U.S. DEPARTMENT OF ENERGY

SRS

Citizen Advisory Board Briefing

Cybersecurity Overview

Lewann M. Belton

Director, Cyber and Information Technology Division

DOE-SR Chief Information Officer

Agenda

- What is Cyber Security?
- What keeps me up at night?
- Challenges
- Capabilities
- External Partnerships
- Questions/Open Discussion

What is Cyber Security?

What is Cyber Security?

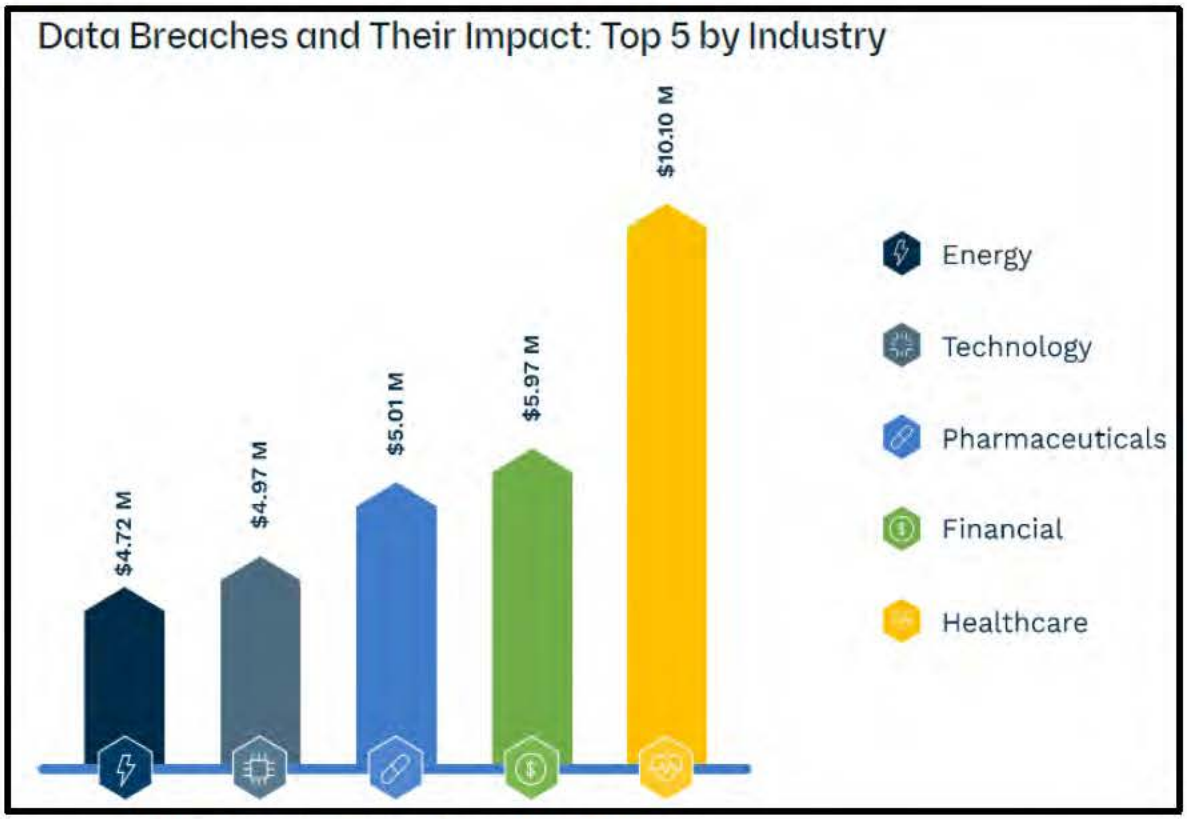
Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

What keeps me up at night?

What are the 10 Most Common Types of Cyber Attacks?

