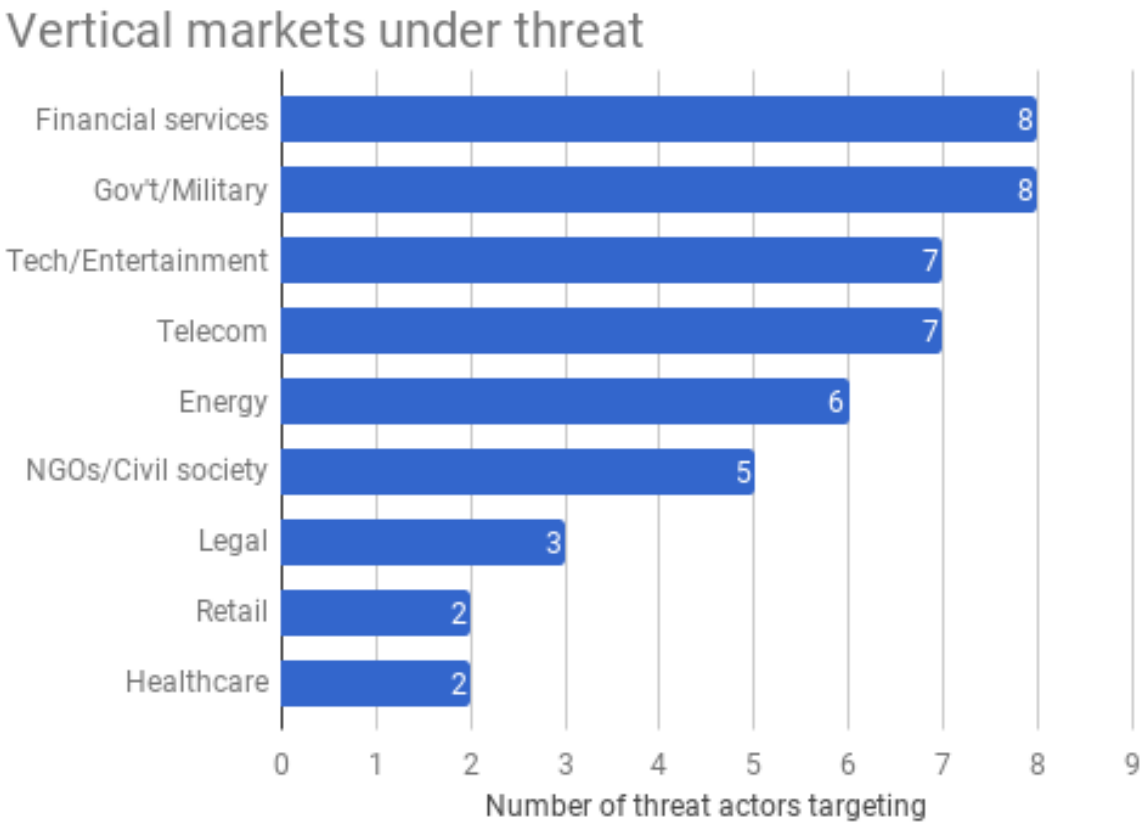
NCUA
National Credit Union Administration

Office of Examination & Insurance (E&I)

# Cybersecurity

*NCUA Board of Directors – October 2019*

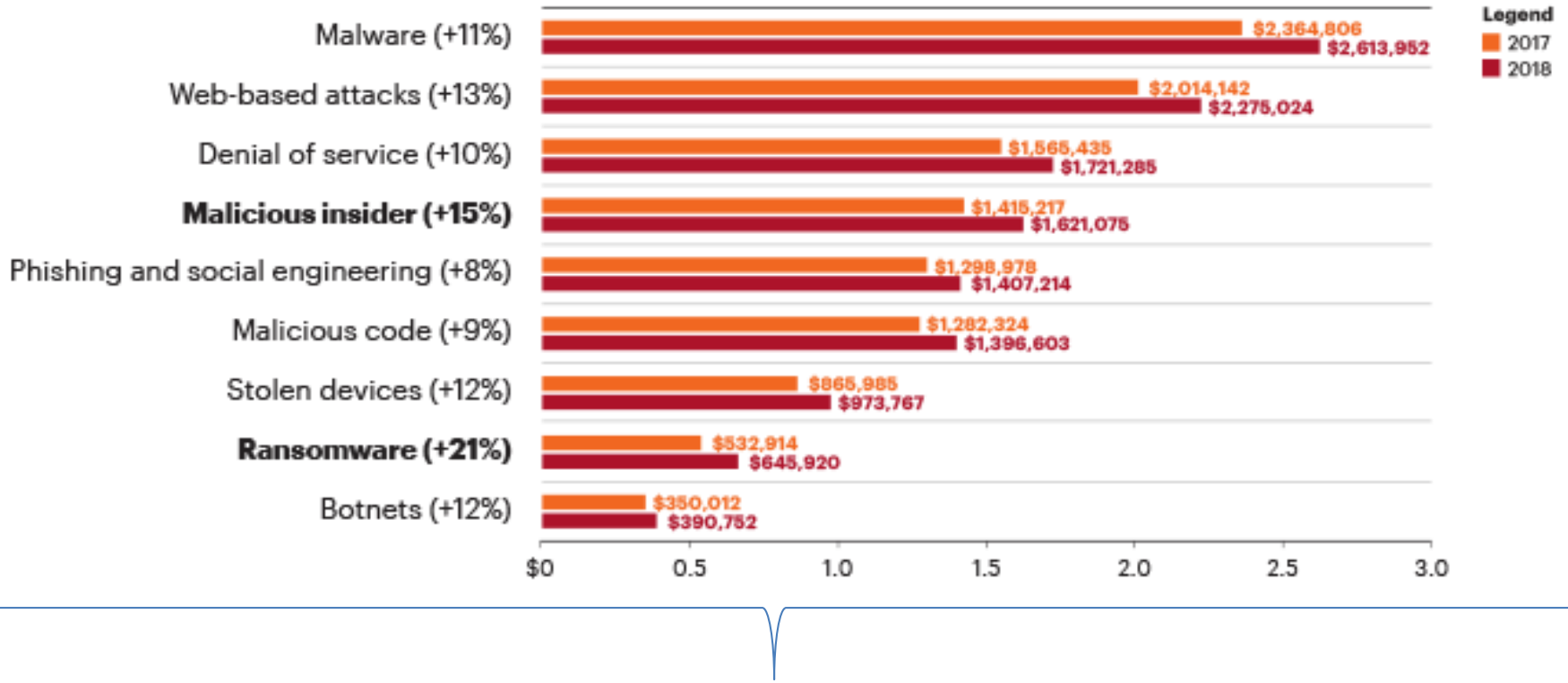
# Cybersecurity Landscape Overview - **Financial Service Target Profile**




