Washington State Cybersecurity Summit 2018

A COMPREHENSIVE APPROACH TO GRID SECURITY

Summary Report from the May 21, 2018 Workshop
Seattle Tacoma International Airport, Seattle, Washington

PNNL-28187

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)

PNNL-28187

WASHINGTON STATE CYBERSECURITY SUMMIT 2018:

A COMPREHENSIVE APPROACH TO GRID SECURITY

Summary Report from May 21, 2018, Workshop at Seattle-Tacoma International Airport Seattle, Washington, USA

Presented by Snohomish Public Utility District, Pacific Northwest National Laboratory, Washington National Guard, Port of Seattle, Puget Sound Energy, Seattle City Light, Tacoma Public Utilities, T-Mobile, Trovares Inc., Washington State Military Department, Washington State Office of the Chief Information Officer, Washington Utilities and Transportation Commission.

Authored by: Jessica Matlock (SnoPUD), Ann Lesperance (PNNL), Gordon Matlock (Trovares, Inc.), Maren Disney (PNNL)

PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

PAGE INTENTIONALLY LEFT BLANK

SUMMARY

On May 21, 2018, the Snohomish County Public Utility District (SnoPUD) and the U.S. Department of Energy's Pacific Northwest National Laboratory (PNNL) co-hosted the fourth Washington State Cybersecurity Summit to focus on the cybersecurity threats and lessons learned nationally and within the State of Washington. The summit aimed to broaden the state's perspective by engaging public and private experts on cybersecurity best practices for critical infrastructure providers.

The 'by-invitation-only event' was coordinated by SnoPUD and PNNL in partnership with the Washington National Guard, Port of Seattle, Puget Sound Energy, Seattle City Light, Tacoma Public Utilities, T-Mobile, Trovares Inc., Washington State Military Department, Washington State Office of the Chief Information Officer, and Washington Utilities and Transportation Commission.

Jessica Matlock (SnoPUD) opened the event by reiterating the workshop's goal to bring together a cross section of public and private experts to examine challenges and opportunities in cybersecurity and critical infrastructure.

Guest speaker **Courtney Gregoire (Port of Seattle)** spoke briefly about the potentially drastic impacts of a cyberattack to the region and the need to think holistically about solutions. This was followed by a pre-recorded video presentation from **Maria Cantwell (U.S. Senate)**, who noted that Washington continues to demonstrate its ability to lead the country in developing cybersecurity solutions and that it is home to a unique ecosystem that serves as a leading model for the entire nation.

Featured guest speaker **Guy Palumbo (Washington State Senate)** discussed the future of cybersecurity from both a private and public perspective and the opportunity within the summit to explore what can be done differently in state-level cybersecurity efforts.

Keynote speaker **Bret Arsenault (Microsoft Corporation)** discussed a security world view around risks and opportunities and outlined how his team simplifies the strategy for security at Microsoft to create clarity, generate energy, and deliver success.

The remainder of the day's agenda featured a series of presentations exploring:

- National perspectives on the impact of the Internet of Everything on network security
- Chief Information (Security) Officers' cyber challenges, vulnerabilities, and security postures
- Cybersecurity in investor-owned and regulated utility providers
- Industry perspective on disruptive technologies, automation, and blockchain.

Ann Lesperance (PNNL) concluded the day's discussions, outlining four emerging themes:

- Information sharing – How do we share more effectively? What do we share? What are the implications?
- Workforce development – How do we build and maintain a robust pool of cybersecurity professionals?
- Exercises and training – How do we build something that brings public and private partners together to look at mutual aid, resource typing, etc.?
- Resources – How do we inventory what resources and capabilities we have and connect with each other?

Participants were invited to sign up to indicate their interest in working groups and/or following up on these focus areas in the near future.

