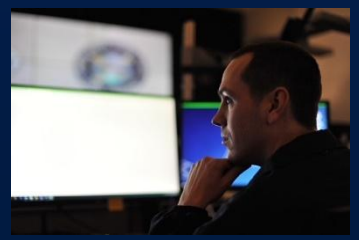


NAWE 2022

U.S. Coast Guard Cyber Command – Current & Future Threats to the MTS

CDR Kerry Feltner, CGCYBER

The Coast Guard Provides

Maritime Safety

Saving lives and
protecting property

Maritime Security

Establishing and maintaining
a secure maritime system

Maritime Stewardship

Managing the sustainable and
effective use of waters and resources

Today's Maritime Environment

95,000
Miles of Coastline

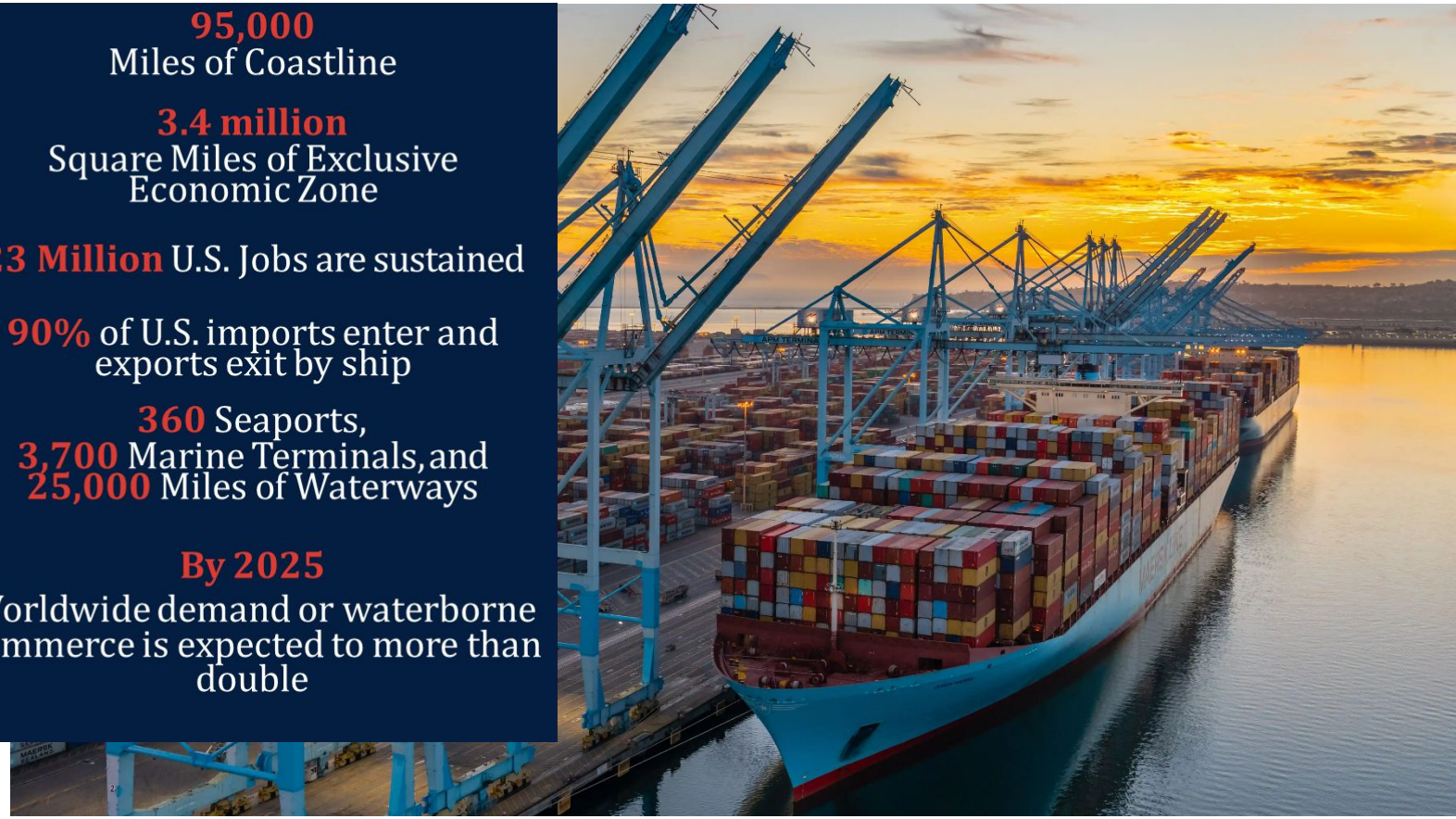
3.4 million
Square Miles of Exclusive Economic Zone

