

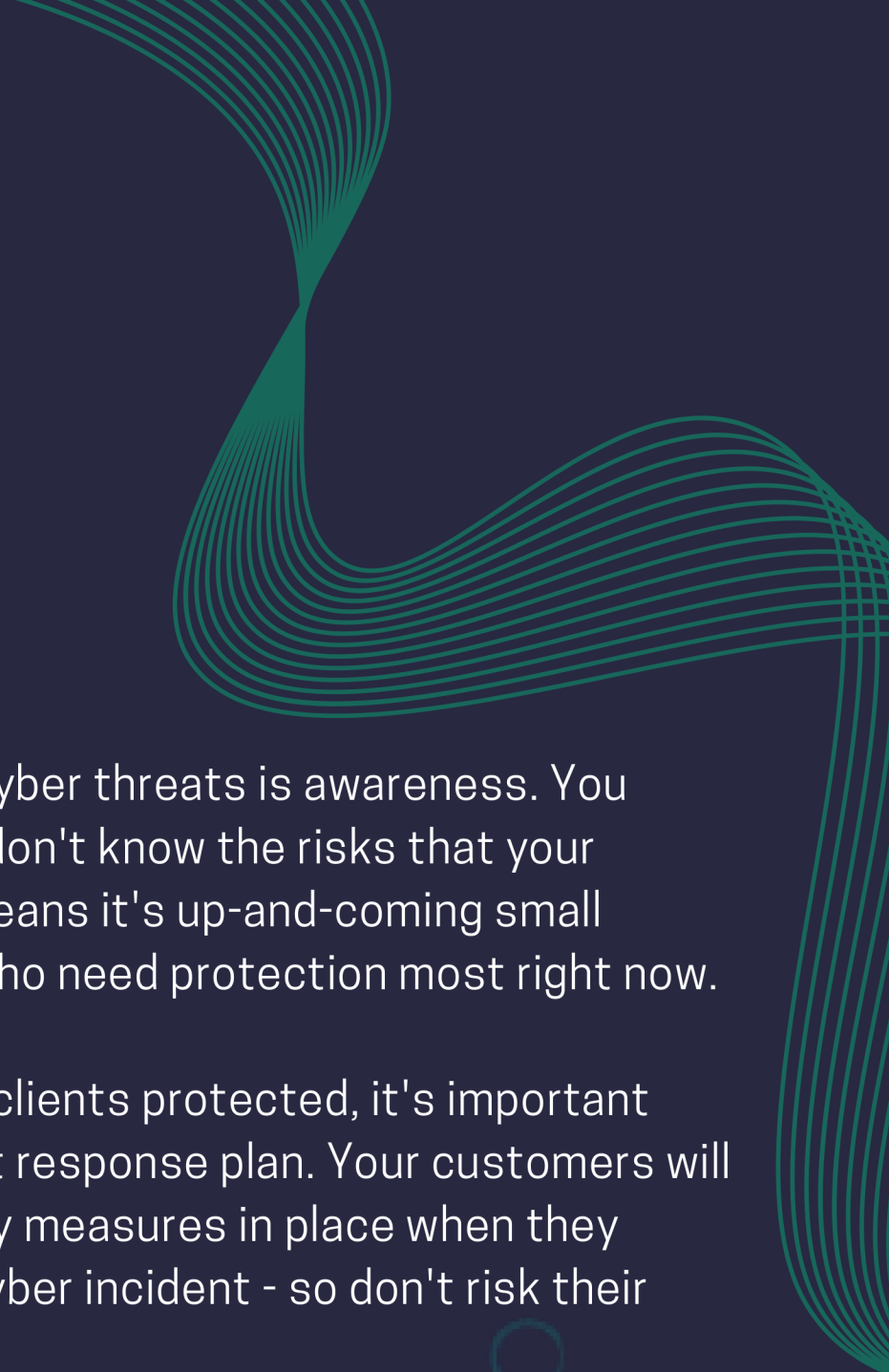


Best Practices Checklist

CYBER THREATS INCIDENT RESPONSE PLAN

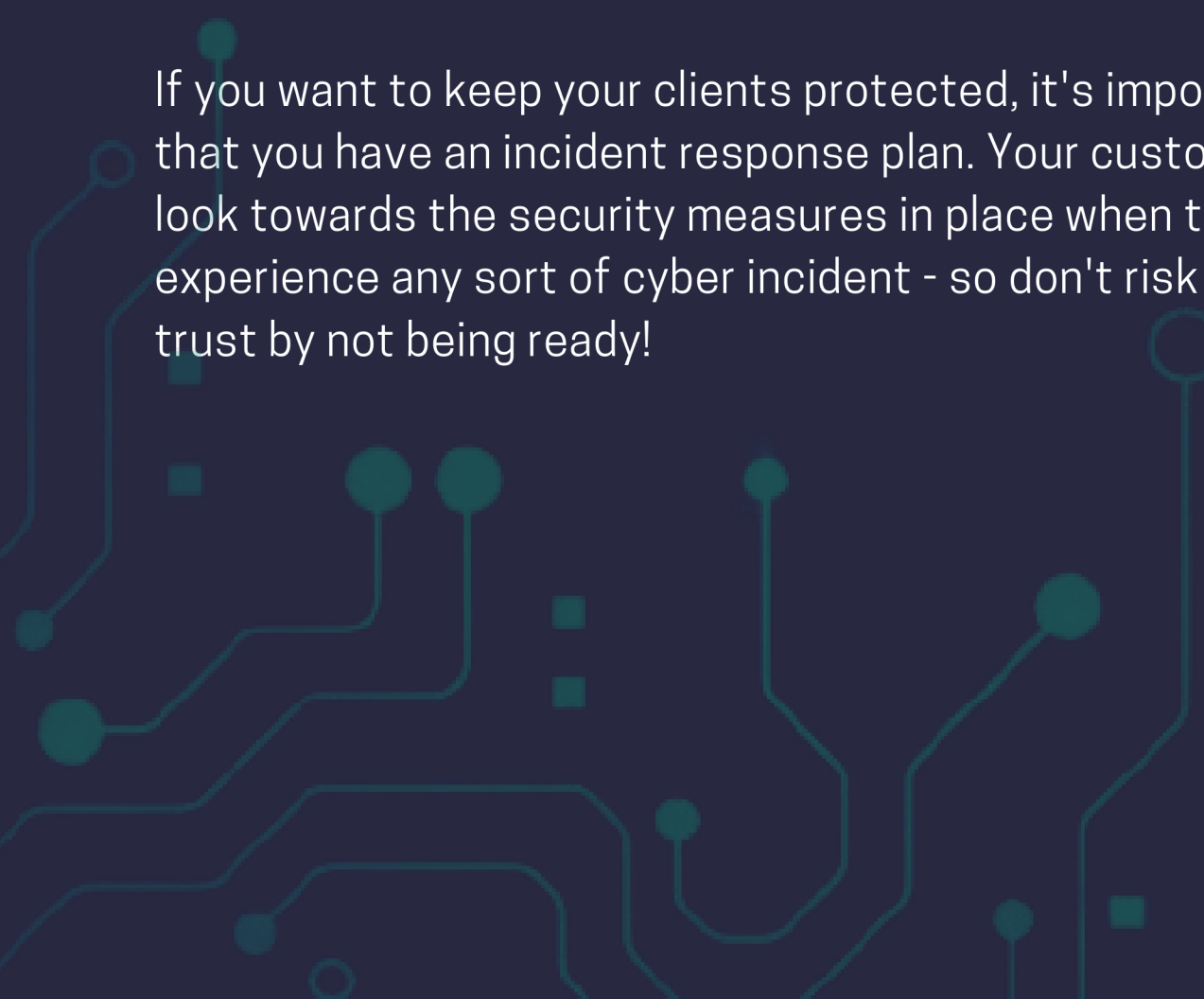
**The Secret to Responding Effectively
to Cyber Incidents**

Prepared by
Cite Technology
Solutions



Awareness

The key to dealing with cyber threats is awareness. You can't be prepared if you don't know the risks that your business faces, which means it's up-and-coming small businesses, like yours, who need protection most right now.



If you want to keep your clients protected, it's important that you have an incident response plan. Your customers will look towards the security measures in place when they experience any sort of cyber incident - so don't risk their trust by not being ready!

Table of Contents

Defining an Incident Response Plan	04
NSIT's 6 Key Steps for Incident Response Process	05
Protecting Your Clients	08
SBA Cybersecurity Tips	09





Defining an Incident Response Plan

An incident response plan is a document that outlines how to respond to any type of external hazard to your customer's business environment, such as a data breach or malware attack. It helps your team recover from incidents quickly and consistently by defining what needs to be done.

An effective incident response plan minimizes potential impacts, such as data loss, resource abuse, and customer confidence loss. We've created a checklist on how to create an incident response plan to help you gain client confidence.

NSIT's 6 Key Steps for Incident Response Process

1

Preparation

This phase is all about getting ready for major incidents ahead of time so that they don't have a detrimental impact on your clients' businesses. You must align the organizations' policies on personal information protection, sensitive data security, and network security objectives with the technology infrastructure during preparation.

During this phase of incident response planning, make sure that users have some comprehension of computer security and basic incident response training to confront a cyber crisis. Everyone must be informed of his or her obligations and responsibilities in the event of a cyber occurrence.

You should also test your response to incidents and identify essential assets. Evaluate how well your customers' technology infrastructure can prevent breaches and their compliance with regulations.

2

Detection & Analysis

This is often the most difficult step in the incident response process. To begin detecting and analyzing an incident for your clients, you must first identify the type of hazard they're facing. High-risk threats are divided into two categories by NIST: precursors and indicators.

An indicator is a signal that something has happened or might happen soon. This will help you find the source of the attack, how to stop it and how long you need to keep evidence.

