Incident Response – Planning and Exercise

What is a Cybersecurity Incident?

A Cybersecurity Incident is any event in an information system or network that poses a threat to a computer or network security. The SANS Institute defines an Information Security Incident as "*an adverse event that negatively impacts the confidentiality, integrity and availability of information that is processed, stored and transmitted using a computer*". Having an Incident Response Plan in place and exercising your plan are key actions necessary to help organizations minimize the impact of a cyber incident. **An Incident Response (IR) Plan** is a collection of processes and procedures that outline how an organization will respond when a cybersecurity incident occurs.

Why is Incident Response Planning Important?

Security incidents happen, it is only a matter of time. When a cybersecurity incident occurs, response time is vital to minimize, or limit damage incurred, to reduce recovery time and costs associated. The old adage "If you fail to plan, you plan to fail" is especially true for cybersecurity incident response. Breaches occur daily and can cost millions of dollars as well as irreparable damage to reputation. Having a comprehensive and well-rehearsed IR Plan enables organizations to respond quickly and efficiently. Furthermore, exercising the IR Plan on a routine basis familiarizes staff with their roles and responsibilities. It also allows for continuous process improvement and targeted plan development.

How Does TechGuard Approach Incident Response Planning and Exercise?

At TechGuard, our incident response planning approach is derived from Center for Internet Security (CIS) Control 19; an eight-step framework that addresses every aspect of an IR Plan. This approach provides an adaptable, customizable framework to meet the unique needs of each organization we serve. Cybersecurity incidents can be categorized in many ways, ranging from theft of a laptop to a server infected with a virus or even a data breach. Each type of incident will have a different approach and varying levels of communication required. In all cases the primary source of guidance will be the Information Security IR Plan. At TechGuard, we not only help organizations devise IR plans, we also develop and oversee tabletop exercises. These exercises allow organizations to put their current plan to the test in a low stress situation – providing all parties time to think through their actions to ensure they are aligned with their responsibilities as defined in the IR Plan. Throughout the exercise, constructive feedback is provided to strengthen the plan or improve current processes.

What is the TechGuard Difference?

We pride ourselves in building and maintaining long-term relationships with our clients. This ensures each client receives a tailored, customized service based on their unique organizational needs. From the initial kickoff meeting to delivery of the finalized Incident Response Plan or Exercise Assessment Report, client satisfaction is our number one concern. At TechGuard, we place the utmost value on the delivery of quality services. Every client is assigned a Project Lead who will serve as their single point of contact throughout the engagement. In addition to the detailed written report provided at the end of the assessment, clients engage in a presentation with their Project Lead. Our report delivery presentation provides the opportunity to discuss details of important action items, next steps, and answer any questions related to remediation recommendations. TechGuard has dedicated the past 18+ years to delivering high-end, professional cybersecurity solutions - making us a trusted partner in both the government and private sectors.