U.S. DEPARTMENT OF ENERGY

SRS™

Cyber Security Overview

Lewann M. Belton

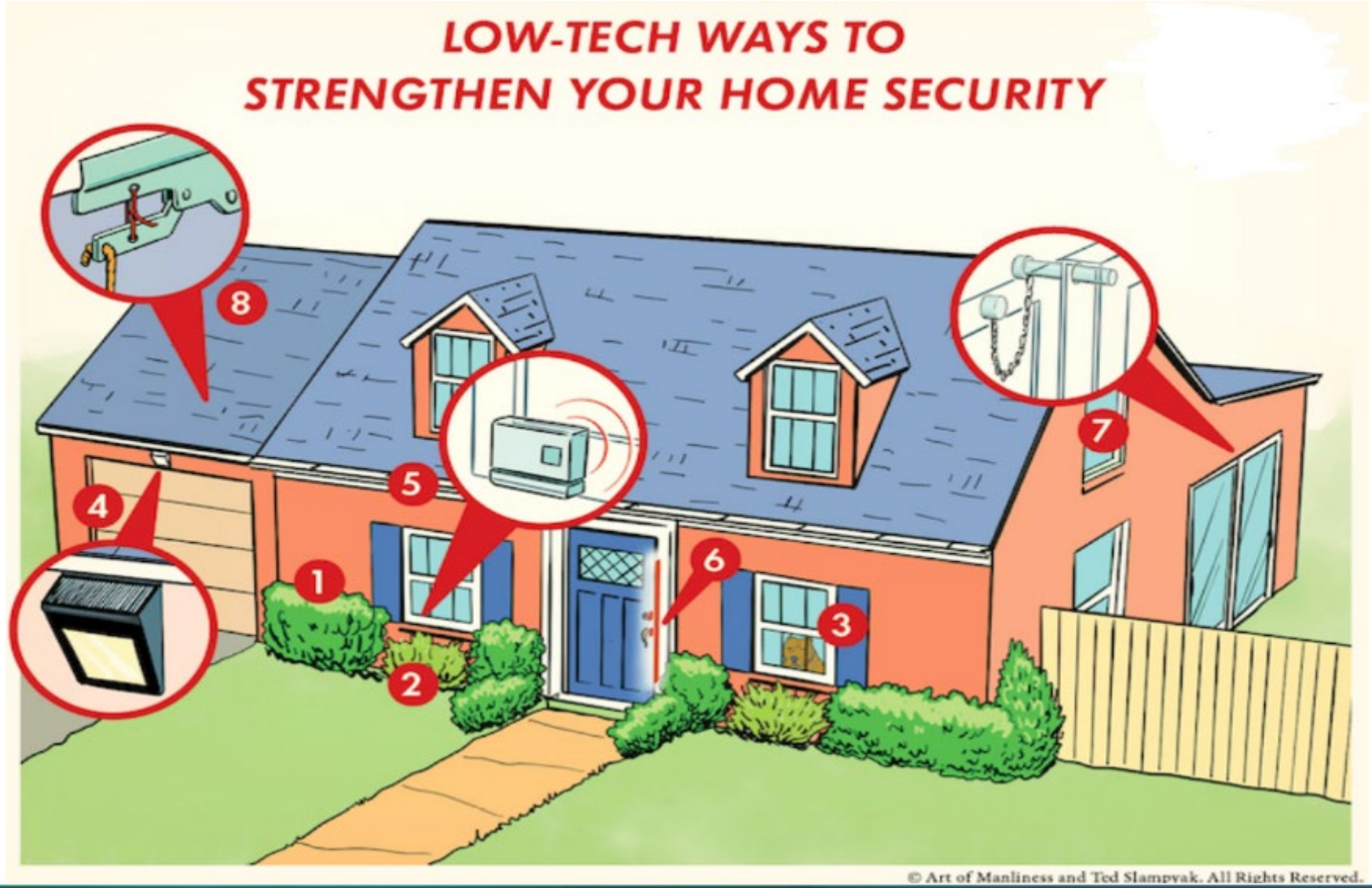
Director, Office of Cyber and Information Technology

DOE-SR Chief Information Officer

Agenda

- Home Security
- What is Cyber Security?
- Tools and Capabilities
- Risk and Challenges
- Changes since transition
- Partnerships
- Questions/Open Discussion

Home 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.

