Tim Segerson, Deputy Director
Office of Examination & Insurance (E&I)
Wayne H. Trout, Supervisor
Division of Critical Infrastructure & Cybersecurity (CIC)

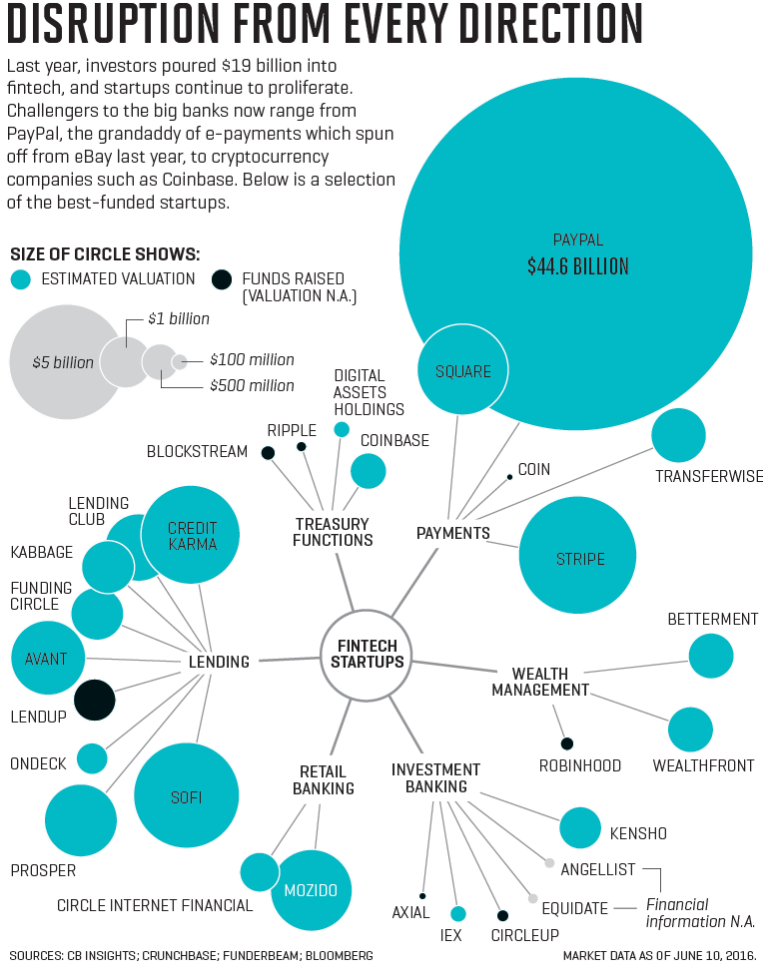
Cybersecurity

Board Briefing
September 15, 2016

The World is Evolving

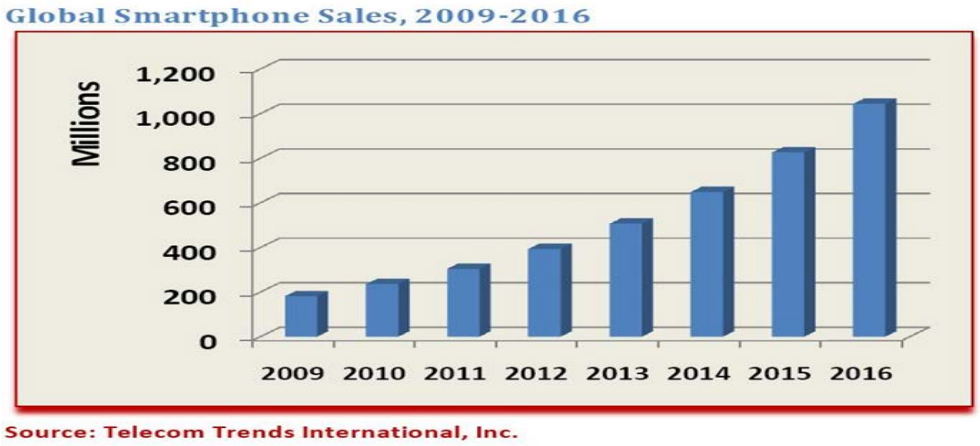
- Market & Technology Innovation
- High Speed Connectivity & Interconnectivity
- Smart Devices and Advanced Algorithms
- New Services & New Delivery Channels
- Market Disruption & New Competition

"Banking's UBER Moment"**

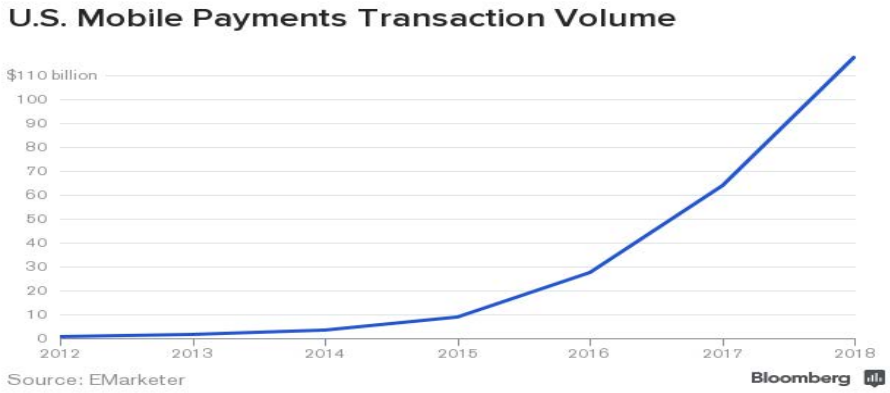


https://*fortunedotcom.files.wordpress.com/2016/06/fintech_003.png*

- **New and Evolving Risks**
- **Digital World Requires Digital Risk Management Strategy**
- **Public Demands and Expectations Evolve**
- **Our Responsibilities Evolve**

