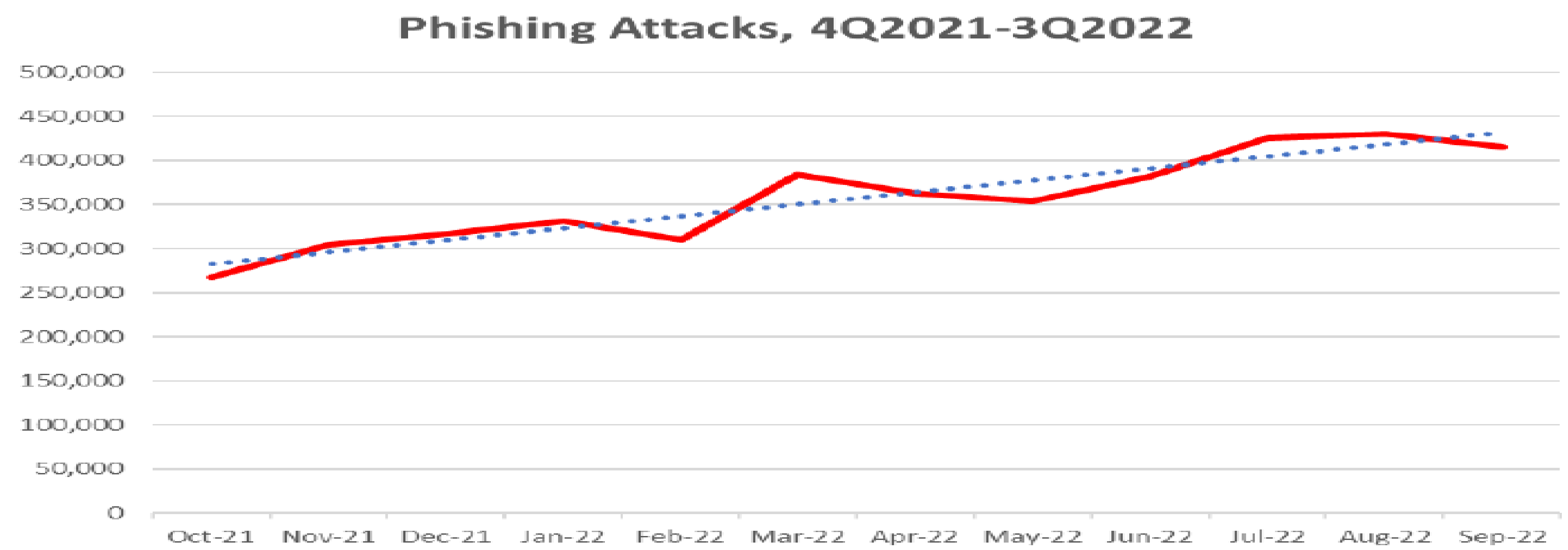
U.S. Customs and Border Protection

Cybersecurity Directorate (CSD)

