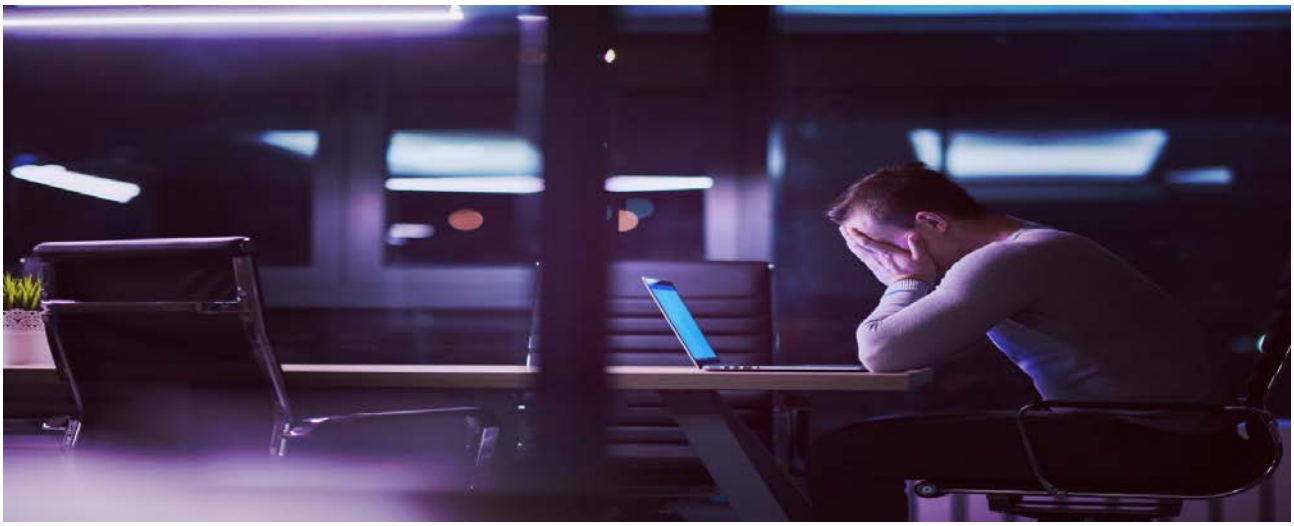
Postlethwaite & Netterville



Incident Response Planning: Too Important to Procrastinate

By Michael Richmond

Experiencing a cybersecurity incident right now? We can help.
Contact us.

It may be one of your worst professional nightmares: your organization is the victim of hacking. Cyber-attacks can cause immediate damage, so knowing how to respond is crucial. By the time most organizations discover hacking, it's too late to create a solid incident response plan. A reactionary approach can prolong the event, increase damages, and even contradict current legal requirements.

Since no one can predict the future, you must assume your company will be hacked at some point and plan accordingly. An incident response plan provides a set of instructions to help staff identify, respond to, and recover from cybersecurity incidents. The goal is to return to normal business operations as swiftly as possible by removing the threat, minimizing damage, and preventing similar incidents in the future.

The Six Stages of Incident Response

A well-defined plan includes steps for each of the six phases of incident response.

Preparation: Maintain and improve incident response capabilities and prevent incidents by ensuring that systems, networks, and applications are sufficiently secure.

Identification: Confirm, characterize, classify, categorize, and prioritize suspected incidents by logging and reviewing appropriate data and having a predefined threshold of what makes an incident become a breach.

Containment: Minimize the loss and/or theft of information, or service disruption.

Eradication: Eliminate the threat.

Recovery: Restore affected services and data sets to pre-incident form quickly and securely.

Post-Incident Activities: Assess the response to better handle future incidents through utilization of reports, "lessons learned," and after-action activities. Mitigate exploited weaknesses to prevent similar incidents from occurring in the future.

It's important to note that incident management isn't always completely linear. There are some aspects of working through a hacking or data breach incident that require continuous consideration. Cross-cutting elements present throughout an incident response plan include:

Communication: Notify appropriate internal and external parties and maintain situational awareness.

Analysis: Examine available data to support decision-making throughout the incident management lifecycle. Make sure that you have the necessary information available to determine indicators of compromise, as well as what data sets have been affected (this could have a significant impact on notification requirements).

Documentation: Record and time-stamp all evidence discovered, information collected, and actions taken from Identification through Post-Incident Activities.

Help is Available

Having cybersecurity professionals on retainer can lighten the burden on your organization. Cybersecurity and forensic services can be placed on standby to safeguard your data, respond to immediate threats, and mitigate future risks. With a service such as **CYBERVEIL**™, your organization is a priority should an event occur.

Whether you need to get your IT staff up to speed and train employees to thwart social engineering attempts, or your organization requires full-time monitoring and response services, P&N can help. Incident response planning is too important to put off. Don't wait until a successful hacking attempt creates a crisis.