Washington State Cybersecurity Summit 3

A COMPREHENSIVE APPROACH TO GRID SECURITY

Summary Report from February 29, 2016 Workshop
University of Washington, Seattle, Washington

Co-Hosted by
Snohomish County Public Utility District and
the Pacific Northwest National Laboratory

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle *Since 1965*

SNOHOMISH COUNTY
PUD
PUBLIC UTILITY DISTRICT NO. 1

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <http://www.ntis.gov/about/form.aspx>
Online ordering: http://www.ntis.gov

This document was printed on recycled paper.
(8/2010)

Washington State Cybersecurity Summit 3

A COMPREHENSIVE APPROACH TO GRID SECURITY

Summary Report from February 29, 2016 Workshop University of Washington, Seattle, Washington

Co-hosted by Snohomish County Public Utility District and Pacific Northwest National Laboratory

Sponsored by Snohomish County Public Utility District, Pacific Northwest National Laboratory, Bridge Partners, Critical Informatics, Microsoft, National Guard, NAVSEA, Puget Sound Energy, Seattle City Light, Tacoma Public Utilities, University of Washington, Washington State Military Department, Washington Utilities and Transportation Commission

Authors: Ann Lesperance, Jessica Matlock, Troy Thompson, and Maren Disney

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

SNOHOMISH COUNTY PUD PUBLIC UTILITY DISTRICT NO. 1

ACRONYMS AND ABBREVIATIONS

DOE	U.S. Department of Energy
ESCC	Electric Sector Coordinating Council
ISAC	Information Sharing and Analysis Center
NAVFAC NW	Navy Facilities Engineering Command Northwest
NCC	National Coordinating Center for Communications
PNNL	Pacific Northwest National Laboratory
Q&A	question and answer
SnoPUD	Snohomish County Public Utility District
UW	University of Washington

CONTENTS

SUMMARY

On February 29, 2016, the Snohomish County Public Utility District (SnoPUD) and the Department of Energy's (DOE) Pacific Northwest National Laboratory (PNNL) co-hosted the third annual Washington State Cybersecurity Summit, bringing together industry leaders and policymakers to review what is being done in the state of Washington and engage in a dialogue about how to build a better defense network, combat cyberattacks, and train next-generation cyber professionals. The goal of the summit was to broaden the state's perspective by hearing from public and private experts on cybersecurity and examining both the newest cyber technologies and what is needed to create more resilient systems.

The meeting began with welcome remarks from **Jessica Matlock (SnoPUD)** and **Bjong "Wolf" Yeigh (University of Washington)** who highlighted the workshop's goal to bring together a cross section of public and private experts to examine challenges, opportunities, and solutions. This was followed by a video presentation from **Senator Patty Murray**, who reflected on the state's unique opportunity to be a leader in cybersecurity education, research, and technology.

Major General Bret Daugherty (Washington State National Guard) spoke briefly about the potentially drastic impacts of a cyberattack to the region and the need to think holistically about solutions then introduced the keynote speakers.

Featured guest speakers **Scott Charney (Microsoft Corporation)** and **Patricia Hoffman (DOE Office of Electricity Delivery & Energy Reliability)** discussed the future of cybersecurity from both a private and public perspective.

PANELS

The keynote speakers were followed by a series of presentations and panels addressing the following focus area and questions:

Emerging threats and response

- What are the threats and how do we protect our assets against rapidly evolving cyber threats?
- What is needed during these types of events and are we getting what we need?
- What is working and not working and where do we need assistance from policymakers and the federal government?

Trends in cyber detection and protection

- What are the trends in cyber detection and protection?
- What is the future looking like?
- What are the new tools and processes that are emerging?

Privacy, public disclosure, and information sharing

- How can we ensure information sharing occurs between the organizations and infrastructure while still addressing some of the public disclosure and privacy concerns?

Workforce development and education

- What are the challenges with growing the cybersecurity workforce for critical infrastructure?
- How do we develop needed faculty?
- How do we work with industry to reflect their needs?
- Do universities need to integrate programs more closely with industry, particularly in this field?
- How do we motivate universities to embrace needed changes?
- What does the ideal world look like for us?

OUTCOMES

This report summarizes the presentations, discussions, and outcomes from the workshop. This and previous cybersecurity summit reports are available at http://www.snopud.com.

ACKNOWLEDGEMENTS

SnoPUD and PNNL would like to acknowledge and thank the participants who attended and actively engaged in this summit, including:

- American Public Power Association
- Avista
- Benton PUD
- Bonneville Power Administration
- Bridge Partners Consulting
- Chelan PUD
- City of Seattle
- City of Tacoma
- Clallum PUD
- Columbia Basin College
- Columbia REA
- Congressman Dave Reichert's Office
- Cowlitz County PUD
- Critical Informatics
- Department of Health and Social Services, Western State Hospital
- DOE Office of Electricity, Delivery & Energy Reliability
- Edison Electric Institute
- Energy Northwest
- Governor Jay Inslee's Office
- Grays Harbor PUD
- Industry Assurance and Policy Advocacy
- Internet Identity
- King County
- Microsoft
- NAVSEA
- Navy Facilities Engineering Command Northwest
- Nebraska Public Power District
- Neoprime Solutions
- NUWest Group
- Office of the Chief Information Officer Washington State
- Overlake Medical Center
- Pacific Northwest Economic Region World Trade Center West
- Peak Reliability
- PNGC Power
- Port of Seattle
- Public Power Council
- Puget Sound Energy
- Seattle City Light
- SEL Engineering Services
- Senator Patty Murray's Office
- State of Washington
- Tacoma Public Utilities
- Tempered Networks
- T-Mobile Corporation
- U.S. Coast Guard
- DOE
- U.S. Department of Homeland Security National Cybersecurity and Communications Integration Center
- U.S. Department of Homeland Security Office of Infrastructure Protection National Programs Directorate, Seattle District
- U.S. Navy
- University of Washington
- Van Ness Feldman
- Washington Military Department's Emergency Management Division
- Washington National Guard
- Washington State University
- Washington Utilities and Transportation Committee
- Whatcom Community College
- Whatcom County PUD

INTRODUCTION

On February 29, 2016, the Snohomish County Public Utility District (SnoPUD) and the Department of Energy's (DOE) Pacific Northwest National Laboratory (PNNL) co-hosted the third annual Washington State Cybersecurity Summit, bringing together industry leaders and policymakers to review what is being done in the state of Washington and engage in a dialogue about how to build a better defense network, combat cyberattacks, and train next-generation cyber professionals. Building on the previous summits, the goal of the event was to broaden the state's perspective by hearing from public and private experts on cybersecurity and examining both the newest cyber technologies and what is needed to create more resilient systems.

Major General Daugherty (Washington National Guard) introduces the keynote speakers.

WELCOME REMARKS

Speakers

- **Jessica Matlock**, Director, Government Relations, SnoPUD
- Chancellor **Bjong "Wolf" Yeigh**, University of Washington
- **Senator Patty Murray**, U.S. Senator, Washington

Jessica Matlock (SnoPUD) welcomed participants to the third annual cybersecurity summit, providing highlights from the previous years' meetings and reiterating the goal for the event: to foster engaging discussion about how to enable more resilient cybersecurity.

Chancellor **Bjong "Wolf" Yeigh** (University of Washington [UW]) shared information highlighting the UW's growing cybersecurity education and research, including work at its Tacoma, Seattle, and Bothell campuses. Wolf reported that the school is currently ranked 10th in best places in the country to study cybersecurity. He also reported that the Tacoma campus will be hosting a cyber symposium later in 2016.

Wolf was followed by a video presentation from **Senator Patty Murray** (U.S. Senate), whose opening remarks reflected on the state's unique opportunity as a regional leader in cybersecurity education, research, and technology. Senator Murray praised the state's growth in cybersecurity leadership and underpinned the importance of convening stakeholders to pioneer the next bold and innovative step forward.

> "Washington State is uniquely positioned to emerge as a national and global hub for cybersecurity."
>
> **Senator Patty Murray**

KEYNOTE SPEAKERS

Speakers

- Major General **Bret Daugherty**, Adjutant General, Washington National Guard
- **Scott Charney**, Corporate Vice President for Trustworthy Computing, Microsoft
- **Patricia Hoffman**, Assistant Secretary, DOE Office of Electricity, Delivery & Energy Reliability

Major General Bret Daugherty (Washington National Guard) shared insight into the potential and drastic impact a cyberattack could have on public infrastructure. Major General Daugherty is the senior official for responding to a major cyber event and homeland security advisor to Governor Jay Inslee. Major General Daugherty highlighted recent advances by the Washington State Military Department to advance security efforts and the forming of a Washington State infrastructure protection subcommittee charged with advising himself and the governor on emergency preparedness. An annual report on statewide cybersecurity readiness is due in the fall.

> "No matter how great our expertise, we can't prevent or respond to an event alone."
>
> **Major General Bret Daughtery**
> **Washington National Guard**

Scott Charney (Microsoft) walked the audience through the historical evolution of cyberattacks, from the early days of young hackers exploring networks to today's forward-looking complexities facing the nation as the Internet of Things (IoT) becomes more prevalent and as militarization of cyberspace continues. He noted that the IoT is here, and with it comes 5 billion assets to secure, and yet many of the IoT devices will not be built by companies with cybersecurity experience.

To that end, Scott showcased Microsoft's "Trustworthy Computing 2.0" model, built around the following:

- Secure and empower customers (security services/ features, transparency, controllability)
- Secure operations (national and international certifications, operational security assurance)
- Secure ecosystems (cybersecurity collaboration, cybercrime prevention, cyber norms)
- Secure development (security development lifecycle, software integrity policies).

> "Cyber used to focus on stealing information, which led to long and slow destruction of a business. Now there are more destructive attacks and the effects are more immediate."
>
> **Scott Charney, Microsoft**

Scott responded to questions regarding the challenges of investing in cybersecurity solutions, noting that hardware roots of trust are being leveraged to address authentication of both devices and individuals. Additionally, it is critical to implement domain isolation, separating critical systems that must be more highly protected. He also noted that since all attacks will not be prevented, there is a need to focus on infrastructure resilience, exploring how to contain an attack to a certain area, how to reconstruct the environment, and how to validate the integrity of data.

Scott Charney (Microsoft) discusses Trustworthy Computing 2.0.

Patricia Hoffman (DOE Office of Electricity, Delivery & Energy Reliability) focused on utility infrastructure and workforce management and how to strengthen the ability to respond cohesively. Patricia noted the need for a tactical approach that addresses infrastructure, enterprise risk strategy, asset management, and access management as well as supply chain and workforce management. She emphasized that as the

cyber landscape evolves, there is a growing need to integrate control systems into major functions as well as education, challenging that more control systems should be brought into major fields. Patricia also emphasized the importance of recovery and the need to focus on it in the coming years.

During the question and answer (Q&A) session, speakers addressed current trends and challenges including:

- The importance of information sharing
- How utilities can use backup servers and redundancies in systems
- Advancing federal standards and how states address utilities
- Hardware risks and prevention solutions
- Integrating cybersecurity into basic education
- The human-computer division of work in industry.

> "If we don't get cybersecurity at scale from a critical infrastructure point of view, we are going to have a great hurdle to overcome. How do we share and incorporate those capabilities?"
>
> **Patricia Hoffman, DOE Office of Electricity, Delivery & Energy Reliability**

EMERGING THREATS AND RESPONSE

This panel explored emerging threats, what is working and not working, and what is needed to better protect our assets against rapidly evolving cyber threats.

Panelists:

- *Facilitator*: **Phillip B. Jones**, Commissioner, Washington Utilities and Transportation Committee
- **SnoPUD/National Guard: Benjamin Beberness**, Chief Information Officer, SnoPUD
- **Edison Electric Institute: Scott Aaronson**, Managing Director, Electric Sector and National Infrastructure Protection
- **Washington Military Department's Emergency Management Division: Robert Ezelle**, Director
- **U.S. Navy: Darla Montgomery-Sherrell**, Command Information Officer, Navy Facilities Engineering Command Northwest

The panel opened with a presentation from **Scott Aaronson (Edison Electric Institute)**, who presented "Industry-Government Partnerships for Critical Infrastructure Security." Scott described the threat landscape relative to the likelihood of an attack versus its consequence. He then outlined current industry-government collaboration and the **Electric Sector Coordinating Council** (ESCC) efforts in overseeing industry-government coordination, leveraging infrastructure and research and development, sharing threat information, and coordinating across sectors.

> "You can't protect everyone from everything. Protection of critical infrastructure is a shared responsibility."
>
> **Scott Aaronson, Edison Electric Institute**

Benjamin Beberness (SnoPUD) presented on the National Guard Penetration Test, an operation in which cybersecurity professionals from the Washington National Guard and a series of industry experts tested the cyber defenses of SnoPUD. The friendly but life-like hack featured a realistic-looking work email disseminated to employees. Benjamin described the challenges and benefits of the effort, explaining that it took support from all ranks and organizational levels to coordinate the successful operation. While a table-top exercise is great, an operation is even better, he said. Benjamin also highlighted the **Electricity Sector Information Sharing and Analysis Center (ISAC)**. The Electricity ISAC, in collaboration with the DOE and the ESCC, serves as the primary security communications channel for the electricity subsector and enhances the subsector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents.