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

ACKNOWLEDGEMENTS

SnoPUD and PNNL would like to acknowledge and thank the event facility host, the Seattle-Tacoma International Airport, and participants who attended and actively engaged in this summit, including:

Alaska Airlines
Bonneville Power Administration
Deloitte
Homestreet Bank
Microsoft Corporation
Port of Seattle
Puget Sound Energy
Seattle City Light
Tacoma Public Utilities
The Boeing Company
T-Mobile
Trovares Inc.
Washington National Guard
Washington State Military Department
Washington State Office of the Chief Information Officer
Washington State Senate
Washington Utilities and Transportation Commission

INTRODUCTION

On May 21, 2018, the Snohomish County Public Utility District (SnoPUD) and the U.S. Department of Energy's Pacific Northwest National Laboratory (PNNL) co-hosted the fourth annual Washington State Cybersecurity Summit, bringing together multidisciplinary leaders to focus on the cybersecurity threats and lessons learned nationally and within the State of Washington. The summit aimed to broaden the state's perspective by engaging public and private experts on cybersecurity best practices and opportunities for critical infrastructure providers.

The 'by-invitation-only' event was coordinated by SnoPUD and PNNL in partnership with the Washington National Guard, Port of Seattle, Puget Sound Energy, Seattle City Light, Tacoma Public Utilities, T-Mobile, Trovares Inc., the Washington State Military Department, Washington State Office of the Chief Information Officer, and Washington Utilities and Transportation Commission.

The discussions outlined in this report are the opinions and perspectives of the speakers as individuals and not an endorsement or representation of their organizations.

OPENING REMARKS

Jessica Matlock (SnoPUD) welcomed participants to the event, providing highlights from the previous years' meetings. Ms. Matlock shared that the event was launched in 2013 based on an emerging focus within the state to enhance cybersecurity and inform policy makers on how to defend against cyberattacks. The event has maintained one goal: to foster engaging discussion about how to enable more resilient cybersecurity and a stronger cybersecurity workforce.

Port Commissioner Courtney Gregoire (Port of Seattle) spoke about the potentially drastic impacts of a cyberattack to the region and the need to think holistically about solutions. She shared a brief overview of the Port of Seattle,

Port Commissioner Courtney Gregoire (Port of Seattle) delivers opening remarks.

highlighting its recent growth as one of the fastest growing ports in the nation. They are working at the nexus of technology to connect supply chains of businesses nationwide while also investing in ways to accommodate the increased traffic and travel, now and in the future. Amid these opportunities, they also seek to enhance their resilience to respond to and recover from a catastrophic event.

Ms. Gregoire noted the Port's focus on enhancing their visibility, automation, security standards, and tool sets. This effort has included exploring cloud solutions where appropriate, integrating their toolsets into control system environments, and increasing involvement in national exercises and partnerships. Ms. Gregoire concluded by emphasizing the need to improve and incentivize infrastructure information sharing thus enabling others to protect security information.

> "We want to continue to help make sure Washington leads by example nationally."
>
> Commission President Courtney Gregoire, Port of Seattle

Via a pre-recorded video, **Maria Cantwell (U.S. Senate)** spoke about the importance of cybersecurity and the need for the state and its stakeholders to think critically about protecting its infrastructure. She noted that Washington

Guy Palumbo (Washington State Senate) speaks about public and private partnerships.

continues to demonstrate its ability to lead the country in developing cybersecurity solutions; it is home to a unique ecosystem that serves as a great model for the entire nation. With its national laboratories, National Guard, public utilities, outstanding academia, and leading private sector effort on cybersecurity, these entities come together to prepare, act, and respond to cybersecurity threats. As Washington continues to lead in cybersecurity (and the rest of the nation looks onward), the nation can better meet its infrastructure challenges.

> "The only way to effectively combat cyber risks is an all hands on deck approach."
>
> U.S. Senator Maria Cantwell (via video)

Following Senator Cantwell, **Guy Palumbo (Washington State Senate)** challenged the audience to use the summit as an opportunity to explore what can be done differently in state-level cybersecurity efforts. He reflected on previous summits, noting that it is from events like this that good ideas bubble up to the legislature. Senator Palumbo encouraged participants to work together to combine their technical expertise and bring forth agendas and good ideas to help enable change in cybersecurity.

KEYNOTE SPEAKER

Bret Arsenault (Microsoft Corporation) reflected on cybersecurity breaches in recent history then opened the discussion around a security world view of risks and opportunities. He noted that the vast opportunities facilitated by cloud technology, the internet, and advanced software and devices also open doors to risks. One risk he highlighted is what he calls 'digital xenophobia,' the varying global regulations with a preference for keeping data within a country. In today's changing environment, he suggested the need to look at security in a comprehensive manner, to enable a transformation in digital security. He highlighted how Microsoft works to enable this transformation through a comprehensive platform, unique intelligence, and broad partnerships.

