# Information Technology Spotlight

This week we are highlighting the **Cybersecurity team**. The Cyber team is comprised of 140 caregivers and is a mission critical component of the Information Technology department. We'd like to provide a brief introduction for those who haven't yet met the team and highlight some of the more recent advances in this area.

The Cybersecurity team is made up of the following key areas:

- The Office of the Chief Information Security Officer (CISO)
  - Program Strategy, Portfolio Management, Financials, Reporting and Analytics

- Cybersecurity Service Management
  - Cyber regional liaisons, cyber service taxonomy and delivery, cyber education and awareness

- Identity and Access Management (IAM)
  - Access and Governance
  - Platform Integration and Governance

- Cyber Governance, Risk and Compliance (GRC)
  - Business Continuity and Disaster Recovery
  - Contract Management/Audits
  - Governance and Compliance
  - Cybersecurity Risk

- Cyber Threat Management
  - Architecture and Forensics
  - Security Operations and Engineering
  - Fusion Center (Security Operations Center, Incident Response, and Security Vulnerability and Assessment)
- Legacy SCL Health Cyber (during 24-month integration)
  - GRC, IAM, Security Operations, and Vulnerability Management

In October of 2011, Intermountain's Cybersecurity organization introduced a Virtual SOC (Security Operations Center), and then a dedicated full-time SOC opened in July of 2015 on the third floor at Lake Park. The new Fusion Center recently opened in September of 2021 and has been relocated to the first floor at Lake Park. It has already gained national attention and received numerous awards. The pictures shown below were taken during a recent tour of the Lake Park facility by our new Technology Organization Executive Leadership Team.
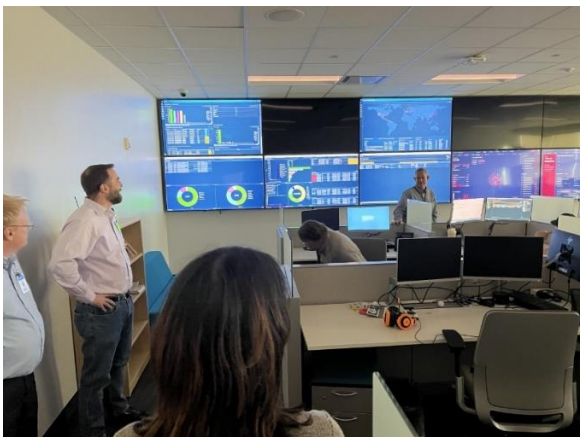
Cyber Vision

A world class cyber program that serves our people and communities, builds trust, and enables access

Vivid Descriptions

1. Complete trust by our patients and members in Intermountain's vigilance at providing a safe environment of care - "we will always do the right thing"

2. A program that constantly monitors, stays abreast, and responds to changes in the overall threat landscape through continual evolution and improvement

3. A One Intermountain cyber program that manages risks and threats, framed on services, leveraging data and analytics, and delivered with expertise, automation and self-service

4. Enable Intermountain caregivers to work securely ANYTIME, ANYWHERE, in ANY environment

5. Educates and guides Intermountain caregivers to work in a safe and secure manner

Top 5 Cyber Strategic Priorities to Mature the Cyber Program

- Caregiver Investment – Develop, mentor, invest and celebrate our diverse cyber caregivers, as they are our most important asset
- Growth & Efficiency – Partner on our inorganic growth strategy and leverage the IOM to drive efficiency into the cyber program
- Risk – Evolve our risk management program with focus on organizational risk tolerance and appetite
- Cyber Maturity – Expand our capabilities to exceed that of the threat actor
- Trusted Business Partner – Be a solution advocate and ease friction while providing world-class protections of our patients, members and organization

Cybersecurity Detailed Functional View

Erik Decker – CISO

Carl Allen – Sr. Director – Office of the CISO
- Program Strategy & Mgmt
- Portfolio Mgmt
- Financials
- Reporting & Analytics

Exec Assistant – Angie Smith

Bruce James – Deputy CISO, Sr. Director – Cyber Threat Mgmt
- Technical Cyber Program
- M&A
- New Ventures / Innovation

Matt Christensen – Director – GRC
- BCDR
- GRC
  - Policy & Exceptions
  - Internal Risk Assessment
  - Third Party Review
  - Controls Framework
  - Controls Validation/PCI/ ISA
  - Risk Models
  - Risk Management
  - MAP Management
  - Contract Mgmt
  - Audit Management

Meridith McGlincy – Director – Cyber Service Mgmt
- Cyber Service Management
- Education & Awareness
- Service Taxonomy
- Service Delivery, SLA, adherence
- Governance Strategy
- Committee Representation
- Incident Outreach
- Liaison Management
  - Desert Region
  - Canyon Region
  - Peaks Region
  - Payor
  - Ventures

Michael Allred – Director – IAM
- Identity Lifecyle Management
- Federated IM
- Virtual Directory
- Design and Deployment
  - SSO
  - AccessHub provisioning
  - Others
- PAM Deployment
- Role Management

Jason King – Director – Architecture & Forensics
- Architecture
  - Standards Setting / PCI Design
  - Cyber Tech/Tools Strategy
  - Medical Device & IOT
  - Project security design & Build
  - SDLC
  - Cyber Consulting
- Forensics
  - Legal Investigations
  - eDiscovery
  - Search and Discovery

Todd Grubbs – Director – Engineering (SecOps)
- "Run" Cyber Ops
- T2 support
- KTLO for Cyber Stack (DLP, WAF, Firewall, AD, CASB, EDR,etc)
- Cloud Security Engineering
- Cyber Testing Environment Mgmt
- Production Deployment
- Active Directory

Nathan Moon – Director – Fusion Center
- Vuln mgmt (& PCI scans)
- Pentesters/Red Team
- Incident Response
- Threat Hunting
- Threat intelligence
- Attack Simulations

Mitzi McIntyre – Director – SCL Health
- Legacy SCL Operations during 24 month integration
  - SecOps
  - Vuln Mgmt
  - IAM
  - SOC T1/T2
  - Training and Education