Five “Must-Do’s” When Developing an Incident Response Plan

US SIGNAL®

Table of Contents

US SIGNAL®

Introduction

Hope for the best but plan for the worst. They're words of wisdom that apply as much to the IT world as every day life. After all, cyber threats, data breaches, equipment failures and other events are a matter of not if but when. And you hope that when they occur — and they most likely will, they won't result in downtime, lost or corrupt data, stolen personal information or anything else that could affect your business.

One of the ways to plan for the worst — and mitigate potential disruption and/or damage — is to have a vetted incident response (IR) plan in place. An IR plan is a written document, formally approved by your company's executive team, that guides your organization in what it should do before, during, and after a confirmed or suspected security incident. It defines roles and responsibilities and outlines key activities.

There's no one-size-fits-all IR plan that will work for every company, but it's easy to use any of the many IR plan templates available (including the one from US Signal) as a starting point. As you go through the process of filling in or modifying an IR plan template, or if you're developing one from the bottom up, the following pages note some of the things to keep in mind.

Incident Response is People Oriented

All the IT security technologies and devices in the world won't necessarily stop a cyber incident. Nor can they handle all aspects of dealing with it. People are at the heart of incident response, and that includes everyone throughout your organization — your IT team, company leadership, the company's legal and public relations teams, and all employees.

While IT takes the lead in IR planning and execution, every individual within your company has the responsibility to report and help mitigate an IT security incident. Your IR plan should include steps you can take to prepare them to do so, whether it's through training, awareness or any of a number of other ways. It's critical that all stakeholders understand their roles and responsibilities, not just your IR team.

Vendors and consultants can be affected by cyber incidents as well — or cause them, so keep them in mind as well when developing your IR plan. Make sure they're aware of the proper IT security protocols they're to follow. Confirm all contact information and contractual agreements for the third parties that do business with your company.

Note: Don't hesitate to repeat communications and other activities to keep all stakeholders aware of their responsibilities for IT security.

US SIGNAL®

Know What You Have and How You're Protecting it

Make sure you understand and have accounted for all IT assets that could be affected by an IT security incident. Map out your network infrastructure, including interconnections with other organizations. Inventory all hardware and software. Include assets that are owned or controlled by outside parties such as remote workers and cloud services.

Take steps to account for shadow IT. Make sure you understand process workflows involving IT assets and any interconnections and dependencies involved. Note of the state of your IT assets. Are all software patches up to date? Is all equipment being serviced regularly according to best practices and maintenance schedules being followed?

Review your security strategy for protecting all assets and processes. Are there gaps? Are there newer technologies or best practices that should be implemented? What about physical security of the facilities where your IT systems are housed?

If critical assets go down or need to be shut down, what plans are in place to maintain business operations? Disaster recovery and business continuity need to be considered in your IR plan as well.

Note: These activities and questions need to be addressed frequently to cover the addition of new assets, previously undetected vulnerabilities and emerging threats.

Take an Outside-In Look

Put yourself in the shoes of a cyber attacker. **If you were trying to infiltrate your company's IT systems, what would you do?** Ask your IR team to do the same. Where are the weaknesses? What are the vulnerabilities? What are the potential — and most promising — targets to attack? What assets and users have access to those targets?

Consider various scenarios in which threats — such as negligence or malicious acts — to your IT systems could be caused by vendors, consultants or even remote workers. The idea is to look at the potential for attacks from various sources, not just from your perspective as someone working in IT. As saying goes, you don't know what you don't know.

This is a good time to have a third-party IT security assessment conducted. An assessment not only looks at the security processes, technologies and protocols you have in place. It will seek out the weaknesses and vulnerabilities you might not see or suspect.

This will all help in planning for the wide range of cyber incidents that could occur. The information can also be used to close various security gaps to lessen the chance of certain cyber incidents taking place.

Note: Compile a collection of various IT threat scenarios and keep updating it. This information can be used for testing your IR plan and various security services and technologies.

US SIGNAL®

Understand the Attack Sequence

When a cyber incident occurs, it will go through various steps. In addition to understanding the various threats, you need to understand how they each could play out.

Map out the chain of events for a ransomware attack and other IT security incidents so you understand where the opportunities lie for detection, blocking or containment, and remediation. This will help in determining how to plan for your response to each and what resources — including personnel — will be required. The sooner you can detect an incident, the sooner you can respond to it and prevent damage.

Keep in mind that new cyber threats are constantly emerging and will likely work differently than the usual ones. New approaches to identifying and remediating them are always in development as well.

It's important to stay on top of what's going on it the IT security world. Your IR plan should cover the most frequently encountered incident types, but allow for changes to meet evolving threats. Frequent reviews of your IR plan will also help in terms of keeping it up to date.

Note: Most cyber-attacks follow a similar pattern: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. Nonetheless, be prepared for deviations to that pattern.

Test.
Fix.
Test Again.

Make sure your IR plan works as intended by putting it to the test. The following are two options to help ensure the plan works the way you expect it to work and to identify components that may need to be revised.

+ **Tabletop Exercise.** Gather key players in a conference room, throw out several breach scenarios and have everyone talk through their part of the response, per your IR plan. It's a useful exercise but you could get a false sense of security if your only testing comes from conversations in a meeting room.

+ **Simulated attacks.** Perform a realistic, fake attack on your IT systems. You can use testers from your own security team or contract with external penetration testers. You can also conduct attacks pre-coordinated with your internal team, or blind attacks with no notice. Simulated attacks work well for identifying gaps in your internal security systems, processes, or integration with an external incident response provider.

Review the test results, adjust the IR plan accordingly, and share the changes with all stakeholders. Test again to make sure things now work as expected. Repeat testing is also a good idea given that staff, third-party consultants, technologies and other aspects of your company's operations can change frequently.

