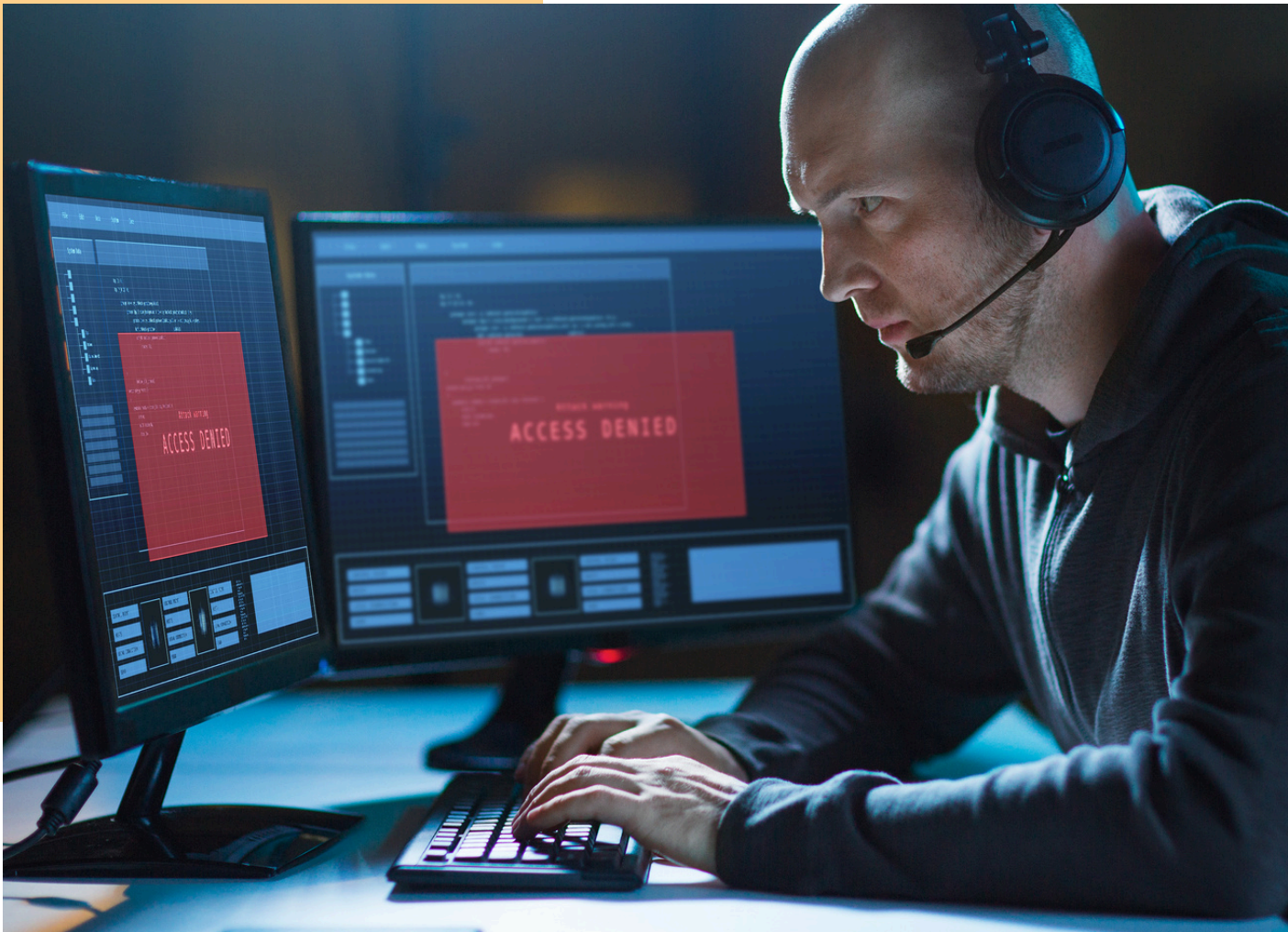
INTELLIGENT TECHNICAL SOLUTIONS

How to Create an Incident Response Playbook

Give Your Business the Best Chance of Survival



Planning is Half the Battle

When is the best time to make sure you're ready to respond in an emergency situation? Before that emergency ever happens, of course. That logic applies to every kind of emergency from a gas leak in your building to a cyberattack on your company's IT environment. Companies that are prepared for trouble often find out that they experience less of it because when employees are on the same page with regards to safety and security, they are much more likely to notice problems before they grow into disasters.

