Erik Charles Decker

Cybersecurity Executive

Results-driven Executive with 24 years of proven achievements in Information Technology and 17 years in Cybersecurity and national leader within the field of Healthcare Cybersecurity. Proven national cybersecurity thought leader. Exceptional success developing and executing strategic cybersecurity programs within academic medicine. Recognized national cybersecurity leader and partner with the U.S. Department of Health and Human Services, leading the development of *Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients*. Former Chairman of the Health Sector Coordinating Council Cybersecurity Working Group. Served a witness and advisor to Congress on related cybersecurity policy issues in healthcare, such as medical device security and interoperability. Industry leader, serving as both leader and member of multiple professional associations and public-private partnerships. Frequent presenter and educator on topics of cybersecurity within healthcare. Core competencies include:

- Strategy & Vision
- Security Governance & Policy
- Risk Assessment & Mitigation
- Budget Oversight & Management
- Security and Privacy Leadership
- Incident Response
- Healthcare Cybersecurity Expert
- Team Building & Mentoring

Professional Experience

Intermountain Healthcare, Salt Lake City, UT (*2021 – Present*)

Intermountain Healthcare is an Integrated Delivery Network headquartered in Salt Lake City, Utah. Comprised of 33 hospitals, a virtual hospital, over 200 clinics and a Health Plan. Over $16b in revenue, 68,000 affiliates and serves over 4 million patients and 1 million Health Plan members. In addition to being a Provider and Plan, Intermountain is also an innovation hub and has created multiple spin-off companies looking to tackle some of Healthcare's toughest challenges. These include companies focused on out-patient imaging, population health, mental health, generic pharmaceutical drugs, and HIT interoperability.

Vice President & Chief Information Security Officer, *3/21 – Present*

Responsible for a team of 150+ employees and charged with protecting the organizational digital systems, workflows, data, and consumer assets. Responsible for a $42m+ budget. Includes the management of all elements of a modern cyber program, including GRC, BC/DR, IAM, Architecture, Engineering, 24x7 Security Operations Center, Cloud Security, Vulnerability Management and Penetration Testing, Cyber Service Management, and M&A growth. *Notable achievements include:*

- Setting a 10-year vision and securing resources and assets to support a "Third Generation" cybersecurity program, codenamed "Gen 3". This included significant investment in human capital and non-labor growth.
- Established a robust M&A playbook to support Intermountain's inorganic growth strategy (which includes acquisitions and large mergers; executed playbook for mergers, acquisitions and divestitures
- Led cyber integration of merger with healthcare organization, SCL Health; merger added 16,000 new employees, 8 new hospitals and $3b in revenue.
- Grew Cyber FTE count from 85 FTEs to 150+ FTEs in first year of Gen3 launch; additional 20+ FTEs added with merger.
- Developed and executed on a 3-year roadmap, supporting the 10-year vision, with the focus of achieving higher maturity ratings, mitigating risk and easing friction inside the organization. Maturity targets established pursuant to NIST CSF. Increased maturity levels by 62 basis points. Process leverages a robust set of external validated assessments.
- Established apprenticeship program, focusing on bringing new cyber talent into the organization by targeting non-traditional education and underserved populations. Cohort of 13 apprentices added year over year, matriculating into fulltime work upon performance goals being met.
- Partnered with Internal Audit to develop and establish Intermountain's Enterprise Risk Management framework with Cybersecurity being the first adopter of the newly developed framework
- Updated GRC program to comprehend systemic risk, how this interrelates with the healthcare eco system, and establish risk models to identify and build management plans associated to material critical functions for the delivery of patient care.
- Led the convergence of multiple identity stacks (encompassing 55k identities) into a single, enterprise program, while supporting a move to Epic Hosting successfully, on time and on budget.

University of Chicago Medicine, Chicago, IL (*2014 – 2021*)

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 $2.5 billion operating budget consisting of 19,000 affiliates.

