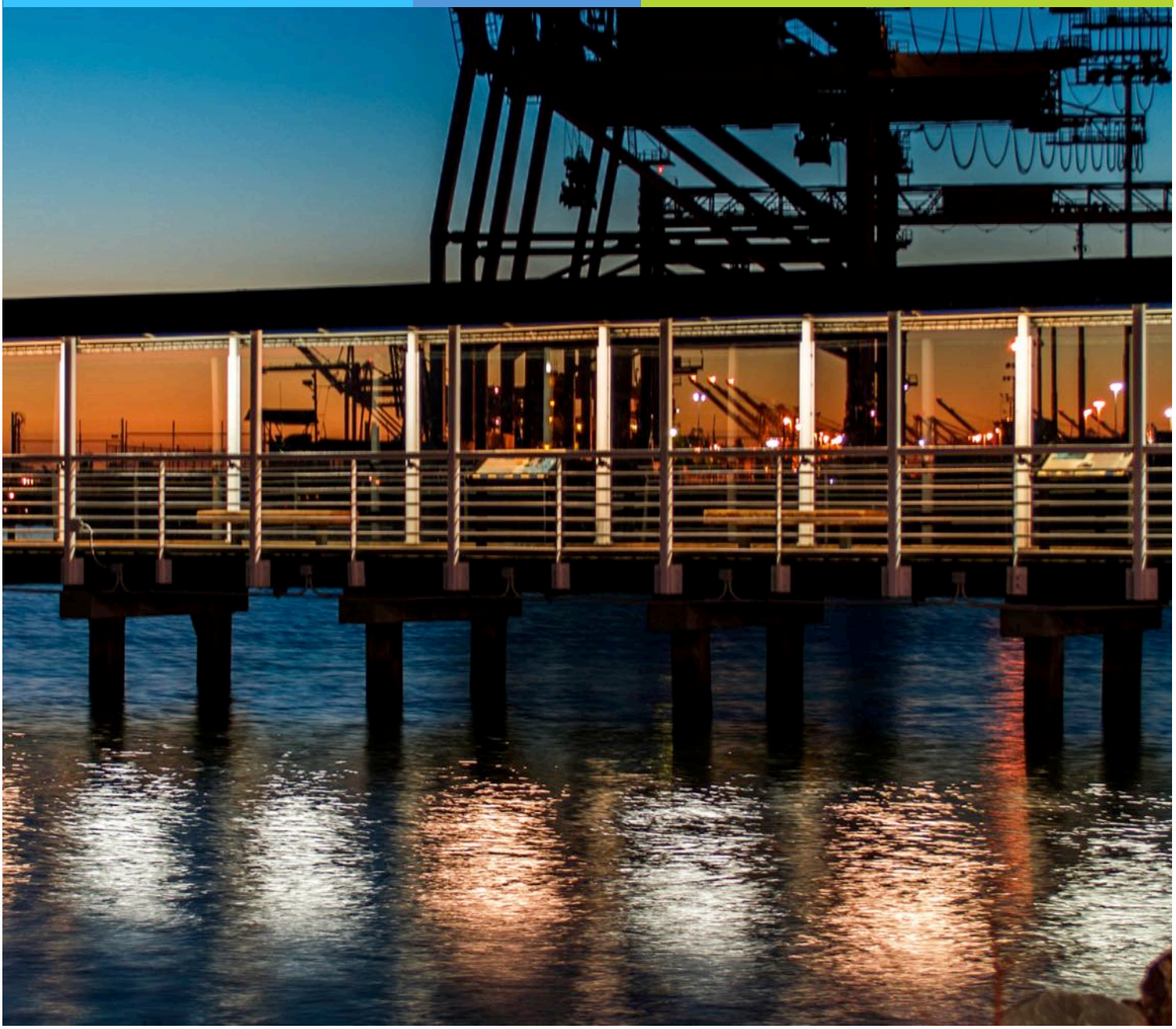
Cybersecurity Education Series

Cybersecurity 101

Cybersecurity Defense Solutions



Understanding Cybersecurity

Cybersecurity involves "threat actors" that want to obtain unauthorized access to your data and systems, and how individuals and companies can defend against these attacks. It is our goal to educate people of all disciplines about Cybersecurity and how we can all make a difference.