> "The [National Guard/SnoPUD] cyber operation made us a little more humble and made my staff rethink cybersecurity and rethink our response."
>
> **Benjamin Beberness, Snohomish County Public Utility District**

Darla Montgomery-Sherrell (Navy Facilities Engineering Command Northwest [NAVFAC NW]) presented "NAVFAC NW Cybersecurity Challenges," describing efforts to work with the critical infrastructure community and lend expertise and capabilities to advance coordinated training. The effort seeks to advise and assist by leveraging a coordinated response, situational awareness, organizational mapping, and security remediation. Darla highlighted challenges, risks, and constraints facing the Northwest and described NAVFAC NW's efforts to build and maintain sustainable facilities, deliver utilities and services, and provide Navy expeditionary combat force capabilities. She highlighted efforts to build on existing successful partnerships with a goal to apply the lessons learned to future collaborations with industry and vendors.

Robert Ezelle (Washington Military Department's Emergency Management Division) discussed how Washington State, both generally and from a military perspective, would respond to a cyber event. Within the last decade, the cyber threat and the potential consequences have come forward in the state's Emergency Management Division response thinking, he said. He cited the SnoPUD exercise as a positive example of the state's response capabilities. Robert emphasized the need for unified coordination and partnerships, from the governor directing state entities to state emergency and outreach centers developing action plans, allocating resources, and facilitating interagency resolution of priorities and conflicts.

> "Cybersecurity is much more than an IT issue—we see it as a matter of public safety."
>
> **Robert Ezelle, Washington Military Department's Emergency Management Division**

Panelists discuss emergency threats and response.

Troy Thompson (PNNL) and Craig Schultz (NeoPrime) discuss trends and emerging challenges in cybersecurity.

Robert also noted future efforts with the Department of Homeland Security, Federal Emergency Management Agency, and the National Guard to enhance cyber resource typing and training. He shared how the National Guard is working with the critical infrastructure community to lend their expertise and capabilities to enable coordinated response, situational awareness, and organizational mapping.

TRENDS AND PERSPECTIVES IN CYBER DEFENSE

Panelists provided industry and government perspectives on emerging trends and tools in cyber defense.

Panelists:

- *Facilitator*: **Gordon Matlock**, Cyber Practice Lead, Bridge Partners
- **PNNL: Troy Thompson**, Chief Information Security Officer
- **Neoprime Solutions: Craig Schultz**, CEO

Troy Thompson (PNNL) began the panel discussion with a presentation on the conventional cybersecurity landscape and the role of national laboratories. He shared how laboratories balance mission needs with cybersecurity demands along with risk tolerance, training, and awareness. Troy noted the importance of considering differing perspectives (adversary versus defender) across the physical, human, and digital domain.

> "The challenge is how quickly can we cycle through and understand mission priorities, what we're doing to detect, respond, recover, and measure effectiveness."
>
> **Troy Thompson,**
> **Pacific Northwest National Laboratory**

Craig Schultz (Neoprime Solutions) focused on the changing economics of attack and defense, the cost of an attack versus the cost of defense. He also reflected on his experiences abroad understanding attackers' views in emergency security and technology control.

During the discussion, Troy and Craig explored the rising challenges and opportunities as people grow more connected across all fronts—at home, at work, in medical technologies, in their cars, etc. They highlighted trends in security products and their lifecycle and compared current-to-emerging next-generation security control models.

During the Q&A session, the audience asked how to protect the local account as attacks continue to escalate. The speakers discussed typical measures such as account lockout, aggressive scanning, and password policies, but reiterated the need for behavior-based approaches, emphasizing the need for new models of user training and awareness.

> "Trends in security products and their lifecycle are making it more dynamic in how security has to be put into place—you can't be static anymore."
>
> **Craig Schultz, Neoprime Solutions**

PRIVACY, PUBLIC DISCLOSURE, AND INFORMATION SHARING

Panelists discussed information sharing among and between critical infrastructure providers and how to address public disclosure and privacy concerns.

Panelists:

- *Facilitator*: **Ann Lesperance**, Director, Northwest Regional Technology Center, PNNL
- **American Public Power Association: Joy Ditto**, Senior Vice President, Legislative and Political Affairs
- **National Cybersecurity and Communications Integration Center U.S. Department of Homeland Security: Mike Roskind**, Deputy Director, National Coordinating Center for Communications
- **Microsoft: Aaron Kleiner**, Director, Industry Assurance and Policy Advocacy

Joy Ditto (American Public Power Association) reviewed recent history from passage of the Energy Policy Act of 2005, which created the Critical Infrastructure Protection standards, to the establishment of the electric sector cyber coalition in 2007 and passage of the Cybersecurity Act of 2015, an information sharing framework across critical infrastructure sectors long sought by the electric sector. Joy also discussed the grid security provisions of the 2015 Fixing America's Surface Transportation Act

Aaron Kleiner (Microsoft) discusses cybersecurity information sharing and risk management.

(5-year, $305 billion). Joy said that Congress has honed in on the concepts regarding with whom information is being shared, encouraging certain information to be unclassified, giving liability protection to the private sector, and facilitating rapid sharing of information. Implementation of the bills passed in 2015 by the Department of Homeland Security, DOE, and Federal Energy Regulatory Commission will be important to monitor and engage in where appropriate.

> "What you've seen all day long about resilience and response—that is where we're working to make improvements."
>
> **Joy Ditto, American Public Power Association**

Mike Roskind (National Coordinating Center for Communications [NCC]) presented on the NCC Communications ISAC. Mike provided an overview of the NCC programs and operations as well as activities to develop a common operating picture for coordinated and local response to ensure communications, protect national security, and enable emergency preparedness. Mike also highlighted how the Communications ISAC, as a function of the NCC, is facilitating voluntary collaboration and information sharing.

> "You have to be able to create the environment from the high levels of management, to clear the deck so the action officers can do their job to develop strategies and implement."
>
> **Mike Roskind, National Coordinating Center for Communications**

To that end, **Ann Spangler (SnoPUD)** spoke briefly on the state's Public Records Act, noting that there are no specific exemptions for critical infrastructure or privacy, except for vulnerability assessments and emergency response plans.

Aaron Kleiner (Microsoft) presented "Cybersecurity Information Sharing: Foundational Element of Risk Management," defining key elements for building an effective and sustainable information sharing program. These building blocks include a

Panel discusses challenges and opportunities for developing next-generation leadership in cybersecurity.

detailed understanding of the methods, models, and mechanisms of exchange; actors involved; scope and purpose; and types of information involved. Kleiner provided a series of recommendations for developing an information sharing network. More information is available in the white paper titled, "**A Framework for Cybersecurity Information Sharing and Risk Reduction.**"

> "Commitment, trust, cooperation, and a clear sense of value are required."
>
> **Aaron Kleiner, Microsoft**

WORKFORCE DEVELOPMENT AND EDUCATION

This panel addressed challenges and opportunities for growing the cybersecurity workforce for critical infrastructure.

Panelists:

- *Facilitator*: **Barbara Endicott-Popovsky**, Ph.D., Professor, UW Institute of Technology
- **T-Mobile Corporation: Bill Boni**, Vice President & Corporate Information Security Officer
- **Critical Informatics: Mike Hamilton**, CEO
- **UW Department of Urban Design and Planning: Jill Sterrett**, Lecturer and Leadership Advisor, Master of Infrastructure Planning and Management Program
- **Columbia Basin College: Matt Boehnke**, Assistant Professor Computer Science/Cyber Security

Mike Hamilton (Critical Informatics) emphasized the need for incoming talent to get first-hand exposure to life in the cyber trenches and the need for industry and government to integrate to develop solutions along with mutual aid. He cited several existing opportunities such as the **Washington Technology Industry Coalition Tech Apprenticeship**, which was established in 2015 and is set to train and place 600 registered apprentices over the next five years. He also highlighted PISCES, the Public Infrastructure Security Collaboration and Exchange System, through which local government can share information and provide rich telemetry.

> "We need new models for user training and awareness. We need new clever approaches that provide the awareness, the training, the so what for our user community."
>
> **Mike Hamilton, Critical Informatics**

Jill Sterrett (UW Department of Urban Design and Planning) discussed major changes affecting infrastructure and requiring the attention of managers and planners, focusing on cybersecurity, climate change/climate instability, and sustainability. Jill noted that all three of these factors are rapidly changing our infrastructure systems and demand approaches other than just hard engineering. Jill urged for solutions that are holistic and integrated across multiple disciplines, solutions that are based on future-casting for an ever-changing world (not forecasting based on trend lines from the past), and solutions that consider lifecycle costs of construction, operations, and maintenance over the full life of the system, including benefits and costs to the full community (not just monetary expenditures). These are all planning and management issues that require a broad understanding of the integration of multiple infrastructures, knowledge of the challenges and threats we face, and awareness of how they interface with the wider community. She also noted the need for universities to integrate with industry to develop professionals to bridge the gaps as the workforce and industry change.

> "We need people who are able to understand those effects of climate change and sustainability across multiple sectors and how sectors can work together."
>
> **Jill Sterrett, UW Department of Urban Design and Planning**

Matt Boehnke (Columbia Basin College [CBC]) discussed efforts to bring military into cybersecurity education and how basic training could require students to think tactically, operationally, and then strategically. The effort aims to ensure students are "shovel ready" with qualified skillsets. He discussed CBC's partnering with PNNL to provide vibrant, dynamic opportunities for students. PNNL supports CBC's Cybersecurity Bachelor of Applied Science Program and welcomes numerous cybersecurity interns to its team annually.

> "The more you're in it, the better you get at it. Students need the motivation of a job and working with an industry where they have an immediate impact."
>
> **Matt Boehnke, Columbia Basin College**

During the Q&A session, speakers discussed opportunities to more effectively leverage better curriculum along with more cutting-edge and less state-centric approaches for workforce development, noting the need for a compelling and challenging working environment as being key to success. They were also asked to identify key skills they see as most important for incoming talent, to which they collectively responded with 1) communications and 2) the ability to work on a team.

> "We can teach methods and concepts, but books alone do not work—the way we get our students ready is to bring people like we have here today into the classroom."
>
> **Barbara Endicott-Popovsky, UW Institute of Technology**

WRAP-UP

Jessica Matlock (SnoPUD) concluded the day's discussions with a recap of the recurring themes and ideas the participants will continue to explore in the future. These included:

- Information sharing, resiliency, and collaboration are important as ever.
- Support has to come from the top.
- Utilities need to look at access management and controls.
- Security cannot be static; it must be dynamic.
- Key approaches include diversion deception techniques, cloaking, decoys, and moving toward zero administrators or specific use access.
- You need to know the specific risk or your risk tolerance.
- We can build walls higher but real change requires behavioral change.
- We need to look at critical infrastructure as a holistic state.
- Cybersecurity should be incorporated into basic education.
- University and colleges need to hear what companies need to structure their programs.
- Observe legislation regarding pre-emption issues of the Sunshine Laws.
- States should enable protections for critical infrastructure.

NEXT STEPS

Looking forward, participants from the workshop will continue to engage and explore opportunities for research and development to address key challenges defined during the summit:

- Building informal public-private partnerships
- Defining a framework for cyber recovery
- Assessing an entity's risk and determining what to spend on cyber
- Building response and recovery plans that protect against vulnerabilities
- Enabling capabilities at scale and informing investment strategies
- Building next-generation cybersecurity professionals

Results from the workshop will be shared with participants and made available on the SnoPUD website (http://www.snopud.com).

KEY PARTICIPANTS

- Scott Aaronson, Managing Director, Electric Sector and National Infrastructure Protection, Edison Electric Institute
- Benjamin Beberness, Chief Information Officer, SnoPUD
- Matt Boehnke, Assistant Professor Computer Science/Cyber Security, CBC
- Bill Boni, Vice President & Corporate Information Security Officer, T-Mobile Corporation
- Scott Charney, Corporate Vice President for Trustworthy Computing, Microsoft
- Major General Bret Daugherty, Adjutant General, Washington National Guard
- Joy Ditto, Senior Vice President, Legislative and Political Affairs, American Public Power Association
- Barbara Endicott-Popovsky, Ph.D., Professor, UW Institute of Technology
- Robert Ezelle, Director, Washington Military Department's Emergency Management Division
- Mike Hamilton, CEO, Critical Informatics
- Patricia Hoffman, Assistant Secretary, DOE Electricity Delivery & Energy Reliability
- Phillip B. Jones, Commissioner, Washington Utilities and Transportation Committee
- Aaron Kleiner, Director, Industry Assurance and Policy Advocacy, Microsoft
- Ann Lesperance, Director, Northwest Regional Technology Center, PNNL
- Gordon Matlock, Cyber Practice Lead, Bridge Partners
- Jessica Matlock, Director, Government Relations, SnoPUD
- Senator Patty Murray
- Darla Montgomery-Sherrell, Command Information Officer, NAVFAC NW
- Mike Roskind, Deputy Director, National Cybersecurity and Communications Integration Center, U.S. Department of Homeland Security
- Craig Schultz, CEO, Neoprime Solutions
- Bjong "Wolf" Yeigh, Chancellor, UW Bothell
- Jill Sterrett, Lecturer and Leadership Advisor, Master of Infrastructure Planning and Management Program, UW Department of Urban Design and Planning
- Troy Thompson, Chief Information Security Officer, PNNL

AGENDA

WASHINGTON STATE CYBERSECURITY SUMMIT 3:

A Comprehensive Approach to Grid Security

February 29, 2016, 8:30 a.m. – 4:00 p.m.