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, spear-phishing, 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 sight.

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.

Chapter 1: Rise in Cybercrime Gives Rise to the Need for an Incident Response Plan (IRP)

Cybercrime has grown exponentially over the last few years and isn't going to slow down anytime soon. In fact, according to a new generative AI and cybersecurity report by Sapio Research and Deep Instinct, 75% of security professionals surveyed said they have seen an uptick in attacks from 2022 to 2023.

Cybercriminals don't discriminate when choosing targets. Every business of every size is at risk of a damaging cyber-attack like ransomware or business email compromise. According to the most recent annual cyber readiness report by Hiscox, 41% of small businesses fell victim to a cyber-attack in 2023, a rise from 38% the previous year.

Eventually, cybercrime is going to come knocking at your desktop.
The question is, what will you do when it arrives?

Chapter 2: Why Does My Business Need an Incident Response Plan

A cybersecurity incident occurs when employees or outside actors take an action that threatens or harms a company's systems and data. Each occurrence of a negative event is an incident - and every company has them.

Only 39% of organizations with a formal, tested incident response plan experience a cybersecurity incident as compared to 62% of those who don't have a plan.

Just like anything else that can damage a business, minimizing those occurrences is always preferable. However, mistakes and incidents happen. By being prepared for cybersecurity emergencies, companies not only ensure that they're making all the right moves in an emergency situation, but they can also reduce the number of incidents they have at all.

Having an incident response plan doesn't just protect your business during and after an incident. With its power to increase your cyber resilience, it also empowers your business to thrive and emerge from an incident with more cash and helps prevent another incident in the future.

Benefits of an Incident Response Plan

Here's how your business can benefit from an incident response plan:

1. RISK MITIGATION

Making, testing, and maintaining an IRP will reduce your company's chances of experiencing a damaging cybersecurity incident. But how much of a difference can it make? When it comes to security incidents, time is crucial to minimize or mitigate the impact. The longer it takes you to respond to an attack, the more significant the damage it can bring.

2 . 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. IBM researchers found that businesses who didn't have a formal, tested IRP spent 58% more per breach at $5.92 million. Conversely, businesses that did test their IRP spent only $3.26 million on average.

