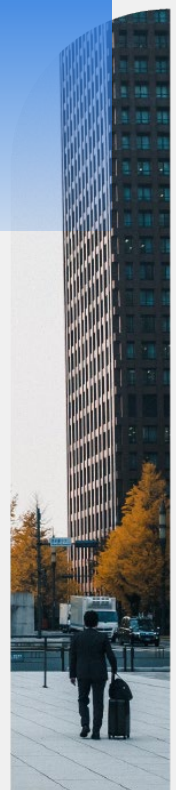
KEY ISSUES IN CYBERSECURITY

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

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

15 February 2023



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 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
- Builds over half of the firewalls sold worldwide (high performing and cost-effective)
- Consistent innovator (3X the patents of any other security company)
- Possesses broad, integrated, and automated capability across the breadth of the digital 'attack surface'
- Generates cyber threat intelligence from 100B+ security events seen daily
- Pioneer in AI-driven automation of cybersecurity
- Award-winning training material and curriculum — used in Oregon

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
- Lead multiple IT sector working groups focused on helping to improve cybersecurity in State, Local, Tribal, and Territorial government
- Joined Fortinet after 34-year career in US Government
  - Created whole-of-government cybersecurity programs for two Presidents
  - “National Intelligence Manager for Cyber” in charge of cyber issues across the 17 agencies/100K personnel of the US Intelligence Community

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 need 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!
- Transferring cyber risk and responsibility from less capable parties (like end users & small agencies) to more capable ones (like tech providers & state government)

Hot Topics and Key trends in cybersecurity

- Impact of Artificial Intelligence and Machine Learning (AI/ML)
  - Used across the breadth of cybersecurity, maturing over 10+ years of experience
- Zero Trust principles and architecture
- Software supply chain risk management (transparency and best practices)
- Convergence between Networking and Security
- Consolidation of technology and vendors: new security devices are not only more powerful, each can replace multiple legacy products and reduce ‘solution creep’ (the proliferation of non-integrated solutions)
- Emergence of MESH/platform architectures — enabling AI/ML-driven transformation

Observations on Threat and Threat Intelligence

- **Advanced persistent threats** (APT's) – typically nation states
- **Ransomware** requires joint action by government, private sector, and users
- **Advanced persistent crime:** ransomware's consistent success is helping criminal stay together and 'level up' in capability
- Cyber Threat Intelligence:
  - Vital since you can't protect yourself against a threat you don't understand and can't detect
  - Produced in multiple ways (e.g., in-house, as a service, in raw vs. 'finished' form), at multiple levels and used for multiple purposes
  - *Impossible to have enough data, visibility, and staff to 'go it alone'*

Thank You for Your Attention

Jrichberg@Fortinet.com