@Team,

Full DRAFT context provided. Let me know if I did not address a question/concern.

- Socializing NIST NICE response informally, NOT for dissemination beyond ‘peer review’
  - Open to forming a formal response for public dissemination at a later date

- Kris, Scott, and Laurin have valuable insight and vision, with possible peer review/sharing enhancing the discussion?
  - Would love to see associated responses

- The attachments should have no direct reference to myself or my organization other than the moniker “Dr.J” for easy reference
  - This is an unaffiliated ‘individual’, passionate scholar/practitioner, feedback/response

/r

“Comments will be accepted until January 13, 2020.”

- ***Responses in BLUE are truncated with option to pivot and discuss in greater detail**

Improvements to the NICE Framework

The following topics are intended to help NIST and its partners who are part of the NICE Community to learn about experiences in applying and using the NICE Framework and explore opportunities for improvement.

1. Describe what components of the NICE Framework have been most useful to you and why.
    1. The framework itself has been most useful, critical in operationalizing Cyber (domain) workforce training programs affecting 500,000+ students (full-time employees and contractors). We are now able to digest current and emerging practitioners at volume, efficiently, using the framework to discover and pursue workforce roles employees and contractors are most passionate about (maximizes recruitment and retention).
    2. The Common Body of Knowledge (CBK) represented in Knowledge 0001-0006, appearing in many of the common operations roles. The knowledge demonstrates you do not have to be an ‘IT specialist’ to work in the Cyber domain.
2. Describe what components of the NICE Framework have been least useful to you and why.
    1. The naming convention ‘Cybersecurity’ Workforce Framework holds fast to discipline-specific operations and linear/myopic perspectives. Cyber (domain) is more relevant and useful.
    2. A lack of standardized vocabulary/common lexicon. Example, organizations struggle with definitions in risk, threat, and vulnerability. Worse when you add marketing phrases like ‘Cyber Threat Intelligence’.
    3. A lack of awareness and acceptance of business acumen across all workforce roles. Failure to address strategic business leader concerns minimizes operational relevance.
3. Share any key concepts or topics that you believe are missing from the NICE Framework. Please explain what they are and why they merit special attention.
    1. For ‘Cybersecurity/SOC/CISSP/Incident Responder’ audiences, nothing is missing, ‘100% ready’
    2. For ‘Cyber domain’ ‘Mature’ ‘Fusion Operations’ and organizations with business acumen, see #2 and the ‘whitepaper’ supplement for more detail, ‘80% ready’.
4. Describe how the NICE Framework can be more useful to a variety of audiences (i.e. employers, employees, education and training providers, learners, small enterprises, etc.).

   1. See supplement ‘whitepaper’. Recommend target strategic leadership in ‘Cyber domain’ ‘Mature’ ‘Fusion Operations’ and organizations with business acumen. Only then will organizations realize the full potential and value of the framework (outside of Government, if leadership does not see the value, the framework does not get utilized).

5. Describe the potential benefits or challenges experienced when aligning the NICE Framework more closely with other related standards, guidance, or resources (e.g., NIST Framework for Critical Infrastructure Cybersecurity, NIST Privacy Framework, other NIST Special Publications, etc.).
   1. Looking at emerging frameworks useful beyond ‘Cybersecurity/SOC/CISSP/Incident Responder’ and toward Commercial Enterprise; start with operational frameworks/alignment such as the Carnegie Mellon SEI Cyber Intelligence Tradecraft Report (2019) for ODNI where on page 14 of the PDF, it explicitly aligns SP 800-181 workforce roles to ‘Mature’ ‘Fusion Operations’ standards/guidance (also cited in the supplement ‘whitepaper’).
6. Explain if you think the scope of the covered workforce as stated by the NICE Framework needs to be adjusted.
   1. If anything, more ‘Cyber’ domain-centric and less ‘Cybersecurity’ discipline-specific. “Resist the urge to retrofit” everything under ‘Cybersecurity’.
7. Describe any improvements that might be made in the current organization of the NICE Framework and its major components such as Categories, Specialty Areas, Work Roles, Knowledge, Skills, Abilities, and Tasks.
   1. None currently. Leave everything ‘as-is’ until greater awareness and acceptance by all industry participants (US Government, DiB, Commercial Enterprise) is achieved. Many participants are still ‘scratching their heads’ and trying to ‘retrofit’ the ‘new roles/positions’ under ‘Cybersecurity/SOC/CISSP/Incident Responder’ positions (just look at the job placement/requirement websites like USAjobs<dot>gov, Clearancejobs<dot>com, and Indeed<dot>com.
8. Describe how the NICE Framework can best document and describe Knowledge, Skills, Ability, and Task statements as well as Competency Areas.
   1. Leave ‘as is’ until version 3.0? The framework does a great job currently and very few organizations comprehend the framework today. Focus on increasing awareness and acceptance instead?
9. Explain whether the NICE Framework indicates which Knowledge, Skills, and Abilities could be considered as foundational for all workforces that regularly interact with networks, systems, and data in cyberspace.
   1. Did anyone notice the Knowledge CBK? As in, most jobs/roles have the same 6 Knowledge (K0001-K0006) points listed? Champion this to start.
10. For each NICE Framework work role, please provide an informative reference that you would like the NICE Framework Resource Center to reference.

    1. None, N/A? Capabilities evolution, recommend establish dynamic role ‘real world’ scenarios/use cases as an organic ‘originator’ source to the Resource Center? Include all sectors equally in use cases from inception (US Gov, DiB, Commercial/Enterprise). A ‘linear/myopic’ perspective ‘start’ will kill this value proposition before it gains traction?

11. Describe which components of the NICE Framework you think are best left as static content and would not change until the next revision and which components could be managed as dynamic content (i.e., more frequent changes or updates to accommodate new information as it becomes available).
    1. Outside of the (3) primary recommendations, I wouldn’t change much. I would instead focus on promoting awareness and acceptance, then look to modify static versus dynamic content on later versions (3.0+)?
    2. Use cases (discussed in the 12/3 Adobe Connect meeting) are a possible beneficial dynamic component.
12. Describe the value or risk in different organizations, sectors of the economy, or organizations with classified versus unclassified workforces to develop customized versions of the NICE Framework tailored to their specific circumstances.
    1. @Risk, this goes back to BUSINESS ACUMEN (see above). Risk to strategic business leaders means legal liability, regulatory and compliance, business continuity, etc. A lack of collaboration exists between public-private organizations where commercial enterprise dismisses unclassified and classified briefings from US GOV because there is no relevant business value in strategic business risk terms.
        1. This results in missed opportunities to discuss or utilize the workforce framework and any offer to customize/tailor to specific circumstances (no perceived business value).

Awareness, Applications, and Uses of the NICE Framework

Recognizing the critical importance of widespread voluntary usage of the NICE Framework to achieve the goals of Executive Order 13870 on America’s Cybersecurity Workforce, NIST solicits information about awareness of the NICE Framework and its application and use by organizations and by individuals.

1. Describe the extent of current awareness of the NICE Cybersecurity Workforce Framework within your organization or sector or among individuals.
    1. Organization – Extensive. Commercial Enterprise; based on executive leadership ‘buy-in’ and sponsorship of an organization-wide (500,000+ students) Cyber (domain) training program seeded at $1,000,000.
    2. Sector – (including Critical Infrastructure) Limited. Largely due to perceptions of ‘US Government pushing SOC/Security’ protocols/knowledge and null value datasets onto ‘high performing’ ‘mature’ organizations.

        1. The undiscovered value is operationalizing the advanced workforce roles like all-source analyst, data analyst/scientist, and knowledge manager.

2. Describe how you or your organization was introduced to the NICE Framework.
    1. Academic self-research project(s) driving organization business value.
3. Describe the greatest challenges and opportunities for increasing awareness and use of the NICE Framework.
    1. Greatest challenges; Awareness and Acceptance
    2. Opportunities; ‘Real world’ operationalization of workforce roles applied systematically (people, process, technology), where we haven’t begun to discuss workforce automation sequencing based on NIST SP 800-181 Tasks using machines to bridge the widening labor pool gap.
4. Explain how you are currently referencing (i.e., applying or using) the NICE Framework and what plans, if any, you have for referencing it during the next year.
    1. Designed, funded, and implemented a comprehensive Cyber (domain) training program, phased approach, with the objective of developing passionate scholar/practitioners (any workforce role):
        1. Bronze/Basic/Awareness 8 days – All students 500,000+
        2. Silver/Intermediate/Proficiency 8 Weeks – 1% expected Bronze capture rate
        3. Gold/Advanced/Practitioner 8 Months – 1% expected Silver capture rate (admission by selection only)
    2. Example, Learning Objective Construct for Bronze and Silver role ‘All-Source Analyst’ ‘AN-ASA-001’

BRONZE/BASIC/AWARENESS - Cyber Intelligence

1.1. TLO: Define Cyber Intelligence
1.2. TLO: Discuss how Cyber Intelligence enhances cyber defense.
1.3. TLO: Explain the key components of Cyber Intelligence
1.4. TLO: Describe how to properly report Intelligence to stakeholders
1.5. Additional Resources (CELL Modules)
- MODULE 1 - Source Identification and Grading
- MODULE 2 - Application of Corporate/Enterprise Intelligence Requirements
- MODULE 3 - Lightweight Binary Risk Assessment
- MODULE 4 - Bottom Line Up Front (BLUF)

