So Your Organization Just Suffered From A Cyber Incident — What Now?

HERJAVEC GROUP

As business and security professionals, we acknowledge that a cyber incident is inevitable.

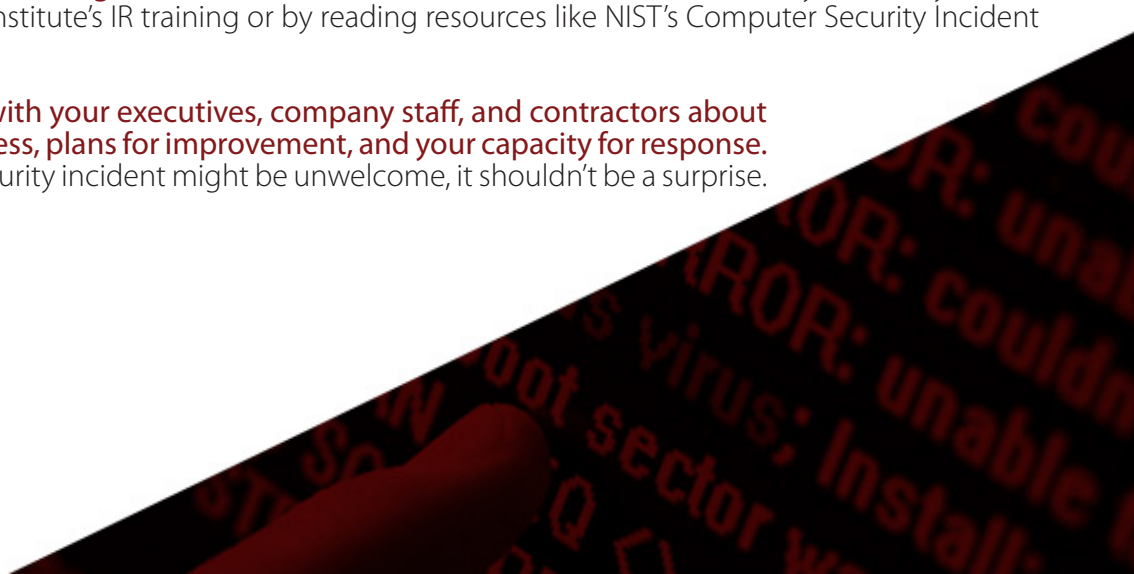
While we balance technology investment, internal process and access controls, it is imperative that our proactive defense strategy also includes the preparation of a comprehensive incident response plan.

After all, emergency preparedness is the difference maker as organizations seek to reduce financial and reputational damage following a breach.

So how can organizations prepare for an incident?

Consider our 10-point plan below as a foundation for incident response:

1. **Don't wait for a breach to get ready.**
2. **Understand your business, and what is critical, important, and meaningful.** Document where those important things are stored, how they're protected, and what the cost and impact is if they're lost or stolen.
3. **Prioritize Security Awareness Training internally.** Ensure that employees across all levels of your organization understand that it is their job to help support the company's security posture.
4. **Create policies, procedures, and guidelines for handling information security incidents.** Create practices for communication by involving your legal departments, staff, law enforcement and customers. Develop and document escalation and authority structures.
5. **Ensure you have visibility into the critical activity and behavior in your environment.** Review how you are receiving and digesting this information, as well as which stakeholders within your organization receive, provide input on, or action the data.
6. **Make incident detection and analysis a core competency for your security program.** Visibility into the data and events occurring on the network and within the data repositories is critical since preventative controls can fail.
7. **Develop and understand your capacity for response.** Hire, contract, or allocate resources that are trained and have the necessary tools and experience in incident response. Develop a plan and process to understand and react to extended incidents, or major incidents that exceed the skill level and capacity of internal staff.
8. **Practice and learn.** Even if you are having regular "live-fire" incidents, review your plan yearly and do simulations to create a continuous improvement cycle.
9. **Leverage expert advice and guidance.** In addition to advice from a trusted security advisor, you can learn a lot from SANS Institute's IR training or by reading resources like NIST's Computer Security Incident Handling Guide.
10. **Talk early, and often, with your executives, company staff, and contractors about your program's readiness, plans for improvement, and your capacity for response.** While discovering a security incident might be unwelcome, it shouldn't be a surprise.



So Your Organization Just Suffered From A Cyber Incident — What Now?

Preparing for an incident is the first step, but how will your team respond to the real thing? Matt Anthony, VP of Incident Response stresses that order, process, and a sense of calm are critical during an incident. "If your team is tired, or stressed there will be a real difficulty in making good decisions," he states.

Once an incident has occurred, our Incident Response experts recommend following the guidelines below to ensure your business can be brought back to normal operation as quickly as possible:

1. Stay **CALM** — **C**ool, **A**nalytical, **L**ogical, and **M**ethodical.
2. Don't take any action without assessing the risk factor of the incident, including the risk of escalation and the risk to your business. If there is a ransom demand, we advise against giving into the demand of cyber criminals, as this does not guarantee your systems will be restored.
3. Do not communicate any information without intent. Keep information on a need-to-know basis. However, your executive management should be notified of the incident immediately.
4. Assemble your management and technical incident response teams and use their shared expertise to determine how to proceed.
5. Build documentation with a timeline of the incident, answering questions such as: What is known? What needs to be known? And What are the required approvals for any future actions that need to be taken?
6. Assess the severity and impact of the incident – with business input and guidance. Ensure that you are constantly revisiting this step at every opportunity.
7. Create plans for scoping, containment, and remediation steps, and then execute them. Even if urgent response is required, take the time to fully consider your options. If your organization has an incident response playbook, follow it accordingly.
8. Suspend all scheduled changes to all affected systems until the incident is resolved.
9. Preserve evidence! This can include system state, network logs, application logs, firewall logs, VM copies, etc. Everything that can be preserved, should be.
10. Take note of all the error messages or other symptoms on your technologies and search the Internet to gain more visibility into the nature of the incident. If it's a ransomware attack or known exploit that affects certain software you use, there may be known security patches available.
11. Lastly, get professional help if you need it. Use Incident Response specialists if you don't have the right capabilities trained and ready to respond right away.

At Herjavec Group, we stress the importance of being prepared. Consider the recommendations above as you are preparing in advance of an incident and while you're triaging a live event.

To learn more about Herjavec Group's Incident Response and Remediation services, please visit: https://www.herjavecgroup.com/services/remediation-services/.