- Cybersecurity & Infrastructure Security Agency (2021)

DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release

Security at home is like security onsite

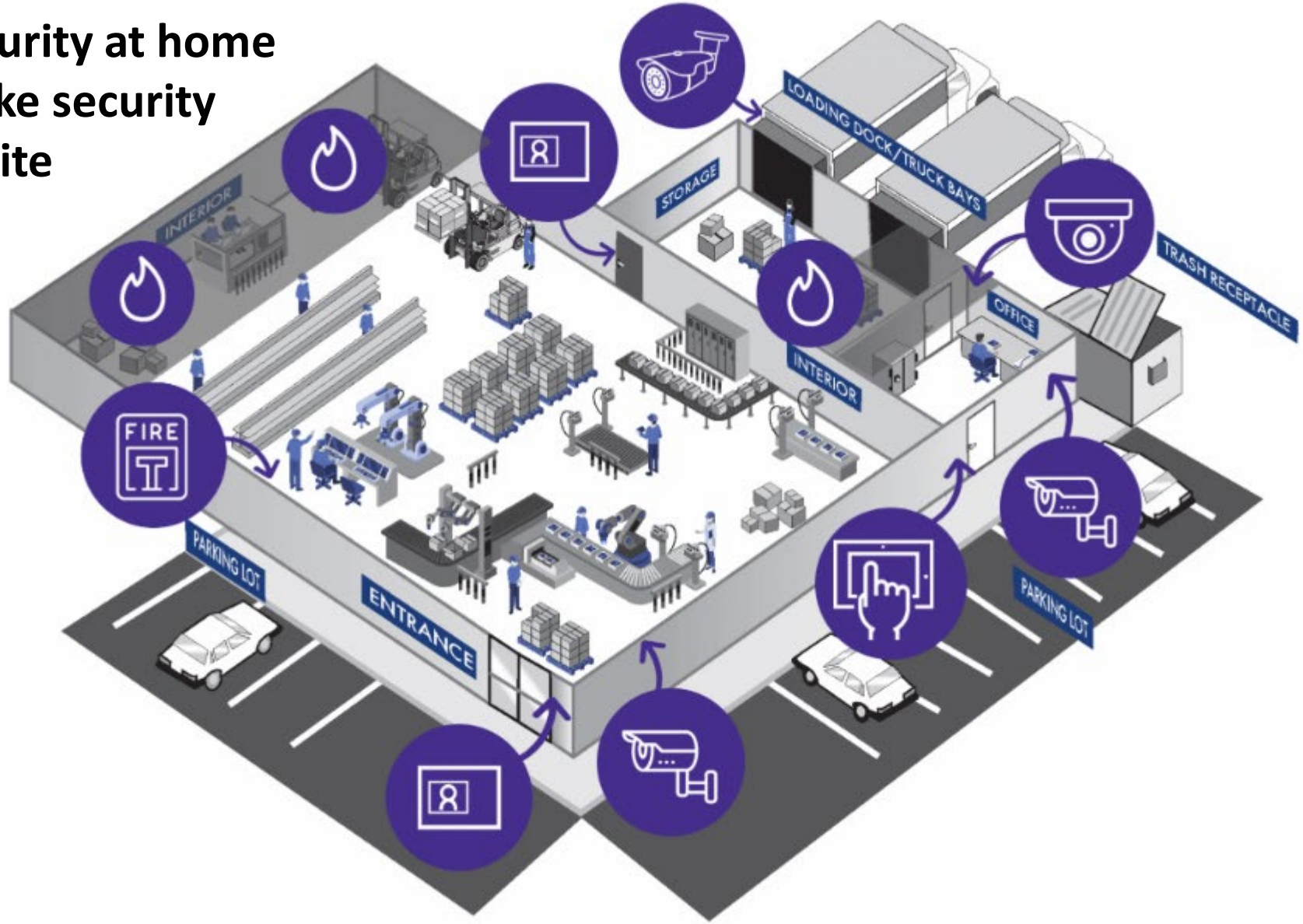


Image for Guardian Protection

DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release

Tools and Capabilities

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

DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release

Risk and Challenges

Distributed Denial of Service (DDoS)

Data Breaches

Outdated Software/Legacy Systems

Malware

Ransomware

Removable Media

Cloud

Supply Chain Risk Management (SCRM)

Phishing/Spoofing

DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release

Changes since transition

- ***Transition to NNSA***
  - *Cyber Security Program*
  - *EM/NNSA Shared Cost (no change)*
  - *SRNS Managing & Operating contractor manages IT Shared Services (e.g. Infrastructure, Network, Data)*
- ***EM manages***
  - *Liquid Waste Scope*
  - *Savannah River National Lab*

DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release

Partnerships

- FBI
- Cybersecurity & Infrastructure Security Agency
- National Institute of Standards and Technology
- Georgia Cyber Center
- USC Aiken

UofSC Aiken
College of Sciences and Engineering

NIST

DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release

DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release

Backup Slides

DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release

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.

DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release

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.

DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release

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.

DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release

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.

DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release

- 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.

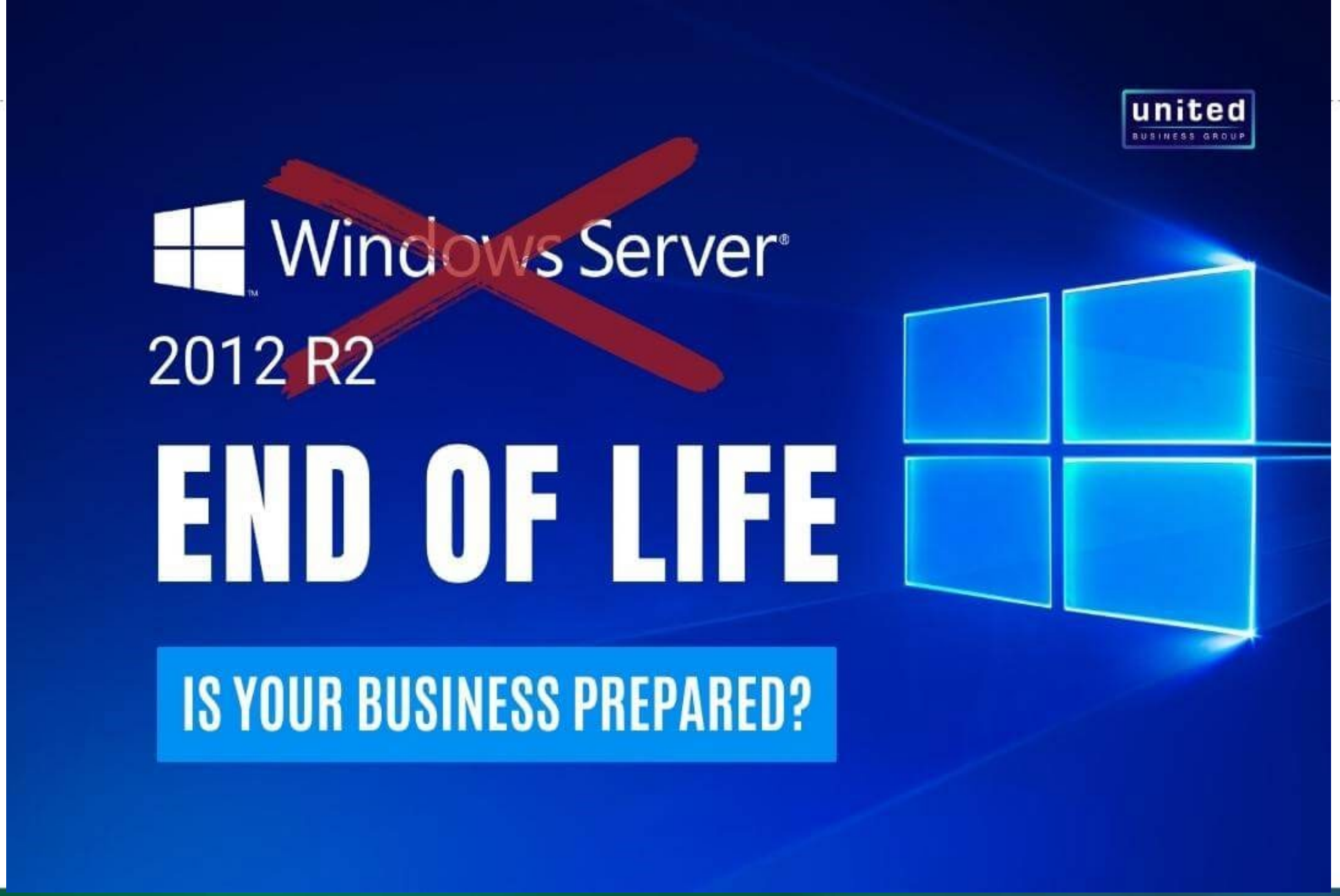
DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release

DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release

Unpatched/Outdated Software/Legacy Systems

- Vulnerabilities occur when unpatched or outdated software has not been updated to include the latest software updates; thus, unauthorized users can gain access to information networks and systems.

DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release



DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release

DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release

Supply Chain Risk Management – 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).

DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release

Supply chain risk management process

01 **Identify and document known risks to the supply chain**

02 **Assess the probability and potential impact of each risk**

03 **Develop strategies for mitigating identified risks**

04 **Implement those mitigation strategies**

05 **Continuously monitor and improve this process**

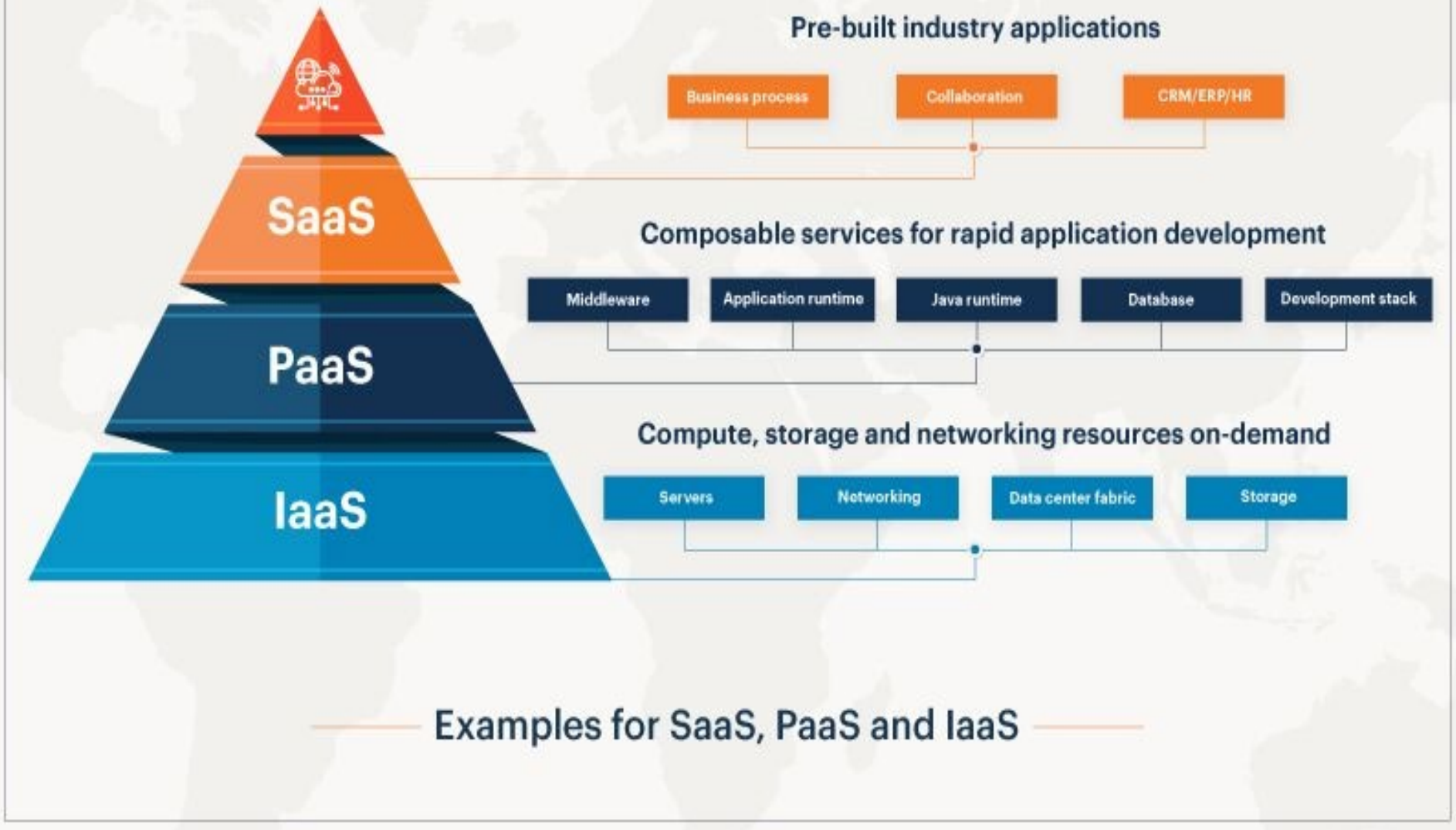
Cloud

- Cloud computing service models come in three broad categories:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

- Each cloud service model provides a different level of control that translates to varying levels of responsibility on you. In a SaaS solution, the service provider manages everything, and you can change some configurations once you sign-up. With IaaS, you have full control because you rent (not own) the infrastructure. With PaaS solutions, you control the application and data while the service provider manages the rest of the stack.

DOE SRS Public Release Review
No: DOE-ROI-61501
Approved for Public Release



Examples for SaaS, PaaS and IaaS