ATARC

FEDERAL CISO SUMMIT

JANUARY 25, 2018 | MARRIOTT METRO CENTER | WASHINGTON, DC

On behalf of the Advanced Technology Academic Research Center, I am proud to announce the release of a White Paper documenting the MITRE-ATARC Cyber Collaboration Symposium held on January 25, 2018 in Washington, D.C. in conjunction with the ATARC Federal CISO Summit.

I would like to take this opportunity to recognize the following session leads for their contributions:

MITRE Chair: Mari Spina

Challenge Area 1: Impact of Presidential Executive Order on Cybersecurity

Government Lead: Mervin A. Bourne, Jr., DOJ
Government Lead: Martin Stanley, DHS
Industry Lead: Matt Mandrgoc, Check Point Software Technologies
MITRE Lead: Michael Aisenberg

Challenge Area 2: Quantifying Security Metrics

Government Lead: Renata Spinks, IRS
Industry Lead: Micah Wilson, Duo Security
MITRE Lead: Scott Paul

Challenge Area 3: Challenges for Ever-Changing and Expanding Threat Surface

Government Lead: John Felker, DHS
Industry Lead: Hayri Tarhan, Oracle Public Sector
MITRE Lead: Bill Hill

Challenge Area 4: Addressing the Cybersecurity Skills Gap

Government Lead: Bill Newhouse, NIST
Academic Lead: Dr. Jonathan Katz, University of Maryland
Academic Lead: Dr. Scott White, The George Washington University
Industry Lead: Mike Cotton, Amazon Web Services
MITRE Lead: Nickyra Jackson

Challenge Area 5: Security Challenges with IoT and Other Emerging Technologies

Government Lead: Bill Fisher, NIST
Industry Lead: Adewale Omoniyi, IBM Global Business Services
MITRE Lead: Brian McKenney

Below is a list of government, academic and industry members who participated in these dialogue sessions:

Challenge Area 1: Impact of Presidential Executive Order on Cybersecurity

Wayne Anderson, McAfee; Magdala Boyer, NRC; Daniel Chandler, OMB; John Cuddehe, Lookout; David DeVries, Dataguise; Joseph Esposito, USDA; Tom Harrell, NIH; Mark Lambdin, Check Point Software Technologies; Frank Lancaster, Check Point Software Technologies; Cynthia Larkins, USDA; Birgit Smeltzer, GSA; Christopher Wilson, NOAA

Challenge Area 2: Quantifying Security Metrics

Paul Capobianco, Dataguise; West Colie, GAO; Ronald Davis, USN; Jim Galie, SBA; Naved Iqbal, EXIM; Wanda Jones-Heath, USAF; Steve Luczynski, Census; Kyle Malo, FBI; Shashi Mehta, SBA; Grace Navas, FRB; Sara Ng, IBM; Kathy Penn, FAA; Richard Wainwright, EXIM

Challenge Area 3: Challenges for Ever-Changing and Expanding Threat Surface

James Aguirre, Citrix; Don Fuller, Treasury; Barbara George, DHS; Mark Kagan, Panoptes Intelligence; Said Masoud, MITRE; Marcie McIsaac, GSA; George McKay, GSA; Victor Pimental, GSA; Duane Royal, GSA; Kamran Shah, USCG; Will Slack, GSA; Sovini Tan, BLM; Kyle Vieira, Carahsoft; Lowell Williams, FBI

Challenge Area 4: Addressing the Cybersecurity Skills Gap

Anthony Adkison, DHS; Harold Blunt, IRS; Mike Cotton, Amazon Web Services; Rich Gallagher, GSA; Greg Garcia, USACE; Paul Hill, TSP; Darrell Maxwell, HHS; Joel Waugh, FBI

Challenge Area 5: Security Challenges with IoT and Other Emerging Technologies

Lawrence Binner, DoS; Guy Francois, DoD-VA IPO; Evan Miller, HHS; Terri Peebles-Hunt, DoD; Benjamin Rollins, DoS; Rodney Ross, DoD; Greg Smith, HHS; Nancy Sumption, MITRE; Harold Youra, Alliance Solutions

Thank you to everyone who contributed to the MITRE-ATARC Cyber Collaboration Symposium. Without your knowledge and insight, this White Paper would not be possible.

Sincerely,

George Thomas Suder

Tom Suder
President, Advanced Technology Academic Research Center (ATARC)
Host organization of the ATARC Federal CISO Summit

JANUARY 2018 FEDERAL CISO SUMMIT REPORT[*]

March 22, 2018

Michael A. Aisenberg, R. Scott Paul, Nickyra M. Jackson,
Bill Hill, Said A. Masoud, Brian W. McKenney,
Mari J. Spina, Justin F. Brunelle
The MITRE Corporation

Tim Harvey and Tom Suder
The Advanced Technology Academic Research Center

[*] APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. CASE NUMBER 17-3231-06. **©2018 THE MITRE CORPORATION. ALL RIGHTS RESERVED.**

Contents

1 Abstract

The Federal Chief Information Security Officer (CISO) Summit includes a set of MITRE-Advanced Technology Academic Research Center (ATARC) led Collaboration Sessions that afforded industry, government, academic, and Federally Funded Research and Development Center (FFRDC) representatives an opportunity to collaborate, and discuss prominent challenge areas facing the CISO community. In some cases, potential solutions for key challenge areas were identified by session participants. The discussions were government focused with the objective of refining gaps, and identifying features of potential solutions or frameworks.

Participants representing government, industry, and academia addressed five challenge areas in federal security policy:

1. Executive Orders
2. Measuring Cyber security Success
3. Closing the Skills Gap
4. Managing in the Threat Environment
5. Preparing for Technology Evolution

This white paper summarizes the discussions in the collaboration sessions. Drawing from these discussions, MITRE and ATARC developed the following actionable recommendations for the government, academia, and industry:

Both industry and government persist in failing to truly understand the motivators of each other's Information and Communications Technology (ICT)/cyber reliance, and thus in spite of repeated effort and good intentions, never succeed in true collaboration. Success in addressing the collective cyber security challenge depends on a true meeting of the minds on motivation, risks and solutions.

Agencies have struggled to turn their available cyber security metrics into actionable intelligence for agency leaders because of the inability to relate cyber-threats to mission impact. This is predominately because of the lack of a specialized skill mix to interpret the data (cyber-knowledge combined knowledge of big data analytics/business intelligence); this skills gap is further aggravated by incompatible cyber security data types, standards for cyber security data, and poorly documented mapping of business processes to agency IT assets, agency mission.

Dealing with the expanding cyber attack surface is an ongoing CISO challenge; with many CISOs feeling that attackers maintain an advantage. Corporate networks, external systems, and partnerships are already too big, numerous, distributed, and complex to keep under complete inventory control, and while those problems are increasing new devices and network services are further expanding the attack surface.

The high demand for cyber security talent correlates to the growing, persistent and complex cyber challenges that both the government and private sector face. Lacking an adequate cybersecurity workforce and understanding the ramifications of inaction on this issue, has led to a range of cyber skills learning initiatives (organized or funded by private industry, government, and academia) to close the skills gap. Continued variation in the way this problem is tackled is crucial, as there are unique needs across industries and organizations within those industries. The key is ensuring knowledge sharing and collaboration happens amongst the different approaches to overall strengthen US cyber capabilities and defense posture.