**Note:** Large amount of Personal and Financial Information and actual Monetary targets

*Source Flashpoint*

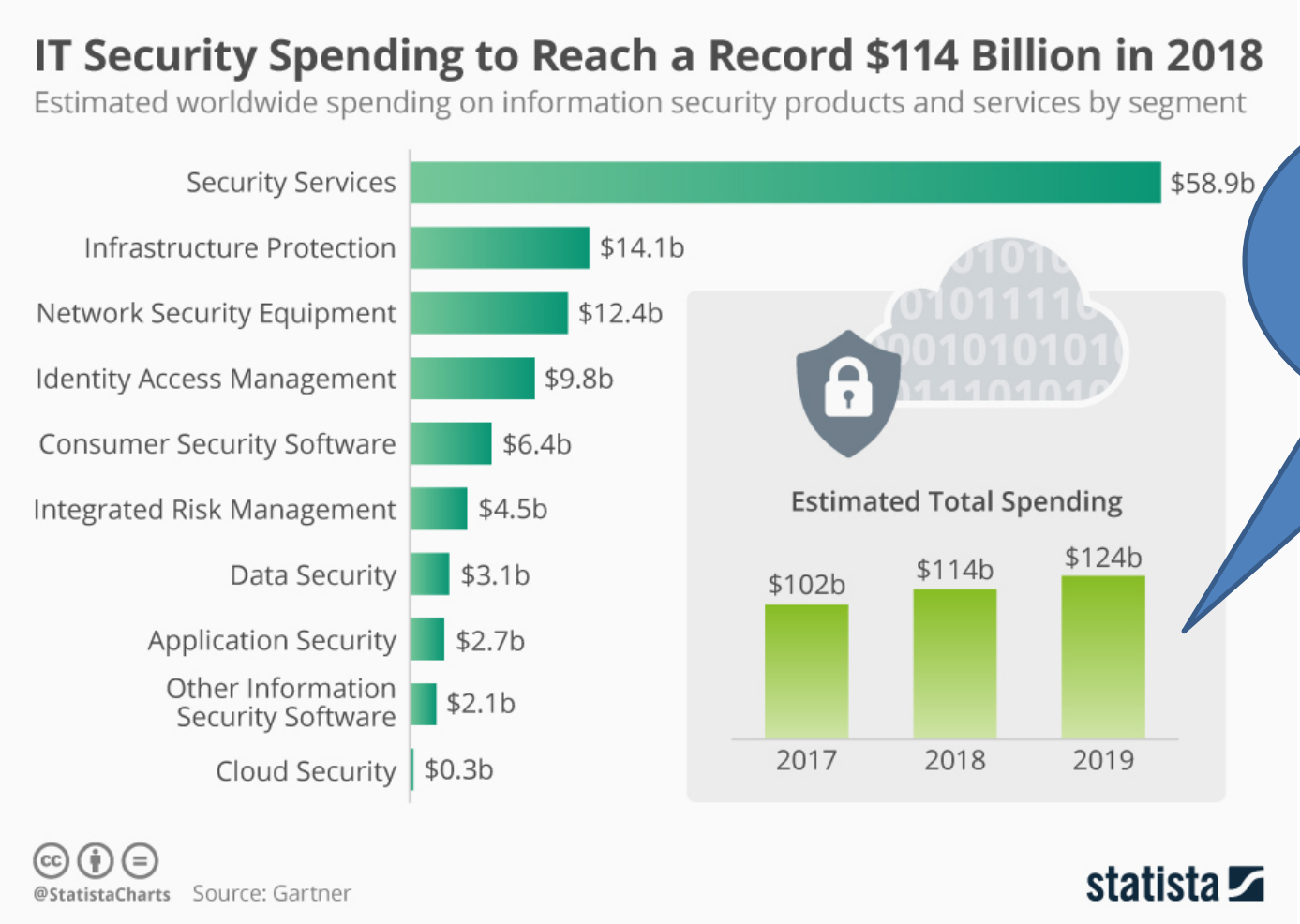
# Cybersecurity Landscape Overview – **Attack Methods**




**Note:** Additional layered complexity and persistence still equates to the same predominate root cause

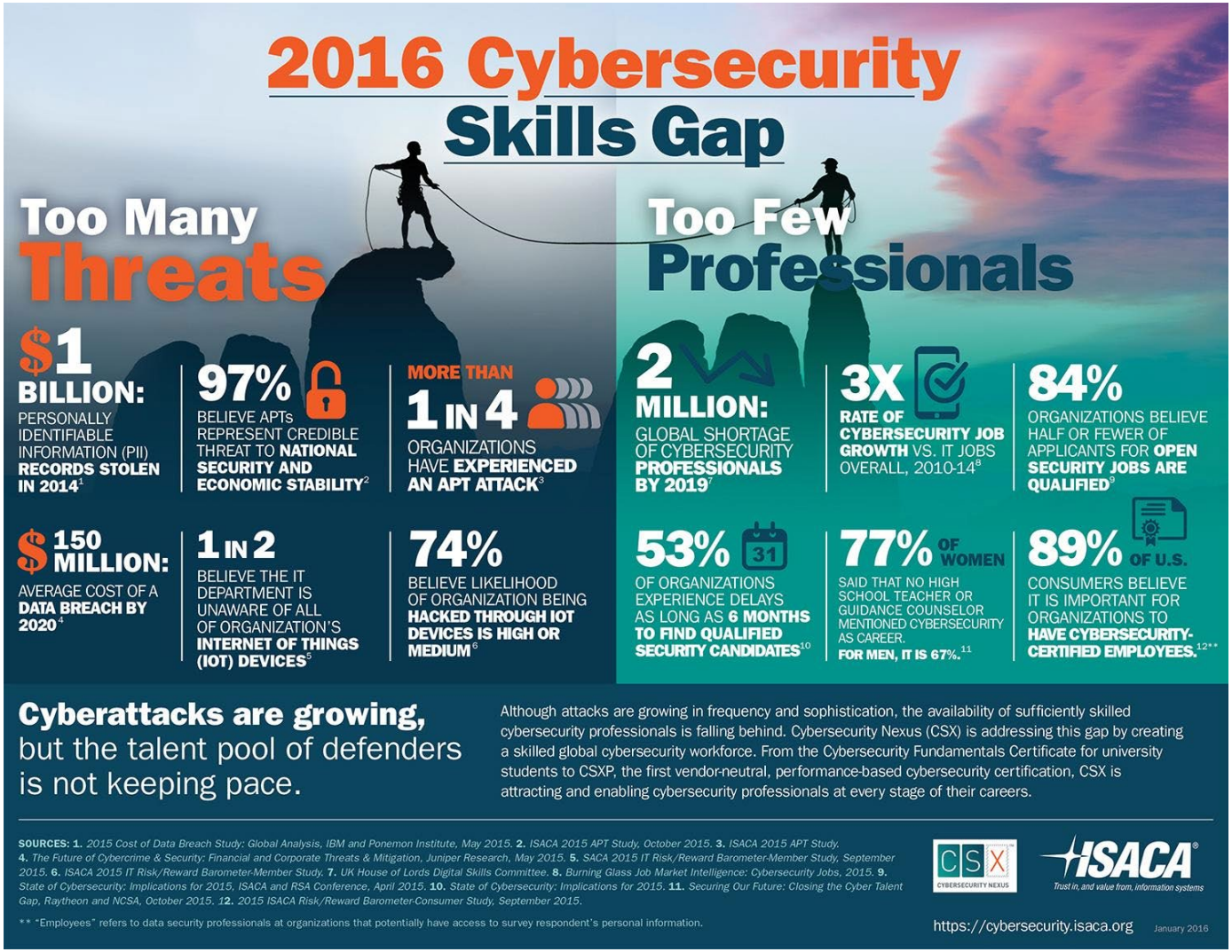
*Accenture 2019 Cost of Cybercrime Study*