—

SILVER/INTERMEDIATE/PROFICIENCY - Cyber Intelligence

2.1. TLO: Define Cyber Intelligence Analyst
2.2. TLO: Demonstrate awareness of requisite Cyber Intelligence practitioner knowledge
2.3. TLO: Demonstrate practical application
2.4. TLO: Demonstrate proficiency and select areas of interest
2.5. Additional Resources (CELL Iterations and Tasks)

Iteration 1 Overview
•Task 1 - Cyber Intelligence Framework (NIST, CM SEI, FAS)
•Task 2 - Analytical acumen – the science
•Task 3 - Exploring structured analytic techniques
•Task 4 - Cognitive biases and logical fallacies
•Task 5 - Good thinking
•Task 6 - Intelligence writing and estimative language (BLUF) / Intelligence briefing

Iteration 2 Overview
•Task 1 - Environmental context
•Task 2 - Intelligence Requirements process
•Task 3 - Intelligence Requirement and Data Source alignment
•Task 4 - Organization information sharing process
•Task 5 - Technology for data acquisition and gathering
•Task 6 - Data source validation
•Task 7 - Applied Intelligence

Iteration 3 Overview
•Task 1 - Understanding 'mature' Cyber Operations
•Task 2 - Risk analysis workflow
•Task 3 - Timeliness and accuracy of risk analysis
•Task 4 - Diversity in technical disciplines
•Task 5 - Traits, core competencies, and skills
•Task 6 - Difference between strategic (risk) analysis and threat analysis
•Task 7 - Strategic analysis skills
•Task 8 - Threat prioritization model

Iteration 4 Overview
•Task 1 - Cyber Intelligence Report Types

•Task 2 - Actionable and Predictive Analysis
•Task 3 - Leadership involvement
•Task 4 - Influence on Decision Making
•Task 5 - Feedback mechanisms for analysts
•Task 6 - Influence of feedback on data gathering and analysis
•Task 7 - Satisfying intelligence consumers
•Task 8 - Capturing Return on Investment (ROI)
•Task 9 - Future Cyber Intelligence tradecraft (using AI/ML)
•Demo

5. If you are an employer, describe how your organization uses the NICE Framework to develop position descriptions, guide skill-based training, facilitate workforce planning, or other uses.
    1. Positions – No current use/reference of NICE.
    2. Training – Explained in previous section #4.
    3. Workforce planning/other – Confidential.
6. If you are an education or training provider, describe how your organization uses the NICE Framework to develop or describe education and training content or associated credentials.
    1. *No credentials necessary. No instant gratification 'trophies or badges' awarded. Demonstrated proficiency and practice rules all outcomes.
        1. Students are required to read NIST NICE CWF 800-181 and select (3) "top roles of interest/passion" (based on NIST Tasks and real-world applications in their business unit or from job postings on the Internet)
        2. A (1) 'top role' is selected then applied to the Bronze and Silver training constructs to develop and demonstrate proficiency (Silver objective) before being selected by a SME/peer for Gold/Practitioner
        3. 'Silver' graduate students are obligated to return to the 'constant contact/engagement' tools like chatrooms as 'TAs' (Teaching Assistants), sharing the 'workload' of SME/Professors with 'full-time jobs', further disseminating the SP 800-181 integrated framework
7. If you are an employee, job seeker or learner, describe how you use the NICE Framework for communicating your competencies or skills to employers, identifying training or professional development needs, or navigating your career pathway.
    1. I read, comprehend, and envision NIST NICE CWF SP 800-181 role TASKS in my head and try to 'match' the tasks to personal experience.
    2. I then take the familiar tasks and 'match' them to existing job market supply/demand 'requirements'
        1. Example, AN-ASA-001 Tasks (T0xxx-T0xxx) and match them to Indeed<dot>com job postings from organizations I would like to work for. The 'bulletized' job requirements typically number 5-10

and relate to NIST role Tasks easily. I can then envision and state with confidence that I have knowledge and/or experience with the job requirements, even when I don’t have actual ‘on the job’ experience. With some practice, this is extremely effective as most employers/hiring managers value EXPERIENCE above certs and degrees (see job postings, ex. “CISSP, nice to have”).

3. Result = 100% interview success rate and multiple job offers with a $100,000 MINIMUM base salary
    1. Class *‘Who wants to be a millionaire?’* This result is reproducible and has been taught/shared as visiting lecturer at Universities like Carnegie Mellon (SEI, graduate Cyber studies). $100k x 10 years = $1M, strong motivation for emerging college educated practitioners

8. Describe any tools, resources, or publications that exist that reference or would benefit by referencing the NICE Framework.
    1. See supplement ‘References’ please
9. Describe any tools, resources, or technical support needed to increase the application and use of the NICE Framework.
    1. See supplement ‘Top (3) Recommendations’ please
10. Propose any improvements for the application and use of the NICE Cybersecurity Workforce Framework.
    1. This response and supplement detail proposed improvements based on audience and how ‘mature’ NIST NICE plans to take this initiative.

Cybersecurity Workforce Framework Input

“Dr. J” Discussion Supplement

Special Publication 800-181

November 2019

National Institute of Standards and Technology (NIST)

National Initiative for Cybersecurity Education (NICE)

Cybersecurity Workforce Framework Input

NIST NICE continues to create business and regulatory value for organizations.

For industry Cyber leadership lacking business acumen outside the confines of ‘Cybersecurity/SOC/CISSP/Incident Responder’ (US Government, Defense Industrial Base/US Government Contracting/Commercial Enterprise) SP 800-181 remains 100% complete (no recommended changes), ‘5-10 years' ahead of the curve (Harvard Business Review, 2019).

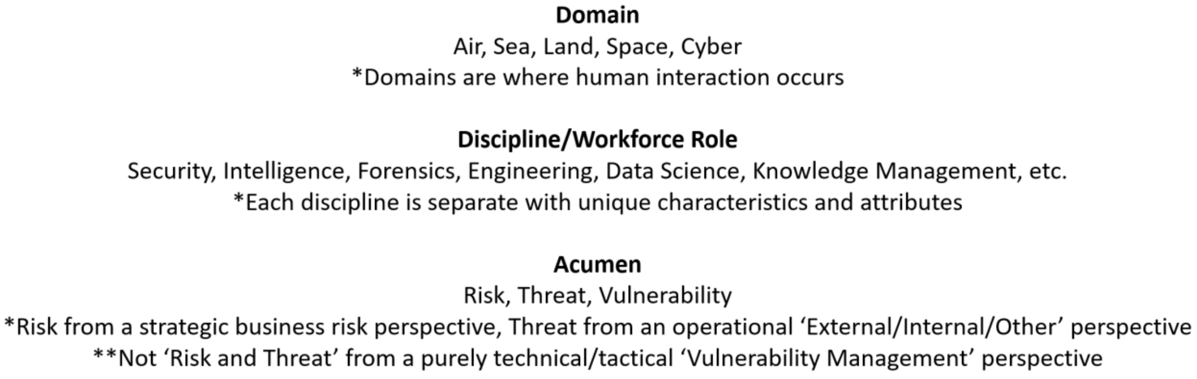
For organizations with Cyber leadership 'high performing' 'Mature' 'Fusion Operations' and advanced business acumen practice in 'strategic (business) risk' terms, not limited to ‘Beginning’ indicator sharing, vulnerability management or technical controls, then SP 800-181 is 80% complete (Carnegie Mellon SEI, 2019).

For the sake of response brevity, the intended audience of this article is the latter (developed business acumen, ‘Mature’, ‘Fusion Operations’, etc.)

Top (3) Recommendations

1. ‘Cyber Workforce Framework’

Truncate the title to reflect DOMAIN-specific application (ex. Air, Sea, Land, Space, now Cyber) not lower order DISCIPLINE-specific (Security, Intelligence, Forensics, Engineering, Data Science, Knowledge Management, etc.)



