Panel 5: Cultivating a CISO, CSO, and CPO Career

Moderator:

Diana Burley, Executive Director & Chair, Institute for Information Infrastructure Protection (I3P)

Panelists:

Dave Summitt, Chief Information Security Officer, Moffitt Cancer Center

Joseph Johnson, Chief Information Security Officer, Premise Health

Orrie Dinstein, Global Chief Privacy Officer, Marsh & McLennan Companies, Inc.

Diana Burley
Executive Director & Chair,
Institute for Information Infrastructure Protection (I3P)

Dave Summitt
Chief Information Security Officer,
Moffitt Cancer Center

Joseph Johnson,
Chief Information Security Officer,
Premise Health

Orrie Dinstein
Global Chief Privacy Officer
Marsh & McLennan Companies, Inc.

Disclaimer

This is not legal advice nor should it be considered legal advice

This presentation and the comments contained therein represent only the personal views of the participants, and does not reflect those of their employers or clients

This presentation is offered for educational and informational uses only

Responsibilities: Broadly Defined

Chief Information Security Officer (CISO)

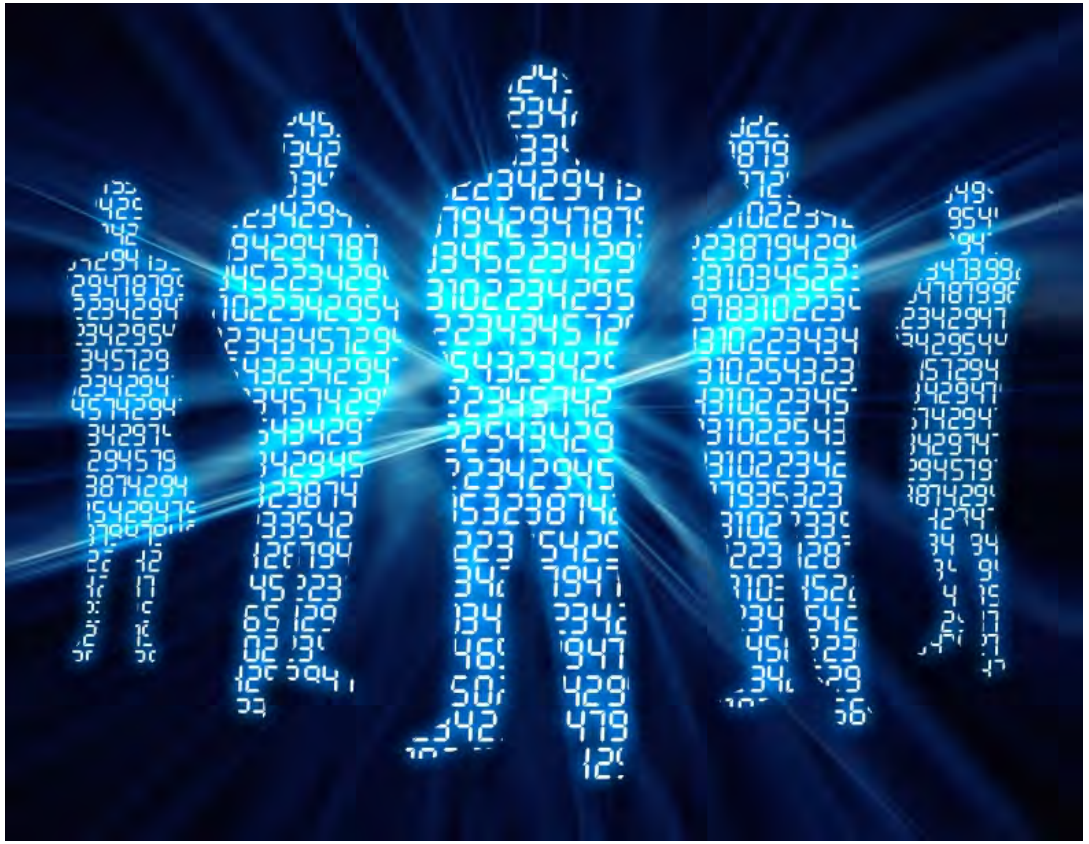
- Responsible for operational security, infrastructure security and employee access management for information technology resources. Stated differently, the CISO is responsible for ensuring that the firm's electronic data is adequately protected.

Chief Security Officer (CSO)

- Responsible for overseeing an organization's security in its entire operating domain.

