



NCUA
National Credit Union Administration

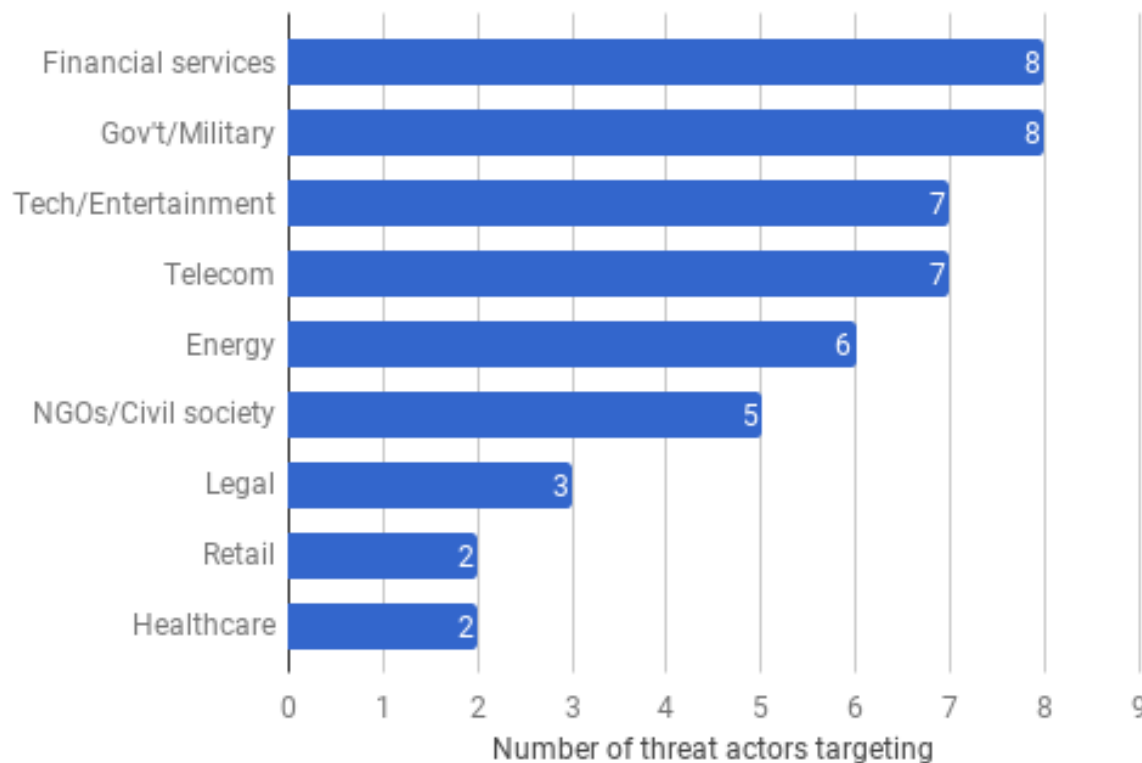
Office of Examination & Insurance
(E&I)

