HOW TO BUILD AN

INCIDENT RESPONSE PLAN

Set your business up for the best chance of survival

ShieldITNetworks

Shielditnetworks.com

PLANNING IS HALF THE BATTLE...

In today's volatile cybersecurity environment, it can often seem like there is a cyberattack waiting for your business around every corner. Threats like ransomware, business email compromise, spearphishing, and other more dangerous cyberattacks are all over the news. With cybercrime consistently on the rise, it's just a matter of time before your business ends up in a cybercriminal's sights.

That's why smart businesses have a plan and are prepared to respond to an incident at any time. Creating, drilling, and updating an incident response plan for cyberattacks is critical to making sure that your business survives the blow. It's also a key component of strengthening your company's cyber resilience to stand strong in the face of trouble. By ensuring that you've got everything in place to handle the worst, you'll ensure that your company's chance of recovery is the best it can possibly be.

How will your business benefit from an incident response plan?

RISK REDUCTION

Making, testing, and maintaining an incident response plan will reduce your company's chances of experiencing a damaging cybersecurity incident.

INCREASED CHANCE OF SURVIVAL

Many businesses are not prepared for the high cost of falling victim to a cyberattack. If you haven't planned how your business will handle a cyberattack, you may not have a solid grasp of the costs involved in a response.

IMPROVED CYBER RESILIENCE

Building your company's cyber resilience is a key component of mounting a successful incident response. Cyber-resilient companies can quickly move to isolate intrusions, minimize damage and keep functioning in any conditions.

FORMING YOUR INCIDENT RESPONSE TEAM

The first and most important step in creating an incident response plan is establishing the team that will craft and carry out the plan. These are the folks who get the call when disaster strikes. One of the most often recommended structures for an incident response team is to establish a Computer Security Incident Response Team (CSIRT). But creating your CSIRT is not quite a one-size-fits-all proposition. Every organization has unique capabilities and resources. This basic framework can be tailored to fit the needs of your organization.

Incident response team functions & responsibilities

An incident response team has **FIVE CORE FUNCTIONS:**

LEADERSHIP

1. Coordinating the overall direction and strategy of each incident response ensures that everyone working on it is focused on minimizing damage, recovering quickly and operating efficiently

INVESTIGATION

2. Getting to the bottom of the incident as quickly as possible is paramount. That information enables teams to close security gaps, mitigate the damage, limit downtime and begin recovery.

COMMUNICATIONS

3. Making sure that relevant communications are reaching the right people is essential. Facilitating communications may be required across an organization's teams and departments - This keeps everyone on the same page.

DOCUMENTATION

4. Everyone must create and preserve accurate records of the incident response. This serves two purposes: making sure that you can analyze the response effort and find areas of improvement, and acting as a reference for future incidents.

LEGAL REPRESENTATION

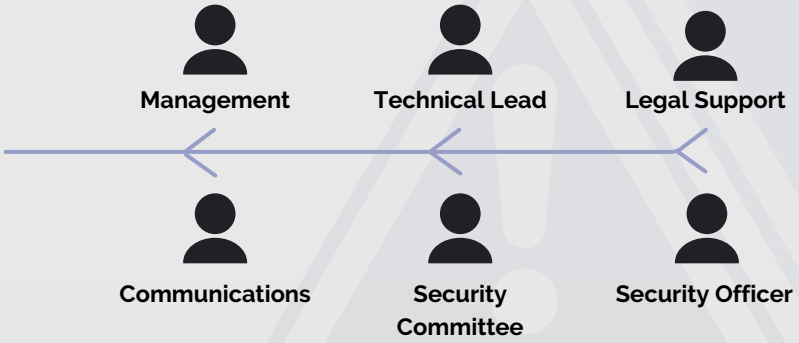
5. An incident always carries legal repercussions. It is important to ensure that incident response actions are being done in accordance with applicable laws and regulations to protect the organization and to ensure legal compliance.

The Six Essential People you need on your team

This team should include everyone who will need to be contacted or take action in the event of a cybersecurity incident like a ransomware attack.

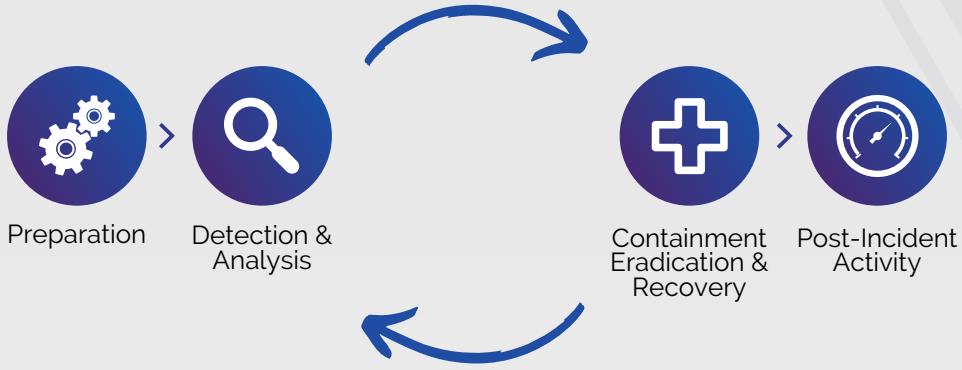
↳ Bear in mind: Your CSIRT team isn't just the people in the IT department. It's everyone in your organization who needs to be involved, including the legal team and your communications organizations.