# Cybersecurity Landscape Overview – **IT Spending**



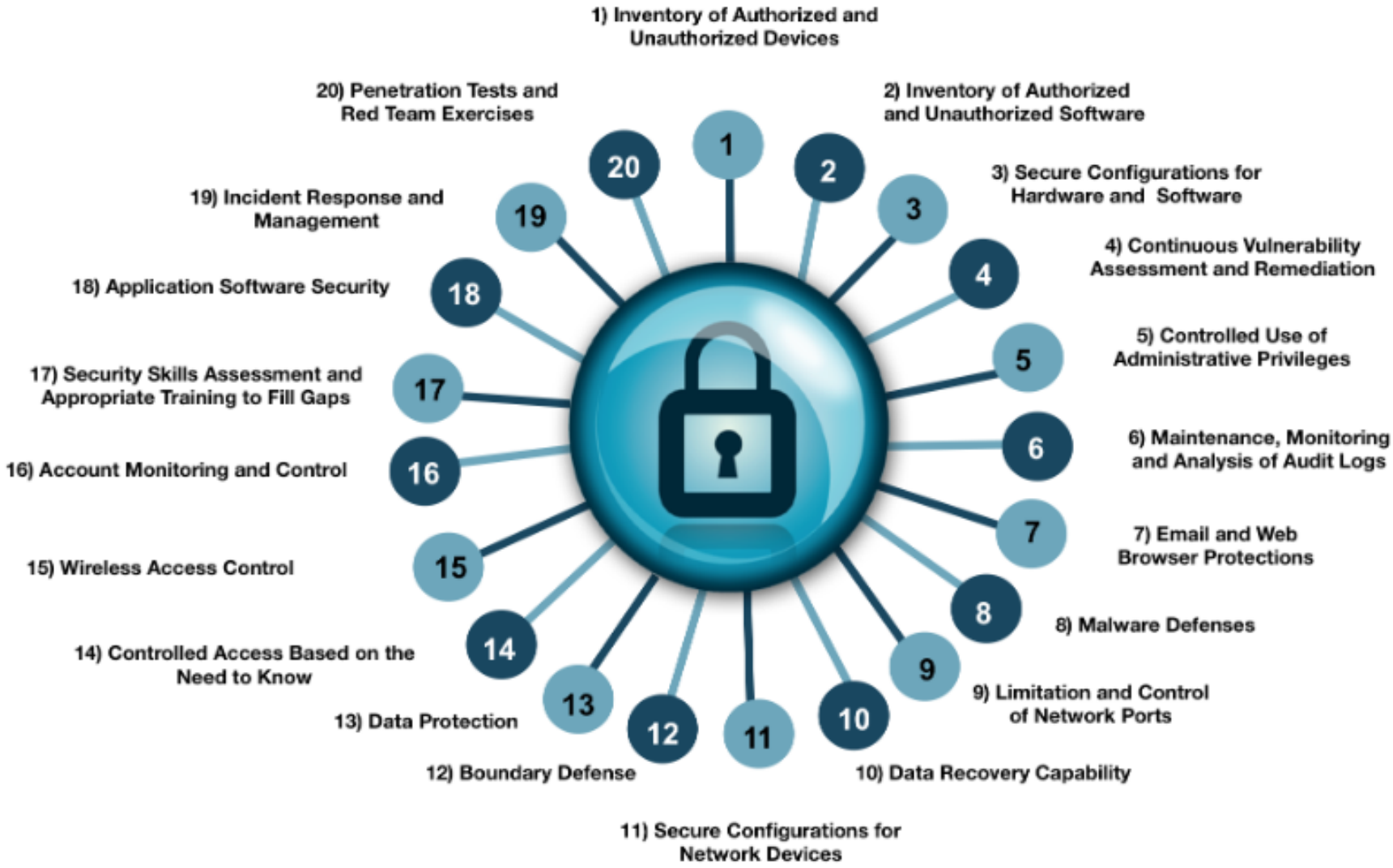

Benefits also share increased **concentration risk** e.g. business services, cloud providers, managed security services

# Cybersecurity Landscape Overview – **Talent Management**




- Highly technical skills e.g. **threat hunt team members** (Red Team/Blue Team, etc.) vs. leadership/ management resources
- Demand more of system administrators, engineers, and programmers by way of **Service Management/ Delivery**

