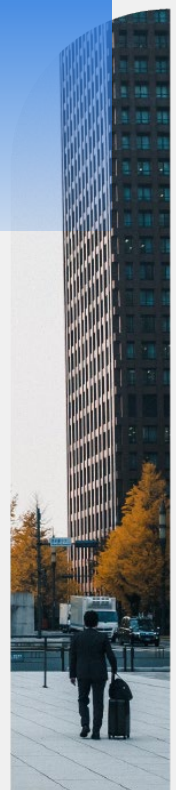

KEY CYBER ISSUES

A Discussion with the Oregon Joint Legislative Committee on Information Management and Technology

Jim Richberg, Public Sector Field CISO and VP of Information Security

18 February 2022

Agenda

- Who is Fortinet?
- Who is Fortinet's speaker at this hearing?
- Key Cyber Challenges for Oregon
- Key Cybersecurity Trends and Hot Topics
- Threats and Threat Intelligence

© Fortinet Inc. All Rights Reserved.

Fortinet is a global leader in cybersecurity

- A US-based company whose products are used by 90% of the Fortune 100, the US Government, and over half of Oregon's state agencies
- Broad, integrated, and automated capability across the breadth of the digital 'attack surface' (network, Cloud, Operational Technology and mobile environments)
- Builds security solutions that are typically high performing and cost-effective
- Generates cyber threat intelligence from 100B+ security events seen daily
- Consistent innovator (3X patents of any other security vendor)
- Pioneer in AI-driven automation of cybersecurity
- Industry leading training material and curriculum — used in Oregon

© Fortinet Inc. All Rights Reserved.

Background on Fortinet witness Jim Richberg

- Field Chief Information Security Officer for the Public Sector (US Federal, state, local, key international partners)
- Represents Fortinet in public-private partnerships and policy bodies ranging from liaison with the US Government to the World Economic Forum
  - Chairs IT sector working group on improving cybersecurity in State, Local, Tribal, and Territorial governments
- Joined Fortinet after 34 year career in US Government
  - Created and oversaw whole-of-government cybersecurity initiative under two Presidents
  - National Intelligence Manager for Cyber—in charge of cyber issues across the 17 agencies/100K staff of the US Intelligence Community

© Fortinet Inc. All Rights Reserved.

Key cybersecurity challenges for Oregon

- Avoiding ‘stovepipe thinking’ as you refresh/modernize infrastructure (IIJA funds)
  - All have digital elements and all need cybersecurity included from the outset
  - Consider building in interoperability, but *at a minimum* infrastructures should share threat data!

- Modernizing/providing greater security across an uneven state landscape of needs and capability

- Dealing with the cyber workforce shortage and skills gap
  - Broadening the talent pool (not all jobs need 4 year degrees or technical specialties)
  - Training and hiring remotely
  - *You cannot close the gap through hiring alone* -- leverage automation and partnership!

© Fortinet Inc. All Rights Reserved.

Key trends and Hot Topics in cybersecurity

Key trends

- Convergence between Networking and Security
  - Exemplars: solutions for hybrid / 'work from anywhere', software defined networking, cloud operations
- Consolidation: new security devices are not only more powerful, each can replace multiple legacy products and reduce 'solution creep' (too many non-integrated solutions)
- Impact of Artificial Intelligence and Machine Learning (AI/ML)
  - Used across the breadth of cybersecurity, maturing over 10+ years of experience

High profile/hot topic issues

- Zero Trust principles and architecture
- MESH/platform architecture — enabling AI/ML-driven transformation!
- Software supply chain risk management (transparency and best practices)

© Fortinet Inc. All Rights Reserved.

Observations on Threat

- **Ransomware** requires joint action by government, private sector, and users
- **Advanced threats** (APT's) have resource constraints and only use their Varsity playbook if needed/warranted by value of the target
- **Supply chain threats**: "bad news, good news" (porous but not elements are equally vulnerable — or valuable)
- C**riminal cyber criminal ecosystem** features more 'Darwin Award winners' than Professor Moriarty-like criminal masterminds
- **Targeted threats are less common** than 'opportunistic' ones
- Increasing **convergence** between **outsider** and **insider threat**
- Damage from insider **risk** is often greater than from insider **threat**

© Fortinet Inc. All Rights Reserved.

Cyber Threat Intelligence

- Cyber Threat Intelligence: produced at multiple levels, used for multiple purposes
  - Tactical (digital signatures for machine-level ‘blocking and tackling’)
  - Operational (adversary Tactics, Techniques and Practices –TTP– and threat actor playbooks used for orchestrating response)
  - Strategic (warnings on threat that can drive changes in organizational behavior)
- Impossible to have enough data, visibility, and staff to ‘go it alone’
  - Striking the balance beyond ‘do it yourself’ and outsourced, commercial vs. public-private partnerships for information sharing/joint production, etc.
- Different consumption and use models:
  - These can differ for data acquisition vs analysis/enrichment
  - Options range from manual to hybrid to fully automated/zero touch

You can’t protect yourself against a threat you don’t understand!

© Fortinet Inc. All Rights Reserved.

Thank You for Your Attention

and I welcome your questions

Jrichberg@Fortinet.com

Jim Richberg | LinkedIn