1. Malware
2. Denial-of-Service (DoS) Attacks
3. Phishing
4. Spoofing
5. Identity-Based Attacks
6. Code Injection Attacks
7. Supply Chain Attacks
8. Insider Threats
9. DNS Tunneling
10. IoT-Based Attacks

10 most common cyber attacks according to Crowdstrike



Top 5 by Industry sourced from Lumificyber

DOE SRS Public Release Review
No: DOE-ROI- 56911
Approved for Public Release

Challenges: What keeps me up at night?

- Data Breaches
- Distributed Denial of Service (DDoS)
- Phishing/Spoofing
- Malware
  - Ransomware
- Unpatched/Outdated Software/Legacy Systems
- Removable Media
- Supply Chain Risk Management (SCRM)
- Cloud

Data Breach

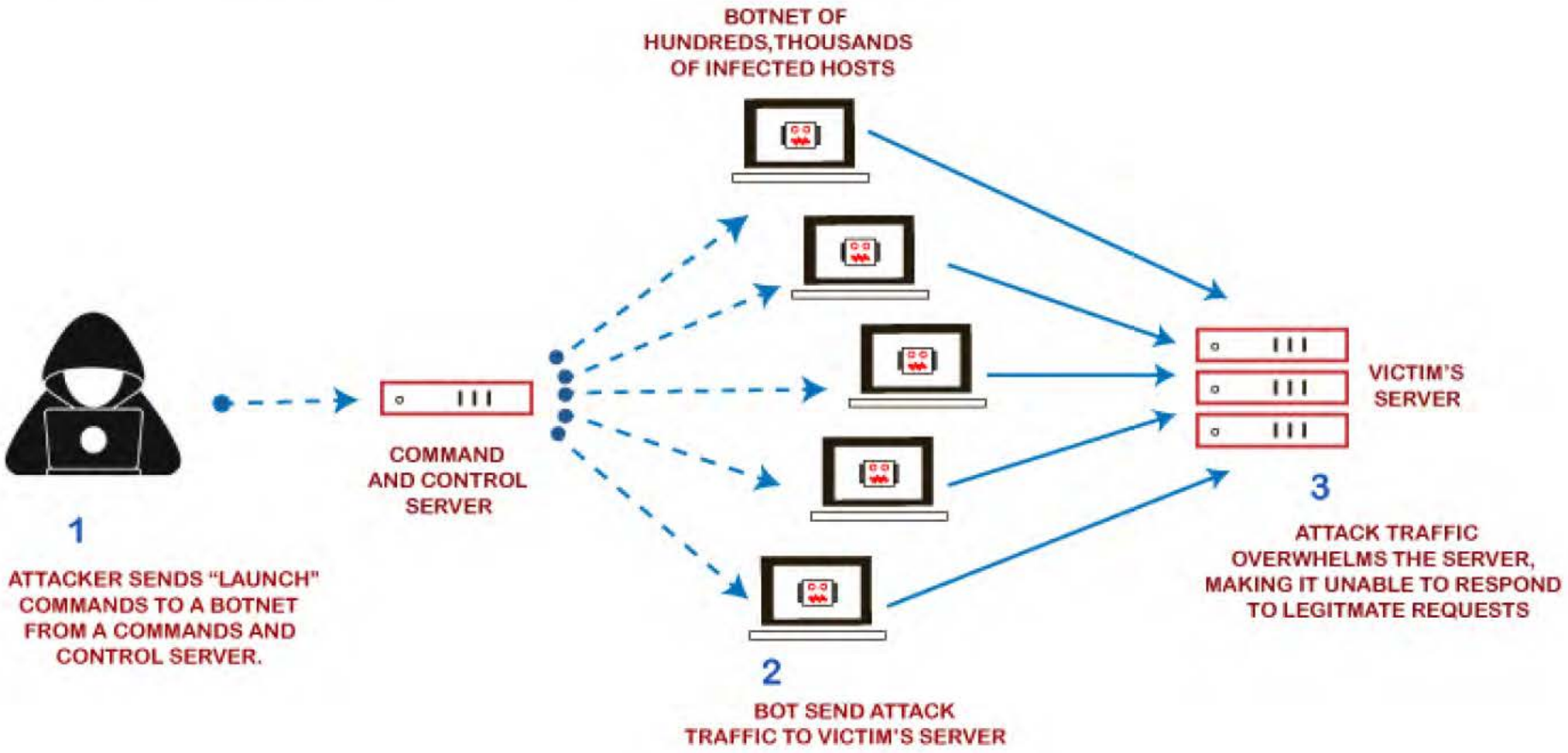
- A data breach is a leak or spill of sensitive, protected, or confidential data from a secure to an insecure environment that are then copied, transmitted, viewed, stolen, or used in an unauthorized manner.