Cybersecurity is everyone's responsibility. Technological solutions alone cannot combat the problem. Education is a powerful ally in the fight against Cyber attacks.

It is our goal at Cybersecurity Defense Solutions to provide free for use educational tools to assist companies and individuals in recognizing and responding to a Cyber attack and what can be done to prevent it. These CDS Cyber Educational Series handouts are one of these tools.

Who are the Threat Actors?

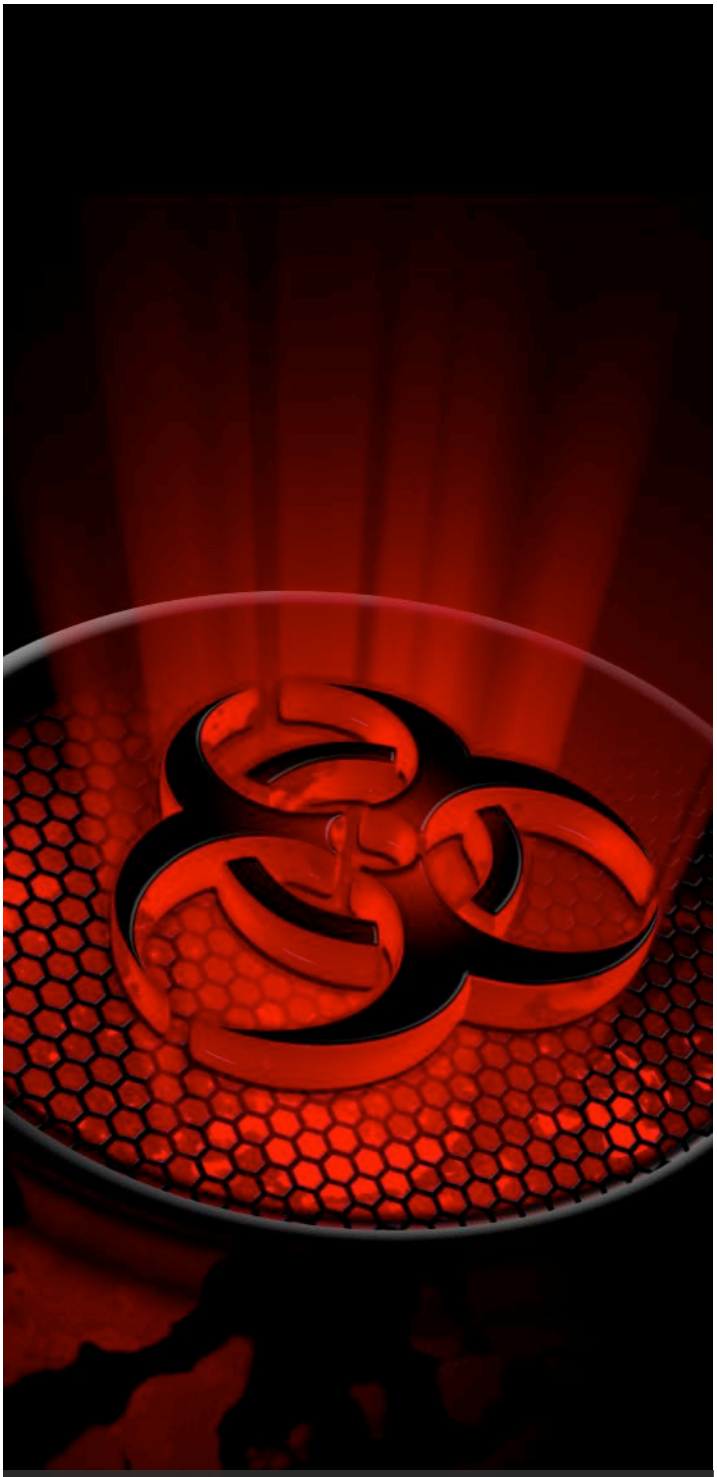
Threat actors come in many different forms, some obvious and some not so obvious. These include:

- Insider Threats (employees, vendors and other generally trusted individuals)
- Hackers
- Cyber-criminals
- Foreign Governments and Intelligence Agencies
- Terrorists
- Organized Crime
- Hacktivism Groups (i.e. Anonymous)

What are the Threat Actors after?

Threat actors want your data and secrets, and/or to blackmail/extort money from you (in the end it comes down to money). This data includes:

- Usernames and Passwords
- Sensitive company documents
- Protected Health Information
- Credit Card and Banking/Financial information
- Export Controlled Technologies
- Intellectual Property and sensitive technological documents
- Personal Identifying Information
- Contact lists (emails, phone directories, etc)
- Confidential Emails



Cyber Attack

Realize that no matter how good your technological defenses, a determined attacker will most likely breach your network.

According to the Ponemon Institute study, 37% of data breaches globally were Structured Threats (malicious or criminal attacks). 35% were caused by a "human factor", i.e. a negligent employee or contractor and 29% were caused by glitches that include both IT and business process failures.

How do Threat Actors compromise or "hack" our systems?

There are many methods that threat actors use to gain unauthorized access to systems. These methods include:

- Malware/Viruses
- Social Engineering (talking, convincing or tricking someone trusted to give a threat actor access to a system over the phone, via email, in person or through other means)
- Phishing or Spear Phishing (sending emails that look legitimate but have malicious links or attachments)
- Unpatched, outdated or vulnerable systems and software
- Baiting (removable media like USB drives)
- Use of weak or default passwords
- Cross Site Scripting attacks (bad websites that can infect your computer with malware/viruses)
- Stolen logon credentials

Of all these methods, the leader in system compromises from outside sources is Social Engineering. Getting a user to click on a Phishing email or give out credentials over the phone or email is how most data breaches start.

If an email looks suspicious or too good to be true, don't click on it. If a person you are unfamiliar with asked for your username and password or other details about your computer systems, verify with your supervisor or IT/IS department before disclosing such information, if at all.

Threat actors can be very convincing and persistent when using Social Engineering techniques. The best defense is an educated end user who questions and verifies before clicking or giving out information.

Understanding the general steps involved with a Cyber attack and knowing what to do to prevent one greatly reduces the risk of becoming a victim and limits the damage done in the advent of an attack.

Overview of a Cyber Attack:

The steps outlined below are general, many other methods can and are used, and some steps take an immense amount of time to execute as compared to others. The process outlined below is intended for a high level understanding of a typical cyber attack/hacking attempt.

1. ***Reconnaissance:*** Threat actors research (sometimes in great depth) individuals and companies with whom they are planning to target. They utilize a multitude of techniques, including gathering data from social media and other publicly available sources.
2. ***Intrusion/Delivery:*** Threat actors gain access to the network via vulnerable systems, social engineering, phishing, baiting, malware or other techniques to gain access to systems at the targeted location.
3. ***Exploitation/Obtaining Credentials:*** Once inside a network, threat actors will try and obtain user credentials, focusing on the "domain administrator" or "root" level access.
4. ***Pivoting/Lateral Movement:*** Once inside, an threat actors may try to move laterally within the network to install as many "back doors" as possible for future and continued exploitation.
5. ***Installation:*** Threat actors may install a multitude of malignant utilities to conduct system administration duties, steal passwords, take screenshots, steal email and infect/control other systems.
6. ***Data Exfiltration/Manipulation:*** Threat actors will obtain emails, documents, databases, files, etc. from victims servers and workstations, and encrypt and send that data to other malicious servers on the Internet. In addition, some attackers can encrypt and destroy your data, holding it "hostage" until a ransom is paid to de-crypt it and make it useable again.
7. ***Maintaining Persistence:*** Once attackers gain access to a network (which sometimes takes a very long time and a considerable amount of effort) they go through extreme lengths to maintain that access by installing additional or updated tools, unknown malware programs, adding additional unknown system accounts, etc. This is also known as Advance Persistent Threats (APT).

