Simplifying Ransomware

T Systems

Let's power
higher performance

What’s a Ransomware attack?

Imagine that a hacker has gotten access to one of your folders on your computer. Now the hacker has locked this folder, and you can no longer access it.

To allow you to access the folder, the hacker demands money (ransom). Unless you pay the ransom to the hacker, the folder remains inaccessible. This type of cyber attack is known as a Ransomware attack.

It’s like holding your stuff hostage until you pay them.
It‘s a serious problem because it can make your computer unusable and can be very costly and frustrating to fix.

Data Exfiltration: Ransomware can also be a spy. It sneaks into your computer, steals your private data (like photos, documents, or passwords), and threatens to expose it unless you pay.

DDoS Attacks: Additionally, some ransomware can act like a bully by overloading websites with too much traffic, causing them to crash. They might demand a ransom to stop the attack.

The unfolding of Ransomware

Hackers trick people into downloading malicious software on their computers. For instance, hackers may send phishing emails that bait people to click and download an attachment.

As soon as this attachment is clicked/opened, the ransomware gets downloaded to the computer. Once it's downloaded, ransomware starts locking (encrypting) the files – making them inaccessible to the user.

Once the files are encrypted, the demand for ransom is communicated by the hacker.

It need not always be a phishing email. You may be lured to visit a fake website that allows your computer to get infected by ransomware. There's a possibility that your system has some existing software vulnerability, which hackers exploit to send ransomware to your computer.

A simple Ransomware attack

Baiting: Baiting a person through phishing attempts, etc.

Infection: Ransomware is downloaded unknowingly and starts infecting.

Encryption: Files start getting encrypted and inaccessible.

Ransom: Ransom demand is made to get the files unlocked/decrypted.

Modern-day advanced Ransomware attack

Campaign Planning: Hackers plan their attack, choosing who they want to target and how they‘ll trick them.

Bait: They create deceptive lures, like phishing emails or infected websites, to get victims to interact.

Injection: Once victims take the bait, the ransomware is introduced into their computer.

Lateral Movement: Ransomware spreads to other parts of the computer or network to lock more files.

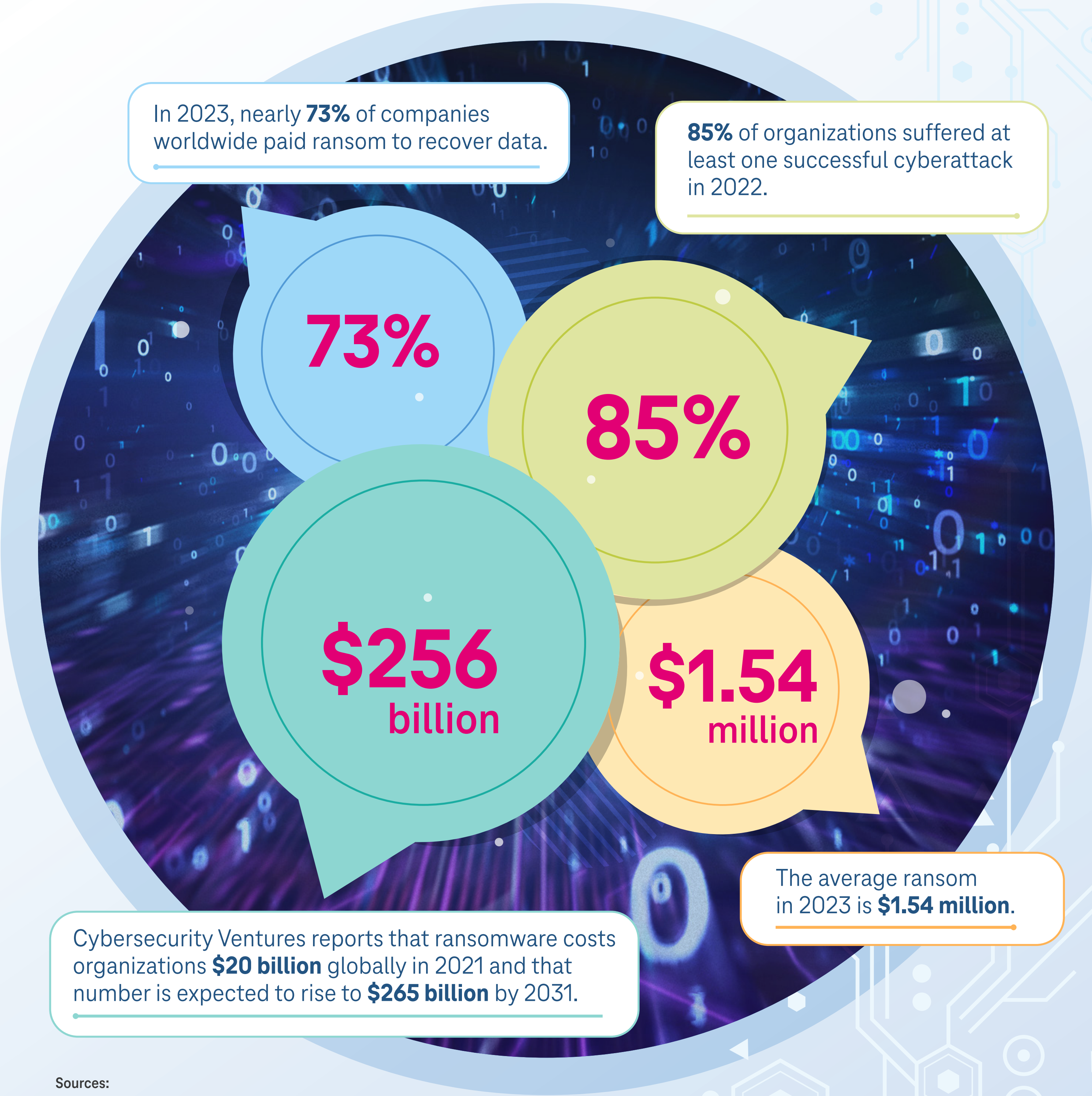
Infection: The ransomware encrypts (locks) the victim‘s files, making them inaccessible.

