# THE SafeHarbor™ BRIEF

Gnostech Inc. Maritime Cybersecurity Newsletter - August 2018

## COMBATTING COMMON USER THREATS

### *Best Practices - PART 2*

As a continuation of last month's newsletter, we will discuss general best practices to ultimately improve the security posture of your organization and its enterprise network.  Part 2 of our Best Practices series will cover implementation of an anti-virus solution, the components of physical security, and how to establish an incident response policy and plan. This overview will help prevent an incident from occurring, as well as plan for when an incident does occur and how to respond appropriately.

These best practices will help save your company time and money when dealing with cyber incidents; the faster a threat or incident can be identified and remediated, the less impact there is to your business operation.

### *Anti-Virus*

Implementing an anti-virus solution for your company is considered a best practice, and provides another layer of protection in your defense-in-depth strategy. User education is vital when it comes to training your personnel against clicking on potentially harmful email attachments and embedded URL links. Pairing an anti-virus program with user education can increase your company's overall security posture as both are designed to identify common worms or viruses and strip them from your email or system before doing any damage to the computer system. Further, ensuring that your cyber security personnel or system administrators frequently update the anti-virus engines (think of it as a plug-in or software update) can help identify new worms or viruses. The goal is to stay ahead of cyber threats before they damage your company's enterprise network.

### *Physical Security*

Physical security describes security measures that are designed to deny unauthorized access to facilities, equipment, and resources, and protect personnel and property from damage or harm (such as espionage, theft, and terrorist attacks). Physical security can be very broad and is subjective to the company's goal, size, and data processed.

Physical security measures can include:

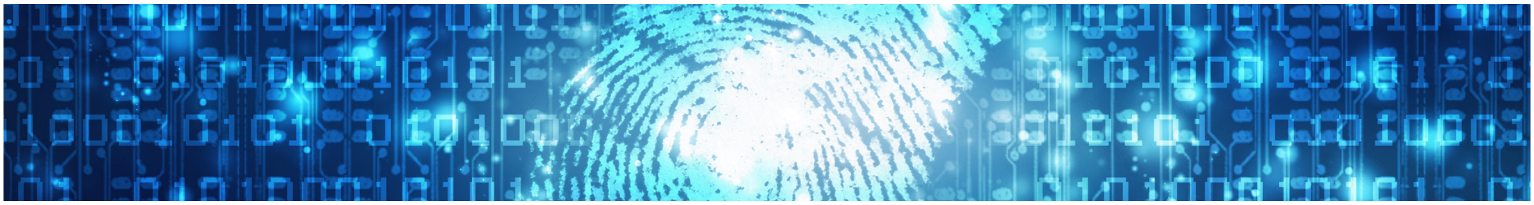
**Perimeter controls** – Consider implementing fences on property border and bollards to prevent the possibility of vehicles ramming the building.

**Building controls** – Consider implementing lighting for property grounds, video cameras, and alarms in addition to requiring badge access to buildings, mantraps, and security guards.

**Data controls** – Consider segregation of system access through security cards (users should only have access to areas where they have required access to perform their duties, especially server

## Many Unaware

*According to a survey conducted by Futurenatics, only 43% of crew members were aware of any cyber-safe policy or cyber hygiene guidelines provided by their company for personal web browsing or the use of removable media.*



rooms); utilize hardware locks to prevent theft of laptops; lock all sensitive data, paper or removable media (CDs, hard drives, flash drives, etc.) in a fire-proof safe.

**Removable Media –** It is highly recommended that companies create and implement a "Removable Media Policy" to prevent the use of removable media for standard users. Not having a policy in place could introduce cyber threats to a company's enterprise network through unintentional negligence. For instance, a user could save a document from their work computer to finish their work at home; by plugging into a computer system outside of the company's control, a user could inadvertently load a virus to their removable media and then upload it to the company's network the next day. Removable media should only be used by cyber security personnel or security administrators sparingly, and it should require their administrative credentials to move data between systems.

## *Incident Response Policy and Plan*

Companies should create an incident response policy to help identify personnel responsibilities in the event of a security incident, whether through a cyber-attack or physical attack or incident. The policy should define what constitutes a security incident and the required response procedures. An incident response plan (IRP) builds upon the incident response policy and provides details on how to respond to incidents. The difference between the incident response policy and incident response plan is that the policy is developed with procedures to help prepare for and prevent incidents. On the other hand, the plan is to provide guidelines on how to react during and after an incident has already occurred.

A comprehensive IRP should include the following elements:

**Define incident types –** Helps your personnel quickly identify the type of incident or if the cyber event is a false positive.

**Roles and responsibilities –** Who does what during an actual incident response. This section should be detailed by listing out personnel by name and what their exact role is during an incident response.

**Identify the cyber incident response team (CIRT) –** This defines a group of personnel trained specifically in incident response procedures to quickly maintain cyber incidents.

**Escalation and reporting requirements –** Determine how and when to escalate a cyber incident. This section comes with experience from your cyber security team and knowing when to escalate the problem up the management chain. Day-to-day cyber incidents such as viruses on user computer systems may not warrant any escalation outside of the cyber security team (except as a report metric), but if the incident has affected a critical component of your network infrastructure, then it needs to be reported to senior management. The company IRP should include who users should report incidents to and how to report them. The determination to escalate an incident should be left to the discretion of cyber security personnel or security administrators.

**Exercises and lessons learned –** Test your IRP regularly through controlled exercises within the company.

Another crucial part of your IRP is going to be the procedures and steps taken to handle a cyber incident. These procedures should include:

**Preparation –** Maintain and update the IRP regularly and help identify and prevent incidents.

**Identification –** Determine whether an event is a real incident or a false positive.

**Containment –** Isolate an incident to minimize damage to the enterprise network.

**Eradication –** Procedures on how to remove the incident from your systems. In the case of malware, this procedure would include getting rid of all file paths, call backs, and registry entries created by the malware to ensure the computer system is clean.

**Recovery –** After the incident has been eradicated, this step returns the affected system to its normal operating state and back onto the enterprise network.

**Lessons Learned –** After every real cyber incident, the lessons learned during the incident should be incorporated into your company IRP to help identify and prevent the same incident from occurring again

## *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.