Cybersecurity Tips for Small Businesses

Teresa Rule, PMP, CISA, CDPSE

RNT PROFESSIONAL SERVICES

Veterans Defending the Digital Universe™

ABOUT THE SPEAKER

Teresa Rule, PMP, CISA, CDPSE, CMMC PA

President, RNT Professional Services, LLC

COMPANY DETAILS

Norman, OK based company specializing in Cybersecurity and Data Privacy

- Veteran Owned and Staffed
- Woman Owned
- Service-Disabled Veteran Owned
- OKDOT Disadvantaged Business Enterprise
- HUB Zone located business
- 70% of team members are US Veterans

CONTACT INFORMATION

Teresa.Rule@RNTPros.com

www.rntpros.com

Our Goals

- At the end of the presentation, attendees will have an increased
  - Knowledge of the basic understanding of cybersecurity principles
  - Understanding of cybersecurity control elements
  - Understanding of protection approaches for small businesses

Critical Infrastructure Sectors

Chemical Sector
The Department of Homeland Security is designated as the Sector Risk Management Agency for the Chemical Sector.

Financial Services Sector
The Department of the Treasury is designated as the Sector Risk Management Agency for the Financial Services Sector.

Commercial Facilities Sector
The Department of Homeland Security is designated as the Sector Risk Management Agency for the Commercial Facilities Sector, which includes a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging.

Food and Agriculture Sector
The Department of Agriculture and the Department of Health and Human Services are designated as the co-Sector-Risk Management Agencies for the Food and Agriculture Sector.

Communications Sector
The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. The Department of Homeland Security is the Sector Risk Management Agency for the Communications Sector.

Government Facilities Sector
The Department of Homeland Security and the General Services Administration are designated as the Co-Sector Risk Management Agencies for the Government Facilities Sector.

Critical Manufacturing Sector
The Department of Homeland Security is designated as the Sector Risk Management Agency for the Critical Manufacturing Sector.

Healthcare and Public Health Sector
The Department of Health and Human Services is designated as the Sector Risk Management Agency for the Healthcare and Public Health Sector.

Dams Sector
The Department of Homeland Security is designated as the Sector Risk Management Agency for the Dams Sector. The Dams Sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities.

Information Technology Sector
The Department of Homeland Security is designated as the Sector Risk Management Agency for the Information Technology Sector.

Defense Industrial Base Sector
The U.S. Department of Defense is the Sector Risk Management Agency for the Defense Industrial Base Sector. The Defense Industrial Base Sector enables research, development, design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts to meet U.S. military requirements.

Nuclear Reactors, Materials, and Waste Sector
The Department of Homeland Security is designated as the Sector Risk Management Agency for the Nuclear Reactors, Materials, and Waste Sector.

Emergency Services Sector
The Department of Homeland Security is designated as the Sector Risk Management Agency for the Emergency Services Sector. The sector provides a wide range of prevention, preparedness, response, and recovery services during both day-to-day operations and incident response.

Transportation Systems Sector
The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.

Energy Sector
The U.S. energy infrastructure fuels the economy of the 21st century. The Department of Energy is the Sector Risk Management Agency for the Energy Sector.

Water and Wastewater Systems Sector
The Environmental Protection Agency is designated as the Sector Risk Management Agency for the Water and Wastewater Systems Sector.

Critical Infrastructure Sectors

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Financial Services Sector
- Emergency Services
- Food and Agriculture Sector
- Dams Sector
- Energy Sector
- Transportation Sector
- Government Facilities
- Critical Manufacturing
- Healthcare and Public Health Sector
- Information Technology Sector
- Defense Industrial Base Sector
- Nuclear Reactors, Material and Waste Sector
- Water and Wastewater Sector

Government Contracting - Cyber

- Know the requirements and references
- Get assessed
- Get required certifications
- Develop a cyber mature culture
- Incorporate cybersecurity into routine protocols
- Keep staff trained

Business Basics

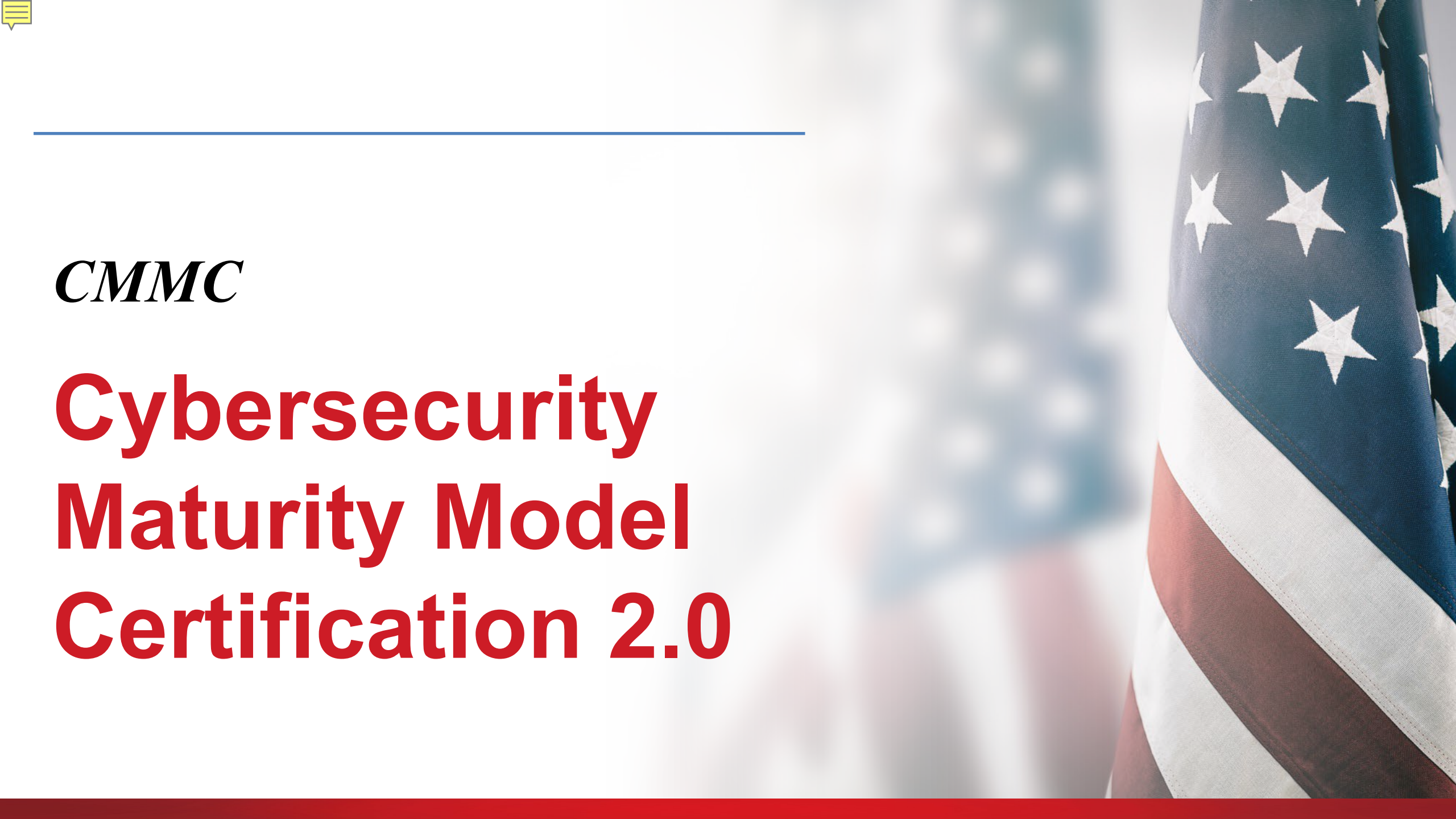
- Know industry standards
- Train your people
- Secure your technology
- Get assessed
- Battle complacency