- Data breaches often occur with confidential information, such as personal records, that may be inappropriately viewed or used by an individual who should not have access to the information.

Distributed Denial of Service

A Denial-of-Service attack, also known as a Distributed Denial of Service (DDoS) attack, occurs when a server is deliberately overloaded with requests such that the Website shuts down. Users are then unable to access the Website.

Distributed Denial of Service



Phishing/Spoofing

- Both spoofing and phishing involve the use of fake electronic documents.
- Spoofing refers to the dissemination of an email that is forged to appear as though it was sent by someone other than the actual source.
- Phishing is the act of sending an email falsely claiming to be a legitimate organization in an attempt to deceive the recipient into divulging sensitive information (e.g., passwords, credit card numbers, or bank account information) after directing the user to visit a fake Website.
- Spear phishing is a more targeted form of phishing and typically involves sending an email that appears to come from a colleague or acquaintance.

From: domain@domain-name.com

To: Your email

Subject: Apple Facetime Information Disclosure

National Security Department

A vulnerability has been identified in the Apple Facetime mobile applications that allow an attacker to record calls and videos from your mobile device without your knowledge.

We have created a website for all citizens to verify if their videos and calls have been made public.

To perform the verification, please use the following link:

Facetime Verification

This website will be available for 72 hours.

National Security Department

From: Newsweek <noreply@alerts-region.com>
Reply-To: Newsweek <noreply@alerts-region.com>
Subject: ALERT: Local SC town being overtaken by foreign species of spiders

Newsweek

ALERT: Local SC town being overtaken by foreign species of spiders

It sounds like something out of a horror film: This Aiken, SC area is being covered in thousands of webs, each crawling with mobs of spiders. ABC news reported that the foreign species was accidentally released into the woods and is now populating at alarming rates. See what you need to do to protect your home and read the full story at Newsweek Online.

Read More

Malware

Malware is malicious software deployed by a threat actor to wreak havoc on an organization or individual. Malware is usually found attached to emails, embedded in fraudulent links, hidden in ads, or lying in-wait on various sites that you (or your employees) might visit on the internet. The end goal of malware is to harm or exploit computers and networks, often to steal data or money.

Types of Malware

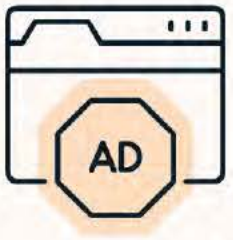
RANSOMWARE

Blackmails you

SPYWARE

Steals your data

ADWARE



Spams you with ads

WORMS

Spread
across computers

TROJANS

Sneak malware
onto your PC

BOTNETS

Turn your PC
into a zombie

Ransomware

- Ransomware is a form of malware in which perpetrators encrypt users' files, then demand the payment of a ransom—typically in virtual currency such as Bitcoin—for the users to regain access to their data.
- An example of ransomware is WannaCry, which infected computers across the globe in May 2017. Ransomware can also include an element of extortion, in which the perpetrator threatens to publish data or images if the victim does not pay. The ransomware is frequently delivered through phishing/spoofing scams.