Domain
Air, Sea, Land, Space, Cyber
*Domains are where human interaction occurs

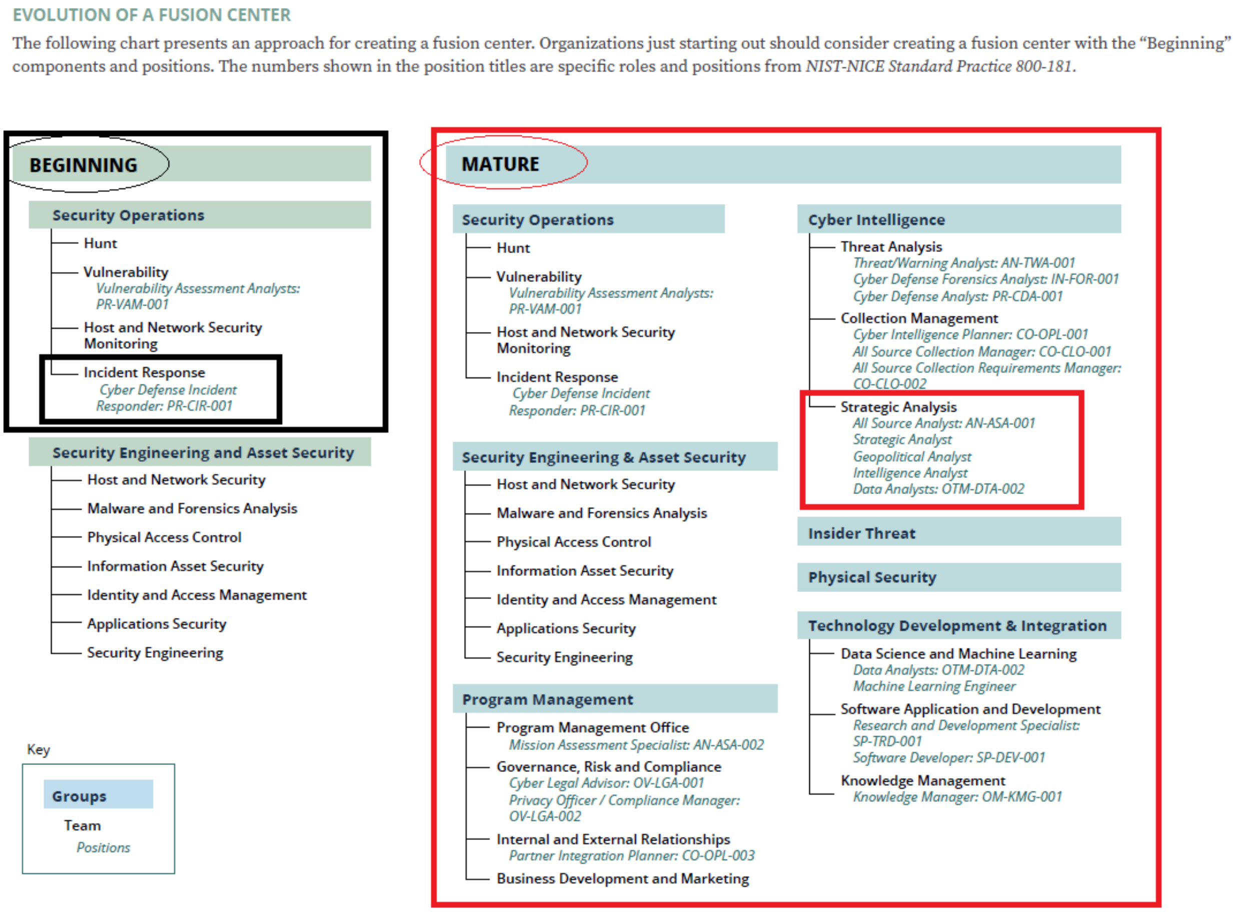
Discipline/Workforce Role
Security, Intelligence, Forensics, Engineering, Data Science, Knowledge Management, etc.
*Each discipline is separate with unique characteristics and attributes

Acumen
Risk, Threat, Vulnerability
*Risk from a strategic business risk perspective, Threat from an operational ‘External/Internal/Other’ perspective
**Not ‘Risk and Threat’ from a purely technical/tactical ‘Vulnerability Management’ perspective

Figure 1. The Cyber Brief, YouTube Channel (2019)

*Disclaimer. Opinions expressed belong solely to the author “Dr. J” and are not associated with the opinions, views, or postures of any specific employer or government.

Further, using ‘Cybersecurity’ in the title enables the (mal)practice of ‘retrofitting everything under the Security discipline’ instead of progressive ‘full-spectrum’ ‘mature’ ‘fusion’ operations (Carnegie Mellon SEI, 2019).



EVOLUTION OF A FUSION CENTER

The following chart presents an approach for creating a fusion center. Organizations just starting out should consider creating a fusion center with the “Beginning” components and positions. The numbers shown in the position titles are specific roles and positions from *NIST-NICE Standard Practice 800-181*.

BEGINNING

Security Operations
- Hunt
- Vulnerability
  Vulnerability Assessment Analysts: PR-VAM-001
- Host and Network Security Monitoring
- Incident Response
  Cyber Defense Incident Responder: PR-CIR-001

Security Engineering and Asset Security
- Host and Network Security
- Malware and Forensics Analysis
- Physical Access Control
- Information Asset Security
- Identity and Access Management
- Applications Security
- Security Engineering

Key

Groups
Team
Positions

MATURE

Security Operations
- Hunt
- Vulnerability
  Vulnerability Assessment Analysts: PR-VAM-001
- Host and Network Security Monitoring
- Incident Response
  Cyber Defense Incident Responder: PR-CIR-001

Security Engineering & Asset Security
- Host and Network Security
- Malware and Forensics Analysis
- Physical Access Control
- Information Asset Security
- Identity and Access Management
- Applications Security
- Security Engineering

Program Management
- Program Management Office
  Mission Assessment Specialist: AN-ASA-002
- Governance, Risk and Compliance
  Cyber Legal Advisor: OV-LGA-001
  Privacy Officer / Compliance Manager: OV-LGA-002
- Internal and External Relationships
  Partner Integration Planner: CO-OPL-003
- Business Development and Marketing

Cyber Intelligence
- Threat Analysis
  Threat/Warning Analyst: AN-TWA-001
  Cyber Defense Forensics Analyst: IN-FOR-001
  Cyber Defense Analyst: PR-CDA-001
- Collection Management
  Cyber Intelligence Planner: CO-OPL-001
  All Source Collection Manager: CO-CLO-001
  All Source Collection Requirements Manager: CO-CLO-002
- Strategic Analysis
  All Source Analyst: AN-ASA-001
  Strategic Analyst
  Geopolitical Analyst
  Intelligence Analyst
  Data Analysts: OTM-DTA-002

Insider Threat

Physical Security

Technology Development & Integration
- Data Science and Machine Learning
  Data Analysts: OTM-DTA-002
  Machine Learning Engineer
- Software Application and Development
  Research and Development Specialist: SP-TRD-001
  Software Developer: SP-DEV-001
- Knowledge Management
  Knowledge Manager: OM-KMG-001

Figure 2. Carnegie Mellon SEI Cyber Intelligence Tradecraft Report (2019)

Example, per the US Naval Academy (2018) and Universities from Harvard to Phoenix, Cyber is the operational domain inclusive of all disciplines. The framework naming convention should reflect this. The acronym stays the same, ‘CWF’.

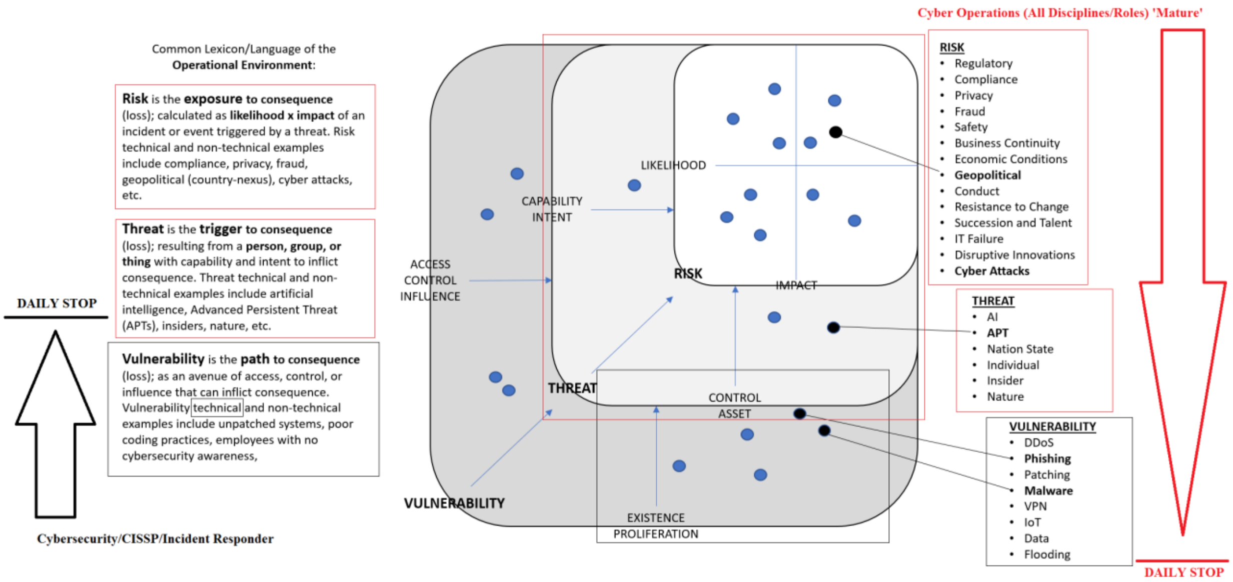
Another great example of the ‘industry culture shift’ can be seen in the recent Defense Civilian Personnel Advisory Service (DCPAS) Direct Hiring Authority ‘Cyber DHA’, not to be confused with the Direct Hire Authority for the 2210 series established by the Office of

Personnel Management (OPM) historically, "… limited to use for one specialty title, Information Security (INFOSEC), within the 2210 IT Management occupational series." (Defense Civilian Personnel Advisory Service (DCPAS), 2019). There is no 'Cybersecurity' DHA for good reason.

2. Standardized Industry Vocabulary/Lexicon

Recommended base vocabulary attached. From policy to practice, the definitions are operationally accurate/correct. A fast way to understand the value is to read the Harvard Business Review (2019) and Infosecurity Magazine (2019) online articles (see References). Know the difference between 'CSO/CISO and C-Suite executive requirements', 'strategic business risk', 'technical vulnerability management', and 'technical controls'.

Problem example. Vendors and 'Cybersecurity/SOC/CISSP/Incident Responders' (mis)use terms like 'risk' and 'threat' in the lowest order of context (technical/tactical, vulnerability management), 'shoe-horning' terms into the 'black box' in the figure below.



Common Lexicon/Language of the **Operational Environment**:

Risk is the **exposure to consequence** (loss); calculated as **likelihood x impact** of an incident or event triggered by a threat. Risk technical and non-technical examples include compliance, privacy, fraud, geopolitical (country-nexus), cyber attacks, etc.

Threat is the **trigger to consequence** (loss); resulting from a **person, group, or thing** with capability and intent to inflict consequence. Threat technical and non-technical examples include artificial intelligence, Advanced Persistent Threat (APTs), insiders, nature, etc.