University of Washington, HUB
4100 E. Stevens Way NE, Seattle, WA 98195

Presented by

bridge partners · critical informatics · Microsoft · National Guard · Pacific Northwest National Laboratory · PSE Puget Sound Energy · Snohomish County PUD · Seattle City Light · Tacoma Public Utilities · University of Washington · NAVSEA · Office of the Chief Information Officer · UTC Utilities and Transportation Commission

The Third Annual Cybersecurity Summit brings together industry leaders and policymakers to identify how we can build a better defense network, combat cyberattacks, and train next generation cyber professionals. This summit will broaden the state's perspective by hearing from public and private experts on cybersecurity and examine the newest cyber technologies and what we need to create more resilient systems.

AGENDA

Time	Topic	Speakers
8:30 a.m.	**Check in**	
9:00 a.m.	**Welcoming Remarks**	◗ **Jessica Matlock,** Director, Government Relations, Snohomish County PUD ◗ Chancellor **Bjong "Wolf" Yeigh,** University of Washington
9:10 a.m.	**Opening Remarks (video)**	◗ **Senator Patty Murray**
9:15 a.m.	**Remarks and Introduction of Keynote**	◗ **Major General Bret Daugherty,** The Adjutant General, Washington State National Guard
	Keynote Speakers Hear a discussion about the future of cybersecurity from a private and public perspective.	◗ **Scott Charney,** Corporate Vice President for Trustworthy Computing at Microsoft ◗ **Patricia Hoffman,** Department of Energy, Assistant Secretary, Office of Electricity Delivery & Energy Reliability
10:30 a.m.	**Break**	

(continued)

Time	Topic	Speakers
10:40 a.m.	**What are the threats and how do we protect our assets against rapidly evolving cyber threats?** **What is needed during these types of events and are we getting what we need?** **What is working and not working and where do we need assistance from policymakers and the federal government?**	*Facilitator*: **Phillip B. Jones,** Commissioner, Washington Utilities and Transportation Committee (UTC) ◗ **SnoPUD/National Guard: Benjamin Beberness,** Chief Information Officer, Snohomish County PUD ◗ **Edison Electric Institute: Scott Aaronson,** Managing Director, Electric Sector and National Infrastructure Protection ◗ **Washington Military Department's Emergency Management Division: Robert Ezelle,** Director ◗ **United States Navy: Darla Montgomery-Sherrell,** Command Information Officer, NAVFAC NW
12:00 p.m.	**BOX LUNCH**	
12:30 p.m.	**What are the trends in cyber detection and protection?** **What is the future looking like?** **What are the new tools and processes that are emerging?** (from industry and government/regulator perspective)	*Facilitator*: **Gordon Matlock,** Cyber Practice Lead, Bridge Partners ◗ **Pacific Northwest National Laboratory: Troy Thompson,** CISO ◗ **Neoprime Solutions: Craig Schultz,** CEO
1:30 p.m.	**Privacy, Public Disclosure and Information Sharing – Finding the Balance** Information sharing among and between critical infrastructure providers is paramount to rapidly addressing cybersecurity threats. How can we ensure information sharing occurs between the organizations and infrastructure while still addressing some of the public disclosure and privacy concerns?	*Facilitator*: **Ann Lesperance,** Director, Northwest Regional Technology Center, Pacific Northwest National Laboratory ◗ **American Public Power Association: Joy Ditto,** Senior Vice President, Legislative and Political Affairs ◗ **National Cybersecurity and Communications Integration Center US Department of Homeland Security: Mike Roskind,** Deputy Director, National Coordinating Center for Communications ◗ **Microsoft: Aaron Kleiner,** Director, Industry Assurance and Policy Advocacy

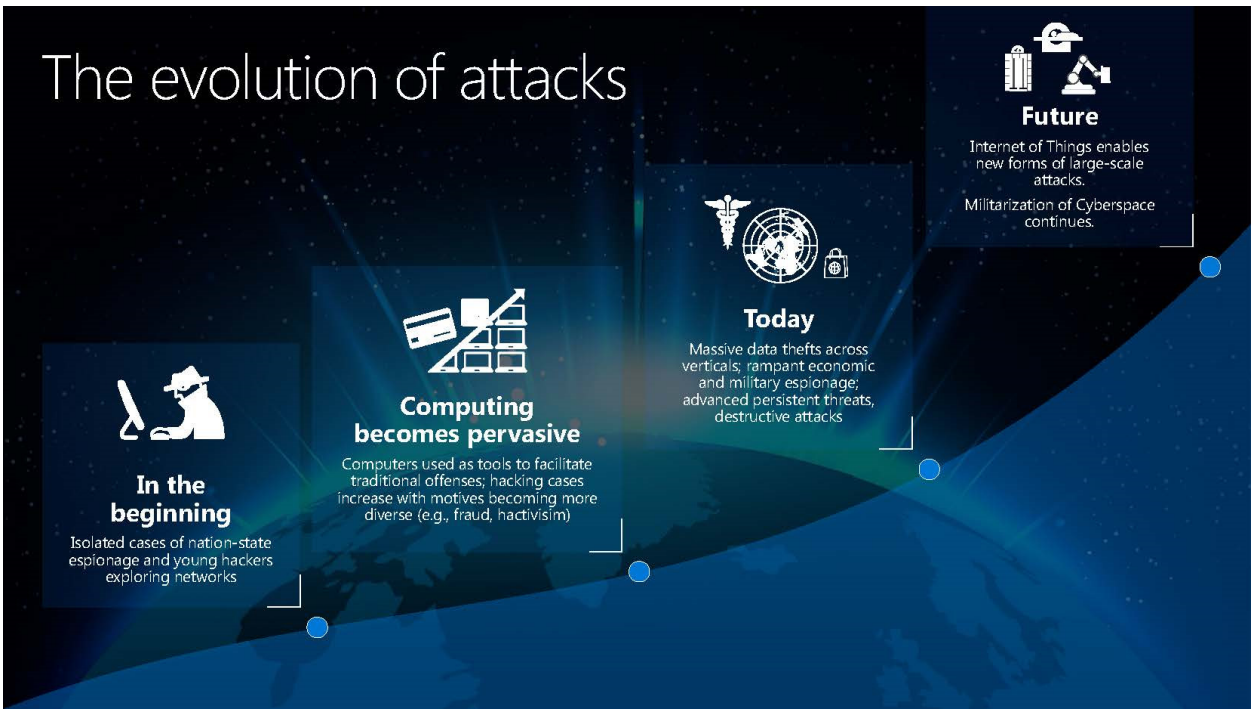
(continued)

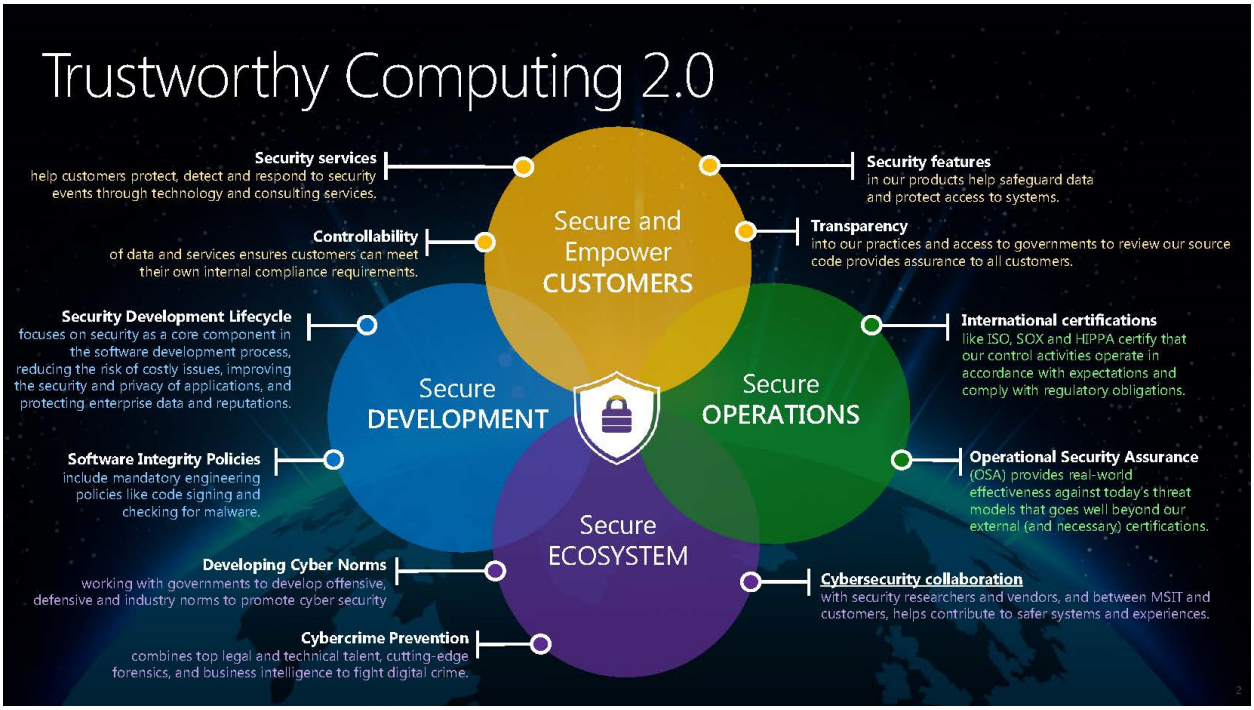
Time	Topic	Speakers
2:30 p.m.	**What are the challenges we have with growing the cybersecurity workforce in the State of Washington for critical infrastructure?** **How do we develop needed faculty?** **How do we work with industry to reflect their needs?** **Do universities need to integrate programs more closely with industry, particularly in this field?** **How do we motivate universities to embrace needed changes?** **What does the ideal world look like for us?**	*Facilitator:* **Barbara Endicott-Popovsky,** Ph.D., Professor, University of Washington Institute of Technology • **T-Mobile Corporation: Bill Boni,** Vice President & Corporate Information Security Officer • **Critical Informatics: Mike Hamilton,** CEO • **University of Washington Department of Urban Planning: Jill Sterrett,** Lecturer and Leadership Advisor, MIPM Program • **Columbia Basin College: Matt Boehnke,** Assistant Professor Computer Science/ Cyber Security
3:30 p.m.	**Wrap-up and next steps, follow-up actions**	

PRESENTATIONS

- The Evolution of Attacks (Microsoft)
- Industry-Government Partnerships for Critical Infrastructure Security (Edison Electric Institute)
- Cybersecurity Challenges (NAVFAC NW)
- Trends & Perspectives in Cyber Defense (PNNL, NeoPrime)
- Privacy, Public Disclosure and Information Sharing: Finding the Balance (American Public Power Association)
- Cybersecurity Information Sharing: Foundational Element of Risk Communication (Microsoft)

The Evolution of ATTACKS (Microsoft)





Industry-Government Partnerships for Critical Infrastructure Security (Edison Electric Institute)

