EXECUTIVE SUMMARY

Cyber Resilience Summit: Securing Systems inside the Perimeter

Topic: Improving System Development & Sustainment Outcomes with Software Quality and Risk Measurement Standards

Hosted by: Consortium for IT Software Quality (CISQ) in cooperation with Object Management Group and IT Acquisition Advisory Council

Date: March 21, 2017, 8:00am – 12:30pm

Location: Hyatt Reston Town Center, 1800 Presidents Street, Reston, VA

Agenda and Presentations: http://it-cisq.org/cyber-resilience-summit-2017

Event Background

As the journey to secure our nation's IT cyber infrastructure gains momentum, it is important to apply proven standards and methodologies that reduce risk and help us meet objectives for acquiring, developing and sustaining secure and reliable software-intensive systems. The theme of the March 21 Cyber Resilience Summit is *Securing Systems inside the Perimeter*. Defending the network is NOT enough. The most damaging of system failures and security breaches are caused by vulnerabilities lurking inside the network at the application layer. Discussion topics: Meeting assurance-driven objectives, digital transformation, cyber risk measurement at scale, risk-managed evolution and practical application of systems engineering to support cloud readiness, big data, technical debt control.

Meeting Notes

Thank you to ANSER (anser.org) for drafting meeting notes.

Welcome and Introductions delivered by:

- Dr. Bill Curtis, Executive Director, Consortium for IT Software Quality
- John Weiler, Vice Chair, IT Acquisition Advisory Council
- Marc Jones, Director of Public Sector Outreach, Consortium for IT Software Quality
- Don Davidson, Chief, Lifecycle Risk Management & Cybersecurity/Acquisition, U.S. Department of Defense

Keynote: Dr. Dale Meyerrose: Major General, US Air Force, and CIO and Information Sharing Executive for DNI

"What's Holding Us Back?"

- Defending inside the perimeter has multiple aspects to it, but fundamentally: we're dishonest.
- Cybersecurity industry, both industry and government, doesn't really address cybersecurity vulnerabilities. 14 research studies show the vast majority of cyber-security attacks occur from the inside. Insider behavior accounts for 90% of all attacks and hacks. Of 12 most major healthcare attacks, 7 were from lost laptop or hard-drive.

- There is a lot of misinformation about cybersecurity, and myths abound. Most cyber-attacks are not sophisticated. 40% of breaches occur through phishing e-mail. Social engineering is still a major method of attack.
- Today's cybersecurity industry ignores the "cyber-attack chain" – stuck in the "signature-based 'mentality' rut of intrusion detection."
- We also aren't honest about our ability to prevent: in reality, it takes about 256 days to detect infiltration, and 90-120 days to remediate (CIOs say 60 days for infiltration, 30 to remediate). The United States government is one of the worst industries for detecting and stopping intrusions.
- Cybersecurity is not a goal in and of itself, it primarily serves the broader objective of securing the enterprise. Thus, cybersecurity is what you do – not what you buy.
- Cybersecurity – and security generally – tends to be highly reactive, not proactive. Lots of sitting around waiting for things to work.
- Big data isn't important, big analysis is important.
- Most organizations don't encrypt data (around 60%).
- Industry is not helpless, there is lot that can be done. Needs the right leadership and needs to tell the right story.
- Two critical items: continuous assessment and resilience.
- Any security person who talks about "restore" should be fired, because they're worthless. If you restore it, you're in the same condition you were in the first time. When you come back online, you want to be better.
- "The GAO attributes the problems with IT programs to '…a lack of disciplined and effective management and inadequate executive-level oversight.'"
- Biggest shock in leaving government: when we contracted with someone, we became a partner.
- IT acquisition focused on process not programmatic success.
- Adversarial relationships start early – persist and never go away; >85% of USG IT initiatives fail to meet budget and timeline – many never come online.
- Cyber/IT drivers for the next decade: Scarcity of talent will grow worse; Expanding digitization of data/info and virtualization of infrastructure will accelerate; Technology-based social networking continually will continually re-define access, crime, law, liability, opportunity, & privacy.
- Security is about protecting the value in the organization: its assets, objects, activities, people, and data.

