Committee on Energy and Commerce
U.S. House of Representatives
Witness Disclosure Requirement - "Truth in Testimony"
Required by House Rule XI, Clause 2(g)(5)

1. Your Name: Erik Decker		
2. Your Title: Chief Security and Privacy Officer, Advisory Board Chairman		
3. The Entity(ies) You are Representing: University of Chicago Medicine, Association of Executives in Healthcare Information Security		
4. Are you testifying on behalf of the Federal, or a State or local government entity?	**Yes**	**No** X
5. Please list any Federal grants or contracts, or contracts or payments originating with a foreign government, that you or the entity(ies) you represent have received on or after January 1, 2015. Only grants, contracts, or payments related to the subject matter of the hearing must be listed. N/A		
6. Please attach your curriculum vitae to your completed disclosure form.		

Signature: [redacted] **Date:** 4/4/18

Erik Charles Decker

[redacted]

Information Security Executive

Results-driven Executive with 20 years of proven achievements in Information Technology and 12 years in Information Security. Exceptional success maintaining crucial relationships with key stakeholders in all branches of large organizations, including the executive team, general counsel, finance, risk management, and public safety/law enforcement. Strategic thinker, proven leader, and skilled team builder in navigating political and cultural climate. Adept at both "*boiling up*" complicated information security issues to key executives, as well as "*diving in the weeds*" with technical personnel. Expert analytical and technical skills.

Proven top performer, with ongoing success in building information security programs and teamwork. Exceptional provider of solutions, with broad array of experience with cross-functional alignment of teams. Proactive leadership role, mentoring managers through valued experience. Exceptional interpersonal skills, including team building, facilitation, and negotiation. Excels in operational improvements, fulfilling aggressive timelines, and multi-tasking. Extremely dedicated with a strong work ethic and careful attention to detail in high pressure situations. Core competencies include:

- Strategy & Vision
- Security Governance & Policy
- Risk Assessment & Mitigation
- Budget Oversight & Management
- Security and Privacy Leadership
- Incident Response
- Academic Medical Center Expertise
- Team Building & Mentoring

Professional Experience

University of Chicago Medicine, Chicago, IL

University of Chicago Medicine (UCM) is the premier academic medical center situated in the southside of Chicago. Comprised of multiple hospitals, ambulatory clinics and a large physician practice. Over $1.9 billion operating budget consisting of 19,000 affiliates.

Chief Security and Privacy Officer *3/17 – Present*

Same responsibilities as Chief Information Security Officer, with the addition of the organization's first Identity and Access Management Program and the Privacy Program. Leads a team of 22 Information Security, Identity and Privacy professionals. *Notable achievements include*:

- As part of the organization's expansion into a health system, transitioned the role of Privacy Officer from the Chief Compliance Officer.
- Expanded the Privacy Program role from HIPAA to include all aspects of privacy, such as Common Rule (IRB and Human Subject research), PIPA, BIPA, and GDPR. Greatly increased scope of privacy program to cover clinical research related functions.
- Grew the Privacy Program from 2 FTEs to 4 FTEs, covering all aspects of the newly formed health system.
- Expanded Information Security Program to cover newly acquired hospital. Set forth the strategic plan and model for managing a health system wide cyber and privacy program.
- Launched the organizations first Identity and Access Management (IAM) program. Established the program by conducting a needs and gap analysis, determination of operational gaps, setting vision for automation and interoperability, and hiring new staff and reconfiguring existing Access Management resources under a single program.
- Leveraging the IAM program through the use of automation, interoperability, and LEAN process management efficiencies, identified opportunities to save and avoid $2.5m over a three-year period of time. Actualized $400k in cost avoidance in the first year.