# Cybersecurity Landscape Overview – **Critical Security Controls (Root Cause)**



# Cybersecurity Landscape Overview – **Resilience**

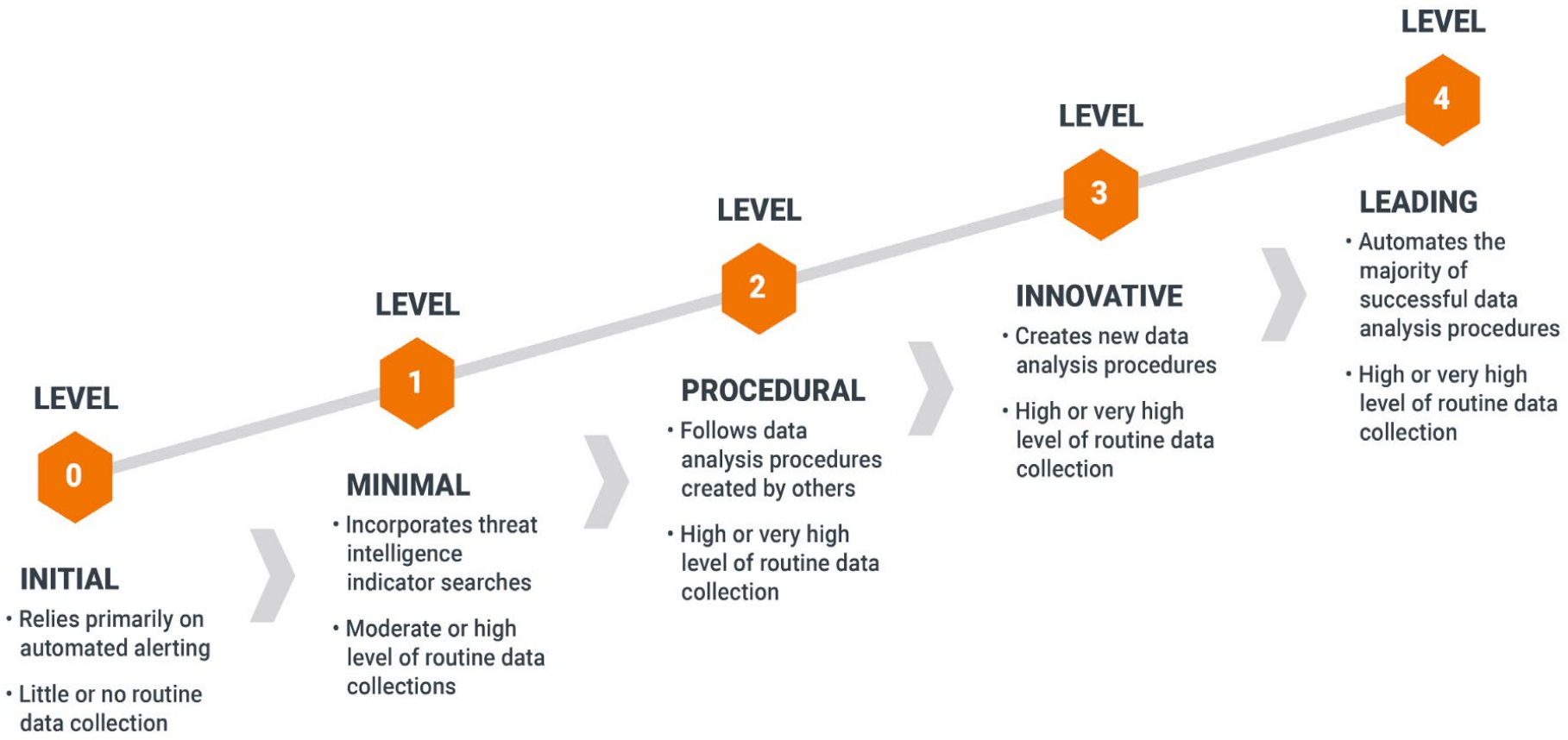
## Cybersecurity Resilience Maturity Framework

| | Maturity Descriptor | Employment of Security Controls | Security Tailored to Mission | Participate in Information Sharing (threat/vul.) | Response to Cyber Threats | Resilience to Cyber Attacks |
|---|---|---|---|---|---|---|
| Step 2: Address Sophisticated Attacks | Level 5: Resilient | Augment CSC Based on Mission | Mission Assurance Focused | Real Time Response to Inputs | Anticipate Threats | Operate Through Sophisticated Attack |
| | Level 4: Dynamic | Augment CSC Based on Mission | Mission Focused | Real Time Response to Inputs | Rapid Reaction To Threats | Able to respond to Sophisticated Attack |
| Step 1: Implement CSC Baseline | Level 3: Managed | CSC Integrated and Continuously Monitored | Partially Mission Focused | Respond to Information Inputs | Respond to Attacks After the Fact | Protection against Unsophisticated Attack |
| | Level 2: Performed | Foundational/ Critical Security Controls (CSC) Implemented | Mission Agnostic | Inconsistent Response to Information Inputs | Respond to Attacks After the Fact | Some Protection Against Unsophisticated Attacks |
| | Level 1: No Resilience | Inconsistent Deployment of Security Controls | None | None | No Response | Susceptible to Unsophisticated Attacks |

The **"when"** paradigm

The **"if"** paradigm

# Cybersecurity Landscape Overview – **Threat Hunting**



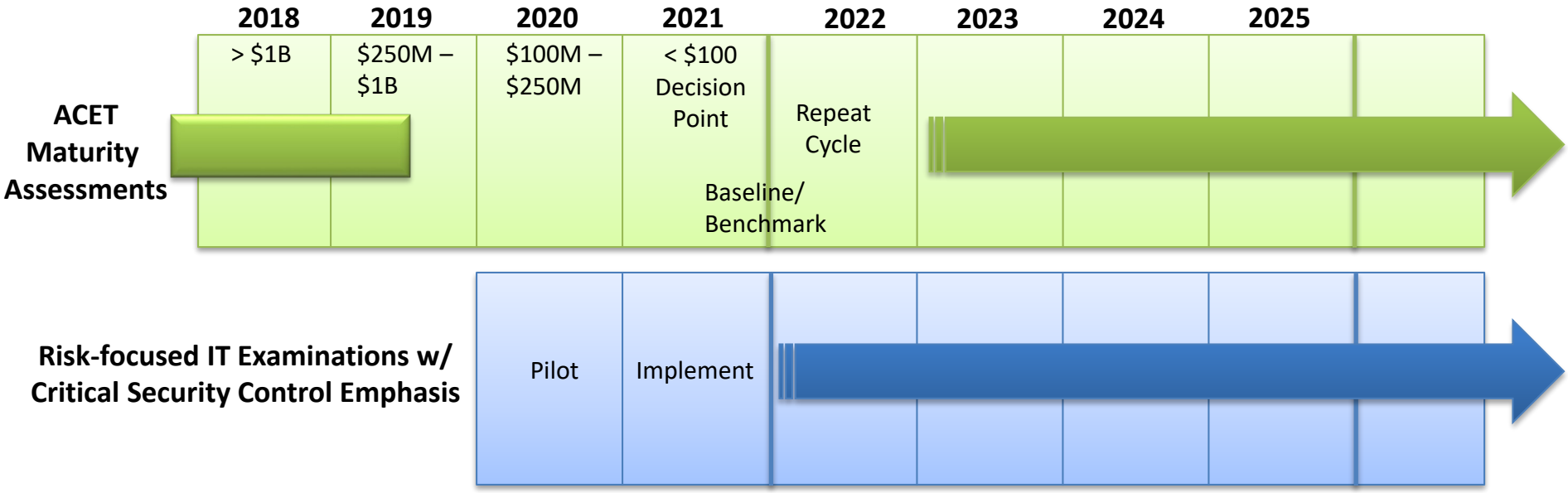

**Note:** Informed by the Risk Assessment/Business Impact Analysis

**"Know the Business"**

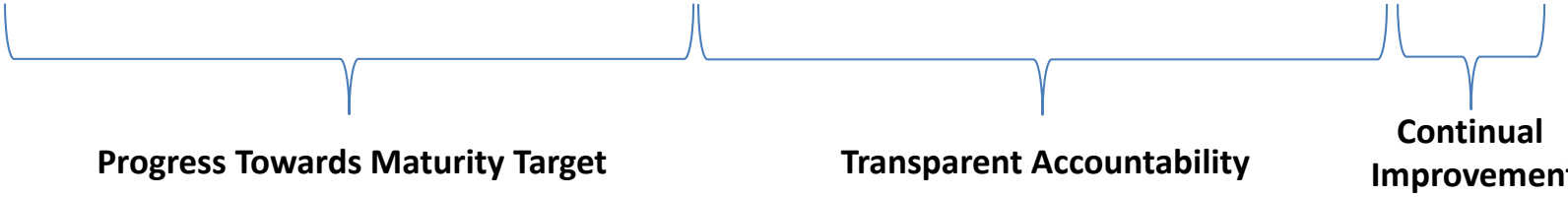
# Chairman's Cybersecurity Priorities

- **Advancing consistency, transparency and accountability within the cybersecurity examination program;**
- **Stimulating due diligence for Supply Chain and Third-Party Service Provider management within the credit union sub-sector;**
- **Assisting institutions with resources to improve operational hygiene and resilience; and**
- **Ensure NCUA's systems and collected, controlled, unclassified information are secure.**