Chief Privacy Officer (CPO)

- Responsible for managing risks of privacy laws and policies, including advising the firm as to what data may be collected, how that data may be used, where and for how long data should be stored, and when it may or must be destroyed. Within the U.S. government, this position was created under Sect. 522(a) of the Consolidated Appropriations Act of 2005.



Framing the Challenge

- "Every IT position is also a cybersecurity position now [. . .]. Every IT worker, every technology worker, needs to be involved with protecting and defending apps, data, devices, infrastructure, and people.“ - Cybersecurity Jobs Report, 2017
  - There will be 3.5 million unfilled cybersecurity jobs by 2021
  - In order to fill this gap, we must use resources not only from IT, but from across the organization as a whole.
- How do we move people into these roles, and how do we effectively manage them?

Historical Perspectives

- Cybersecurity became an organization wide concern in the 1990's
  - The interceding decades same a rise in the role of cybersecurity personnel in the running of a company, but they are still on the outside looking in.
- One of the greatest barriers to getting the right people into these roles, is that there is not a great pipeline for developing talent.
  - Requires education and expertise across multiple functions, including technical, business, legal, and risk.
- While there are idiosyncrasies for each, the same structural issues exist for CSO, CISO, CPOs.

Cybersecurity Reporting in Organizations

- How does the reporting structure within your organization function?
  - Does the CISO, CSO, or CPO report to the CIO, CEO, or the Board? Most organizations are moving towards direct reporting to the CEO and away from the CIO, as cybersecurity moves from an IT process to a standalone element of a company's processes.
- How does the CISO, CSO, or CPO get information to the Board of Directors? Once the information is there, how can you make sure that it acted upon.
- Regulations are beginning to set reporting requirements
  - I.e. NY DFS cybersecurity regulations:

    The CISO of each Covered Entity shall report in writing at least annually to the Covered Entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity's cybersecurity program. The CISO shall report on the Covered Entity's cybersecurity program and material cybersecurity risks.

The Rise of the Cheap Information Security Officer

- Low-ball recruitment of information security professionals.
- Some organizations facing budgetary restrictions may set out to hire a CISO or other C-suite officers, but set a low pay rate and limited working hours. The organization would end up hiring a part-time information security generalist with just the title of CISO or other C-suite officer.
- Hiring a generalist for a position that requires systematic oversight, legal compliance, and specialized knowledge of information security will create problems in the future that will incur costs the organization hoped to save.

A New Necessity: The Rising Role of the CPO and DPO

- CPOs – long time in the making but only really came into the mainstream in the last 10-15 years
- Functional placement and reporting – remains a mix
- Background, skills and qualifications- remains a mix
  - Lawyer vs non-Lawyer
- "Professionalization" of the role—the rise of the IAPP [4,000-33,000 in 10 years]
- CPO vs Privacy Counsel
- CPO vs CISO
- The rise of the DPO—"75,000 DPOs needed"
- The rise of the data governance officer

Developing the CISO, CSO, CPO Skillset

- A good CISO, CSO, CPO, has a blend of education and experience, including: technical skills, people skills, business skills, managerial skills, understanding of legal principles, and how to effectively blend those skills.
- The recruiting world must understand this and search for multidisciplinary candidates, rather than just siloed experts.
- Ultimately, the success of the CPO – and therefore the successful protection of the company's reputation and business – depends on how the role is integrated into the organization.

Questions?

Appendix

Dr. Diana Burley
Executive Director & Chair,
Institute for Information Infrastructure Protection

Contact:
E:dburley@gwu.edu
URL: www.linkedin.com/in/dianaburley/

JLCW
JOURNAL OF LAW & CYBER WARFARE

Diana L. Burley, Ph.D. is executive director and chair of the Institute for Information Infrastructure Protection (I3P) and full professor of human & organizational learning at The George Washington University. She is a globally recognized cybersecurity expert who was named the 2014 cybersecurity educator of the year by the Colloquium for Information Systems Security Education (CISSE) and as one of the top ten influencers in information security careers by Careers Info Security magazine. In 2013, she served as co-Chair of the US National Research Council Committee on Professionalizing the Nation's Cybersecurity Workforce and she currently co-chairs the ACM Joint Task Force on Security Education.

Dr. Burley has written 60+ publications on cybersecurity, information sharing, and IT-enabled change - including her 2014 co-authored book "Enterprise Software Security: A Confluence of Disciplines." Prior to GW, she served as program director at The National Science Foundation where she managed a multi-million dollar computer science education and research portfolio and led the CyberCorps program. Based on her work at NSF, she was honored by the Federal CIO Council and CISSE for outstanding efforts toward the development of the federal cybersecurity workforce. She served several years as research co-pi of the National CyberWatch Center and two appointments on the Cyber Security Advisory Committee of the Virginia General Assembly Joint Commission on Technology & Science (2012, 2013).

