RSAConference2019

San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: LAB2-R03

Cybersecurity Leadership Effectiveness Using the McKinsey 7S Framework

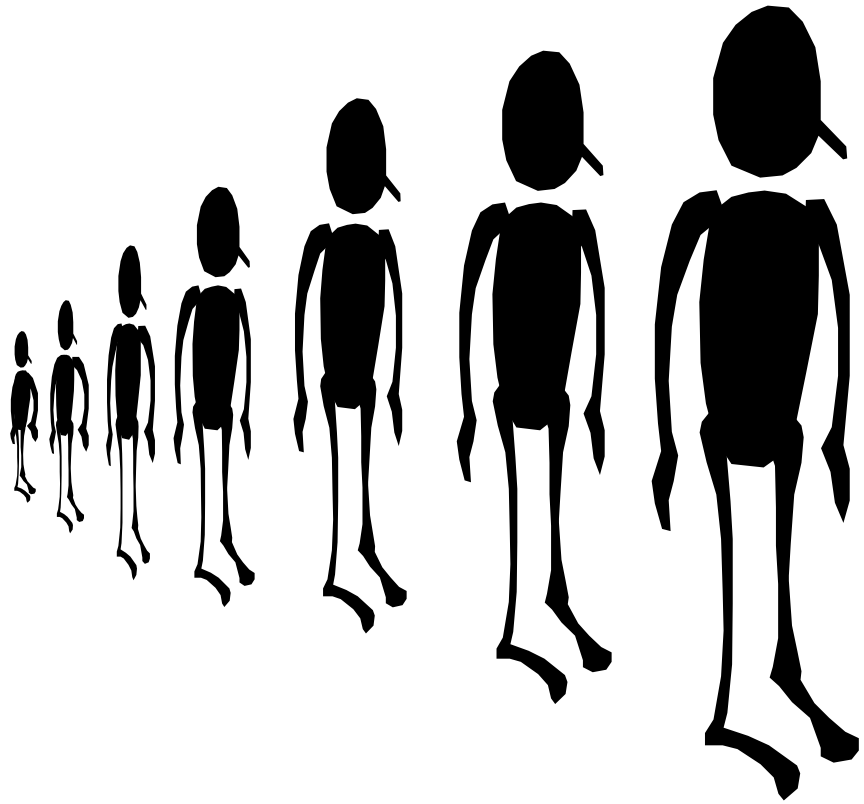
3/7/19 9:20 AM - 11:20 AM

Todd Fitzgerald, CISSP, CISA, CISM,
CIPP/US, CIPP/EU, CIPP/CANADA,CIPM, ISO27001, PMP, ITILv3f

Managing Director/CISO
Cybersecurity Leadership Author
CISO SPOTLIGHT, LLC
@securityfitz

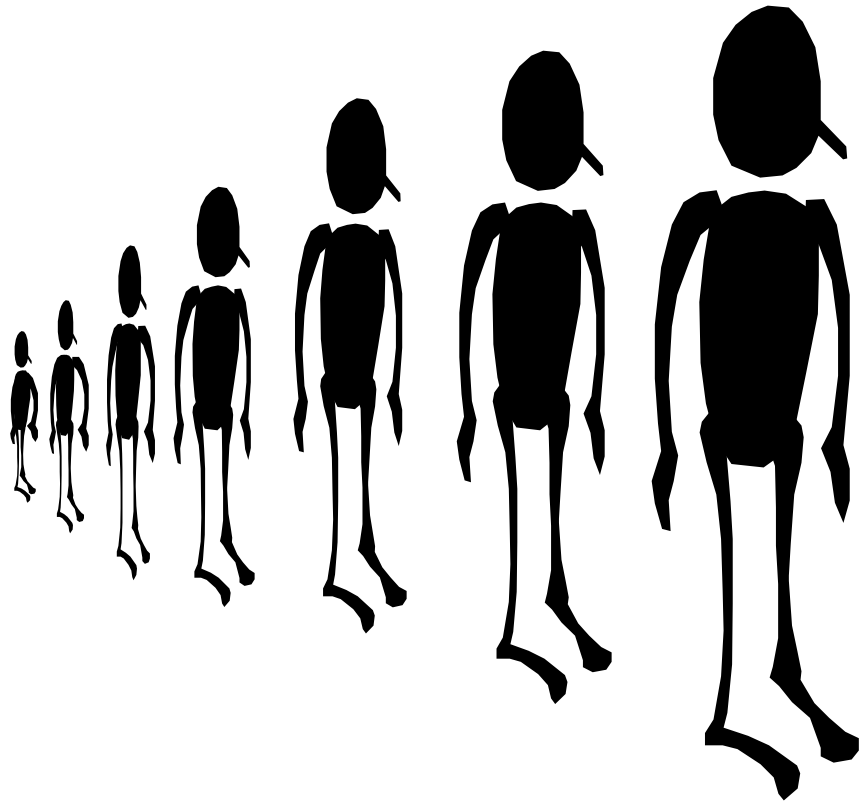
Introductions… And You Are???

- Hi My Name Is…
- I Work for…
- My role is…



Introductions… And You Are???

- Hi My Name Is…
- I Work for…
- My role is…



How can we make this session a success??

ABC’S OF CYBERSECURITY

A. 55 MILLION

B. 1.4 BILLION

C. 11.5 BILLION

D. 136…807…9,003

We have a data protection problem

Enter…. The Chief Information Security Officer (CISO)

Where Do CISOs Come From ?

- Born as natural paranoid leaders
- Raised their hand at the wrong time during a meeting
- Didn't attend the selection meeting
- Last IT guy in the shop
- Worked on compliance stuff
- Chose this career (full deck should be checked)

Hey We Need a CISO – Here is the Job Description

- The CISO position requires a visionary leader with sound knowledge of business management and cybersecurity technologies covering the corporate network and the broader digital ecosystem. As the organization's senior IT security officer, the CISO has enterprise-level responsibility for all data/information security policies, standards, evaluations, roles, and organizational awareness. The CISO is responsible for the establishment and overall management of the information security program for the company, and must proactively work with business units and ecosystem partners to implement practices that meet agreed-on policies and standards for information security. He/She must understand Information Technology and oversee a variety of cybersecurity and IT related risk management activities necessary to ensure the achievement of business outcomes.

- The CISO should understand and articulate the impact of cybersecurity on (digital) business and be able to communicate this at all levels of the organization, up to the board of directors. The CISO serves as the process owner of the appropriate second-line assurance activities not only related to confidentiality, integrity and availability, but also to the safety, privacy and recovery of information owned or processed by the business in compliance with regulatory requirements. The CISO understands that securing information assets and associated technology, applications, systems and processes in the wider ecosystem in which the organization operates is as important as protecting information within the organization's perimeter. A key element of the CISO's role is working with executive management to determine acceptable levels of risk for the organization.

