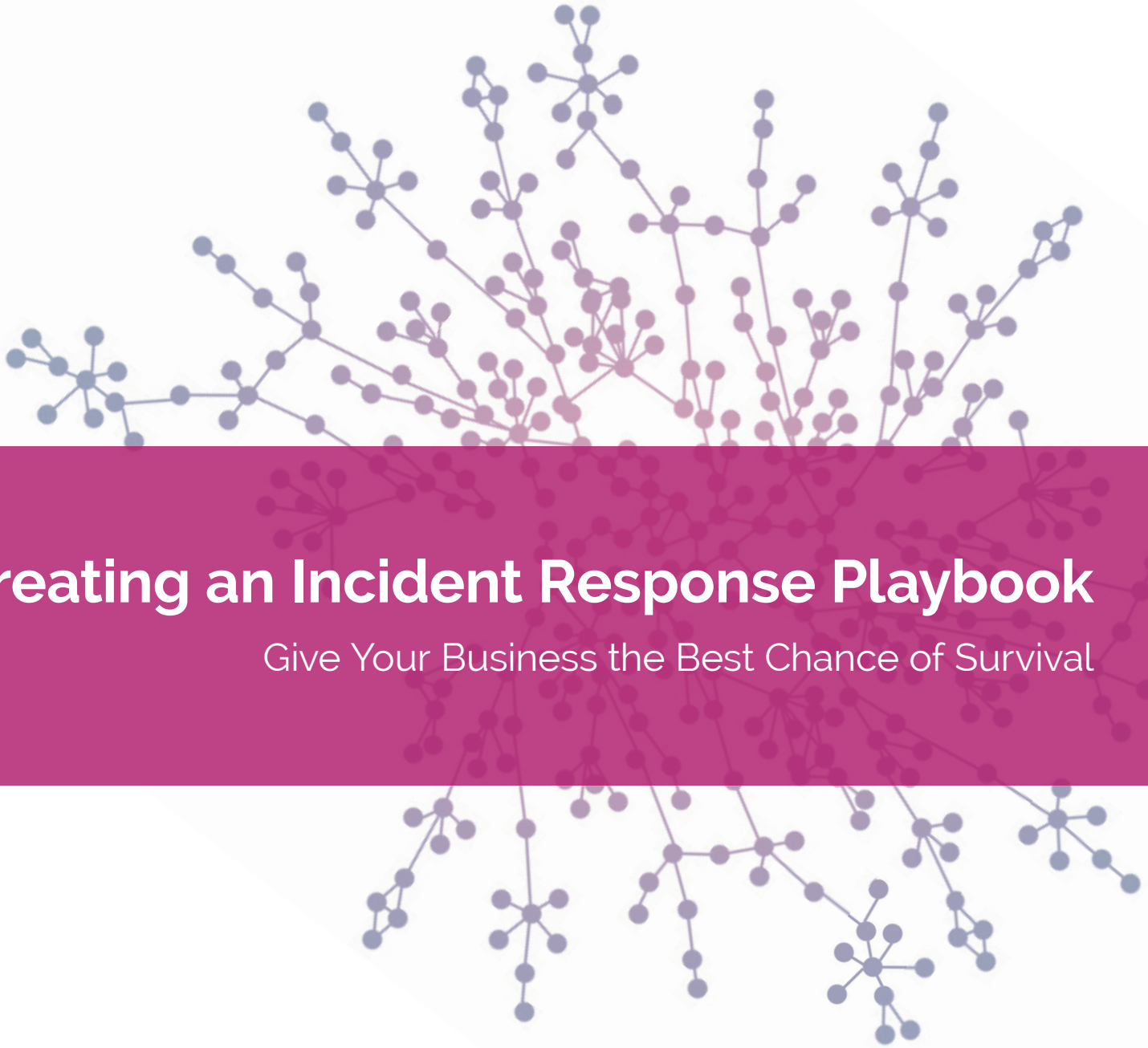
GRAPHUS
A Kaseya COMPANY



Creating 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 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.

RISE IN CYBERCRIME GIVES RISE TO THE NEED FOR AN INCIDENT RESPONSE PLAN

Cybercrime has grown exponentially over the last few years and isn't going to slow down anytime soon. About 67% of respondents in an IBM study said that the volume and severity of cybersecurity incidents that they face markedly increased in 2021.

