BlueVoyant

CASE STUDY:
INCIDENT RESPONSE PLAN

Cyber Events Require Organizational Response

1. RESOLUTION REQUIRES COORDINATION

Cybersecurity events are not resolved in a vacuum. Resolution often requires a joint effort between technical and non-technical teams in order to address all facets of risk posed to the organization.

2. PREPARATION IS KEY TO RISK REDUCTION

During a cybersecurity event, time is of the essence with risk and liability the organization faces increasing by the minute. Preparing for these types of events is one of the best ways to streamline response and reduce risk.

3. RESPONSE IS ORGANIZATION SPECIFIC

Organizations differ in the way they operate within their industry, as well as differ in the critical assets they aim to protect. Response plans must be customized and optimized for each organization.

INCIDENT RESPONSE PLAN

Our incident response plans bridge policies with each of the processes required for an organization's streamlined response to a critical incident. This involves defining incidents and severity levels for critical events, identifying stakeholders and point of contact information, and developing communication templates to increase response times and information sharing. When performed alongside our MSS implementation, it provides the connective tissue that bridges technical and nontechnical incident response processes with our MSS service.

	Type	Purpose	Benefit	Example
Strategic	**Policy**	Establishes the overall governance for a function. It defines why a function exists, its intent, and framework.	Alignment with Organizational Objectives	**Information Security Policy**
	Plan	Formalizes the operating model for a function. This includes scope, phases, roles and responsibilities, and PoCs.	Standard for Operational Implementation	Disaster Recovery Plan **Incident Response Plan** Business Continuity Plan
Operational	**Process**	Defines a phased approach for generating targeted outcomes to include resources, inputs, outputs, and information flows.	Systematic Understanding of Operations	Escalation Process **Response Process** Communication Process
	Playbook	Outlines a methodology for specific scenarios. This includes process flows, decision points, and integration.	Efficient Execution of Operational Tasks	Fraud Playbook **Ransomware Playbook** Insider Threat Playbook
Tactical	**Procedure**	Detailed sequence of action between two or more entities required to carryout a specific task.	Optimized Repeatable Tasks	**Host Containment Procedure** **Network Isolation Procedure** **System Reimage Procedure**

CASE STUDY

Client Challenges

A privately owned real estate company, upgrading to our MSS offering, had previously integrated IT and IT Security response plan. Foreseeing expansion in the coming years, the organization sought out a response plan that optimized operations and could grow with the organization.

Approach

Modular Design and Integration
Segmenting IT Security response, now updated with our MSS offering, from traditional IT response enabled more granular descriptions of the overall function. This level of granularity allowed for defined connection points and trigger criteria for IT and broader organization response plans and processes.

Organization Specific
Defining severity levels and criteria for cybersecurity events and aligning those with existing classification criteria within different departments so everyone spoke the same language.

Streamlined Processes
Creating communication templates and developing call trees across the organization for rapid coordination.

Results

The organization experienced a physical security event at one of their data centers and was able to utilize the Incident Response plan's communication templates, call trees, and touchpoints with the legal crisis communication plan and HR's quick termination process to resolve the event within hours with minimal effect to the organization.

For more information please visit:
www.bluevoyant.com

Secure your business now:
sales@bluevoyant.com

About BlueVoyant

BlueVoyant is an analytic-driven cybersecurity company whose mission is to protect businesses of all sizes against agile and well-financed cyber attackers by providing unparalleled visibility, insight, and responsiveness. BlueVoyant provides Advanced Threat Intelligence, Managed Security Services and Incident Response through offices in the United States, the United Kingdom, Israel, and Spain.