Agencies continue to address the mismatch of increasing consumer expectations vs. enterprise adoption and security approval of IoT devices. The value model of both sides need to be understood, as well as expressing and sharing risk decisions for IoT devices across the Federal government. This includes need for guidance on assessing tradeoffs between functionality, productivity, and security of IoT devices to support business, mission, and workforce requirements, as well as understanding implications of devices for evolving enterprise security architectures.

2 Introduction

During the most recent Federal Chief Information Security Officer (CISO) Summit, held on January 25th 2018, five MITRE-ATARC (Advanced Technology Academic Research Center) Collaboration Sessions gave representatives from industry, academia, government, and MITRE the opportunity to discuss challenges the government faces in mobile computing. Subject matter experts who would not otherwise meet or interact used these sessions to identify challenges, best practices, recommendations, success stories, and requirements to advance the state of mobile computing technologies and research in the government. Participants ranged from the CTO, CEO, and other executive levels from industry and government to practitioners from government, industry, and MITRE to researchers, students, and professors from academia.

The MITRE Corporation is a not-for-profit company that operates multiple Federally Funded Research and Development Centers (FFRDCs) [3]. ATARC is a non-profit organization that leverages academia to bridge between government and corporate participation in technology[1]. MITRE works in partnership with ATARC to host these collaborative sessions as part of the Federal CISO Summit. The invited collaboration session participants across government, industry, and academia worked together to address challenge areas in cyber security, as well as identify courses of action to be taken to enable government and industry collaboration with academic institutions. Academic participants used the discussions as a way to help guide research efforts, curricula development, and to help produce graduates ready to join the workforce and advance the state of security research and work in the government.

This white paper is a summary of the results of the collaboration sessions and identifies suggestions and recommendations for government, industry, and academia while identifying cross-cutting issues among the challenge areas.

3 Collaboration Session Discussions and Outcomes

The conference break-out sessions were targeted to address the topics most noted by public sector constituents as areas creating anxiety in the CISO ranks. The topics selected are listed below.

- Session 1: Impacts of Executive Order 13800

[1] `https://www.atarc.org/about`

- Session 2: Quantifying Security Metrics
- Session 3: Challenges for Ever-Changing and Expanding Threat Surface
- Session 4: Addressing the Cyber security Skills Gap
- Session 5: Security Challenges with IoT and Other Emerging Technologies.

3.1 Session 1: Impact of EO 13800

With the new administration came a renewed push for employment of shared services and common cyber security solutions. This session discussed the recent guidance coming from the executive branch including the Presidential Executive Order (EO) 13800, Strengthening the Cyber Security of Federal Networks and Critical Infrastructure[2], the Report to the President on Federal IT Modernization, and Secretary of Defense memo Accelerating Enterprise Cloud Adoption. The session assessed the impacts upon federal agencies and discussed possibilities and options for achieving associated objectives.

3.1.1 Session 1: Summary of Discussions

The attendees in this session comprised a diverse group of both government and industry interests, including senior agency officials, industry C-suite individuals, and included many with information technology policy experience as well as germane government acquisition expertise.

In spite of – or, perhaps, as a result of – the diverse nature of the participants in this working group, there was broad agreement among the session participants that the evidence of the level of national policy consensus on cyber security, particularly as reflected in EO 13800, but dating back through several decades, at least with regard to the role of United States Government (USG) agencies' leaders, and in particular CISOs, is insufficient both as a source of cyber security policy generally and as basis for effective guidance to agencies. Clearly, the "long pole in the tent" is the pervasive concern with the nature and adequacy of engagements between the vendor community and the government customer, at a level sufficiently robust to produce effective dialogue regarding actionable cyber security policy, and the deployment of effective measures.

The key consensus findings/concerns of the group framed several topics which the participants agreed have continuing impact on the conduct of information security practice in

[2] https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

USG agencies and the resulting cyber security posture of the entire U.S., and, by extension, global Information and Communications Technology (ICT) ecosystem.

The participants found that a risk-creating, unaddressed technology gap exists between rapidly evolving/increasing technical expertise among the ICT developer and vendor communities and much of the (aging) government employee population

They identified a critical corollary to the technology gap: advances in technology are outpacing technical education, and without a program of tailored training and education targeted to leadership, acquisition staff, users and operators and others responsible for elements of the USG ICT fabric, dangerous security risk will persist.

Similarly, a consequential risky disconnect exists between government and private sector key staff regarding their mutual (mis)understanding of technology, vulnerabilities, and the drivers of each other's practices. Decision makers in government are not appropriately familiar with the structure of the private sector ICT industry on which they depend (including research activities, products, business drivers, practices, and role of government business in the overall commercial ICT marketplace).

Another key finding is viewed as a *cultural issue*: The persistent, sometimes baffling, evidence of the "disconnect" between industry leaders and their USG customers is apparent in the role of classification system and privacy considerations used as barriers to information sharing.

The working group participants also identified several other core concerns, particularly from the industry perspective.

One very important "pre-cursor" issue identified is the need for a widely shared lexicon of key common terms.

Closely related to, and perhaps the real issue for which the above-cited "cultural issue" might contribute is an overall lack of trust. The group found that process contributing to the building of *trust* between industry (ICT vendors) and government is important, and presently lacking, and impactful.

Substantively, the structure and execution of the *procurement/acquisition* process for ICT products and services, both Commercial Off The Shelf (COTS) and embedded in major systems acquisition is a, if not *the* key problem.

A number of session participants described the environment as one in which there is no shortage of practices and techniques to address specific cyber security threats and vulnerabilities (e.g., access controls, secure configuration, protective software, supply chain management); yet due to implementation and inconsistent practice or poor execution by both vendors and USG customers, the resulting overall environment retains unacceptable levels of risk. This was summarized under the phrase cyber security is not a “tools” problem, it is an *attitude* problem.

Participants identified an emerging view that USG agencies as a community (Congress, as well) do not understand and thus do not behave with an awareness of the scope and scale of the critical role of *data*, associated storage requirements/options (and Total Life Cycle implications) across the whole of government (including State/Local/Tribal). This is true whether National Security and Intelligence agencies and missions, critical infrastructure such as the money system and finance (Treasury/IRS/SEC), health care, (HHS/FDA), food supply (Ag), or the broader civilian economy.

Related to this is the fact that the EO 13800 does not address this persistent lack of understanding regarding several of the already-cited recurring root-cause issues:

- The nature and pace of technology change
- The companion issues of inconsistency of awareness of cyber security among agency leadership (e.g., C-suite leadership, key employees, contracting officers)
- USG customer mission requirements by vendor industry leadership
- The practice of ICT Acquisition by the USG
- The structure of ICT industry, including its legal obligations (fiduciary duty) to shareholders
- The continuing characterization of and deference to social media (Facebook, Twitter) as “technology”

3.1.2 Session 1: CISO Business Concerns

A critical precursor issue exists which pervades the entire cyber security conversation: the need exists for a widely shared lexicon of key common ICT and related cyber terms. We must be able to communicate; we should begin by agreeing with how we express what we are talking about. The Intelligence Community (IC) lexicon under ICD 700[3], the Committee on National Security Systems (CNSS) Glossary and others exist and provide great value; an important contribution would be an exercise to harmonize and widely adopt a common integrated lexicon. For example, consider the Common Expression STYX/TAXI[4] exercise for vulnerabilities expression which has now become an industry standard.