World Customs Organization (WCO)
Cybersecurity: Trends, Hardening, and Strategy

October 2023

Emerging Cyber Threats & Trends



Source: Anti Phishing Working Group Phishing Activity Trends Report Q3 2022

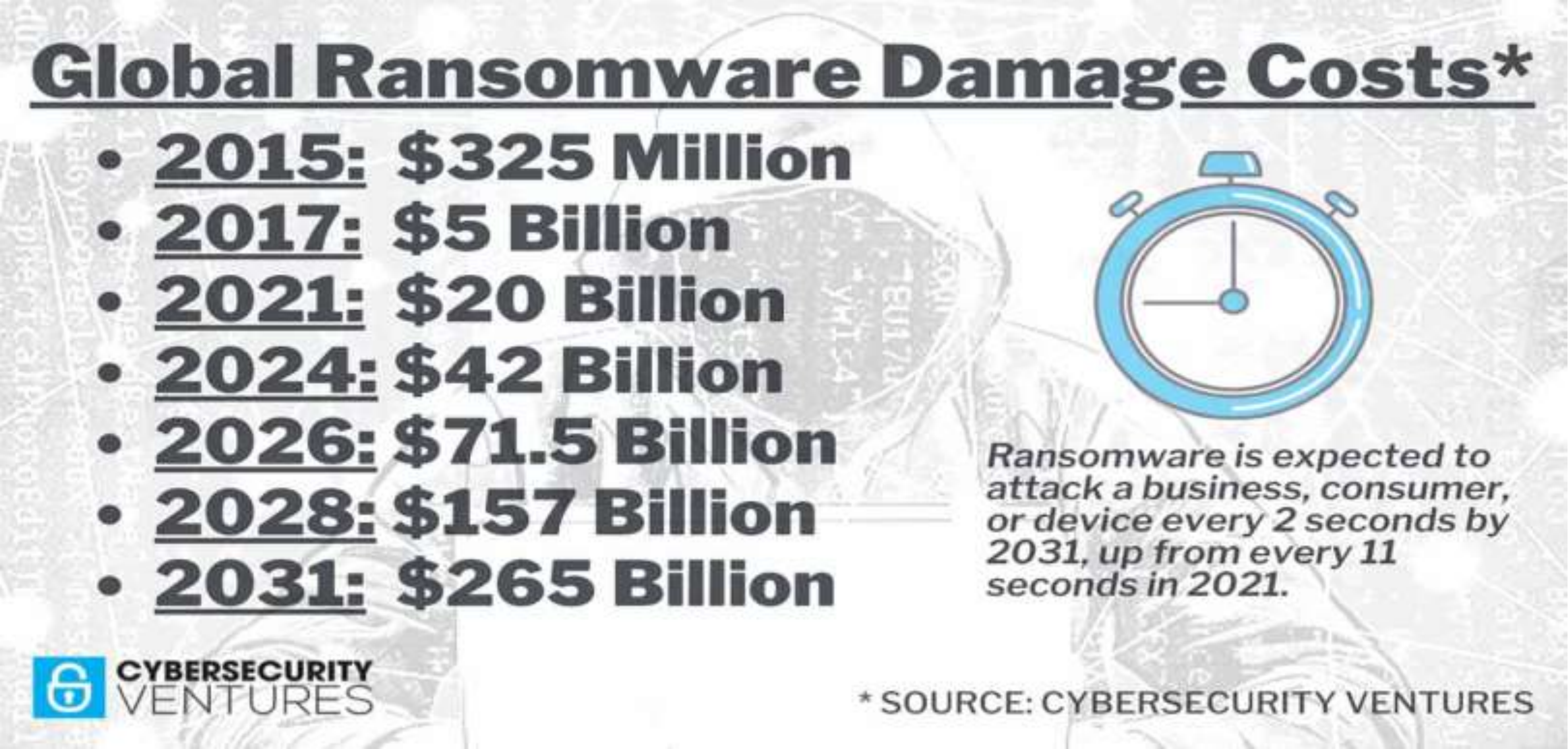
Supply Chain Compromise

- Third party suppliers & products
- Weakest points in supply chains targeted
- Trust throughout supply chain gets exploited
- Ransomware attacks on the supply chain have increased by 66% in the last three years Source: British Standards Institution (BSI)

Targeting of Infrastructure & Trade

- DHS Secretary Mayorkas testified in 2022 that cyberattacks are largest threat to U.S. ports.
- Anti Phishing Working Group: large increase in phishing/fraud emails targeting Logistics and Shipping sector
- Recent news: U.K. Royal Mail victim of “cyber incident” and unable to process exports

Emerging Cyber Threats & Trends



Global Ransomware Damage Costs*

- **2015:** $325 Million
- **2017:** $5 Billion
- **2021:** $20 Billion
- **2024:** $42 Billion
- **2026:** $71.5 Billion
- **2028:** $157 Billion
- **2031:** $265 Billion

Ransomware is expected to attack a business, consumer, or device every 2 seconds by 2031, up from every 11 seconds in 2021.

CYBERSECURITY VENTURES

* SOURCE: CYBERSECURITY VENTURES

Ransomware

- Rise in usage of Ransomware-as-a-Service (RaaS)
- Reduces technical knowledge required
- Multiple RaaS payment models
- Ease of initial ransomware deployment
- Phishing, spear phishing, social engineering remain prevalent

Hardening & Securing Systems

System hardening is **paramount** to preventing and reducing the impact of ransomware and cyber attacks

Study of major shipping and logistics companies:

- 90% had open remote desktop or administration ports at IP addresses on their network
- Most had no protection against phishing and spoofing attacks.