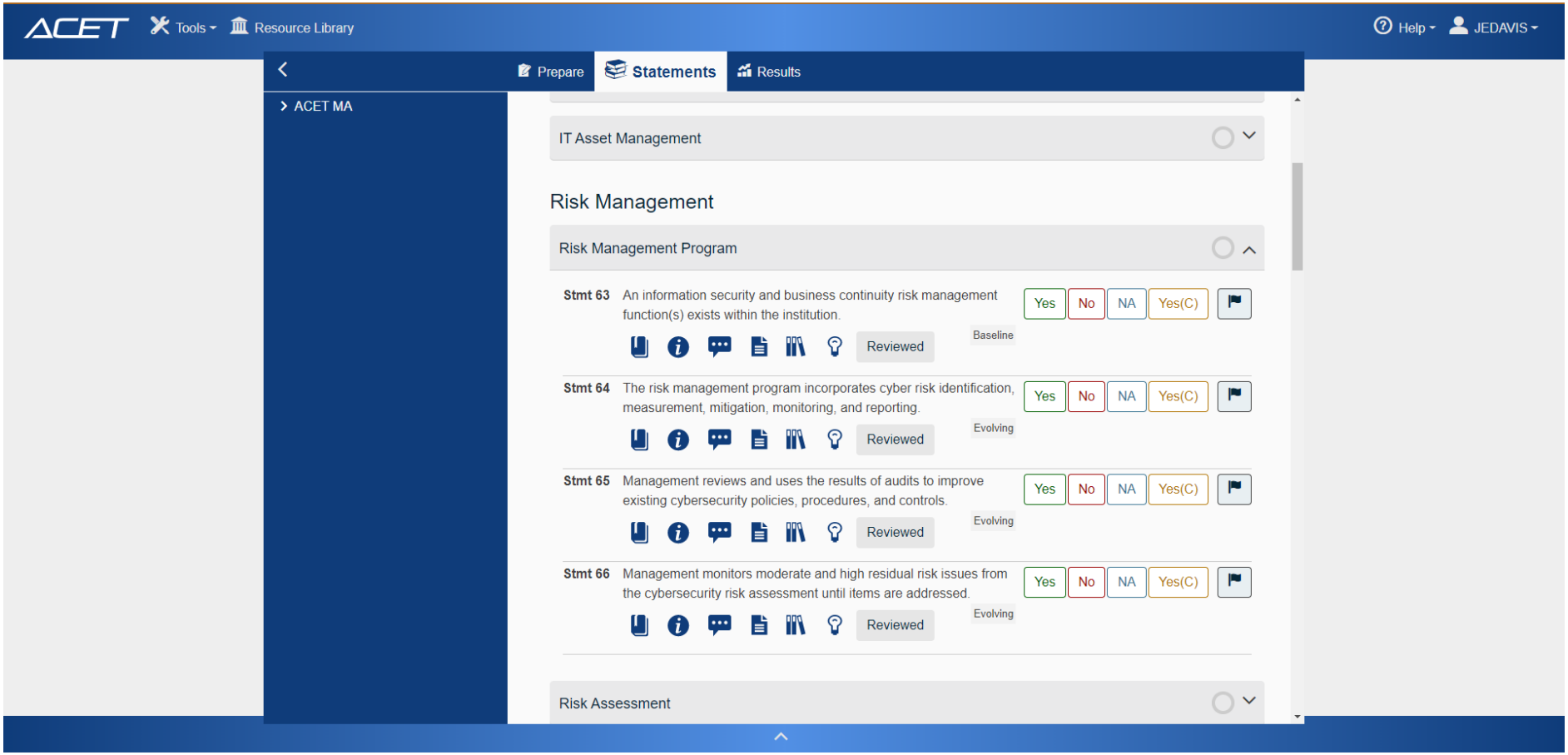
# Projected Phased Implementation Plan




*["High Risk" Scoping Proof of Concept]*



# Automated Cybersecurity Examination Toolbox (ACET) Maturity Assessments

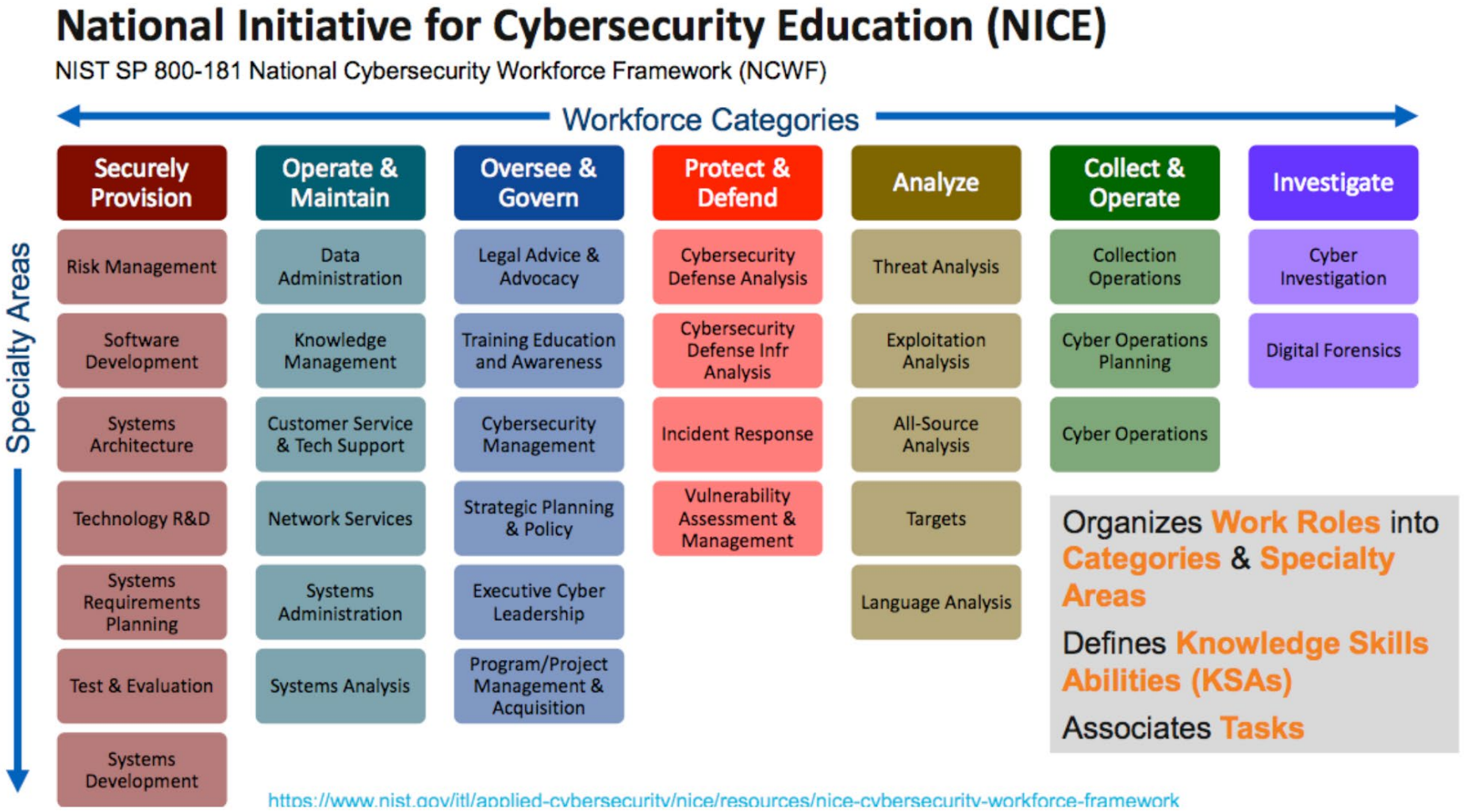



**Note:** Enhancement of ACET with Idaho National Labs (INL) based on the DHS Cyber Security Evaluation Tool (CSET) will be offered to industry via ncua.gov in 2020

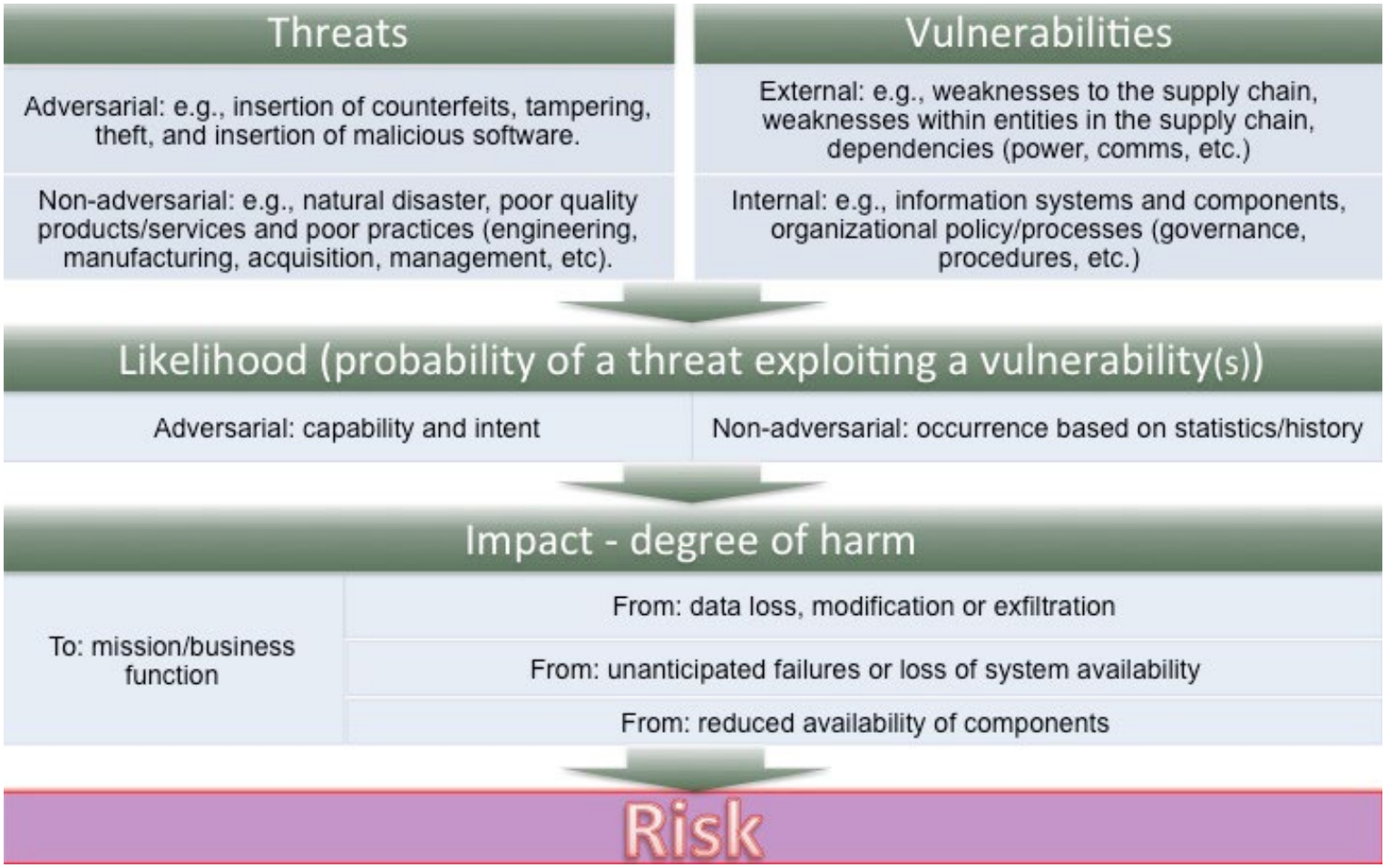
# Training, Education, & Awareness (TEA) – Current Evolution

| New Examiners STEP | CORE Technical | Subject Matter Examiner (SME) | National and Regional Information Systems Officers | Industry and Agency Conferences |
|---|---|---|---|---|
| ▪ **STEP 9: Risk-Focused Examination Process (#119)**<br>▪ **eLearning: Information Technology for Examiners (#125)** | ▪ **Cybersecurity – C Examiner Training Series (Cyber-C) eLearning Plan**<br>▪ **Cybersecurity Examination Process (#227)**<br>▪ ***LearnCenter – Information Technology, BSA/AML, Payments, etc*** | ▪ **ISACA CSX Cybersecurity Fundamentals Workshop (#361)**<br>▪ **IT SME OJT (#254)**<br>▪ **IT SME Forum (#704)**<br>▪ *LearnCenter – Information Technology, BSA/AML, Payments, etc* | ▪ *LearnCenter – Information Technology, BSA/AML, Payments, etc* | ▪ **FIS Regulatory University - Information Technology, BSA/AML, Payments, etc.**<br>▪ **FFIEC/FDIC - Information Technology, BSA/AML, Payments, etc.**<br>▪ **Professional Designations and External Conferences**<br>**- FFIEC IT Conference** |