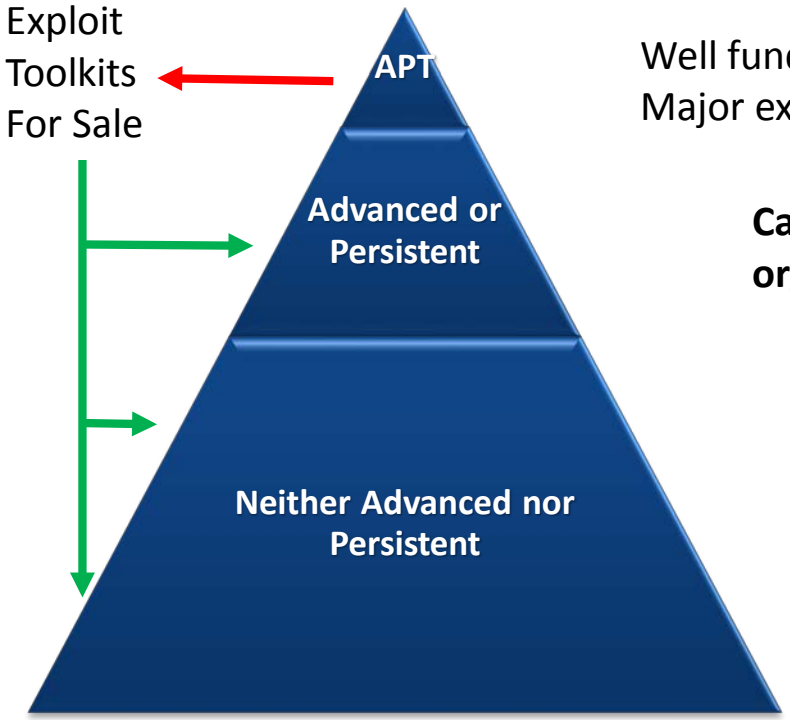


Source: Telecom Trends International, Inc.



***Citi GPS; Digital Disruption, How FinTech is Forcing Banking to a Tipping Point, March 2016 pg. 12.*

Changing Threat Landscape



Well funded, organized and capable of compromising at will
Major exfiltration, disruption and damage

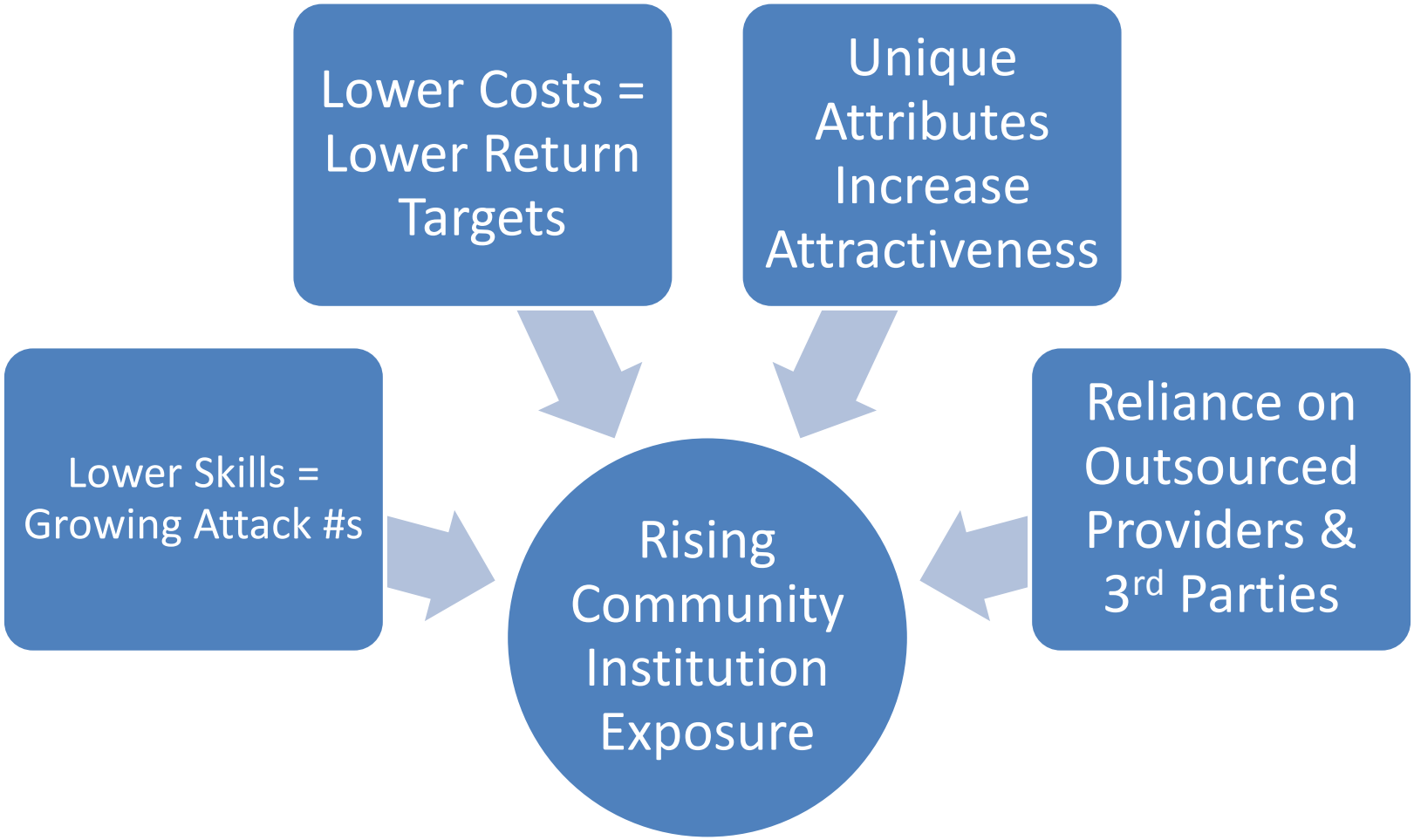
Capable of advanced attacks, less funding, less organization