Cybersecurity

*NCUA Board of Directors –
October 2019*

Cybersecurity Landscape Overview - Financial Service Target Profile

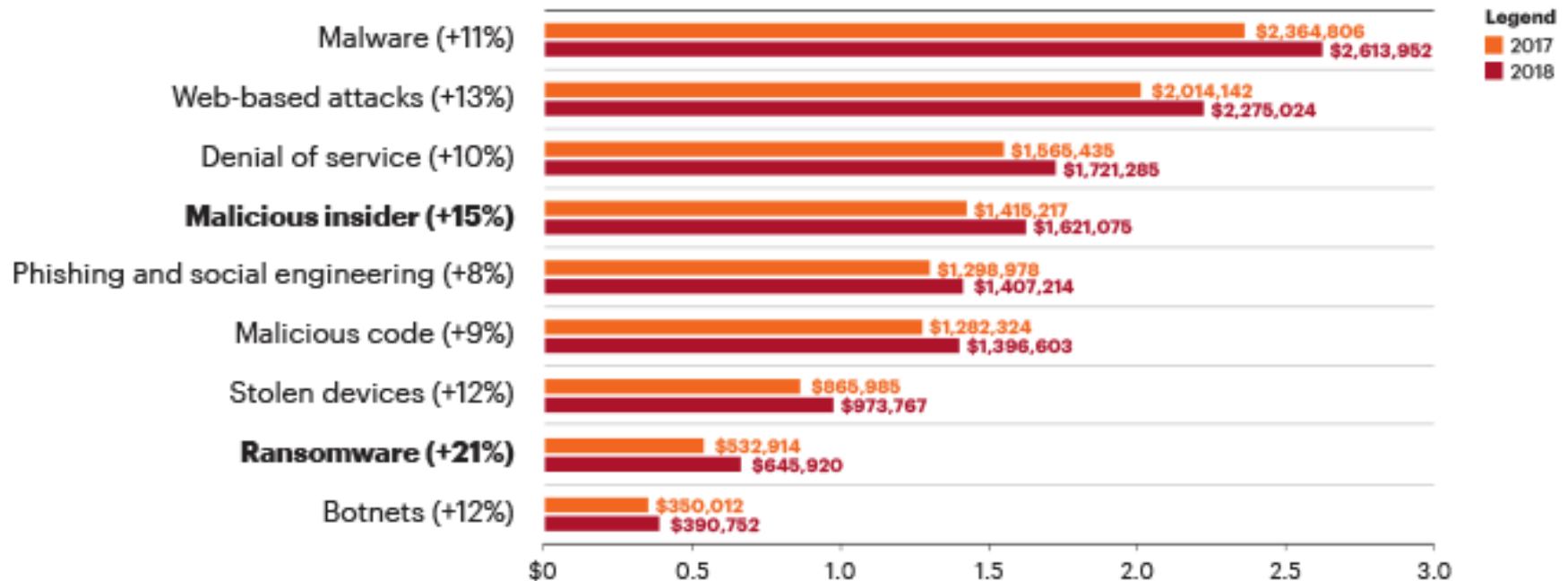
Vertical markets under threat



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

Source Flashpoint

Cybersecurity Landscape Overview – Attack Methods

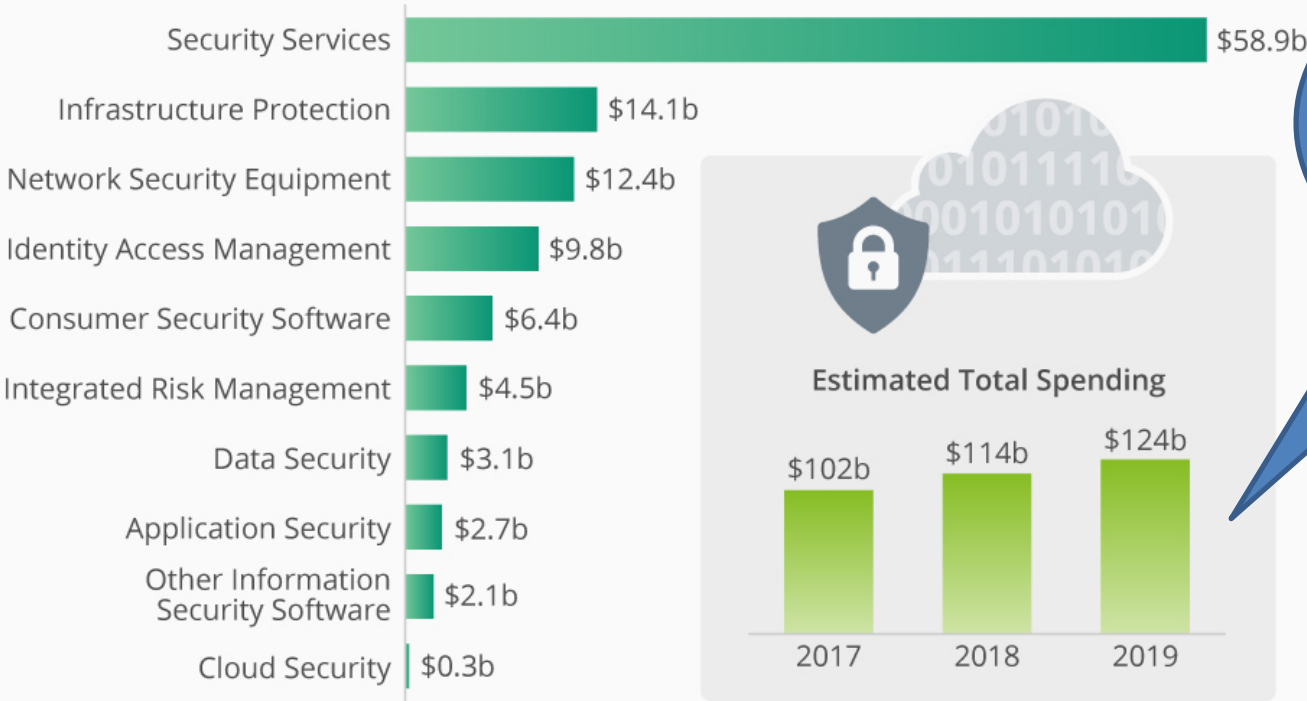


Note: Additional layered complexity and persistence still equates to the same predominate root cause