Mr. Arsenault outlined three leadership principles and practices at Microsoft: Create Clarity, Generate Energy, and Deliver Success. The principle around creating clarity is the guiding thought that led him to develop the security strategy currently implemented at Microsoft. This approach has helped executives and colleagues around the company understand the topic more clearly. This clarity has also helped the company develop a program that enables a risk-based approach for managing information security, physical security, and customer and employee privacy-related matters.

During a question and answer segment with the audience, Mr. Arsenault spoke more about risks and challenges. In a question relating to privacy, he noted that companies need to take a holistic, global view.

> "How you recover, how resilient you are, is as important as how you protect yourself."
>
> Bret Arsenault, Microsoft Corporation

Following the keynote address, participants from private and public partners presented on a series of focus areas, including:

- National perspective on the impact of the Internet of Everything on network security
- Chief Information (Security) Officers' (CIO or CISO) cyber challenges, vulnerabilities, and security postures
- Cybersecurity in investor-owned and regulated utility providers
- Industry perspective on disruptive technologies, automation, and blockchain.

NATIONAL PERSPECTIVE

Topic: What are the threats and lessons learned and how do we protect the Internet of Everything and its impact on security of all networks?

- *Facilitator*: **Gordon Matlock**, Chief Strategy Officer, Trovares Inc.
- **Bill Boni**, Senior Vice President of Information Security, T-Mobile
- **Col. Gent Welsh**, Commander 194th Wing, Camp Murray

Bill Boni (T-Mobile) emphasized the need to make critical infrastructure assurance a priority. While organizations vary widely in their ability to respond to an event, few have actually trained together, integrating across entities. Mr. Boni suggested creating a training curriculum that leverages cyber ranges, academic and industry domains, and exercises will build confidence that organizations can execute when called upon. Effective public-private partnering could further secure the right skillsets on both the civilian and military side.

Col. Gent Welsh (Commander 194th Wing, Camp Murray) reflected on the emerging challenge that with today's technological capabilities, essentially every device can be weaponized or misused to fundamentally disrupt the economy and citizens' daily lives. He applauded the summit for bringing together so many partners—military, industry, and academia—to tackle this emerging threat. Col. Welsh noted that, from a military employer/industry perspective, bringing personnel from industry to the National Guard helps raise technical expertise while military personnel bring to industry a sophisticated understanding of the adversary.

Bret Arsenault (Microsoft Corporation) delivers the keynote address.

During the question and answer session, the presenters were posed the question of how to enable the public-private training opportunities prevalent during the day's discussion. The speakers noted that Washington State has been at the forefront of this challenge, having assembled a cybersecurity emergency management plan, joint industry-military red team exercises, etc. They emphasized the need to move the needle by expanding current models, implementing incentives to encourage information sharing, creating case studies, and engaging the legislature.

The electric grid is becoming decentralized with more distributed things attached on the consumer side and industry and third parties. The speakers were asked to identify one critical thing utilities could focus on in terms of supply chain and protecting those devices while allowing the utility to protect itself.

> "The bad guy of the future isn't after your credit card. He's after your light switch."
>
> Colonel Gent Welsh

Mr. Boni suggested having a strong regulatory structure can allow an operator to connect to the device and to research and refine networks to prevent failure. Col. Welsh also emphasized the need to balance access and reliability with security and automation.

The speakers also addressed workforce development, championing the need to expose students to career opportunities earlier in their academic careers. The University of Washington–Bothell internship program and similar efforts were highlighted for transforming students with diverse backgrounds into cybersecurity professionals. Immersive opportunities like this deepen the worker pool immediately but also fill the pipeline long-term, giving participants both classroom and on-the-job training fit for the cybersecurity mission.

The session concluded with a discussion focused on timely information sharing. Participants cited the positive work of PRISM, Cyber Incident Response Coalition and Analysis Sharing (or CIRCAS), and Fusion Centers. Speakers discussed pilots in progress to create local and statewide cybersecurity incident reporting but noted the consistent challenges with standing up cyber emergency response capabilities, including funding, resource typing, and indemnification.