Chief Information Security Officer *7/14 – 3/17*

Leads a team of 8 Information Security professionals. Established the first strategic Information Security Program for the UCM. Oversees all aspects of Information Security Program, such as Governance, Policy and Procedures, Risk Management, Security Operations, Incident Response, and Security Awareness. Responsible for a $4+ million security budget (a growth from .7% of IT budget in 2014 to 6% in 2017): *Notable achievements include*:

- Launched the organizations first Information Security Program. Established the Program by conducting enterprise risk assessments, determining institutional gaps, identification of necessary human and financial resources, and establishing a three-year strategic plan to mature its operations. Grew team from no FTEs to 8 FTEs over a three-year period.
- Establishing the first executive risk committee, chaired by the EVP for Medical Affairs of the University of Chicago. Committee responsible for setting policy, owning cybersecurity risk and setting risk tolerance direction.
- Established third-party risk management program, covering over 300 business partnerships, to ensure data protection and institutional cyber risks have been managed through supply chain processes.
- Established a robust phishing education program, reducing employee susceptibility by 300%+ (26% to 6% susceptible, on average) to phishing attacks for over 16,000 individuals.
- Created and expanded cybersecurity incident response processes from an 8x5 operation to 24x7 through the use of strategic partnership with a Managed Security Service Provider. This partnership outsources Tier 1 cyber incidents to the MSSP through the use of well defined runbooks and escalation. This partnership also expanded the organizations detection capabilities by leveraging MSSPs engineering capabilities and expanding threat detection functions within internal systems.

- Built out an automated data protection program. The automated system covers multiple data transmission channels, such as email, file storage, removable media and web browsing usages. System provides feedback in real-time to employees when mishandling sensitive information.
- Implemented analytics driven monitoring system of key clinical applications (such as the EMR and Imaging systems). System monitors employee usage to ensure privacy policies are adhered to and detects the usage of insider threat and fraudulent usage.
- Established a continuous improvement and monitoring program, leveraging the LEAN discipline and key metrics, to ensure sustained operations and improvement of cybersecurity capabilities.
- Established a financial chargeback model for health system constituents, which accounts for the recovery of over $800k in expenses.
- Established the organizations first set of cybersecurity policies.

COLUMBIA UNIVERSITY MEDICAL CENTER, New York, NY

Columbia University Medical Center's (CUMC) is the health care component of greater Columbia University with a $1.8 billion operating budget consisting of 17,000 affiliates made up of 13,500 staff, faculty and 3,500 graduate students within 5 schools.

Assistant Director, Information Security *3/11 – 7/14*

Leads a team of 8 Information Security professionals and managers. Oversees all aspects of Information Security Program, such as Governance, Policy and Procedures, Risk Management, Security Operations, Incident Response, and Security Awareness. Promoted during tenure to current position. *Notable achievements include*:

- Developing and executing the medical center's Information Security Management Program.
- Formed an executive information security steering committee, comprised of senior executives, and charged with strategic management of institutional risk.
- Aligned research protocol review with risk management program; implemented process gate to ensure protection of electronic-sensitive data covering 9,000 protocols totaling over $800,000 in research grants annually.
- Managing a $2.1 million budget; includes direct recovery of more than $600,000 in expenses.
- Implemented a continuous HIPAA/HITECH related risk assessment and remediation efforts for medical center, comprised of over 600 risk systems, including *(i)* technical vulnerability assessments, *(ii)* configuration review, *(iii)* business process and procedure reviews, and *(iv)* business continuity planning.
- Developed and implemented a comprehensive security awareness and security training program, including: training over 17,000 users and 100 system administrators within 28 different IT groups.
- Developed key performance and risk indicators (KPIs & KRIs) for measurement of the Information Security Program.
- Developed and implemented a medical center-wide "Endpoint Security Campaign" charged with identifying and securing over 30,000 endpoint devices.
- Advancing policy and procedures as University Policy Advisory Committee member; leading task force to analyze and consolidate 43 disparate University policies into a framework of 13 information security policies.
- Leading Security Operations team, responsible for providing security services such as: web and email data loss prevention, secure email gateway, enterprise proxy server, advanced persistent threat protection systems, log and security management, network access control, *and others.*
- Liaising with the General Counsel's Office on legal issues and related matters.
- Leading Incident Response Team.