Dr. Dale Meyerrose keynote

Dr. Bill Curtis: Executive Director, Consortium for IT Software Quality

“Advances in Measuring the Security and Architectural Integrity of Mission-Critical Systems”

- Why measure IT Applications? Bad software is insecure software.
- “Six digit defects” now affect CEOs, board of directors, etc.
- Auditors don’t have anything they can grab ahold of.
- CISQ’s charter is to define automatable measures of software size and quality that can be measured in the source code, and promote them to become standards. (OMG, ISO standards bodies)
- Study of structural quality measures and maintenance effort across 20 customers in a large global system integrator – showed a .24 TQI increase dropped costs 50% on corrective maintenance.
- CISQ structural quality measures developed by looking at specific problems in the code – security, reliability, performance efficiency, and maintainability. Violations contained in standard must be fixed.
- Modern applications are a technology stack: 1) unit level – code style & layout; 2) Technology level – single language / technology layer; 3) System level – integration quality, architectural compliances
- Standard measures help with Service Level Agreements. If it’s customer facing, can assist with accountability. Metrics can be used to monitor progress overtime – technical code quality, overall quality, and cost-effectiveness.
- CISQ’s roadmap includes embedded software, Internet of Things, and software supply chain.

Panel Discussion: Modernizing and Security Legacy IT

Lead: John Weiler, Vice Chair, IT Acquisition Advisory Council

Speakers:

- **Dr. Mitch Crosswait**, Deputy Director, Net Centric and Missile Defense Systems, Operational Test and Evaluation, U.S. Department of Defense
- **Dr. J. Brian Hall**, Acting Deputy Assistant Secretary of Defense for Developmental Test and Evaluation
- **Jason Hess**, Chief, Cloud Security, Office of the Chief Information Officer (OCIO), National Geospatial-Intelligence Agency
- **David McKeown**, GS-15, CISSP, Chief, Cyber Security Center, Joint Service Provider, DISA
- **Tony Davis**, Acting Command Acquisition Executive, USCYBERCOM

Modernizing and Securing Legacy IT panel

Theme: Security Requirements

- Threats to stand against (what threats should be resisted to preserve being able to execute the mission)
- How it should start to fail to allow continued mission performance (specifically, acceptable degradation when suffering damage from an attack to allow some mission capability)
- What needs protecting to accomplish the mission? How well should it be protected?

Dr. J. Brian Hall:

- Oversees major defense programs, identifying what works well and what does not. What you test and evaluate in OT is different than DT. Looking at performance problems, interoperability, and cybersecurity vulnerabilities.
- Several initiatives to improve DOD posture: many cybersecurity vulnerabilities identified late in the process. Many programs don't start testing during development, because no policy for defense programs to start testing for cybersecurity in DT. Problem is: setting JCIDS requirement, establishing implementation guidance, developing workforce, test cybersecurity, and validation methodology.
- Overview of cybersecurity efforts. Requirements: Joint Staff updated System Survivability Key Performance Parameters to include cybersecurity; first real cybersecurity requirement for major defense programs. Requirements need to translate into contract requirements, so that cybersecurity is incorporated at program inception. Guidance material: DOD test and evaluation guidebook on six-phase Cybersecurity T&E process, will update at end of year. DOD CIO with US Acquisition published cybersecurity guidebook on integrating risk management process. Joint staff released cyber implementation guide in establishing requirements. Defense Acquisition guidebook updated to include six-step cybersecurity teaming process.
- As far as training, serve as career field manager. Update, approve, and certify T&E course. Updated test 204 and 303 classes on cyber-teaming process. Initiated series of cyber training table-top exercises (4 or 5), training 100. Nine additional table-tops planned.
- Quarterly cross-service cyber-teaming with SLAAD at white sands missile range. In policy, updated DOD 5000 (DOD acquisition regulation instruction) including some risk management framework and parts of six-phase cybersecurity. DOD programs funded to requirements.
- Making investments in test infrastructure by expanding national cyber-range, increasing fidelity of major defense programs cybersecurity, establishing test resource management center, and Army as executive agent for cyber-training ranges. Established FY17 PALM initiative to executive cybersecurity T&E events. Have pot of money to help programs fund cybersecurity.