Vulnerability is the **path to consequence** (loss); as an avenue of access, control, or influence that can inflict consequence. Vulnerability technical and non-technical examples include unpatched systems, poor coding practices, employees with no cybersecurity awareness,

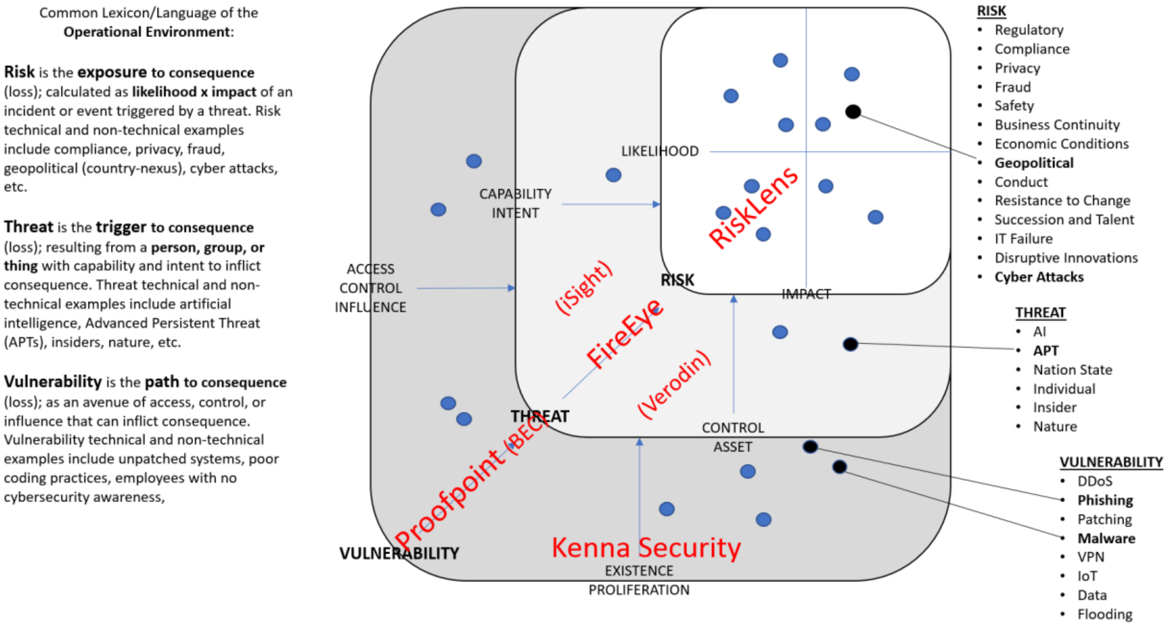
Figure 3. The Cyber Brief, YouTube Channel (2019)

The 'vocabulary confusion' condition has been made worse recently by vendors and security practitioners trying to market/sell products and services using the term 'Cyber Threat

Intelligence' without knowing the context of 'threat' and having never performed intelligence (practice).

In that context, **Cyber** is the Domain, **Threat** (the "who", not threat TTPs or operational phases limited to Cyber Attack threat actors) is nothing without evaluating Risk first (in strategic business risk terms), and **Intelligence**/Analyst (ex. AN-ASA-001) is a single workforce role/discipline, not the same as Security/Incident Responder (ex. PR-CIR-001) (NIST, 2017). Every example presented to date using the term 'Cyber Threat Intelligence' is a marketing pitch promoting the value of technical telemetry, at best.

If NIST NICE CWF SP 800-181 qualified practitioners (all disciplines, specifically Knowledge Manager OM-KMG-001, not 'retrofit' as a Microsoft 'SharePoint Admin') were to leverage existing vendors 'beyond CTI', this is an example what the landscape looks like with industry product and service leaders as of 2019.



Common Lexicon/Language of the **Operational Environment**:

Risk is the **exposure to consequence** (loss); calculated as **likelihood x impact** of an incident or event triggered by a threat. Risk technical and non-technical examples include compliance, privacy, fraud, geopolitical (country-nexus), cyber attacks, etc.

Threat is the **trigger to consequence** (loss); resulting from a **person, group, or thing** with capability and intent to inflict consequence. Threat technical and non-technical examples include artificial intelligence, Advanced Persistent Threat (APTs), insiders, nature, etc.

Vulnerability is the **path to consequence** (loss); as an avenue of access, control, or influence that can inflict consequence. Vulnerability technical and non-technical examples include unpatched systems, poor coding practices, employees with no cybersecurity awareness,

Figure 4. The Cyber Brief, YouTube Channel (2019)

*Disclaimer. Opinions expressed belong solely to the author "Dr. J" and are not associated with the opinions, views, or postures of any specific employer or government.

3. Champion Business Acumen – A Cyber Industry 'Culture Shift'

Fully digest the Harvard Business Review (2019) article, the Infosecurity Magazine (2019) article, and the Carnegie Mellon SEI Cyber Intelligence Tradecraft Report (2019) for ODNI before reading on.

The pervasive 'daily struggle for operational relevance' by Cybersecurity leaders and security staff/personnel is over. Cyber leaders don't have to remain frustrated in attempts to demonstrate business value using technical (telemetry) data alone (minimum operational relevance to executive leaders). Demonstrating business acumen and addressing concerns of strategic leaders (risk) increases business value (maximum operational relevance to executive leaders). Consider leveraging language from existing risk models in the proper 'Mature' context under the Factor Analysis of Information Risk (FAIR) cyber risk framework (FAIR Institute, 2019).

Example, efforts to artificially increase the importance of technical indicator exchange ("threat indicators") between the US Government and Commercial Enterprise organizations using linear/myopic perspectives and definitions of 'risk' and 'threat' with minimum operational value, resulted in US Congress being unimpressed by the current rate of progress. Why? A lack of business acumen.

"Two years after DHS established its Automated Indicator Sharing (AIS) program, just six non-federal organizations are using it to share threat indicators with the government, a DHS official told CyberScoop." "“That's unacceptable and it surely doesn't reach the threshold I hoped it was going to achieve,” Rep. Jim Langevin, D-R.I., told CyberScoop." (Cyberscoop, 2018).

If the system addressed strategic leadership concerns in business risk first as ‘the’ priority, then shared supplement technical data related to vulnerability management and security technical controls only on demand/request, then maybe more commercial enterprise leaders would agree the system has business value and should be supported/utilized.

In this scenario, DHS Intelligence and Analysis (I&A; Cyber Intelligence) would lead efforts, not DHS Cybersecurity (NPPD, now CISA; Cybersecurity). An All-Source Analyst (AN-ASA-001, not Cybersecurity/SOC/CISSP/Incident Responder PR-CIR-001) would increase public-private collaboration, focused on matching DHS HSEC SINs to Corporate Enterprise Intelligence Requirements (IRs), addressing and mitigating strategic (business) risk under existing legislation (Cybersecurity Information Sharing Act of 2015).

The lack of awareness and action summarizes the industry problem and delays in operationalizing the NIST NICE CWF 800-181 framework.

Conclusion

The recommendations/changes are simple and critically important. How fast industry (all participants) can transition or prioritize focus on becoming ‘high performing' 'Mature' 'Fusion Operations' with advanced practiced business acumen in 'strategic (business) risk' terms determines the value proposition and performance measurement NIST NICE CWF SP 800-181 presents.

A sign of progress will be observed in job portals for the specific segments (ex. US Government USAjobs<dot>gov, DiB/Contracting Clearancejobs<dot>com, Commercial/Enterprise Indeed<dot>com, LinkedIn, etc) when we can ‘Google’ the NIST NICE CWF role nomenclature explicitly (ex. search on Indeed<dot>com for “AN-ASA-001”) and get return values.

References

Carnegie Mellon SEI. (2019). Cyber Intelligence Tradecraft Report: The State of Cyber Intelligence Practices in the United States (Study Report and Implementation Guides). https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=546578

CyberScoop. (2018). Private sector isn’t sharing data with DHS’s threat portal. https://www.cyberscoop.com/dhs-ais-cisa-isnt-used-jim-langevin/

Defense Civilian Personnel Advisory Service (DCPAS). (2019). Direct-Hire Authority for Cyber Mission Forces Matters. https://www.dcpas.osd.mil/content/documents/CyberOneStop/CES/CyberDHAFAQS.pdf

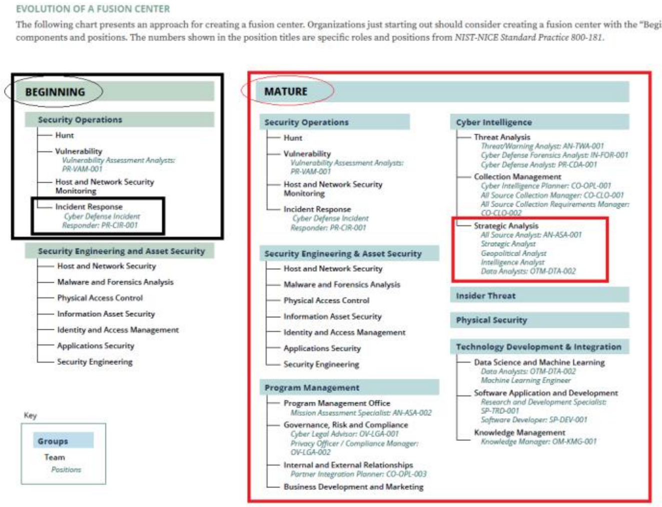
FAIR Institute. (2019). What is the FAIR Institute? https://www.fairinstitute.org/fair-training-and-certification-courses

Harvard Business Review. (2019). Companies Need to Rethink What Cybersecurity Leadership Is. https://hbr.org/2019/11/companies-need-to-rethink-what-cybersecurity-leadership-is

Infosecurity Magazine. (2019). Building a Cyber Risk Report Your Board Will Love. https://www.infosecurity-magazine.com/opinions/build-risk-report-board-love/

NIST. (2017). NIST Special Publication 800-181. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

US Naval Academy. (2018). SY110. https://www.usna.edu/CyberDept/sy110/calendar.php?type=class&event=3



EVOLUTION OF A FUSION CENTER

The following chart presents an approach for creating a fusion center. Organizations just starting out should consider creating a fusion center with the "Beginning" components and positions. The numbers shown in the position titles are specific roles and positions from *NIST-NICE Standard Practice 800-181*.

