

e⁺

The Shared ISO Model



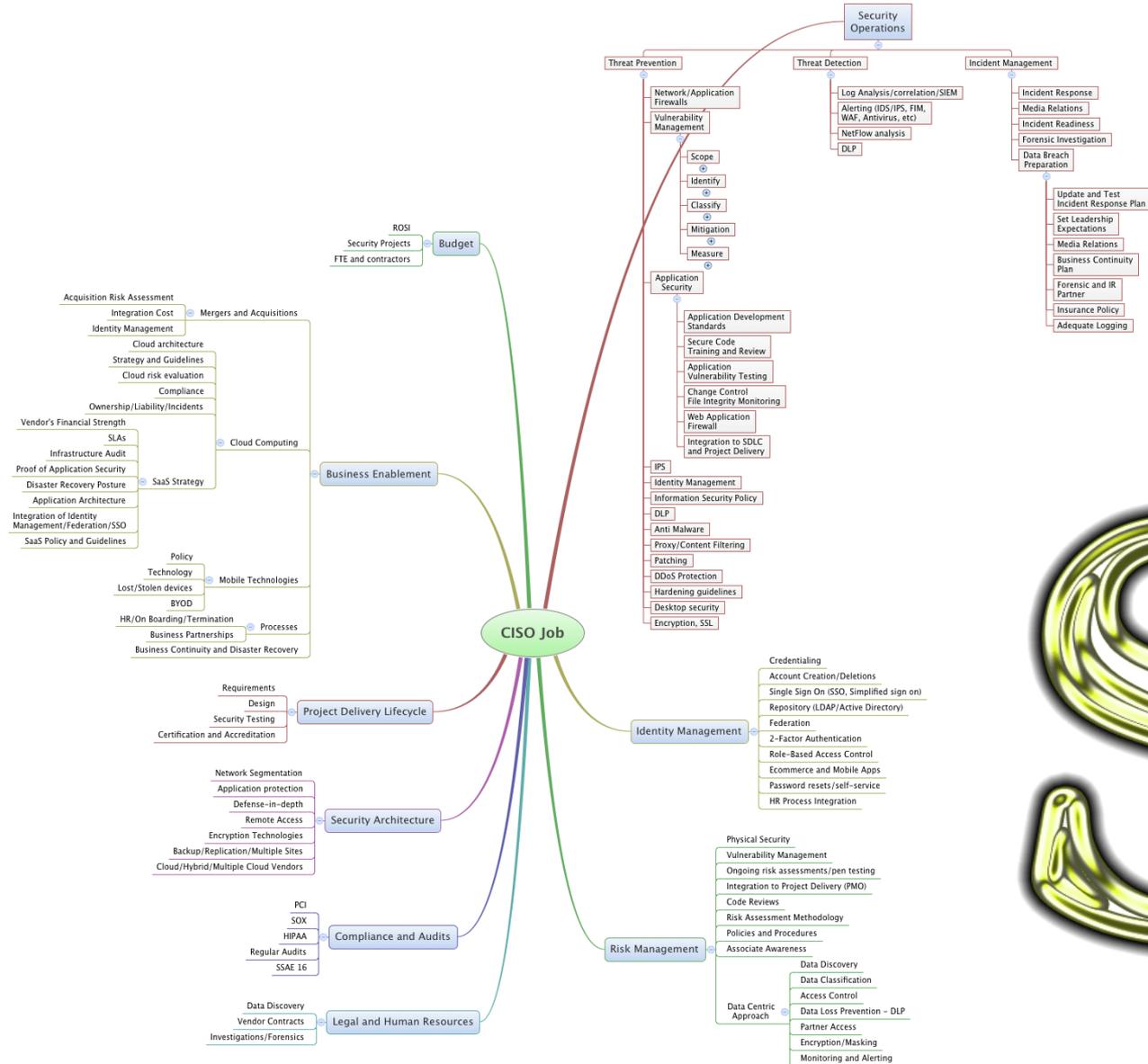
EXCELLENCE THROUGH EXPERIENCE

Tom Bowers
vCISO
ePlus Technologies, Inc
Spring 2015

**PRO
BLE
M**

Technology





- + Philadelphia
 - Bucknell U
 - Franklin and Marshall College
 - Susquehanna U

- + New York 6
 - Liberal Arts universities
 - 250 mile radius
 - Upstate NY

- + Howard County MD
 - CISO in Residence
 - Howard Technology Council

The original



- + Working with CIOs
 - Secondary responsibility is security
- + Translate security into CIO speak
- + Mentor
- + Coach
- + Personal Trainer



