GreyCastle security

INCIDENT RESPONSE AND DISASTER RECOVERY

Nothing is 100% secure. Ever. An organization should expect adversaries getting past their network perimeter. The question is:

How fast can we detect these intrusions and how fast can we eradicate them?

If your business goes away, we all suffer. We must be prepared to respond to and recover quickly from cyberattacks. We need to mitigate the initial attack with a meaningful and practiced incident response plan and need an effective way to recover data and information systems. It's never too late to get started and there's no good reason to put it off. Even a bad plan is better than no plan. And a practiced plan is even better.

A GOOD INCIDENT RESPONSE PLAN WILL:

- Take your current network infrastructure into account, including system architecture and information flows. It should also identify vulnerabilities and points of attack.

- Assign roles and responsibilities to predetermine who does what in the event of a cyberattack or breach. This can include technical staff, media outreach, legal, and executive sponsors.

- Provide for a communication strategy. Your incident response plan should specify who will handle internal communications with personnel and clients as well as external communications with the media or mandated reporting agencies.

- Define response requirements and timelines. Everything from what resources are needed to contain the security breach to what the minimum response times are.

- Be tested regularly. An incident response plan shouldn't be a "check the box" initiative. Routine testing can help your team to better execute, develop a sort of muscle memory, identify the latest vulnerabilities and create solutions to fix these problems.

A GOOD DISASTER RECOVERY PLAN WILL:

- Include a business impact analysis (BIA). The BIA will help your team determine how much data your organization is storing, where it is located, and how critical it is to the operation of your business. It also allows you to set standard metrics for determining how much a disruption impacts the organization and how long the business can survive without this data.

- Compile an inventory of all hardware and software, in priority order.

- Establish recovery time objectives and recovery point objectives.

- Ensure that all vendors and service-level agreements account for disasters. This should be a binding agreement that defines what level of service will be delivered in a disaster situation.

- Define procedures to safeguard sensitive information during the recovery process.

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