Cybersecurity Landscape Overview – IT Spending

IT Security Spending to Reach a Record \$114 Billion in 2018

Estimated worldwide spending on information security products and services by segment



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



@StatistaCharts Source: Gartner



Cybersecurity Landscape Overview – Talent Management

2016 Cybersecurity Skills Gap

Too Many Threats

\$1 BILLION: PERSONALLY IDENTIFIABLE INFORMATION (PII) RECORDS STOLEN IN 2014¹

97% BELIEVE APTs REPRESENT CREDIBLE THREAT TO NATIONAL SECURITY AND ECONOMIC STABILITY²

MORE THAN 1 IN 4 ORGANIZATIONS HAVE EXPERIENCED AN APT ATTACK³

\$150 MILLION: AVERAGE COST OF A DATA BREACH BY 2020⁴

1 IN 2 BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION'S INTERNET OF THINGS (IOT) DEVICES⁵

74% BELIEVE LIKELIHOOD OF ORGANIZATION BEING HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM⁶

Too Few Professionals

2 MILLION: GLOBAL SHORTAGE OF CYBERSECURITY PROFESSIONALS BY 2019⁷

3X RATE OF CYBERSECURITY JOB GROWTH VS. IT JOBS OVERALL, 2010-14⁸

84% ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR OPEN SECURITY JOBS ARE QUALIFIED⁹

53% OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS 6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES¹⁰

77% OF WOMEN SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS CAREER. FOR MEN, IT IS 67%.¹¹

89% OF U.S. CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO HAVE CYBERSECURITY-CERTIFIED EMPLOYEES.^{12**}

Cyberattacks are growing, but the talent pool of defenders is not keeping pace.

Although attacks are growing in frequency and sophistication, the availability of sufficiently skilled cybersecurity professionals is falling behind. Cybersecurity Nexus (CSX) is addressing this gap by creating a skilled global cybersecurity workforce. From the Cybersecurity Fundamentals Certificate for university students to CSXP, the first vendor-neutral, performance-based cybersecurity certification, CSX is attracting and enabling cybersecurity professionals at every stage of their careers.

SOURCES: 1. 2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, May 2015. 2. ISACA 2015 APT Study, October 2015. 3. ISACA 2015 APT Study, October 2015. 4. The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation, Juniper Research, May 2015. 5. ISACA 2015 IT Risk/Reward Barometer-Member Study, September 2015. 6. ISACA 2015 IT Risk/Reward Barometer-Member Study, September 2015. 7. UK House of Lords Digital Skills Committee. 8. Burning Glass Job Market Intelligence: Cybersecurity Jobs, 2015. 9. State of Cybersecurity: Implications for 2015, ISACA and RSA Conference, April 2015. 10. State of Cybersecurity: Implications for 2015. 11. Securing Our Future: Closing the Cyber Talent Gap, Raytheon and NCSA, October 2015. 12. 2015 ISACA Risk/Reward Barometer-Consumer Study, September 2015.

** "Employees" refers to data security professionals at organizations that potentially have access to survey respondent's personal information.