3. INCREASED CYBER RESILIENCE

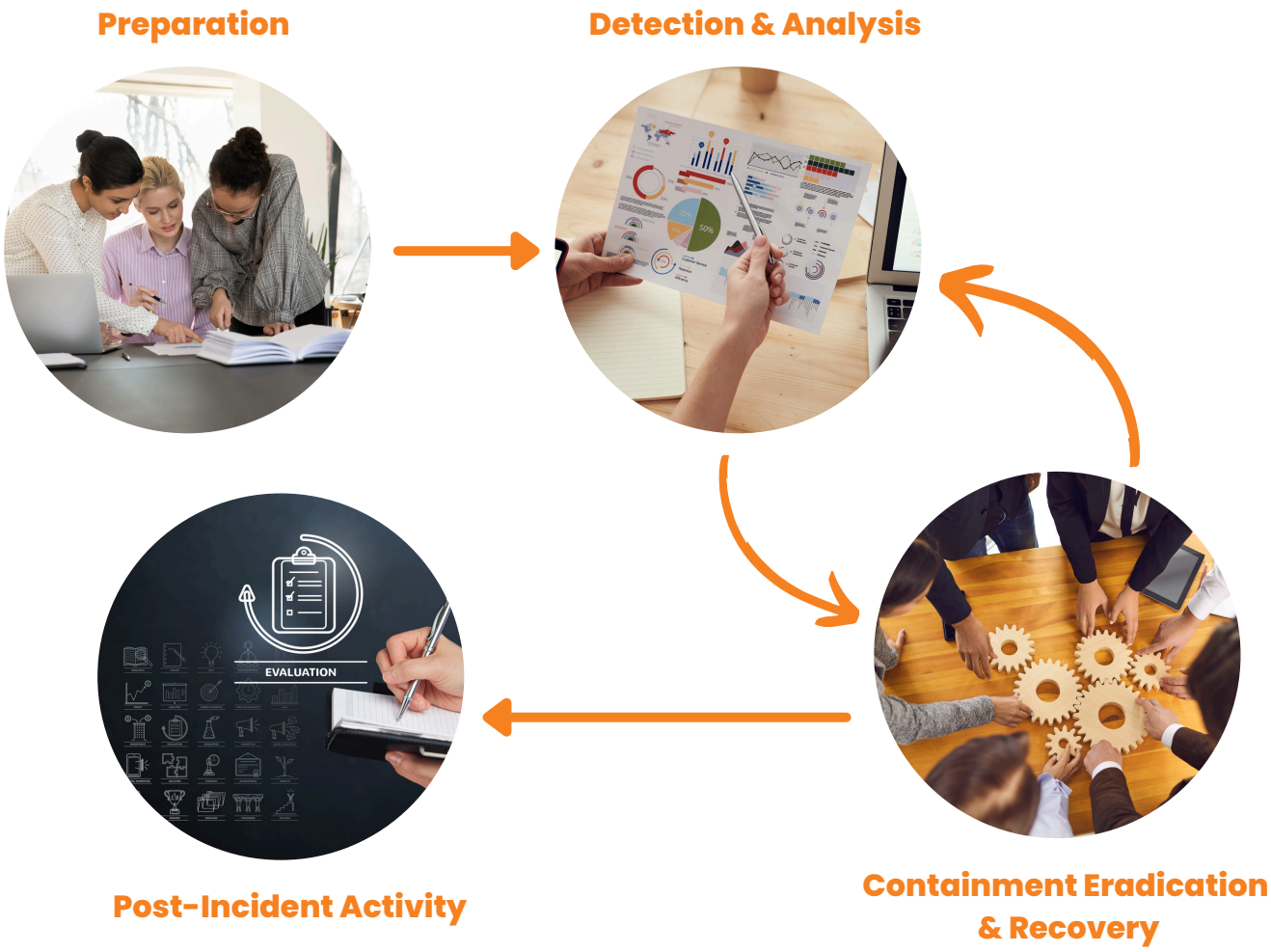
Building your company's cyber resilience is critical to a successful incident response. Cyber-resilient companies can quickly move to isolate intrusions, minimize damage, and keep functioning in any conditions. Regularly updating and reviewing incident response plans was a key reason why cyber resiliency improved for 47% of high performers in an IBM survey.

Chapter 3: Why Leverage the NIST Response Cycle?

The most prominent set of industry best practices for cybersecurity incident response is maintained by the U.S. National Institute of Standards and Technology (NIST). While the agency is not a regulatory entity, its research into cybersecurity planning and risk management has led them to develop rigorous protocols for recording, reporting, and responding to breaches and incidents.

Their 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:

- Preparation
- Detection & Analysis
- Containment, Eradication & Recovery
- Post-Incident Activity



Chapter 4: 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 establishing 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 your organization's needs.

But, before you choose your team, it's important to understand their roles.

Incident Response Team Functions and Responsibilities

An incident response team has five core functions:

1. LEADERSHIP
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.

2. INVESTIGATION
It is paramount to get to the bottom of the incident as quickly as possible. That information enables teams to close security gaps, mitigate the damage, limit downtime, and begin recovery. Knowing how an incident started is also critical for preventing the same thing from happening again.