Least organized and least funded. **Shear numbers could strip mine vulnerabilities especially in unprepared institutions**

- ❑ Lower level threats – large and growing numbers - advanced tools
- ❑ APT/Nation States – Act like criminals and hacktivists
- ❑ Hacktivists - Act like terrorists and criminals
- ❑ Criminals (Guns for Hire i.e. Nation States/hacktivists)

Increasing Risk **Increasing Cost**

Growing Exposure



Risk Trends

- **Existing vulnerabilities continue to be exploited.**
- **New platforms create new ways to exploit Financial Institutions and consumers.**
- **Lines between cyber actors are blurring as attack tools are commercialized.**
- **Interconnectivity is expanding the sources of risk.**
- **Technology advances speed transactions and minimize intermediaries.**

Risk Trends

- Use of social networking enables more effective and targeted attacks
- Malware continues to evolve and now includes data destruction and encryption and back office functions
- Global unrest results in US symbols, including financial institutions being targeted

Risk Trends

Potential Impacts

- Financial – cost of loss and cost to mitigate
- Operational – respond and recover
- Legal – lawsuits
- Lost consumer confidence (damaged reputation)

CYBERSECURITY INITIATIVES

FFIEC Cybersecurity Efforts

- **Cybersecurity Critical Infrastructure Working Group (CCIWG)**
  - **Benchmark Risk Assessment – Agency Self Assessment – GAPs and Action Plan**
  - **Industry Outreach and Communication.**
    - Joint statements and alerts – Observations report
    - Cybersecurity awareness website and CEO webinar.
    - Cybersecurity assessment of community institutions.
    - Issue the Cybersecurity Assessment Tool.
  - **Enhance incident analysis and preparedness.**
  - **Align, update and test crisis management protocols.**
  - **Develop training programs for staff.**
  - **Increased collaboration with Law Enforcement.**
- **Information Technology Subcommittee**
  - **Enhance focus on Technology Service Providers.**
  - **Modernize the *Information Technology Examination Handbooks.***

FFIEC Cybersecurity Assessment Tool

Objective

To help institutions identify their risks and determine their cybersecurity maturity. The Assessment provides a repeatable and measureable process to inform management of their institution's risks and cybersecurity preparedness.