23 Million U.S. Jobs are sustained

90% of U.S. imports enter and exports exit by ship

360 Seaports,
3,700 Marine Terminals, and
25,000 Miles of Waterways

By 2025
Worldwide demand or waterborne commerce is expected to more than double



U.S. Coast Guard Lines of Effort (LOE)

LOE 1: Defend and Operate the Enterprise Mission Platform

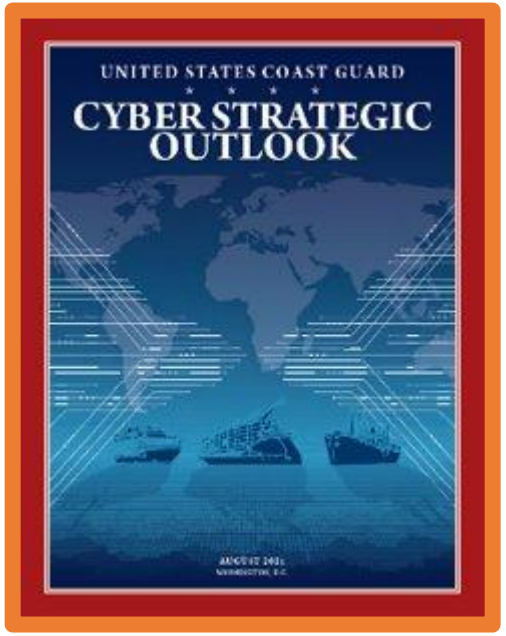
- The Coast Guard must defend and operate the U.S. Coast Guard Enterprise Mission Platform (EMP), its portion of the Department of Defense Information Network (DODIN), which includes Coast Guard technology.

LOE 2: Protect the Marine Transportation System (MTS)

- The Coast Guard must employ frameworks, standards, actionable intelligence, and best practices in prevention and response activities to identify and manage cyber risks to the MTS.