Requirements & References

- NIST – National Institute of Standards and Technology
  - www.nist.gov
- SPRS – Supplier Performance Risk System
  - www.sprs.csd.disa.mil
- CMMC – Cybersecurity Maturity Model Certification
  - www.acq.osd.mil
- DFARS – Defense Federal Acquisition Regulation Supplement
  - www.acquisition.gov

CMMC

Cybersecurity Maturity Model Certification 2.0

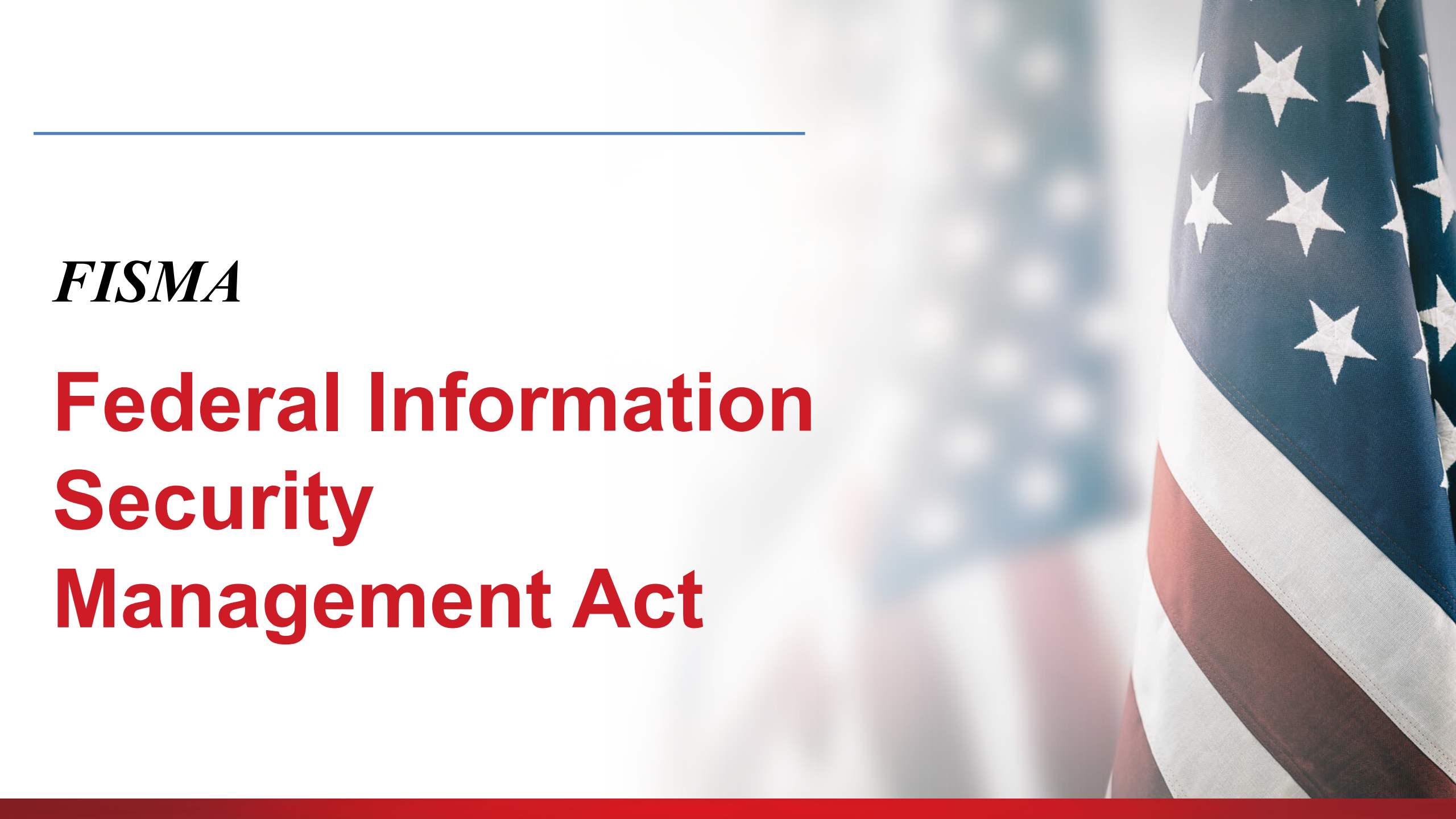


(SPRS)