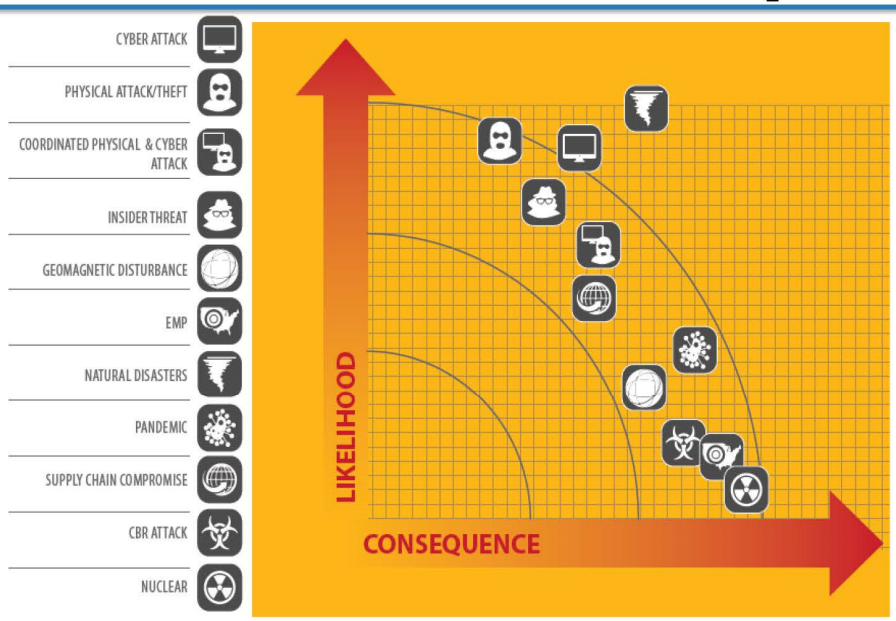
EEI
Edison Electric
INSTITUTE

Industry-Government Partnerships for Critical Infrastructure Security

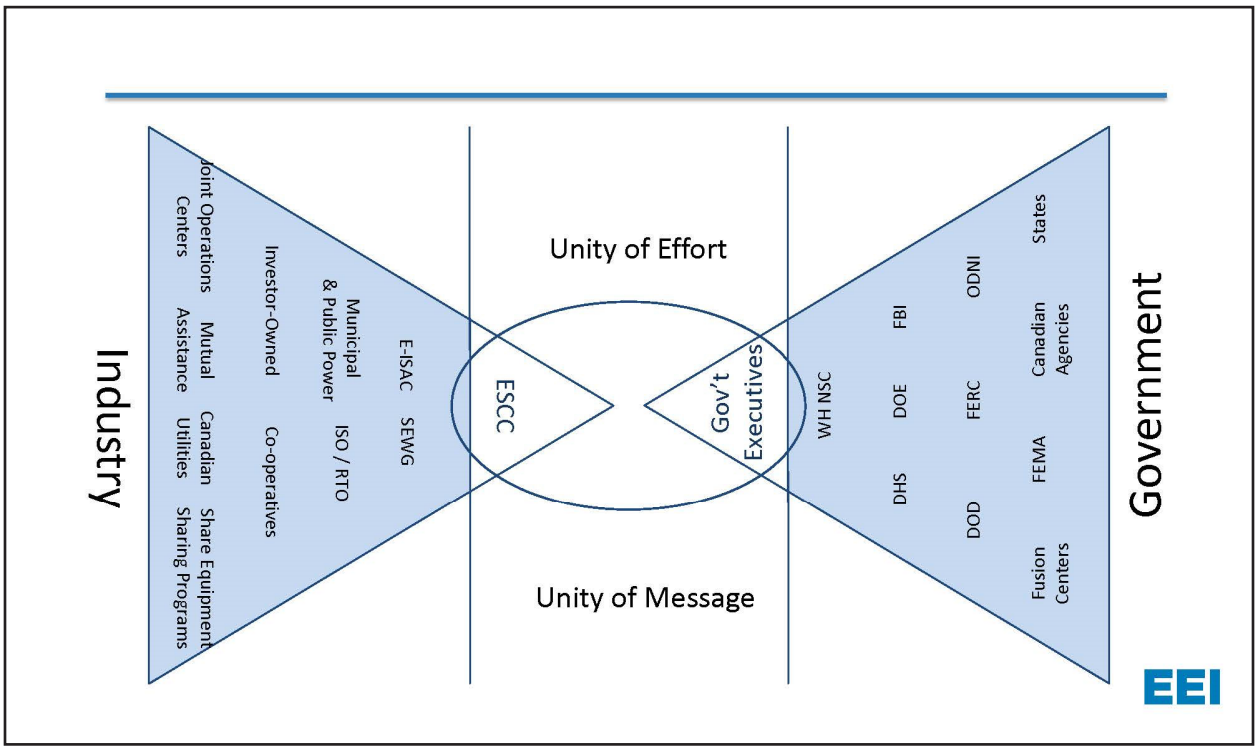
UW Cyber Summit Panel
February 29, 2016

Scott Aaronson
Edison Electric Institute

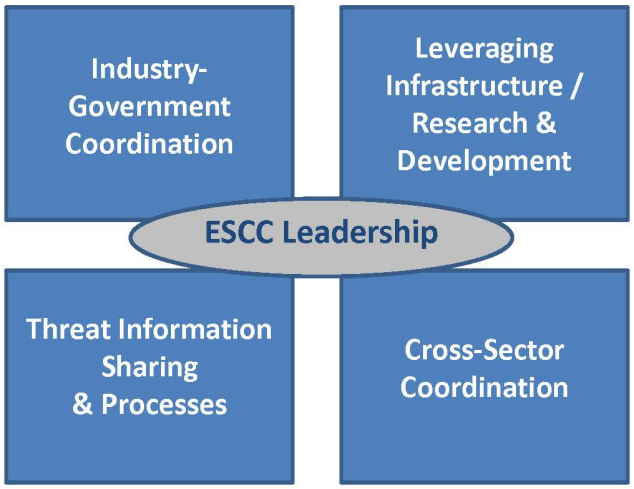
The Threat Landscape



EEI



ESCC Committee Structure



EEI

The Edison Electric Institute (EEI) is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for 220 million Americans, operate in all 50 states and the District of Columbia, and directly employ more than 500,000 workers.

With $100 billion in annual capital expenditures, the electric power industry is responsible for millions of additional jobs. Reliable, affordable, and sustainable electricity powers the economy and enhances the lives of all Americans.

EEI has 70 international electric companies as Affiliate Members, and 270 industry suppliers and related organizations as Associate Members.

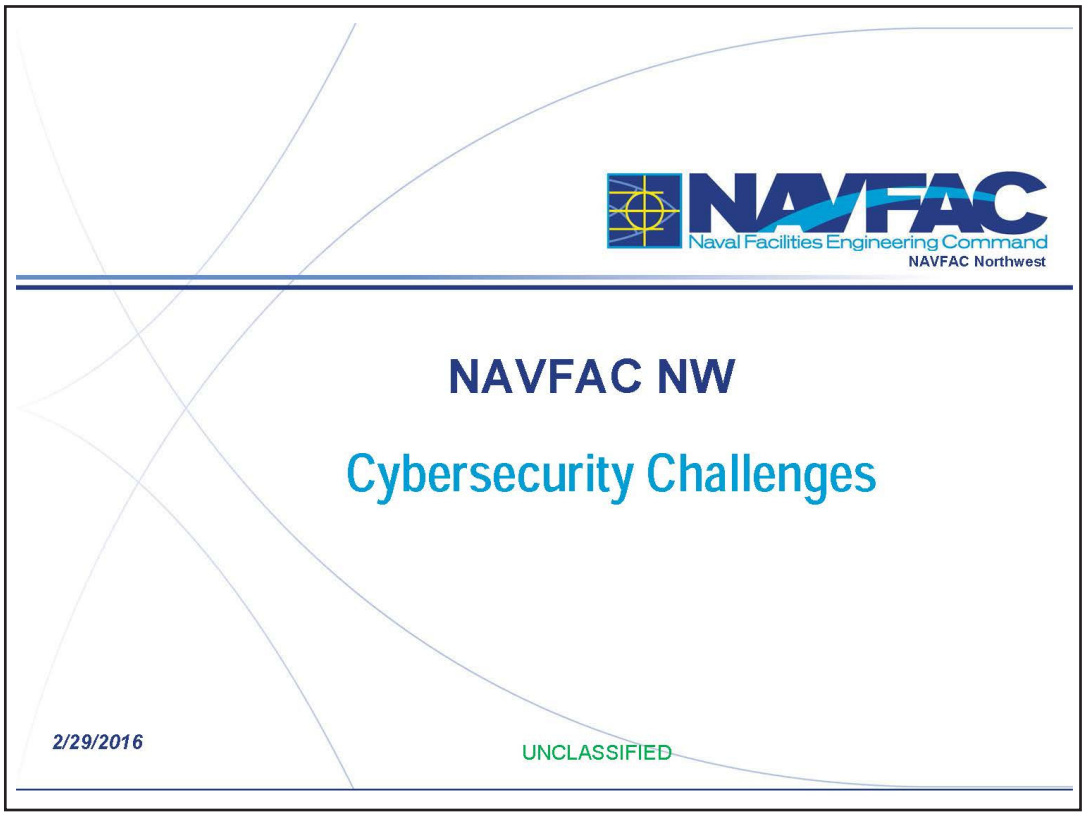
Organized in 1933, EEI provides public policy leadership, strategic business intelligence, and essential conferences and forums.

For more information, visit our Web site at www.eei.org.

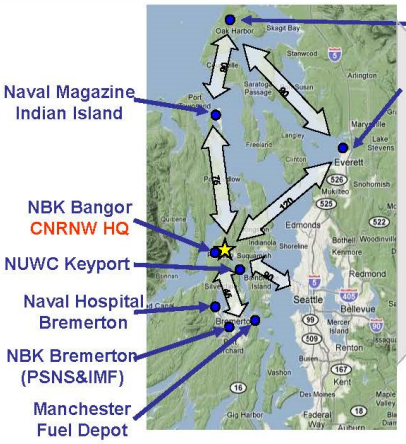
January 2016

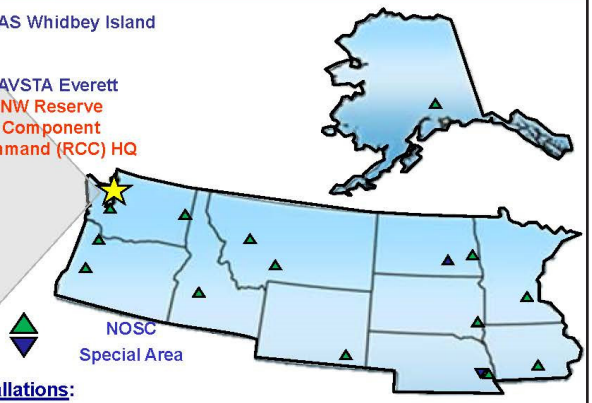
EEI

Cybersecurity Challenges (NAVFAC NW)



NACFAC NW Area of Responsibility





Installations:
- NAVBASE Kitsap (Bangor, Bremerton, Keyport, Manchester)
- NAVSTA Everett (Jim Creek, Smokey Point, Pacific Beach)
- NAVAIRSTA Whidbey Island (Ault Field, Seaplane Base)
- NAVMAG Indian Island

Navy Operational Support Centers (14) in 11 states:
Alaska, Idaho, Iowa, Minnesota, Montana, Nebraska, North Dakota, Oregon, South Dakota, Washington, Wyoming

Two Special Areas: LaMoure, ND; Omaha, NB

Geographic Challenges
- Most inter-installation travel requires ferry
- Traffic congestion and pre-ferry wait times
- Time and expense to command

3 READINESS – PERFORMANCE - SUSTAINABILITY

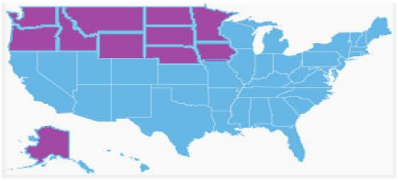
NAVFAC's Cybersecurity Responsibility

- NAVFAC is the SYSCOM for Cybersecurity and Information Technology of Control Systems (CS) Ashore, per Secretary of the Navy (SECNAV) Instruction 5400.15c
- Life-cycle support including research and development, design, procurement, testing, etc…
- More than execution - Technical Authority

