering the sensitive nature of the data it maintains on clinical trials, IP and patient information. Also, a breach in a pharmaceutical or medical devices company can have a damaging impact on wider society. Life sciences companies should enhance security measures and be ready to mitigate and recover from a potential ransomware attack that targets identities.

Financial: Cyberattacks on financial institutions can lead to major losses, regulatory penalties and a decline in trust. Banks, insurance companies and other financial institutions already have stringent cybersecurity policies. However, these companies must continue to invest in keeping threat detection and response protocols ahead of the curve to safeguard customer data and maintain trust in the industry.

Education: Identity-based ransomware attacks in academic institutes can lead to the loss of sensitive student and staff information, disrupt online learning websites and apps, and compromise years of educational records. The education sector must invest heavily in cybersecurity infrastructure and train both staff and students about best practices to combat the risk of cyberattacks.

Success story

Global manufacturer protects its Active Directory from potential ransomware attacks

Business needs

- Provide ransomware protection for critical global infrastructure and an Active Directory environment with more than five domains
- Ensure faster recovery from security incidents

Solution

- Deploy Identity Threat Detection and Recovery Services powered by Semperis
- Identify an implementation roadmap, backed by complete visibility into the Active Directory infrastructure
- Leverage Active Directory Forest Recovery (ADFR) expertise to ensure seamless implementation in 6 months
- Adopt NTT DATA's Managed Services model for constant threat monitoring and response services

Outcome

- Delivers comprehensive Active Directory infrastructure protection with a recovery and rollback timeline of less than 6 hours

What steps can organizations take to strengthen their defenses against ransomware?

With ransomware attacks, it's not if, but when an organization will be targeted. How an organization prepares to monitor and protect against identity system attacks is as critical as its capability to recover from a breach. After all, if identity is compromised, then nothing else is secure anymore. Being able to roll back identity systems like Active Directory (AD) within hours instead of days or weeks will help organizations avoid irrevocable reputational damage. It also protects society and consumers who might otherwise be impacted by a prolonged interruption to essential digital services.

Organizations must focus on a holistic approach: deploying comprehensive ransomware threat monitoring and detection along with a recovery plan to limit the impact of a ransomware incident.

Be prepared to defend against potential ransomware attacks:

- Conduct training programs for users to recognize phishing and social engineering and be aware of safe online practices. This knowledge is the first line of defense, as cyberattacks can escalate privileges gained through phishing to seize control of privileged accounts.
- Regularly back up critical identity data and systems on an immutable storage to provide quick recovery without paying the ransom.
- Conduct a comprehensive identity system vulnerability assessment to identify and address security vulnerabilities. These include risky misconfigurations, unpatched flaws and indicators of exposure, such as expired passwords and elevated admin privileges.
- Implement continuous monitoring of the identity system to flag unwanted changes — both operational errors and potential malicious activity.
- Make sure the identity system backup is decoupled from the operating system to avoid malware infecting the backup.
- Regularly conduct identity system recovery drills to document recovery time objectives.
- Define a robust recovery plan that factors in all scenarios and has a clear communications plan. It should also mobilize a core team that knows how to collaborate with extended teams as required; make sure backup and provisioning hardware have not been compromised; begin the process of Active Directory Forest Recovery (ADFR); and establish renewed policies, credentials and trust in identity systems.
- Implement an automated recovery solution that not only backs up the identity system but also automates the entire recovery process. In the case of Active Directory, for example, that process includes tasks such as rebuilding the Global Catalog, provisioning new hardware to virtual or physical machines and other steps involved in an AD cyber disaster.
- Use additional layers of authentication, such as biometrics or multifactor authentication, to fortify identity protection.
- Implement comprehensive identity system threat detection and response to flag malicious changes in the system. Doing so will also automatically remediate risky changes that often move too fast for human intervention.
- Avoid relying solely on log- or event-based monitoring systems, as sophisticated attacks such as DCShadow can evade those solutions.
- Conduct regular assessments to keep all systems and software up to date with advanced security patches to address known vulnerabilities.
- Execute the principle of least privilege to restrict access rights and limit damage in case of a cyberattack.
- Split networks to mitigate the risk of ransomware and minimize the impact on critical systems.