Supplier Performance Risk System

FISMA

Federal Information Security Management Act



HIPAA

Health Insurance Portability and Accountability Act

GDPR

General Data Protection Regulation

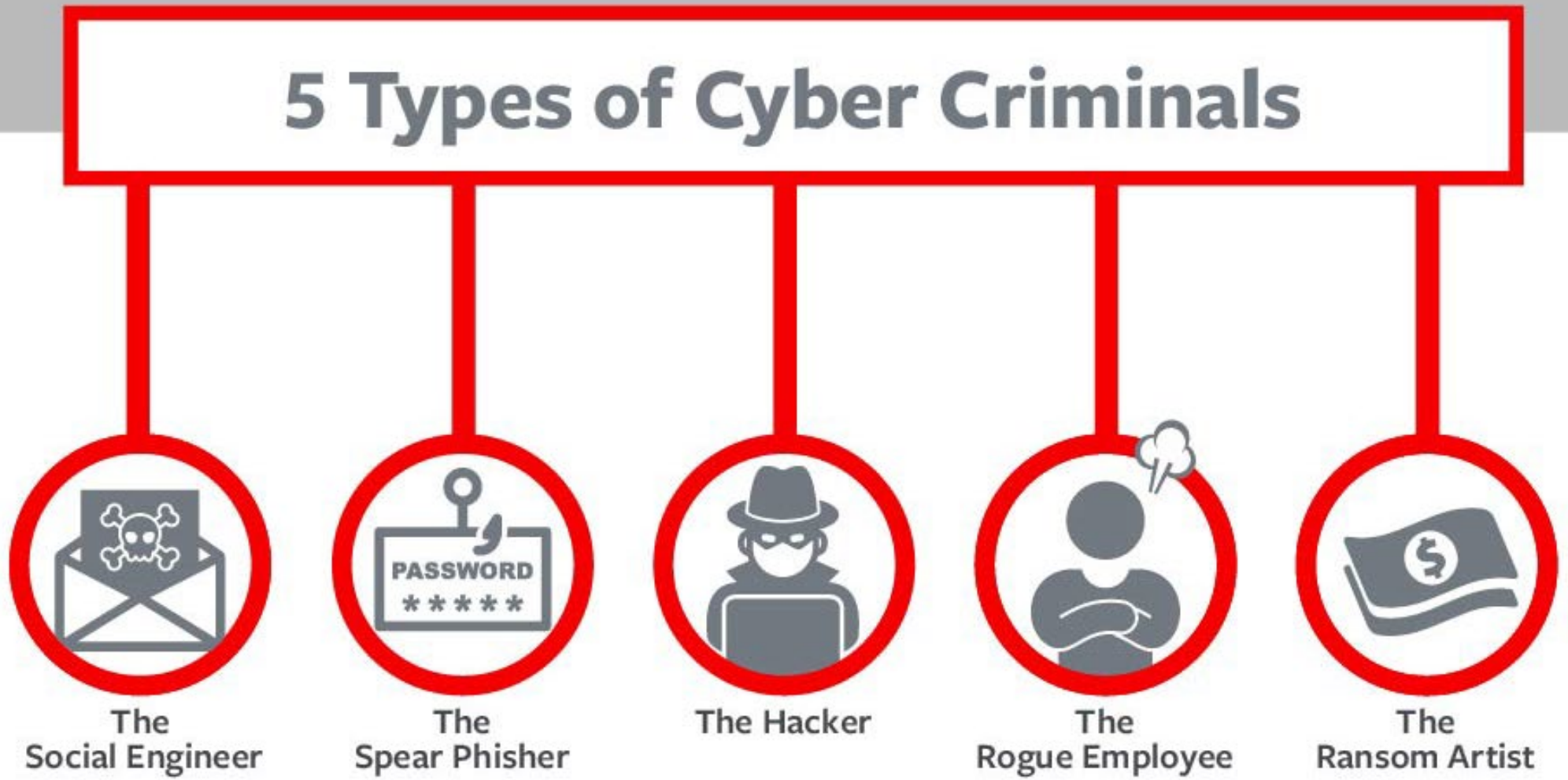
Types of Cyber Attacks

- Cyber Warfare – Nation to Nation
- Terrorism – Organization to Nation
- Espionage – Nation to Nation
- Insider Threat – Commerce
- Crime – Commerce
- Hacktivism – Commerce

Did you know

- 60% of small businesses fold within 6 months of a cyber attack?
- 62% of small businesses do not have an active cybersecurity strategy – or a strategy at all?
- 43% of cyber attacks target small businesses?
- There is a hacker attack every 39 seconds?
- 95% of cybersecurity breaches are due to human error?