… With Responsibilities

• Develop, implement, maintain, and monitor a comprehensive strategic information security program to ensure that appropriate levels of confidentiality, integrity, availability, safety, privacy and recovery of information assets are met• Provide leadership through strong working relationships and collaboration to develop strategic goals for information security compliance and risk mitigation• Liaise with external partners as necessary to ensure the organization maintains a strong security posture against relevant threats and advancing threat landscape• Develop a KPI, metrics and reporting framework to measure the efficiency, effectiveness, and continuous increase in the maturity of the information security program• Lead and coordinate the development and maintenance of information systems security policies, procedures, standards, and guidelines in compliance with corporate, federal and state laws and regulations• Develop and maintain the Computer Security Incident Response Plan. Provide hands on leadership of the C-SIRT team to contain, investigate, and prevent future breaches of personal or confidential information• Identify and assess risks in implementing business innovations. Provide assessment of those risks to business stakeholders• Design and execute penetration tests and security audits• Monitor compliance with the organization's information security policies and procedures among employees, contractors, alliances, and other third parties• Oversee the development and implementation of training programs and communications to make systems, network, and data users aware of and understand security policies and procedures• Work with legal, risk and compliance staff to ensure all information owned, collected, and controlled by or on behalf of the company is processed and stored in accordance with applicable laws and other regulatory requirements. Collaborate and liaise with privacy officer to ensure that data privacy requirements are included in the security program• Stay well-informed of best practices in the IT security field, coordinate and/or evaluate new and emerging security practices and technologies, and recommend and promote adoption as appropriate• Work closely with Information Technology, and the Security Operations Center (SOC) to identify cybersecurity risks and develop remediation strategies• Inform IT security architecture to include engineering best practices for security controls• Manage an information security risk mitigation plan based on sound risk analysis • Develop and mature the organization’s security assessment program. Perform regular security assessments of effectiveness of policies/procedures and systems security safeguards• Ensure the timely remediation of security vulnerabilities within the environment and produce compliance KPIs;• Consult IT and technical teams on addressing security risk, providing security information and input to strategic and tactical planning, and the appropriate and effective use of IT resources;• Implement, manage and enforce information security directives within regulatory mandates to protect PHI, including Federal HIPAA and HITECH and any applicable state laws.• Cooperate with the regulatory bodies in any lawful compliance reviews or investigations related to patient health information security• Support compliance through participation in regulatory compliance and information security committees• Serve as the information security lead on the Privacy Council; • Build external relationships to identify external cybersecurity threats impacting the industry and influence threat intelligence sharing. • Monitor changes in legislation and accreditation standards that affect information security.

… And Qualifications

Qualifications Bachelor's degree in a related field (Computer Science or related field).

Advanced degree preferred.

• 10-15 years of progressive IT Security experience, including cybersecurity and risk management, within a large corporate environment with at least 5 years in a management role• Must possess professional security management certification such as a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), or other similar credentials

• Demonstrated knowledge of common information security management frameworks such as ISO/IEC 27001 and or HITRUST, ITIL, COBIT and NIST, and an understanding of relevant legal and regulatory requirements such as Payment Card Industry/Data Security

• Demonstrated experience of leading an advanced security program including sophisticated technologies in a defense-in-depth architected environment

• Knowledge of network related protocols and security event log management and reporting tools.

• Experience with maintaining operational computer and network security, firewall administration, virus protection, intrusion detection and prevention, automated security patching, and vulnerability scanning systems

• Experience with data breach management and managing an actual data breach.

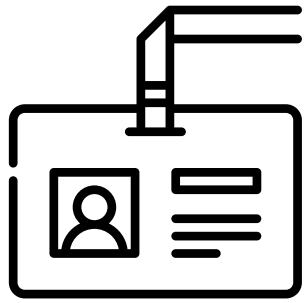
• Demonstrated experience with leading a SOC utilizing advanced threat and intelligence technology

• Leadership qualities, and proven experience as an effective manager and influencer of people

• Outstanding interpersonal and communication skills• High degree of integrity and trust, and ability to work independently

• Ability to weigh business risk and enforce appropriate information security measures

5 STAGES OF CISO EVOLUTION 1995-2020s



1. Limited Security= Logon & Password FIRST CISO 1995

1990s-2000

2. Regulatory Compliance Era CISOs Hired

2000-2004

3. Risk-Oriented CISO Emerges

2004-2008

4. Threat-Aware Cybersecurity, Socially-Mobile-Cloud CISO

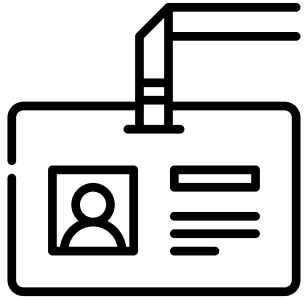
2008-2016

5. The Privacy and Data-Aware CISO

2016-2020s

Source: T. Fitzgerald, *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers* (2019, Auerbach Publications)

5 STAGES OF CISO EVOLUTION 1995-2020s



1 Limited Security= Logon & Password FIRST CISO 1995

1990s-2000

2 Regulatory Compliance Era CISOs Hired

2000-2004

3 Risk-Oriented CISO Emerges

2004-2008

4 Threat-Aware Cybersecurity, Socially-Mobile-Cloud CISO

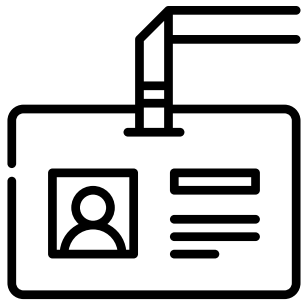
2008-2016

5 The Privacy and Data-Aware CISO

2016-2020s

Source: T. Fitzgerald, *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers* (2019, Auerbach Publications)

5 STAGES OF CISO EVOLUTION 1995-2020s



1 Limited Security= Logon & Password FIRST CISO 1995

1990s-2000

2 Regulatory Compliance Era CISOs Hired

2000-2004

3 Risk-Oriented CISO Emerges

2004-2008

4 Threat-Aware Cybersecurity, Socially-Mobile-Cloud CISO

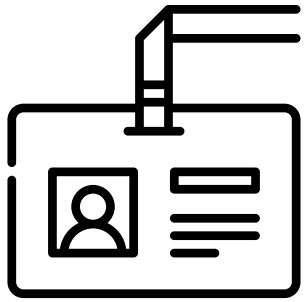
2008-2016

5 The Privacy and Data-Aware CISO

2016-2020s

Source: T. Fitzgerald, *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers* (2019, Auerbach Publications)

5 STAGES OF CISO EVOLUTION 1995-2020s



1 Limited Security= Logon & Password FIRST CISO 1995

1990s-2000

2 Regulatory Compliance Era CISOs Hired

2000-2004

3 Risk-Oriented CISO Emerges

2004-2008

4 Threat-Aware Cybersecurity, Socially-Mobile-Cloud CISO

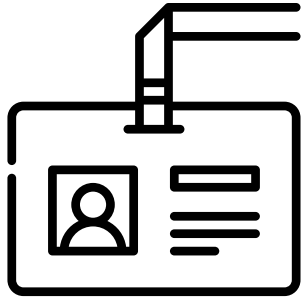
2008-2016

5 The Privacy and Data-Aware CISO

2016-2020s

Source: T. Fitzgerald, *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers* (2019, Auerbach Publications)

5 STAGES OF CISO EVOLUTION 1995-2020s



1 Limited Security= Logon & Password FIRST CISO 1995

1990s-2000

2 Regulatory Compliance Era CISOs Hired

2000-2004

3 Risk-Oriented CISO Emerges

2004-2008

4 Threat-Aware Cybersecurity, Socially-Mobile-Cloud CISO

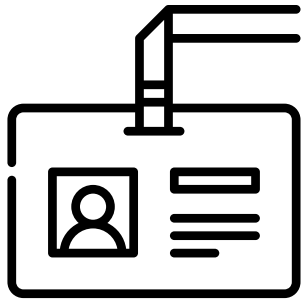
2008-2016

5 The Privacy and Data-Aware CISO

2016-2020s

Source: T. Fitzgerald, *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers* (2019, Auerbach Publications)