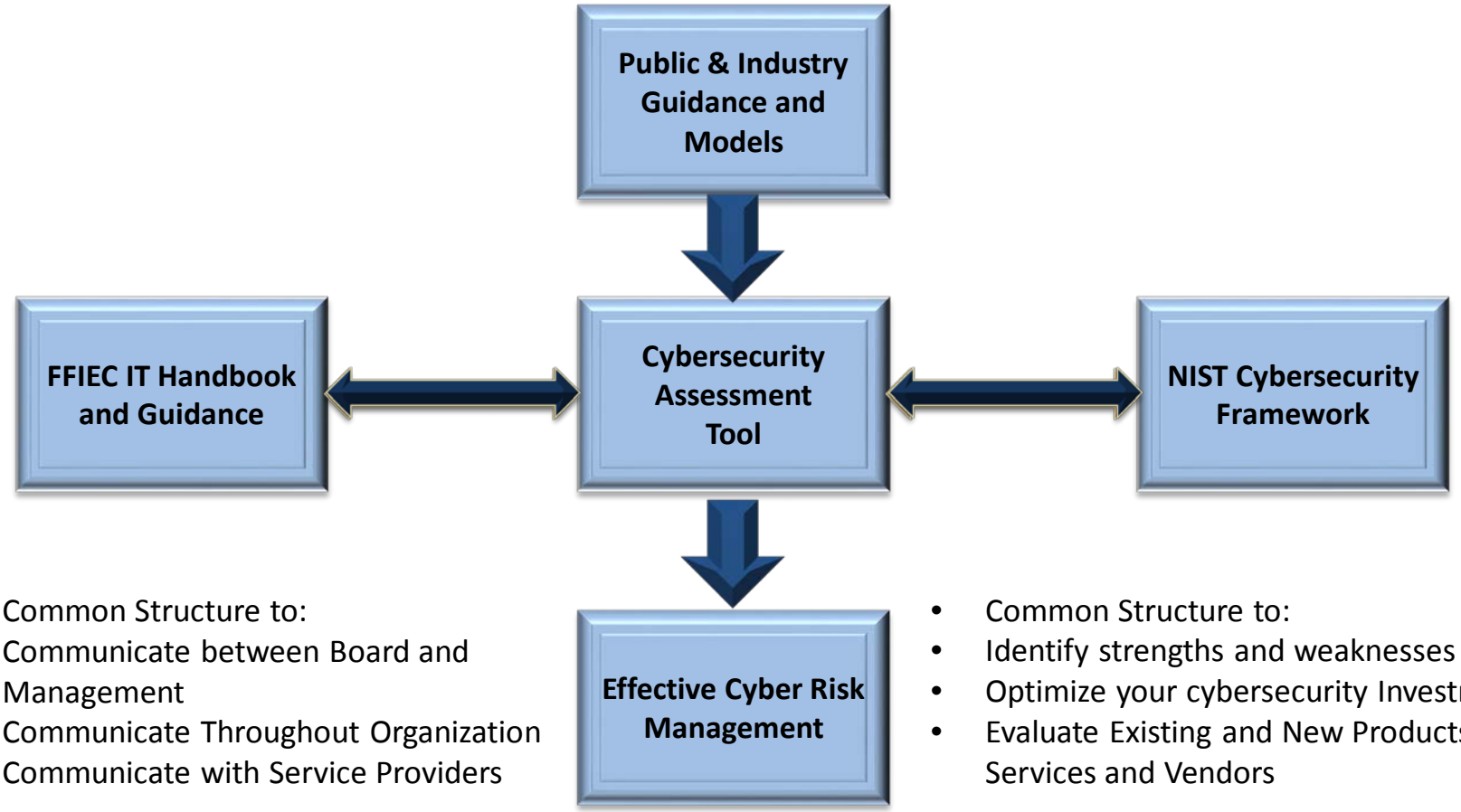
Consists of two parts

Part One: Inherent Risk Profile

Part Two: Cybersecurity Maturity

Strong Industry Foundation and Benchmark

Comprehensive with a Relevant and Cross Referenced Foundation

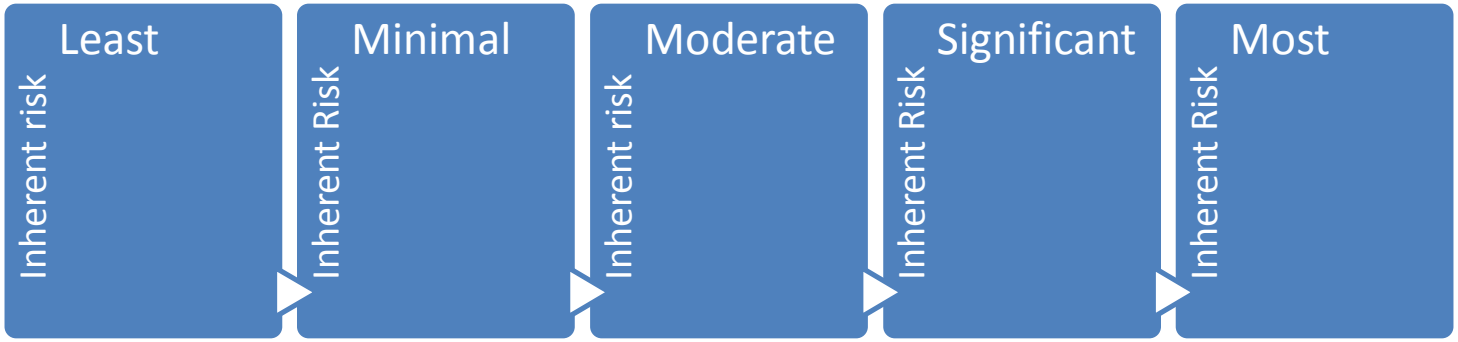


- Common Structure to:
- Communicate between Board and Management
- Communicate Throughout Organization
- Communicate with Service Providers

- Common Structure to:
- Identify strengths and weaknesses (gaps)
- Optimize your cybersecurity Investment
- Evaluate Existing and New Products, Services and Vendors