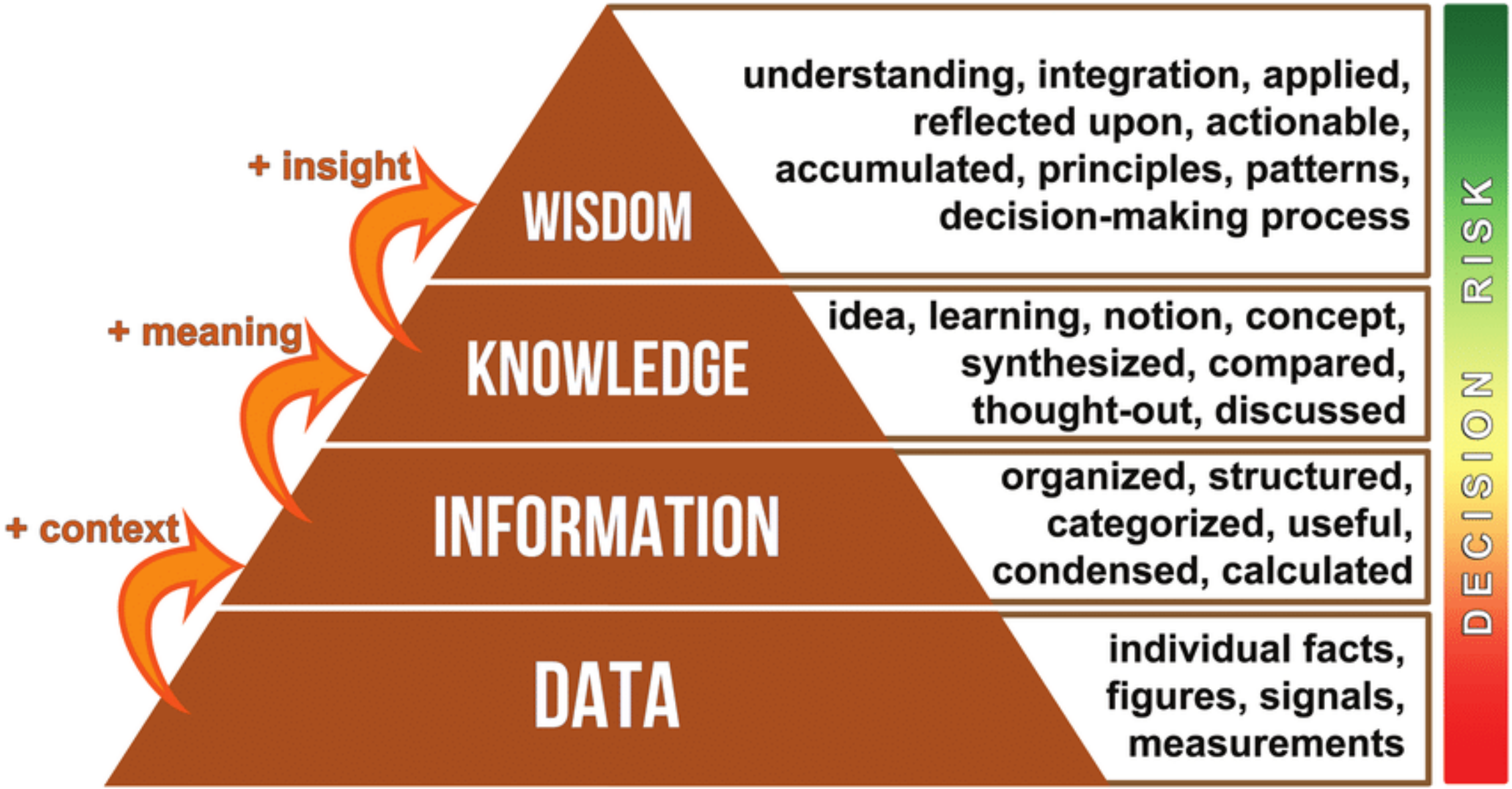
5 Types of Cyber Criminals



Managing the Risk

- Advanced Persistent Threat (APT) – effective and secure firewalls,
- Phishing – Training, Backups
- Distributed Denial of Service (DDoS) – Internet Service Provider
- Inside Attacks – Role Based Access Controls
- Malware – Training, Backups, Controls, Antivirus
- Password Attacks – Limited attempts, password length, password policies
- Ransomware – Backups and Training

DATA


+ insight
+ meaning
+ context
WISDOM
understanding, integration, applied, reflected upon, actionable, accumulated, principles, patterns, decision-making process
KNOWLEDGE
idea, learning, notion, concept, synthesized, compared, thought-out, discussed
INFORMATION
organized, structured, categorized, useful, condensed, calculated
DATA
individual facts, figures, signals, measurements
DECISION RISK

Cybersecurity Objectives

- Confidentiality of Data
- Integrity of Data
- Availability of Data

CIA

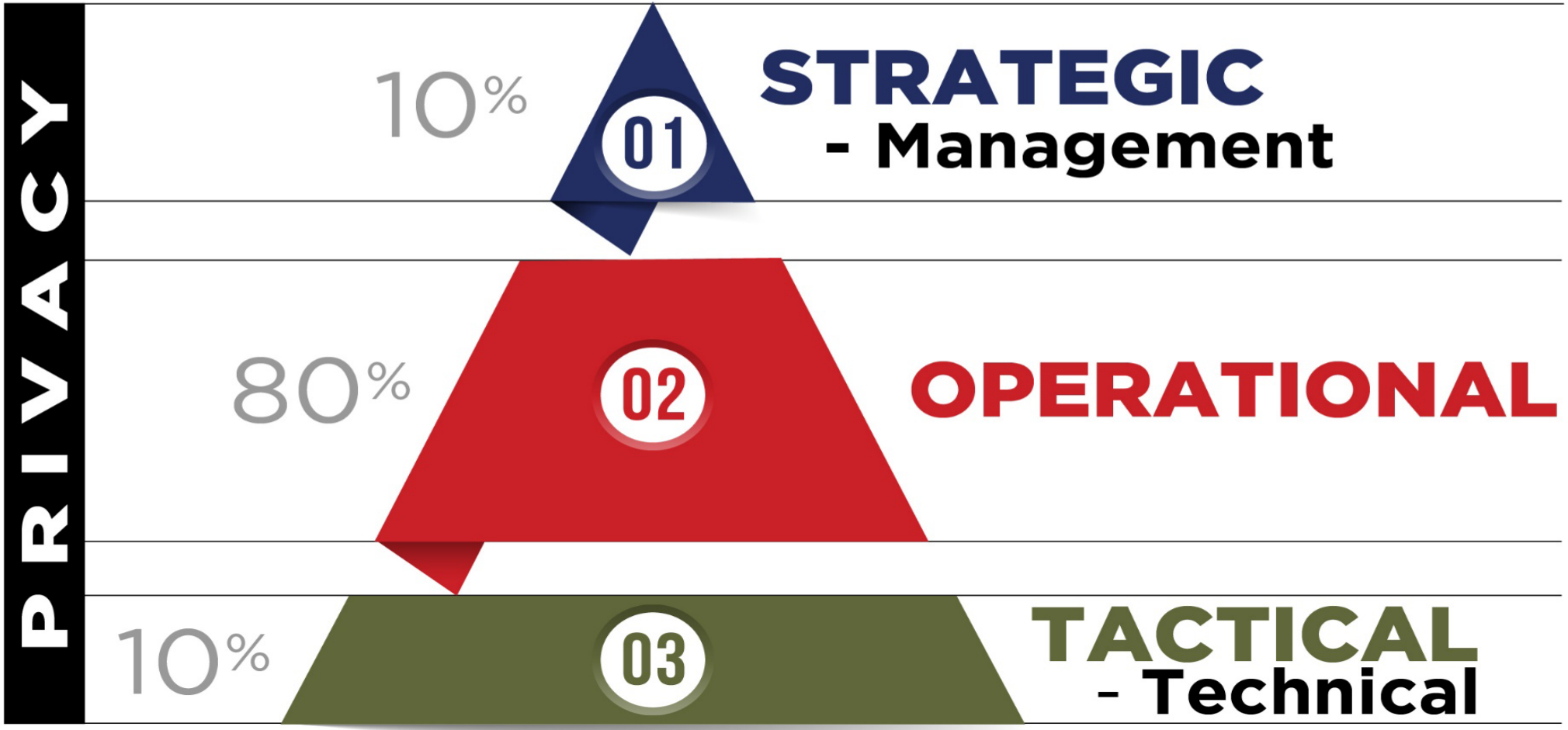
Control Areas

- **Management**: Management-level scope.
- **Operational**: Infrastructure or project-level scope.
- **Technical**: System-level scope.
- **Privacy**: Corporate (including all organizational levels) scope pertaining to Personally Identifiable Information (PII).