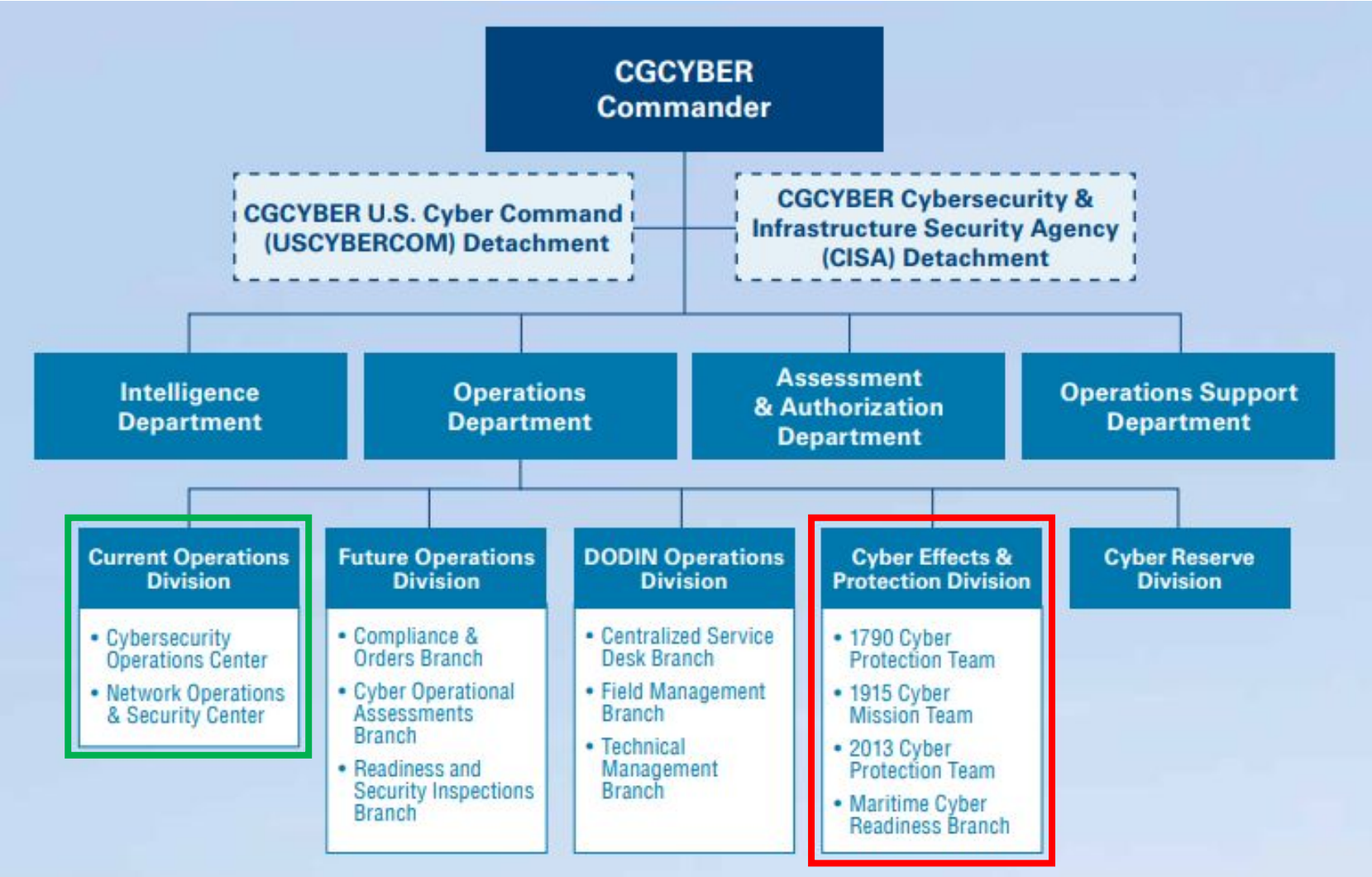
LOE 3: Operate In and Through Cyberspace

- The Coast Guard must implement cyber planning into traditional missions and execute collaboration across cyber operations that combines the Service's unique authorities, capabilities, and workforce to deliver mission success.