Source: PRNewsWire

Ransomware prevention:

- Patch and update systems
- Track vulnerabilities and their impact to your systems (NIST Vulnerability Database - NVD)
- Have antivirus deployed, keep it updated
- Back up data regularly

Source: TechTarget

Source: HackerCombat

Source: Hagerman & Co.

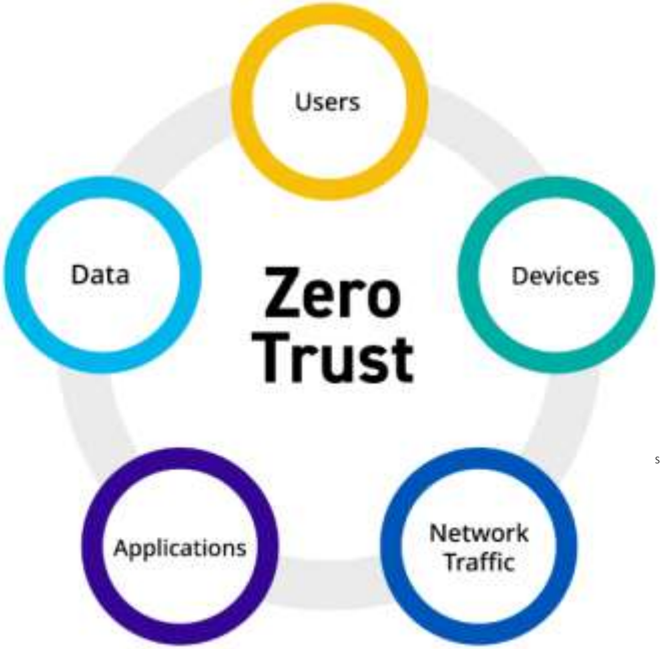
Hardening & Securing Systems

Zero Trust Implementation

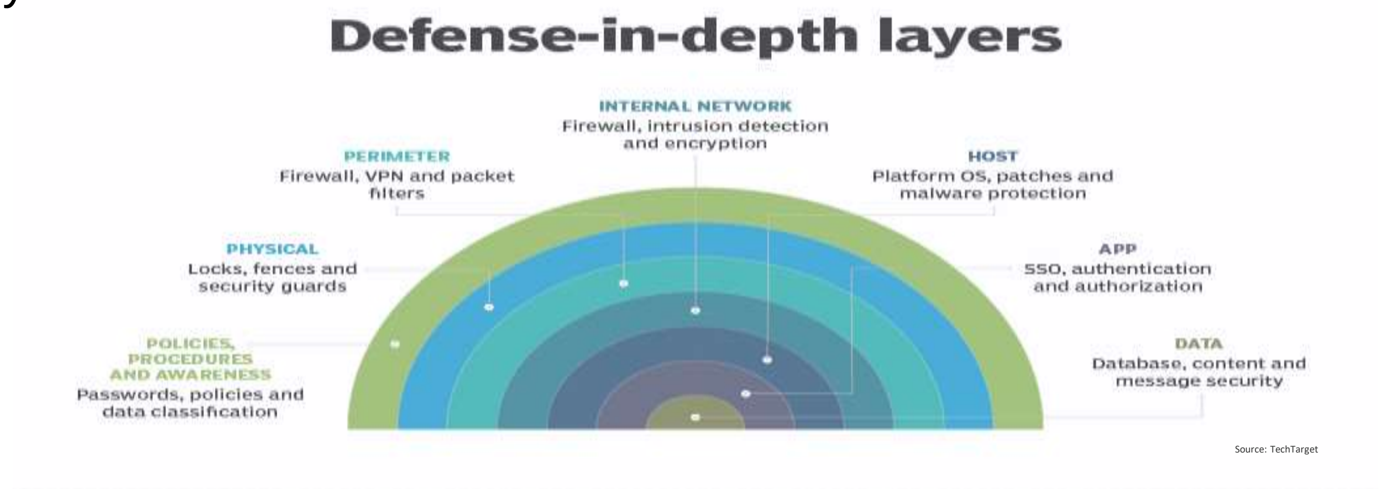
- Never trust any application or resource accessing your network
- Main pillar: Principle of Least Privilege