DEPARTMENT OF BIOMEDICAL INFORMATICS, COLUMBIA UNIVERSITY

Associate (Adjunct Professor) *4/11 – 7/14*

Developed Information Security and HIPAA Privacy course for an NIH funded Healthcare Information Technology certification program sponsored by the CUMC Department of Biomedical Informatics. Instructed 5 cohorts of students (5 separate semesters).

LOYOLA UNIVERSITY CHICAGO, Chicago, IL

Loyola University Chicago (LUC), a Jesuit academic institution with a global presence. LUC consists of 16,000 students, 2000 faculty and 1200 staff.

Senior Security Analyst *11/07 – 2/11*

Oversaw security operations for the University Information Security Office, including all enterprise Information Security strategy and operations. Internally promoted during tenure to stated position. *Notable achievements:*

- Co-developed, with Information Security Officer, risk-based organizational Information Security Program based on the ISO 27001/27002 standards; program consists of policy development, risk assessment, project prioritization, security operations, key performance security indicators, metrics and reporting.
- Instrumental in forming an information security sub-committee comprised of key business stakeholders and responsible for Information Security governance, policy development and prioritizing security projects.

- Conducted risk assessments leveraging NIST SP800-30 against enterprise solutions such as ERP (PeopleSoft/Oracle), eCommerce, Identity Access Management, system infrastructure and critical business processes.
- Brought organization into PCI-DSS compliance by creating an enterprise compliance strategy; accomplished by limiting scope of the credit card processing environment and incorporating changes to over 40 merchant accounts.
- Lead Loyola's Incident Response Team, and matured the implementation of the Incident Response Plan; built metrics and incorporated results into the strategic roadmap.
- Resident expert for Business Continuity and Disaster Recovery Plan development; conducted business impact analysis and built business recovery plans prioritized by business critical functions.
- Directly managed student workers, and consultants.
- Developed security internship program, drawing from the extremely capable pool of computer science graduate students, exposing them to entry-level Information Security responsibilities.
- Liaised with the General Counsel's Office on legal issues and related matters.

IGNATIAN SPIRITUALITY PROJECT, Chicago, IL

Consultant *2010*

Hired as an external consultant to analyze existing business practices and processes, offer recommendations, and implement recommendations for improving customer relationships through the use of Salesforce CRM.

TOWN OF NORMAL, Normal, IL

Network Administrator *20002-2007*

Network and security engineer at the Town of Normal, a local municipality located in the twin city of Bloomington/Normal Illinois. The Town supports 50,000 residents. Internally promoted during tenure to stated position.

Notable achievements:

- Oversaw security operations for the municipality.
- Directly managed team of 2 PC specialists.
- Oversaw compliance with crucial regulations: PCI-DSS compliance, HIPAA (paramedic access to patient records) and Law Enforcement Agencies Data Systems (LEADS) compliance.
- Developed and implemented organizations Business Continuity and Disaster Recovery Plan (BCP/DR); conducted Business Impact Analysis (BIA) to determine critical systems for backup and recovery strategy; developed partnership with County Administration to serve as recovery sites for one another.
- Lead network engineer on all network architecture, design, implementation, maintenance in key networking projects.
- Implemented centralized Security Information and Event Management system; consolidated, correlated and defined system alerts for security monitoring, incident response and forensics.
- Liaison and leader on between city, county and Illinois State University joint community, leveraging municipal "right of way" land access to build out a multi-city and county fiber ring to be shared by all municipalities, reducing need for leased lines, saving on yearly upkeep costs.