[3] https://definedterm.com/intelligence_community_directive_icd_700

[4] https://oasis-open.github.io/cti-documentation/

A risk-creating, unaddressed technology gap exists between rapidly evolving/increasing technical expertise among the ICT developer and vendor communities and much of the (aging) government employee population. This includes the users of ICT systems, and their superiors who define agency policy, request authority and funding, and thus define the USG component of the technology *ecosystem.*

Especially as a result of politically dictated leadership turnover, the inconsistencies in levels of familiarity and understanding can become debilitating to the achievement of agency cyber security objectives and programs. New Congressmen and Senators are sent to policy process training at the Kennedy School between their election and their swearing in; new agency leadership should receive at least a basic familiarization with generic and agency-specific cyber security issues.

A critical corollary observed by participants, perhaps contributing to the inconsistent levels of understanding is the fact that advances in technology are outpacing technical education, so that even Subject Matter Experts at agencies may not have the most current understanding of elements of the environments for which they are responsible.

A similar risky disconnect exists between government and private sector (staff) regarding their mutual understanding of technology, vulnerabilities, and the drivers of each other's practices.

As evidence of this "disconnect", participants cited what was described as a "cultural issue", to be found in the role of the classification system and privacy considerations used as barriers to information sharing. The misperception of each community's imperatives/requirements must be first addressed within government as practical policy issue.

Several specific examples of this disconnect exist. For example, emerging practice from DoD increasing the responsibilities under the Defense Federal Acquisition Regulation Supplement (DFARS) for Controlled Unclassified Information (CUI) in hands of federal contractors, the proliferation of Top Secret-cleared population in government, not matched by clearances for critical industry partners, and the continuing failure of NARA and custodian agencies to declassify 35 billion pages of determined over-classified data.

3.1.3 Session 1: CISO Business Solutions

In transiting from issue spotting and findings towards actionable recommendations, the working group identified opportunities for changed or improved practices. In the procurement/acquisition area, developing a cyber threat-aware acquisition process is a key problem and opportunity.

The procurement system must be revamped with a more accurate understanding of the realities of the vendors' practices. Acquisitions of ICT must be linked to "total product lifecycle", with CISO/security concerns taken in to account in mission discussions, procurement design/specification, the actual acquisition process (beyond the important DoD-style Program Protection Plan process, which *must* be expanded to all agencies), and system deployment.

This means that such security linked procurement "events" must be more strictly institutionalized through policy (statute, regulation, DFARS, DFRAR model provisions, training, vendor dialogue). Such elements and obligations as the emerging CUI obligation on contracting vendors, the incorporation of supply chain-aware elements in vendor solicitations during the pre-milestone A processes of acquisition (e.g., specification development, request for information (RFI)).

The USG acquisition process is antiquated compared to the pace and scale of ICT industry evolution. (Note the evolution of once vaunted products such as lap-top computers to the level of disposable commodity.) The failure of USG acquisition to maintain currency with industry results in wasteful, often cosmetic procedures. In cyber security, examples of counter-productive procedures are legendary. For example: note the discrediting of access control régimes, where practice in the IC has been the requirement 18-character passwords changing every 90 days. These "mismatches" between many agency practices and actual risk endangers security through non-compliance and risky work-arounds.

An issue of the procurement process repeatedly cited as a source of disruption, inefficiency and risk is the persistence of the single year Annual Congressional Budget and Appropriations process. The one year process is a fundamental impediment to quality and sensible secure acquisition of ICT and necessary cyber modernization.

Related to this, is the structure of the account system applied to ICT acquisitions adopted by many agencies, which functions as a gimmick, retaining authority in specific line organizations to the detriment of agency improvements, especially in ICT (e.g., VA Directive 6500. And associated Handbook 6500; 356 pp.[5]). The pervasive characterization of relatively short-life expectancy ICT equipment as requiring treatment of many ICT acquisitions under capital funds, rather than operating budgets is typical of the finance machinations which ultimately impair security, by unnecessarily attenuated acquisition processes, often layered over long, post-obsolescence retention of the legacy devices in the first place. Participants referenced the need to adopt practices to make current agency operating funds available for purchases of ICT to support the cyber modernization which is a pervasive need across government.

As noted, participants cited inconsistent understanding as a root contributor to "disconnects" resulting in practices which constitute cyber security risks. One term of great impact is

[5] https://www.va.gov/vapubs/search_action.cfm?dType=1

the concept of “critical infrastructure.” What does the CISO and broader USG agency security community understand to constitute Critical Infrastructure? Is it my agency’s; the nations? This must be understood before specification, acquisition, deployment, and funding can be done in a manner that makes sense and stands a chance of being successful.

Another area of practice ripe for improvement is the question of specific CISO obligations and reporting relationships. Under Federal Information Security Modernization Act of 2014 (FISMA 2014) and its implementation under Rev. OMB Circ. A-130, the scope and detail of specific cyber security practice under CISO management has become more specific; however, the responsibility and accountability for agency cyber security is now, by statute, focally located with the agency head and the Chief Information Office (CIO).

This begs the issue under some, especially, large agency, and long-standing cyber practice (e.g., DoD, VA, HHS, DHS) of “what will the CISO do?” Questions to be asked and policies to be revised include “What information sharing pathways exist between mission/users, CIO team, program specifiers/architects, acquisition teams, and funding managers in organizational and agency front office?”

And, emerging as a key companion issue to be addressed is “What is the Role of DATA in defining cyber security risks/responsibilities?” This implicates the structure and authority of the emerging role of Chief Data Officer (CDO): is the CDO the new ombudsman/honest broker independent of EACH other key agency role (e.g., CIO, mission/users)?

Participants also identified the government’s approach to Internet of Things (IoT) including ambiguities of understanding and scope (e.g., IoT, Internet of Everything, Industrial IoT, Cyber Physical Systems, Industrial Control Systems/Supervisory Control and Data Acquisition (SCADA) in critical infrastructure): What is it? Must each agency develop a *local* understanding, definition, training and implementation? As with the rest of technology, the underlying technology is both expanding in scope and scale, and constantly morphing; can we keep up? What are the criteria underlying effective agency understanding of this new area, shared with its critical private sector partners?

Participants also noted, however, that “IoT an example of a transient hot button phenomenon/catch phrase that can become impediment to action: Prior examples cited include: data breach, critical infrastructure, information sharing, privacy, US Person. And, even before the discussion of IoT is resolved, or even truly scoped and ripened, new complexities are arising around the above-cited role of “data”, data architecture, data stewardship as a phenomenon and discipline, rife with cyber security implications, yet potentially out of the scope of responsibility for existing agency roles such as CIO and CISO Emerging: data.

3.1.4 Session 1: CISO Business Recommendations

The discussions summarized in this section led not only to the specific findings and suggestions of areas warranting further research and policy development, but also specific recommendations for action, largely by agencies, but in some instances, by industry or by partnerships.

To address the pervasive concern regarding disconnect between vendors and customer agencies on fundamental issues of ICT/cyber security, agencies should revisit, revise and promptly deploy – in consultation with industry and academic sources – new, revised baseline substantive cyber training for IT/cyber security to government employees.