FFIEC Cybersecurity Assessment Tool

Inherent Risk Profile Risk Levels



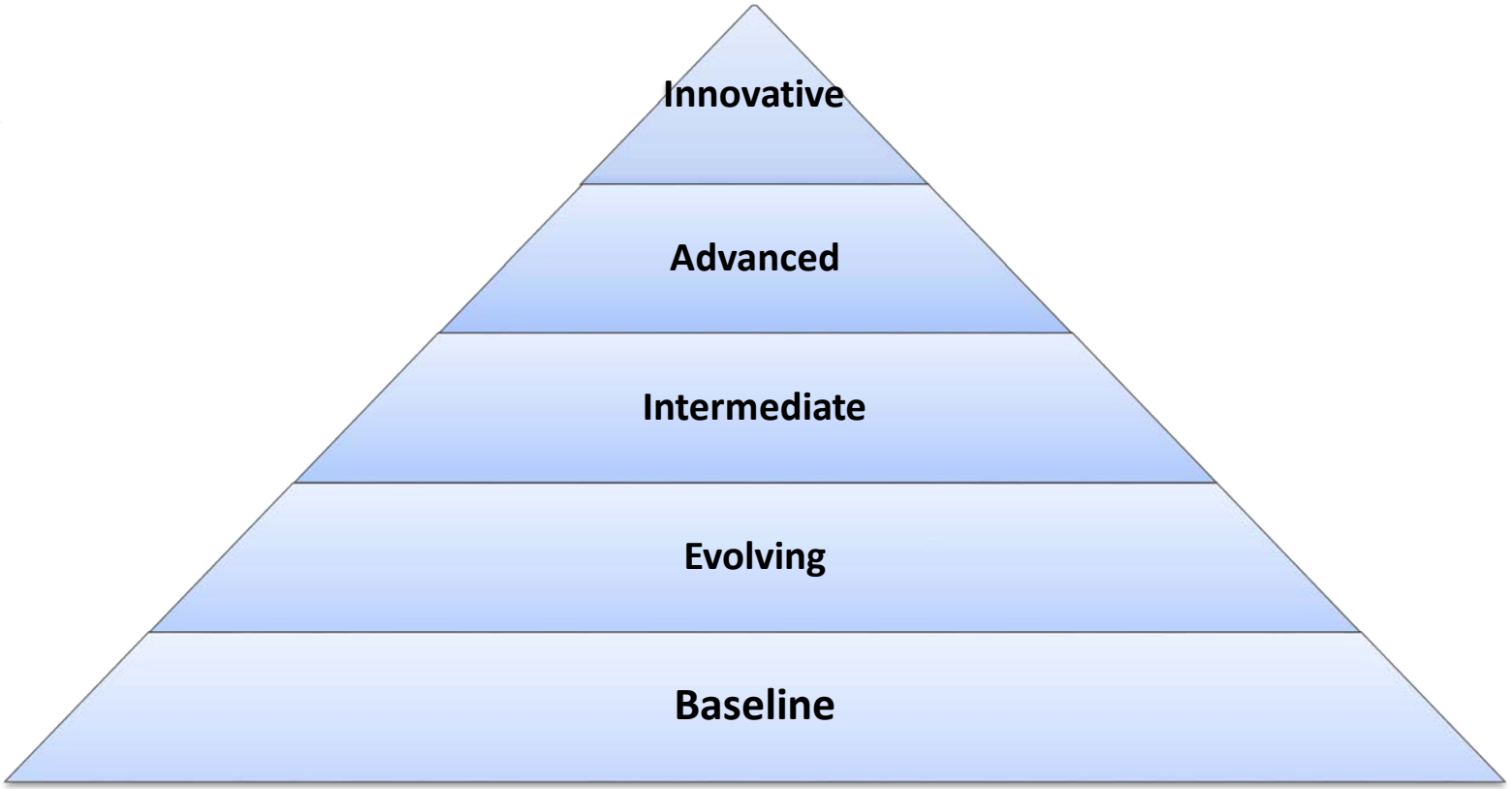
Type, volume, and complexity of operations and threats directed at the institution contribute to the risk level

FFIEC Cybersecurity Assessment Tool

	Domain	Assessment Factors
1	**Cyber Risk Management & Oversight**	• Governance • Risk Management • Resources • Training and Culture
2	**Threat Intelligence & Collaboration**	• Intelligence Sourcing • Monitoring and Analyzing • Information Sharing
3	**Cybersecurity Controls**	• Preventative Controls • Detective Controls • Corrective Controls
4	**External Dependency Management**	• Connections • Relationships Management
5	**Cyber Incident Management & Resilience**	• Incident Resilience Planning and Strategy • Detection, Response and Mitigation • Escalation and Reporting