5 STAGES OF CISO EVOLUTION 1995-2020s



1. Limited Security= Logon & Password FIRST CISO 1995

1990s-2000

2. Regulatory Compliance Era CISOs Hired

2000-2004

3. Risk-Oriented CISO Emerges

2004-2008

4. Threat-Aware Cybersecurity, Socially-Mobile-Cloud CISO

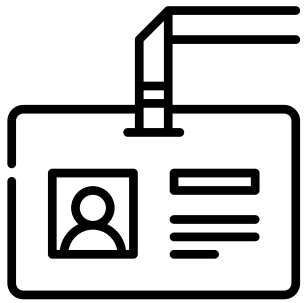
2008-2016

5. The Privacy and Data-Aware CISO

2016-2020s

Source: T. Fitzgerald, *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers* (2019, Auerbach Publications)

5 STAGES OF CISO EVOLUTION 1995-2020s



1 Limited Security= Logon & Password FIRST CISO 1995

1990s-2000

2 Regulatory Compliance Era CISOs Hired

2000-2004

3 Risk-Oriented CISO Emerges

2004-2008

4 Threat-Aware Cybersecurity, Socially-Mobile-Cloud CISO

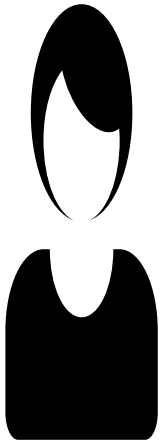
2008-2016

2016-2020s

5 **The Privacy and Data-Aware CISO**

Source: T. Fitzgerald, *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers* (2019, Auerbach Publications)

And The Process Is Simple



STEP 1: Start as a Programmer Analyst

STEP 2: Education to Become a Security Analyst

STEP 3: Get Extra Certifications and Training

STEP 4: Oversee a Security Team

STEP 5: Attain an MBA with an IT Security Focus

Step 6: Promotion to CISO

Source: Adapted from a cyber security education website promoting higher education, July 2018

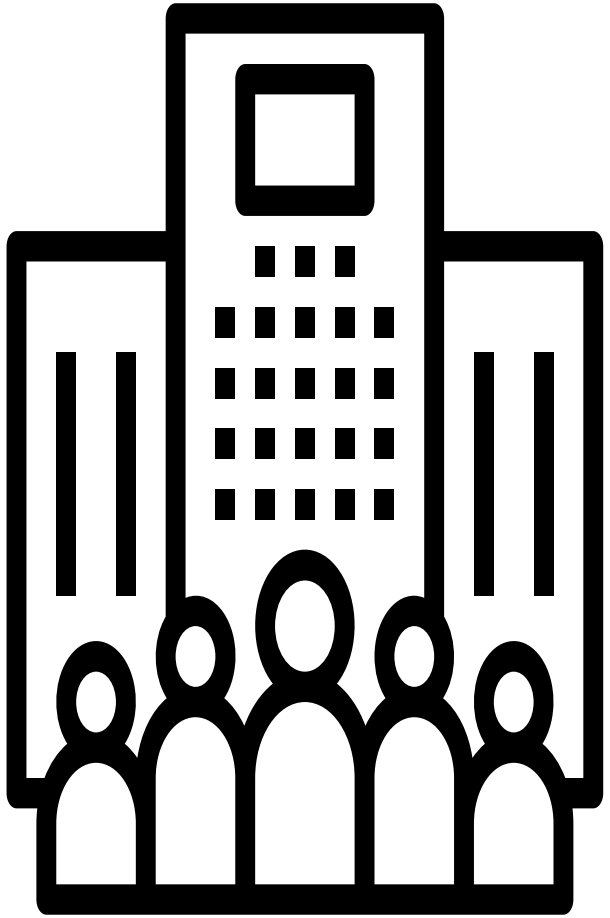
What Degrees Do the Fortune 500 CISOs Prefer ?

UNDERGRADUATE	GRADUATE
Computer Science 18.4%	MBA 44.8%
Business 9.2%	Computer Science 7.7%
Management Information Systems 8.9%	Management Information Systems 5.0%

Source: 2017 Forrester Research, Base 326 Fortune 500 CISOs reporting undergraduate education on LinkedIN; 181 Fortune 500 CISOs reporting graduate degrees

Do CISOs Get Promoted from Within ?

59% Fortune 500 CISOs External Hires



Few F100 hired first-time CISO; rest of F500 ok with that

4% CISOs have SVP title; 2/3 were external hires

F500 CISOs average tenure 4.5 years

Source: 2017 Forrester Research, CISO Career Paths: Plot Your Course for Advancement

Evolution of the CISO Role Pre-2000 to Present

Dimension	Pre-2000	2000-2003	2004-2008	2008-2016 & 2016-2020s*
Technology	Firewalls Anti-Virus	GRC Tools	Identity Management	Social Media iPads/Tablets File sharing Virtualization
Organization	Data Center	Committee	CISO in IT	CISO outside IT
Laws/Regs	EU Directive	HIPAA, GLBA, PCI, FISMA	NIST Regs, ISO27001:05	*Privacy Focus (2016-2020s) *Data Aware (2016-2020s)
Media Incidents	Infrequent	Breach Notification	Few companies, big attention	Many companies, large ones noticed
Security Issue	Technology	Technology Compliance	Risk	Vendor Consumer

WE NEED GOVERNANCE OVER CYBERSECURITY

"**Information Security governance** is a subset of enterprise governance that provides strategic direction, ensures objectives are achieved, manages risk appropriately, uses organizational resources responsibility, and monitors the success or failure of the enterprise security programme."

- IT Governance Institute

WIKIPEDIA EXPANDS THE DEFINITION…

- **Governance** relates to decisions that define expectations, grant power, or verify performance. It consists either of a separate process or of a specific part of management or leadership processes. Sometimes people set up a government to administer these processes and systems.
- In the case of a business or of a non-profit organization, governance relates to consistent management, cohesive policies, processes and decision-rights for a given area of responsibility. For example, managing at a corporate level might involve evolving policies on privacy, on internal investment, and on the use of data.

LATIN ORIGINS TO DENOTE ‘STEERING’

- Steering Vs “Power Over”
- Defines expectations
- Grants power
- Verifies performance
- Avoids undesirable consequences
- Coordinates and controls activity
- Provides processes to control an activity

NO SILVER BULLET TO SOLVE THE DATA BREACH PROBLEM ??

