

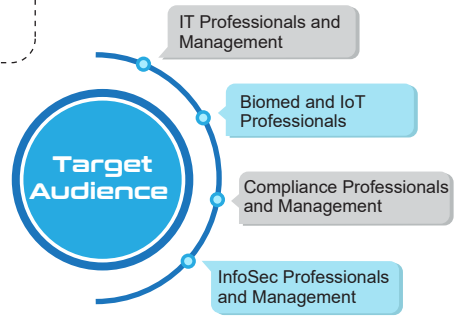
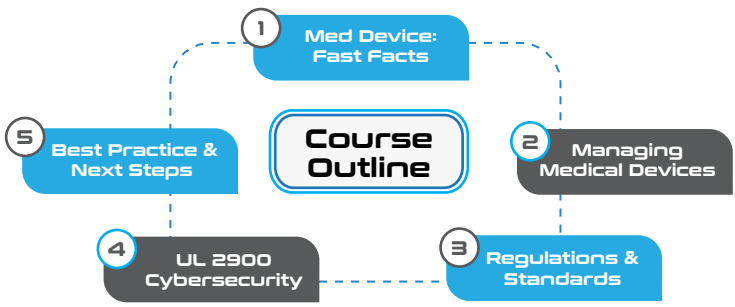
**Certified Biomed Cybersecurity & Compliance Professional<sup>SM</sup> (CBCCP<sup>SM</sup>)**

**Establishing a credible, evidence-based medical device cybersecurity program**

CBCCP<sup>SM</sup> program is focused on demonstrating knowledge of core regulations and standards in the area of biomed and Internet of Things (IoT) cybersecurity.

**Learning Objectives**

- 🔥 Examine healthcare cybersecurity compliance mandates that impact biomed and IoT devices and systems
- 🔥 Step thru key cybersecurity standards for protecting sensitive patient, medical and other sensitive information processed by biomed and IoT devices
- 🔥 Walk thru a sample biomed and IoT cybersecurity policy
- 🔥 Review best practices for establishing a credible, evidence-based biomed and IoT cybersecurity program
- 🔥 Learn how to quantify, rank, interpret and remediate vulnerabilities and assets for HIPAA compliance



**Certification Exam (Delivered at end of program)**

**Modules**

**Module 1**  
**Med Device: Fast Facts**

- 🔥 Types of Medical Devices
- 🔥 Categorization of Medical Devices
- 🔥 Lifecycle of Medical Devices
- 🔥 Medical Device Information Systems
- 🔥 Medical Device Information Flow

**Module 2**  
**Managing Medical Devices**

- 🔥 Asset Management of Medical Devices
- 🔥 Stakeholders in Medical Devices Security
- 🔥 Shared Responsibility: Medical Device Safety, Performance and Security

**Module 3**  
**Regulations & Standards**

- 🔥 State of biomed and IoT Cyber Risk
  - 💡 Vulnerabilities
  - 💡 IoT & DDoS
- 🔥 Global Harmonization Task Force (GHTF)
- 🔥 Healthcare Cybersecurity Compliance Mandates
  - 💡 HIPAA & PHI
  - 💡 SB 327 & PII
- 🔥 Cybersecurity Program
  - 💡 NIST Cybersecurity Framework
  - 💡 NIST IR 8228

**Module 4**  
**UL 2900 Cybersecurity**

- 🔥 Understanding UL 2900
- 🔥 Network Connecting Products, UL 2900-1
- 🔥 Medical and Healthcare Systems, UL 2900-2-1
- 🔥 Industrial Control Systems, UL 2900-2-2
- 🔥 Security and Life Safety Signaling Systems, UL 2900-2-3
- 🔥 IoT Cybersecurity

**Module 5**  
**Best Practice & Next Steps**

- 🔥 Getting Started: Key Steps
  - 💡 Risk Assessment
  - 💡 Vulnerability Assessment
  - 💡 Asset Management
  - 💡 Remediation
  - 💡 Policy
  - 💡 Procedure
  - 💡 Evidence



Kris Laidley

Kris.Laidley@ecfirst.com