BEGINNING

Security Operations
- Hunt
- Vulnerability
  - *Vulnerability Assessment Analysts: PR-VAM-001*
- Host and Network Security Monitoring
- Incident Response
  - *Cyber Defense Incident Responder: PR-CIR-001*

Security Engineering and Asset Security
- Host and Network Security
- Malware and Forensics Analysis
- Physical Access Control
- Information Asset Security
- Identity and Access Management
- Applications Security
- Security Engineering

MATURE

Security Operations
- Hunt
- Vulnerability
  - *Vulnerability Assessment Analysts: PR-VAM-001*
- Host and Network Security Monitoring
- Incident Response
  - *Cyber Defense Incident Responder: PR-CIR-001*

Security Engineering & Asset Security
- Host and Network Security
- Malware and Forensics Analysis
- Physical Access Control
- Information Asset Security
- Identity and Access Management
- Applications Security
- Security Engineering

Program Management
- Program Management Office
  - *Mission Assessment Specialist: AN-ASA-002*
- Governance, Risk and Compliance
  - *Cyber Legal Advisor: OV-LGA-001*
  - *Privacy Officer / Compliance Manager: OV-LGA-002*
- Internal and External Relationships
  - *Partner Integration Planner: CO-OPL-003*
- Business Development and Marketing

Cyber Intelligence
- Threat Analysis
  - *Threat/Warning Analyst: AN-TWA-001*
  - *Cyber Defense Forensics Analyst: IN-FOR-001*
  - *Cyber Defense Analyst: PR-CDA-001*
- Collection Management
  - *Cyber Intelligence Planner: CO-OPL-001*
  - *All Source Collection Manager: CO-CLO-001*
  - *All Source Collection Requirements Manager: CO-CLO-002*
- Strategic Analysis
  - *All Source Analyst: AN-ASA-001*
  - *Strategic Analyst*
  - *Geopolitical Analyst*
  - *Intelligence Analyst*
  - *Data Analysts: OTM-DTA-002*

Insider Threat

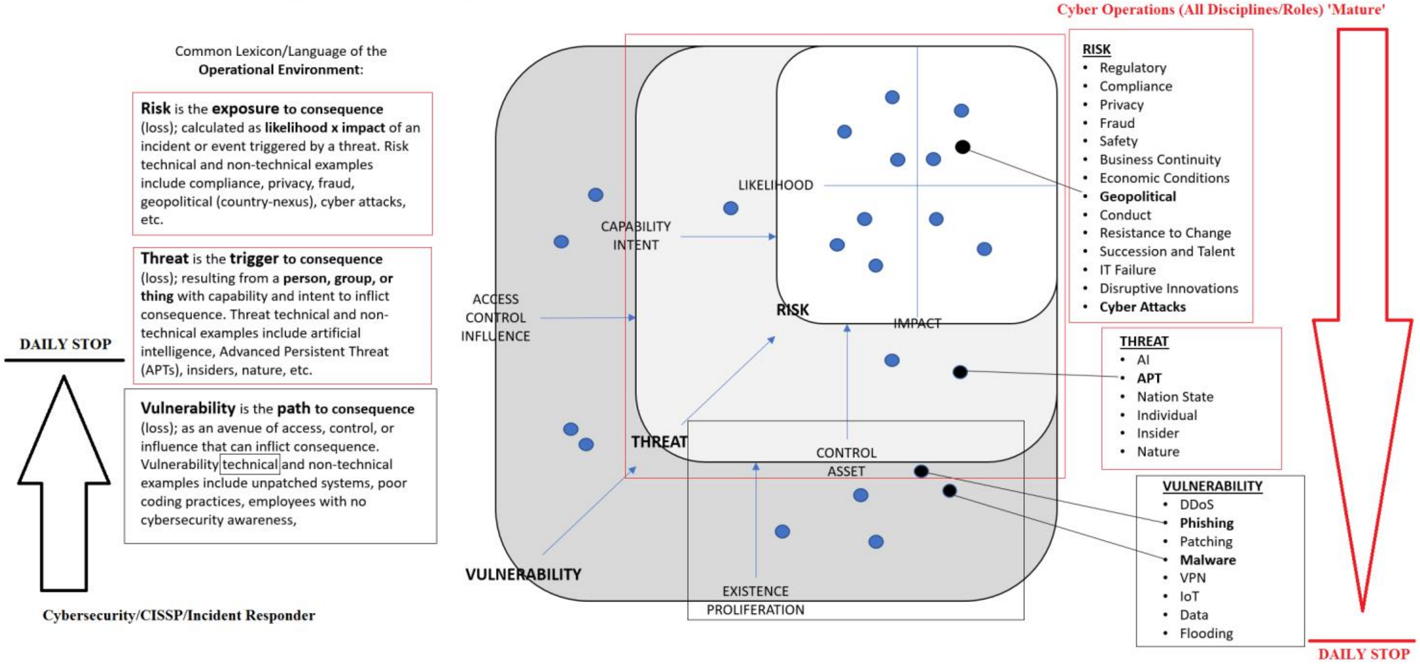
Physical Security

Technology Development & Integration
- Data Science and Machine Learning
  - *Data Analysts: OTM-DTA-002*
  - *Machine Learning Engineer*
- Software Application and Development
  - *Research and Development Specialist: SP-TRD-001*
  - *Software Developer: SP-DEV-001*
- Knowledge Management
  - *Knowledge Manager: OM-KMG-001*

Key

Groups
Team
Positions

Fig 1. **Carnegie Mellon SEI 'Cyber Intelligence Tradecraft Report' for ODNI, 2019**



Common Lexicon/Language of the **Operational Environment:**

Risk is the **exposure to consequence** (loss); calculated as **likelihood x impact** of an incident or event triggered by a threat. Risk technical and non-technical examples include compliance, privacy, fraud, geopolitical (country-nexus), cyber attacks, etc.

Threat is the **trigger to consequence** (loss); resulting from a **person, group, or thing** with capability and intent to inflict consequence. Threat technical and non-technical examples include artificial intelligence, Advanced Persistent Threat (APTs), insiders, nature, etc.

Vulnerability is the **path to consequence** (loss); as an avenue of access, control, or influence that can inflict consequence. Vulnerability technical and non-technical examples include unpatched systems, poor coding practices, employees with no cybersecurity awareness,

Cyber Operations (All Disciplines/Roles) 'Mature'

RISK
- Regulatory
- Compliance
- Privacy
- Fraud
- Safety
- Business Continuity
- Economic Conditions
- **Geopolitical**
- Conduct
- Resistance to Change
- Succession and Talent
- IT Failure
- Disruptive Innovations
- **Cyber Attacks**

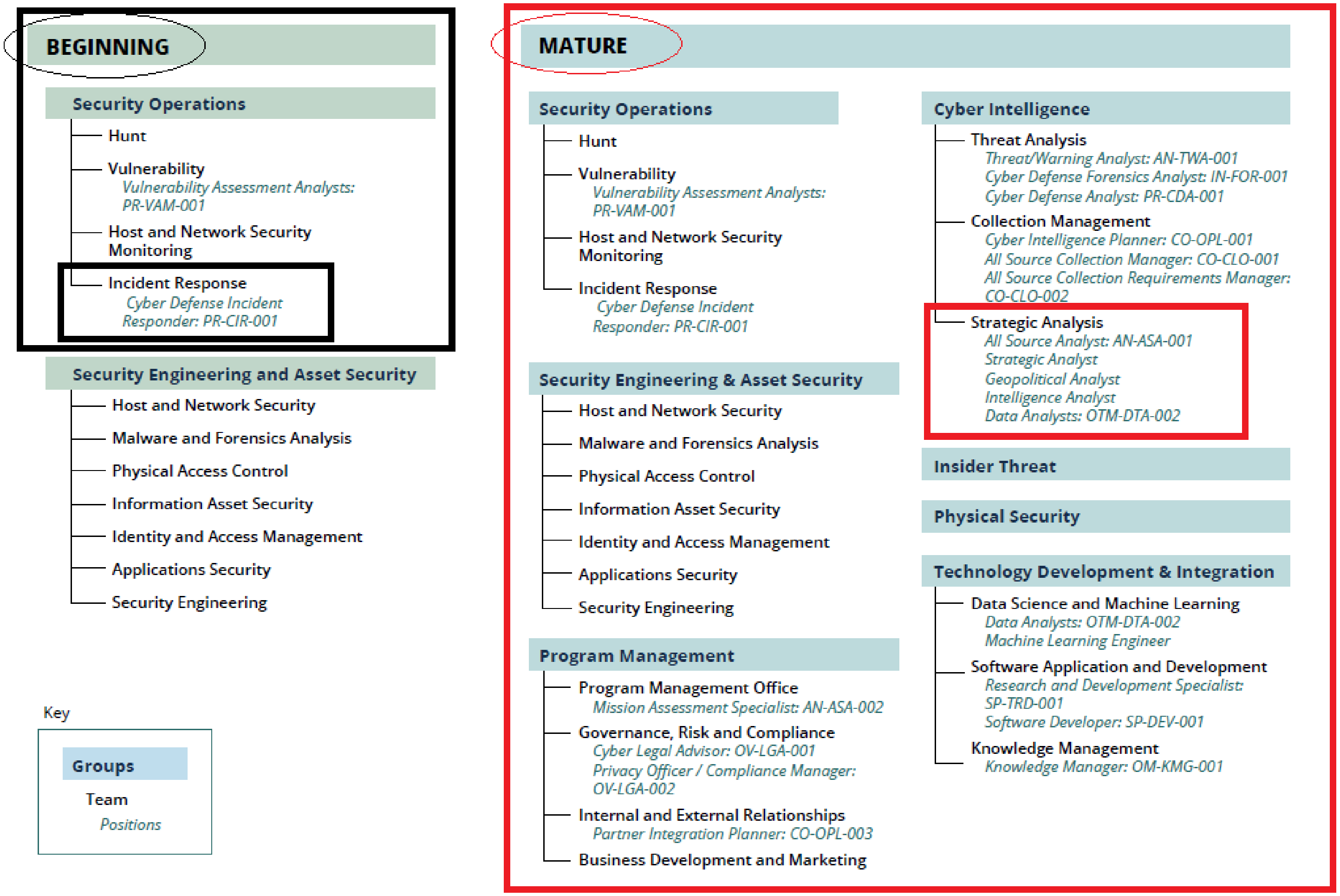
THREAT
- AI
- **APT**
- Nation State
- Individual
- Insider
- Nature