Dr. Mitch Crosswait:

- Does major testing on all acquisition programs before they hit the field. Almost all programs (minus one) have a cybersecurity component. We do operational testing and assess live networks (combatant command networks), including global command and control (top operating level). System can change a lot when in the field – could get better if combatant commander understands and supports cybersecurity, or could get worse. Cybersecurity testing provides assessment on current cybersecurity posture, as it could change the next day.
- Writes an annual report to Congress. Last year's (2016) report noted: We're better at operational defense of system and networks, because of increased focus on cybersecurity. Many critical missions remain vulnerable to cyber-attacks. Same problems in commercial happen in military: lack of role-based privileges, data encryption, centralized logging, understanding network activity, Share Point and chatrooms may be left wide-open.
- We go out and assess networks live and seen marked improvements. First time, red teams could not crack the networks. Combatant command networks were not perfect, so not appropriate to try for perfection. Red team will always get in – the goal is to prevent them from getting access to main information (if really great, create watering hole to think they're in). Most sophisticated defenders will let red team get in, then watch and manipulate.
- Bottom-line: Need to fight through cyber, need to practice, fight through, COOP planning. Need to invest in cyber-test infrastructure. Improve test environment.

David McKeown:

- I am a defender of the Pentagon's network, which is key terrain. Have active defenders doing end-point defense. Joint service provider an experiment to provide common IT for the customer base. Goal: Become single IT provider in the Pentagon. See lots of initiatives colliding at the same time: mandates to consolidate data centers, move to the cloud, and modernize. All have inertia to stop them from moving – having oceans of code to examine on any given app. It takes time to mature security on those systems.

- For a long time operations and functionality won out. We did not tolerate slow-downs, security took a backseat. However, we're more focused now: POTUS and SECDEF put more emphasis on security.
- Need to hire new staff to look at code, reverse engineer what it does, requirements, and see how to migrate somewhere else and get it to work.
- Funding is a huge issue. Need to show that these issues are being worked into five year funding planning.

Tony Davis:

- Spent last few years getting into agile acquisition. Culture in SOCOM means almost no legacy systems in command, because very operationally-focused. Willing to take 70-80% solution and adopt (COTS) + some vulnerability testing. Across SOCOM portfolio, although smaller in scope, share lessons learned across the many organizations. Way too much oversight for anything above Cat-3.
- Important to be aware of risks, but important to do so without all the oversight. Delegation is also important: two programs bigger than Cat-3. An O-6 is decision authority. Willingness to accept risk also a big issue. At CYBERCOM to start up acquisition program. Having many conversations on spectrum of risk – low to high – and can make decisions about how much risk to assume that turn into time, cost, and other programmatic decisions.

Jason Hess:

- Two years ago, NGA moved to shift everything to cloud and tried to reinvent how to do security. Leveraging RMF flexibility. Building a vision to get an ATO in a day, using software and DevOps. Fully embraced DevOps culture, integrating full DevOps process. Doing security testing up front. Closest to 1 day is 7 days, but that's still a huge (10x) improvement.
- Systems need to be developed to tear-down and rebuild in hours, not decades. Repaving entire environment every day, giving attackers only a few minutes to mess around.

John Weiler: What do we need to do to improve the policies?

- **Dr. Mitch Crosswait:** Change culture in DOD from cybersecurity being administrative back-office to a war-fighting function. Places with good cybersecurity talk like soldiers not network admins.
- **David McKeown:** Agree with Mitch. Cybersecurity center's main purpose is security. On operational and engineering side, have mixed priorities with security not #1. Need to change priorities through training and making them part of Cybersecurity team, to show that Cybersecurity is a team sport.
- **Jason Hess:** Cybersecurity needs to be part of the mission, not the other way around. Understand the risks for not providing timely information. Need to make sure we're acquiring quality tech and providing leadership to make it effective.
- **Tony Davis:** Biggest thing is to understand the limits of toolsets we use to do IT acquisition. At SOCOM, try to understand every vehicle and its limits – how far we can push it. Getting additional authorities from Congress, but in law, only given to DARPA and services. Have to go to OSD to delegate authority. Spent 1.5 years on regular OSD cloud process, but ended up going to .com because we couldn't get on gov cloud for purpose desired. Need to find how to share better – lots of people doing things in small groups, but no good way to share widely.
- **Dr. J. Brian Hall:** Cyber needs to be considered war-fighting domain. Major defense programs will always have cost and schedule pressure. Recent system went to field without pen-testing

Question for Tony Davis: You mentioned being proactive, how do you execute and use programs without getting into trouble?