CYBER SECURITY OPERATIONAL LEVELS

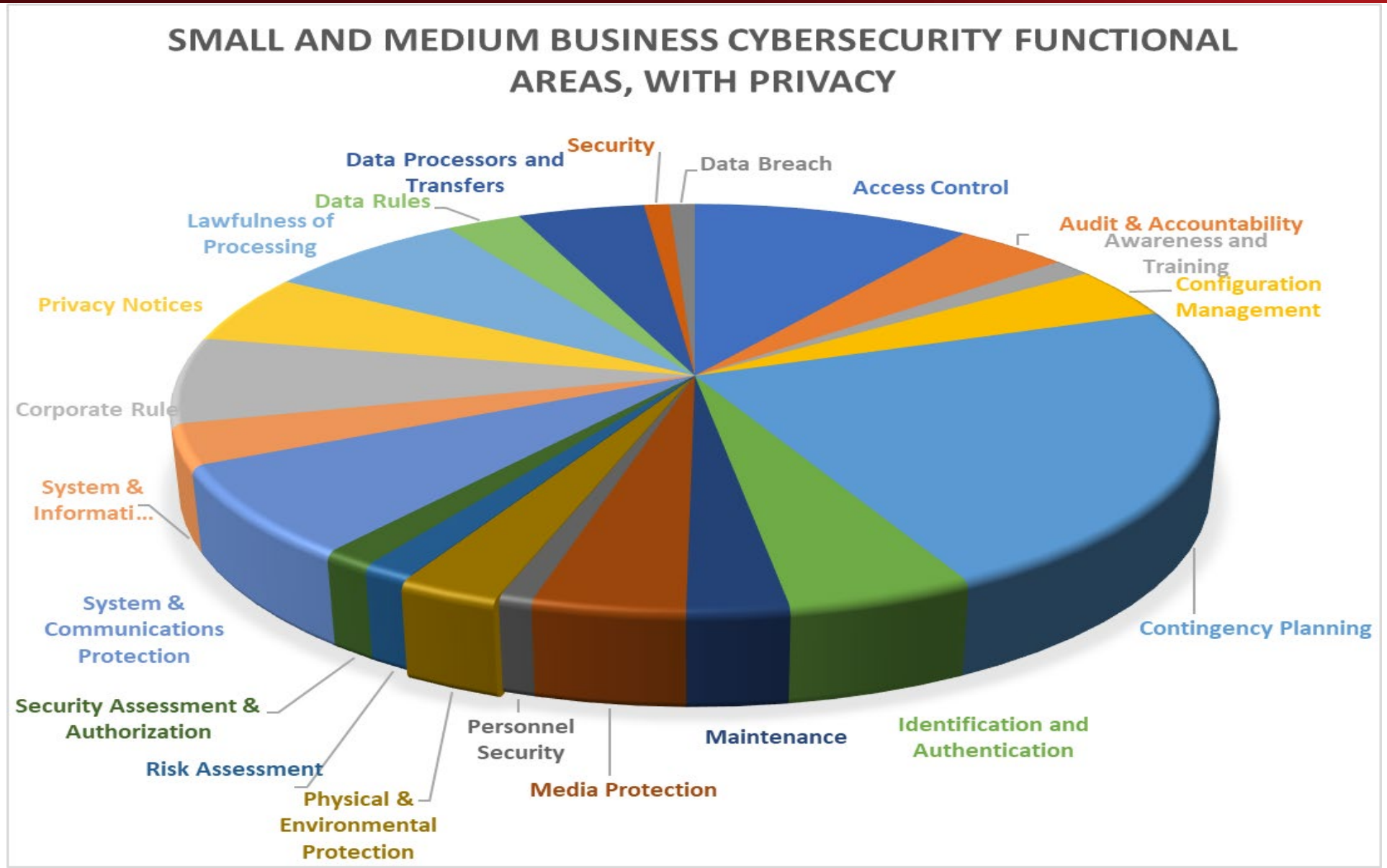
RNT PROFESSIONAL SERVICES
Veterans Defending the Digital Universe