VULNERABILITY
- DDoS
- **Phishing**
- Patching
- **Malware**
- VPN
- IoT
- Data
- Flooding

*Disclaimer. Opinions expressed belong solely to the author "Dr. J" and are not associated with the opinions, views, or postures of any specific employer or government.

EVOLUTION OF A FUSION CENTER

The following chart presents an approach for creating a fusion center. Organizations just starting out should consider creating a fusion center with the “Beginning” components and positions. The numbers shown in the position titles are specific roles and positions from *NIST-NICE Standard Practice 800-181*.



BEGINNING

Security Operations
- Hunt
- Vulnerability
  - *Vulnerability Assessment Analysts: PR-VAM-001*
- Host and Network Security Monitoring
- Incident Response
  - *Cyber Defense Incident Responder: PR-CIR-001*

Security Engineering and Asset Security
- Host and Network Security
- Malware and Forensics Analysis
- Physical Access Control
- Information Asset Security
- Identity and Access Management
- Applications Security
- Security Engineering

MATURE

Security Operations
- Hunt
- Vulnerability
  - *Vulnerability Assessment Analysts: PR-VAM-001*
- Host and Network Security Monitoring
- Incident Response
  - *Cyber Defense Incident Responder: PR-CIR-001*

Security Engineering & Asset Security
- Host and Network Security
- Malware and Forensics Analysis
- Physical Access Control
- Information Asset Security
- Identity and Access Management
- Applications Security
- Security Engineering

Program Management
- Program Management Office
  - *Mission Assessment Specialist: AN-ASA-002*
- Governance, Risk and Compliance
  - *Cyber Legal Advisor: OV-LGA-001*
  - *Privacy Officer / Compliance Manager: OV-LGA-002*
- Internal and External Relationships
  - *Partner Integration Planner: CO-OPL-003*
- Business Development and Marketing

Cyber Intelligence
- Threat Analysis
  - *Threat/Warning Analyst: AN-TWA-001*
  - *Cyber Defense Forensics Analyst: IN-FOR-001*
  - *Cyber Defense Analyst: PR-CDA-001*
- Collection Management
  - *Cyber Intelligence Planner: CO-OPL-001*
  - *All Source Collection Manager: CO-CLO-001*
  - *All Source Collection Requirements Manager: CO-CLO-002*
- Strategic Analysis
  - *All Source Analyst: AN-ASA-001*
  - *Strategic Analyst*
  - *Geopolitical Analyst*
  - *Intelligence Analyst*
  - *Data Analysts: OTM-DTA-002*

Insider Threat

Physical Security

Technology Development & Integration
- Data Science and Machine Learning
  - *Data Analysts: OTM-DTA-002*
  - *Machine Learning Engineer*
- Software Application and Development
  - *Research and Development Specialist: SP-TRD-001*
  - *Software Developer: SP-DEV-001*
- Knowledge Management
  - *Knowledge Manager: OM-KMG-001*

Key

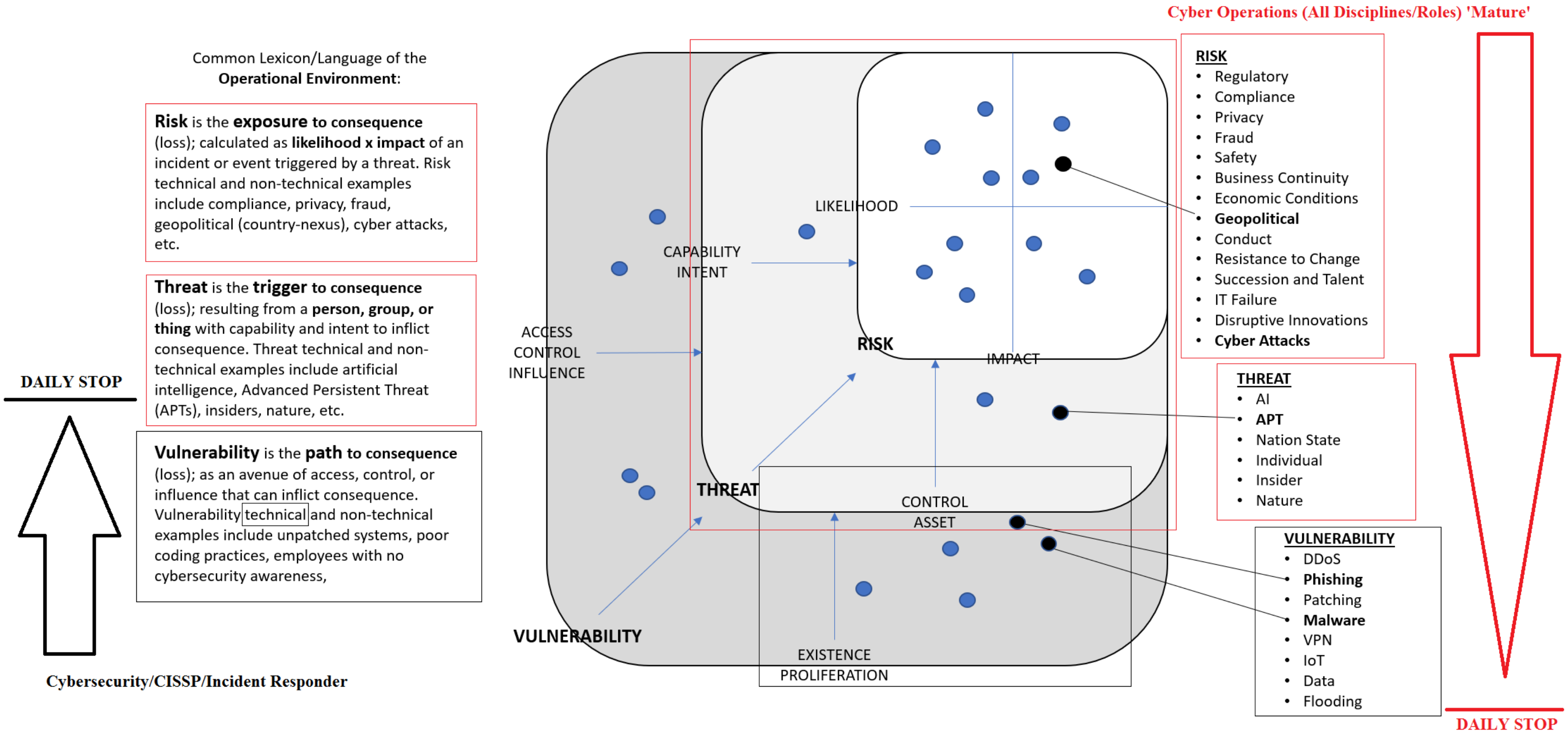
Groups

Team

Positions

Fig 1. **Carnegie Mellon SEI 'Cyber Intelligence Tradecraft Report' for ODNI, 2019**

*Disclaimer. Opinions expressed belong solely to the author “Dr. J” and are not associated with the opinions, views, or postures of any specific employer or government.



Cyber Operations (All Disciplines/Roles) 'Mature'

Common Lexicon/Language of the **Operational Environment**:

Risk is the **exposure** to consequence (loss); calculated as **likelihood x impact** of an incident or event triggered by a threat. Risk technical and non-technical examples include compliance, privacy, fraud, geopolitical (country-nexus), cyber attacks, etc.