<https://cybersecurity.isaca.org>

January 2016

- 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

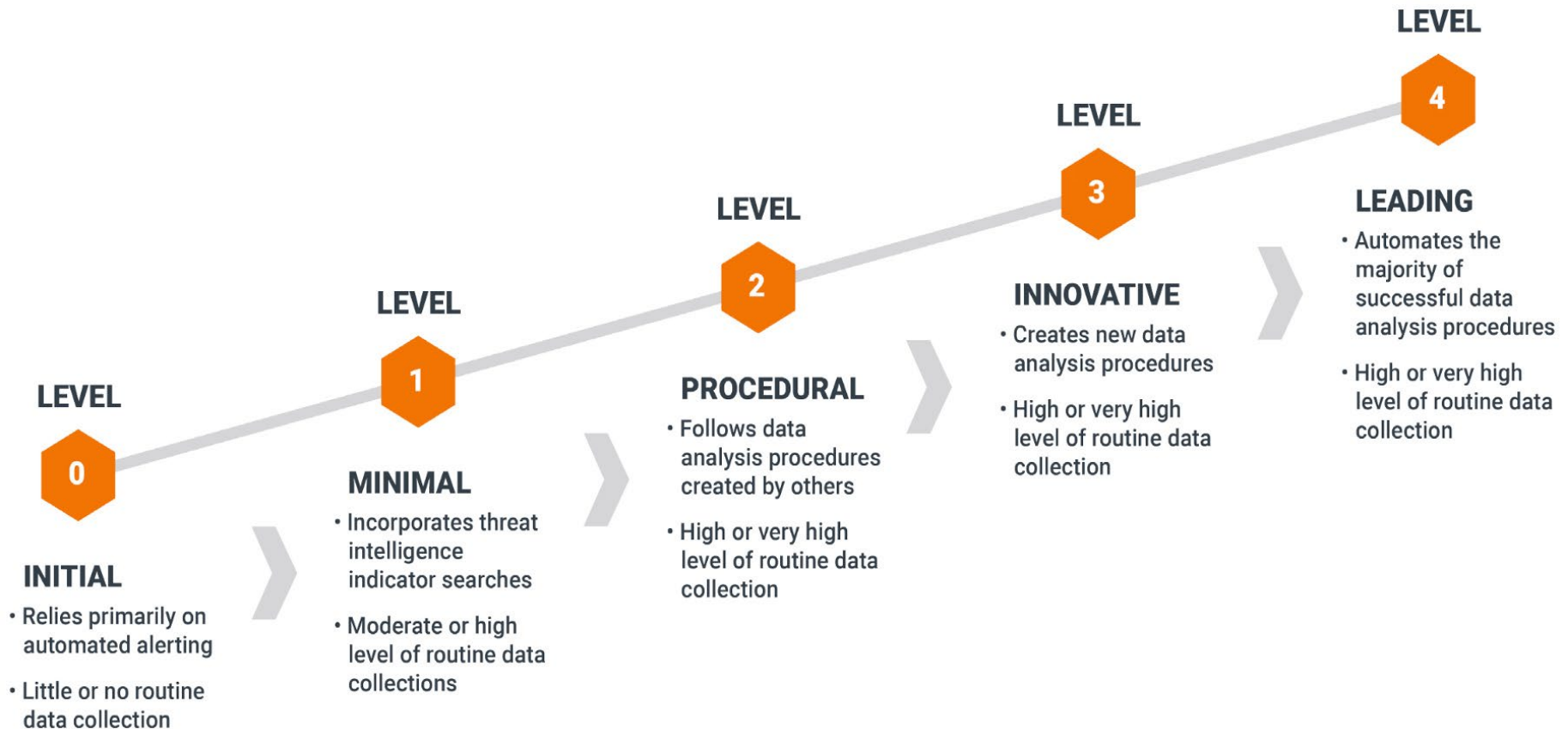
Cybersecurity Resilience Maturity Framework

	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	RealTime Response to Inputs	Anticipate Threats	Operate Through Sophisticated Attack
	Level 4: Dynamic	Augment CSC Based on Mission	Mission Focused	RealTime 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