Chief Information Security and Privacy Officer, *7/14 – Present (Promoted with additional Privacy responsibilities in 2017)*

Same responsibilities as Chief Information Security Officer, with the addition of the organization's first Identity and Access Management Program and the accountability of the UCM Privacy Program. Leads a team of 28 Cybersecurity, Identity and Privacy professionals. Responsible for a $4+ million security budget (a growth from .7% of IT budget in 2014 to 6% in 2020): *Notable achievements include:*

Security

- Launched the organizations first Cybersecurity Program. Established the Program with the vision of delivering a threat-centric, risk-based program to appropriate manage risk to a tolerable level to the organization leveraging analytics, automation and continuous improvement (through LEAN methodologies). Achieved the results of this program through multiple cycles of strategic planning and tactical execution. Core activities include: 24x7x365 security operations and incident response, security architecture & engineering, vulnerability management and threat hunting, automated data protection, training and education, governance risk and compliance, business continuity and disaster recovery and identity and access management.
- Established executive cybersecurity risk governance, chaired by the chief executive of the health system, with C-Suite members of the health system. Committee responsible for setting policy, owning cybersecurity risk and setting cybersecurity risk appetite.
- Key stakeholder in the development of an organization wide Enterprise Risk Management program. Adopted existing risk management techniques into the newly established model and assisted other verticals on their ERM journey (Finance, Legal, Operations, and Compliance).
- Developed and established ERM model for Cybersecurity. Measure cybersecurity risk across 6 key risk indicators (including patient and life safety as a key critical risk) while showing security ROI as a component of growth in cybersecurity maturity leveraging the NIST Cybersecurity Framework. Moved from Tier 2 organization to Tier 3 organization.
- Developed and executed methodology for assisting the organization with Mergers and Acquisitions. Built a risk assessment playbook and methodology for determining risk of newly merged or acquired practice in the short term with the longer-term goal of implementing cybersecurity shared services and standards.
- Established Cybersecurity Shared Services, which are a set of practices run by a dedicated team to determine to scale over to the UCM Health System. These shared services apply consistently in cybersecurity practices and avoided $1.6m in additional spend for newly acquired hospital and physician practices.
- Launched the organizations first Identity and Access Management (IAM) program consisting of 10 FTEs. 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 $1.6m in cost avoidance in the first year.

Privacy

- As part of the organization's expansion into a health system, promoted to include the Chief Privacy Officer role
- Expanded the Privacy Program role from HIPAA to include all aspects of privacy, including human subject research (Common Rule), PIPA, BIPA, and GDPR. Greatly increased scope of privacy program to cover clinical research related functions.
- Grew the Privacy Program from 2 FTEs to 6 FTEs, covering all aspects of the newly formed health system.

COLUMBIA UNIVERSITY MEDICAL CENTER, New York, NY (*2011 – 2014*)

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 Cybersecurity professionals and managers. Oversees all aspects of Cybersecurity 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*:

- Managed a $2.1 million budget; includes direct recovery of more than $600,000 in expenses.
- Developed and executed the medical center's Cybersecurity Management Program.
- Established the first executive Cybersecurity 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.
- 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 and implemented a medical center-wide "Endpoint Security Campaign" charged with identifying and securing over 30,000 endpoint devices.

Erik Charles Decker

Department of Biomedical Informatics, Columbia University

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

Developed Cybersecurity 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

Loyola University Chicago, Chicago, IL (*2007 – 2011*)

Loyola University Chicago (LUC), a Jesuit academic institution with a global presence. LUC consists of 16,000 students, 2000 faculty, 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.
- Developed security internship program, drawing from the extremely capable pool of computer science graduate students, exposing them to entry-level Information Security responsibilities.

Ignatian Spirituality Project, Chicago, IL, *Consultant* (*2010*)
Town of Normal, Normal, IL, *Network Administrator* (*2002-2007*)
CareScience, *San Francisco, CA, Desktop Analyst, 2000-2001*
University of Illinois, *Champaign, IL, Shockwave and HTML Developer 1999, Network Technician, 1997-1998*
Creative Systems, *Normal, IL, Computer Technician, Summer 1998*

Education

Loyola University Chicago, Chicago, Illinois
Masters of Science (2010) – Information Technology/Information Assurance, *Awarded Special Distinction for Academic Excellence*
University of Illinois at Champaign/Urbana, Champaign, Illinois
Bachelor of Science (2000) – Cell and Structural Biology

Awards & Recognitions

2024 Top Global CISOs, Cyber Defense Magazine, 2024
2023 Baldrige Foundation Award for Leadership Excellence, Cybersecurity, 2023
C100 Cisco Connect, Top 100 CISOs, 2022
Global CISO 100, 2020
T.E.N ISE® North America Executive: Academic/Public Sector, 2019
AEHIS Health Information Security Innovator of the Year, 2019
Becker's CISOs Top 100 CISOs to Know, 2019
Most Wired, 2020, 2019, 2018, 2016
Chicago Area CISO of the Year, 2017
AITP Most Effective IT Team, 2015