CHALLENGES FACED BY CIO/CISO

Topic: What is unique and interesting that you are doing regarding cyber? What has been working well or not? What are your approaches to validating cyber vulnerabilities? What are you doing to improve their security posture? What advice do you suggest?

- *Facilitator:* **Selena Tonti,** CISO, Port of Seattle
- **Nathaniel Callens,** CISO, Alaska Airlines
- **Paul Dodd,** Information Security Chief Strategist, The Boeing Company
- **Dave Wolf,** CISO, Homestreet Bank
- **Ben Berry,** Information Technology and CIO, Bonneville Power Administration

(Left to right) Bill Boni (T-Mobile), Col. Gent Welsh (Commander 194th Wing), and Gordon Matlock (Trovares, Inc.) discuss national perspectives on the Internet of Everything and network security.

Facilitator **Selena Tonti (Port of Seattle)** posed to the CIO/CISO panel questions about the cybersecurity challenges their organizations face. Below is a summary of the dialogue.

What keeps you up at night? How do you prioritize?

- Getting cybersecurity done fast enough and integrated enough. Making the case of why we need to do it.
- Knowing you were better today than you were yesterday. If we are becoming better at detecting and recovery from threats, we are being successful.
- Keeping pace if developers are building faster than we can build solutions. To change fundamentally, we need regulation that helps the supply chain, etc.
- Understanding how your technology is being used, your customer expectations, and where you should invest or not invest because it does not align to your strategy.
- Prioritizing, understanding the base building blocks, and making sure you build what you want.

> "How do you effectively know you were better today than you were yesterday? We're always going to have a list of things we didn't get to. As long as we check those things out and become better at detecting threats and recovering from them, we are being successful."
>
> Nathaniel Callens, Alaska Airlines

How do you help determine what is important?

- Pick one standard. Depending on maturity, an organization may look at fewer or more controls, but there is no need to use all the controls or all the frameworks. Start with the top five controls on the list.
- Determine the most valuable task. Invite staff to compile tasks then sort by value.

Panelists during the CIO/CISO discussion on current cybersecurity challenges.

Where does risk management fall in your organization relative to cyber? Are you taking on the risk management function?

- Define the difference between proper risk management and security operations. Many learn about risk management on the job.
- Join an analyst team with security experience to engage diverse skill sets.
- Risk management is an area where there is a lack of understanding in the information security world—continue learning and adapting to become more of a partner with risk organizations on a team.

Standards are often considered a playbook for an offensive attack. Would you agree?

- Consider the role of compliance when setting standards. If your threat model is focused on compliance, you are treating your auditor as your adversary.
- Look at governance, risk, and compliance. To understand risk, we must understand the business, which entails working with the audit committee.
- Conduct due diligence in cybersecurity (risk frameworks) and intertwine with business risk coming from the customer.
- Do not work to check the box; work toward protecting things. Do not silo risk management and risk discussions; engage with the cybersecurity side of your organization.
- Educate end users, customers, etc., and identify avenues that will help customers better understand cybersecurity.

You have different, diverse environments. What is most important for the next year or beyond?

- Mission-critical systems for the grid.
- Moving from data centers to the cloud.

For those of us with smaller information technology groups, where do we start?

- Invite your counterparts for lunch. Talk to other districts. Build relationships.
- Reach out to your own various lines of business. Understand how they do their job and what the dependencies are to make their process function. If you do not understand the value chain in your business model, it will be a failure for you to actually protect it.
- Join Information Sharing Analysis Centers (ISACs). For example, the National Defense ISAC conducts semi-annual engineering summits.
- Connect with federal intelligence communities and groups.
- Team with other power marketing agencies and national laboratories to conduct data calls together and share information.

What information are you receiving (or not) that is valuable?

Participants indicated they find value in receiving:

- Real insight and comparison information. There is value in strong nondisclosure so that answers are legally protected.
- Threat data, threat or malware occurrences, from assets in the field.
- Job expectations for cybersecurity. Integrate cybersecurity into every position. If it is everyone's responsibility, something should be written in the job description.
- Ways to bring outsiders in. Look outside of the information technology or normal cybersecurity pool—diverse backgrounds bring diverse perspectives.

Regarding what they do not find valuable, participants indicated a desire for less information about attribution, noting that the focus should be on whether protecting customers' information and ensuring infrastructure is in place and sustained.

