GreyCastle security

INCIDENT RESPONSE AND YOUR BUSINESS

You will experience a cybersecurity incident. Being prepared isn't just for big organizations. While the threat level is escalated and the impacts are ever increasing, the steps to prepare are well-known and doable.

Your business is critical to you, so why would you treat it any differently?

TIME IS MONEY...

The above is especially true when it comes to incident response. The faster an incident or breach is identified and contained, the lower the cost to the organization. In the Ponemon Institute's "2018 Cost of Data Breach" study, they found that the average cost for each lost record in a breach was $148. Their research found that deploying an incident response team reduced the cost by as much as $14 per compromised record.

And if that incident response team is working quickly? The report noted that companies that contained a breach in less than 30 days saved over $1 million versus those that took more than 30 days.

THE FIRST 24 HOURS...

A tiered response plan can help prioritize actions in an escalating situation. A serious breach may require digital forensics as well as legal and public disclosures.

Sticking to your incident response plan will be key to remediation. Your incident response team should work quickly to identify and contain the incident. Their work will help terminate the activity. The first step is often to isolate affected systems and, if necessary, deploy backups to ensure business continuity. This may be followed by the need to perform a risk analysis and determine if there is a need to shut down critical systems.

Communication components of the incident response plan will be triggered as your response team works on containing the incident. Information about the incident needs to be shared with executive leaders, the board of directors, legal teams, public relations, and other impacted departments. These discussions, particularly those between senior leadership and legal, will evaluate the requirement to disclose the breach to relevant stakeholders and/or the public.

Post-crisis, your incident response team will likely collaborate with your legal team and compliance officers.

4 TIPS FOR A MORE EFFECTIVE INCIDENT RESPONSE PLAN

- ☑ **Prepare for the most likely scenarios.** Don't waste time preparing for security events that aren't likely to affect your organization
- ☑ **Identify your priorities.** What people and tools do you need to have available to deescalate an issue? What is the most important need that should be addressed first?
- ☑ **Have skilled resources, ready and able to start deploying solutions immediately.** You need the tools, but it is just as important to be skillful in utilizing them.
- ☑ **Review your incident response plan annually.** Don't risk your security, compliance, or even your job on outdated procedures. This is a continuous process.

AFTER THE INCIDENT...

Just because the incident has been contained and remedied doesn't mean the work is over. Take the time afterward to ask the following questions:

- Have we completely recovered?
- Why and how did this security incident happen?
- What can we do to prevent this in the future?
- How can we improve our cyber incident response plan based on this occurrence?

You won't be able to predict when you will experience an incident, but having the ability to respond swiftly and skillfully could make the difference between a successful outcome and a total loss.

Are you ready to face a security incident? Email GreyCastle Security at intel@greycastlesecurity.com or call us at (518) 274-7233, and we can help you develop an incident response plan that ensures the resilience of your business.

IF YOU'RE CURRENTLY EXPERIENCING A SECURITY INCIDENT, CALL GREYCASTLE SECURITY IMMEDIATELY AT (800) 403-8350.