Cybercriminals don't discriminate when choosing targets. Every business of every size is at risk of a damaging cyberattack like ransomware or business email compromise. An estimated 50% of ransomware incidents in 2020 happened to SMBs with less than 100 employees.

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

WHY DOES MY BUSINESS NEED AN INCIDENT RESPONSE PLAN?

A cybersecurity incident is an adverse condition that is caused by employees or outside actors taking an action that results in a threat or harm to a company's systems and data. Each individual 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 preferrable. 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, 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. Now, with increased 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.

About 94% of executives say their firms have experienced a cyberattack or compromise that impacted their business within the past 12 months.

Plan Ahead to Win

Here's how your business can 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. But how much of a difference can it make? Well, an enormous one. IBM researchers announced that less than one in four organizations with a formal, tested incident response plan experienced an incident as compared to 62% of those that didn't have a plan.

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. SMBs spend an average of $955,429 to restore normal business in the wake of a cyberattack. However, having a tested incident response plan can save 35% of the cost of an incident.

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. Regular updating and review of incident response plans was a key reason why cyber resiliency improved for 47% of high performers in an IBM survey.

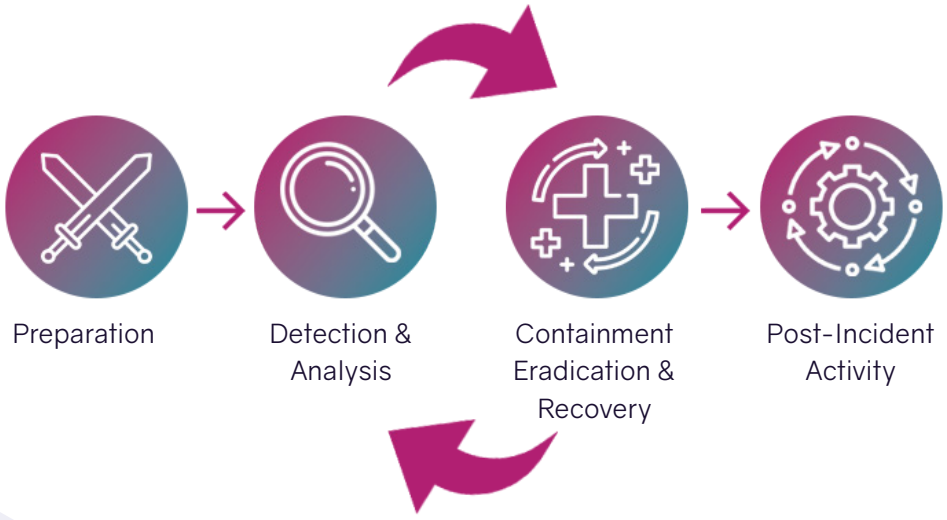
PREPARING YOUR INCIDENT RESPONSE

The most important part of a successful incident response is having a plan in the first place. Unfortunately, far too many companies don't. Only 26% of respondents in the IBM Cyber Resilient Organizations Study 2021 said that their organizations have cybersecurity incident response plans that are applied consistently across the entire enterprise. However, regularly updating and reviewing incident response plans was a key reason why cyber resilience improved for 47% of high performers.

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). The 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.

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



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 and responsibilities

Before you choose your team, it's important to understand what they'll be doing. An incident response team has five core functions:

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.

Investigation - 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. Knowing how an incident started is also critical for knowing how to prevent the same thing from happening again.

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.

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.

Legal representation - 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. In some industries, regulators or authorities will need to be notified and kept apprised of the situation, or other actions may be needed 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.

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. 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 roles 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 CSRIT listed in the previous section. Then use that list to fill these roles:

1. Management
2. Technical lead
3. Legal support
4. Communications
5. Interface to the security committee
6. Security officer

Source: Science Direct

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 from other team members

Source: Science Direct

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 then gather their team.

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 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 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 and 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?