# DHS National Initiative of Cybersecurity Education (NICE) Framework

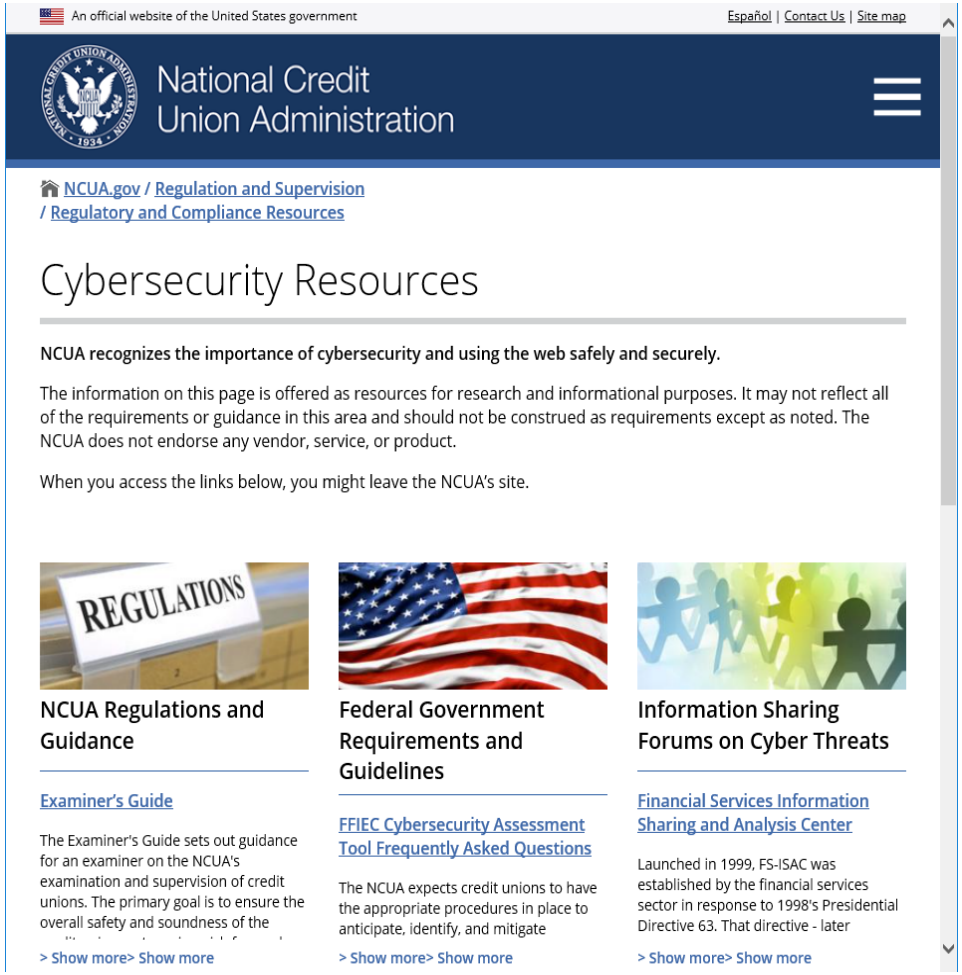


# Supplier Risk Management




**Note:** Due diligence with additional resources e.g. contracts, service level agreements, Key performance indicators (KPI), key risk indicators (KRI)

# Cybersecurity Resources



An official website of the United States government

Español | Contact Us | Site map

National Credit Union Administration

NCUA.gov / Regulation and Supervision / Regulatory and Compliance Resources

## Cybersecurity Resources

**NCUA recognizes the importance of cybersecurity and using the web safely and securely.**

The information on this page is offered as resources for research and informational purposes. It may not reflect all of the requirements or guidance in this area and should not be construed as requirements except as noted. The NCUA does not endorse any vendor, service, or product.

When you access the links below, you might leave the NCUA's site.




### NCUA Regulations and Guidance

Examiner's Guide

The Examiner's Guide sets out guidance for an examiner on the NCUA's examination and supervision of credit unions. The primary goal is to ensure the overall safety and soundness of the

> Show more> Show more



### Federal Government Requirements and Guidelines

FFIEC Cybersecurity Assessment Tool Frequently Asked Questions

The NCUA expects credit unions to have the appropriate procedures in place to anticipate, identify, and mitigate

> Show more> Show more

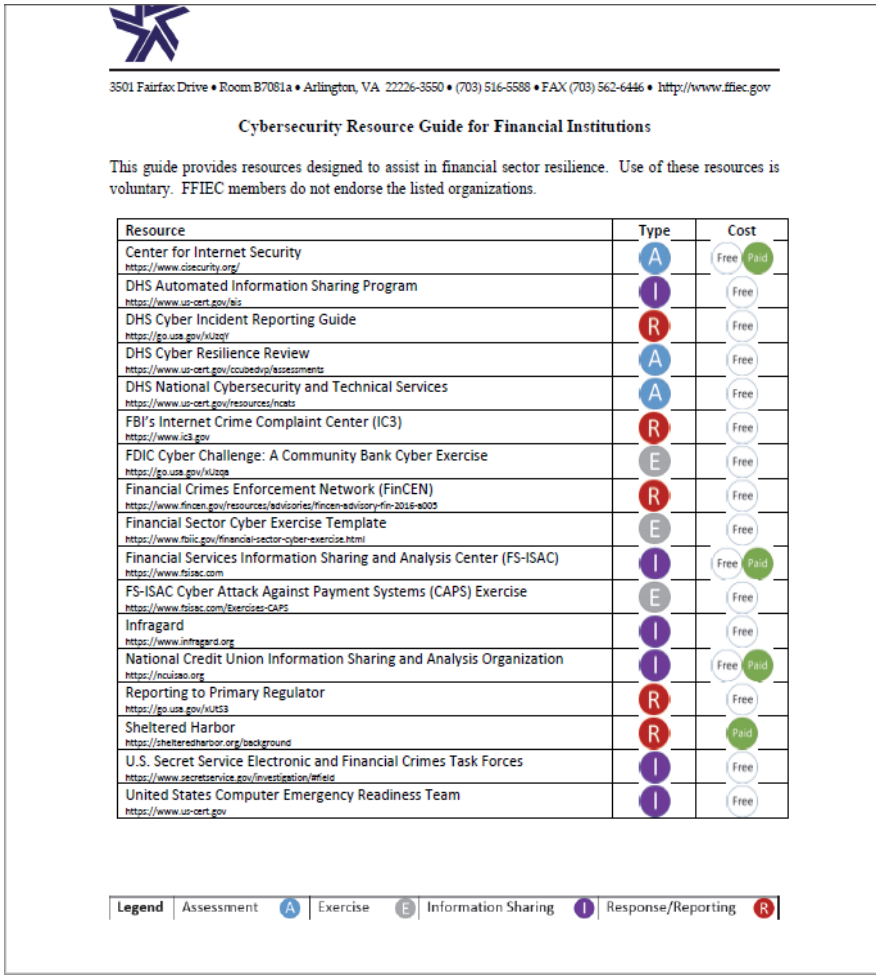


### Information Sharing Forums on Cyber Threats

Financial Services Information Sharing and Analysis Center

Launched in 1999, FS-ISAC was established by the financial services sector in response to 1998's Presidential Directive 63. That directive - later