Respond to a ransomware attack:

- Activate an incident response plan to contain the attack, isolate affected systems and minimize further damage.
- Establish clear communication channels to inform relevant stakeholders and plan actions.
- Make sure the identity system monitoring system can detect attacks that bypass traditional log- or event-based monitoring systems such as SIEMs.
- Make sure the monitoring system can capture malicious changes even if security logging is turned off, logs are deleted, agents are disabled or stop working, or changes are injected directly into AD.
- Implement change tracking across the hybrid identity system — including on-premises AD and Entra ID, for example — to catch attacks that start in the cloud and move to the on-premises environment or vice versa.
- Deploy a monitoring system with a hybrid-identities view to make sure malicious changes across on-premises AD and Entra ID are tracked.
- Implement automatic rollback of malicious changes to respond to attacks that move too fast for human intervention.
- Identify and isolate malicious changes to support Digital Forensics and Incident Response operations.
- Integrate identity system security data with a SIEM solution.

Recover from a ransomware attack:

- Activate the recovery plan defined during the ransomware preparation phase; restore the AD instance in the shortest possible time to avoid business disruption or paying ransoms; and establish renewed policies, credentials and trust in identity systems.
- Conduct regular ADFR drills to validate recovery time objectives and troubleshoot risky vulnerabilities in the recovery plan.
- Reduce downtime by deploying an ADFR solution that automates the complex and time-consuming process of restoring AD to a malware-free state.
- Make sure the identity system backup can be restored to any hardware, virtual or physical, to reduce provisioning time during the chaotic incident response scenario.
- Speed recovery by using an automated recovery solution that uses a small AD backup decoupled from the operating system to avoid malware reinfection upon restore.
- Implement post-breach forensics analysis tools to close backdoors and eliminate persistence.

Conclusion

In today's digital world, everything starts with an identity. And if the identity infrastructure itself is infiltrated, then there will be a cascading effect on the rest of the enterprise — impacting the security and reputation of an organization while disrupting critical infrastructures. Organizations must adopt a proactive, multilayered approach to minimize the risk and impact of ransomware attacks while providing the fastest recovery of critical identity infrastructure to minimize business disruptions.

Let's get started

Our end-to-end Identity Threat Detection and Response (ITDR) services and solutions use the industry's most comprehensive Active Directory protection from Semperis. ITDR not only proactively protects an organization's AD deployment but also guarantees full recovery in a matter of hours in case of a ransomware incident.

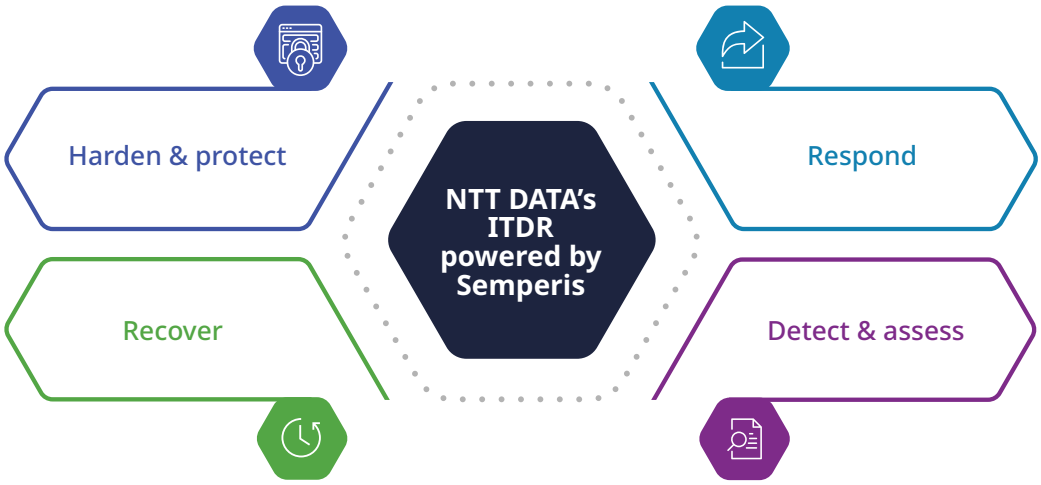


Figure 4: NTT DATA's Identity Threat Detection and Response services (ITDR)

With ITDR from NTT DATA, you get:

- **Advisory Services**
  - Conduct a comprehensive review of the organization's privilege access, digital identity security posture and disaster recovery (DR) readiness of hybrid identity infrastructure
  - Design a high-level roadmap for gap remediation with Semperis products
- **Implementation Services**
  - ADFR implementation
  - DSP implementation
  - Recovery for Azure AD
  - Extending DSP to Azure AD
- **Managed Services**
  - Make sure threat monitoring and remediation using Semperis products runs efficiently
  - Regularly assess DR services effectiveness to recover digital identity infrastructure
  - Provide audit support for external and internal compliance requirements
- **Optional features**
  - Onboarding new forest, domain and tenants, in addition to the existing identity infrastructure
  - On-demand disaster recovery services
  - Provide SIEM services or integrate with existing SIEM
  - On-demand assessment of the end-user experience within the protected environment

See what NTT DATA can do for you

As a trusted global cybersecurity services provider, we seamlessly integrate ITDR services with unified managed detection and response services to enhance our clients' overall security posture and minimize cyber risk across their organizations. Get in touch with our cybersecurity experts to assess your security posture and shield your business performance against threat actors.

Sources

1. Statista. “In 2023, nearly 73% of companies worldwide paid ransom to recover data.” https://www.statista.com/statistics/700894/global-ransom-payers-recovered-data/
2. CyberReason. “Ransomware: The True Cost to Business 2024.” https://www.cybereason.com/ransomware-the-true-cost-to-business-2024
3. Carly Page. “MOVEit, the biggest hack of the year, by the numbers.” TechCrunch. August 25, 2023. https://techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers/
4. Steve Morgan. “Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031.” CyberCrime Magazine. July 7, 2023. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/
5. Marcus Law. “Changing security needs for the hybrid network.” Cyber Magazine. July 6, 2023. https://cybermagazine.com/articles/changing-security-needs-for-the-hybrid-network
6. Danny Palmer. “Three billion phishing emails are sent every day. But one change could make life much harder for scammers. ZDNet. March 23, 2021. https://www.zdnet.com/article/three-billion-phishing-emails-are-sent-every-day-but-one-change-could-make-life-much-harder-for-scammers/
7. Statista. “Global firm targeted by ransomware 2023.” https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/
8. Keman Huang, Xiaoqing Wang, William Wei and Stuart Madnick. “The Devastating Business Impacts of a Cyber Breach.” Harvard Business Review. May 4, 2023. https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach
9. Stu Sjouwerman. “Seven Factors Analyzing Ransomware’s Cost To Business.” Forbes. July 29, 2021. https://www.forbes.com/sites/forbestechcouncil/2021/07/29/seven-factors-analyzing-ransomwares-cost-to-business/?sh=135fa60d2e98
10. Rachelle Blair-Frasier. “Security leaders chime in after ex-Uber security chief is sentenced.” Security Magazine. May 11, 2023. https://www.securitymagazine.com/articles/99338-security-leaders-chime-in-after-ex-uber-security-chief-is-sentenced
11. U.S. Securities and Exchange Commission. “SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures.” October 30, 2023. https://www.sec.gov/news/press-release/2023-227
12. Filip TRUȚĂ. “Ransomware-stricken firm tells laid-off employees to seek new jobs amid stymied recovery efforts.” Bitdefender. January 6, 2020. https://www.bitdefender.com/blog/hotforsecurity/ransomware-stricken-firm-tells-laid-off-employees-to-seek-new-jobs-amid-stymied-recovery-efforts/
13. Swetha Krishnamoorthi and Jarad Carleton. “Active Directory holds the keys to your kingdom, but is it secure?” Frost & Sullivan. March 20, 2020. https://www.frost.com/frost-perspectives/active-directory-holds-the-keys-to-your-kingdom-but-is-it-secure/
14. Catherine Reed. “30 Social Engineering Statistics – 2023.” Firewall Times. September 18, 2023. https://firewalltimes.com/social-engineering-statistics/
15. Help Net Security. “30% of online users suffered security breaches due to weak passwords.” December 10, 2021. https://www.helpnetsecurity.com/2021/12/10/poor-password-practices/
16. Statista. “Number of data compromises in manufacturing industry U.S. 2022.” https://www.statista.com/statistics/1367262/us-annual-number-of-data-compromises-in-manufacturing/

Visit us.nttdata.com to learn more.

NTT DATA is a trusted global innovator of business and technology services, helping clients innovate, optimize and transform for success. As a Global Top Employer, we have diverse experts in more than 50 countries and a robust partner ecosystem.
NTT DATA is part of NTT Group.