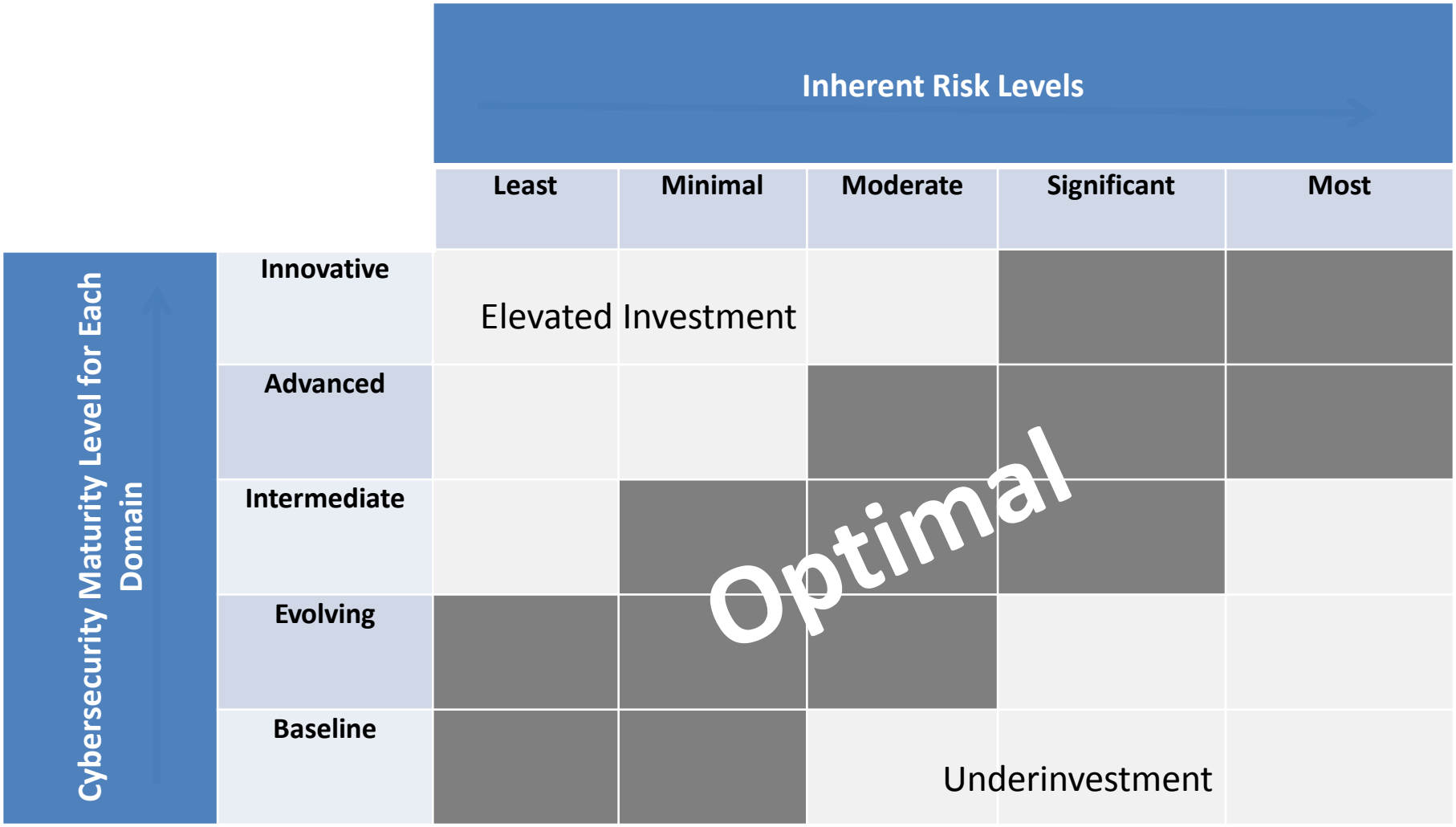
Cybersecurity Maturity/Risk Relationship