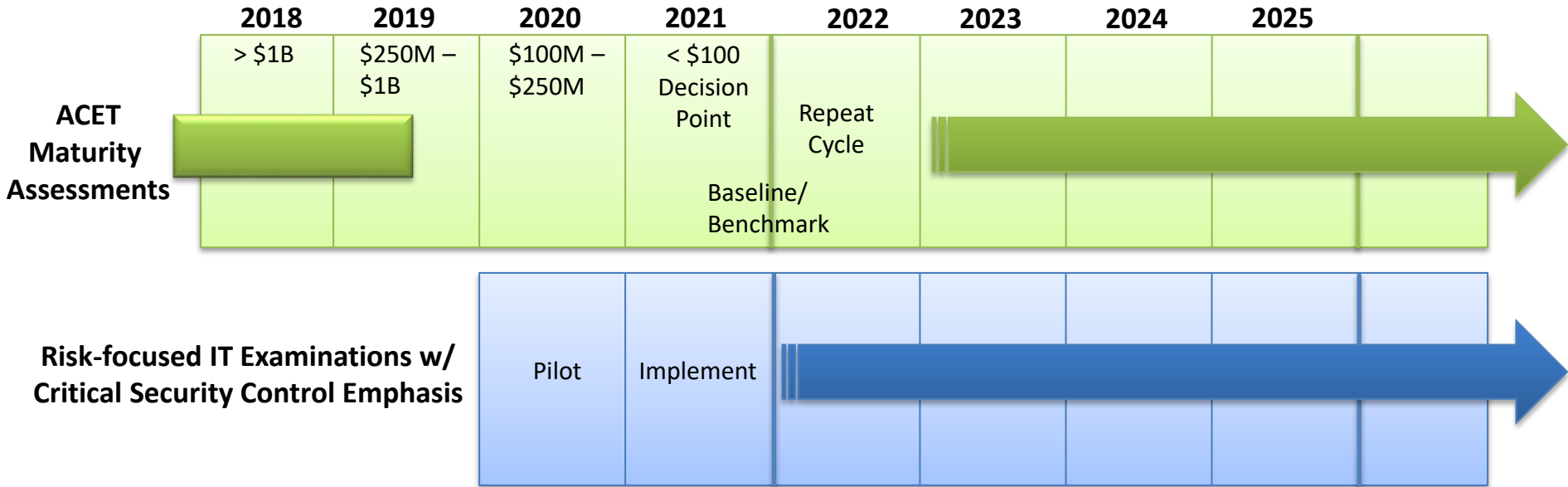


Note: Informed by the Risk Assessment/Business Impact Analysis
“Know the Business”

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

The screenshot displays the ACET Maturity Assessment (MA) interface. The top navigation bar includes the ACET logo, 'Tools', 'Resource Library', 'Help', and the user 'JEDAVIS'. The main navigation tabs are 'Prepare', 'Statements', and 'Results'. The left sidebar shows the navigation path: '> ACET MA'. The main content area is titled 'Risk Management' and contains a 'Risk Management Program' section. Below this, four statements (Stmnt 63, 64, 65, 66) are listed, each with a description, a 'Reviewed' button, and a maturity level (Baseline or Evolving). Each statement also has a set of response buttons: 'Yes' (green), 'No' (red), 'NA' (blue), and 'Yes(C)' (yellow), along with a flag icon.

Statement ID	Description	Reviewed	Maturity Level	Yes	No	NA	Yes(C)	Flag
Stmnt 63	An information security and business continuity risk management function(s) exists within the institution.	Reviewed	Baseline	Yes	No	NA	Yes(C)	Flag
Stmnt 64	The risk management program incorporates cyber risk identification, measurement, mitigation, monitoring, and reporting.	Reviewed	Evolving	Yes	No	NA	Yes(C)	Flag
Stmnt 65	Management reviews and uses the results of audits to improve existing cybersecurity policies, procedures, and controls.	Reviewed	Evolving	Yes	No	NA	Yes(C)	Flag
Stmnt 66	Management monitors moderate and high residual risk issues from the cybersecurity risk assessment until items are addressed.	Reviewed	Evolving	Yes	No	NA	Yes(C)	Flag