Defense in Depth

- Multiple layers of defense can stop attacks
- Example: Email security tool combined with network and host security tools



Source: LogRhythm

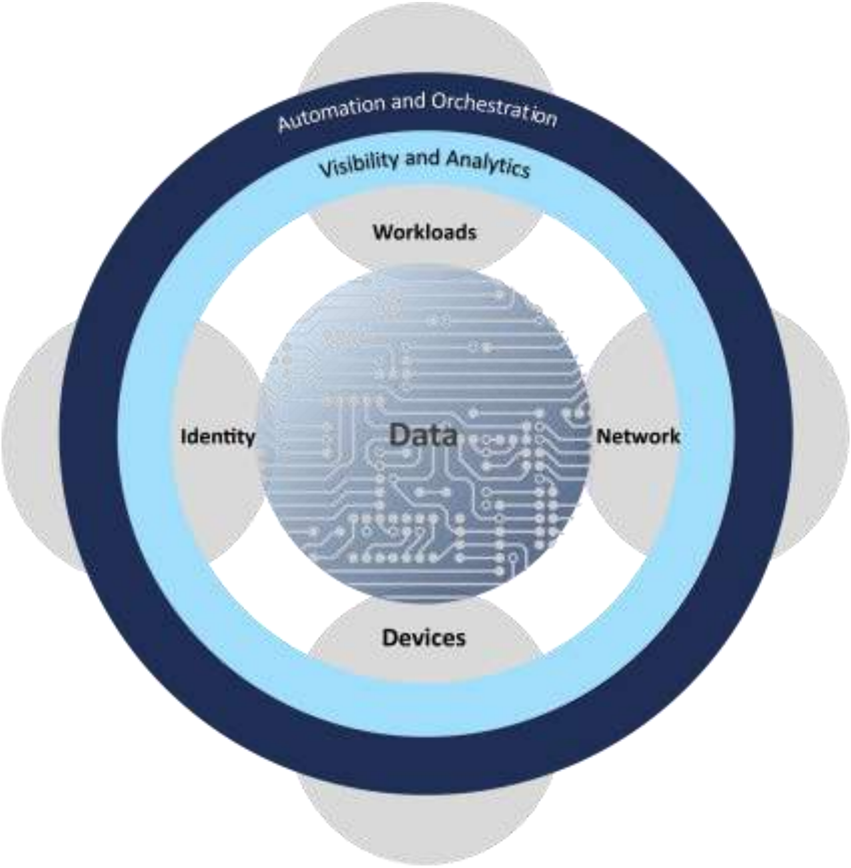

Defense-in-depth layers
INTERNAL NETWORK
Firewall, intrusion detection and encryption
PERIMETER
Firewall, VPN and packet filters
HOST
Platform OS, patches and malware protection
PHYSICAL
Locks, fences and security guards
APP
SSO, authentication and authorization
POLICIES, PROCEDURES AND AWARENESS
Passwords, policies and data classification
DATA
Database, content and message security

Source: TechTarget

What is Zero Trust Architecture?

Goal: Prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible.

- **Tenets/Principals:**
  - Assume a Hostile Environment - Never Trust, Always Verify
  - Grant user resource access on a per-session basis
  - Rigorously perform authentication and enforce authorization
  - Establish explicit permission
  - All communications must be secured regardless of network location
  - Apply unified operations and analytics



“See Yourself In Cyber”

I changed all my passwords to "incorrect".
So whenever I forget, it will tell me "Your password is incorrect."

There is a nexus between your safety and your organizational safety. Success depends on YOU!

CBP has a variety of safeguards in place to protect against cyber threats, including tools and policies, but our employees are the first line of defense.

Cyber attacks know no borders. Be vigilant at work, at home, and everywhere.

Overarching Cyber Goals

1. Defend Mission Operations by Improving Cyber Hygiene
2. Improve Threat Detection and Response Capabilities
3. Shift CBP Cyber Protection from Primarily Perimeter-facing into Zero Trust Archtecture
4. Involve all CBP in Cybersecurity Governance, Risk Management, and Compliance

Develop goals to shape your ability to be more proactive, resilient, and responsive to cyber threats

Questions

U.S. Customs and Border Protection