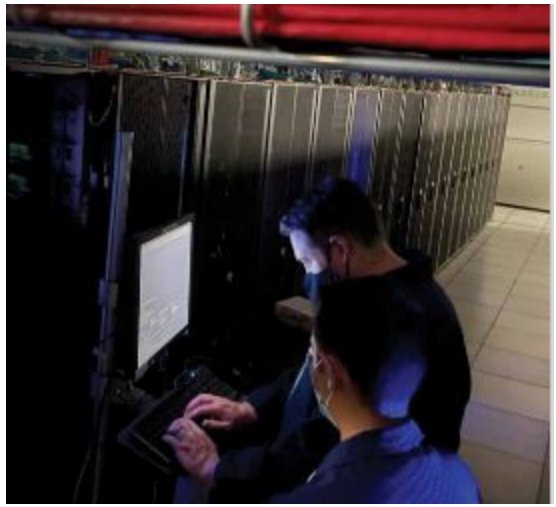


For more information visit www.uscg.mil/Cyber

CGCYBER Overview

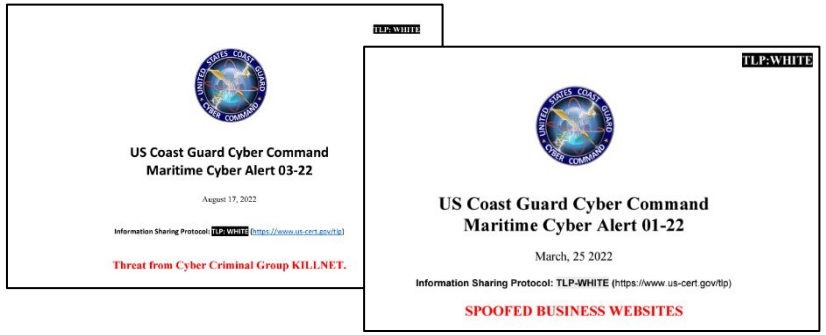


Coast Guard Cyber Protection Teams



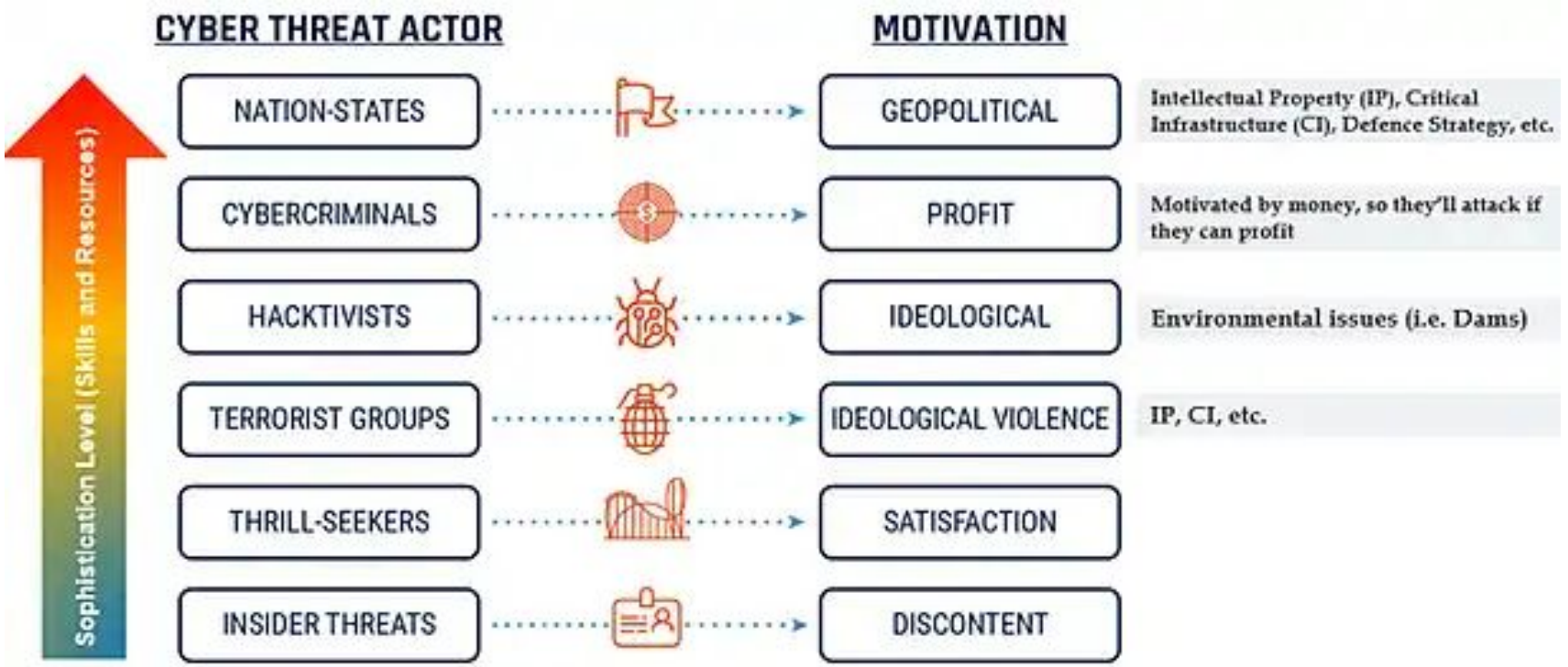
- **Assess**
  - Identify vulnerabilities and weaknesses in Critical Infrastructure **before** exploitation causes a major incident
  - Guidance and recommendations to secure and protect MTS networks
  - Provide situational awareness to Coast Guard leadership on cybersecurity risk posture of U.S. MTS Infrastructure
- **Hunt**
  - Discover yet-undetected adversary on MTS networks **before** the compromise impacts critical systems or services
  - Analyze malicious tactics, techniques and procedures
- **Incident Response**
  - Advise on mitigation & remediation steps and best practices
  - Forensic analysis to inform mitigation & remediation steps.
  - Assistance with integration of FBI, CISA & other agencies.