Removable Media

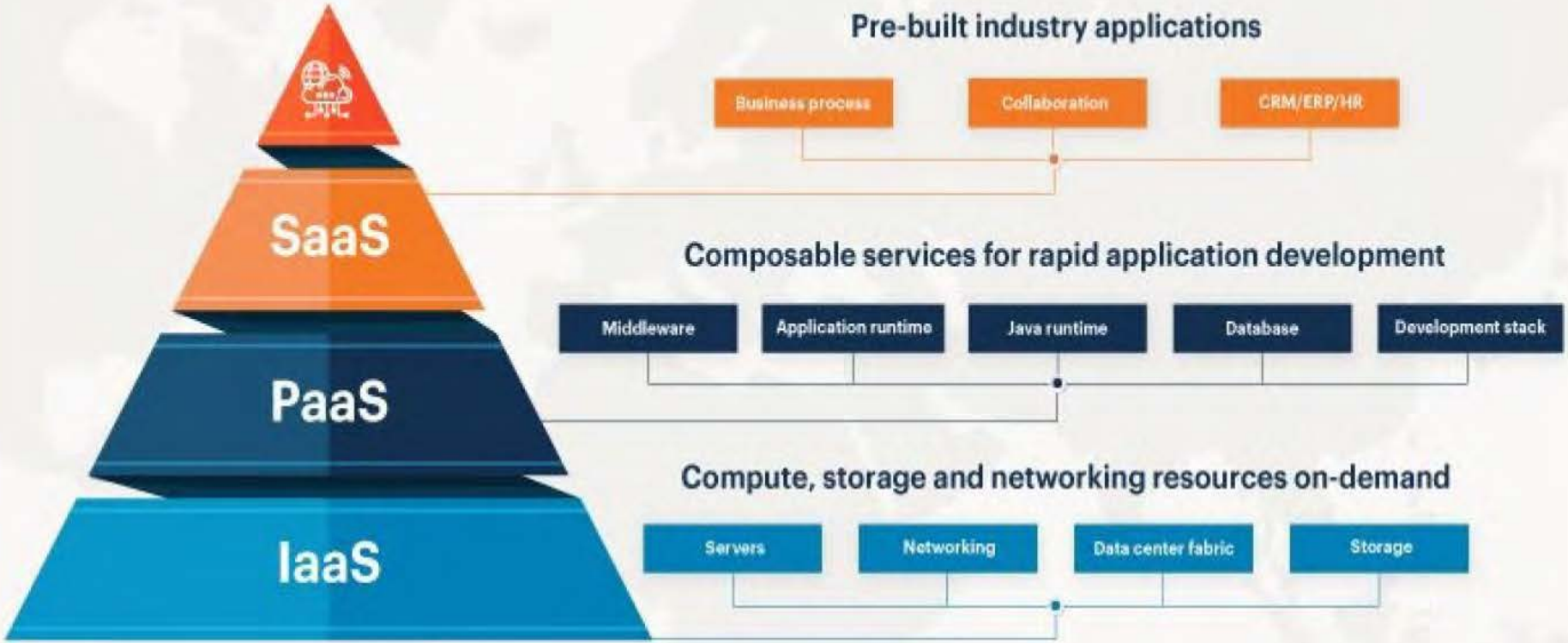
Media devices that can be connected to computers, such as thumb drives, CDs, DVDs, and external hard drives, also pose challenges to cybersecurity. First, these storage devices can be easily stolen. Second, corrupted devices can be intentionally or unwittingly connected to computers. Once opened, files from the device can then infect the computer with malware.

Supply Chain Risk Management – Suspect Counterfeit items

A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplies product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).

Cloud

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.



Examples for SaaS, PaaS and IaaS

Capabilities

- Automated threat detection
- Threat remediation
- Intrusion detection and prevention
- Forensic analysis
- Penetration testing, systems/application scanning
- Disaster recovery and incident response teams

Other Cyber Security related examples

- Policy compliance
- Cyber security awareness training
- Secure configuration management

External Partnerships

- Fort Eisenhower Cyber Protection Team
- Federal Bureau of Investigation
- Cybersecurity & Infrastructure Security Agency
- Center for Internet Security
- National Institute of Standards and Technology
- Georgia Cyber Center
- USC Aiken

NIST

UofSC Aiken
College of Sciences and Engineering

CIS®