Chief Information (Security) Officers from Port of Seattle, Alaska Airlines, Boeing, Homestreet Bank, and Bonneville Power Administration discuss challenges in cybersecurity.

"If [cybersecurity] is everyone's responsibility, there should be something written in the job description."

Ben Berry, Bonneville Power Administration

WASHINGTON UTILITIES AND TRANSPORTATION COMMISSION

Topic: An overview of how the Washington Utilities and Transportation Commission (UTC) considers cybersecurity in its role as a regulator of investor-owned utilities

- **Ann Rendahl,** Commissioner, Washington UTC

Ann Rendahl (Washington UTC) shared a brief overview of the UTC and discussed the role of cybersecurity in investor-owned utilities, including how the UTC evaluates the reliability of regulated utilities. She addressed cyber and emergency preparedness and her work with energy regulators nationally and internationally in evaluating utility cybersecurity.

Ms. Rendahl shared the role of state commissions and standards in ensuring reliability and compared state-level and North American Electric Reliability Corporation standards. As she noted, state public service commissions are responsible for ensuring utilities provide safe and reliable service to customer at rates that are fair, just, reasonable, and sufficient. The commissions can require utilities to make improvements to ensure safe and adequate service, but it depends on the agency's statuary authority.

Ann Rendahl (Washington State UTC) speaks about the role of cybersecurity in investor-owned utilities.

She spoke about the Washington UTC's cybersecurity focus, including:

- Reviewing national guidelines on cybersecurity
- Setting policy for collecting sensitive information and developing guidelines for reviewing utility cybersecurity and critical infrastructure prevention and planning efforts
- Conducting annual meetings to explore utility cybersecurity practices
- Establishing best practices for regulated companies
- Meeting with cybersecurity partners
- Conducting tabletop exercises and testing.

Ms. Rendahl highlighted some of the UTC's cybersecurity strategy and partnerships (including the Emergency Management Division, National Guard, U.S. Department of Justice, FBI, U.S. Department of Commerce, PNNL, University of Washington, and others) as well as the work of the National Association of Regulatory Utility Commissioners (NARUC), which has an international program focused on regulatory issues and support to different countries and regions. NARUC also created a cybersecurity primer and online portal.

> "What we have in Washington has been effective in the different services working together—not being afraid of going outside your domain or being afraid someone is going to take over your realm."
>
> Ann Rendahl, Washington Utilities and Transportation Commission

Ms. Rendahl also shared her experiences engaging regulators and efforts being explored by other countries, including efforts aimed at harmonizing and coordinating cross-border electricity trading frameworks. She has met with staff and commissioners from other countries dealing with more intense and physical threats but noted all face essentially the same cybersecurity threat.

During the question and answer session, Ms. Rendahl further discussed her experiences with organizations nationally and abroad. She noted some countries had similar public records requirements, whereas some countries did not want to ask for information or some cannot trust digital information they have in their remote systems.

Regarding how to incentivize people toward a productive path, Ms. Rendahl shared that her organization approached it in a collaborative way by sharing best practices and inviting the FBI to meetings to share information about the Fusion Center, among other approaches. She noted that as more utilities have their cybersecurity groups tied into their information and operational technology groups, they may become more responsive and less confrontational.

DISRUPTIVE TECHNOLOGIES, SETTING THE STAGE, OPPORTUNITIES AND CHALLENGES

Topic: A big picture perspective on disruptive technologies (e.g., depth, breadth, pace of innovation) and what it means from a security perspective).

- *Facilitator:* **Jodie Ryan,** Senior Manager, Threat Intelligence, T-Mobile
- **Michael Mylrea,** Manager, Cybersecurity and Energy Technology Electricity Infrastructure, PNNL
- **Sudharma Thikkavarapu,** Sr. Manager, Cybersecurity Transformation, T-Mobile
- **Prakash Santhana,** Managing Director, Cyber Risk, Deloitte

Michael Mylrea (PNNL) spoke about the value of integrating cyber and physical assets, noting the potential impacts to energy and but to transportation and beyond. How do we optimize and make systems more resilient? Michael encouraged a more holistic approach, citing efforts at PNNL focused on cyber resilience.

He cited the need to better inventory risks and understand emerging challenges and opportunities.