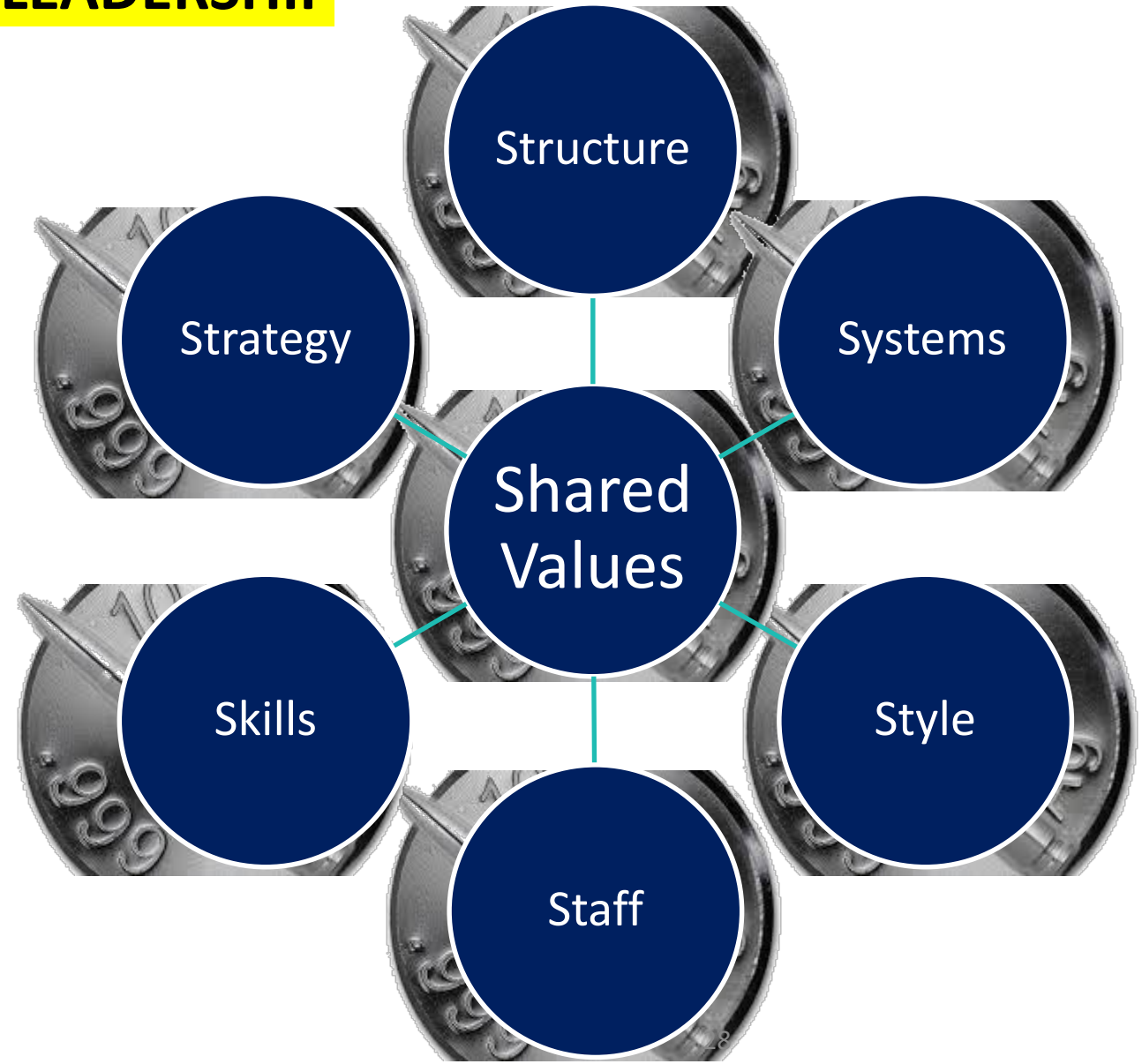
MAYBE, BUT

Here Are 7 Bullet Points ("Factors") To Help the CISO

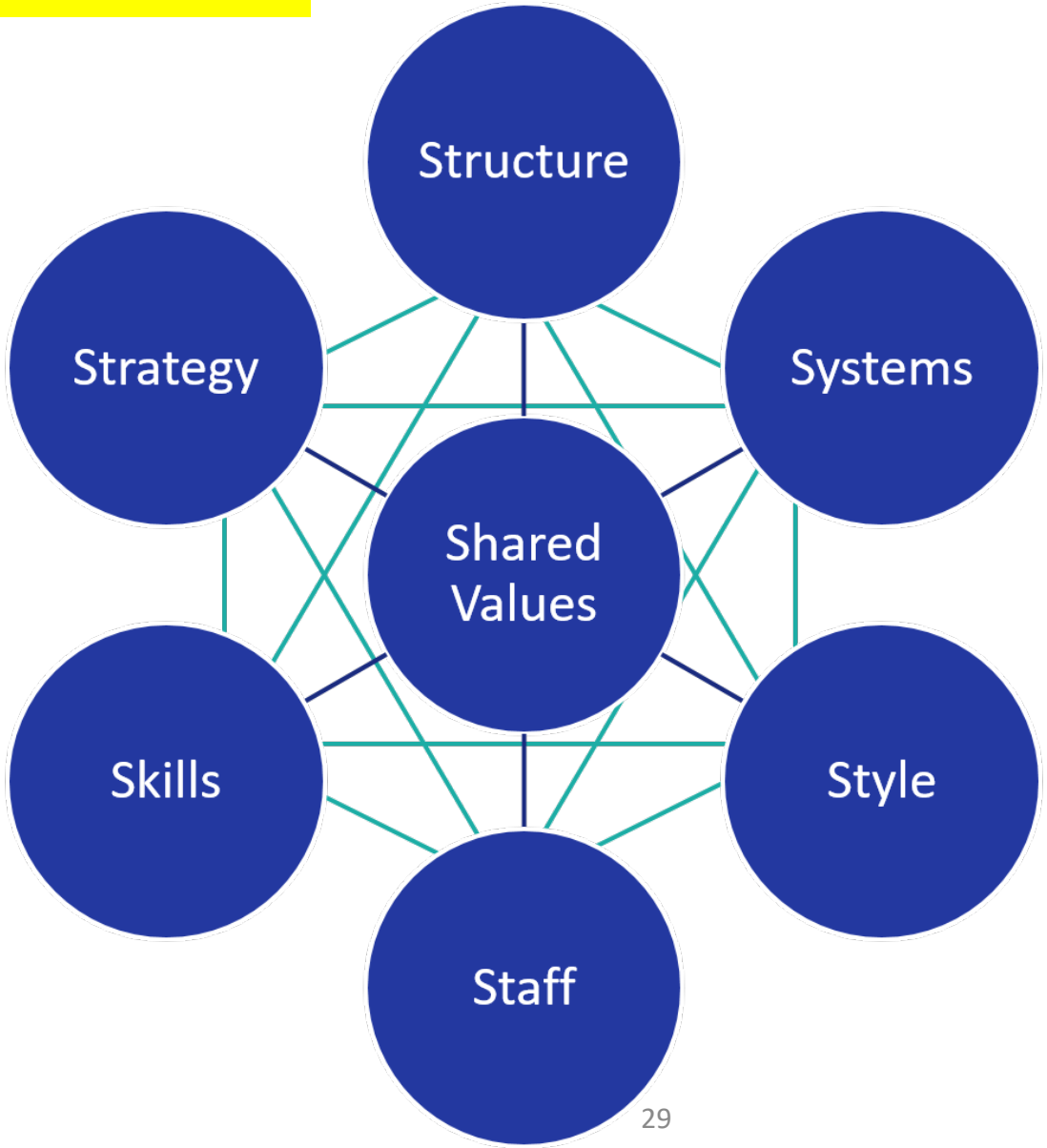
CISO SPOTLIGHT, LLC
Trusted Cybersecurity and Privacy Training