Three Levels of Cyber Security Expertise

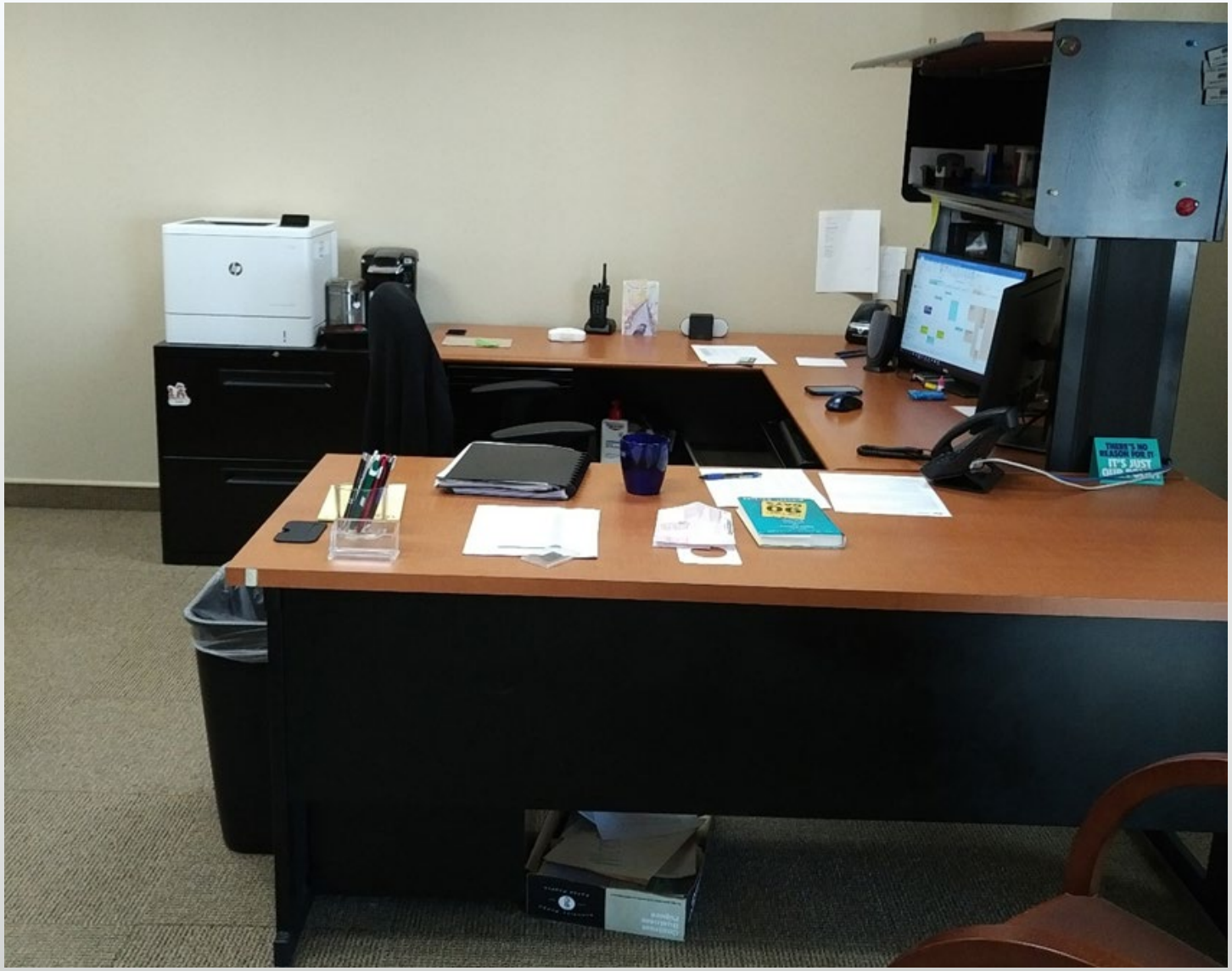


Common Vulnerabilities

- Lack of Executive Support
- Decreased awareness of consequences of unsecured environment
- Outdated/unlicensed hardware and software
- Ineffective or nonexistent policies and procedures
- Sparse oversight
- Lack of training
- Loose enforcement
- Patch and Vulnerability Management delays
- Legacy/Unsupported technology
- Inconsistent Risk Assessment methodology


SMALL AND MEDIUM BUSINESS CYBERSECURITY FUNCTIONAL AREAS, WITH PRIVACY
Security
Data Breach
Data Processors and Transfers
Access Control
Data Rules
Audit & Accountability
Lawfulness of Processing
Awareness and Training
Configuration Management
Privacy Notices
Corporate Rule
System & Informati...
System & Communications Protection
Contingency Planning
Security Assessment & Authorization
Personnel Security
Identification and Authentication
Risk Assessment
Maintenance
Physical & Environmental Protection
Media Protection

Examples from life



Equipment Maintenance

Media Protection

Physical and Environmental Security

Paperwork, Plans, and Responsibility

- Develop a Security Plan
- Develop Contingency Plans
  - Business Continuity Plans
  - Disaster Recovery Plans
  - Cyber Incident Response Plan
    - *BACKUP!!!*
  - Know who to call

Where to Start

1. **Assess** – Conduct an Assessment of your environment to determine vulnerabilities, systems and levels of compliance
2. **Categorize** – Determine which systems are necessary to the organization
3. **Review** – Ensure policies include protocols which will protect environment and *your* specific data
4. **Plan** – Develop plan to migrate environment to a compliant and risk minimal status
5. **Implement**- Policies, procedures, risk assessment, mitigation actions
6. **Re-examine**- Evaluate the changes/updates made
7. **Start over**- Continuous monitoring process

What is involved in an assessment?

- Self Assessment
- Third Party Assessment
- Documentation Review
- System Assessment
  - Architectural Design
  - Vulnerability Scans
  - Web Application Scans
- Plan of Action and Milestones
- Final Report with Recommendations
- Develop Security Plan
- Implement Continuous Improvement

Thanks!

Any questions?

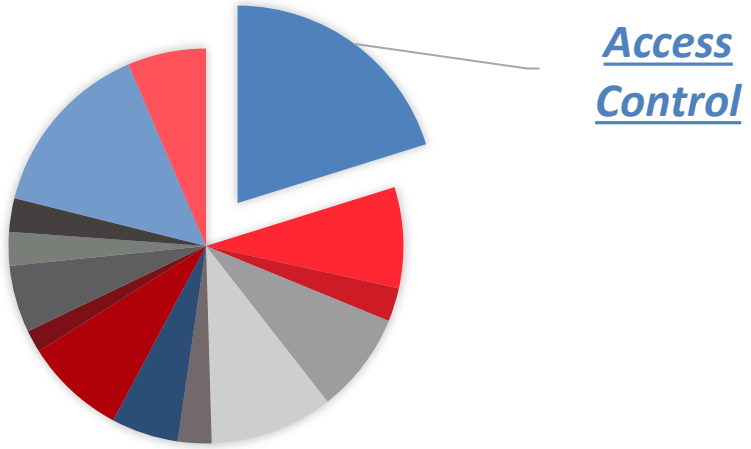
You can find me at:

- 619.928.7600
- Teresa.Rule@RNTPros.com

RNT PROFESSIONAL SERVICES

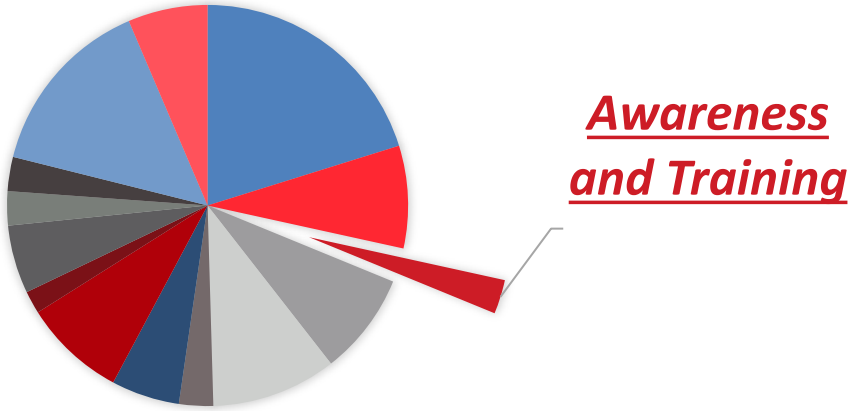
Veterans Defending the Digital Universe™

Access Control (AC)



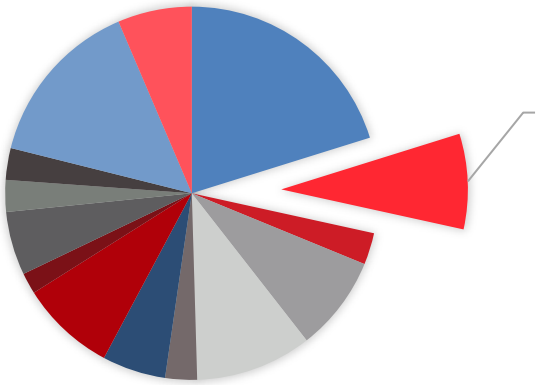
- Is user access limited to authorized personnel?
- Is there an auto disconnect?
- Do you have procedures for searching, reporting and archiving user access to files or folders?