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

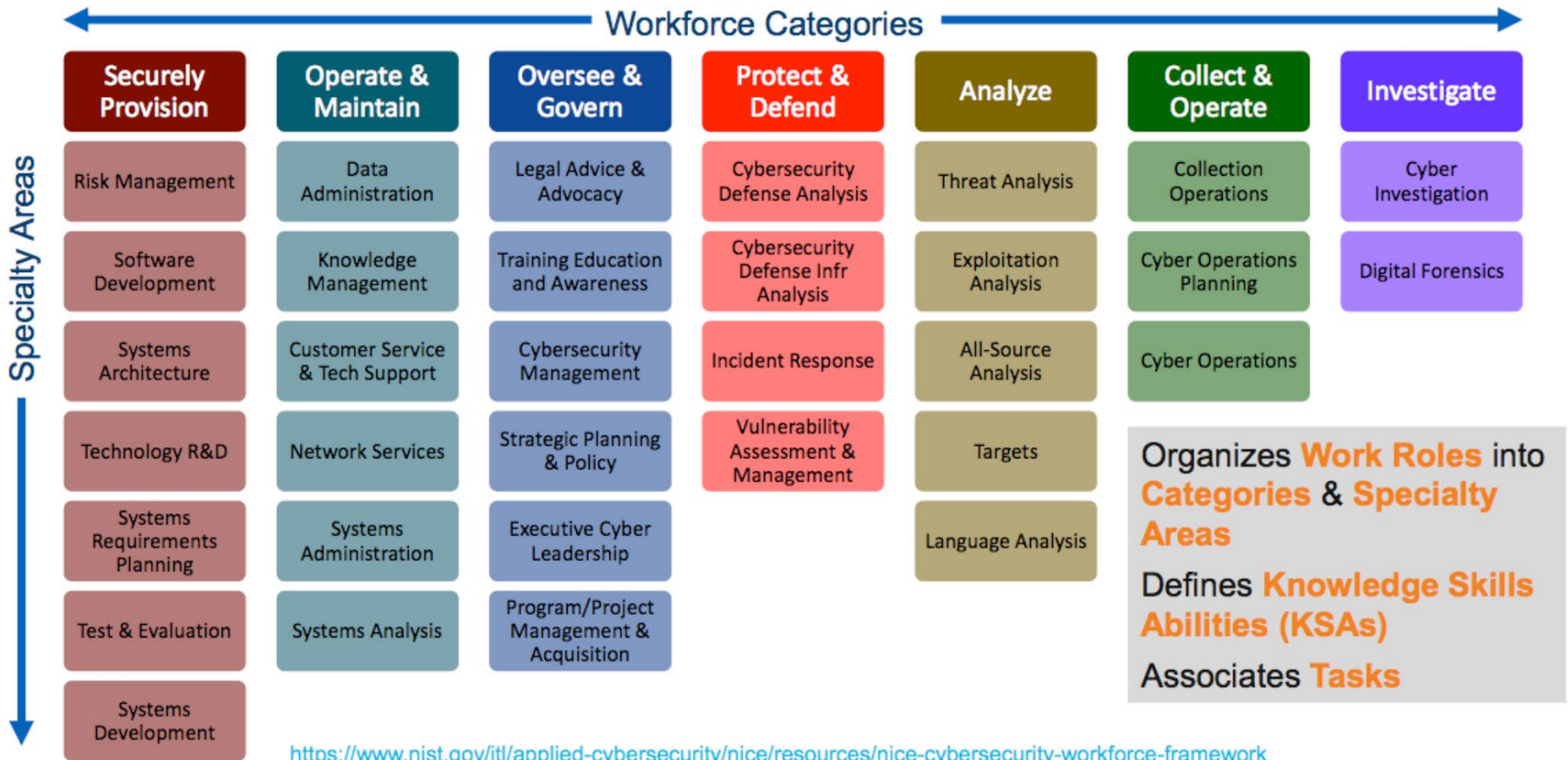
Training, Education, & Awareness (TEA) – Current Evolution

New Examiners STEP	CORE Technical	Subject Matter Examiner (SME)	National and Regional Information Systems Officers	Industry and Agency Conferences
<ul style="list-style-type: none"> ▪ STEP 9: Risk-Focused Examination Process (#119) ▪ eLearning: Information Technology for Examiners (#125) 	<ul style="list-style-type: none"> ▪ Cybersecurity – C Examiner Training Series (Cyber-C) eLearning Plan ▪ Cybersecurity Examination Process (#227) ▪ <i>LearnCenter – Information Technology, BSA/AML, Payments, etc</i> 	<ul style="list-style-type: none"> ▪ ISACA CSX Cybersecurity Fundamentals Workshop (#361) ▪ IT SME OJT (#254) ▪ IT SME Forum (#704) ▪ <i>LearnCenter – Information Technology, BSA/AML, Payments, etc</i> 	<ul style="list-style-type: none"> ▪ <i>LearnCenter – Information Technology, BSA/AML, Payments, etc</i> 	<ul style="list-style-type: none"> ▪ FIS Regulatory University - Information Technology, BSA/AML, Payments, etc. ▪ FFIEC/FDIC - Information Technology, BSA/AML, Payments, etc. ▪ Professional Designations and External Conferences - FFIEC IT Conference