RSAConference2019

CYBERSECURITY LEADERSHIP Roadmap 7-S FRAMEWORK APPLIED TO CYBERSECURITY LEADERSHIP

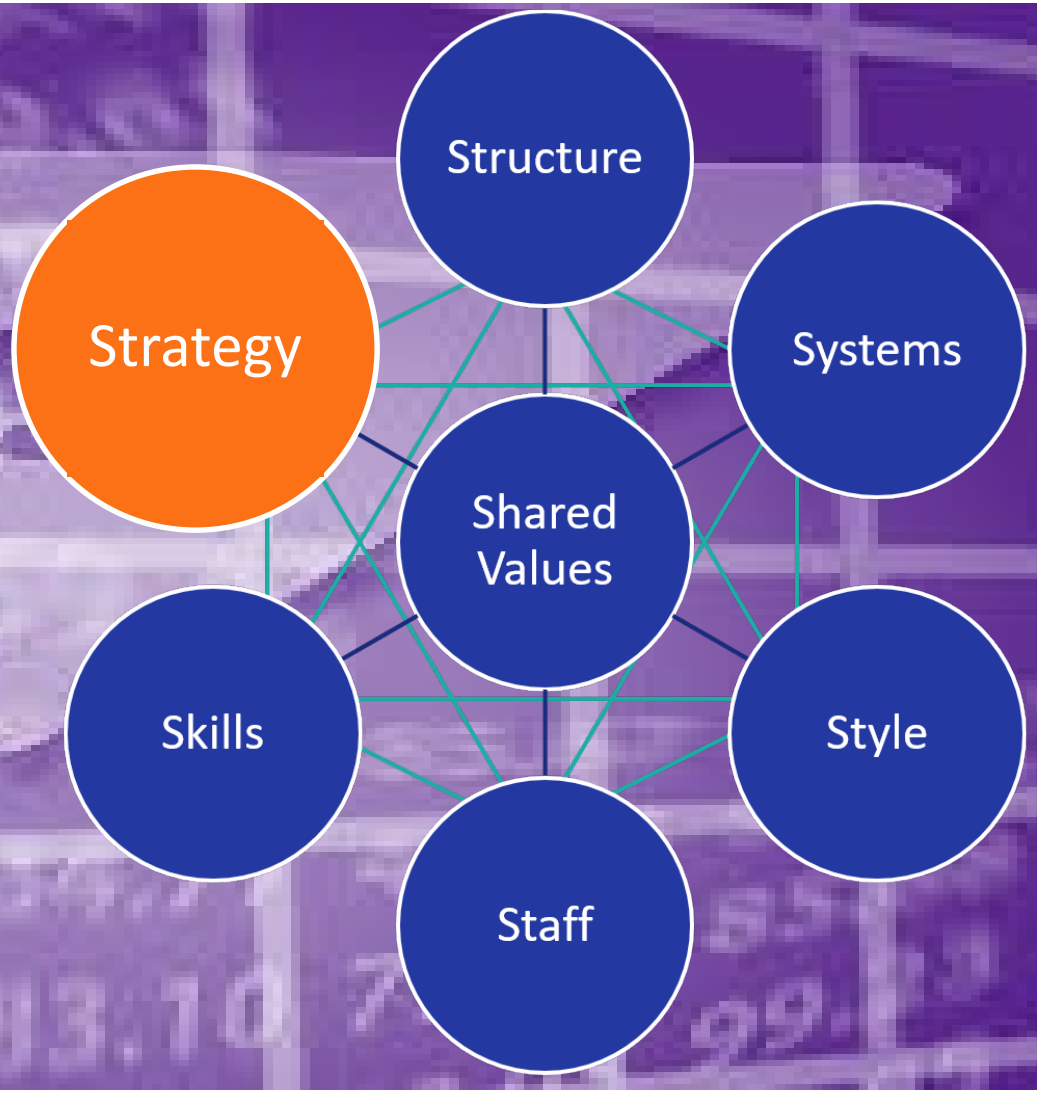


CYBERSECURITY LEADERSHIP Roadmap 7-S FRAMEWORK APPLIED TO CYBERSECURITY LEADERSHIP



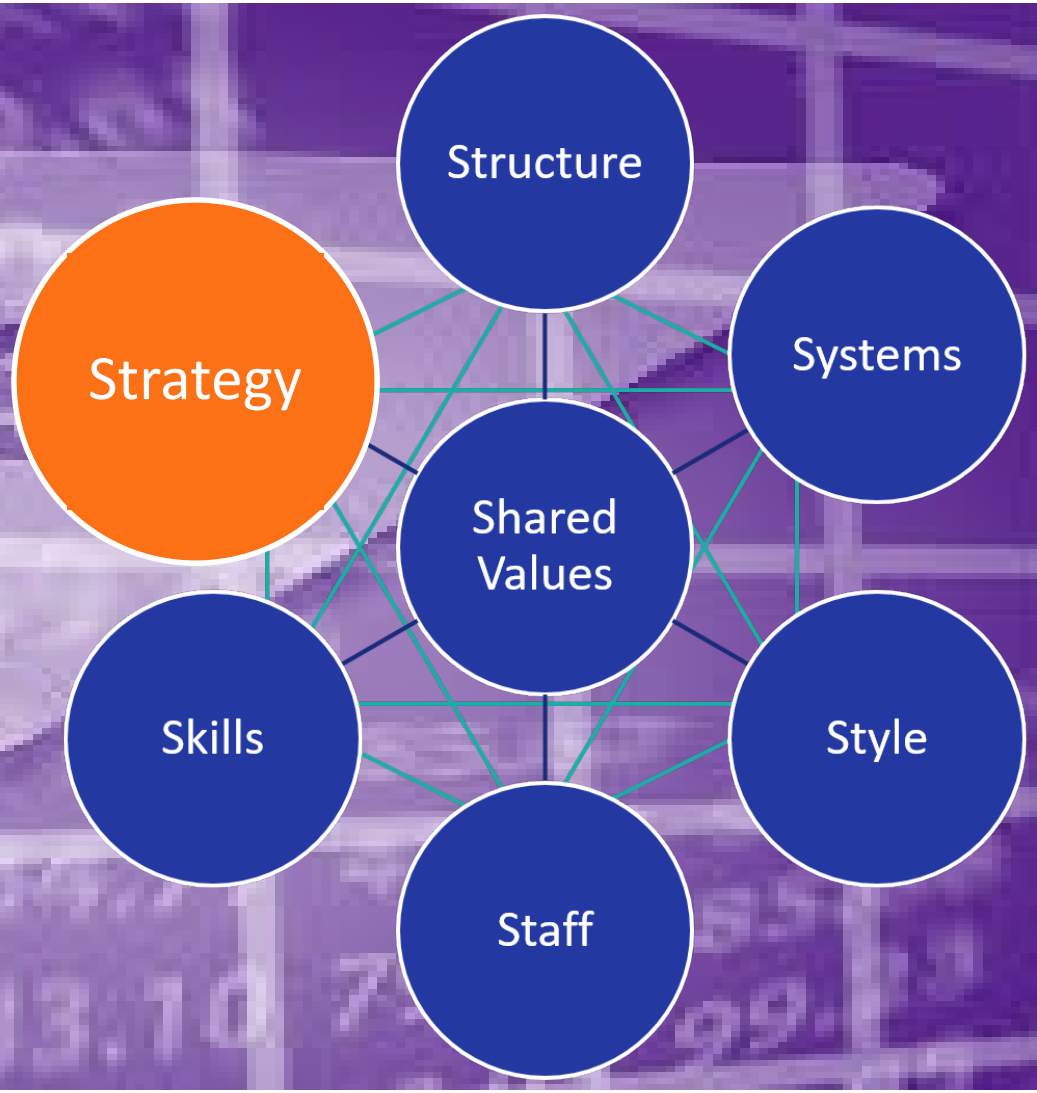
CYBERSECURITY STRATEGY

HOW DO WE MEET OUR ORGANIZATION'S OBJECTIVES SECURELY?