Highest Risk Institutions



Lowest Risk Institutions

FFIEC Cybersecurity Assessment Tool

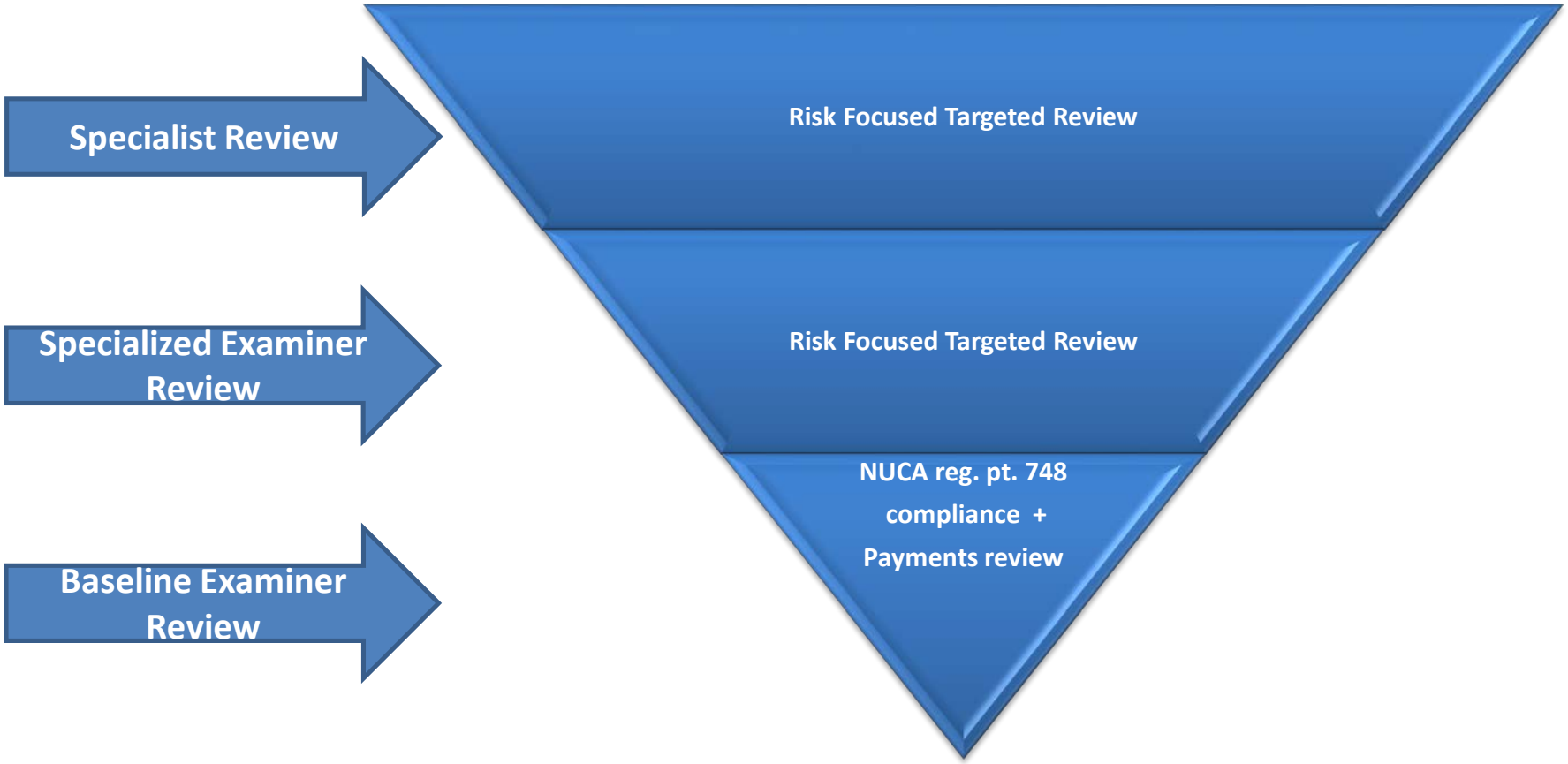


NCUA CYBERSECURITY EXAMINATION

Agency Objectives

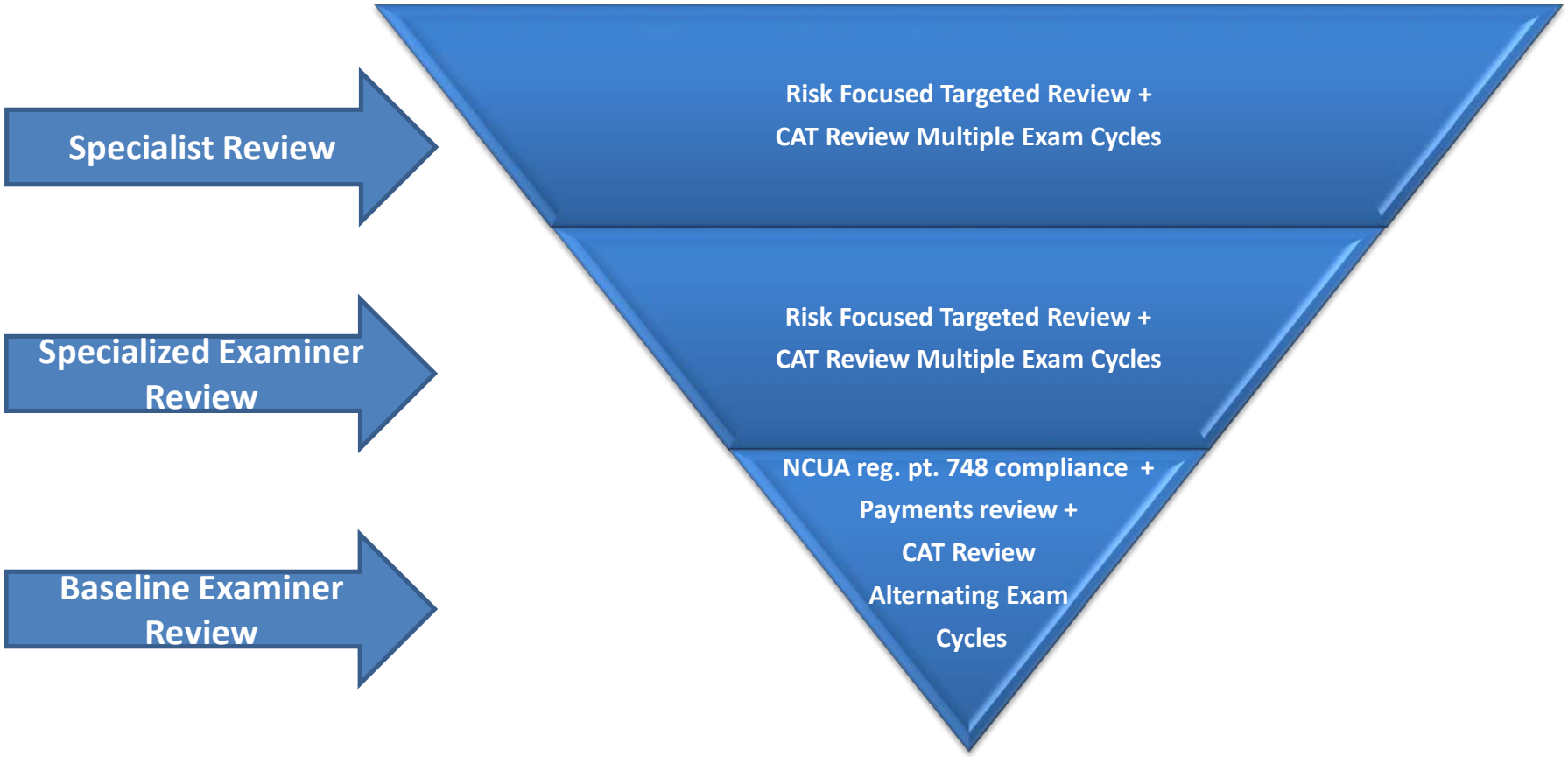
- Build Internal Awareness and Capacity
- Drive Industry Awareness and Resilience
- Structured approach toward resilience and industry "hardening" using scalable expert systems/tools
- Stimulate an ongoing industry dialogue
- Improve knowledge and data to make informed supervisory decisions

