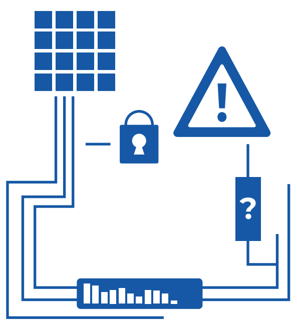
Nationwide®
is on your side

9 Steps to Take in Response to a Cyberattack

As cyberattacks continue to rise in cost and frequency across industry lines, it's important for your business to be prepared to handle these incidents as quickly as possible and minimize related losses. After all, it doesn't take long for cyberthreats to cause significant damage and destruction. With this in mind, it's clear that your business can't afford to waste any time when a cyber incident strikes. Here are nine steps to take if you suspect a potential cyberthreat or attack:[1,2]

1 Know the signs.



First, it's crucial for you and your employees to understand common indicators of a cyber incident. Knowing these signs will ensure timely detection and allow for a fast response. Key indicators of a cyberthreat or attack include unauthorized access attempts within company networks; unexplained system slowdowns; unexpected changes in online traffic on organizational platforms or services; the presence of unknown code, files or software on workplace devices; and any other unusual system activity or behavior.

2 Isolate the threat.

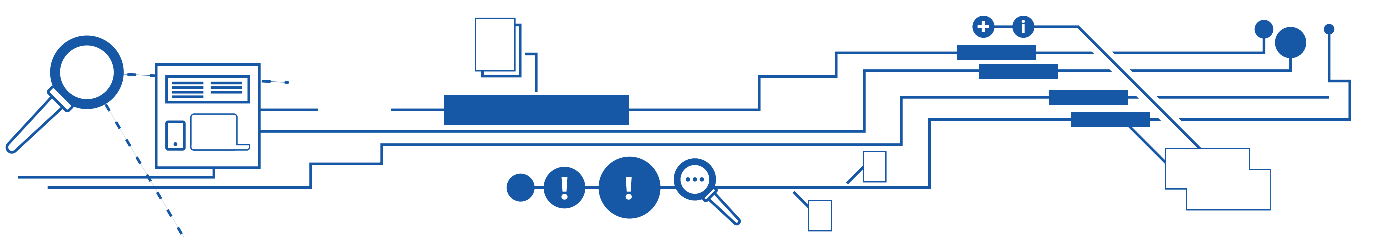
Upon confirmation of a cyberthreat or attack, focus on isolation to prevent the incident from causing widespread disruption and associated losses. This generally entails identifying compromised devices and systems and promptly disconnecting them from organizational networks.

3 Assess the impact.

The next step is to evaluate the impact of the incident. In particular, by reviewing compromised devices and systems, you can better determine the overall scope and severity of the incident as well as analyze any ongoing risks and potential for additional damage.

4 Engage your response team.

Considering the impact of the cyberthreat or attack, it's best to mobilize your company's incident response team. This team should consist of trusted personnel across different organizational levels and departments who are capable of executing continuity plans and limiting further losses amid the incident. Each member of the incident response team should have designated responsibilities to uphold during a cyberthreat or attack.



5 Gather evidence.

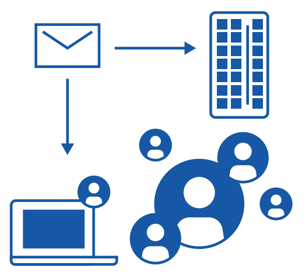
It's critical to document all relevant details regarding the cyberthreat or attack and preserve key evidence. This may include system reports, organizational device logs and network traffic data. Such documentation and evidence can help your business identify the source of the incident and better explain the situation to other appliable parties.

6 Mitigate additional damage.

The next step is to reduce the likelihood of any further destruction from the incident and prevent subsequent attacks. Mitigation measures may involve scanning systems for software vulnerabilities and deploying patches, enhancing network controls and restricting employees from accessing technology or data that isn't essential to their roles, and implementing additional user authentication measures.

7 Notify affected parties

Depending on the impact of the cyberthreat or attack and applicable data privacy laws, your business may need to inform parties affected by the incident. Commonly impacted parties include customers, investors, vendors, employees and other stakeholders. Be sure to provide clear and accurate details to these parties and offer additional resources (e.g., call centers, credit monitoring services and government guidance) to help them protect against any associated cybersecurity concerns.



8 Remediate and recover.

Following a cyberattack, it is important for your business to focus on remediating and recovering from the attack. This may entail restoring affected systems, networks and devices, as well as conducting a thorough post-incident assessment to determine vulnerabilities that led to the attack and how to avoid similar scenarios in the future. By performing this assessment, your company can also evaluate the effectiveness of existing cybersecurity measures and identify areas in need of improvement.

9 Enhance cybersecurity measures.

The final step is to adjust your organizational cybersecurity policies and procedures based on the results of your company's post-incident assessment. This may involve upgrading or introducing new software solutions, revising incident response plans and improving overall digital hygiene practices. Employees should be trained on these adjustments and provided with any other relevant information on protecting against the latest cyberthreats.

Remember, your business is not alone in the event of a cyber incident.

It is vital to contact your cybersecurity partners as soon as possible, including your insurance broker, your insurance company and other professionals, such as attorneys and data breach response partners. Doing so will ensure that your organization has access to the guidance it needs and that further damage is limited.

Time is of the essence when it comes to handling a cyberthreat or attack. By following these steps, your business can swiftly detect and respond to potential incidents, thus keeping related damage to a minimum and deterring future attacks.

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://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
[2] https://www.cisa.gov/shields-guidance-organizations

Nationwide®

The information contained in this page is intended for general informational purposes only and is not intended to provide legal or other expert advice. You should consult knowledgeable legal counsel or other knowledgeable experts as to any legal or technical questions you may have. Neither Nationwide nor its employees or agents shall be liable for the use of any information or statements made or contained in any information provided herein. This document may contain third-party websites solely for informational purposes and as a convenience to readers, but not as an endorsement by Nationwide of the entities referenced or the contents on such third-party websites. Nationwide is not responsible for the content of linked third-party websites and does not make any representations regarding the content or accuracy of materials on such linked websites. The opinions and positions expressed in this report are the authors' own and not necessarily of Nationwide.

Products, coverages, discounts, insurance terms, definitions and other descriptions are intended for informational purposes only and do not in any way replace or modify the definitions and information contained in individual insurance contracts, policies, and/or declarations pages from Nationwide-affiliated underwriting companies, which are con-trolling. Such products, coverages, terms and discounts may vary by state, and exclusions may apply. Products are underwritten by Nationwide Mutual Insurance Company and affiliated companies, Columbus, Ohio, and are subject to underwriting guidelines, review and approval. Availability varies by state. Nationwide, the Nationwide N and Eagle and Nationwide is on your side are service marks of Nationwide Mutual Insurance Company.