This training is especially relevant for contracts/acquisitions employees, who appear to lack the experience necessary to make the best security decisions.

This training to staff should be provided in consultation with ICT industry, recognizing issues around agency cyber security requirements, data scope and scale, and data privacy. Delivery should be tailored to specific USG staff audiences:

- Program for FISMA-responsible agency heads, CIOs
- Program for other agency decision makers
- Program for contracting officers and those engaged in spending agency funds
- ICT products and services

The community – industry and government, must create more fora for information sharing between strategic vendors and USG agencies re: cyber/ICT products.

In the area of governance, it was recommended that heads of agencies must individually take responsibility to set the proper *tone* for cyber security (e.g., FISMA 2014); it was observed that taking CISO out of statutory responsibility loop may have been error.

But, as suggested, assumption of responsibility is only a first step; effective improvements in the resolution of the variety of cyber security issues falling into the responsibility of senior agency officials will depend on both internal and external measures. Not only must authorities and governance be clarified and restated, but the essential elements of effective vendor engagements and resulting collaborative security measures and practices must occur for there to be meaningful impact on the ongoing and evolving suite of cyber security challenges. Whether these necessary authorities and governance directions have been captured in EO 13800 is open to serious debate. It may be concluded that they have not addressed the question of what policy instruments will be required to assure appropriate behavior change to address present and future cyber security challenges.

3.2 Session 2: Quantifying Security Metrics

With the focus on recent EOs, CISOs across government will be asked for more metrics and improved measures of success. CISO's are expected to report their status and demonstrate their achievements yet little guidance or common practices exist to support the CISO in this task. At the same time, today's security products are generating greater and greater amounts of cyber related data. This session focused upon measures of cyber effectiveness and various means for reporting. It discussed common metrics used by CISOs and the role of Security Information and Event Management (SIEM) systems, cyber analytics, and the use of big data systems in tracking and measuring cyber security effectiveness.

3.2.1 Session 2: Summary of Discussions

The group focused discussion on Quantifying Security Metrics with some discussion on emerging technologies, such as artificial intelligence (AI) and big data analytics. Several key Quantifying Security Metrics themes emerged:

- *People/Process/Technology Gaps*: Personnel skill-sets and agency business processes have not kept up with advances in security metrics and analytics
- *Lack of business value from security metric reports*: While there are lots of security metrics produced, there is little value or actionable information generated from security metrics
- *A shift in agency culture shift is needed to benefit from security metrics*: To maximize value from security metrics, agency culture needs to shift from being Information Assurance focused to being Cyber-Security focused
- *Regulations and standards are still emerging for security metrics*: As a result of unclear guidance and evolving standards, it is difficult to generate reports with meaningful security metrics

In summary, it is clear that agencies struggle with having the necessary skills to address quantifying security metrics around agency goals.

3.2.2 Session 2: CISO Business Concerns

Four (4) significant topics emerged in this discussion including business gaps, value, leadership, and emerging regulations and standards.

People/Process/Technology Gaps: In general, the group agreed that there is a lack of cyber-enterprise skill-sets that can analyze and interpret security metrics. Agencies have too many non-integrated tools and business processes generating security metrics. As a result, security metric data generated from different business areas is not correlated. Adding to this inability to correlate different data streams, agencies have not updated or standardized their rating systems (e.g., high, medium, and low risks). From an infrastructure perspective, agencies are starting to struggle with the burden and expense of storing massive amounts of security data. Legacy systems need special monitoring and security monitoring tools that will integrate with modern security metrics platforms.

Business value: Security metric reports need to be tailored to specific business audiences. One-size-fits-all reports add very little value to an agency. Security metric reports for agency leaders must focus on impacts to mission/business, including ROI and portfolio management. Other specific value-added security metric-generated reports that the group would like to see include:

- Automated compliance reports generated using security information and event management technologies
- Insider threat and Threat Risk Model for planning offensive Threat Modelling (APT), including a baseline
- Security metrics on Shadow IT (Shadow IT metrics is viewed as a part of Insider Threat)
- Security metrics that show increased/reduced risk through cloud migration
- Security metrics to support acquisition risks (e.g., software with foreign investors)

A shift in agency culture shift is needed to benefit from security metrics: Most agency policies are written around information assurance, focusing predominately on technology without an agency context. Policies and procedures need to be updated to incorporate the impact and risk of IT system security to agency business/mission. This will require a change from the top – agency leadership needs to embrace a cyber-view of their computing environment. Many CIO's fear sharing agency security metric data with their counterparts, which results in an overall weakening of agency security posture. Agency policies also lack clear and definitive enforcement mechanisms for non-compliance.

Regulations and standards are still emerging for security metrics: Agencies are struggling with security metric generation for systems that process sensitive data (e.g., Personally Identifiable Information/Protected health Information (PII/PHI)). There is vague and/or conflicting guidance on the security metrics requirements for sensitive data. Agencies also have special data handling requirements for systems involved with acquisitions and Federal Acquisition Regulations (FAR), which have not translated into clear security metrics requirements for those systems.

Within industry, correlation of data is difficult because naming standards do not exist for security tools and metrics. The group agreed that there is a need for a common taxonomy for:

- Cyber vs IA
- Cyber Threat Model (confidentiality, integrity, availability):
- Anticipate
- Respond
- Cyberthreats
- People/process/technology
- Threat risk model (heat map)

In summary, agencies are not equipped with the skills to present security metrics that provide business value. A shift in leadership approach to towards greater priority on security metrics development and presentation is suggested.

3.2.3 Session 2: CISO Business Solutions

Some agencies with mature security metric programs could utilize existing business intelligence and data science teams to analysis security metrics and generate reports. Successful security metric teams also leveraged their agency strategic communications teams to disseminate reports and gather feedback. All group members agreed that artificial intelligence will help to bridge the “people skills” gap in the future in the generation of meaningful security metrics.

The most effective way to deliver security metric reports to leadership and change their views on security metrics were through presentation of high-level heat maps that included a baseline for security metrics and the “deltas” or anomalies. Coupled with suggested actions, these reports gave leadership the high-level situational awareness they needed that lead to action. Agency leaders respond best to custom security metric reports that allowed the business leaders to understand the security posture of agency.

While there was no consensus as to how to deal with Federal regulation requirements for security metrics, individual agencies were creating their own policies regarding the security metrics needed on their sensitive data. Some agencies were utilizing the NIST Risk Management Framework[6] to set risk levels.

In summation, as we look across the array of topics discussed, we can see that the best solutions to quantifying security metrics always are linked to the needs of the business.

3.2.4 Session 2: CISO Business Recommendations

As a result of discussions in this interest group, four substantive recommendations for improving agency skills, developing presentation formats, and leadership guidance are provided.

People/Process/Technology Gaps: Agencies are learning to perform cross-training of existing data analysis teams. They have found it is easier to teach a big data analyst cyber security, than it is to teach a cyber-professional how to do big data analytics. By going outside of traditional cyber security communities, they have been able to find new sources for needed skills and bring new perspectives to their security metrics.

Leveraging their business intelligence and big data analytics teams, some agencies were looking at cyber-metrics on their own workforce to look for opportunities to provide targeted cyber-training. To increase the cyber security posture of agency employees, agencies are putting on “cyber security roadshows” where they showcase their cyber security metrics, putting them in context for their audience. The employee outreach programs are supplemented with follow-on training/testing that comes with rewards (e.g., Director for a Day experience, group awards, 59-minute early dismissal).