Things to do to help prevent a Cyber Attack:

Things you can do to help as an individual:

- Use a complex, alphanumeric password and if available, use two-factor authentication.
- Use different passwords for every site that you have access to and change your passwords regularly.
- Do NOT open emails or attachments from unfamiliar sources, even if they look official or important.
- Do NOT install or connect any personal software or hardware to your companies network or computer systems without permission from the IT/IS Dept.
- Do NOT run unexpected executable files from the Internet, even from websites that you trust.
- Do NOT give credentials or other information about your company or it's systems to anyone that is not authorized to have that information.
- Report all suspicious or unusual problems (pop-ups, pornography, ads, unusual system slowness) with your computer to the IT/IS department.

Things that Management and IT Personnel can do:

- Implement Cyber Defense-in-depth – look at People, Processes and Technologies that can enhance your Cyber defenses.
- Provide all your employees with Cybersecurity Awareness training on at least an annual basis.
- Implement and update technical defenses such as Firewalls, Intrusion Detection and Prevention Systems, Anti-virus/malware programs, Threat and anomaly detection, etc.
- Perform Vulnerability Assessments of all your network and IT systems at least semi-annually.
- Regularly perform and document security patch management processes and assure that they are followed.
- Change ALL manufactures default passwords on systems and software.
- Monitor, log and alert on attempted intrusions to your systems and networks.

Cybersecurity is EVERYONE'S responsibility! Most network intrusions go unnoticed for over 7 months! Report all suspicious cyber incidents to your IT/IS Department, manager and/or owner.