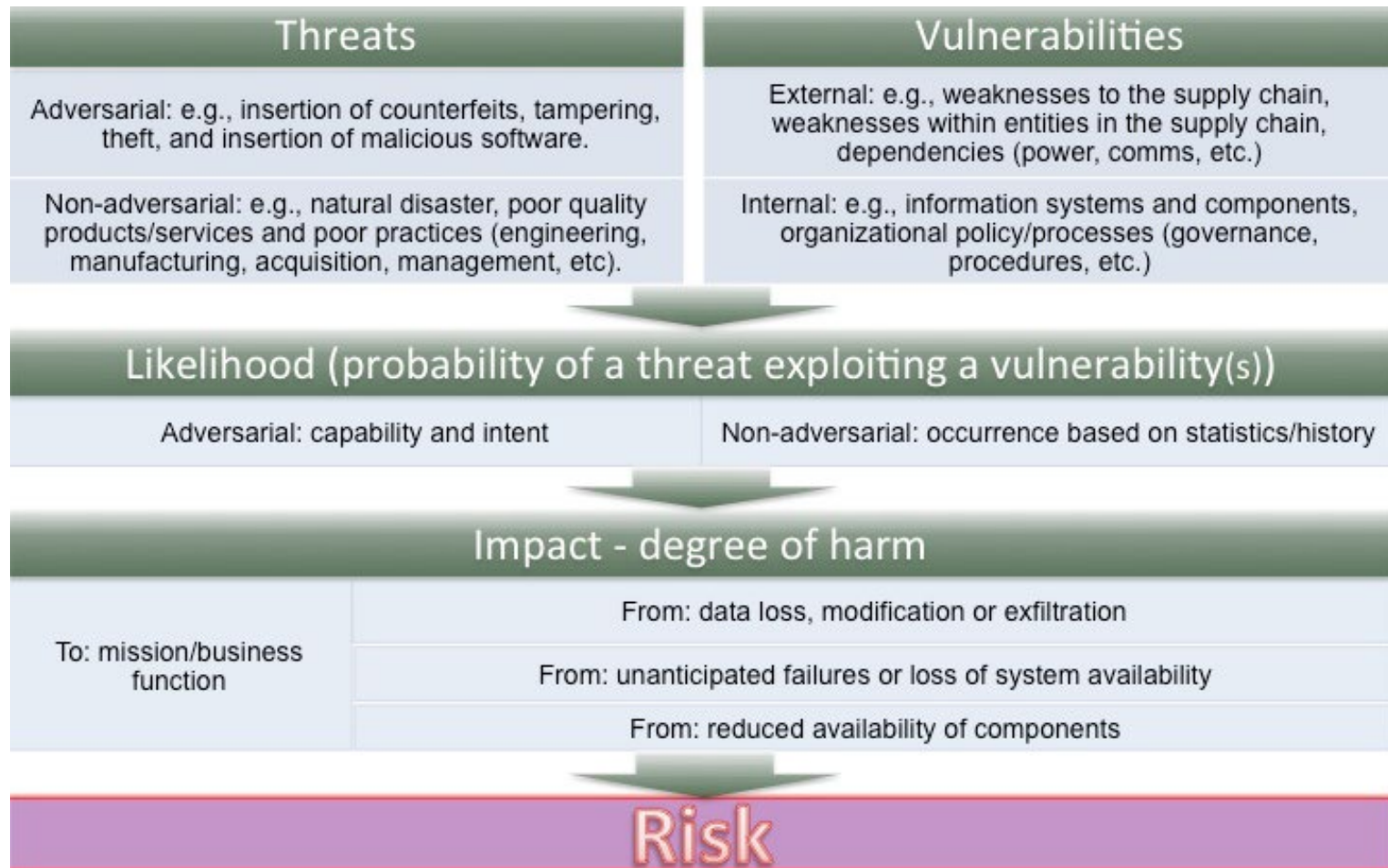
DHS National Initiative of Cybersecurity Education (NICE) Framework

National Initiative for Cybersecurity Education (NICE)

NIST SP 800-181 National Cybersecurity Workforce Framework (NCWF)



