AUDITING

SBS CyberSecurity

INCIDENT READINESS ASSESSMENT

PROACTIVE PREVENTION AND PREPAREDNESS

You invest time, resources, and energy to prevent a cybersecurity breach at your organization, but as we've seen far too often, no defense strategy is bulletproof.

What happens when a cybercriminal finds a hole in your defense? How long would it take your organization to discover there had been a breach? How would you know an incident had occurred? Who's in charge of each step of the response? Rapid action is critical in a highly stressful cyber-attack scenario. Not being able to confidently answer those questions opens an organization up to insurmountable financial and brand damage.

The Incident Readiness Assessment is a proactive approach to cyber incident prevention and preparedness. The assessment will evaluate your organization's ability to detect, respond, and recover from an incident by focusing on the key elements of an incident response program - people, process, and technology.

- The readiness of the **people** in charge of responding to an incident.
- The **processes** in place to mitigate the effects of an incident and resume operations.
- The **technology** designed to prevent and detect when an attack is occurring.

SPEAK TO AN SBS SOLUTIONS EXPERT TODAY!

sales@sbscyber.com | 605-923-8722 | www.sbscyber.com/auditing

Mature Your Incident Response Program

Get an unbiased review of how prepared you are for an incident and recommendations to mature your incident response program. The NIST Incident Response framework is the foundation of the assessment and includes, but is not limited to, reviews of the following:

- The **team** you have in place to respond to an incident, including internal employees, outsourced vendors, legal representation, and insurance coverage.
- The **plans and processes** you have in place with how to respond to a cybersecurity incident, including incident response plan, escalation, testing, change management, and access control.
- The **technical controls** in place to prevent and/or detect cyber incidents, including identification/alerting and containment/eradication.

Risk-Rated Recommendations

Following the assessment, you will receive a report containing risk-rated recommendations that give you an idea of the order in which to implement them.