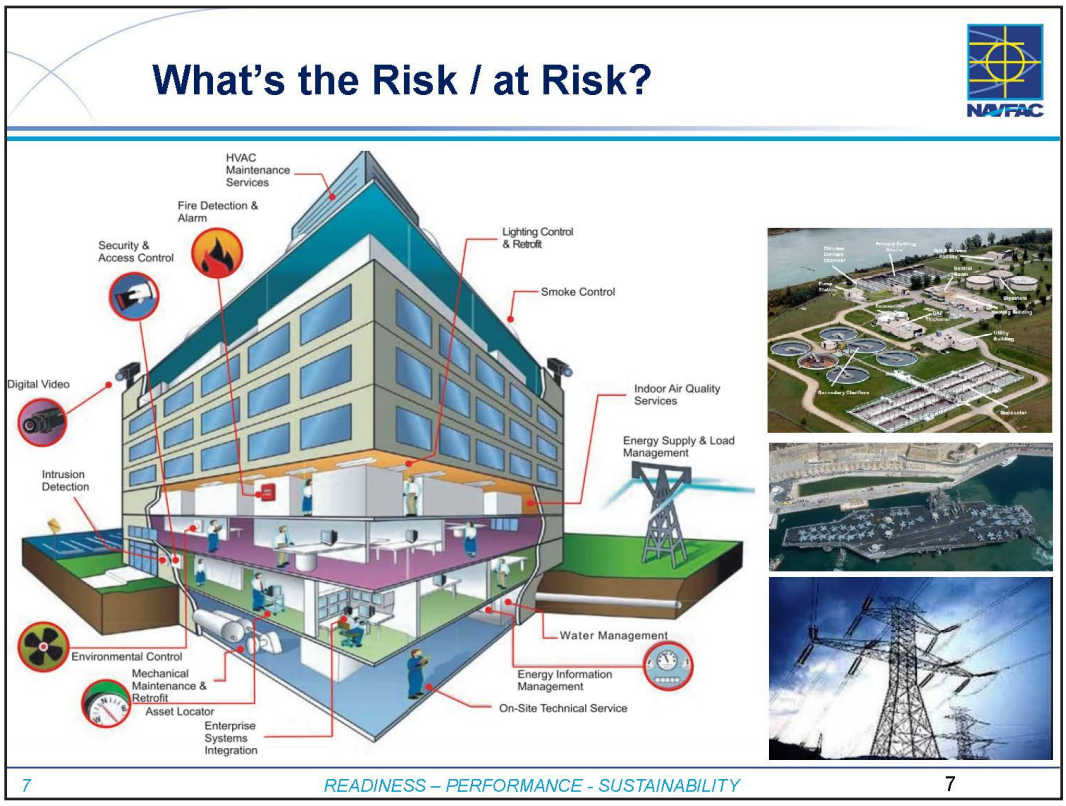
4 READINESS – PERFORMANCE - SUSTAINABILITY

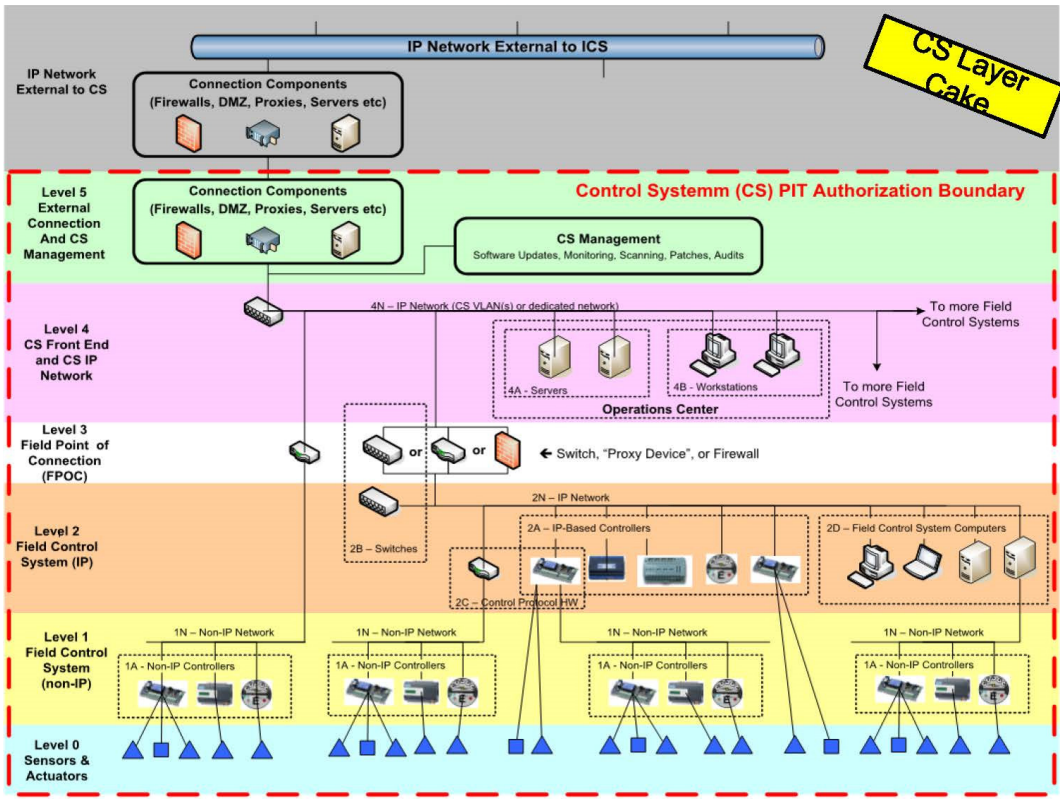
Challenges / Constraints in the Northwest

- Recruiting and retaining qualified employees and planning for attrition
- NW has four years execution over corporate
- No current policy ensuring CIO involvement in project acquisition - planning, development, and execution
- Design to implementation timelines
  - Installation technology can quickly become obsolete or obsolescent by the time it's implemented
- Procurement difficulties
- Lots of systems and no standardization between them
- Articulating the requirements across industry and vendors since some of the Navy language is different or not aligned with industry standard



- Use of technologies that are not developed with Cybersecurity as a design imperative
- Disparate Transport Systems
- Inheritance of unsecured wireless technologies
- Volume of networked and IP connected sensors and devices
- To date we've seen that most OT is typically developed in a vacuum with a very specific mission and little or no consideration to logical security


What's the Risk / at Risk?
NAVFAC
HVAC Maintenance Services
Fire Detection & Alarm
Security & Access Control
Lighting Control & Retrofit
Smoke Control
Digital Video
Indoor Air Quality Services
Energy Supply & Load Management
Intrusion Detection
Water Management
Environmental Control
Mechanical Maintenance & Retrofit
Energy Information Management
Asset Locator
On-Site Technical Service
Enterprise Systems Integration
7
READINESS – PERFORMANCE - SUSTAINABILITY
7


IP Network External to ICS
CS Layer Cake
IP Network External to CS
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
Control Systemm (CS) PIT Authorization Boundary
Level 5 External Connection And CS Management
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
CS Management
Software Updates, Monitoring, Scanning, Patches, Audits
Level 4 CS Front End and CS IP Network
4N – IP Network (CS VLAN(s) or dedicated network)
To more Field Control Systems
4A - Servers
4B - Workstations
Operations Center
To more Field Control Systems
Level 3 Field Point of Connection (FPOC)
or
or
Switch, "Proxy Device", or Firewall
2N – IP Network
Level 2 Field Control System (IP)
2A – IP-Based Controllers
2D – Field Control System Computers
2B – Switches
2C – Control Protocol HW
Level 1 Field Control System (non-IP)
1N – Non-IP Network
1A - Non-IP Controllers
Level 0 Sensors & Actuators


Where are DoN Control Systems?
NAVFAC
NAVY
EVERYWHERE
9
READINESS – PERFORMANCE - SUSTAINABILITY

Trends & Perspectives in Cyber Defense (PNNL, NEOPRIME)

Neo Prime Solutions

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Trends & Perspectives in Cyber Defense

People ⇔ Process ⇔ Technology

CRAIG SCHULTZ

TROY THOMPSON

Washington State Cyber Summit III
February 29, 2016
Seattle, WA

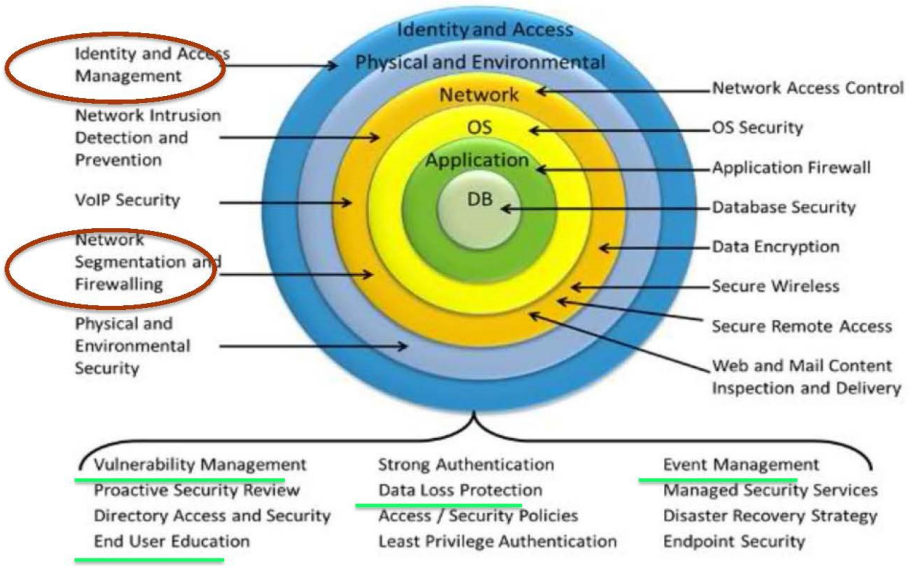
1

Neo Prime Solutions

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Conventional Cybersecurity Landscape

…Complex and Dynamic



2

Neo Prime Solutions

Attacker's View Into An Organization

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Stealth Attacks: Why Hackers Love Networks That Are 'Crunchy on the Outside and Chewy on the Inside', - McAfee Business Blog 2014

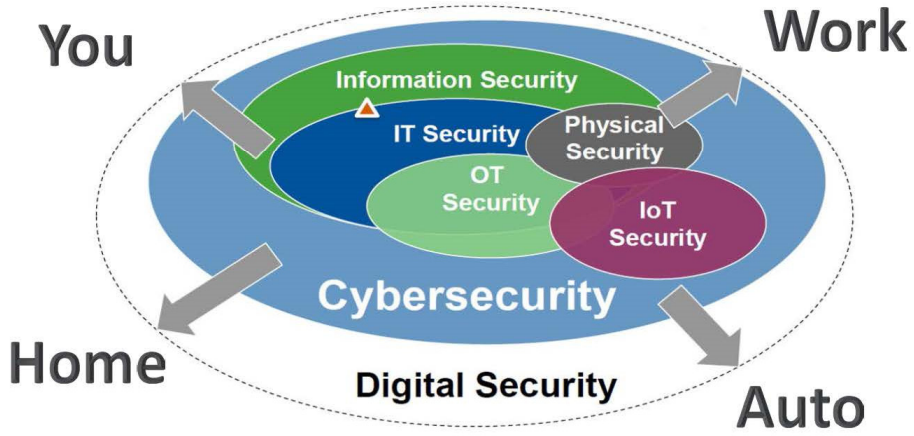
3

Neo Prime Solutions

Cyberspace is rapidly evolving

... more complex, merged and dynamic!

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965



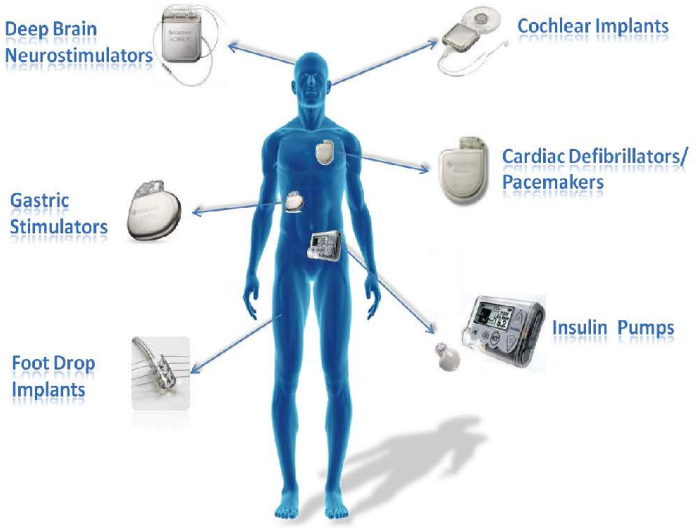
4

Neo Prime Solutions

Cyberspace and your medical technology…

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

WIRELESS IMPLANTABLE MEDICAL DEVICES



5

Neo Prime Solutions

Cyberspace and your home…

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

6

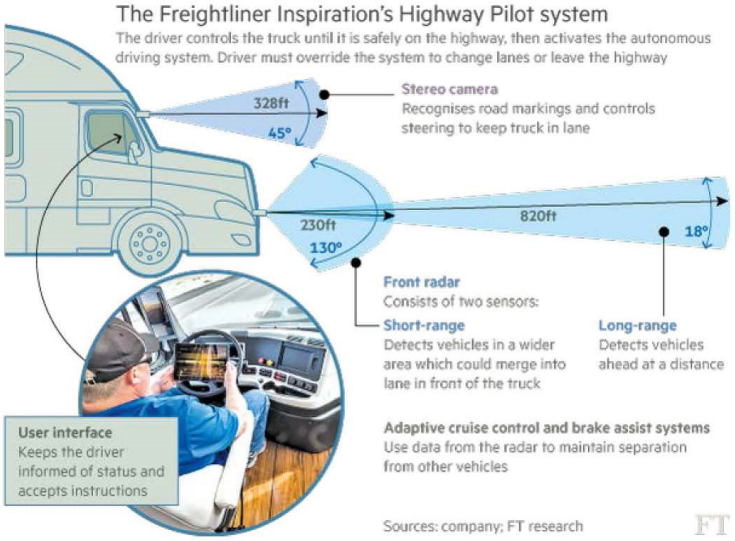
Neo Prime Solutions

Cyberspace and your car…

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

The Freightliner Inspiration's Highway Pilot system

The driver controls the truck until it is safely on the highway, then activates the autonomous driving system. Driver must override the system to change lanes or leave the highway



Stereo camera
Recognises road markings and controls steering to keep truck in lane

Front radar
Consists of two sensors:

Short-range
Detects vehicles in a wider area which could merge into lane in front of the truck

Long-range
Detects vehicles ahead at a distance

User interface
Keeps the driver informed of status and accepts instructions

Adaptive cruise control and brake assist systems
Use data from the radar to maintain separation from other vehicles

