THE SafeHarbor™ BRIEF

Gnostech Inc. Maritime Cybersecurity Newsletter - October 2018

ESTABLISHING COMPANY GUIDELINES AND POLICIES

Plans and Policies - PART 2

Building upon topics from last month's newsletter, we will continue our discussion on plans and policies. This month, we will cover additional elements your organization might consider as part of your security plans and policies, including intrusion detection and continuous monitoring, remote access, physical security, auditing, incident response, and risk assessment policies. Remember, policies are high-level documentation that establish the outline of your program, and plans are the more detailed process of how your company plans to establish and follow your written policies. The elements recommended here and in the previous newsletter do not cover all the components of a potential security plan, but the ones Gnostech has mentioned are highly recommended to meet the National Institute of Standards and Technology (NIST) standards.

Intrusion Detection and Continuous Monitoring

Intrusion detection is the use of a computer system or application to monitor your company's computer systems and network traffic for malicious activities. Continuous monitoring is a process to manage risk within a company's enterprise network by using security applications to provide a real-time assessment of implemented security controls. Continuous monitoring not only checks your cyber assets but your personnel as well to ensure that established security policies are effective.

Intrusion detection and continuous monitoring policies should establish technologies to detect malicious anomalies within your network, as well as personnel responsible to respond to such an event; this policy will typically point to an Incident Response Plan (IRP) for instructions to handle an incident. This is where you will establish your continuous monitoring process for your company's cyber assets. The intrusion detection and continuous monitoring plan should provide further detail on how your technologies listed in the policy are used, the frequency with which they are updated and monitored, and the steps to take in the event of a potential intrusion (which should point to your IRP).

Remote Access

The remote access policy is used to establish guidelines to determine if company personnel can connect to the enterprise network when they are not physically connected (on-site, in-person). If you prefer personnel to not have remote access, a policy should be in place stating that it is prohibited. It is highly recommended that personnel with access to your network connect through a secure virtual private network (VPN), and the policy should accurately document who has access and detail in what instances a remote connection would be allowed.

Physical Security

A physical security policy is used to establish the mechanisms in place to physically protect personnel, cyber assets, and the data that resides on your cyber assets. Physical controls include lighting, fencing, camera systems, personnel verification (security badges), and security guards. This policy should also identify how to respond to physical threats during any event that could prove harmful to your company personnel and assets, as well as identify personnel responsible to notify local authorities (police, firefighters, etc.).

Auditing

The auditing policy will cover a wide range of topics such as technical assessments of implemented cybersecurity measures. This will maintain appropriate paperwork on

personnel training, account access requests, and personnel signed acceptable use policy paperwork. The cybersecurity measures should identify how logs are maintained and stored. This would include the length of time such logs will be kept in addition to how to maintain and secure a record for all signed documents. The process to update and maintain all company policies should be included in the auditing policy.

The following are elements a company should consider when putting an auditing policy together:

- How to maintain and safeguard personnel records and personnel signed documentation
- What security logs to capture from cyber assets and how long to maintain them
- Test personnel periodically to ensure they are aware of processes to protect their personnel data and company assets

Auditing covers a large range of subjects that can be detailed in their respective policies and plans. Topics should be identified at a high-level in the auditing policy while pointing out which policy or plan the detailed process can be found.

Incident Response

Given the risk-based approach to cybersecurity and that there is no such thing as a system that is 100% secure, management is advised to create a proactive plan to address physical and cyber incidents. At the policy level, roles and responsibilities should be established for personnel, as well as basic steps to take if an incident has been identified. It is recommended that you create a "cheat sheet" for personnel to keep at their desks detailing how to respond to an incident (escalating the problem). Personnel should not attempt to address the issue themselves and should escalate the issue through an established process. In most instances, employees would notify their cybersecurity team or security administrators. The IRP should provide a more detailed approach on how the company will handle incident response, both proactive and reactive.

Here are some considerations for your IRP:

Types of incidents - Create a system to identify the type of incident when they occur. This can include separating potential incidents: a physical incident, cyber related (worms, viruses, etc.), or personnel related (insider threat).

Severity Level - Establish severity levels to determine if the risk posed by the incident is considered minor or catastrophic, and has the potential to bring down your enterprise network. Severity levels can be established based on the type of incident.

Responsibilities - Determine who is responsible to respond to the different types of incidents and detail the process to fix or mitigate the incident.

Documentation - Create a process to document all incidents. This documentation should be detailed from start to finish and include information on who identified the incident, time of incident, time of reporting, whether your intrusion detection systems detected it, whether anti-virus identified it, the severity level, escalation procedures, steps to correct the incident, and how long the affected systems were impacted. Gnostech advises organizations consider documenting and collecting information with the thought that a criminal investigation will be initiated. In this scenario, proper evidence handling techniques should be followed.

Lessons Learned - After every major incident, a "lessons learned" report should be created to help ensure the problem does not persist and is protected against in the future. This document should become a part of the IRP and is integrated into your cybersecurity measures.

The IRP is a living document that should be updated frequently with steps to protect the company against any newly identified threats. The initial plan will be a concept to help prevent incidents, but will grow over time as threat patterns are detected and new threats arise within the cybersecurity community. Never assume that your network is impenetrable. There is always a chance, and your cybersecurity team should be ever vigilant in the protection of your company's enterprise network.

About Gnostech Inc.

Gnostech Inc. is an applied engineering and consulting company with over 35 years of experience and expertise in information assurance and cybersecurity engineering, and major combat and space systems development and integration. Gnostech provides the necessary knowledge and technology to ensure success of critical missions for customers in both the defense and maritime industries. To learn more, visit www.gnostech.com.

Only 37% of organizations have a cybersecurity response plan

- DVN GL