Maritime Cyber Readiness Branch (MCRB)



- Maritime Cyber Readiness Branch (MCRB)
  - MCRB provides guidance and mitigation tactics
    - Based on lessons learned from cyber incidents
    - Maritime Cyber Alert (MCA)
    - Marine Safety Information Bulletins
    - Maritime Commons Posts
    - https://www.dco.uscg.mil/Our-Organization/CGCYBER/Maritime-Cyber-Readiness-Branch/
    - maritimecyber@uscg.mil

Threat Actors



Source: https://gca.isa.org/blog/common-ics-cybersecurity-myth-5-financially-motivated-cyberattacks

MTS Attack Surface

- ***Global Interconnections***
- ***Old meets New***
- ***Intermodal***
- ***Public / Private Partnerships***

Insights - Incidents and Findings (2021)

In 2021, USCG observed a 68% increase in the number of reported MTS cyber incidents

As of October 1, 2021, MTSA-regulated facilities are required to address cybersecurity risks and vulnerabilities in their facility security plans and facility security assessments.

Access Control & Authentication

- Easily Guessable Credentials
- Weak Password Policy
- Easily Crackable Passwords
- *May relate to Security Measures for Access Control (i.e., 33 CFR 105.255)*

Least Privilege

- Elevated Service Account Privileges
- Non-essential Use of Elevated Access
- Open Mail Relay
- *May relate to Security Measures for Restricted Areas (i.e., 33 CFR 105.260)*

System Maintenance

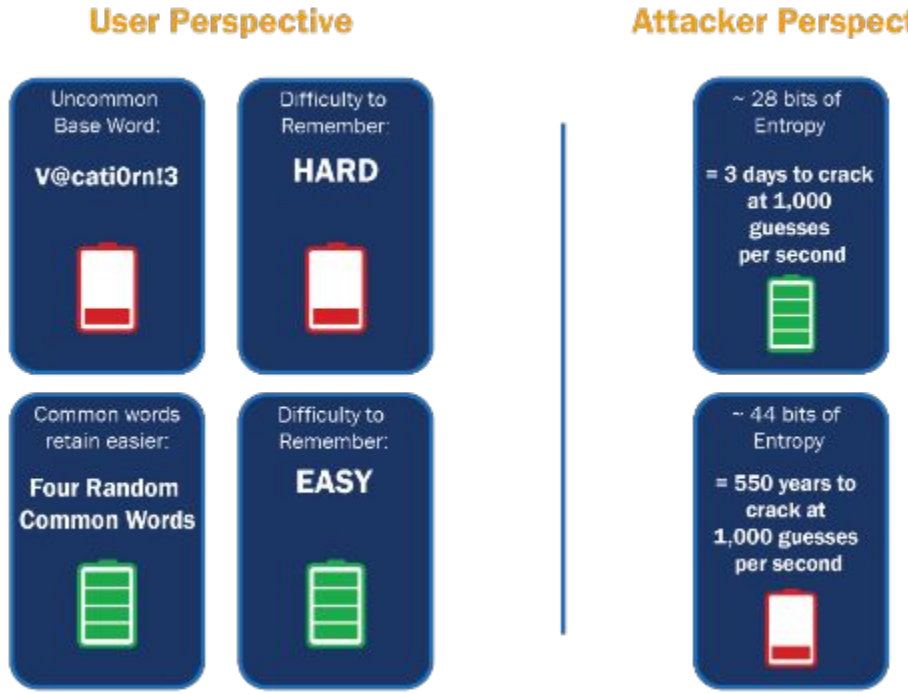
- Patch Management
- Unsupported OS
- *May relate to Security Systems and Equipment Maintenance (i.e., 33 CFR 105.250)*