Fill These Roles



INCIDENT RESPONSE CYCLE

The U.S. National Institute of Standards and Technology (NIST) agency's four-part incident response cycle is the model most organizations use to create their own incident response plan. The NIST incident response cycle divides the practical elements of handling a cybersecurity incident into four distinct steps that take you from start to finish.



WHAT WOULD AN INCIDENT RESPONSE LOOK LIKE FOR ME?

In this example, we'll use ransomware as the cause for your security incident and map out what each step might entail based on the NIST Incident Response Cycle.

PREPARATION - This may be the hardest step because it's easy to rush through it. However, this is also the most important step. Having the right people and processes in place before an emergency happens can mean the difference between quickly righting the ship or floundering.

Create a team: Call your CSRIT into action. Each of the six members will round up.

Establish a protocol: How exactly will everyone be informed and get their instructions on how to handle the incident – and who is empowered to make hard decisions? This is where your decision matrix fits into your plan

The framework of your plan can use any criteria you choose and be customized for your business. The most important part of this step is to establish the parameters of your planning framework, then use that framework to create your response plan for every incident. Consistency in format and layout for each plan will make it easy for your CSRIT to execute it during a disaster, enabling them to stay focused on the next two steps.

DETECTION & ANALYSIS - The first step to fixing the problem (and mitigating the damage) is to figure out the problem. To continue with the ransomware scenario, this is the step where your security personnel find the cause, extent, and location of the damage, then report it to the CSRIT

What is the problem?: In our scenario, it's ransomware. So, we'll start at the most likely point of infection — email accounts — because most ransomware attacks start with a phishing email (like 90% of all cybersecurity threats do).

What caused the problem?: Let's say an employee got caught by a phishing email and downloaded a PDF that contained ransomware.

Where did the damage start & where has it spread?: The team determines that the ransomware originated from that employee's email account. Performing some basic forensics then enables us to see where else it may have migrated.

CONTAINMENT, ERADICATION, AND RECOVERY

Containment: In this step, your CSRIT will decide how to minimize the damage from the incident and keep the business running. This may also be a place where you'll need to know what can be sacrificed if necessary

Example ransomware incident questions: Is the data or network encrypted? Can we isolate the infection or impacted systems? What systems and data did the affected computer have access to? Can this incident be handled remotely?

Eradication: This is the step where your CSRIT decides what the most expedient and effective way of eliminating the problem is for your business. Every business has unique needs and capabilities, so this step may vary dependent on the systems and data affected. You may want to include multiple options that account for each variable that affects the choices that your team will encounter here.

Example ransomware incident questions: Can we remove the ransomware? Can we restore our data and systems from backup? What will we do if we can't?

Recovery: This is the step that requires the most pre-planning. Restoring your business to full operations may be impossible without secure backup and recovery options for your data. You may also need to bring in specialists to handle PR, technical and legal issues, especially if your industry or location means that you're dealing with complicated compliance issues or extensive reputation damage.

Example ransomware incident questions: Where are the backups? Who has access to the systems and software that you need to get back to work? How do we fix the damage?

POST-INCIDENT ACTIVITY - After the incident ends and you've started getting back to normal, an after-action report is a must. It pays to immediately analyze your incident response plan, your CSRIT 's performance, and your decision matrix. Finding weaknesses in the plan or process and addressing them immediately will help you create a better plan for the future.

Then, spend some time determining what you can do to reduce the chance of this being a problem for your business in the future. In our scenario, a staffer unleashed a ransomware nightmare because they were fooled into interacting with a phishing email. How can you prevent that from happening again?

Example ransomware incident questions: Is there reporting to be filed with the government or industry officials? What went right with our incident response plan? What went wrong? How can your team improve their performance next time? Do we need to adjust our plan?

THE BEST WAY TO RESPOND TO AN INCIDENT IS TO NEVER HAVE ONE AT ALL...

With Shield IT Networks' elite stack of cybersecurity solutions, we minimize the chance of your company ever being attacked. Schedule a cybersecurity assessment to see how your current cybersecurity stacks up.

SCHEDULE A COMPLIMENTARY CYBERSECURITY ASSESSMENT