Sources: company; FT research

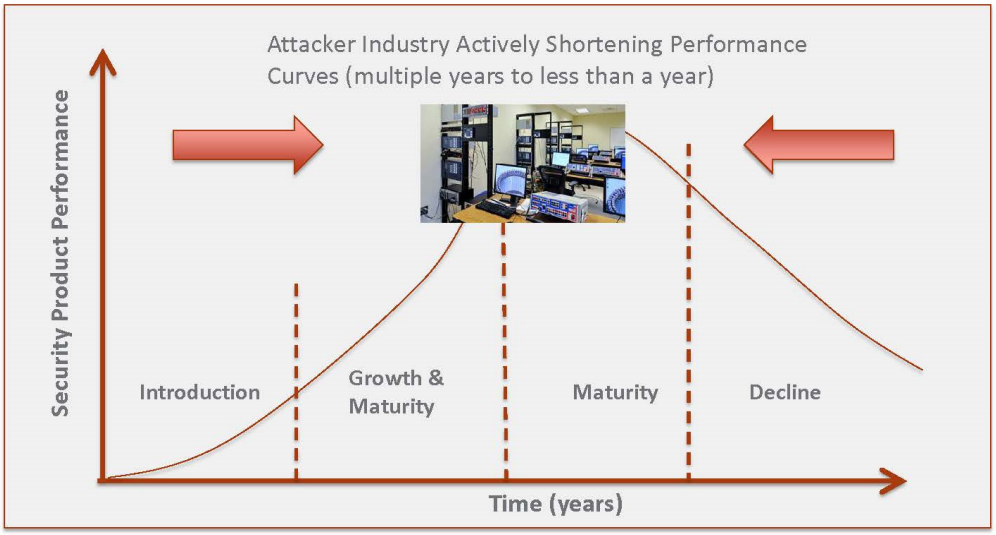
FT

7

Neo Prime Solutions

Trends of Security Products and their Lifecycle

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

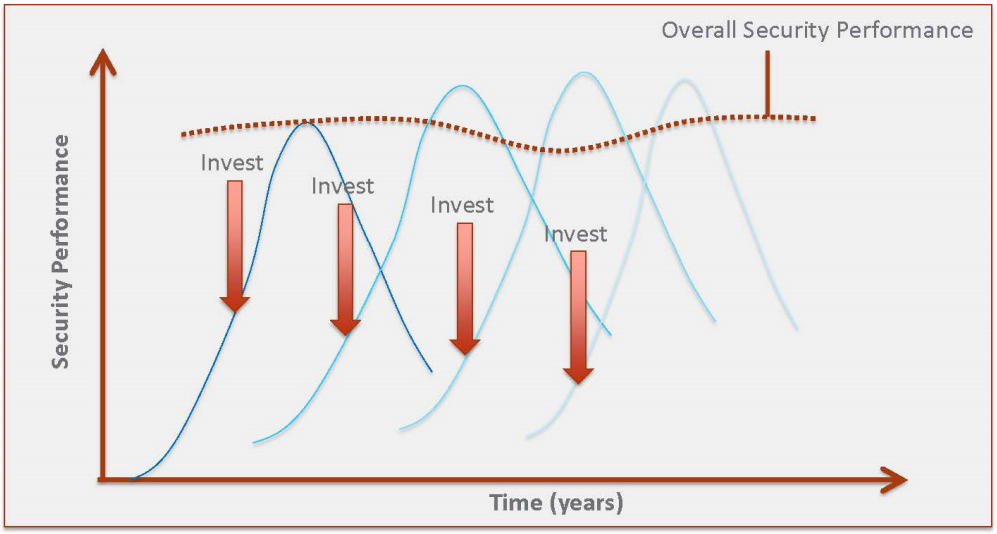


8

Neo Prime Solutions

Companies at High Risk Moving to Adopt Early, Adopt Often

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965



9

Neo Prime Solutions

Next Generation Security Controls Moving Towards Active Defense

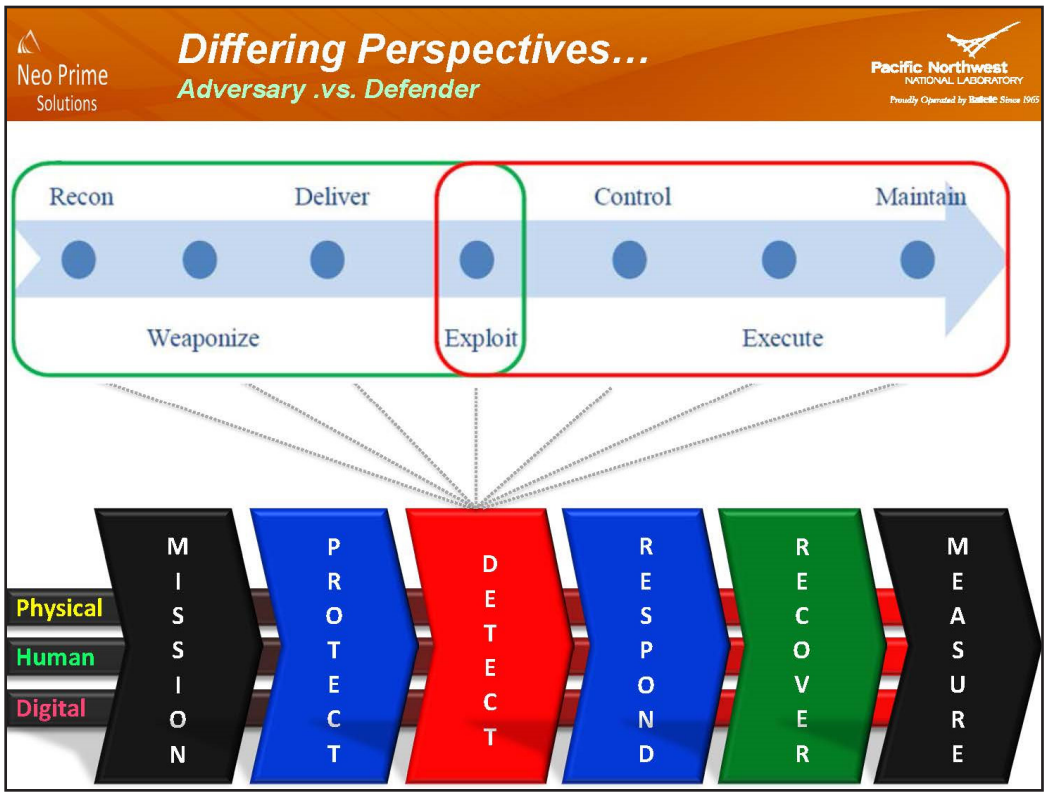
Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

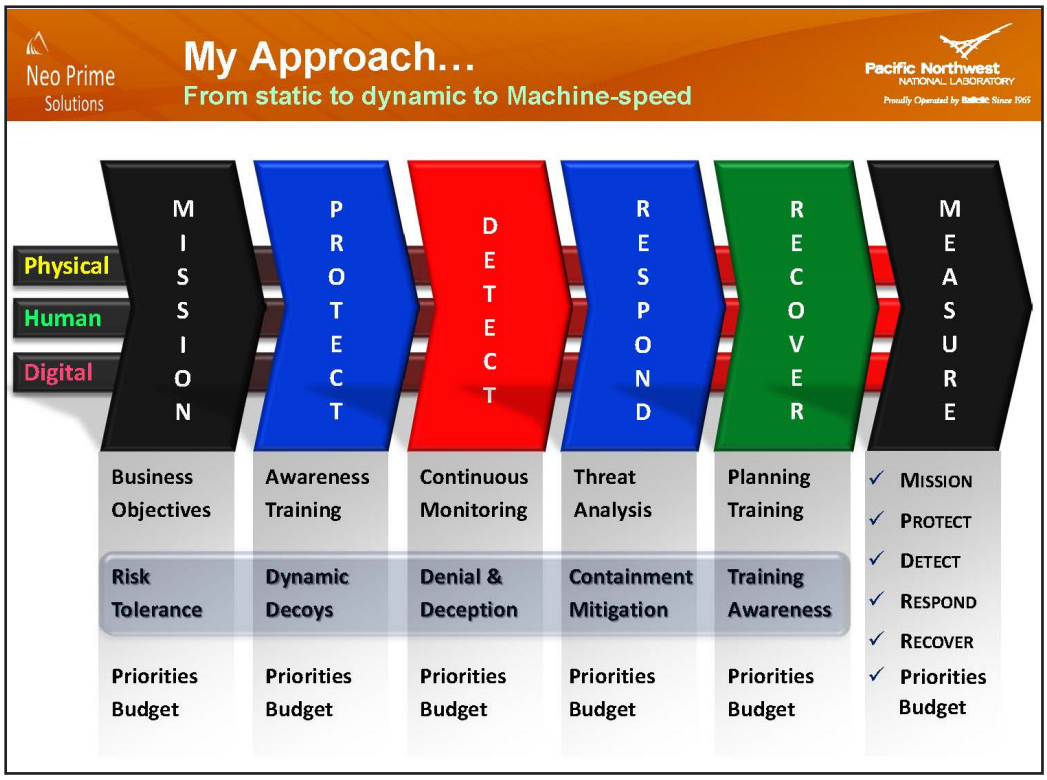
Current Model	Emerging Model
Signatures	Sandboxes
Protection	Isolation
Detection	Diversion
Physical	"Virtual"
Static	Dynamic & Deceptive

"Comprehensive protection requires an adaptive protection process integrating predictive, detective and response capabilities."

Neil MacDonald and Peter Fristbrook,
Gartner National Harbor Conference, June 23, 2014

10

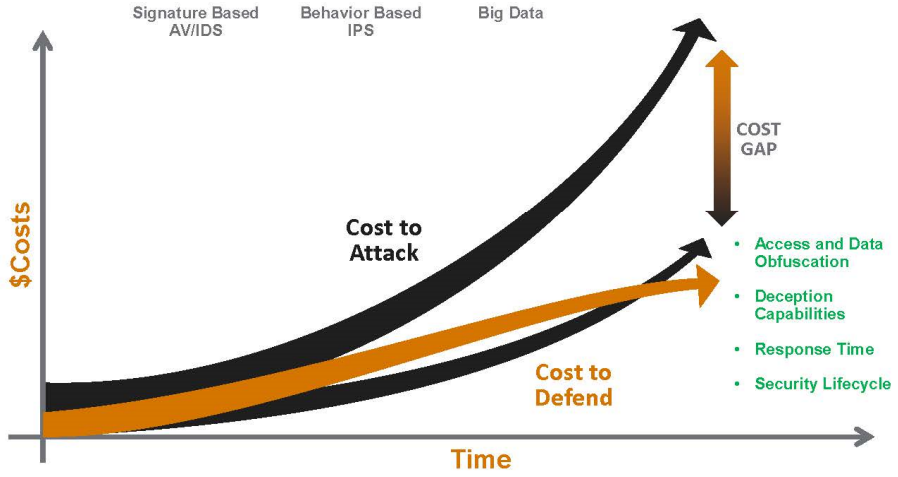

Neo Prime Solutions
Differing Perspectives…
Adversary .vs. Defender
Pacific Northwest NATIONAL LABORATORY
Recon
Deliver
Control
Maintain
Weaponize
Exploit
Execute
Physical
Human
Digital
MISSION
PROTECT
DETECT
RESPOND
RECOVER
MEASURE


Neo Prime Solutions
My Approach…
From static to dynamic to Machine-speed
Pacific Northwest NATIONAL LABORATORY
Physical
Human
Digital
MISSION
PROTECT
DETECT
RESPOND
RECOVER
MEASURE
Business Objectives
Awareness Training
Continuous Monitoring
Threat Analysis
Planning Training
Risk Tolerance
Dynamic Decoys
Denial & Deception
Containment Mitigation
Training Awareness
Priorities Budget
Priorities Budget
Priorities Budget
Priorities Budget
Priorities Budget
✓ Mission
✓ Protect
✓ Detect
✓ Respond
✓ Recover
✓ Priorities Budget

Neo Prime Solutions

Active Defense Value Proposition
Change Economics of Attack and Defense

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965



"The goal would be to deter future cyber attacks by changing the adversary's cost-benefit calculations."

- Center for a New American Security, Feb 2013

13

Neo Prime Solutions

Backup

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

14

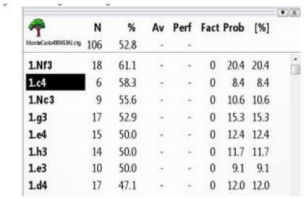
Active Defense: Bringing the House of Stanton to Cyber

Neo Prime Solutions

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Chess Risk Gaming Analysis

- Opponents Skill, Methods, Objectives
- Opportunity to Capture King
- Risk of Loss to Your King



	N	%	Av	Perf	Fact	Prob	[%]
	106	52.8	-	-			
1.Nf3	18	61.1	-	-	0	20.4	20.4
1.c4	6	58.3	-	-	0	8.4	8.4
1.Nc3	9	55.6	-	-	0	10.6	10.6
1.g3	17	52.9	-	-	0	15.3	15.3
1.e4	15	50.0	-	-	0	12.4	12.4
1.h3	14	50.0	-	-	0	11.7	11.7
1.e3	10	50.0	-	-	0	9.1	9.1
1.d4	17	47.1	-	-	0	12.0	12.0

Next Best Move?

Chess is Hard Enough Against a Skilled Opponent!

Now Imagine…
The Game Board, Pieces, and Objectives Change Over Time

Cyber Risk Gaming Analysis

- Opponents Skill, Methods, Objectives
- Opportunity to Prevent Movement
- Risk of Loss to Your Critical Asset

Next Best Move?