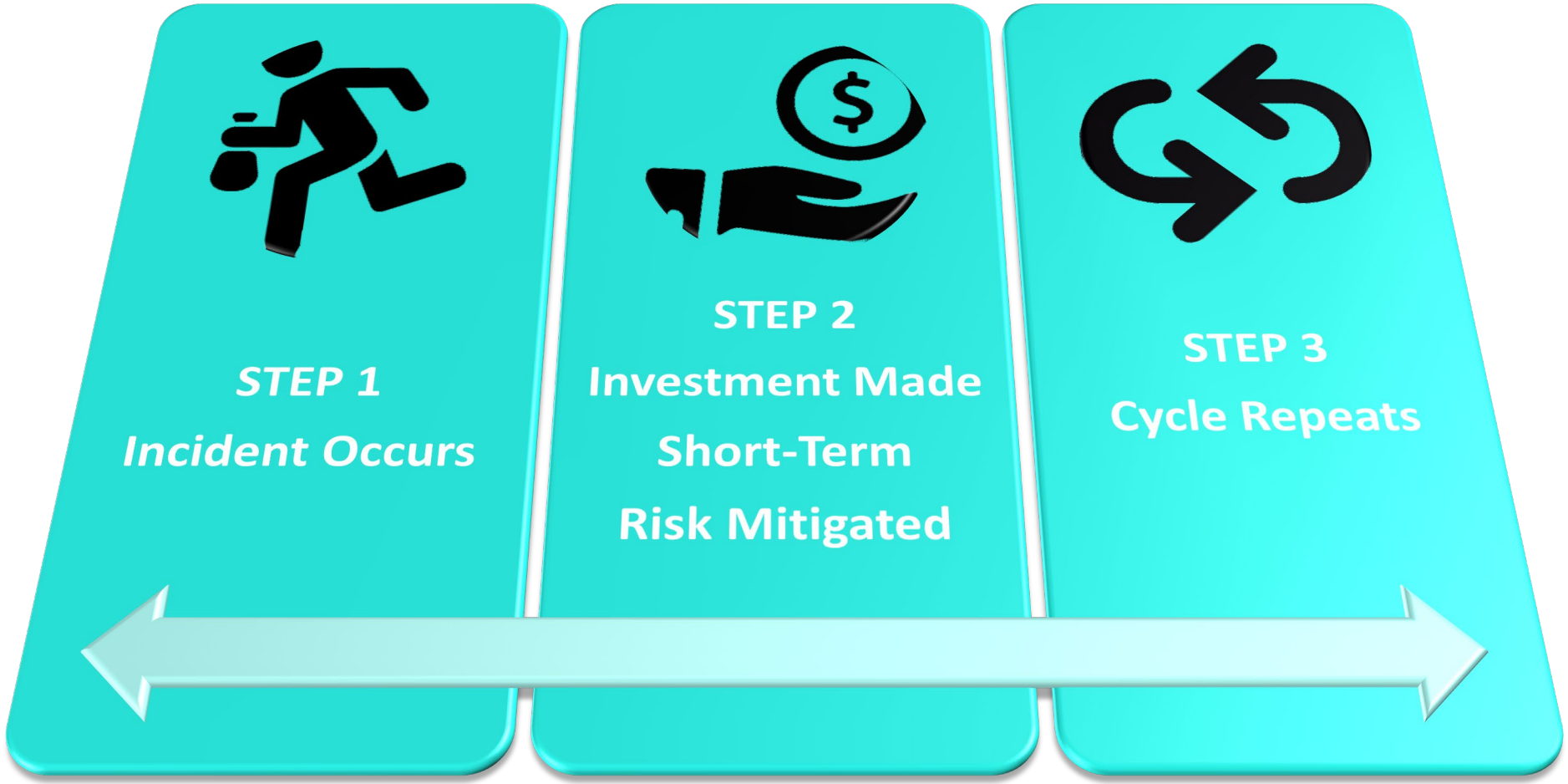


DEVELOPING STRATEGY

- 4 Cybersecurity Development Methods
  - Incident-driven
  - Top-down (Vision)
  - Bottom-up (Infrastructure)
  - Toss-the-ball-in-bushel-basket
- 6-step Vision to Plan approach
- Mind-Mapping
- Balanced Scorecard
- SWOT Analysis

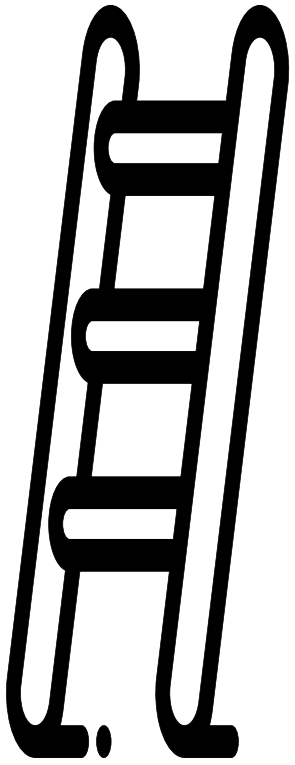


Strategy Approach #1: Incident-Driven Strategy



Incident-Driven Strategy

Strategy Approach #2: Top-Down (Vision)



Company Vision

Company Mission Statement

Cybersecurity Mission Statement

Cybersecurity Goals Aligned to Business Goals

12-18 Month Initiatives (Short-term)

18 Month-3 year Initiatives (Long-Term)

Year 3-5+ Initiatives (Future Consideration)

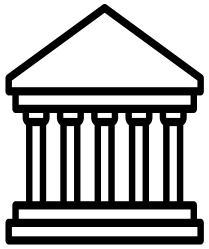
Cybersecurity Project A

Cybersecurity Project B

Cybersecurity Project C

Strategy Approach #3: Bottom-Up (Infrastructure)