> "The weaving together of cyber and physical assets has created new value, new prosperity, new jobs, new wealth—but also new challenges. What secures you today could be very different tomorrow."
>
> Michael Mylrea, Pacific Northwest National Laboratory

Sudharma Thikkavarapu (T-Mobile) presented "Shifting Security Left through Automation and Orchestration." He spoke about the transformational journey and changing norms in automation. He shared the value of being CALM (Calm, Automation, Lean, and Measurable):

- **C**ulture – He noted the changing tides in organizational culture, reiterating the value of finding someone not necessarily with cybersecurity experience but with the willingness to learn and passion to drive it.
- **A**utomation – He emphasized the value of the application programming interface (API), and that it must be consumable, stating that if we cannot deliver capability in an API, everything we drive must be an API.
- **L**ean – He noted that small themes can deliver solution-based capabilities with greater impact across the organization. Where processes can potentially create laziness, workflow engines can allow users to move and shift.
- **M**easurable – He emphasized the value of measurable metrics and data-driven security, noting that without data, you cannot effectively focus on security.

Finally, **Prakash Santhana (Deloitte)** presented "Blockchain: Practical applications and why does it matter so much to us?" Mr. Santhana opened the discussion by defining *blockchain* as

(Left to right) Panelists from Deloitte, PNNL, and T-Mobile discuss the challenges and opportunities of distruptive technologies.

a "… value transfer protocol that transfers value between computers connected on the internet without the need for a central intermediary." He provided a brief history back to the early 1990s and then provided a brief overview of the blockchain protocol, comparing it to typical credit card networks. Mr. Santhana summarized the most commonly praised aspects of the blockchain are its:

- Disintermediation of entities or processes
- Audit trail
- Immediate settlement.

During the question and answer session, the speakers reiterated the value of skills sets, taking a holistic approach in which multidisciplinary partners are a part of the solution, and cross-organizational training. Additionally, they spoke briefly about the challenges of identity management, protection of cyber-physical assets, and emerging trends such as autonomous vehicles.

> "We think technology and threats are increasing exponentially—but they are linear. The future is artificial intelligence and machine learning where we can make a tremendous impact in making decisions much quicker."
>
> Sudharma Thikkavarapu, T-Mobile

WRAP-UP

Ann Lesperance (PNNL) concluded the event with a summary of the recurring themes from the discussions throughout the day:

- Information sharing – How do we share more effectively? What do we share? What are the implications?
- Workforce development – How do we build and maintain a robust pool of cybersecurity professionals?
- Exercises and training – How do we build something that brings public and private partners together to look at mutual aid, resource typing, etc.?
- Resource – The Pacific Northwest is a thriving region of public, private, and academic partners. How do we inventory what resources and capabilities we have and connect with each other?

Participants were invited to sign up to indicate their interest in initiating working groups and/or following up on these focus areas.

Ann Lesperance (PNNL) shares emerging themes from the day's discussion.

NEXT STEPS

Looking forward, PNNL and SnoPUD will follow-up with participants based on their interested indicated in each of the focus areas listed above. Additionally, results from the workshop will be shared with participants and made available on the SnoPUD website (http://www.snopud.com) and on the PNNL Northwest Regional Technology Center website (http://nwrtc.pnnl.gov).

KEY PARTICIPANTS

Bret Arsenault, Chief Information Security Officer, Microsoft Corporation
Ben Berry, Information Technology and Chief Information Officer, Bonneville Power Administration
Bill Boni, Senior Vice President of Information Security, T-Mobile
Nathaniel Callens, Chief Information Security Officer, Alaska Airlines
Senator Maria Cantwell, U.S. Senator (video)
Paul Dodd, Information Security Chief Strategist, The Boeing Company
Courtney Gregoire, Port Commissioner, Port of Seattle
Ann Lesperance, Director, Northwest Regional Technology Center for Homeland Security, Pacific Northwest National Laboratory
Gordon Matlock, Chief Strategy Officer, Trovares Inc.
Jessica Matlock, Snohomish County Public Utility District
Michael Mylrea, Manager, Cybersecurity and Energy Technology Electricity Infrastructure, Pacific Northwest National Laboratory
Senator Guy Palumbo, Washington State Senate
Ann Rendahl, Commissioner, Washington Utilities and Transportation Commission
Jodie Ryan, Senior Manager, Threat Intelligence, T-Mobile
Prakash Santhana, Managing Director, Cyber Risk, Deloitte
Sudharma Thikkavarapu, Senior Manager, Cybersecurity Transformation, T-Mobile
Selena Tonti, Chief Information Security Officer, Port of Seattle
Col. Gent Welsh, Commander 194th Wing, Camp Murray
Dave Wolf, Chief Information Security Officer, Homestreet Bank