You should also take care of post-incident measures for customers. This includes checking for security flaws, measuring damage, accurately documenting what happened, and telling affected people. You also need to report the breach to the authorities and other affected parties.

NSIT's 6 Key Steps for Incident Response Process



3 **Containment**

At this stage of the incident response plan, you must think about how to minimize the consequences of the breach. This phase should contain key activities such as assessing backups, privileged access credentials, and ensuring that all required security updates have been installed.

- What systems may be turned off?
- Is anything else safe to erase?
- What is the first step in carrying out the strategy?
- What is the long-term plan?

4 **Eradication & Recovery**

The main goals of this stage of the cyber incident response plan are to understand the initial cause of the breach and to respond to it immediately. During this stage, the system will need to be patched, malicious software will be removed, and outdated software will be updated.

If you let any signs of malicious software or security challenges develop in your customers' systems, it can hurt your reputation. You could also be held legally responsible.

Your ultimate objective is to restore the harmed systems. This will be determined by whether you've addressed the vulnerabilities in your clients' systems and what measures you may take to prevent them from being attacked again.

Because it checks, monitors, and validates the afflicted systems, this step in the cyber event response plan is essential. Without adequate recovery, preventing a similar catastrophe in the future will be difficult.

NSIT's 6 Key Steps for Incident Response Process



5 **Post-Incident Activity**

This phase is all about collecting information, notifying agency leadership, fortifying the environment to avoid future attacks, and learning from them in order to improve the response. The analysis's main goals are as follows:

- Mitigate the underlying problem
- Resolve infrastructure issues
- Assess organization's procedures
- Update authorities, interfaces, and roles to ensure clarity
- Review technical or operational training
- Analyze tools for security, detection, analysis, or response



6 **Coordination**

It is very important that the Certified Information Systems Auditor (CISA) and the Federal Civilian Executive Branch (FCEB) agency work together when there is an incident, communicating as soon as possible. Note: certain agencies have special privileges and information that can be very helpful in a crisis.

Protect Your Clients

Checklist to Defend Against Cyber Attacks

- **Update Passwords Consistently**
Passwords that are strong are not always safe. They can be easier to hack if they are stored for a long time. You should tell your customers to change their passwords every six months.
- **Use a VPN**
Assist your clients in establishing a VPN (Virtual Private Network) to protect their corporate network from hackers. This will make it more difficult for hackers to discover which websites people visit, what passwords they use, or any other critical data.
- **Provide Security Training**
Educate your clients' employees on cybersecurity best practices to safeguard them. You may prevent them from making simple mistakes by educating them on the many threats that might jeopardize their business's security, such as data breaches and ransomware.
- **Run Phishing Tests**
MSPs may employ phishing simulators to determine how well their customers comprehend security standards. These exercises can assist end users detect a fraud when they encounter one.
- **Reset Access Controls**
You may further secure your network by using identity and access management solutions to control who has access to client resources. Only those who truly need it may be given access, lowering the risk of cyber attacks. You'll also be able to keep track of, identify, and figure out who is accessing which data.
- **Use MFA**
Two-factor authentication is a security measure that makes it more difficult for someone to hack into your clients' online accounts. This is a simple and easy measure that IT service providers can take to increase account security for customers.

SBA Cybersecurity Tips

United States Small Business Association (SBA)

○ **Browsing Practices**

Passwords that are strong are not always safe. They can be easier to hack if they are stored for a long time. You should tell your customers to change their passwords every six months.

○ **Avoid Suspicious Downloads**

Ensure that your consumers run the latest software updates on a regular basis, and be on the lookout for questionable emails. Educate them on how to tell the difference between a genuine and a suspicious website, as well as how not to download files by blindly clicking on links in emails.

○ **Use Strong Passwords**

You can assist your customers in securely accessing their saved credentials on any device and from anywhere by offering password management as a service. This will also decrease the number of daily password reset requests. You're encouraging consumers to establish good password practices and increase their security awareness levels by allowing them to create their own unique password rules.

○ **Protect Sensitive Information**

It's critical for your company to safeguard consumer information, since it is based on consumers' data. If hackers get hold of crucial client data, you and your clients will be damaged. By executing routine security inspections and ensuring that customer systems are up to date, you can protect your business and theirs.

○ **Maintain Good Cyber Hygiene**

Make sure your clients follow the following cyber hygiene precautions:

- Checking for viruses and running antivirus software
- Using a firewall to keep intruders from obtaining information
- Regularly update all devices' operating systems, web browsers, and programs
- Wiping and reformatting hard drives

Additional Resources: Semel Systems – Incident Response Professional Practice NIST Special Publication (SP) 800-61, rev. 2: Computer Security Incident Handling Guide | Incident Handler's Handbook | NIST 800-171 Self-Assessment – Incident Response | Department of Technology of the state of California – Incident Response plan sample. Reference: 1CISA Cybersecurity Incident & Vulnerability Response Playbooks



Questions?
Let's Talk.

CONTACT US



www.citetechnology.com



support@citetechnology.com



337-706-1169