RELATED EXPERIENCE

CARESCIENCE, *San Francisco, CA*
Desktop Analyst *2000-2001*
UNIVERSITY OF ILLINOIS, *Champaign, IL*
Shockwave and HTML Developer *1999-2000*
Network Technician *1997-1998*
CREATIVE SYSTEMS, *Normal, IL*
Computer Technician *Summer 1998*

EDUCATION

Loyola University Chicago, Chicago, Illinois
Masters of Science (2010) – Information Technology, concentration in Information Assurance
Awarded Special Distinction for Academic Excellence

University of Illinois at Champaign/Urbana, Champaign, Illinois
Bachelor of Science (2000) – Cell and Structural Biology

Erik Charles Decker

[redacted]

Awards & Recognitions

Chicago Area CISO of the Year, 2017
AITP Most Effective IT Team, 2015
Nominee, Chicago Area CISO of the Year, 2015

Certifications

Certified Information Systems Security Professional (CISSP, #351885)
EnCase Certified Examiner (ENCE)
ITIL Foundations 2011 (GR750102769ED, PeopleCert Verification)
MOR Associates IT Leadership Program Graduate (ITLP)
Expired Cisco Certified Network Associate (Ex-CCNA, #CSC011235182)
Expired GIAC Penetration Testing Certified (GPEN, #6644)
Expired GIAC Security Essentials Certified (GSEC, #7561)

Industry Affiliations

Advisory Board Member (Chair, 2018), Association of Executives in Healthcare Information Security, 2015-2018
Association of CISOs within the Healthcare Industry, providing education, professional development and advocacy. Over 850 members.

Industry Lead, Cybersecurity Act 2015, Section 405(d), "Aligning Cybersecurity Best Practices within Healthcare", 2017-2018
Co-lead of 130+ task group within a public-private partnership with the Department of Health and Human Services. Group has delivered a best practice guide for small, medium and large sized healthcare organizations in 2018.

Leader in the Healthcare Sector Specific Joint Cybersecurity Working Group, within the Healthcare Sector Coordinating Council, 2017-2018
A public-private partnership for establishing cybersecurity practices to the Healthcare Industry, as a designated critical infrastructure under the National Infrastructure Protection Plan.

Advisory Board Member, Scottsdale Institute, 2018
A not-for-profit membership organization of prominent healthcare systems whose goal is to support its members as they move forward to achieve clinical integration and transformation through information technology

Member of EDUCAUSE IAM Governance Task Force, 2013

Presentations And Publications

Presenter:
Secure XII, ISSA and ISACA Chicago Chapter, CISO Panel Member, June 2018
Chicago Healthcare Leaders, Keynote Speaker, June 2018
Collision Between Cyber Risk & the Trend to Home Healthcare, Speaker, May 2018
HIMSS Cybersecurity Forum, How to be an Effective Security Leader, Keynote, February 2018
HIMSS, Connected Medical Devices in Cyber Age, Panel Member, February 2018
ISSA Chicago Chapter Meeting, Industry Led Development of Healthcare Cybersecurity Best Practice Guide, Keynote Speaker, February 2018
AEHIS Fall Summit, Effective Board Level Engagement, Moderator, October 2017
Columbia University IRB Annual Conference, Database Security, 2012 & 2014
Association of Clinical Research Professionals (ACRP) Symposium, Crisis Management in Clinical Research, September 2013.
Aligning Identity and Access Management with Your Information Security Program, EDUCAUSE, April 2013
Academic Medical Center (AMC), Security and Privacy Issues in Research, April 2012.
Loyola University Chicago, Penetration Testing using Open Source Tools, 2010
Illinois State University, Information Systems and Operation Management, 2005 & 2006

Publication:
Top 10 Best Practices for Healthcare Cybersecurity, Author and Master Editor, 2018
EDUCAUSE IAM Toolkit, Columbia University IAM Use Case, Author, May 2013

Regulatory Competencies

Expert on regulatory and compliance regimes such as: HIPAA/HITECH, FISMA, PCI-DSS, FERPA, Red Flag, ISO 27001/27002, and NIST 800-53, 800-30, 800-36.