Agencies are also leveraging Federal-level and industry tools to bridge the technology and skills gap (e.g., SANS study on reporting metrics[7], NSCSAR[8] and govCAR Scorecard[9], DHS demark metrics/reports[10]).

Business value: Agency leaders seem to get the most value from security metric reports that provide trend analysis. Agencies with successful security metric programs use data scientists to help provide business context to the security issues described in their security metric reports. The reports also contain potential resolutions and impacts for leadership. The security metrics must be tied to the cyber-architecture that support business portfolio.

[6] https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview

[7] https://www.sans.org/reading-room/whitepapers/auditing/guide-security-metrics-55

[8] https://disa.mil/~/media/Files/DISA/News/Conference/2016/AFCEA-Symposium/3-Dinsmore_NSCSAR.pdf

[9] Notyetpubliclyavailable

[10] https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-08-Jan16.pdf

Some agencies use business intelligence tools specifically designed to show portfolio risk metrics (e.g., Tanium, Tableau).

A shift in agency culture shift is needed to benefit from security metrics: In order to change agency culture regarding the use of security metrics, teams who report their findings must be transparent with leadership regarding the security metrics and their meaning. It is important to build trust between the cyber security teams and leadership in order for security metrics to be used as a reason for leadership to make impactful changes to agency operations. As part of building trust and changing agency culture, some cyber security teams employ their strategic communication team to craft message to C-Suite. To encourage transparency between agencies, the group recommends teaming with other agencies that have a similar size and risk profile.

Next steps and opportunities for collaboration include:

- Agencies with similar size and risk profiles can share security metric data and best practices
- Team with industry and trade groups to develop a common taxonomy for security metrics
- Agencies with similar sensitive data concerns can share security metric reporting requirements and best practices
- Agencies can pool "hard to find" skill-sets, such as big data analytics, in the development of their security metrics

3.3 Session 3: Challenges for the Ever-Changing and Expanding Threat Surface

Cyber-attack sophistication is increasing (e.g., autonomous machine hacking, ransomware). The cloud is morphing the boundary and extending the cyber threat surface. Long term approaches and strategies for governing in this ever changing mostly indeterminate environment are vital to a CISO's success. This session addressed proactive and reactive approaches to managing in this environment. Organization governance approaches were shared and examined.

3.3.1 Session 3: Summary of Discussions

When considering the concept of cyber-attack surface, three dominant lines of concern and discussion emerged. First, clearly the group felt that dealing with the existing attack surface was very challenging, and in some areas not fully possible to manage. Corporate networks and external systems and partnerships are too big or numerous, distributed, and complex to keep under complete inventory control. Second, the expansion of all traditional types of existing surface area threats. External systems, suppliers and partners, shadow IT and other known issues are proliferating, compounding the management challenge. Third, new types of devices, new use cases, and new networks services challenge the ability of organizations to anticipate and manage further expansion of the surface area.

Like the members of this discussion group, CISOs facing these concerns frequently report a strategic conflict. The most popular approaches to these challenges essentially amount to “doubling down” on current approaches; trying to exert better control on devices and the network, patching better and faster, improving supply chain management, improving design, and simplifying. Yet these approaches are expensive and unsatisfactory today, and the lack of a substantial shift in that reality leaves us trying to reconcile how doing more of the same will produce a different result.

3.3.2 Session 3: CISO Business Concerns

Most important among the concerns discussed are listed in this section.

Hardware: Many CISOs are concerned about the hardware used to power their systems, especially in the wake of the “Meltdown” and “Spectre” vulnerabilities[11] impacting most CPUs. These vulnerabilities cast increasing doubt on the security and reliability of hardware sold by vendors that maintains critical government infrastructure.

IoT: The IoT has opened up a “Pandora’s Box” of new attack surfaces. With more and more appliances and pieces of hardware connecting to the Internet, attack surfaces are appearing everywhere, including smart watches, Closed Circuit Television (CCTV) cameras, refrigerators, etc. Because IoT can be found anywhere, this opens the risk for users who are not well versed in cyber security to cause an unintentional breach into critical systems.

AI Poisoning: The advent of artificial intelligence (AI) is seen by some as a potential new attack surface. For example, could a nefarious actor “poison” an AI algorithm such that it predicts inaccurate results? Could an algorithm be fed bad training data to throw off predictions? This attack surface is very difficult to address, as AI as a practice is relatively new

[11] ttps://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-every-modern-processor-has-unfixable-

and a notable AI “poisoning” attack has not yet taken place. One specific example discussed in the session included adding tape to a stop sign. This tricked an AI algorithm trained to assist with autonomous driving to interpret the stop sign as a speed limit sign, causing the autonomous vehicle to run through the stop sign.

Hardware Supply Chain: Supply chains can introduce many attack surfaces. Two were discussed during the session: hardware and software supply chains. Because many hardware appliances are manufactured overseas, there is a large amount of concern over whether a nefarious actor can infiltrate a link in the supply chain and introduce compromised hardware, which eventually arrives at facilities supporting critical infrastructure. Another way hardware could introduce an attack surface is by authorized personnel acquiring hardware from third-party vendors.

Software Supply Chain: Regarding software, many modern-day applications are built using open-source software, as it is generally cheaper than acquiring proprietary software and typically has a well-establish community supporting the software. Often, when software is built, software “dependencies” (software packages that are used to build other software) are downloaded from common repositories via the Internet. If these repositories ever become compromised, malicious code could make its way into software applications supporting critical infrastructure.

Cloud: Many organizations want to move to the cloud to save on IT cost, increase IT resource elasticity, and incorporate new cloud-based technologies into their systems. However, many organizations do not perform due diligence when it comes to securing their cloud environments. There have been multiple public incidents where sensitive data was stolen from cloud accounts that did not properly secure their data repositories, and left the data wide open to the public.

Users: Perhaps the most difficult attack surface to address, despite the threat being around for a very long time, is common users. Users authorized to access critical systems are prone to make mistakes, including falling for social engineering exploits. Even individuals well versed in proper information security can sometimes fall for social engineering.

There are certainly many more attack surfaces than what were covered during the session; however, the ones covered show how sophisticated and difficult to address some of them could be. The session also showed how some attack surfaces can potentially be in the last place one would ever think to look; even a smart refrigerator (IoT attack surface) could pose as a risk! With this in mind, CISOs must be ever vigilant and continue to search for potential attack surfaces before they are exploited.

3.3.3 Session 3: CISO Business Solutions

The examples discussed show that cyber-attack surfaces continue to emerge as new technologies are developed and adopted by the industry and government. Some experts have compared this satiation to a game of "cat-and-mouse". As mitigations for new attack surfaces are developed more and more attack surfaces emerge and must be addressed. This shows one of the most difficult challenges that CISOs have to face on a daily basis.