> Show more> Show more



3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 • http://www.ffiec.gov

**Cybersecurity Resource Guide for Financial Institutions**

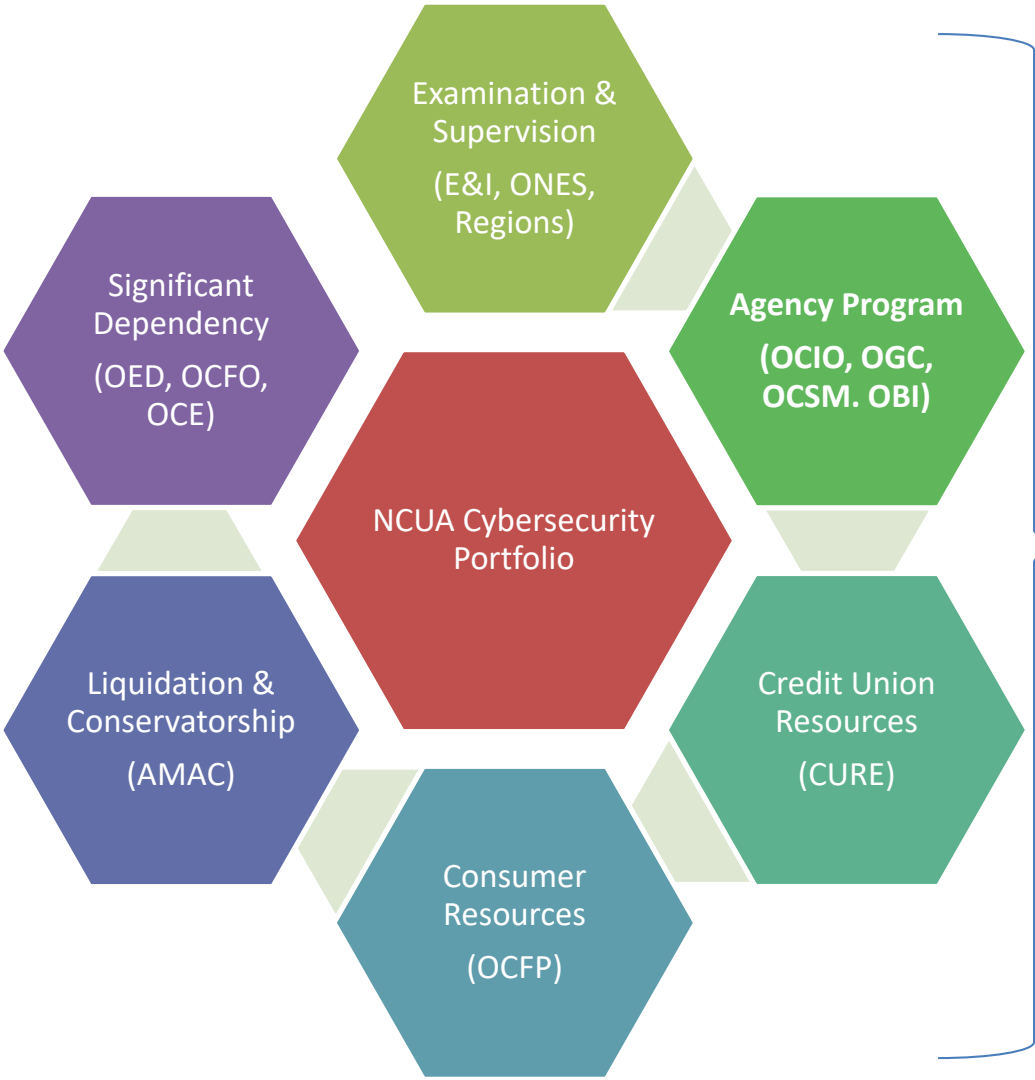
This guide provides resources designed to assist in financial sector resilience. Use of these resources is voluntary. FFIEC members do not endorse the listed organizations.

| Resource | Type | Cost |
|---|---|---|
| Center for Internet Security<br>https://www.cisecurity.org/ | A | Free Paid |
| DHS Automated Information Sharing Program<br>https://www.us-cert.gov/ais | I | Free |
| DHS Cyber Incident Reporting Guide<br>https://go.usa.gov/xUzqY | R | Free |
| DHS Cyber Resilience Review<br>https://www.us-cert.gov/ccubedvp/assessments | A | Free |
| DHS National Cybersecurity and Technical Services<br>https://www.us-cert.gov/resources/ncats | A | Free |
| FBI's Internet Crime Complaint Center (IC3)<br>https://www.ic3.gov | R | Free |
| FDIC Cyber Challenge: A Community Bank Cyber Exercise<br>https://go.usa.gov/xUzqa | E | Free |
| Financial Crimes Enforcement Network (FinCEN)<br>https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005 | R | Free |
| Financial Sector Cyber Exercise Template<br>https://www.fdic.gov/financial-sector-cyber-exercise.html | E | Free |
| Financial Services Information Sharing and Analysis Center (FS-ISAC)<br>https://www.fsisac.com | I | Free Paid |
| FS-ISAC Cyber Attack Against Payment Systems (CAPS) Exercise<br>https://www.fsisac.com/Exercises-CAPS | E | Free |
| Infragard<br>https://www.infragard.org | I | Free |
| National Credit Union Information Sharing and Analysis Organization<br>https://ncuisao.org | I | Free Paid |
| Reporting to Primary Regulator<br>https://go.usa.gov/xUtS3 | R | Free |
| Sheltered Harbor<br>https://shelteredharbor.org/background | R | Paid |
| U.S. Secret Service Electronic and Financial Crimes Task Forces<br>https://www.secretservice.gov/investigation/#field | I | Free |
| United States Computer Emergency Readiness Team<br>https://www.us-cert.gov | I | Free |

Legend | Assessment A | Exercise E | Information Sharing I | Response/Reporting R

**Note:** Recent example in the pending State Cybercrime resource list

# Agency Cybersecurity Portfolio




**Establish Cybersecurity Coordination**
**<u>Working Group</u> Under**
- Enterprise Risk Management Committee (ERMC) and/or
- Cybersecurity Steering Committee (CSSC)

Office of Examination & Insurance (E&I)

# NCUA BOARD MEETING – OCTOBER 2019