Access Control & Authentication

Top 10 Default Usernam		Top 10 Default Passwords	
Admin	553	<BLANK>	418
<BLANK>	372	admin	275
<N/A>	261	PASSWORD	133
root	145	1234	46
Administrator	73	epicrouter	18
User	37	0	34
guest	33	root	19
MGR	23	system	23
operator	23	user	19
system	21	DEMO	21

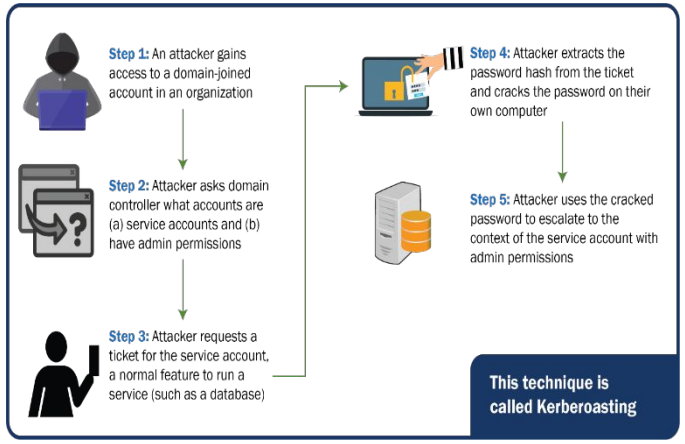
Top 20 Most Common Passwords		
Rank	Password	Time to Crack
1	123456	<1 Second
2	password	<1 Second
3	12345	<1 Second
4	123456789	<1 Second
5	password1	<1 Second
6	abc123	<1 Second
7	12345678	<1 Second
8	qwerty	<1 Second
9	111111	<1 Second
10	1234567	<1 Second
11	1234	<1 Second
12	iloveyou	<1 Second
13	sunshine	<1 Second
14	monkey	<1 Second
15	1234567890	<1 Second
16	123123	<1 Second
17	princess	<1 Second
18	baseball	<1 Second
19	dragon	<1 Second
20	football	<1 Second

Multi Factor Authentication (MFA) reduces risk by 99%



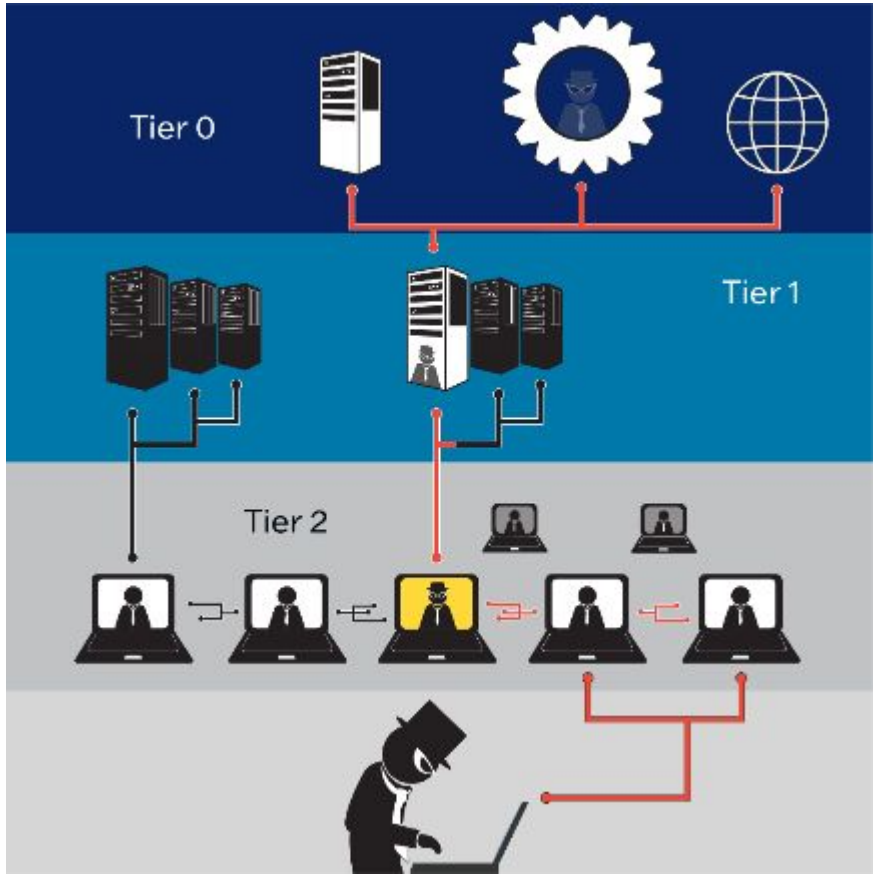
Source: https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default-Credentials/default-passwords.csv