+ Security as Business Risk

+ The more supported OUs, diverse the OUs are or complex the challenges

- the more seasoned the resource required
- the more expensive the resource is

+ Each supported OU has

- Unique risk appetite
- Political climate
- Own view on importance of security
- Varying levels of security maturity

Functionally How Does This Work?

- + Shared ISO is located at one OU location
- + Supports others remotely normally
- + Makes scheduled visits to all supported OUs
- + Creates Security Council with all OUs
- + Promotes innovation and common practices among OUs
- + Fosters N/S and E/W communication



+ Tabletop assessment of each supported OU

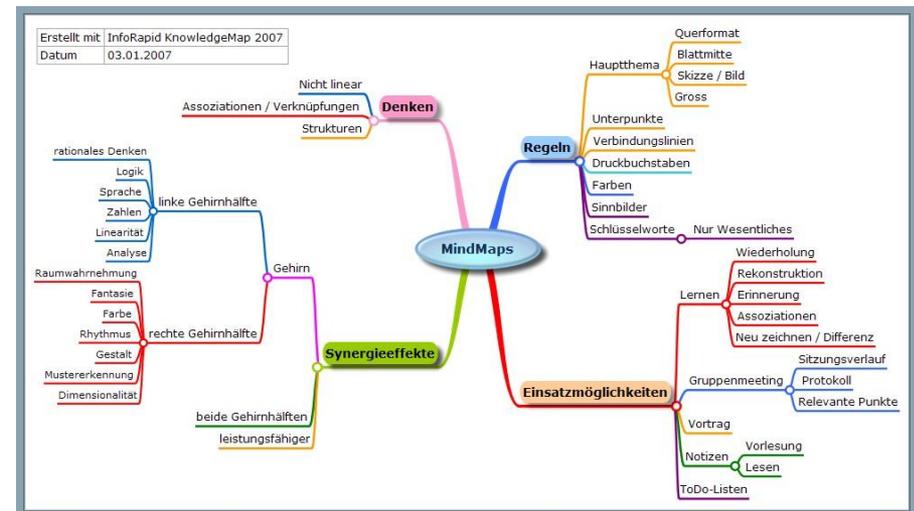
1

- Risks
 - Appetite
 - Enterprise
- Culture
 - Security
 - Political
- Maturity
- Policies
- Current deployed technologies
- Sensitive data types and usage
- Security / business alignment

2

+ Create

- Immediate needs / wins
- Prioritized road map for maturity



- + Change management
- + Patch management
- + **Weakness in any of these results in greater enterprise risk**

THE THIEF



- + Communication amongst OUs is critical
- + The ISO interprets threats into business risk for the OUs
- + The ISO fosters creation of a common threat management protocol
- + The ISO creates a common threat communication protocol
- + The ISO converts OSINT into actionable intelligence for the OUs



- + The ISO should assist each OU with:
 - Is the OU taking reasonable security steps
 - Does the OU have a written security improvement plan with timetable
 - Does the OU have a security framework in place / in progress?
 - OU Incident Response Plan / Team
 - Has the OU IR Team been trained?
 - Does the OU have an IR Communication Plan?
 - Does the OU have a LEO Engagement Plan?



How do You Get Started?

- + Determine the OUs who are interested
- + Determine common objectives for security
- + Determine cost sharing model
- + Determine where the ISO will reside
- + Hire or Appoint?





tbowers@eplus.com