Dr. Burley's board service includes: AlphaTech Group, George Mason University Volgenau School of Engineering Department of IS&T, Goodwill Industries International, Norfolk State University IA-REDI, and Open Mind. She holds a BA in Economics from the Catholic University of America; M.S. in Public Management and Policy, M.S. in Organization Science, and Ph.D. in Organization Science and Information Technology from Carnegie Mellon University where she studied as a Woodrow Wilson Foundation Fellow.

Dave Summitt
Chief Information Security Officer,
Moffitt Cancer Center

Contact:
E: Dave.Summitt@moffitt.org
URL: www.linkedin.com/in/davesummitt/

Dave is the Director of Cyber Security Operations at the H. Lee Moffitt Cancer Center and Research Institute in Tampa, Florida. With over 25 years of experience in information technology, Dave's experience spans across federal and private sectors – concentrating predominantly on information systems, network and engineering operations and within the last 10 years focusing on cyber-security initiatives.

Dave's role in his current and past positions have been to establish a robust information security management program that fits within the strategic vision of the organization. This involved not only building security teams but revamping policy and procedures. His current responsibility is building a Security Operations Center and deploying an Identity and Access Management initiative for Moffitt. Prior to his role at Moffitt, Dave held the Chief Information Security Officer role with the University of Alabama at Birmingham Health System and Manager of Information Security at Bayfront Medical Center in St. Petersburg Florida. Before entering the healthcare sector, Dave left a 21 year federal career with the Department of Defense where he held various roles including the Naval Sea Systems Command's Technical Representative for a major missile defense program, security data custodian, Information Systems Security Officer, Data and Configuration manager and Change Control chairman for several other military programs.

Dave earned his undergraduate degree in Information Systems Management from the University of South Florida and his Masters in Information Security with a Digital Forensics concentration from Norwich University. He maintains the Computer Information Systems Security Professional (CISSP) certification and is currently a member on the Saint Petersburg College Advisory Board for CE Health, the Florida InfraGard, Central Florida ISSA, AEHIS.

Joseph Johnson
Chief Information Security Officer,
Premise Health

Contact
E: Joey.johnson@premisehealth.com
URL: www.linkedin.com/in/joey-johnson-6453999/

Joey Johnson is Chief Information Security Officer at Premise Health, provider of large employer sponsor health and wellness centers for employees. Joey is responsible for leading all organizational efforts related to security operations and engineering, information technology and security compliance, identity access management, policy development, security audit, and vendor risk management to meet challenging security and compliance demands. In his six years with Premise Health, Joey has been instrumental in implementing a proactive security and risk management environment focused organizational risk awareness that is transformative in the healthcare industry. He successfully launched a cutting-edge vendor and business associate maturity development program that dynamically empowered business partners of various scales and complexity to meet challenging security and compliance demands. Additionally, he has worked to develop a team driven by passion in security, with a focus on empowering and fostering women in the security field. In 2016 Joey was presented CISO of the Year award by the Nashville Technology Council.

Prior to joining Premise Health, Joey was the Chief Security Officer for the United States Department of Commerce, Office of Computer Services. He has over 15 years of experience in the cyber-security industry including leadership roles in both the public and private sectors, with a focus on organizations in the federal government, information technology, healthcare, and transportation industries. Outside of Premise Health Joey maintains an active leadership presence in the healthcare cyber-security industry participating in numerous steering and advisory committees with the National Healthcare Information Sharing & Analysis Center (NH-ISAC), various threat intelligence and sharing groups, security news groups, and private/public sector partnerships. He serves on the Editorial Board for the Journal of Law and Cyberwarfare helping to shape the future national and international regulatory landscape around cybersecurity, and also works as a senior advisory member on the E-Health Initiative Federal Executive Advisory Board on Privacy & Security. Joey additionally works as a technical advisor with various security & technology investment organizations and product companies, as well as frequently serving as a speaker at numerous security industry events.

Orrie Dinstein
Global Chief Privacy Officer,
Marsh & McLennan Companies, Inc.

Contact:
E: Orrie.Dinstein@mmc.com
URL: https://www.linkedin.com/in/orrie-dinstein-487ab12/

Orrie Dinstein is the Global Chief Privacy Officer at March & McLennan Companies. He has global responsibility for data protection, and he works closely with the Legal & Compliance, IT and Information Security teams, as well as other functions, to establish policies, procedures, processes and tools related to privacy and data protection matters. Prior to joining Marsh & McLennan, Orrie was the Chief Privacy Officer at GE Capital.