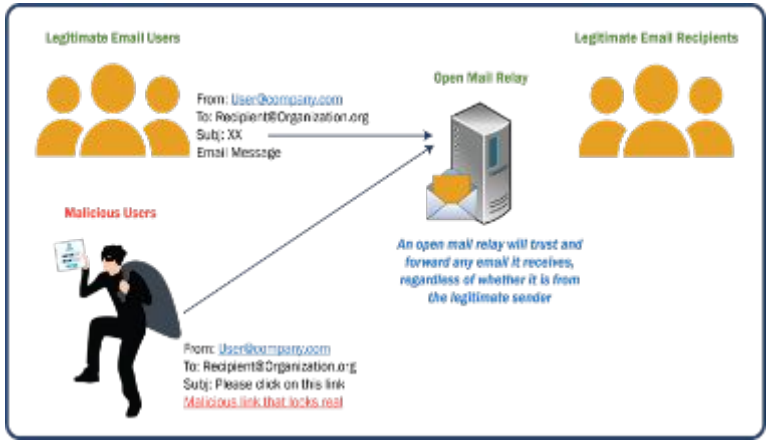
Least Privilege



Elevated Service Accounts

Non-essential Use of Elevated Accounts





Open Mail Relay

Source: https://xkcd.com/936/

System Maintenance

Windows 7 Operating System has 680 known exploits since Microsoft stopped providing updates in 2020