The session developed a number of solutions for the six attack surfaces discussed, including:

- Hardware: rapid patching of hardware/firmware, maintaining a proper inventory of hardware (and software) to facilitate quick patching of all assets, and deploying countermeasures to disclosed vulnerabilities.
- IoT: organization policies to manage use of IoT, strict network access control of all devices (including non-IoT devices), restricted access/use of IoT (including barring certain devices from premises), and applying network segmentation to separate users' personal devices from devices intended for work-related use.
- AI poisoning: adding controls to an AI algorithm when it's developed to prevent poisoning, asking earlier in the development lifecycle how the system can be abused (and what steps could be taken to mitigate the threat), and looking into regulating AI to help deter such threats.
- Supply chain: using a private software "artifact" repositories to control software dependencies used, evaluating vendors/companies/contractors (e.g., via questionnaire), and sharing vendor information between organizations to help others select trusted vendors that have previously been vetted.
- Cloud: making content available via APIs static and separated from internal systems, using cloud service provider provided tools to design and build cloud environments (such as the AWS NIST Quickstart template[12]), developing and prototyping open-source applications in the public (so that public developers and help test/review/harden the code base), and introducing a "white-hat" bug bounty program to reward developers financially who confidentially report software bugs before they are taken advantage of.
- Users: automating certain tasks to remove users as an attack surface, providing proper InfoSec education to users, and holding users accountable for negligence.

[12] https://aws.amazon.com/about-aws/whats-new/2016/01/nist-800-53-standardized-architecture-on-the-

Overall, against the backdrop of solutions posed and pending a jump in the efficacy of traditional methods, the consensus was that incremental improvements did offer important value.

3.3.4 Session 3: CISO Business Recommendations

Some solutions discussed are adequate to address the respective attack surface. Others, such as the ones discussed for AI poisoning, are still an unknown as industry and government have yet to experience an attack of significant magnitude from this surface. One thing that is clear: CISOs must take a proactive role in continuing to identify potential attack surfaces, and research potential mitigations before nefarious actors can have a chance to exploit that surface. Every organization and every CISO can find in this list areas needing attention and improvement, and best practice approaches. Some may find their own nicely performing practices are not listed, which is an invitation to share new tactics within the CISO community.

An important point to focus on is that sharing skills, techniques, and methodologies with other CISOs can be a crucial factor in helping the community to prevent attacks. Every CISO can't possibly research and discover every possible attack vector alone; but by leveraging the knowledge and experience of their peers, the CISO community at-large can help to minimize each organization's risk.

3.4 Session 4: Closing the Skills Gap

The demand for cyber security skills in government is unlikely to be met by industry supply for the foreseeable planning horizon. USG is increasingly reliant on millennials who grew up freely sharing everything on the Internet. As a result, today's emerging workforce is potentially less security conscious than those of the past making the insider threat ever more insidious. Approaches to finding talent and handling the insider threat in today's budget constrained business environment were shared and examined.

3.4.1 Session 4: Summary of Discussions

This session featured dialogue about today's Cyber security Skills Gap, giving attention to related mission/business implications, and specific operational challenges that contribute to the Cyber Skills Gap. As part of the session's discussion, associated disciplines were acknowledged as being foundational to cyber security and key to the success of individuals of the cyber security workforce. This session covers notable themes shared.

- Having adequate cyber staff who are well-versed in related, supporting disciplines, work areas, and technologies (e.g., cloud computing [1], mobile computing [2]) that commonly facilitate organizations' mission or business strategies, solutions and operations. Specifically, cloud computing is a highly-desired IT solution and service within the federal space, bearing a considerable security component. Organizations need cyber professionals who are also well trained and knowledgeable in cloud computing, understanding the technology, its capabilities, and impact from a security perspective, highlighting security strengths and shortcomings.

- The need for cyber professionals to be equipped with certain fundamentals and foundational knowledge belonging to or from other disciplines to execute core, mandatory cyber functions. Critical thinking and an understanding of computer science fundamentals or concepts are vital to cyber functions, such as secure software design and development, reverse-engineering, malware analysis, and vulnerability assessments.

- Operational constraints, such as clearances, funding/budgets, and red tap/bureaucracy protocols impact cyber profession recruitment, hiring and staffing efforts, training and awareness needs and/or priorities. Management within the federal cyber space understands the needs, associated demands, and have given thought to ways to address their cyber security needs and challenges, however are unable to execute because of institutional hindrances outside of their control/area of responsibility.

- The lack of competitiveness with the private industry in terms of technology, research and development, agility and ingenuity, diversity, benefits – including salary and growth opportunities. Private industry has far more money than the public sector to consider and institute clever methods and incentives to recruit, acquire, and retain cyber talent. This makes it hard for the federal government to become a serious contender. Highlighting solid retirement benefits and job security just is not enough to attract and successfully recruit young, talented cyber professionals.

- An inadequate number of cyber professionals to fill or satisfy cyber jobs/roles/tasks within various federal organizations. Federal organizations have more cyber jobs than the number of current and available qualified staff to fill the positions. This significantly impacts organizational productivity, job satisfaction (which tightly correlates with employee retention issues), and the ability for organizations to focus on more strategic efforts.

While touchpoint issues to the cyber skills gap problem were raised, and had relevancy with certain organizations more than others, it was very clear that they were not considered the crux of the cyber skills gap problem, but rather, the shortage of cybersecurity professionals with the required skills, background (e.g., work, academic), and credentials being the primary source of the issue.

3.4.2 Session 4: CISO Business Concerns

The cyber security skills gap is a legitimate problem, affecting both federal and private industries. There are simply not enough professionals with the desired, appropriate skills to fill available cyber security-related positions or roles. The high demand for and shortage of cyber security talent combined, create a recruitment and hiring disparity between the federal and private industry. Private industry has far more money to appropriate to effective recruitment strategies that offer certain benefits and incentives most appealing and beneficial to cyber professionals. However, as the high demand for cyber security professionals tapers, cyber job salaries are likely to do the same, lending some level of relief to federal recruitment and hiring of cyber talent.

The cyber security skills gap is a component of a larger challenge – the STEM skills gap. In recent years, STEM education at all learning levels has become a top priority nationwide and with nations abroad to address this skills gap problem. However, in comparison to other technical disciplines, cyber security is still a relatively new one that educators at various levels, particularly college institutions, have been trying to aptly define more concretely. Without a sound understanding of the field, applicable skills, and the types of issues and problem solving associated with this industry, faculty are unable to effectively design and deliver courses and college certificate and degree programs that are relevant, practical, and invaluable to the cyber security field for interested students. Therefore, it is imperative that industry leaders share and partner with academia to form curriculums that help to produce graduates that employers desire – graduates with the right knowledge, skills, and real-world experience.

3.4.3 Session 4: CISO Business Solutions

An array of CISO business solutions were offered and discussed by session participants.

- Continued funding and execution of STEM programs and activities (e.g., challenges, games, robotic competitions). These activities expose children and young adults to the field of cyber security early and allow them to gain related skills in their early years. These types of STEM experiences can influence their decision to major in related subjects in higher education and pursue cyber careers.

- The need for continuing education and training opportunities for current staff or professionals. Organizations need to make ongoing investments in their employees, where employees are provided opportunities to refresh or enhance existing skills and/or obtain new skills within cyber security or touchpoint disciplines (e.g., privacy, enterprise architecture).

- Obtaining higher education/college degree in cyber security or in a related field (e.g., computer science, systems engineering) and/or a security certification (e.g., Computer Information System Security Professional-CISSP). Oftentimes, a college degree and/or certification in a relevant field, along with relevant work experience are strongly desired, if not required for cyber security positions. Having these credentials will afford you an advantage over individuals without them with regards to serious consideration for employment.