Certifications

Digital Directors Network (DDN) Qualified Technology Expert (QTE), 2021
SIM Regional Leadership Forum, Program Graduate - 2019
MOR Associates IT Leadership Program, Program Graduate (ITLP)
Certified Information Systems Security Professional (CISSP, #351885)
EnCase Certified Examiner (ENCE)
ITIL Foundations 2011 (GR750102769ED, PeopleCert Verification)
Expired Cisco Certified Network Associate (Ex-CCNA, #CSC011235182)
Expired GIAC Penetration Testing Certified (GPEN, #6644)

Erik Charles Decker

Expired GIAC Security Essentials Certified (GSEC, #7561)

Industry Affiliations

Chairman, Healthcare Sector Coordinating Council, Joint Cybersecurity Working Group, 2022-2024

Executive Council, Healthcare Sector Coordinating Counsel, Joint Cybersecurity Working Group, 2019-2021

A public-private partnership for establishing cybersecurity practices to the Healthcare Industry, as a designated critical infrastructure under the National Infrastructure Protection Plan. Integral in relaunch of Joint Cybersecurity Working Group, leading charter revision and adoption for over 400 members.

Industry Lead, Hospital Cyber Resiliency Initiative, 2022-2023

Co-lead, with HHS CMS, a task group of the HSCC Joint Cybersecurity Working Group, studying the current state of cyber resiliency of US hospitals. Group delivered a Landscape Analysis publication.

Industry Lead, Cybersecurity Act 2015, Section 405(d), "Aligning Cybersecurity Best Practices within Healthcare", 2017-2024

Co-lead of 150+ task group within a public-private partnership with the Department of Health and Human Services. Group delivered Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients publication for small, medium and large sized healthcare organizations

Advisory Board Member (Chair, 2018, Vice-Chair, 2017, Chair of Public Policy Committee, 2017), Association of Executives in Healthcare Information Security, 2015-2018

Advisory Board Member, Scottsdale Institute, 2018

Member of EDUCAUSE IAM Governance Task Force, 2013

Presentations And Publications

Thought Leadership

Setting strategy with \he Deputy National Security Advisor, White House, and Deputy Secretary of HHS, on Health and Public Health Cybersecurity Mandates, White House, Washington D.C., January 2024

Established Health and Public Health Cybersecurity Performance Goals in partnership with the Deputy Secretary of HHS, the Critical Infrastructure Security Agency, and the National Security Council of the White House, January, 2024

Cabinet Level Healthcare Cybersecurity Executive Forum, White House, Washington D.C., June 15, 2022, Participant

Testimony:

Subcommittee on Health, House Energy and Commerce; Preparing for and Responding to Future Public Health Security Threats, May 11, 2023; Expert Witness, Cybersecurity, Testimony Before Congress

Subcommittee on Privacy, Confidentiality and Security, National Committee on Vital and Health Statistics July 14, 2021; Expert Witness

Subcommittee on Oversight and Investigations, House Energy and Commerce, Legacy Medical Devices, October 2018

Subcommittee on Health, House Energy and Commerce; Pandemic and All Hazards Preparedness Act, June 6, 2018; Expert Witness, Cybersecurity, Testimony Before Congress

Subcommittee on Oversight and Investigations, House Energy and Commerce; Software Bill of Materials for Medical Device Security Roundtable, October 2017

Publications:

Preventing the Next Big Cyber Attack on U.S. Healthcare, Harvard Business Review, Author, May 2024

Hospital Cyber Resiliency Initiative: Landscape Analysis, Industry Lead, Author, Editor, April 2023

Health Industry Cybersecurity Tactical Crisis Management guide, Industry Co-Lead, Author, Editor, May 2020

A Simple Model to Discuss Cyber Risks with Executives, The 405(d) Post: Healthcare Industry Cybersecurity News and Emerging Issues, September 2019

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, Industry Lead, Lead Author and Master Editor, December 2018

CISO Compass, Navigating Cybersecurity Leadership Challenges with Insights from Pioneers, Todd Fitzgerald, Contributor, December 2018

Best Practice Standards in Cybersecurity Risk Management, Scottsdale Institute, Contributor, October 2017

EDUCAUSE IAM Toolkit, Columbia University IAM Use Case, Author and Contributor, May 2013

Regulatory Competencies

HIPAA/HITECH, FISMA, PCI-DSS, FERPA, Red Flag, ISO 27001/ 27002, HITRUST and NIST CSF, NIST 800 Series