ENTERPRISE INFORMATION SECURITY TEAMS

Old School VS STATE OF THE ART

MISSION

Old School: Concentrates on conventional security activities such as:
- Developing policy
- Implementing and operating security controls

State of the Art: Shifts focus to business-centric and advanced technical activities such as:
- Business risk analysis
- Asset valuation
- IT supply chain integrity
- Cyber threat intelligence
- Security data analytics
- Data warehousing
- Process optimization

EXPERTISE

Old School: IT professionals with security skills

State of the Art: Multidisciplinary group of specialists with diverse business leadership and technical skills

FOCUS

Old School: Focuses on reactive and day-to-day activities

State of the Art: Focuses on proactive and strategic activities

APPROACH

Old School: Siloed approach with "we'll do it all ourselves" attitude

D.I.Y.

State of the Art: Collaborative approach with shared accountability for protecting information

VIEW OF RISK

Old School: Check-list or compliance view whereby Security's goal is to mitigate all risks

State of the Art: Business units own the risk/reward decisions. Security operates a risk consultancy to advise the business on assessing and managing risks

THREAT DETECTION

Old School: Look at security events generated by dedicated security devices

State of the Art: Use intelligence-driven security to detect malicious activity within business processes
- Collect data from various internal and external sources
- Apply data-enrichment and analytics techniques

CONTROLS OPERATION

Old School: Basic infrastructure security controls are operated by Security

State of the Art: Selected, well-established, repeatable security processes are delegated to internal and external service providers
- Governed by Security through Service Level Agreements (SLAs)

CONTROLS ASSESSMENT

Old School: Auditors periodically assess security controls using manual methods

State of the Art: Controls assurance analysts continuously collect evidence on the efficacy of security controls using more automated methods. Auditors use this evidence in their assessments

PROCESS IMPROVEMENTS

Old School: Security processes are improved on an ad-hoc basis

State of the Art: Security processes are consistently tracked, measured, and optimized based on process expertise and formalized methods

TALENT

Old School: Mostly backgrounds in IT and security

State of the Art: Broadened to also include backgrounds such as data science, math, history, economics, military intelligence, and business analysis