- Availability of public (low-cost, accessible) cyber security resources, including books, web-based training, awareness messaging and activities. Not all individuals interested in cyber security careers have the amount of time necessary to take formal training and/or have the funding from employers to sponsor their training. Public cyber resources provide these individuals an alternate way to ascertaining key cyber skills at a pace and cost more suitable and flexible to their individual circumstances.

- Outsourcing all or larger portions of the cyber function within organizations. If federal organizations lack the necessary funding needed to acquire the latest technology, as well as hire and retain high-caliber cyber talent/resources, largely or fully outsourcing cyber functions within the federal space address this dilemma. Outsourcing to private industry (where there's a large pool of talented cyber professionals, more money, and less bureaucracy to acquire technology, conduct research, and develop solutions) would bring greater efficiency to federal cyber security operations.

- Augment recruiting techniques and measures in a way that more effectively targets and incentivizes the millennial and Gen Z workforce to federal government cyber careers. Consider and institute clever ways to attract, hire and retain cyber talent, particularly young cyber talent, as they are the future federal leaders and officials. Examples included travel opportunities and inter-agency rotational programs.

While most solutions shared involved furthering efforts in cyber skills learning and training, there were a couple of solutions (i.e., creative and attractive recruiting methods, expansive outsourcing) that reflected the group's willingness and ability to think creatively and out-of-the-box to address a difficult problem, deemed a mission and business hindrance.

3.4.4 Session 4: CISO Business Recommendations

STEM education needs to remain a national priority, supported by state and federal government as well as private industry and academia. The standing incorporation of STEM education in school curriculums, as well as STEM extracurricular clubs and activities, such as Capture the Flag, code.org, and robotic competitions, help to expose and stimulate interest in children and young adults to STEM careers early, as well as allow them to gain understanding of key principles and skills critical to STEM professions. Further, tailoring the delivery of STEM education to reach female and male students of varying backgrounds is paramount for ensuring students' enthusiasm about the subject and effective comprehension of the lessons.

Higher education – degree and certificate programs, as well as professional certifications, based on cyber security or a related discipline, undoubtedly provides greater access and possibility to a career in cyber than the absence of it. Today, most employers require it, and will make exceptions only in times where candidates have rich experience in a specialized skill or domain expertise, critical to their current business needs and goals.

In some cases, the cyber security skills gap issue is organizational, mission-specific, and/or operational-specific and, therefore, should be individually evaluated and addressed accordingly. To this point, major cyber priorities of one organization might rank entirely different in other organizations. Another example of this point is that certain skills might be classified highly specialized in certain companies, while in others, deemed standard or expected. That said, there will be more standardized approaches to the cyber skills gap when concerning students/professionals with cyber career goals than organizations tackling their unique cyber skills gap challenges.

The federal government is lending serious consideration to outsourcing a large portion or its entire cyber function/capability should only be entertained under very few, defined, temporary, unlikely, but possible circumstances, if any. Doing so would create too much private-sector influence and power, diminishing real oversight, ideals of checks-and-balances, and solid representation of the public-service perspective in the cyber security field. Additionally, it would greatly stifle, if not remove federal innovation and forward thinking within the cyber security domain.

Continued cyber skills learning and training opportunities are truly critical to solving the cyber skills gap issue. Stakeholder groups who can affect change in this area most, are involved. And this is noble. However, these groups should carefully review and refine their contributions, on a standing basis, to ensure that the contributions are clearly aligned to their organization's objectives and activities. This approach ensures a substantive gain for not only trainees and students, but for stakeholder groups too, as their time, money, and resources (materials, instructors, mentors) are often dedicated.

3.5 Session 5: Security Challenges with IoT and Other Emerging Technologies

On the forefront: IoT and other emerging technologies touting greater connectivity, increased functionality, and broader resource sharing. Strategies for defining policy and technical solutions to IoT device management were identified and discussed. Governance models for addressing the changing technology and security landscape were shared and examined.

3.5.1 Session 5: Summary of Discussions

The group focused discussion on IoT with some discussion on emerging technologies, such as cloud services and big data analytics. Several IoT topics aligned with common themes.

- Mismatch of consumer expectations and enterprise use of devices. Examples surfaced were enterprise security policies that prohibit use of devices in secure facilities, as well as emerging devices that are not embraced or implemented by an enterprise. The value model of both sides need to be understood.

- Understanding or expressing risk decisions with IoT devices, including analysis of tradeoffs, vetting and approving devices, and greater automation of device security evaluations. Person and enterprise risks were discussed, including supply chain. Challenges with supply chain risk management include tracking and validating origin of components (e.g., firmware) that make up devices.

- Governance and security controls are needed to ensure that data is adequately protected, whether data is on the device, transmitted, or stored in the cloud. A data-centric approach for IoT is critical.

- Need for both pre- and post-market security controls for IoT devices (e.g., requirements for procurement language).

- Need help prioritizing which devices to focus on with enterprise. Organizations may already be doing risk assessments on devices before they are deployed, but don't have the resources to handle scale of IoT (e.g., every light bulb comes with a chip and wireless connection).

Most of group discussion focused on workforce and security challenges with approving and implementing IoT devices (things) within the enterprise. Analysis and expression of tradeoffs between security, functionality, and business efficiencies need to be clearly understood across multiple stakeholders. This includes sharing security assessments, trade studies, best practice guidance, and common use cases across the Federal government.

3.5.2 Session 5: CISO Business Concerns

IoT challenges, such as security, privacy, and interoperability, will continue for the next several years due to maturity of standards and implementations across a variety of sectors. However, recent progress has been made with understanding IoT lexicon, use cases, considerations, and typical architectures. Several consortiums are addressing security for frameworks, checklists, devices, protocols, reference/solution architectures, and testbeds. Areas for continued development include device software and hardware security, network security, management and monitoring security, Identity and Access Management (IdAM), cyber resiliency, privacy, and safety. The opportunity is now for “Baking In” security vs. “Bolting It On” later.

Though progress is being made, currently the burden of security is very much on the end user/implementers as many IoT developers eschew expensive security controls for more marketable features and functionality. Organizations deploying IoT devices need to educate themselves on the new risks realized by the addition of sensors and actuators into their IT infrastructure to include cyber-physical systems (CPS).

3.5.3 Session 5: CISO Business Solutions

The group discussed several general solutions associated with major themes above. These included

- Understanding value proposition between consumer expectations and enterprise use of devices. This includes embracing technologies used by the young workforce and updating organizational policies with vetting and approving new technologies.

- Assessing IoT risks will be aided by understanding elements of ecosystem and identifying threats with associated mitigations. This includes analysis of residual risks for consumer (i.e., person) and the enterprise. Analysis of end-to-end data flows are also critical. Risk scores based on modeling, analytics, and behavior were discussed. Guidance on tradeoffs between functionality and security should be developed. Additional solutions discussed included:

  - Independent evaluations of devices (e.g., NIAP[13], Underwriters Lab (UL)[14], nutritional label) by organization to determine level of trust for devices.
  - Device security capabilities, such as hardware/software security controls, code signing, software ID tag, Network Admission Control (NAC), and controlling degrees of functionality.

- A data-centric strategy is important for IoT, including threat modeling. This includes ensuring confidentiality, integrity, availability, and privacy of data, including use of network segmentation for added isolation of devices/data.

