



The essential incident response checklist: 21 steps to navigating a cyber attack

Leave a Comment / Security / By Jason Buckley

Preparation is important. In today's business world, cybersecurity attacks have become commonplace. According to a University of Maryland study, a hacker attack happens every 39 seconds. If you don't prepare your business for a security breach, the consequences could be costly—think reputation damage, downtime, and potential legal issues. For these reasons, an incident response checklist is critical. Not only can it save you headaches, it may also be your best business investment this year, as it can help you scale your business and cut costs.

The phases involved in creating your incident response checklist

So how do you prepare a cyber incident response checklist? There are six phases that make up any good plan: preparation, identification, containment, eradication, recovery, and review. Within them are 21 steps that can ready your business for a cyber attack. Below is a walkthrough of each phase and step to help you create your own incident handling checklist.

Preparation

The preparation phase sets the stage for all the others, and it's vital for the successful handling of security incidents. Here are some key actions to take to help you prepare:

- 1. Define the term 'security incident' for your organization** – Doing so ensures you will know when a breach occurs.
- 2. Assign roles and establish who's in charge** – From your HR Manager to your CIO, every one should know their role and the actions to take. Choose one employee to be the leader who will navigate your team through the breach.
- 3. Create your emergency IR kit** – This is similar to an emergency preparedness kit for an earthquake, tornado, or another natural disaster—but for IT. It should contain an incident response journal or tablet, the contact details of all IR team members, USB drives, a laptop, software to repair file systems, and everything you need to contain, eradicate, and recover from the incident.
- 4. Find a backup means of communication** – In case your main phone line or other communication devices are compromised.
- 5. Prepare public relations statements** – You may need to contact clients, partners, or vendors ASAP if you're breached, so it's wise to prepare a statement beforehand when stress levels are low.

Identification

When a security breach happens, you need to understand exactly what you're dealing with. Here's how to do that:

- 6. Confirm it's a real incident** – And not a false alarm, technical glitch, or employee mistake.
- 7. Investigate the breach** – Collect as many details about the incident as possible. Who discovered it, when did it happen and where? Also, try to understand how the breach will affect business operations.

Containment

The goal in this phase is to isolate the incident, prevent further damage, and contact the appropriate parties. Here are some important actions to take:

- 8. Isolate the incident** – Identify which systems and/or devices must be isolated to contain the breach.
- 9. Determine the damage of the affected systems** – And note if any sensitive data has been compromised.
- 10. Utilize your backups (if necessary)** – If you need to access your data and the breach has made it unavailable, restore it now using your backup.
- 11. Get in touch with your legal team** – Determine if the breach has impacted any regulations.
- 12. Consider contacting authorities** – Law enforcement may be able to help you resolve your issue faster and, depending on your country and industry, you may be legally required to contact authorities.

Eradication

In this phase, the goal is to exterminate risks and collect evidence. Keep these three points in mind:

- 13. Eliminate the security risk** – Patch your systems, close network access, reconfigure applications, reset passwords, and do everything to block and prevent further attacks.
- 14. Rebuild systems** – That couldn't be cleaned or are damaged beyond repair.
- 15. Collect forensic data** – This can be used for insurance purposes or may be needed for submission to authorities.

Recovery

Now that the threat is gone, it's time to return your business's operations to normal. Here's how to do that:

- 16. Restore systems from backups** – If you haven't done so already, do it now. Then continue with your normal backup routine to be ready for future incidents.
- 17. Ensure the integrity of your systems** – Make sure they're available, working properly, and that your confidential data is protected.
- 18. Tighten your security** – Once a system has been attacked, it's more likely to happen again. Prepare your business by improving your security measures and training.

Review

To protect your network from future breaches, it's best to learn what caused your current one. So take some time to review and reflect on the incident, documenting these key points:

- 19. Identify what went well and what didn't** – The first step to preventing future breaches is to review the incident. What holes in your systems, staff training, or processes did the breach point out? Identify the deficiencies that led to the breach.
- 20. Plan for how you can improve in the future** – Perhaps you need more advanced security, better training, or to hire a security expert or company.
- 21. Document what you learned** – Write up an incident response report which should include all the details from the event and proposed solutions to resolve any issues.

A security breach doesn't have to be a business disaster

While cybersecurity attacks are becoming more and more common, that doesn't mean you have to suffer the downtime, panic, and loss of morale that comes with a breach. Follow the steps above and you can prevent the worst-case scenario.

While you've now learned the essential points for an incident response plan, know there are other steps that can help streamline the process and provide further protection for your business. To learn more, [contact us today](#) to get in touch with one of our security experts.

← Previous Post

Leave a Comment

Your email address will not be published. Required fields are marked *

Type here..

Name* Email* Website

Save my name, email, and website in this browser for the next time I comment.

I'm not a robot reCAPTCHA Privacy - Terms

POST COMMENT »

Search...

Recent Posts

- [The essential incident response checklist: 21 steps to navigating a cyber attack](#)
- [Why an incident response plan may be your best business investment this year](#)
- [Why IT strategy is important for SMBs](#)
- [Understanding IT support costs: Is it worth investing in managed services?](#)
- [Five reasons to move to managed IT services](#)

Recent Comments

- Shammy Peterson on [How to ensure your practice benefits from telehealth](#)
- ICTechnology on [Understanding IT support costs: Is it worth investing in managed services?](#)
- globalmplus on [What is telehealth?](#)
- Chris Q on [Real world examples of security breaches from Las Vegas companies](#)

Archives

- [June 2021](#)
- [May 2021](#)
- [April 2021](#)
- [March 2021](#)
- [January 2021](#)
- [December 2020](#)
- [November 2020](#)
- [October 2020](#)
- [September 2020](#)
- [August 2020](#)

Categories

- [Business](#)
- [Healthcare](#)
- [Security](#)
- [Managed IT Services](#)
- [Security](#)