Note: Whatever kind of testing you conduct, remember to plan for the human resources aspects. For example, suppose your plan states that when a security incident causes operations to go down for a half day, everyone is sent home. Do you expect them to actually leave for the day and if they do, will they still get paid?

US SIGNAL®

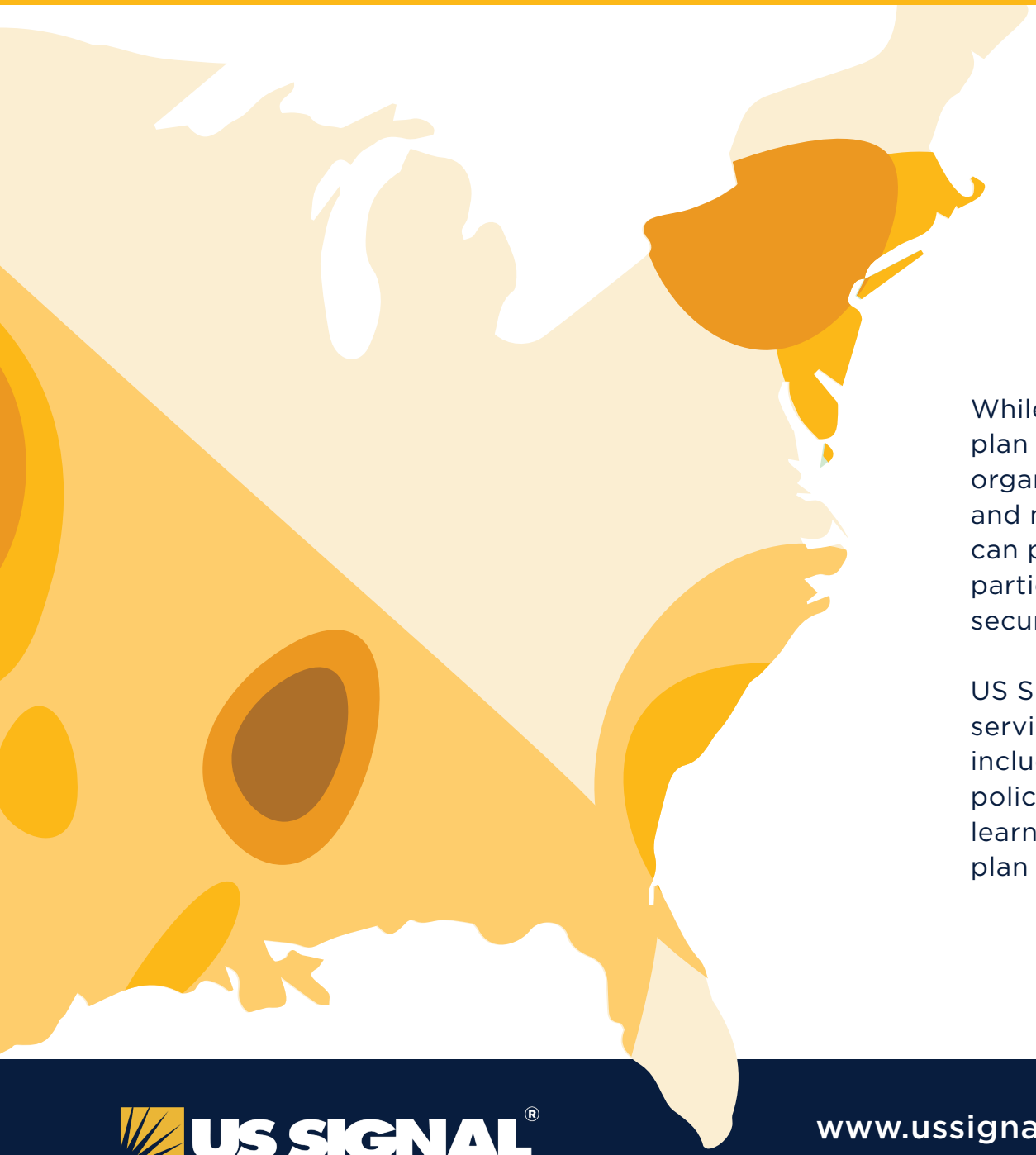
IR Plan Checklist

In addition to the information provided in this eBook and in whatever IR plan template you choose to use, answering these questions can also be of assistance in developing a comprehensive IR plan.

- Who is responsible for each phase of the incident response process (identification, containment, eradication, recovery, and lessons learned)?
- Who will work with law enforcement officials, if necessary?
- Does your plan account for who discovered or reported the incident and when and where it was discovered?
- Does your plan consider the impact various types of security incidents would have on business operations and what actions would be required? This would nclude things like communications and work stoppages.
- What is the extent of the incident with the network and applications?
- Are you prepared to contain various types of cyber incidents and if you can't, do you have plans for an alternative course of action?
- Are plans in place to protect critical data and/or keep operations going in the event of a cyber incident?
- Do you have plans for fixing infected systems and securing them once they are fixed?
- How will infected systems be deployed back into production?
- When will infected systems be deployed back into production?
- What operations will be restored first during the recovery phase?
- What testing and verification should be done on infected systems?
- Once the incident and lessons learned are documented, who needs to see this information?
- Who is responsible for developing and implementing fixes to the IR plan?

US SIGNAL®

Partner with Security Experts



While an IT security incident response plan is something your internal organization must develop, implement and maintain, third-party companies can provide some assistance – particularly those specializing in IT security services.

US Signal offers both IT security services and security advisory services, including assessments, virtual CISO, and policy and procedure development. To learn how we can help you with your IR plan and overall IT security, contact us.

US SIGNAL®

www.ussignal.com | 866.274.4625