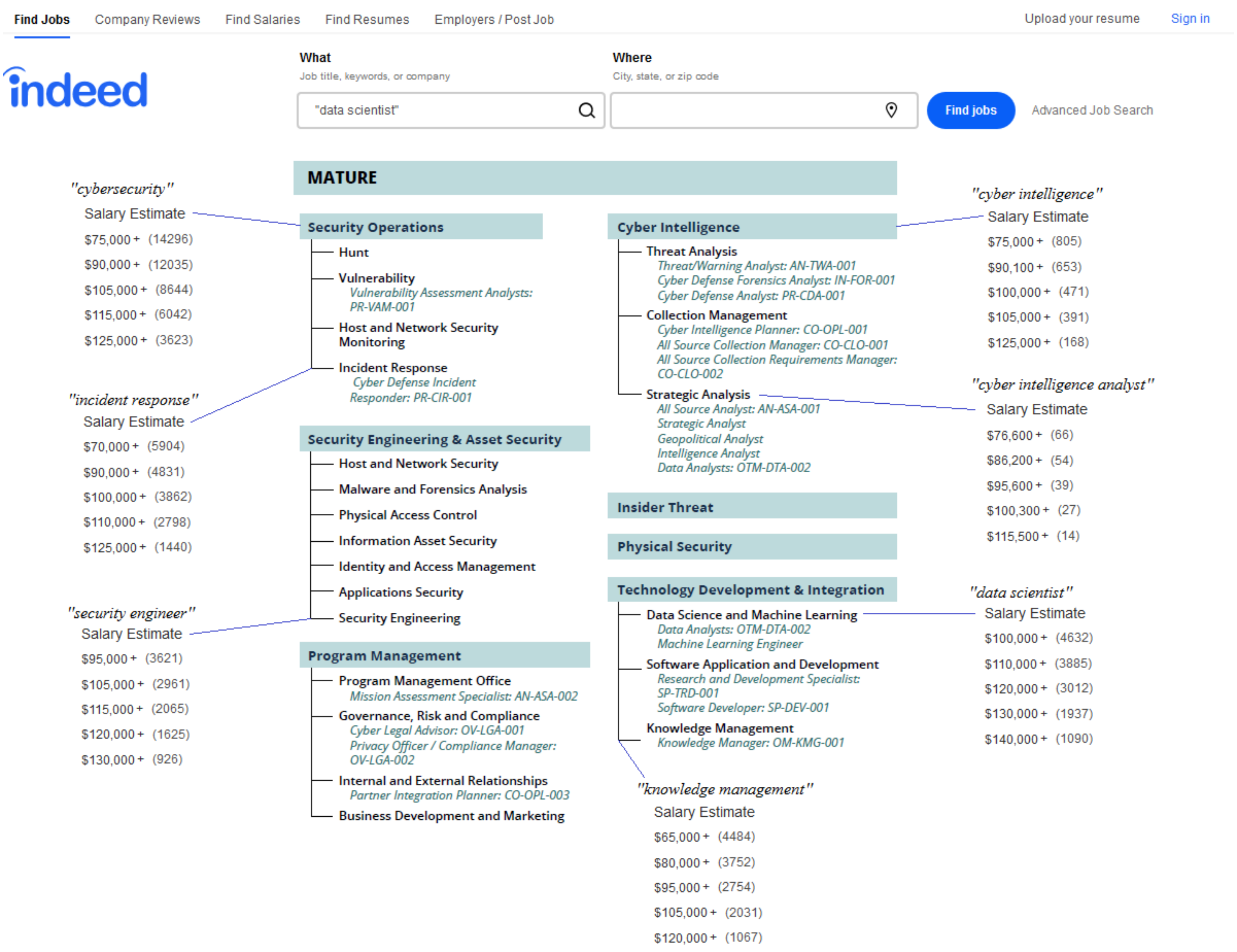
Threat is the **trigger** to consequence (loss); resulting from a **person, group, or thing** with capability and intent to inflict consequence. Threat technical and non-technical examples include artificial intelligence, Advanced Persistent Threat (APTs), insiders, nature, etc.

Vulnerability is the **path** to consequence (loss); as an avenue of access, control, or influence that can inflict consequence. Vulnerability technical and non-technical examples include unpatched systems, poor coding practices, employees with no cybersecurity awareness,

RISK
- Regulatory
- Compliance
- Privacy
- Fraud
- Safety
- Business Continuity
- Economic Conditions
- **Geopolitical**
- Conduct
- Resistance to Change
- Succession and Talent
- IT Failure
- Disruptive Innovations
- **Cyber Attacks**

THREAT
- AI
- **APT**
- Nation State
- Individual
- Insider
- Nature

VULNERABILITY
- DDoS
- **Phishing**
- Patching
- **Malware**
- VPN
- IoT
- Data
- Flooding



MATURE

Security Operations
- Hunt
- Vulnerability
  - *Vulnerability Assessment Analysts: PR-VAM-001*
- Host and Network Security Monitoring
- Incident Response
  - *Cyber Defense Incident Responder: PR-CIR-001*

Security Engineering & Asset Security
- Host and Network Security
- Malware and Forensics Analysis
- Physical Access Control
- Information Asset Security
- Identity and Access Management
- Applications Security
- Security Engineering

Program Management
- Program Management Office
  - *Mission Assessment Specialist: AN-ASA-002*
- Governance, Risk and Compliance
  - *Cyber Legal Advisor: OV-LGA-001*
  - *Privacy Officer / Compliance Manager: OV-LGA-002*
- Internal and External Relationships
  - *Partner Integration Planner: CO-OPL-003*
- Business Development and Marketing

Cyber Intelligence
- Threat Analysis
  - *Threat/Warning Analyst: AN-TWA-001*
  - *Cyber Defense Forensics Analyst: IN-FOR-001*
  - *Cyber Defense Analyst: PR-CDA-001*
- Collection Management
  - *Cyber Intelligence Planner: CO-OPL-001*
  - *All Source Collection Manager: CO-CLO-001*
  - *All Source Collection Requirements Manager: CO-CLO-002*
- Strategic Analysis
  - *All Source Analyst: AN-ASA-001*
  - *Strategic Analyst*
  - *Geopolitical Analyst*
  - *Intelligence Analyst*
  - *Data Analysts: OTM-DTA-002*

Insider Threat

Physical Security

Technology Development & Integration
- Data Science and Machine Learning
  - *Data Analysts: OTM-DTA-002*
  - *Machine Learning Engineer*
- Software Application and Development
  - *Research and Development Specialist: SP-TRD-001*
  - *Software Developer: SP-DEV-001*
- Knowledge Management
  - *Knowledge Manager: OM-KMG-001*

"cybersecurity"

Salary Estimate	
$75,000+	(14296)
$90,000+	(12035)
$105,000+	(8644)
$115,000+	(6042)
$125,000+	(3623)

"incident response"

Salary Estimate	
$70,000+	(5904)
$90,000+	(4831)
$100,000+	(3862)
$110,000+	(2798)
$125,000+	(1440)

"security engineer"

Salary Estimate	
$95,000+	(3621)
$105,000+	(2961)
$115,000+	(2065)
$120,000+	(1625)
$130,000+	(926)

"cyber intelligence"

Salary Estimate	
$75,000+	(805)
$90,100+	(653)
$100,000+	(471)
$105,000+	(391)
$125,000+	(168)

"cyber intelligence analyst"

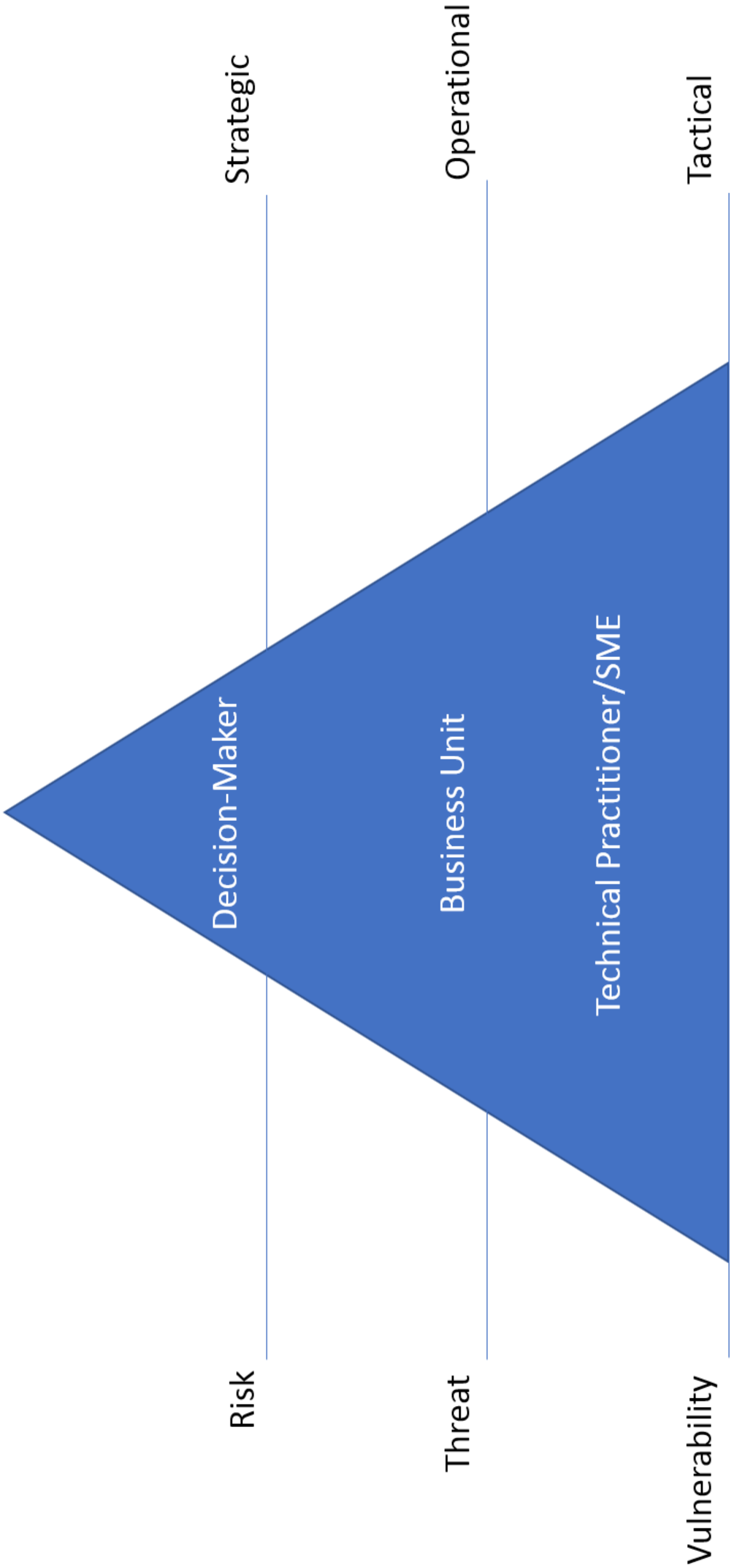
Salary Estimate	
$76,600+	(66)
$86,200+	(54)
$95,600+	(39)
$100,300+	(27)
$115,500+	(14)

"data scientist"

Salary Estimate	
$100,000+	(4632)
$110,000+	(3885)
$120,000+	(3012)
$130,000+	(1937)
$140,000+	(1090)

"knowledge management"

Salary Estimate	
$65,000+	(4484)
$80,000+	(3752)
$95,000+	(2754)
$105,000+	(2031)
$120,000+	(1067)



*Disclaimer. Opinions expressed belong solely to the author “Dr. J” and are not associated with the opinions, views, or postures of any specific employer or government.