Awareness and Training (AT)



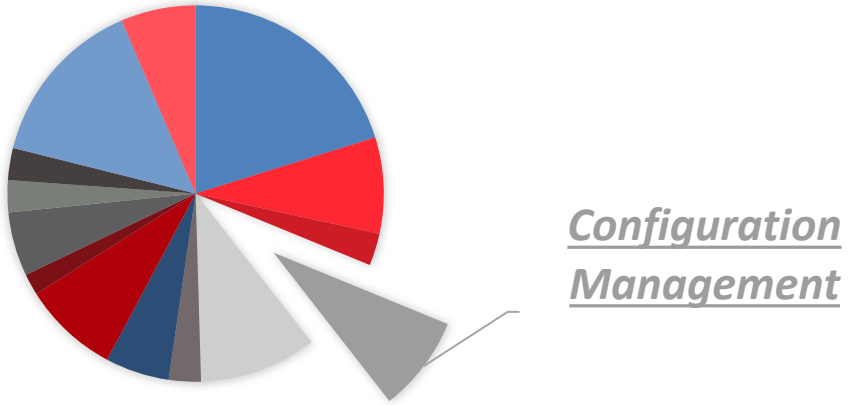
- Is there a system in place to make managers and users aware of security risks?
- What is the procedure for updating employees on updates to standards, regulations, etc.?
- Are users trained to carry out their assigned duties?

Audit and Accountability (AU)



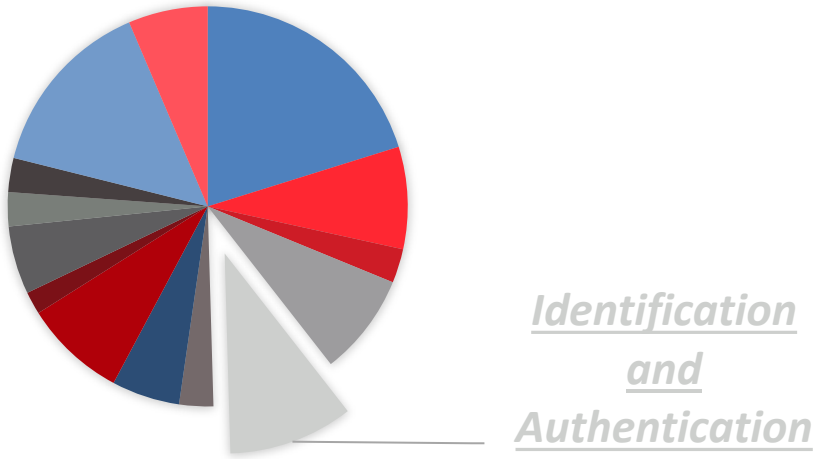
- Are audits conducted on information systems?
- If so, how are those audit records maintained?
- Can actions be traced back to the individual user?

Configuration Management (CM)



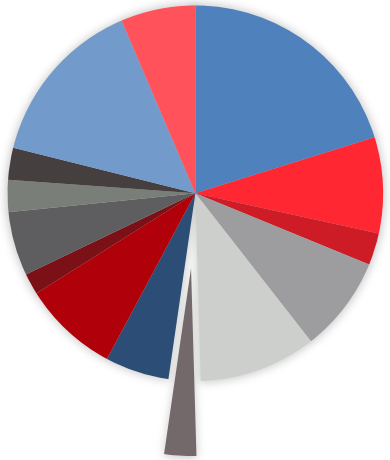
- Has the organization established a baseline configuration?
- Are organizational information systems inventoried?

Identification and Authentication (IA)



- Are all users properly identified and security details logged?
- What authentication steps are in place prior to user access of systems?
- What automated systems are allowed access on behalf of authorized users?

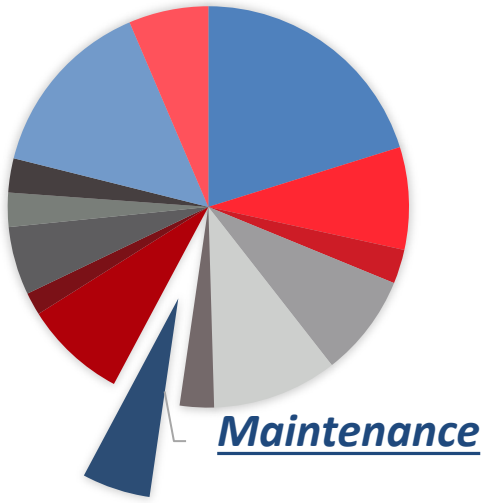
Incident Response (IR)



Incident Response

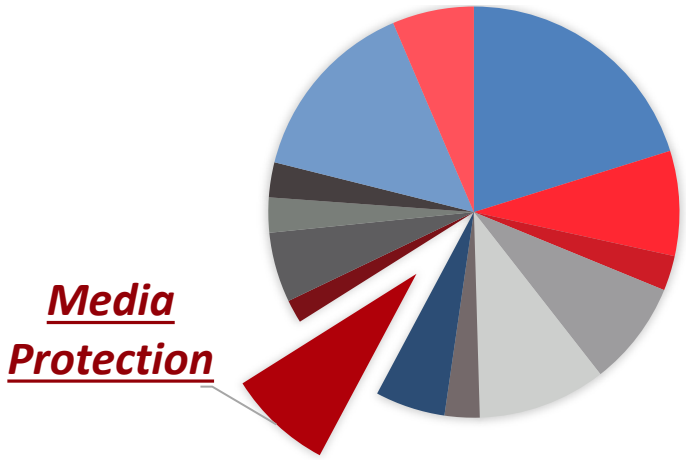
- How are incidents detected?
- What processes are in place for containment if something is detected?
- Are recorded incidents properly escalated and reported per in-house policies and procedures?

Maintenance (MA)



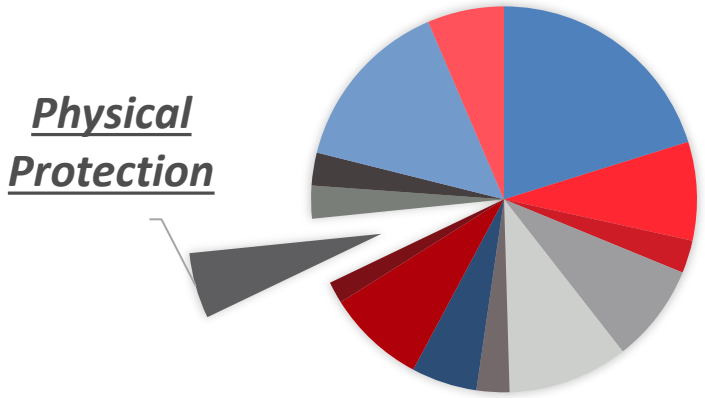
- Is there a documented schedule that shows upcoming maintenance to the information system?
- What processes are in place for maintenance to not impact other operations?
- Are those that should have maintenance access the only ones allowed to access the system?