- **Tony Davis:** Educated risk – talk to Intelligence Community about threat, and Ops community about how they're going to implement. Take things out to field in limited risk environments. Need to take practical steps to manage.

Question: As a practicing systems engineer, how are you going to fashion a cyber-security requirement?

- **Dr. J. Brian Hall:** Best answers come from requirements developers. First piece starts with requirements – without a requirement, the project manager doesn't get funding - no contract - doesn't inform design.

- **Dr. Mitch Crosswait:** Need to incorporate cybersecurity into mission requirements (i.e., if cyber-attack occurs, how does that reduce mission?) Goes back to cyber-defenders. Need red-teaming to identify gaps.
- **Dr. J. Brian Hall:** Never going to be a panacea.
- **John Weiler:** That's where standards bodies help.

Dr. Ben Calloni, co-chair of the OMG's Systems Assurance Task Force

- Inter-relationships of assurance: Systems assurance, information assurance, software assurance, and safety assurance all support mission assurance. Without a baseline of product quality, assurance is impossible.
- Biggest insider threat: People don't know how to build good software.
- All invited to March 21 afternoon OMG Cybersecurity Workshop, 1:30pm – 6:00pm.

Panel Discussion: Titans of Cyber: Critical Insights from the Front Lines of the Cyber Risk Management Battle

Lead: Don Davidson, Chief, Lifecycle Risk Management & Cybersecurity/Acquisition, U.S. Department of Defense

Speakers:

- **Dr. Ray Letteer**, Chief, Cyber Security Division, U.S. Marine Corps
- **Dr. Ron Ross**, Fellow, National Institute of Standards and Technology (NIST)
- **Dr. Barry Horowitz**, Professor and Dept. Chair of Systems Engineering, University of Virginia
- **Rod Turk**, Acting CIO, U.S. Department of Commerce
- **Danny Toler**, Deputy Assistant Secretary, CS&C, NPPD, U.S. Department of Homeland Security

Titan of Cyber panel

Rod Turk:

- Commerce has 12 components, a highly federated environment with broad functionality. Responsibilities range from bottom of ocean to the sun. Implement NIST standards. Therefore, very decentralized and each component has a CISO. Heavily involved with outsourcing and consolidation – moving towards consolidation. Cybersecurity without security operating centers. Security operation is moving to Fairmont to be layered on NOAA's system.

- Stack of cybersecurity tools already there. Seeking to integrate security operations to provide enterprise picture for Sec. Commerce. (Working on this as we speak). Involved in continuous diagnostics and mitigation, doing pilot for phase 1. Federated nature causes problems; getting everyone moving in the same direction.
- One of the first enterprise services in Commerce has broken the paradigm of federated structure towards common solution-set. Hoping it pays dividends on building culture going first.
- Don't want my whole office to be Cybersecurity PhDs, because then you get lots of Cybersecurity science projects but not much ability to present it right to CFO on why I need program. Need well-rounded professional to present in a cogent way.

Danny Toler:

- Easier to talk about what we're not doing in cybersecurity. We are doing: EINSTEIN outside of parameter of departments and agencies split into a few different areas. EINSTEIN-1 net-flow information, E-2: intrusion detection (suspected bad things), and E-3: known-bads and e-mail scrubbing. Also offer US-CERT, part of NCCIC 24/7-365 cyber operations center, taking calls from agencies, CI, state, local, and tribal. CERT looks at cyber-physical connection. Industrial control systems looking at vulnerabilities and how to mitigate them. Offer red and blue team services to departments, agencies, critical infrastructure, state, local, etc.
- Experts attempt to get in and what you need to do to keep them out. CDM breaking paradigms - first program of centrally-funded to deploy tools to departments and agencies with staffing support to make it happen.
- Assume the perimeter is breached. Critical part is having a defined infrastructure with defined gaps. Want to focus scarce resource on fixing the worst first. We are focused on what to do to move into the future. Not ignoring cloud or mobile; have not fully addressed from cybersecurity standpoint.
- Looking at Trusted-Internet Connection and how that can morph into the future. Also seeking to operationalize work at NIST – programs that embrace cyber framework.