Exam Current State



Examiner baseline review may layer over the existing Part 748 (privacy) and Payments Reviews. RISO/SME may custom target broad risk management or focused risk area during review depending on risk drivers.

Exam Future State



SME Review may layer over the existing 748 and Payments Reviews. RISO/SME may custom target broad risk management or focused risk area during review depending on risk drivers

Exam Depth Will Vary

- **Specialist Risk Focused Targeted Review**
  - Deep dive reviews in specialized areas using structured NCUA or FFIEC tools and other more advanced tools and methods.
  - Periodic Cybersecurity Assessment Tool Structured Assessment
- **Specialized Examiner Review**
  - Targeted reviews using NCUA and Federal Financial Institution Examination Council Exam work plans.
  - Routine Cybersecurity Assessment Tool Structured Assessment
  - Routine Privacy and Payment Systems Assessments
- **Examiner Review**
  - Routine Cybersecurity Assessment Tool Structured Assessment
  - Routine Privacy (part 748 NCUA Regs.

Cyber/IT Examination Vision

Examiners scale the review in this area based on their understanding of risk (your risk profile). Under expected cyclical reviews, we plan to collect assessments on all institutions over a multiyear period to understand industry trends and adjust exam strategies.

Cyber & Information Technology Exam Program Vision – NCUA

	Financial Examiner Review	Specialized Examiner Review	Specialist Review
Advanced Review Specialized Areas	Unlikely	Less Frequent/improbable	More Frequent
NCUA/FFIEC* Selected Reviews using FFIEC/NCUA work plans	Less Frequent/improbable	Less Frequent/improbable	More Frequent
Cyber Assessment Tool Structured Review	More Frequent	More Frequent	Less Frequent/improbable
Part 748 Privacy Compliance Review	More Frequent	More Frequent	Less Frequent/improbable

Alternating Reviews of Privacy and Cybersecurity will be the foundation of the program. Intermediate and Advanced reviews will be performed by skilled and specially trained examiners and specialists. Long term goal to perform periodic reviews using a structured cybersecurity assessment tool approach in all credit unions.

*Federal Financial Institution Examination Council

CAT Review Vision

- **Examiner Performed.**
- **Uniform Approach – Protocol Structure – Wide Application.**
- **Interactive Review – Examiner performed, with management observations and input.**
- **Benchmarking using the Cybersecurity Assessment Tool structure.**
- **Discussion/Sharing Results.**
- **Work with Management to Identify Opportunities.**

CAT Review Impact

- **Pre-exam**
  - More data requested in advance
  - Advance review of available information
  - Initial risk classification
  - Initial attribute identification
- **During Exam**
  - New discussions in new areas
  - Review of results – verify output
  - Observe and verify activity based attributes
- **Post Exam**
  - Aggregate data across industry and institutional features
  - Inform supervisory process and industry guidance.

NCUA Moving Forward

- **Extensive Examiner Training – Institutionalize Training and Development.**
- **Test Field Reviews and Data Collection through mid 2017.**
- **Tool/Process improvement early 3rd qtr. 2017.**
- **Process Rollout late 3rd qtr. early 4th qtr. 2017*.**

*Commitment to Ensure Tight Process and Well Trained Examiners Before Rollout.

Credit Union Need to Knows

- **CAT is voluntary**
- **Productive Dialogue and Collaboration**
- **Expectations Scale to Resources/Risk**
- **NCUA is committed to a Value Added Approach to the Cyber Exam.**

Credit Union Should Do's

- **Commit to effective security.**
- **Identify a comprehensive risk management approach.**
- **Identify risks and risk posture.**
- **Identify your strengths and weaknesses.**
- **Benchmark your current and desired future state.**
- **Implement a plan.**
- **Set expectations and monitor external dependencies.**

This Concludes Our Briefing

Go to NCUA's Cybersecurity Resource Page for more Information

https://www.ncua.gov/regulation-supervision/Pages/policy-compliance/resource-centers.aspx

Or search for Resource Centers at NCUAs main page www.NCUA.gov

Office of Examination and Insurance

EIMail@ncua.gov