RICOH
imagine. change.

Cybersecurity | Article

5 Facts About Ransomware—'Ware' Do We Begin?

The true test of security lies in the strength of its weakest link. No matter how robust other security measures are, if one part is vulnerable, the entire cybersecurity ecosystem is at risk.

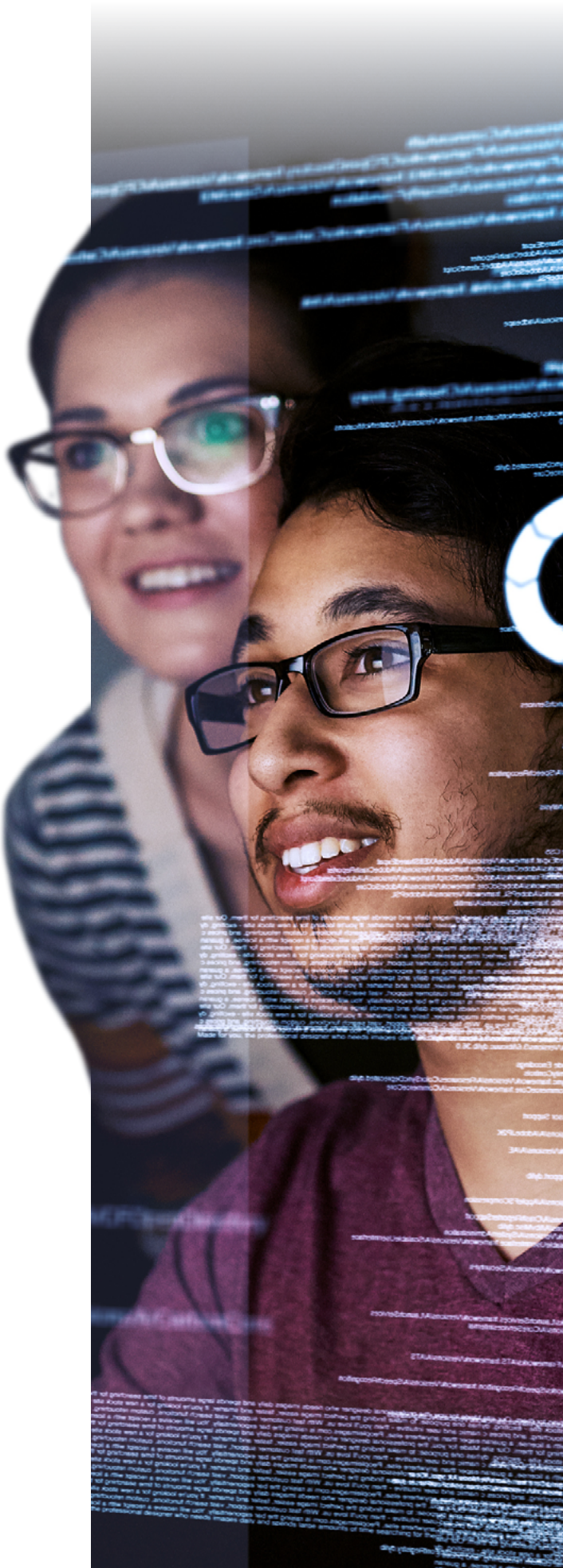
In today's rapidly changing cybersecurity world, there is hardly any room for error.

> Ransomware will cost its victims more around $265 billion (USD) annually by 2031.[1]

Enhanced levels of sophistication in attacks, from double-extortion to ransomware-as-a-service, have made ransomware threats and their threat actors more dangerous than ever. It's essential for businesses to gain clarity in understanding ransomware—its mode of operation, how to prevent it, and how to effectively safeguard operations from it. With a deep foundational understanding of ransomware, you can take steps to secure business continuity for your organisation and achieve enhanced compliance and security.

Uncover five facts about ransomware and have the upper hand in managing emerging threats and proactively protecting your systems and data.

[1]Braue, D. (2022). Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031. Cybersecurity Ventures.



Fact #1 Go beyond minimising risk at the initial intrusion point

Security strategies tend to rely on penetration testing and phishing training for employees to keep the business safe. These are undoubtedly crucial factors in a security plan, but it leaves out the next phase of damage control—when an attacker finds an avenue to enter. The next steps after a breach are just as important, if not more so. Otherwise, your digital platform stands at risk of significant compromise and irreparable damage.

What you can do

You can push for proactive solutions and roll out initiatives like real-time monitoring with machine learning in the background. This may seem like a regular security practice, but it makes a world of change in ransomware prevention. A holistic view of a digital environment and the ongoing actions within its systems are vital in assessing, identifying, and stopping attacks.

Fact #2 A basic oversight? A threat overnight

> Improving and maintaining IT infrastructure security is a significant priority for organisations as they tackle rising threats, particularly to endpoint devices in the new hybrid work environment.[2]

In the cybersecurity world, the assumption that all cyberattacks are inherently advanced and complex is frequently met with scepticism, mainly due to the lack of concrete evidence to support such claims. However, since most companies operate with inadequate cybersecurity frameworks, cybercriminals do not necessarily face significant hurdles in penetrating their systems.