- Security Control Measure
- Security Process
- Organizational Change
- Communication Plan

15

Emerging Technology Still Face Strong Challenges

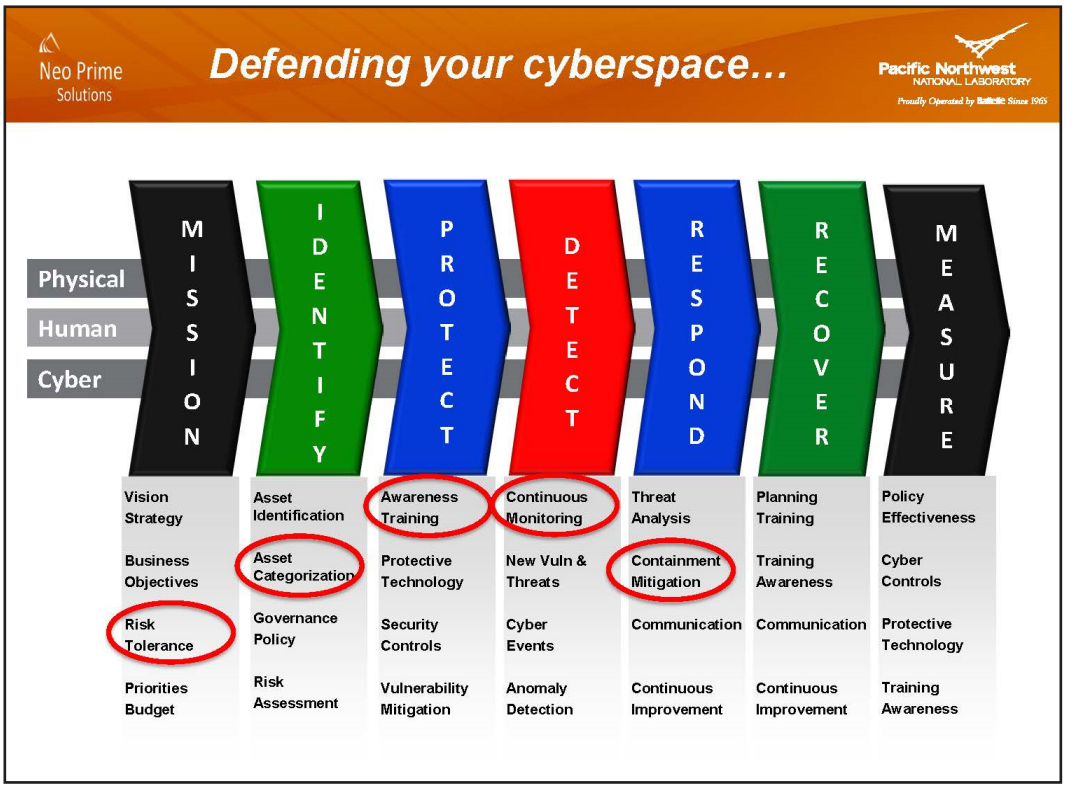
Neo Prime Solutions

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Technology	Challenges
1 Sandboxing and Detonation	• Short duration testing • Unrealistic environment
2 Containment and Isolation	• Lateral Propagation is key • Cannot determine Intent
3 Diversion and Obfuscation	• Currently Web Applications • Cannot determine Intent
4 VM based HIDS	• Visible HIDS shut down by attackers • Standard VM images are give away
5 Analytics and Threat Intelligence	• Need for clean baseline and data • Understanding propagation tactics

16


Cyber Kill Chain
1
RECONNAISSANCE
Harvesting email addresses, conference information, etc
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goal


Neo Prime Solutions
Defending your cyberspace...
Pacific Northwest NATIONAL LABORATORY
Physical
Human
Cyber
MISSION
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
MEASURE
Vision Strategy
Business Objectives
Risk Tolerance
Priorities Budget
Asset Identification
Asset Categorization
Governance Policy
Risk Assessment
Awareness Training
Protective Technology
Security Controls
Vulnerability Mitigation
Continuous Monitoring
New Vuln & Threats
Cyber Events
Anomaly Detection
Threat Analysis
Containment Mitigation
Communication
Continuous Improvement
Planning Training
Training Awareness
Communication
Continuous Improvement
Policy Effectiveness
Cyber Controls
Protective Technology
Training Awareness

Washington State Cybersecurity Summit 3: A Comprehensive Approach to Grid Security

Privacy, Public Disclosure and Information-Sharing—Finding the Balance

Joy Ditto, SVP Legislative & Political Affairs
American Public Power Association

February 29, 2016

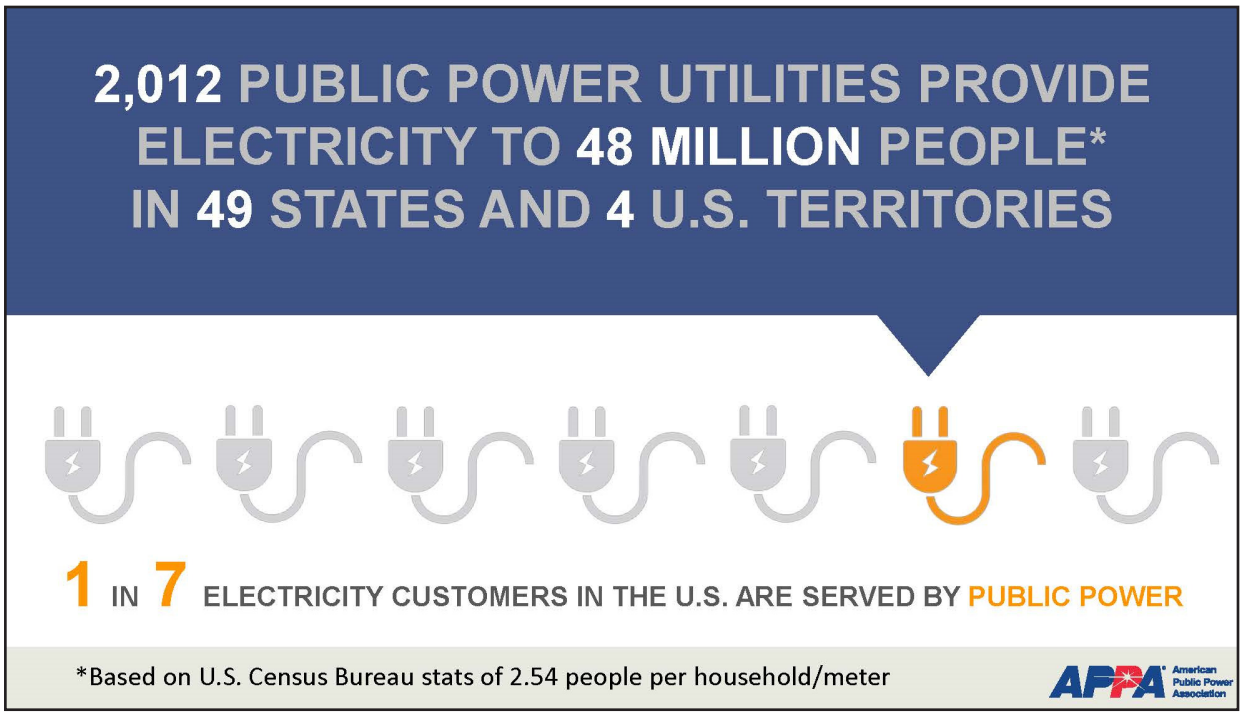
PUBLIC POWER REACH

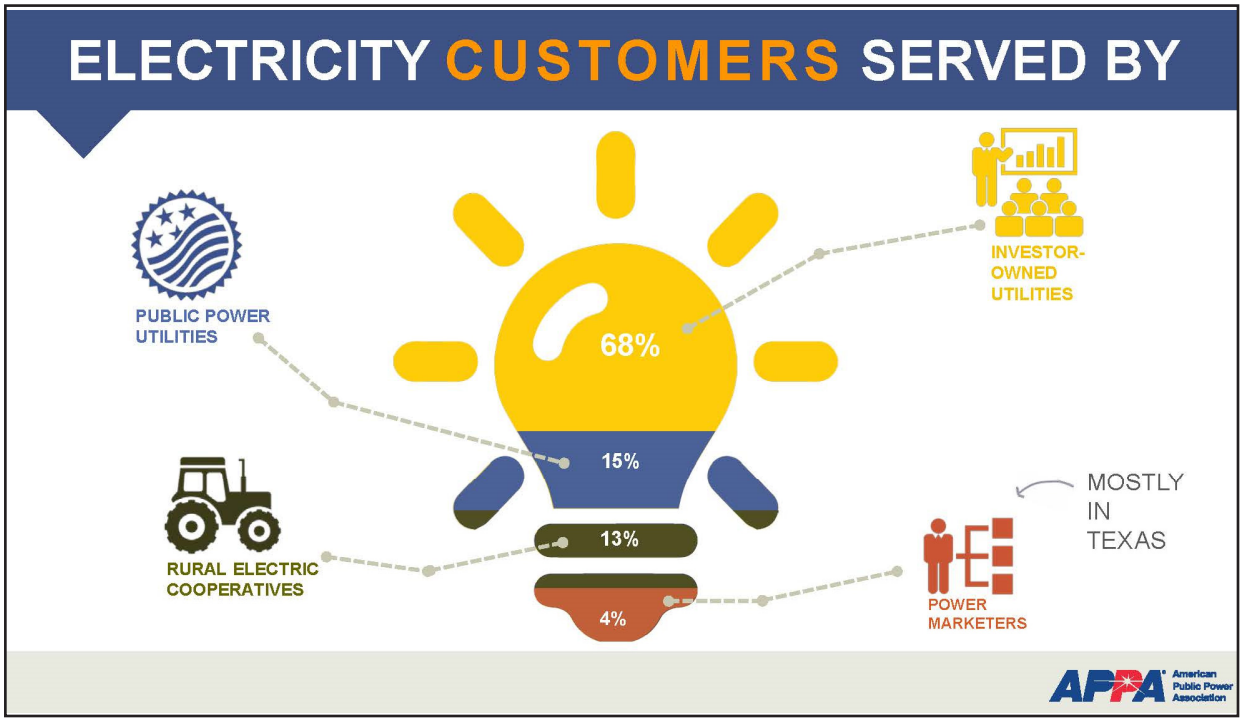
Public power's share of the U.S. electricity market

10% of generation

10% of transmission

16% of distribution


2,012 PUBLIC POWER UTILITIES PROVIDE ELECTRICITY TO 48 MILLION PEOPLE* IN 49 STATES AND 4 U.S. TERRITORIES
1 IN 7 ELECTRICITY CUSTOMERS IN THE U.S. ARE SERVED BY PUBLIC POWER
*Based on U.S. Census Bureau stats of 2.54 people per household/meter
APPA American Public Power Association


ELECTRICITY CUSTOMERS SERVED BY
PUBLIC POWER UTILITIES
68%
INVESTOR-OWNED UTILITIES
15%
RURAL ELECTRIC COOPERATIVES
13%
4%
POWER MARKETERS
MOSTLY IN TEXAS
APPA American Public Power Association

History of Info-Sharing & Grid Security Legislation

- **August 8, 2005 –** Energy Policy Act of 2005 includes amendment to Federal Power Act -- Section 215 establishing a regime for mandatory reliability standards (including cyber-security standards) for the North American bulk-power system.
- **December 2006** – Idaho Nation Lab Test of "Aurora" vulnerability
- **Early 2007** – some in industry alerted to vulnerability, but told to not share broadly
- **Spring 2007** -- alert more broadly disseminated to industry, but info not "actionable"
- **September 2007** – CNN shows video of Aurora vulnerability test
- **Fall 2007** – hearings on Capitol Hill question new NERC mandatory reliability standards regime
- **Fall 2007** – establishment of electric sector "cyber-coalition" (now grid security coalition)

APPA American Public Power Association

History of Info-Sharing & Grid Security Legislation (Cont.)

- **Fall 2007** – legislation developed in the House known as the GRID Act would have imposed additional standards on electric sector overriding the framework of Section 215. One piece industry supported was additional authority for FERC or DOE to use during presidentially declared emergency.
- **2010** – Despite industry opposition, GRID Act passes House, but not Senate.
- **2011-2012** – Cyber-security legislation developed in Senate giving DHS additional regulatory authority across industry sectors and duplicative of NERC standards. Electric sector opposed. Failed on the Senate floor in summer and fall 2012.

APPA American Public Power Association

History of Info-Sharing & Grid Security Legislation (Cont.)

- **2012-2015** – Cyber-security information-sharing legislation revisited and gaining support. Managed primarily via Intelligence Committees. Broad industry coalition -- including electric sector, and led by U.S. Chamber -- supports.
- **December 4, 2015** – President signs into law the Fixing America's Surface Transportation (FAST) Act, which includes several grid security provisions, including emergency authority for DOE.
- **December 18, 2015** – Cybersecurity Act included in Division N of H.R. 2029, the Consolidated Appropriations Act for FY 2016, signed into law on this date.

APPA American Public Power Association

Cybersecurity Act of 2015

- Title I of the Cybersecurity Act incorporates the Cybersecurity Information Sharing Act of 2015, and is relevant to electric sector. Key provisions include:
  - Mandatory development of procedures for sharing of cyber threat indicators (CTIs) and defensive measures (DMs) across the government and with industry.
  - Mandatory development of procedures for federal government to be able to receive information about CTIs and DMs.
  - Authorization for industry to share or receive information about CTIs and DMs with each other and with the federal government.
  - Limited liability protection for industry to share such information.