Extortion: Hackers demand a ransom from the victim in exchange for the key to unlock their files.

Insights on Ransomware

In 2023, nearly **73%** of companies worldwide paid ransom to recover data.

85% of organizations suffered at least one successful cyberattack in 2022.

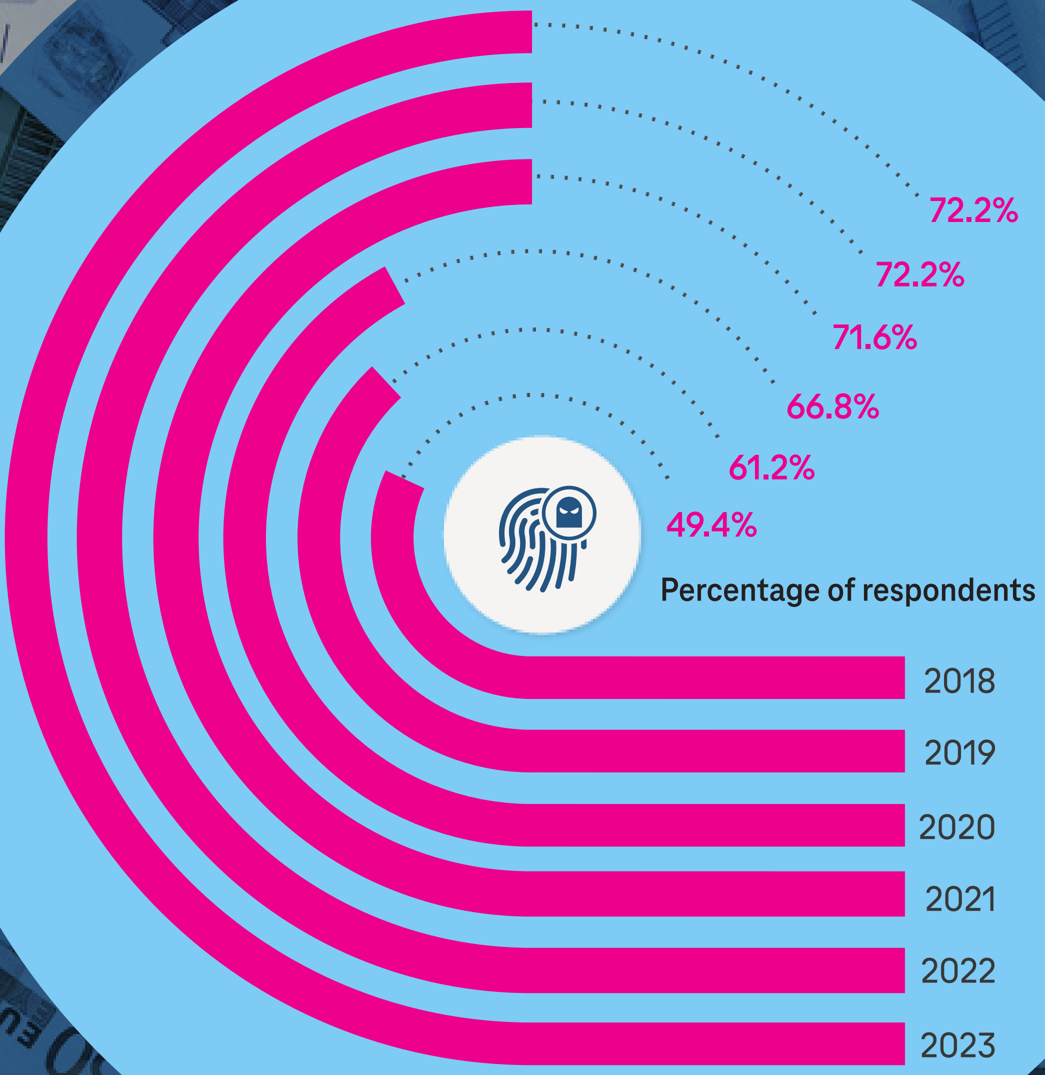


The average ransom in 2023 is **$1.54 million**.

Cybersecurity Ventures reports that ransomware costs organizations **$20 billion** globally in 2021 and that number is expected to rise to **$265 billion** by 2031.

Sources:
Cyberedge, Forbes, Statista, Sophos State of Ransomware

Annual share of companies globally that paid the ransom and recovered data from 2018 to 2023



Sources: Cyberedge, Forbes, Statista, Sophos State of Ransomware

Some infamous Ransomware attacks

1. Ryuk:

- Ryuk targeted large organizations and demanded $1 million ransom per target.
- In September 2020, it caused $67 million in damage to the Universal Health Service (UHS). Ryuk waits a couple of days after infiltrating a system before encrypting files and disabling Windows System Restore.

2. REvil (Sodinokibi):

- REvil was a Russia-based Ransomware-as-a-Service operation.
- In 2021, it focused on US companies and triggered a cybersecurity crackdown. Net losses were estimated at around $200 million.

3. TeslaCrypt:

- TeslaCrypt targeted gaming files, encrypting saved data, player profiles, custom maps, and game modifications.
- Victims were prompted to pay $500 to get the decryption key.

4. NotPetya:

- NotPetya used the EternalBlue hack to infect systems and was modified for irreversible encryption even if the ransom was paid.
- It was politically motivated and targeted against Ukraine, causing financial losses of $10 billion.

5. WannaCry:

- WannaCry used the EternalBlue exploit to infect thousands of computer systems across 150 countries.