Dr. Ron Ross:

- Need to have a tough discussion; we're spending more and doing more (for cybersecurity) but failures continue to plague us. Problem: we think of cybersecurity in terms of kinetic terms, but cybersecurity is different. A whole world we have not addressed yet. Pay attention to what Jason Hess (NGA) said – churn the infrastructure fast. These are things you can address as consumers – patch system, configure, do inventories – but these are above the waterline. Need to look below the waterline to where adversaries operate. Look at system stack from software to middleware to hardware.
- Two Defense science reports: military 2013 cyber resilience and another for DOD on cyber resiliency. Reports talk about vulnerabilities. Three levels: 1: Known, 2: Zero-days (unknown), and 3: Adversary-created new vulnerabilities that can be exploited later. Zero-days and adversary-created are off the radar and not captured in current tools. Building the most complex infrastructure ever. Need good engineering and architecture.
- Big appetite for innovation. In OPM, attackers were in system for a long period. Folks stealing documentation and innovation regularly (i.e., theft of F-35 plans). This is a slow-bleed.
- In publication now is great guidance on how to integrate system security into the engineering process (IEEE and ISO standard). Security requirements do not pop up at the end, but are integral from the start. Tools are out there to bring this into the lifecycle process to stop issues at the front door and limit the damage. Want to limit the time on target – in the case of OPM, may only get 500 records vs. several million. We need to do more.

Dr. Barry Horowitz:

- Led research effort on physical systems for DOD. Physical systems have finite physical states. If waypoint on UAV is changed, there should be a change in the communication system. If not, there may be a cyber issue. Therefore, look at whether doctrine and system are consistent.
- Ran live tests and showed we could detect attacks. Did 3D printers monitoring temperature controls, location of part in the machine, monitoring materials, cars. Theme is dual-knowledge: not many know about both cyber and physical issues.

- Services disagree about where they want (and if they want) humans in the loop. Ran an experiment in AF base, found that delays occur in search for other information. Securing monitor for UAV needs to be very secure. UAV experiments built software three times.
- Need to keep scale under control to take advantage of tools. Army working with us (University of Virginia) on weapons system and embedding into design.

Dr. Ray Letteer:

- My mission: How can I be assured I can get the information to the warfighter so they can accomplish their goal when they need to? May get a call at the last minute, hundreds of miles away, and need current information protected without compromise so they can act on it. I am responsible for what needs to be done.
- Cyber is three things: connection (what am I connecting with?), communications, and cognizance. This is our hardware, software, and firmware problems. So, what is the real issue? Humans. We can't seem to follow-through. "Let's just check to make sure we got it right."
- I don't understand how to get people to understand their responsibilities and accountability: what happened with OMB? Where is the accountability? If I do something wrong because I messed up, I'm held accountable from leadership. PM says cost, schedule, performance, but operator says threat vulnerability and consequence. So, mixed up lexicon.
- Must get in to address aggressively. Automate, automate, automate. Working with DOD: NIC isolates before you're plugged in so updates are pushed as needed. Therefore, humans don't need to get involved.
- Command and Control is big for us and that's done on information technology. Marine Corps enterprise services in KC. At department, building service in. Based on Cybersecurity 1253 standard.

Question: Where is education? We can't hold people accountable without the basics, including senior leaders.

- **Dr. Barry Horowitz:** We (University of Virginia) started a technology leaders program to expose folks to mechanical and systems engineering. Many departments don't want to make it a mainstay; pressure is to get degree faster for less.
- **Danny Toler:** We're very concerned about training and education of our workforce. Incentivize people to gain professional certs that are relevant and timely. Through blue team, educate on threats. Also focused on using expertise to inform on an ongoing basis.
- **Rod Turk:** Education is important, but only a piece. Problem is you can train once a year or so, but if they forget for a small moment, they'll click on something. Put posters on the wall, announce it, and demonstrate what to look for. Be proactive when events likely to occur. Before traveling, expect phishing e-mails to come in ~30 days in advance.