Example EXECUTIVE (CSO/SES/GO) Approved and Stated Requirements

Intelligence Requirements (IRs) *<Commercial; CSO/CISO or VP approved>**:***

The EXECUTIVE has reviewed and approved Intelligence Requirements and Priority Intelligence Requirements. These standards serve as the basis for the Cyber Intelligence Collection Plan.

1. Identify notable organization cyber risks
2. Identify notable trends in fraud or insider threat
3. Identify cyber threats targeting the organization
4. Identify cyber threats targeting related industries (telecom, mobility, entertainment, retail…)
5. Identify cyber risks of organization vendors and partners

Priority Intelligence Requirements (PIRs) *<Commercial; VP+ approved>:*

A. Identify who in the organization is being targeted (person, group, or other entity)
B. What is the motive behind the targeting (criminal, political, espionage, or other)?
C. What threat actors/groups are doing the targeting? (enact threat actor/group profiles)
D. What are the organization risks?
E. What are the compensating controls?

Special/Specific Intelligence Requirements *<Commercial; Director+ approved>:*

Each reporting requirement has a daily collection function that correlates to an existing EXECUTIVE approved Intelligence Requirement, resulting in absolute relevance. Each function, or analyst task, is prioritized for effect, making every employee a potential "sensor", regardless of discipline (Security/Intelligence/Forensics/Engineering, or Other).

SIR description:

1. Locations of threat Command and Control infrastructure
2. Locations of threat cache/distribution sites
3. Location and size of indirect threat action (DDoS, etc)
4. Location and size of threat forces
5. Unexplained article, indicator, behavior, or infrastructure
6. Threat reconnaissance activity
7. Significant changes in threat Tactics, Techniques, and Procedures (TTPs)
8. Insider threat attempts against the organization
9. Names, numbers, social nets of (direct/indirect) threat support
10. Attacks on enterprise critical operational areas
11. Damage to enterprise critical operational areas
12. Attacks on related industry verticals
13. Sentiment of country government toward threat forces
14. Information network unwilling or unable to share information
15. Threat force use of Information Operations or propaganda
16. Threat force objective or motive
17. Threat force organizational (enterprise) target(s)

*Disclaimer. Opinions expressed belong solely to the author "Dr. J" and are not associated with the opinions, views, or postures of any specific employer or government.

Vocabulary/Lexicon

• **Cyber Intelligence** – "acquiring, processing, analyzing, and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities in the cyber domain to offer courses of action that enhance decision making" (Carnegie Mellon SEI, 2019).
• **Risk** – **Exposure** to consequence (loss); calculated as '**Likelihood** times **Impact**' of an incident or event triggered by a threat. Risk technical and non-technical examples include Regulatory and Compliance, Privacy, Fraud, Geopolitical (Country-Nexus) and Cyber Attack.

> **Risk** - Combination of the likelihood of an event and its consequence. The business response to risks can be the creation of a requirement. Non-compliance with such a requirement will leave the data/system open to the risk and require security risk management.
>
> Also see '**Blanket Risk'**, '**High Level Organizational Risk** (HLOR)'

• **Threat** – **Trigger** to consequence (loss); resulting from a person, group, or thing with **capability** and **intent** to inflict consequence. Threat technical and non-technical examples include autonomous Artificial Intelligence, Advanced Persistent Threats (APTs), Insiders, Nature, etc.
Threat - The combination of the capability to exploit a vulnerability in order to carry out an attack, together with the intent to do so, thus giving the likelihood of the vulnerability being exploited.
• **Vulnerability** – **Path** to consequence (loss); as an avenue of access, control, or influence that can inflict consequence. Vulnerability **technical and non-technical** examples include unpatched systems, poor coding practices, employees with no cybersecurity awareness, etc.
Vulnerability - Any **weakness** that could be exploited to compromise a system or data, the information it contains, or could be used to compromise other systems. Such a compromise might affect the availability, confidentiality or integrity of the system or data. Vulnerabilities can have varying severities.
• **Domain** - a specified sphere of activity or knowledge. Domains are where humans interact. The physical domains of Air, Sea, Land, Space are now joined by the logical domain of Cyber.
Domain - A collection of networked elements that provide value or service to the company.
• **Discipline** - a branch of knowledge. Disciplines may include Security, Intelligence, Forensics, Engineering, Data Science, or Knowledge Management to name a few.
• **Decision Support** - an information system that supports business or organizational decision-making activities.
• **Bias** - prejudice in favor of or against something.
• **BLUF** – (Bottom Line Up Front) a very short statement where the conclusions and recommendations are placed at the beginning, rather than the end, to facilitate rapid decision making.
• **Operational Environment** - the combination of conditions, circumstances, and influences which will determine the use of resources and help executive leaders make decisions.
• **Intelligence Requirements** - an executive leadership requirement for intelligence to fill a gap in knowledge used in decision-making.
• **Information Sharing** – facts conveyed to maintain the confidentiality, integrity and availability of data.

• **Intelligence Sharing** - acquiring, processing, analyzing, and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities in the cyber domain to offer courses of action that enhance decision making.
• **Data Source Validation** - checking the accuracy and quality of source data before using, importing or otherwise processing data.
• **Admiralty Code** - a method for evaluating collected items of intelligence. The system comprises a two-character notation assessing the reliability of the source and the assessed level of confidence on the information.
• **Cyber Workforce** - the total number of workers actively employed in, or available for work in the Cyber domain.
• **Cyber Operations** - strategic employment of cyber capabilities where the primary purpose is to achieve objectives in or through the Cyber domain.
• **Security Operations** - discipline specific operations that deal with security issues on an organizational and technical level.
• **Common Body of Knowledge** - a core framework of all the relevant subjects a practitioner should be familiar with. A set of concepts, terms and activities that make up a professional practice, mastery over which is required for success in a field or profession.
• **Strategic Analysis** - the collection, processing, analysis, and dissemination of intelligence that is required for forming policy and plans at the 'C-Suite' and Board level.
• **Risk Assessment** – determination of the likelihood and impact of events and incidents resulting in positive or negative consequence and organization tolerances. Risk assessment is an inherent part of a broader risk management strategy to "introduce technical and non-technical control measures to eliminate or reduce" any potential negative risk-related consequences.

> **Risk Assessment** - The process by which a risk is assessed in order to obtain a Risk Assessment Rating. The risk assessment combines Vulnerability Assessment, Impact Assessment and Threat Assessment.
>
> > Also see '**Risk Acceptance** ', '**Risk Analysis**', '**Risk Assessment Rating**', '**Risk Management**', '**Risk Management Assessment** (RMA)'

• **C-Suite** - a cluster of an organization's most important senior executives. C-suite gets its name from the titles of top senior staffers, which tend to start with the letter C, for "Chief," as in Chief Executive Officer (CEO).
• **Actionable Intelligence** – transformative information as a timely and relevant answer to leadership requirements, giving enough recommendation or course of action to enhance decision making.
• **Predictive Analysis** - encompassing a variety of techniques from data mining, predictive modelling, and machine learning, to analyze current and historical facts and make predictions about future or otherwise unknown events and incidents.
• **Tradecraft** (Cyber Intelligence) – tools, techniques, and procedures used to acquire, process, analyze, and disseminate information that identifies, tracks, and predicts threats, risks, and opportunities in the cyber domain to offer courses of action that enhance decision making.
• **Return on Investment** (ROI) - performance measure used to evaluate the efficiency of an investment.
• **Practitioner** - a person actively engaged in an art, discipline, or profession, especially in the Cyber domain.
• **Cyber Intelligence Framework -** analytical framework that provides a structure for cyber intelligence efforts. Components include; Environmental Context, Data Gathering, Threat

Analysis, Strategic Analysis, Reporting and Feedback, and Human-Machine Teaming as a Center of Gravity

- **Center of Gravity** (Cyber Frameworks) – primary source that possesses the inherent capability to achieve the objective
- **Acumen** - the ability to make good judgments and quick decisions, typically in a particular domain.
- **Estimative Language** – terms used in analytic reporting to convey the likelihood and impact of events or incidents.

*Disclaimer. Opinions expressed belong solely to the author "Dr. J" and are not associated with the opinions, views, or postures of any specific employer or government.