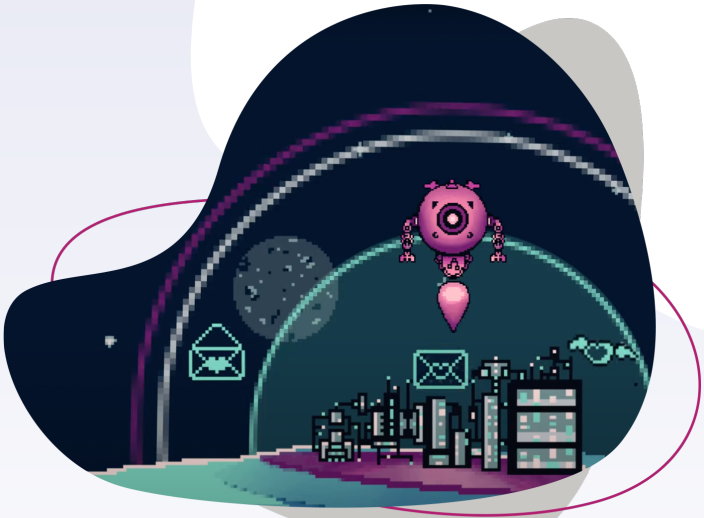
Example ransomware incident questions: Is there reporting to be filed with the government or industry officials? What went right with our incident response plan? What went wrong? How can your team improve their performance next time? Do we need to adjust our plan?

GRAPHUS PREVENTS PHISHING ATTACKS FROM BECOMING PHISHING DISASTERS

We used a phishing email that unleashed a ransomware attack in our example for a reason. Phishing is the most likely way for a cyberattack to strike your business. That means it is critical that you establish a smart defense against phishing to reduce your organization's chance of getting walloped by a cyberattack.

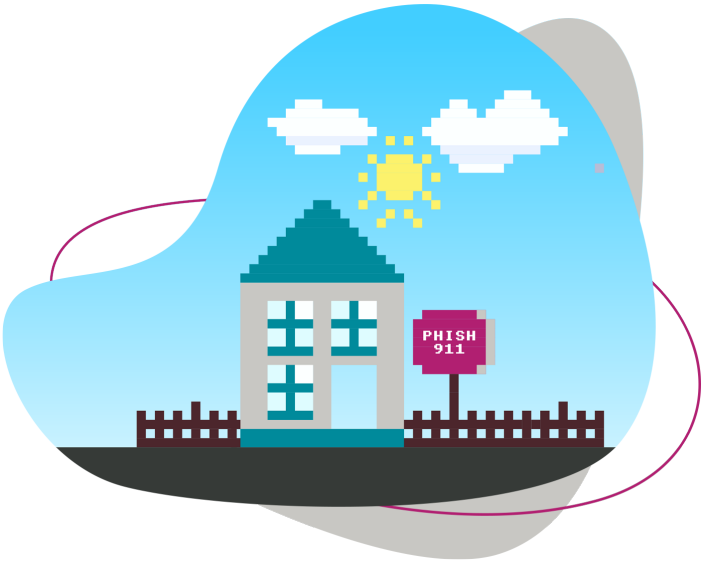
Automated, AI-powered email security from Graphus is the ideal choice to combat the flood of dangerous phishing emails heading for your organization. Automated email security with a solution like Graphus stops 40% more phishing messages from reaching an employee inbox than conventional security or a SEG. How? By putting three powerful shields between your employees and a phishing email.

- **TrustGraph** uses more than 50 separate data points to analyze incoming messages completely before allowing them to pass into employee inboxes. TrustGraph also learns from each analysis it completes, adding that information to its knowledge base to continually refine your protection and keep learning without human intervention.



- **EmployeeShield** adds a bright, noticeable box to messages that could be dangerous, notifying staffers of unexpected communications that may be undesirable and empowering staffers to report that message with one click for administrator inspection.

- **Phish911** enables employees to instantly report any suspicious message that they receive. When an employee reports a problem, the email in question isn't just removed from that employee's inbox — it is removed from everyone's inbox and automatically quarantined for administrator review.



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

Why take the chance of a phishing email causing a massive disaster for your business? Stop phishing immediately with Graphus – the most simple, automated and affordable phishing defense available today. Schedule a demo with one of our email security experts now.

▶ SCHEDULE YOUR DEMO

GRAPHUS

A Kaseya COMPANY

sales@graphus.ai

graphus.ai/demo

03022021