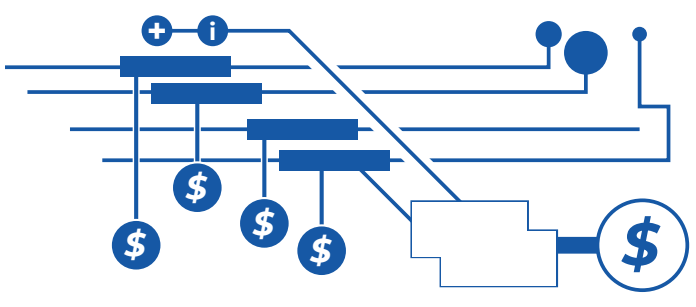
Nationwide®
is on your side

Guarding against and responding to ransomware attacks



Ransomware is a type of malicious software (malware) that infects a target's networks or systems, encrypts the data, and blocks access until a ransom is paid.

During a ransomware attack, a cybercriminal may disrupt a target's operations and block access to confidential files or sensitive information until the target pays a ransom. **Any business can be targeted in a ransomware attack,** resulting in significant downtime, lost or damaged data, reputational damage and large-scale financial losses.

In fact, ransomware is one of the costliest cyberattack methods, totaling an average of more than **$4.5 million in losses per incident** (not including the actual ransom payment). What's worse, growing cybercriminal sophistication and evolving attack techniques have caused ransomware incidents to skyrocket; over the past decade, these attacks have surged by more than 240%.

Fortunately, businesses can reduce the risk of ransomware attacks by strengthening their digital defenses and purchasing sufficient cyber coverage. This infographic outlines a ransomware attack scenario, offers suggestions to prevent such incidents and summarizes the associated cyber insurance claims process.

Ransomware attack scenario

While specific ransomware attack methods can vary, these incidents often follow the same overall layout. Here are the steps in a general ransomware attack scenario:

Finding an entry point

In order for a cybercriminal to compromise a target's networks or systems, they must first infiltrate this technology by finding an attack entry point. This may entail exploiting software vulnerabilities, leveraging phishing scams (e.g., convincing staff to download malware via deceptive emails) or implementing other social engineering tactics to steal employees' credentials.

Launching the attack

After infiltrating the target's networks or systems, the cybercriminal will infect this technology with malware, often bringing the affected company's operations to a halt and restricting access to critical files or information. Next, the cybercriminal usually delivers a warning message, ordering the target to issue a payment in exchange for restoration; yet, the particular terms of the ransom demand will depend on the type of ransomware being used. Common forms of ransomware include the following:

Locker ransomware—As this ransomware physically locks the target out of their networks or systems, it requires them to make a payment in order to access their technology. In the meantime, the target is only able to view a lock screen containing the ransom demand.

Encrypting ransomware—This ransomware encrypts the target's sensitive records, prompting them to issue a payment before getting the keys to decrypt their data and threatening to delete this information permanently if the ransom deadline passes.

Leakware—Such ransomware follows the same framework as encrypting ransomware; however, instead of the target being threatened by data loss, they are warned that this information will be released publicly in the absence of payment.

Destructive ransomware—While this ransomware also mirrors the formula of encrypting ransomware, data restoration is not guaranteed. That is, even after the target pays the ransom, their information may still be deleted, compounding their total losses.

Mobile ransomware—Such ransomware can only be deployed on the target's mobile devices (e.g., smartphones or tablets), generally through the use of a malware-ridden application. From there, this ransomware operates similarly to locker ransomware.

Scareware—Relying on various scare tactics, this ransomware manipulates the target into issuing a payment through seemingly legitimate prompts, such as a fake computer virus alert urging the target to purchase new software to better safeguard their technology.

Prevention tips

Businesses should consider implementing the following cybersecurity measures to help enhance their digital defenses and minimize ransomware attacks:

- Equip company systems with **adequate security features** (e.g., antivirus programs, virtual private networks, firewalls, email authentication technology, endpoint detection and response solutions, and patch management software), and upgrade these features when necessary.
- Provide **routine training** to educate employees on how to detect and respond to common ransomware attack scenarios.
- Leverage **access control policies** (e.g., the principle of least privilege and multifactor authentication) to confirm employees only utilize the technology and information needed to perform their jobs.
- **Segment all company networks** to better identify suspicious activity and prevent cybercriminals from being able to move laterally across these networks and cause widespread damage or disruptions amid ransomware attacks.
- **Back up critical data** to secure locations on regular schedules and establish data recovery procedures to ensure swift restoration amid possible attacks.
- Develop a **cyber incident response plan** that outlines steps to promote timely remediation and keep losses to a minimum when ransomware attacks arise.
- Work with IT experts, legal counsel and insurance professionals to **update cybersecurity measures** and make coverage adjustments as needed.

The claims process

If a business falls victim to a ransomware attack, cyber insurance can make all the difference in helping to limit the financial fallout and bolster its recovery capabilities. Here's an outline of the claims process that a company may follow when it experiences a ransomware incident:

Validation and plan execution—As soon as a ransomware attack has been detected or reported, the business should assess the alert to confirm that it's a genuine threat. Upon validation, the company should execute its cyber incident response plan to help limit associated losses and contact necessary parties, such as the cyber insurer, legal counsel and law enforcement, to decide the next steps.

Collaboration with experts—Once the cyber incident response plan is in action, the company's cyber insurer will likely put the business in contact with preapproved third-party IT experts, forensic specialists, breach counsel and cyber extortion case managers. Together with legal counsel and law enforcement, these experts will help the business investigate the attack, negotiate the ransom demand and ensure timely restoration.

Notification and reporting—After remediating the attack, the previously mentioned experts will assist the business in reviewing the damage and determining whether the company is required under applicable data breach notification laws to inform the government, stakeholders or other impacted individuals that sensitive information was compromised amid the incident. At this time, the business should also file a claim with its cyber insurer and provide a detailed report outlining the attack, supplemental evidence, related losses and all mitigation measures taken.

Evaluation and resolution—With essential attack details and documentation in hand, the cyber insurer will conduct an in-depth analysis to evaluate the associated claim. This entails assessing the extent and validity of the claim based on applicable policy terms and conditions, as well as determining specific coverage capabilities. During this process, the business should foster open communication and collaboration with the cyber insurer, providing additional information and addressing any questions or concerns to help reach the best possible claim resolution.

Conclusion

As ransomware attacks continue to rise, businesses can't afford to ignore the need for proper risk mitigation measures and cyber insurance. By implementing effective prevention tactics and coverage solutions, businesses can minimize their exposures and limit large-scale losses.

This document is a general overview and doesn't replace the need to consult cybersecurity experts and legal counsel for tailored guidance. Click here for more information on Nationwide's cyber risk management solutions and insurance offerings.

1 https://www.ibm.com/topics/ransomware
2 https://www.iafci.org/app_themes/docs/Federal%20Agency/2022_IC3Report.pdf
3 https://www.cisa.gov/sites/default/files/2021-01/NCIJTF%20Ransomware_Fact_Sheet.pdf
4 https://www.cisa.gov/stopransomware/ransomware-faqs