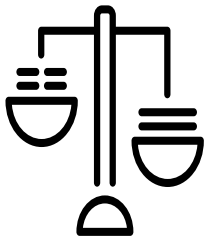
Technology Gap Focus



Laws

Regulations

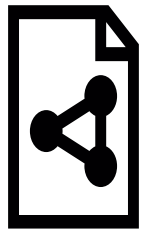
Industry Practices



Audit Finding Mitigation

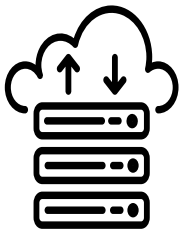
Technical Gap Analysis

New Vendor Products



Control Frameworks

Configuration Standards



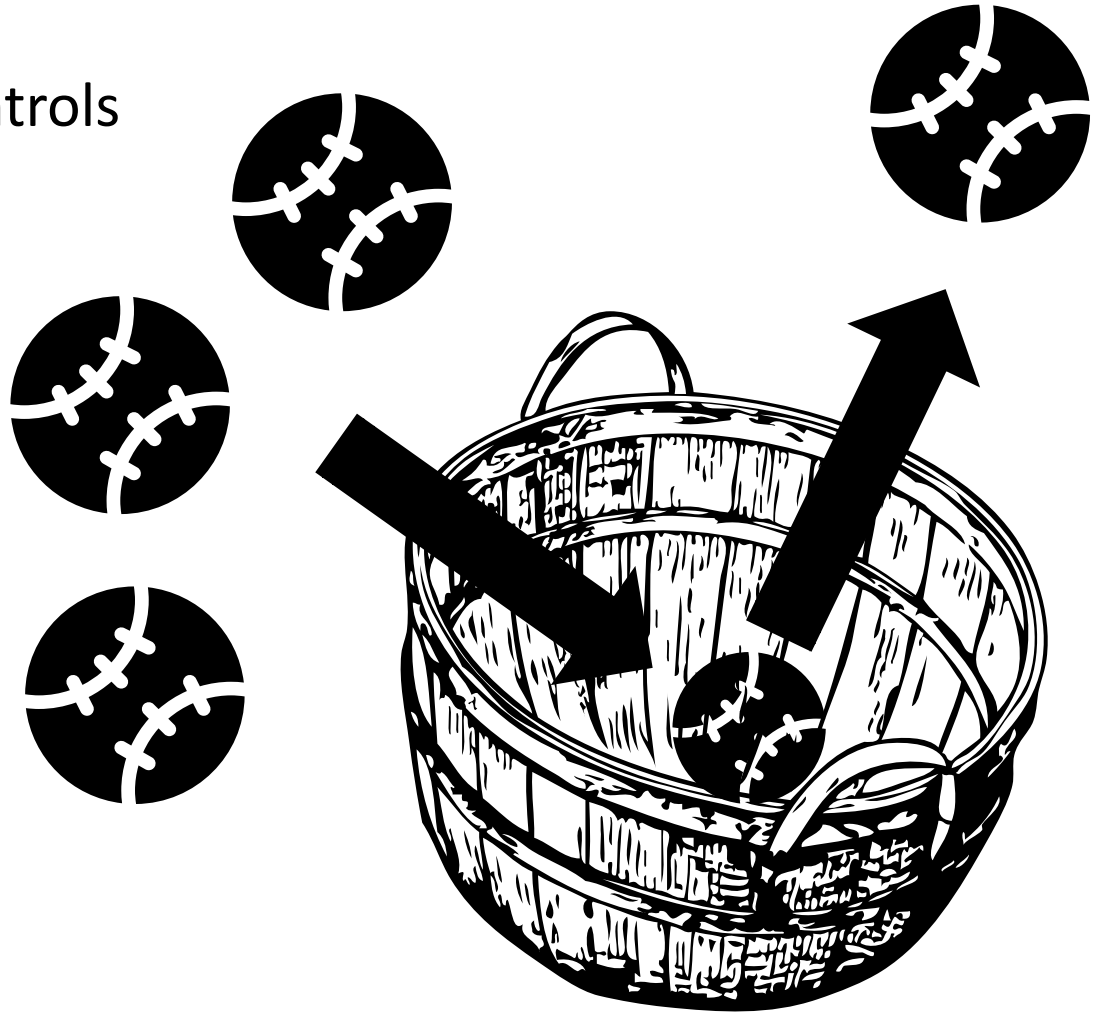
Technical Architecture

Strategy Approach #4: Toss-a-Softball-In-The-Bushel-Basket Unconscious Approach

Technical Controls

Administrative Controls

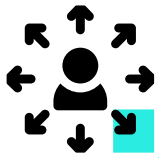
Operational Controls



Alternative Approach: SWOT Analysis

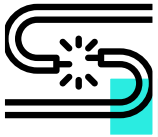
STRENGTHS

- Phishing Program
- Alignment to control framework
- Tracking of Laws
- Vendor Risk Management



OPPORTUNITIES

- Increase Metrics
- Offload to MSSP
- Acquire Cyber Insurance
- Intern Program



WEAKNESSES

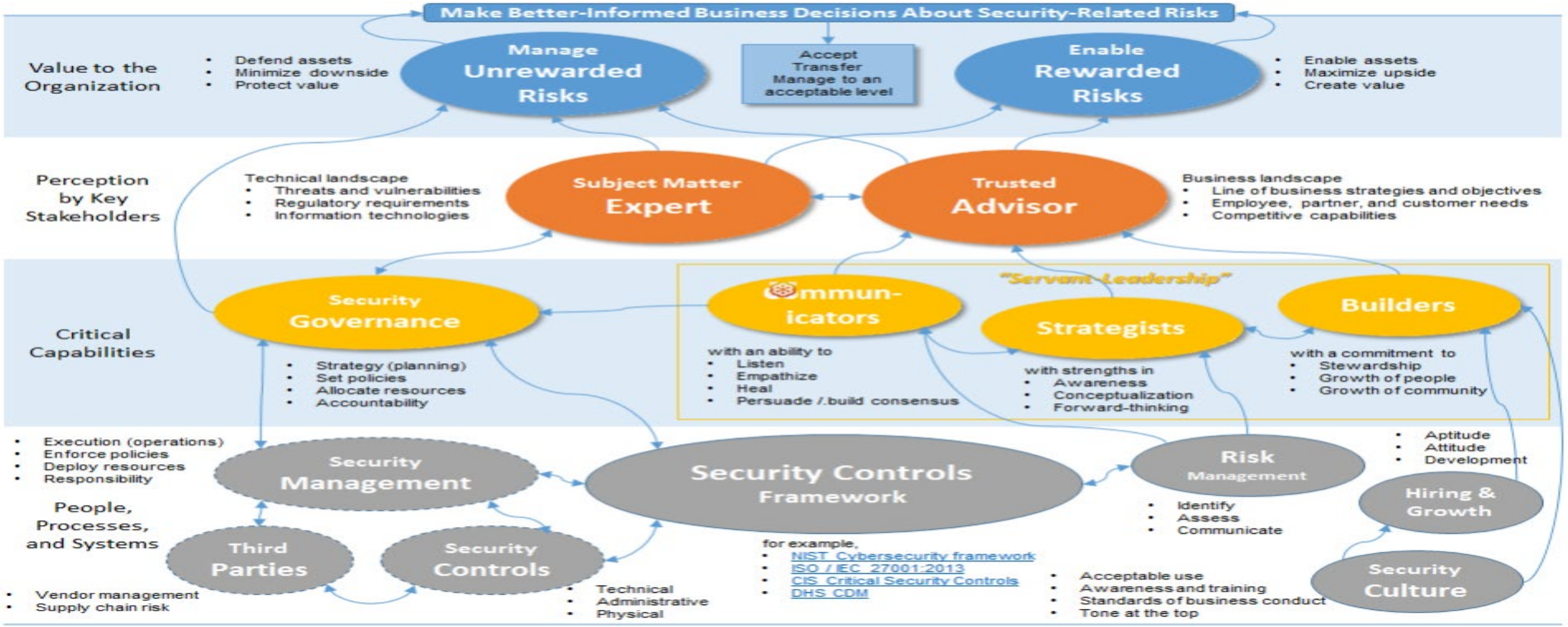
- Available Security Expertise
- Asset Inventory
- Intrusion Detection

THREATS

- Ransomware
- Hacktivists
- Upcoming Merger
- Potential Security Program Budget Cuts

CISO SPOTLIGHT, LLC
Trusted Cybersecurity and Privacy Training

Alternative Approach: Balanced Scorecard



Source: Figure 3.11 *CISO COMPASS: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers*, Cybersecurity Balanced Scorecard (Reprinted with Permission From Brink,D.,A Strategy Map forSecurityLeaders,2018.)

Cybersecurity Strategy 6-Step Approach

STEP ONE
Determine Why You Were Hired

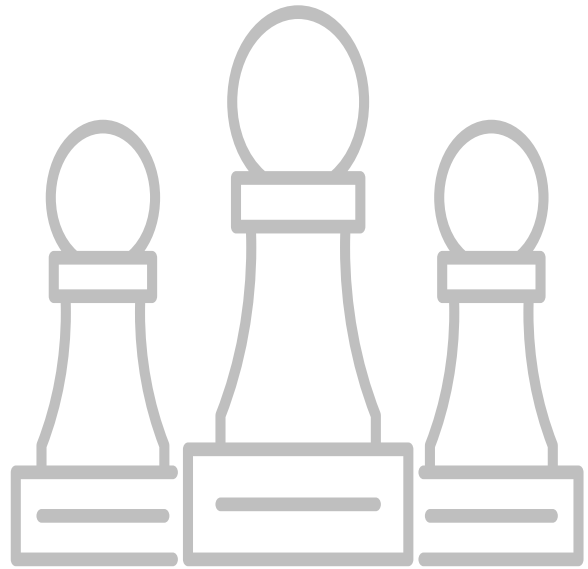
STEP TWO
Create Security Vision Statement