Orrie received an LL.M. degree in intellectual property from NYU School of Law and is a graduate of the Hebrew University of Jerusalem School of Law. He is a member of the New York State Bar and the Israel Bar. He is a Certified Information Privacy Professional (CIPP) and a frequent speaker on privacy, security, technology and social media matters.

Case Law

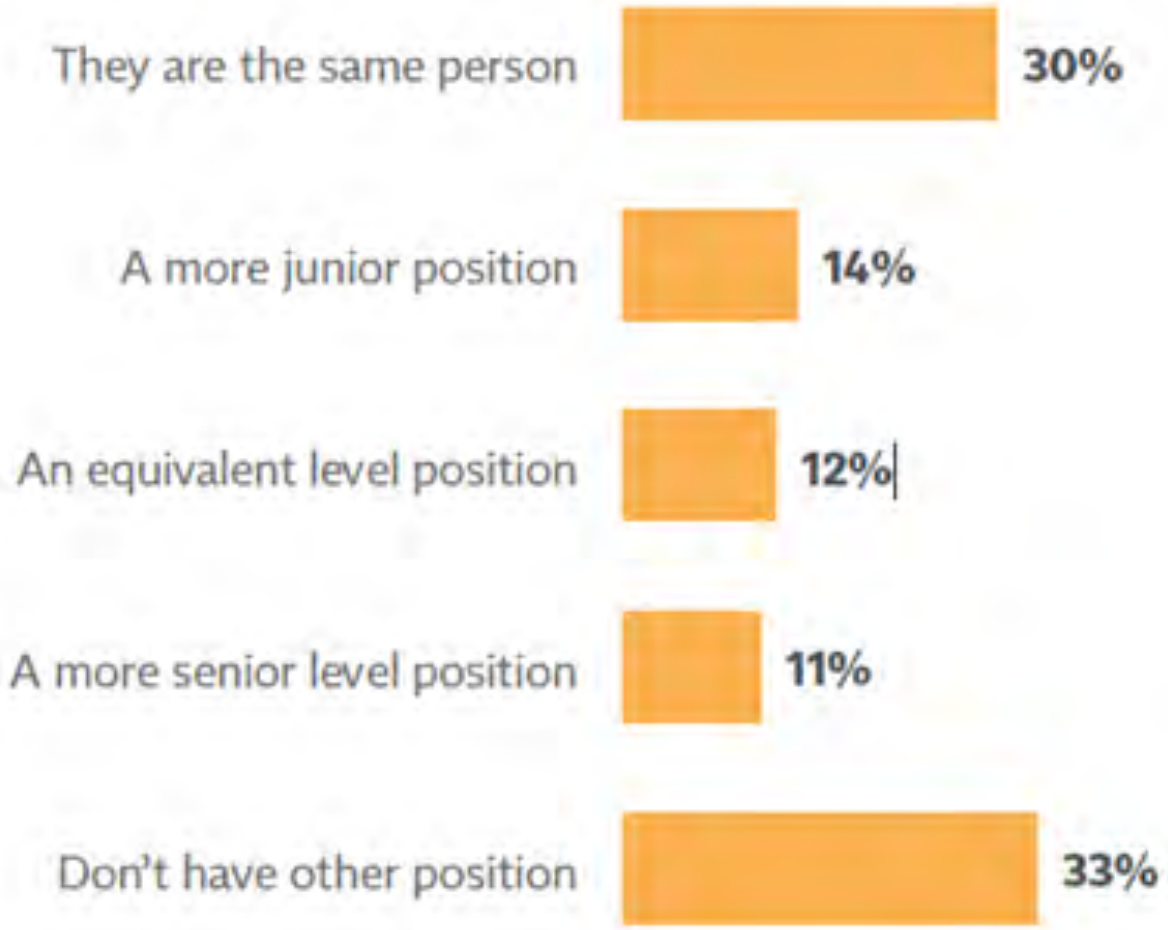
Music Group Macao Commercial Offshore Ltd. V. Foote 2015 WL 3882448 (N.D. Cal. 2015)

- **Fact:** A company hires its former Chief Technology Officer (CTO) as a contractor to provide IT services. The company's computer network subsequently suffers a cyber attack, and the company sues the CTO.
- **Issue:** Whether a CTO, or an officer responsible for planning and managing the network infrastructure, owes a legal duty to the company arising from their professional services.
- **Holding:** A genuine issue of material fact exists as to whether there was a professionalized standard of care.
- **Reasoning:** Though the court could not find precedents where professional negligence principles had been extended to a CTO or other IT professionals, it nonetheless held that a reasonable jury could conclude that a CTO, in his professional role, was responsible for network security. In this instance, the court noted that the CTO could have implemented better cybersecurity measures to protect against the attacks.