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

4. DOCUMENTATION
Everyone must be cognizant of the need to create and preserve accurate records of every facet of an 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 similar future incidents.

5. LEGAL REPRESENTATION

An incident always carries legal repercussions. It is essential to ensure that incident response actions are done per applicable laws and regulations to protect the organization. In some industries, regulators or authorities must be notified and kept apprised of the situation, or other actions may be necessary to ensure legal compliance.

Source: TechTarget

The 6 Essential People You Need on Your Incident Response 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. Remember: Your CSIRT team isn't just the people in the IT department. Everyone in your organization must be involved, including the legal and communications teams. These teams will also handle aspects of incident response in other departments, such as dealing with legal issues or communicating with the press. Think of these as mini departments.

To compile your team, you'll need to determine who in your organization is qualified to fulfill the core functions and responsibilities of a CSIRT listed in the previous section. Then, use that list to fill these roles:

- Management
- Technical Lead
- Legal Support
- Communications
- Interface to the Security Committee
- Security Officer

Each team member must be ready to act and be empowered to make the decisions necessary to mitigate the damage. A decision matrix for your team enables restoration to run smoothly when you're in the trenches.

Like a RACI Chart, the components of that decision matrix should include:

1. **Owner:** Decision maker and process owner
2. **Helpers:** Team members who help out on a process
3. **Advisors:** Team members who advise on a process
4. **Implementers:** People doing the work
5. **Updaters:** Team members updated with the status and actions of other team members

Source: Science Direct

Chapter 5: What Would an Incident Response Look Like for You?

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.

Step 1: Preparation

This may be the most challenging step because it's easy to rush through. However, this is also the most crucial step. **Having the right people and processes before an emergency can mean the difference between quickly righting the ship or floundering.**

- **Create a team:** Call your CSIRT into action. Each of the six members will then gather their team.

- **Establish a protocol:** How exactly will everyone be informed and instructed 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 establishing the parameters of your planning framework and then using that framework to create your response plan for every incident. Consistency in format and layout for each plan will make it easy for your CSIRT to execute it during a disaster, enabling them to stay focused on the next two steps.

Step 2: Detection and 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 your Computer Security Incident Response Team (CSIRT).

- **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, and where did it spread?** The team determines that the ransomware originated from that employee's email account. Performing some basic forensics lets us see where else it may have migrated.

Step 3: Containment, Eradication, Recovery, and Post-Incident Activity

1. Containment

In this step, your CSRT 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.

Guide Questions to Ask Yourself:

- 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?

2. Eradication

This is the step where your CSIRT decides the most practical and effective way to eliminate the problem for your business. Every business has unique needs and capabilities, so this step may vary depending on the systems and data affected. Consider including multiple options that account for each variable that affects the choices that your team will encounter here.

Guide Questions to Ask Yourself:

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

3. Recovery

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

Guide Questions to Ask Yourself:

- 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?

4. Post-incident Activity

After the incident ends and you've started returning to normal, an after-action report is necessary. It pays to immediately analyze your incident response plan, your CSIRT '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.

Guide Questions to Ask Yourself:

- How can you prevent that from happening again?
- Is there reporting to be filed with the government or industry officials? What went right with your incident response plan?
- What went wrong?
- How can your team improve their performance next time?
- Do weyou need to adjust ourthe plan?

Ready to Create Your Own Incident Response Playbook?

Everyone is vulnerable to cyber-attacks, but that doesn't mean you have to be the next target. Taking the time and investing in the right cybersecurity measures can help keep you from falling prey. That might seem like a big project, but it's one worth doing because the best way to respond to an incident is to prevent one from happening at all.

For over two decades, Intelligent Technical Solutions (ITS) has helped hundreds of businesses boost their cybersecurity efforts. Want to find out where your current cybersecurity measures stand? Fill out our form for a free IT security assessment.