- Though IoT devices present new challenges, organizations can implement mitigations for IoT risk now with some basic security hygiene, such as device hardening, network segmentation, and flow control.

A key theme from group was needing to understand how IoT devices (things) fit in a broader ecosystem context, including the components and services that make up and support the end-to-end architecture and associated data flows. An important topic was security and privacy of data since IoT involves processing, storage, and movement of data in multiple locations. This may include use of segmentation approaches for added isolation and separation of critical functions and sensitive data.

3.5.4 Session 5: CISO Business Recommendations

Organizations need to anticipate the technology needs of emerging workforce and how range of devices can be used to support a variety of business and mission services. A typical consumer may own several devices, such as smartphone, smartwatch, fitness tracker, and medical device. Organizations will need a strategy to assess risks of permitting the growing number of devices within an enterprise by ensuring proper balance between security, functionality, and productivity.

Assessing risks for IoT begins with understanding end-to-end architecture, intended use cases, types of devices, sensitivity of data, and identification of threats. This includes

[13] https://www.niap-ccevs.org/

[14] https://www.ul.com/

security for device itself, device-to-device, device to gateway, and device to cloud/data center communications. Data security must be addressed at-rest and in-transit within the end-to-end architecture. This type of analysis would be aided by best practice examples, security frameworks, and threat modeling tools. A benefit of device evaluations is evidence for meeting security requirements and standards, including expression on security controls supported by device and how the device should be used in intended environment. For example, the development of Manufacturers Usage Description (MUD) Specifications will benefit understanding of types of access and functionality required for device to properly function.

A data-centric approach for IoT is critical since data is collected, aggregated, transmitted, and stored in multiple locations in the IoT ecosystem. This includes endpoint, communications, configuration, and monitoring data protection spanning IT, mobile and cloud infrastructures. This strategy also aligns with emerging protection strategies, such as adaptive security and Zero Trust model, where specific focus is ensuring that access to sensitive data is protected end-to-end by authorized user/device from any location and variety of contexts.

Next step collaboration opportunities include:

- Analysis and recommendations for inclusion of IoT devices with Continuous Diagnostics and Mitigation (CDM). Continued analysis and demonstrations of best practice examples for IoT (e.g., National Cybersecurity Center of Excellence-NCCOE).
- Application of threat and risk modeling tools for IoT architectures.
- Sharing of IoT trade studies, device evaluations, and implementation examples across the Federal government. For example, in February 2018, NIST released draft NISTIR 8200 Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)[15], Interagency Report on Status of International Cyber Security Standardization for the IoT. This report provides useful information on cyber security areas, risks, and standards landscape for IoT.
- Practical guidance for addressing consumer vs. enterprise expectations for IoT.

In summary, the next steps reinforced the need for sharing of trade studies, device evaluations, best practice guidance, and threat modeling for IoT. Continued sharing and awareness of IoT activities across the Federal government will minimize duplication of efforts and maximize efficiency of applied resources. This includes development of use cases and design

[15] https://csrc.nist.gov/publications/detail/nistir/8200/draft

patterns for integrating IoT devices within evolving enterprise architectures to support IT modernization and cybersecurity requirements.

4 Conclusions and Summit Recommendations

Drawing from the discussion and content generated during the Collaboration Sessions, MITRE and ATARC developed several key overarching recommendations:

Industry and government must collaborate in developing comprehensive training for responsible government actors encompassing the nature of industry (especially vendor and critical infrastructure), the role played by ICT, the risks posed by cyber threats, and the capacity of each community to develop, deploy, and mature effective security measures. This training is an essential continuing precondition to other changes in the relationships between the government customer and its technology vendors, including more candid and continuing relationships prior to, during and after the ICT acquisition process, as well as continuing operational collaborations between agency and vendor security professionals, up to and including the CISO level.

Achieving an environment to assure such effective, actionable industry-government collaborations now and in the face of future cyber challenges may well require legal and policy measures which do not presently exist. Consideration of comprehensive national cyber legislation with more than cosmetic effect is clearly appropriate.

Security metrics should be presented to top agency leaders in terms of mission impact for them to make informed mission-based decisions. However, the skills required to produce business-based reports relies on a highly specialized and expensive mix of skills (cyber knowledge, big data analysis, and business intelligence). While AI will eventually help to bridge this “people skills” gap in the future, agencies who cannot leverage their existing big data analysis/business intelligence teams should partner with agencies of similar size and risk profile who do have these resources available.

CISOs facing these concerns frequently report a strategic conflict. Popular “solutions” essentially amount to “doubling down” on current approaches; trying to exert better control on devices and the network, patching better and faster, improving supply chain management, improving design, simplifying. Yet these approaches are expensive and unsatisfactory today, and the lack of a substantial shift in that reality leaves us trying to reconcile how doing more of the same will produce a different result. A consensus view is that CISOs must do what they can to manage the problem with current approaches, while hoping that a more comprehensive and effective approach will be developed in the future.

The need to grow and develop the Cybersecurity workforce is evident. Measures that relevant industry sectors have taken to-date have shown to deliver fruitful and positive outcomes. Therefore, it is recommended to continue with these initiatives, enhancing them with appropriate rigor and tailoring. Effectively satisfying this objective will require active and solid collaboration and knowledge sharing between industry sectors, particularly partnerships cultivated between academia and cyber industry sectors – government and private.

Assessing IoT risks will be aided by understanding elements of ecosystem and identifying threats and mitigations. This includes analysis of end-to-end architecture and residual risks for consumer (person) and the enterprise. This analysis would benefit from best practice examples, device evaluations, security frameworks, and threat modeling tools. Device evaluations would provide evidence for meeting security requirements and standards, including how the device should be used in intended environments. A data-centric approach for IoT is critical since data is collected, aggregated, transmitted, and stored in multiple locations in IoT ecosystem (e.g., devices, gateways, edge, cloud, and backend applications/services).

ACKNOWLEDGMENTS

The authors of this paper would like to thank The Advanced Technology Academic Research Center and The MITRE Corporation for their support and organization of the summit. The authors would also like to thank the session leads and participants that helped make the collaborations and discussions possible. A full participant list is maintained and published by ATARC on the FedSummits web site[16]. A special thanks goes to Adewale Omoniyi (IBM) and Bill Fisher (NIST) for their contribution the Session 5 write-up.

REFERENCES

[1] J. F. Brunelle, S. Anand, G. Barmine, M. Spina, K. Warren, A. Winston, M. Javid, A. Kemmer, C. Kim, S. Masoud, T. Harvey, and T. Suder. August 2017 federal cloud & data center summit summary. Technical Report 17-3231-2, The MITRE Corporation; The Advanced Technology Academic Research Center, 2017.

[16] https://www.fedsummits.com/ciso/

[2] C. McRae, P. Benito, C. Brown, D. Keppler, J. Stein, K. Boston, C. Rieser, J. F. Brunelle, T. Suder, and T. Harvey. October 2017 federal mobile technology summit report. Technical Report 17-3231-5, The MITRE Corporation; The Advanced Technology Academic Research Center, 2018.

[3] The MITRE Corporation. FFRDCs – A Primer. `http://www.mitre.org/sites/default/files/publications/ffrdc-primer-april-2015.pdf`, 2015.