Two weak links fuel the persistent aggression and success of cyberattacks—workforce shortage and high turnover rates. According to the 2021-2023 Emerging Technology Roadmap for Large Enterprises (Gartner, 2021)[2], as organisations face increasing threats, particularly to endpoint devices in the new hybrid environment, enhancing and preserving IT infrastructure security has become a crucial priority.

What you can do

You can better manage your risks toward ransomware by:

- Ensuring that your software is up-to-date and data back-ups are regularly done
- Providing sufficient and continuous training to ensure that your employees can identify and avoid phishing emails and other social engineering attack modes often used in ransomware.

[2]2021-2023 Emerging Technology Roadmap for Large Enterprises (2021). Gartner.

Fact #3 Steps for proactive maintenance of digital security

50%

50% of respondents say their organisations are wasting limited budgets on investments that don't improve their cybersecurity posture.[3]

Cybersecurity is a critical issue in today's world. With the increasing reliance on digital systems and networks, it becomes essential for organisations to protect their data from threat actors. However, many companies are unable to fund cybersecurity efforts adequately due to limited budgets; funding tends to focus on systems and solutions instead.

Antiviruses are not enough to provide appropriate protection against cyber threats. This can leave organisations vulnerable to attackers that seek out weaknesses they can exploit, using techniques like ransomware, advanced malware, and phishing attacks.

What you can do

To combat cyber threats, organisations have to think beyond prevention and take extra steps to secure their systems. These include:

- Ensuring all systems are patched regularly with the latest security updates, addressing any vulnerabilities before attackers exploit them
- Educating users about cybersecurity best practices, such as implementing strong passwords and two-factor authentication
- Investing in solutions like firewalls and encryption protocols to give additional layers of protection against potential breaches or intrusions.

With these measures, you can better protect your business and customers from potential threats and keep them safe.

[3]The Economic Value of Prevention in the Cybersecurity Lifecycle (2020). Ponemon Institute.

Fact #4 The unshakable silence about ransomware attacks

We only hear about ransomware attacks through headlines. The most telling details of the attack itself, from the breach to lateral movement to extortion (and even the ransom payment), are relatively unknown, save for a select number of key people like the insurer and incident response specialist. This leaves out crucial information other businesses could learn and improve from, like the methods and mode of exploits used. It is, therefore, difficult to understand and decipher the exact plan of attack and the latest techniques applied.

What you can do

One alternative that can give you a better picture of ransomware threats and tactics is by staying updated through cybersecurity industry publications, attending webinars or conferences, and participating in information-sharing groups. In doing so, you can take the necessary precautions to protect your business and prevent reputational damage and financial costs.

Fact #5 Zero trust—the only trust you can count on

The zero trust mindset in cybersecurity assumes that no one can be trusted and everything must be verified before granting access. This offers many benefits, including the ability to give the right access and tools to the right people, limiting lateral movement in the event of a compromise, better visibility into network activity, and enhanced compliance.

By treating each network resource as an independent entity, the zero trust approach makes it difficult for hackers to move laterally and cause widespread damage.

What you can do

By following Zero Trust principles and deploying Zero Trust security solutions and Secure Access Service Edge (SASE), you can ensure better protection for access across multiple applications, data, tools, and resources.

The Four Steps of a Ransomware Attack

1

A hacker scans the network for computer resources.

2

They attempt to break into the Active Directory using stolen credentials.

3

The hacker will create an admin or superuser account, which grants them access to a computer's databases and systems.

4

They can now duplicate and download sensitive information, destroy and encrypt data, and demand a ransom for the stolen data.

It is vital to adopt a culture of 'security by design' in your cybersecurity framework to limit the risk of your network being infiltrated. This is because the culture takes a proactive, pragmatic, and strategic approach in dealing with risk and security, which improves your overall posture in facing evolving digital threats.

Ready to Deploy Ricoh Cybersecurity Solutions?

With the right approach, mindset, and tools, you will be able to manage risk better. In this ever-changing digital landscape, it is necessary to have the right cybersecurity solution provider by your side. Ricoh's cybersecurity solutions, combined with our curated partnership with leading cybersecurity specialists, can give you the confidence to do business while we help protect your organisation from threats.

Talk to us today about Ricoh's cybersecurity offerings. Our key benefits include:

- Ransomware mitigation, which reduces the risk of reputation damage and business showdown
- Helping operations continue despite an attack
- Reducing visibility to ransomware attackers
- Enhancing your IT security posture
- Adding rigour to your IT compliance practice
- Round the clock expert cybersecurity support.

Discover how **Ricoh's Cybersecurity Solutions** can help you strengthen your defenses, ensure compliance, and protect your business digitally.

About RICOH

Ricoh is empowering digital workplaces by utilising innovative partners and technologies and providing expert services that enable individuals to work smarter from anywhere. With cultivated knowledge and organisational capabilities nurtured over its 85-year history, Ricoh is a leading provider of digital services, process automation, and information management solutions designed to support digital transformation and optimise business performance.

Learn more about our Cybersecurity solutions at **ricoh-ap.com**

RICOH
imagine. change.