98% of systems infected with WannaCry ran Windows 7 unsupported

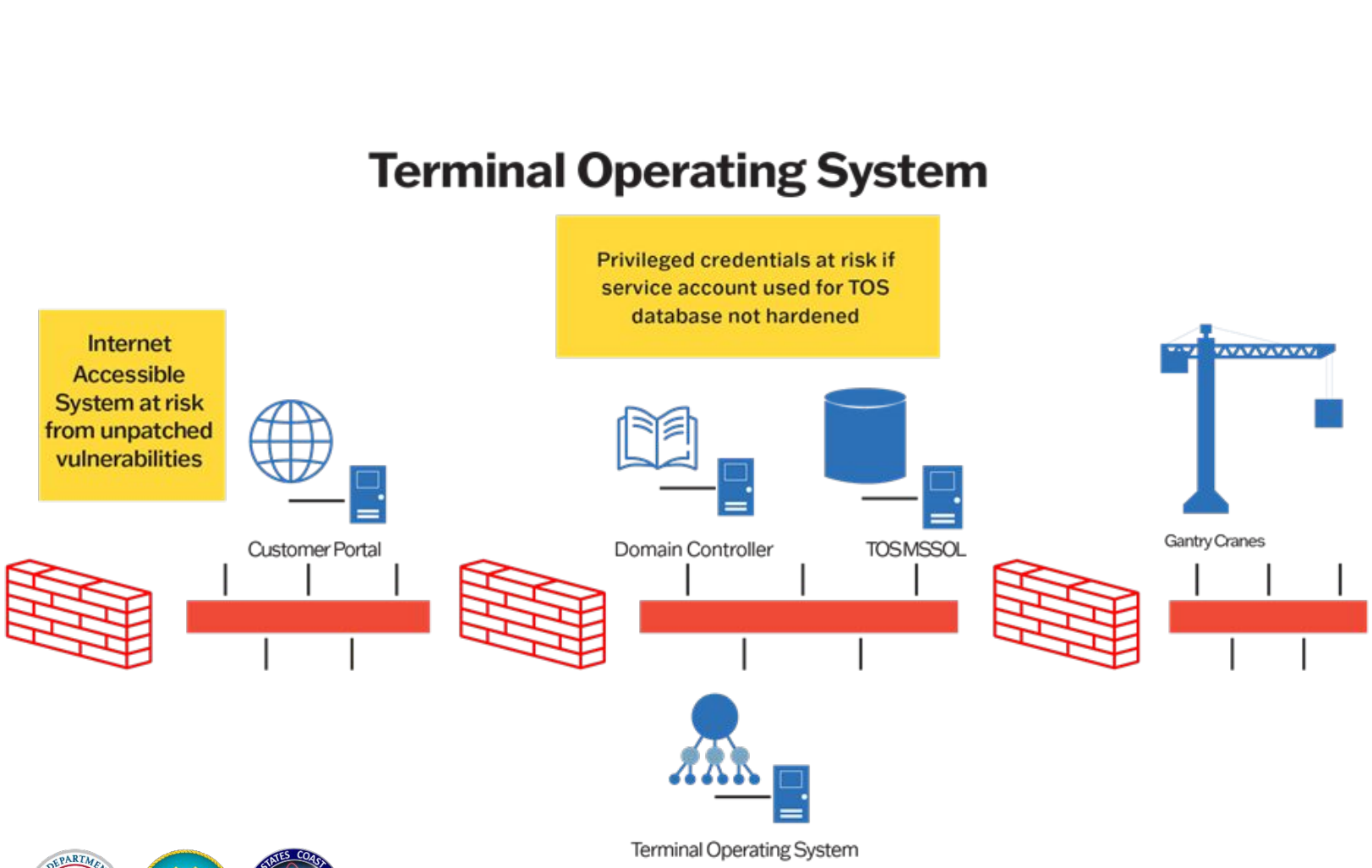
60% of breach victims said they were breached due to an unpatched known vulnerability where the patch was not applied

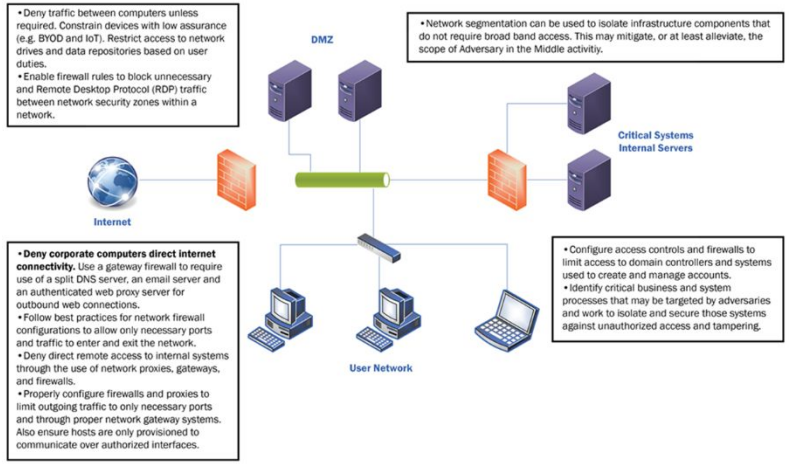
62% were unaware that their organizations were vulnerable prior to the data breach

52% of respondents say their organizations are at a disadvantage in responding to vulnerabilities because they use a manual process

Source: https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html
Source: https://www.documentcloud.org/documents/7013545-Windows-7-End-of-Life-PIN-20200803-002-EC.html

Operational Technology





Source: C-TIME Report USCG
-https://www.dco.uscg.mil/Portals/9/2021CyberTrendsInsightsMarineEnvironmentReport.pdf

Questions/Discussion