Question: Confusing terminology often emerges; a lot of people don't know what Cyber Resilience means. Is it part of cybersecurity, subset, superset?

- **Ron Ross:** Subset of resiliency. We're witnessing a massive convergence of physical and cyber systems. Need to look in context of system – each element has different level of trustworthiness. Collection of components gives a sense of system trustworthiness. Need to limit vulnerability. Resilience means still functioning in a weakened state. Cybersecurity is a property of the system, like safety. In cars and other systems, safety equipment is built into the system (i.e., NASCAR).

Question: How do we develop talent when universities refuse to teach the courses?

- **Dr. Ray Letteer:** Where are we building the training processes? Seem to have lost how to adapt into standard training program. Let's go back to vocational model. We start attaching folks to train – work as journeymen to learn the basics. Go back to vocational model: bring you in and show you how to do these things.

Barry Snyder, DevOps Manager, AD&M Development Services, Fannie Mae

"**Use Case: Putting CISQ Standards into Action at Agile Speed"**

- Fannie Mae’s main mission: make housing affordable; bundle loans into securities sold to investors. Overseen by FHFA as a Government Sponsored Entity (GSE) blending characteristics of government and commercial. Governance is a part of our organization.
- Strategic initiatives: shift in culture, enterprise simplification, change how we build software – DevOps, supply chain, monitor & measure
- Executives meeting with Amazon, Google. Reading about the Phoenix project (good starting point on DevOps). DevOps became clarion call for shifting organization.
- DevOps is a journey; doesn’t happen overnight.
- Baked in code quality, reflected in quality of applications. Seen a 30-48% increase in quality and some even higher, because now continuous improvement is part of the DNA in quality.
- Through metrics on code quality, can empower team to improve performance.

Curtis Dukes, Executive Vice President, Center for Internet Security

The Value of Security Benchmarks and Controls

- Center for Internet Security (CIS) now home to Top 20 critical security controls. Developed cybersecurity architecture review for SIPRNet, etc. to look at what actors want to do and what can be done for prevention.
- Still have big problem above the waterline. Vast majority of problems are because of known solutions. At NSA, did incident response for OPM and commercial. In all breaches, adversaries got through phishing attack, few use “stealth” attacks. Should concentrate on five basic defenses.
- About the only improvement on phishing attacks is improving grammar and spelling mistakes, but still highly effective. For all the training, someone is still going to click on link or attachment (they may be stressed; about to leave for a trip and not thinking).
- Few defenders have automated workflow, increasing complexity.
- 15,000 cases worked by Cyber Defense Operations Center; 80-90% of incidents could have prevented by patching vulnerabilities, removing admin privileges, and using strong passwords or multi-factor authentication.
- “The Fog of More” – each framework or standard has unique management interface and console. Challenge to manage the information and take action on it.
- Defender’s Dilemma: What’s the right thing to do, and how much do I need to do? How do I actually do it? How can I demonstrate to others that I have done the right thing?
- C-suite keeps asking how to demonstrate they’re doing due diligence. Almost all fortune 500 companies now have cyber insurance. Gap is: criteria used to underwrite cyber insurance policies.
- Focus on the first six controls:
  1. Know what you’re protecting: used to ask companies to list out what assets they have. Many couldn’t do it. How can you protect a network if you don’t know what you have?
  2. Define secure configuration baseline: have tools to demonstrate compliance against benchmarks.
  3. Continuously monitor vulnerability of resources.
  4. Limit and monitor administrative privileges: adversary goal is to go from local access to root access. Not enough attention to who needs admin privileges.
  5. Continuous monitoring / situational awareness: looking at logs for signs of potential ripples in network.
  6. With these in place, adversaries forced to use zero-day approaches.

Contacts:

Dr. Bill Curtis
Executive Director
Consortium for IT Software Quality
bill.curtis@it-cisq.org

John Weiler
Vice Chair
IT Acquisition Advisory Council
john@itaac.org

Tracie Berardi
Program Manager
Consortium for IT Software Quality
tracie.berardi@it-cisq.org
781-444-1132 x149