- It demanded ransoms in Bitcoin and caused disruptions, including £92 million (approx. $104.36 million) in losses in the healthcare sector, affecting the NHS systems in England and Scotland.

> These Ransomware attacks have had significant financial and operational impacts on various organizations and sectors.

Sources: Cyber Magazine, Tech Target

Reacting to a Ransomware attack: 8 steps to consider

1. Isolate and Contain

Immediately isolate infected systems to prevent the malware from spreading within the network. Disconnect affected devices from the internet and the internal network.

2. Secure Backups

Ensure that your backups are secure and unaffected by the attack. Backups are crucial for data recovery without paying the ransom.

3. Assess the Situation

Determine the scope and impact of the attack. Identify the type of ransomware and the compromised data. This information will guide your response.

4. Communicate Internally and Externally

Inform internal stakeholders and law enforcement if necessary. Open lines of communication with Ransomware attackers are generally discouraged.

5. Mitigate the Attack

Take action to stop the ransomware from encrypting or stealing more data. This may involve applying patches, deploying security tools, or using decryption tools if available.

6. Decide on Payment (if necessary)

Organizations should generally avoid paying ransoms as they fund criminal activities. Evaluate the situation carefully and consider legal implications.

7. Recover and Restore

Once the threat is contained, restore affected systems from secure backups. Ensure the systems are clean of malware before bringing them back online.

8. Review and Improve

After the incident, conduct a post-attack review to identify vulnerabilities and weaknesses in your security posture. Implement necessary changes to prevent future attacks.