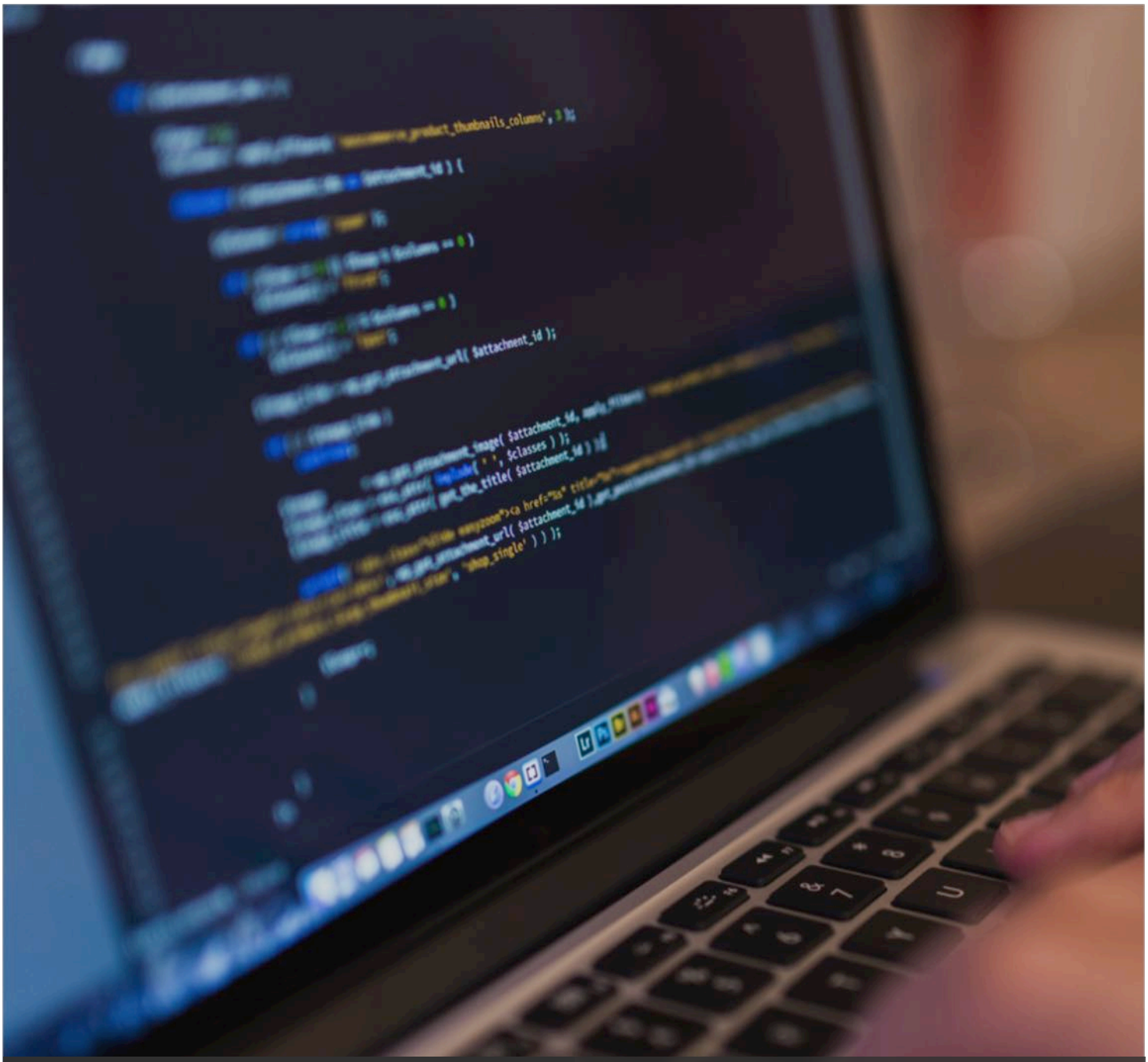
"Be aware that there are people and groups, many of them organized, sophisticated and well funded that want your data. They have the upper hand"

- CDS

Being diligent and reporting suspicious events can mean the difference between detecting an attack and remediating it immediately, or giving hackers access to your network and systems for months and months to steal data and cause damage. The following are some signs to look for and report your IS/IT Department, Manger and/or Owner:

- ***System Failure or Disruption*** – has your system failed or access to other systems disrupted? Has your company website been defaced or become inaccessible?
- ***Suspicious or over-zealous questioning*** – has someone either in person, over the phone or via email attempting to gain information such as usernames and passwords, network diagrams, software reports or other Cybersecurity information from you or a co-worker?
- ***Unauthorized Access*** – Are you aware of anyone (internally or externally) this is trying to gain or has gained unauthorized access to your systems or company systems/data?
- ***Unauthorized or unexpected changes*** – Has anyone made unauthorized or unexpected changes in hardware, software or systems?
- ***Suspicious emails*** – Have you or your co-workers received any suspicious emails that contain unsolicited attachments or requests for sensitive information (do NOT click on the attachment, ever!)?
- ***Unauthorized Use*** – Are unauthorized individuals (former employees, contractors, vendors, etc.) using your system or asking to use your system for any reason whatsoever?
- ***Strange System Behavior*** – Is your system behaving strangely (pop ups out of no where, mouse moving/typing on it's own, extreme/unusual system slowness)?

You are the first line of defense! Help protect your company's data and your data by reporting suspicious behaviors that may be related to a Cyber attack.



Cybersecurity Defense Solutions

13720 Jetport Commerce Parkway STE 13
Fort Myers, FL 33913

http://www.cybersecdefense.com