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

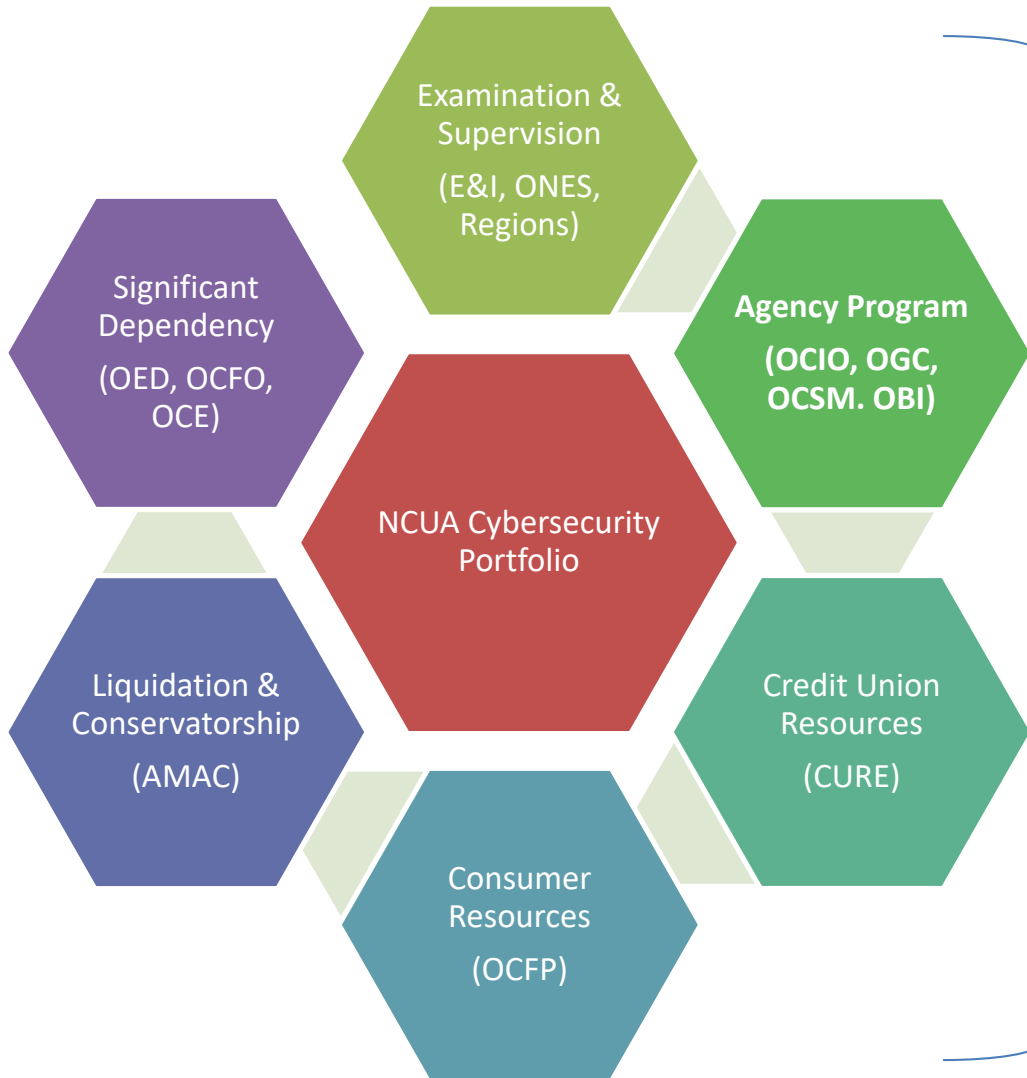
This guide provides resources designed to assist in financial sector resilience. Use of these resources is voluntary. FFIEC members do not endorse the listed organizations.

Resource	Type	Cost
Center for Internet Security https://www.cisecurity.org/	A	Free Paid
DHS Automated Information Sharing Program https://www.us-cert.gov/a/s	I	Free
DHS Cyber Incident Reporting Guide https://go.usa.gov/x1z9qf	R	Free
DHS Cyber Resilience Review https://www.us-cert.gov/coalition/assessments	A	Free
DHS National Cybersecurity and Technical Services https://www.us-cert.gov/resources/ncats	A	Free
FBI's Internet Crime Complaint Center (IC3) https://www.ic3.gov	R	Free
FDIC Cyber Challenge: A Community Bank Cyber Exercise https://go.usa.gov/x1z9qe	E	Free
Financial Crimes Enforcement Network (FinCEN) https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2018-0003	R	Free
Financial Sector Cyber Exercise Template https://www.ffiec.gov/financial-sector-cyber-exercise.html	E	Free
Financial Services Information Sharing and Analysis Center (FS-ISAC) https://www.fsisc.com	I	Free Paid
FS-ISAC Cyber Attack Against Payment Systems (CAPS) Exercise https://www.fsisc.com/Exercises-CAPS	E	Free
Infragard https://www.infragard.org	I	Free
National Credit Union Information Sharing and Analysis Organization https://ncuisao.org	I	Free Paid
Reporting to Primary Regulator https://go.usa.gov/x1z9s3	R	Free
Sheltered Harbor https://shelteredharbor.org/background	R	Paid
U.S. Secret Service Electronic and Financial Crimes Task Forces https://www.secretsservice.gov/investigation/efcft	I	Free
United States Computer Emergency Readiness Team 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

Working Group Under

- Enterprise Risk Management Committee (ERMC) and/or
- Cybersecurity Steering Committee (CSSC)

Office of Examination & Insurance (E&I)

NCUA BOARD MEETING – OCTOBER 2019