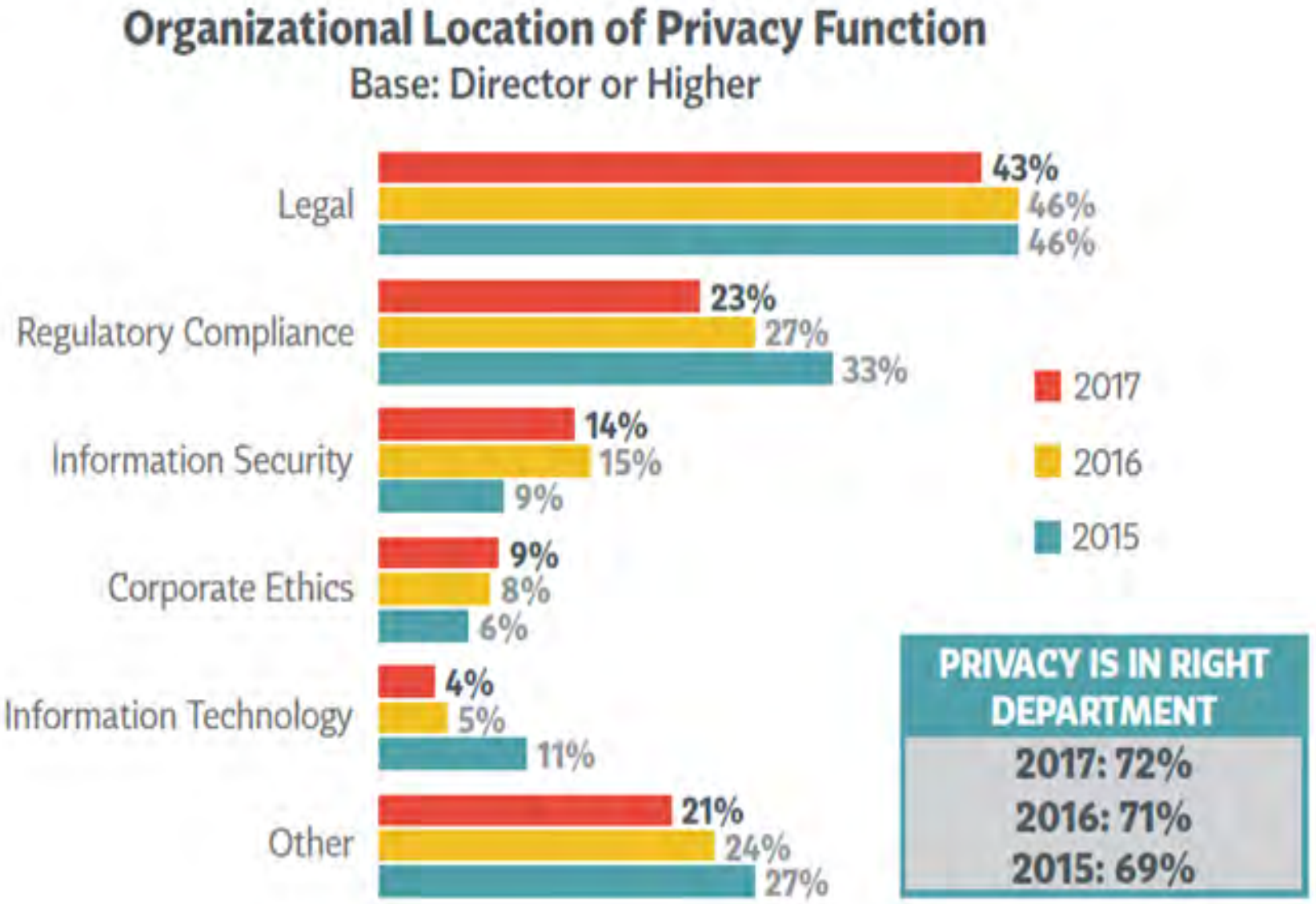
Data on Privacy Professionals

Privacy Leader Relative to Chief Privacy Counsel

Base: Director or Higher



*Charts from the IAPP 2017 Governance report



Privacy Leader Relative to Data Protection Officer

Base: Director or Higher