Media Protection (MP)



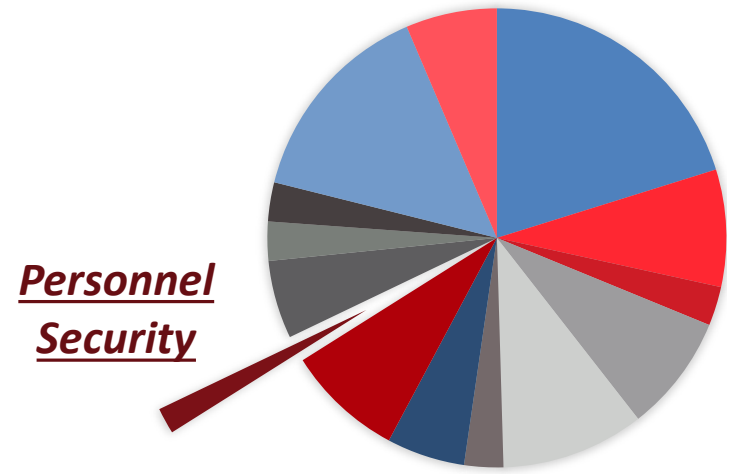
- How is information system media protected?
- Do only authorized users have access to said information media?
- How is that access being audited/monitored?
- How is media sanitized or disposed?

Physical Protection (PE)



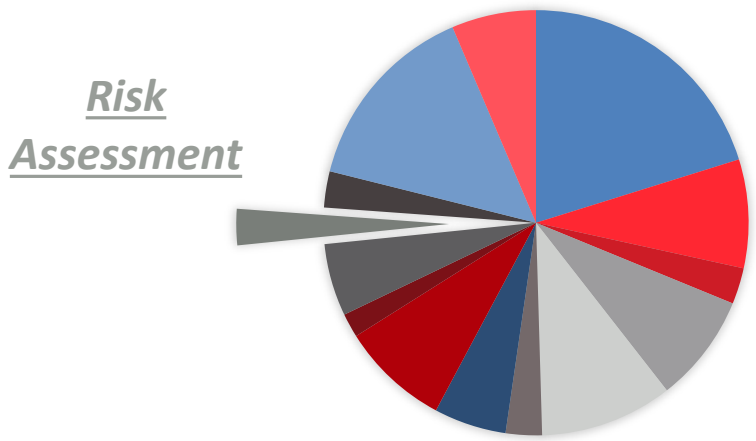
- What barriers are in place to limit access to operating environments?
- Are there supporting utilities for the information system?
- How are the systems protected from environmental hazards?
- Are the necessary facility controls in place?

Personnel Security (PS)



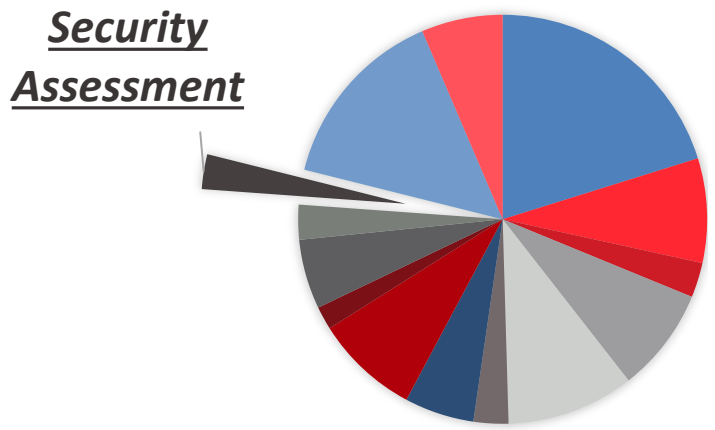
- Have all individuals, including third-party vendors, been vetted through approved security criteria?
- What policies and procedures are in place for terminated or transferred associates?
- Are there formal sanctions in place for someone who fails to comply with organizational policies and procedures?

Risk Assessment (RA)



- When was the last risk assessment completed?
- What is the potential fallout to the organization's image or reputation from negative assessment?
- Were all aspects of the operational information systems reviewed -- Including items such as the storage of organizational information?

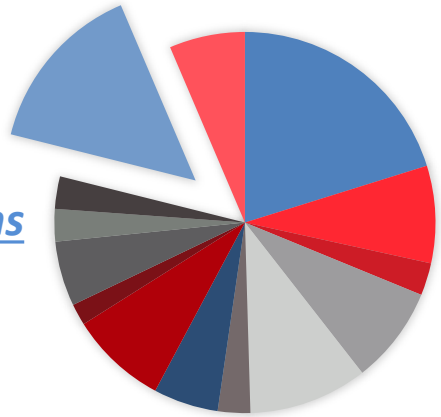
Security Assessment (SA)



- Has the organization allocated enough resources to protect the information systems?
- Are there installation restrictions within the system?
- Do vendors provide adequate protection of organizational information?

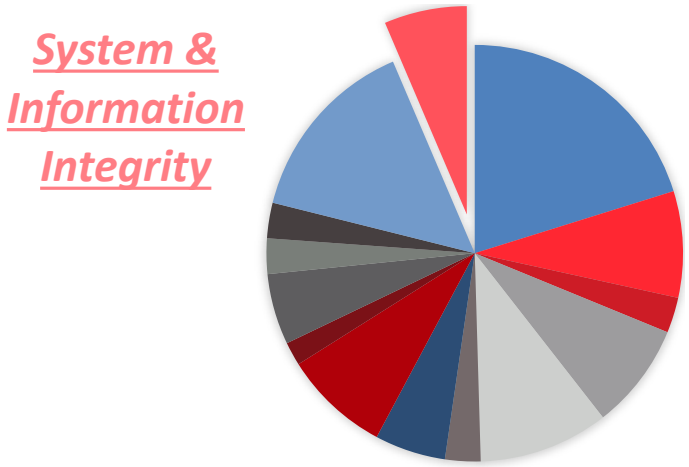
System and Communications Protection (SC)

System & Communications Protection



- How is organizational communication monitored and controlled?
- Are there anti-phishing processes in place?
- What architectural designs and software development techniques are in place to promote effective information security?

System & Information Integrity (SI)



- How are system flaws identified, reported, and corrected?
- Are there safeguards in place to protect from malicious code?
- What policies and procedures are in place to respond to a security alert?