AGENDA

WASHINGTON STATE CYBERSECURITY SUMMIT 4:

A Comprehensive Approach to Critical Infrastructure Security

May 21, 2018, 8:30 a.m. – 4:00 p.m.

Sea-Tac Airport Conference Center • International Auditorium
17801 International Blvd., Seattle, WA 98158

PRESENTED BY

The Washington State Cybersecurity Summit 4 brings together industry leaders and policymakers to focus on the threats and lessons learned nationally, and within our state. And how do we, as critical infrastructure providers, share ideas and best practices.

AGENDA

Time	Topic	Speakers
8:30 a.m.	**Check in**	
9:00 a.m.	**Welcome and Logistics**	◗ **Jessica Matlock,** Snohomish County PUD
	Opening Remarks	◗ **Courtney Gregoire,** Port Commissioner, Port of Seattle ◗ **Senator Maria Cantwell,** U.S. Senator (video) ◗ **Senator Guy Palumbo,** Washington State Senate
9:30 a.m.	**Keynote**	◗ **Bret Arsenault,** CISO, Microsoft Corporation
10:15 a.m.	**Break**	
10:30 a.m.	**National Perspectives** *Lessons learned, what is the internet of everything and impact on security of all networks*	*Facilitator:* **Gordon Matlock,** Chief Strategy Officer, Trovares ◗ **Bill Boni,** Senior VP Information Security, T-Mobile ◗ **Col. Gent Welsh,** Commander 194th Wing, Camp Murray

(continued)

Time	Topic	Speakers
11:30 p.m.	**Lunch (provided) and Networking**	
12:00 p.m.	**Hear from CIO/CISO's on challenges they've faced and how they have addressed them** *What is unique and interesting that you are doing in regards to cyber? What has been working well? What does not work well? Approaches to validating cyber vulnerabilities. What are people doing to improve their security posture. What advice would they suggest.*	*Facilitator*: **Selena Tonti,** CISO, Port of Seattle • **Nathaniel Callens,** CISO, Alaska Airlines • **Paul Dodd,** Information Security (IS) Chief Strategist, The Boeing Company • **Dave Wolf,** CISO, Homestreet Bank • **Ben Berry,** Information Technology and CIO, Bonneville Power Administration
1:30 p.m.	**Washington Utilities and Transportation Commission** *Commissioner Rendahl will provide an overview of how the Washington UTC considers cyber security in its role as a regulator of investor-owned utilities, how the UTC evaluates the reliability of regulated utilities, in particular cyber and emergency preparedness, as well as discuss her work with energy regulators nationally and internationally in evaluating utility cyber security.*	• **Ann Rendahl,** Commissioner, Washington Utilities and Transportation Commission
2:15 p.m.	**Break**	
2:30 p.m.	**Disruptive Technologies, Setting the Stage, Opportunities and Challenges.** *A big picture perspective on disruptive technologies, e.g. depth, breadth, pace of innovation, and what it means from a security perspective. Third or Fourth Industrial Revolution?*	*Facilitator*: **Jodie Ryan,** Senior Manager, Threat Intelligence, T-Mobile • **Michael Mylrea,** Manager, Cybersecurity and Energy Technology Electricity Infrastructure, Pacific Northwest National Laboratory
	Shifting Security Left Through Automation and Orchestration	• **Sudharma Thikkavarapu,** Sr. Manager, Cybersecurity Transformation, T-Mobile
	Blockchain: Practical applications and why does it matter so much to us?	• **Prakash Santhana,** Managing Director, Cyber Risk, Deloitte
3:30 p.m.	**Next Steps**	*Facilitator*: **Ann Lesperance,** Director, Northwest Regional Technology Center for Homeland Security, Pacific Northwest National Laboratory