APPA American Public Power Association

Grid Security Provisions of FAST Act

- Defines critical electric infrastructure (CEI)
- Defines critical electric infrastructure information (CEII)
- Directs FERC, in consultation with DOE, to establish a process for designating and protection CEII
- Defines grid security emergency and grants DOE additional emergency authority to protect CEI.
- Exempts CEII disclosure under state sunshine laws.
- Directs DOE to explore development of strategic transformer reserve.

Implementation of Laws

- Electric sector already working together on implementation.
- New territory on information-sharing.
- Process for designating CEI & CEII at FERC important.

Cybersecurity Information Sharing: Foundational Elment of Risk Communication (Microsoft)

Microsoft

Cybersecurity Information Sharing: Foundational Element of Risk Management

Aaron Kleiner, Director, Industry Assurance & Policy Advocacy
Microsoft Global Security Strategy & Diplomacy

Information sharing: what is it?

Incidents

Details of attempted and successful attacks that may include a description of information lost, techniques used, intent, and impact. The severity of an incident could range from a successfully blocked attack to a serious national security situation.

Threats

Yet-to-be-understood issues with potentially serious implications; indicators of compromise, such as malicious files, stolen email addresses, impacted IP addresses, or malware samples; or information about threat actors. Threat information can help operators detect or deter incidents, learn from attacks, and create solutions that can better protect their own systems and those of others.

Vulnerabilities

Vulnerabilities in software, hardware, or business processes that can be exploited for malicious purposes.

Mitigations

Methods for remedying vulnerabilities, containing or blocking threats, and responding to and recovering from incidents. Common forms of such information include patches to plug vulnerabilities, antivirus updates to stop exploitation, and directions for purging malicious actors from networks.

Situational awareness

Information that enables decision-makers to respond to an incident and that may require real-time telemetry of exploited vulnerabilities, active threats, and attacks. It could also contain information about the targets of attacks and the state of critical public or private networks.

Best practices

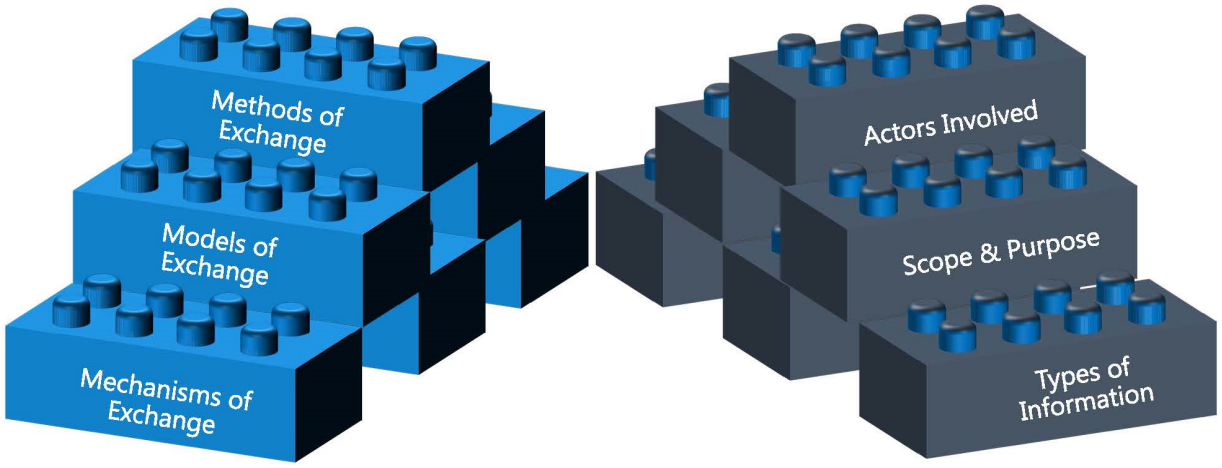
Information related to how software and services are developed and delivered, such as security controls, development and incident response practices, and software patching or effectiveness metrics.

Strategic analysis

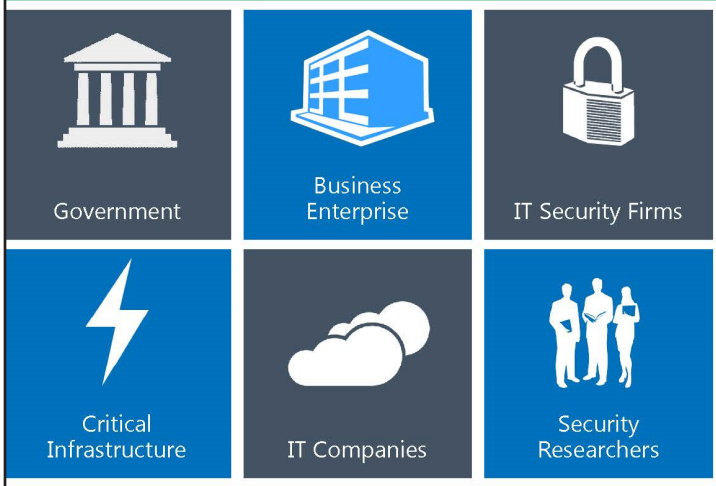
Gathering, distilling, and analyzing many types of information to build metrics, trends, and projections. It is often blended with projections of potential scenarios to prepare government or private sector decision-makers for future risk.

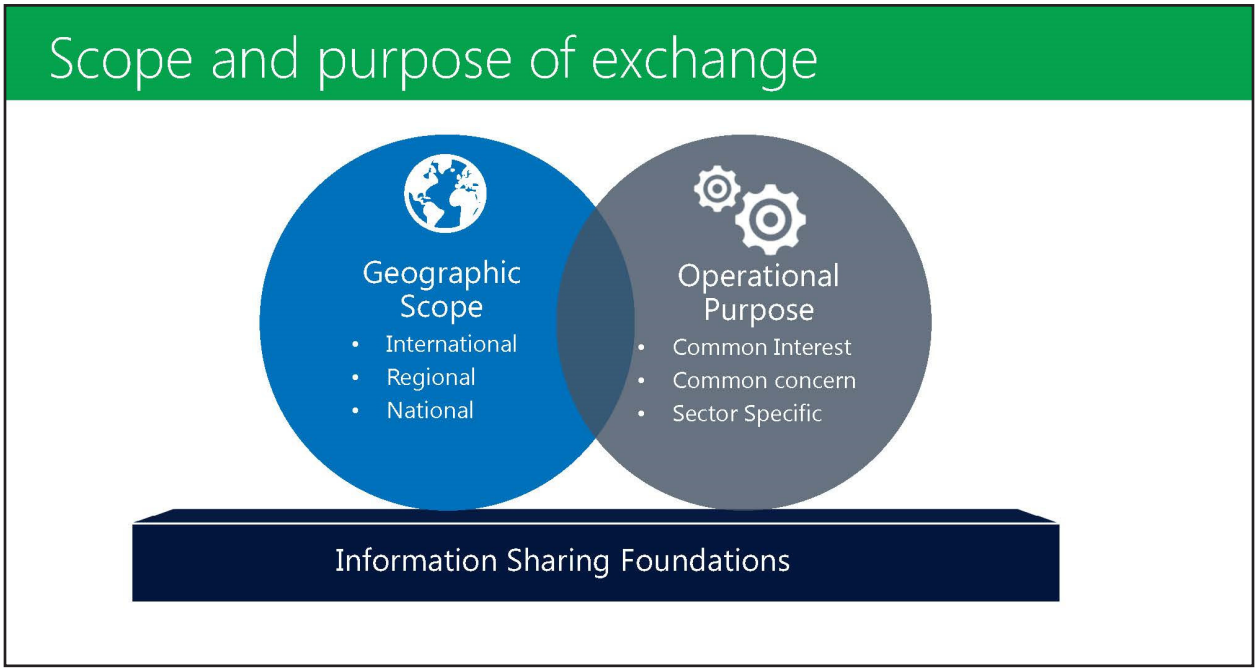
Who should share information?
What should be shared?
When should it be shared?
What is the quality and utility of what is shared?
How should it be shared?
Why is it being shared?
What can be done with the information?

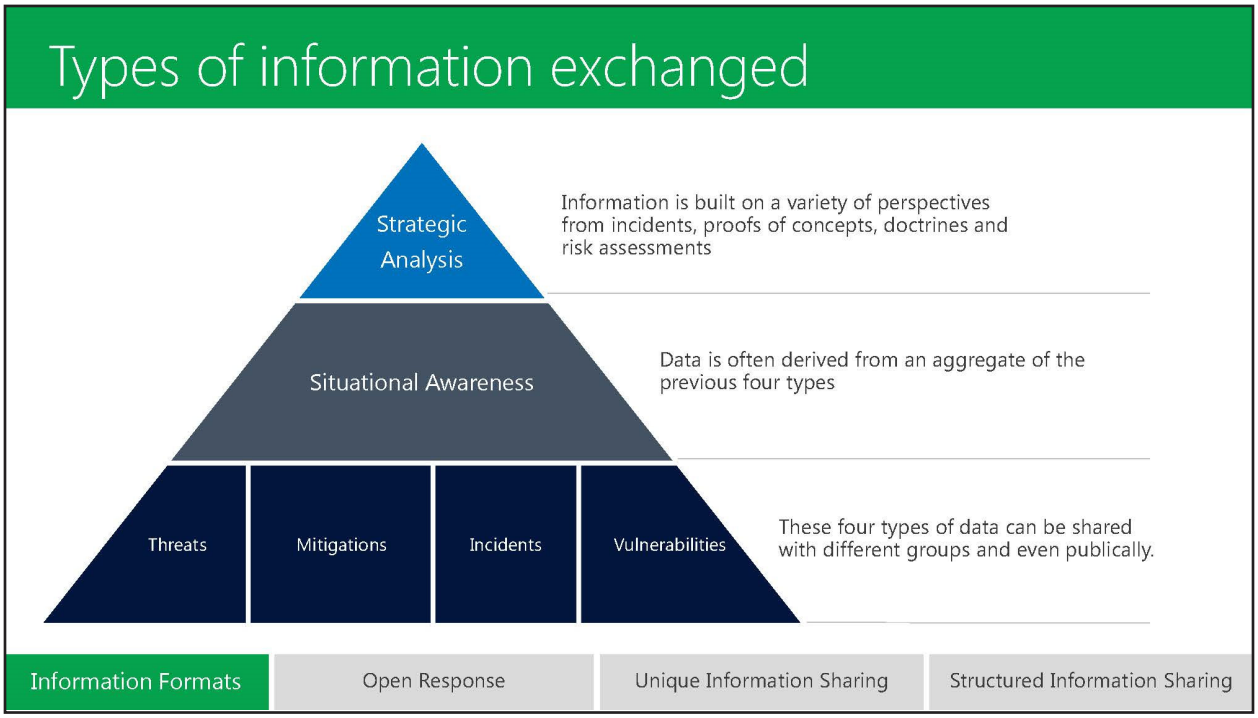
Information sharing: sustainable building blocks



Actors involved in information sharing




Scope and purpose of exchange
Geographic Scope
• International
• Regional
• National
Operational Purpose
• Common Interest
• Common concern
• Sector Specific
Information Sharing Foundations


Types of information exchanged
Strategic Analysis
Information is built on a variety of perspectives from incidents, proofs of concepts, doctrines and risk assessments
Situational Awareness
Data is often derived from an aggregate of the previous four types
Threats
Mitigations
Incidents
Vulnerabilities
These four types of data can be shared with different groups and even publically.
Information Formats
Open Response
Unique Information Sharing
Structured Information Sharing

Models of information exchange

Voluntary Exchange Models

- The richest and most valuable exchange that exists in the cybersecurity ecosystem.
- The most effective scenarios for sharing information are be company–to-company exchanges, in addition to the collective responses to large incidents or threats.
- Governments must consider how to deepen trust, provide a collective benefit while minimizing reputational risk, and respond to a clearly articulated national incident

Mandatory Disclosure Models

- Mandatory incident reporting is inherently one-directional and does not, on its own, improve operational security or response.
- Governments increasingly require the disclosure of security event information to regulators and other government authorities, investors, or impacted individuals.
- It is critical that governments do not conflate incident reporting or their own need for situational awareness with information sharing between trusted parties.

Principles for Incident Reporting Policies

1. Should be aligned to clearly defined outcomes, such as public safety, response coordination, or improving security defenses.
2. Should be flexible and commercially reasonable and should leverage commonly accepted approaches and international standards, where possible, avoiding incompatibility.
3. Should also balance the risks and benefits associated with publishing incident details.
4. Timelines for reporting incidents should be mapped to specific outcomes and not arbitrarily chosen.
5. Should be supported with research and development in both the public and private sectors.

Methods of information exchange

Formalized exchanges	Security clearance-based exchanges	Trust-based exchanges	Ad hoc exchanges

Recommendations for developing an information sharing framework

Commitment, trust, cooperation, and a clear sense of value required.

Develop an overarching strategy for information sharing and collaboration.	Spur voluntary information sharing by building interpersonal relationships.
Design with privacy protections in mind.	Require mandatory information sharing only in limited circumstances.
Establish a meaningful governance process.	Make full use of information shared, by conducting analyses on long-term trends.
Focus sharing on actionable threat, vulnerability, and mitigation information.	Encourage the global sharing of best practices.

Microsoft

Proudly Operated by **Battelle** *Since 1965*

September 2016

PNNL-25715