Handling a Ransomware attack requires a well-prepared and coordinated response to minimize the damage and recover as swiftly as possible.

To pay or not to pay?

Deciding whether to pay a ransom in a Ransomware attack is a complex and often controversial decision for organizations. Here's a general framework to consider:

1. Legal and Ethical Considerations

Evaluate the legal and ethical implications of paying a ransom. Some countries have laws against paying ransoms, and paying could support criminal activities.

2. Financial Impact

Weigh the financial cost of paying the ransom against the cost of recovery, downtime, and potential reputation damage. In some cases, paying may be more cost-effective.

3. Ransom Amount

Consider the ransom amount. Some attackers demand exorbitant sums, while others ask for more reasonable amounts. Negotiating with the attackers might be an option.

4. Reputation and Trust

Think about the impact on your organization's reputation. Paying a ransom can be seen negatively by customers and partners.

5. No Guarantee

Remember that paying does not guarantee data recovery or that the attackers won't return for more ransom.

6. Backup and Recovery

Evaluate your backup and recovery capabilities. If you have reliable backups and can restore your data without paying, that's a preferable option.

Defend against Ransomware with strong security

1. Backup Your Data

Regularly back up your important files on an external device or a secure cloud service. This way, you can restore your data if it's encrypted by ransomware.

2. Keep Software Updated

Install updates for your operating system and all software, including antivirus programs. These updates often include security fixes.

3. Be Cautious with Email

Don't open email attachments or click on links from unknown sources. Cybercriminals often use email to spread ransomware.

4. Use Strong Passwords

Create strong, unique passwords for your accounts and change them regularly. Consider using a password manager for added security.

5. Educate Employees

Train your staff to recognize phishing attempts and suspicious links. They should know how to stay safe online.

6. Firewall and Security Software

Use a firewall and reliable security software to block malicious websites and files.

7. Access Control

Limit access to important files and systems.
Not everyone needs full access, so restrict permissions.

8. Patching and Updating

Ensure all devices are updated with the latest security patches and updates. This closes vulnerabilities that ransomware might exploit.

9. Network Segmentation

Divide your network into segments, so that if ransomware enters one segment, it can‘t easily spread to the others.

10. Disaster Recovery Plan

Have a disaster recovery plan in place to respond quickly and effectively if a Ransomware attack occurs.

11. Cyber Insurance

Consider investing in cyber insurance. It can help cover the costs associated with a Ransomware attack, including recovery, legal, and reputation management expenses.

By following these measures, you can significantly reduce the risk of falling victim to a Ransomware attack and protect your important data.

Understanding Cyber Insurance

Cyber insurance is like a safety net for businesses. It helps protect them if they‘re hit by a cyberattack, like ransomware. Here‘s how it works:

What is Cyber Insurance?

It‘s an insurance policy that covers the costs when a business faces a cyberattack. This includes expenses for fixing the damage, recovering lost data, and dealing with legal and public relations issues.

How Does It Work?

When a business gets cyber insurance, they pay a premium (like a fee) to the insurance company. If a cyberattack happens, the insurance company helps pay for the recovery and damages. It‘s like having someone to support you in a tough situation.

What‘s Needed to Get Cyber Insurance?

To get cyber insurance, a business usually needs to show that it has good cybersecurity practices in place. This might include having strong security measures like password policies, antivirus software, endpoint protection, policy controls, employee awareness trainings, and more.

Cyber insurance is a way for businesses to prepare for the unexpected and get help when they need it most in the digital world.

Cyber insurers will assess your business by evaluating:

Insurers want to know if your business has strong security measures like password policies, antivirus software, endpoint protection, policy controls, employee awareness training, and more.

Data Protection

They‘ll ask how you store and protect customer data. Are you careful with sensitive information?

Employee Training

Insurers might check if your employees are trained to spot phishing and other online threats.

Incident Response Plan

Do you have a plan for what to do in case of a cyberattack? Having a strategy in place is important.

History

They may ask about past cyber incidents to understand your risk.

By answering these questions, insurers assess your cybersecurity readiness and determine the cost of your cyber insurance. It‘s like a safety check to make sure your business is prepared for online threats.

Get in touch with us

Andreas Pecka

Head of International Expert
Sales & Presales Cyber Security

T-Systems International GmbH

a.pecka@t-systems.com

in https://www.linkedin.com/in/andreas-pecka/

cyber.security@t-systems.com

T Systems

Let’s power
higher performance