STEP THREE
Examine Internal and External Constraints

STEP FOUR
Identify Crown Jewels

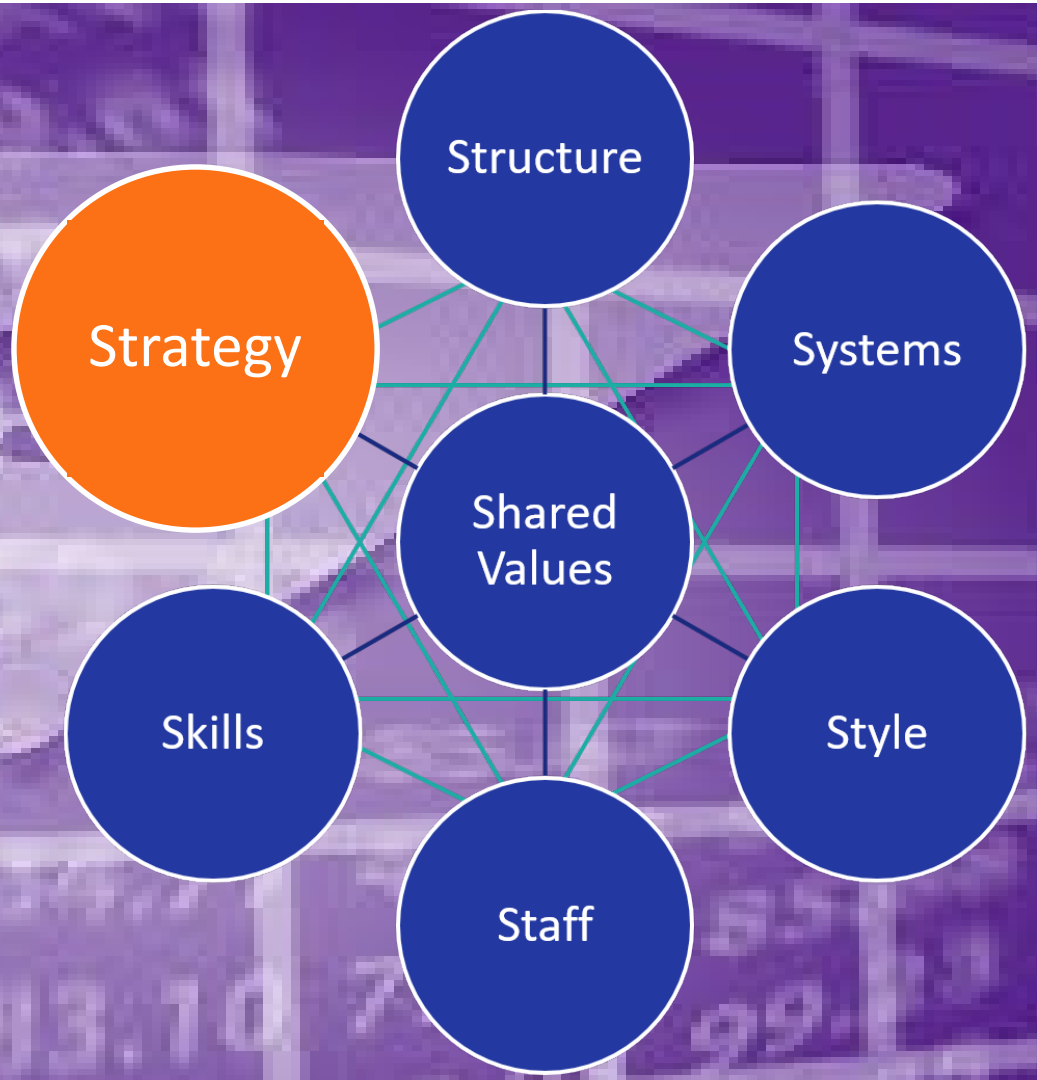
STEP FIVE
Create Protection Mind Map

STEP SIX
Create 12 month, 24 month, 3-5 year plans

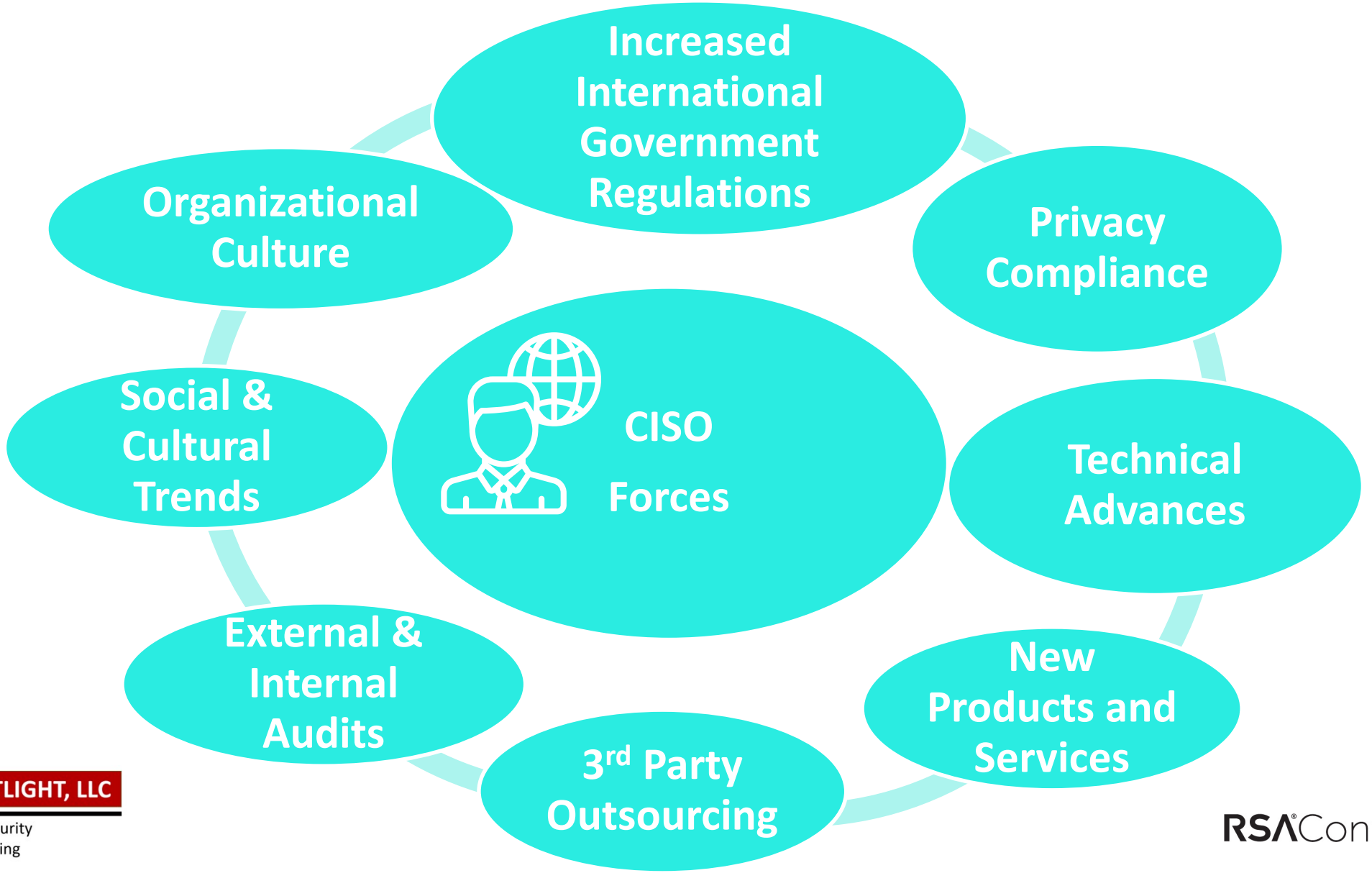


EXAMINE EMERGING TRENDS AND TECHNOLOGIES

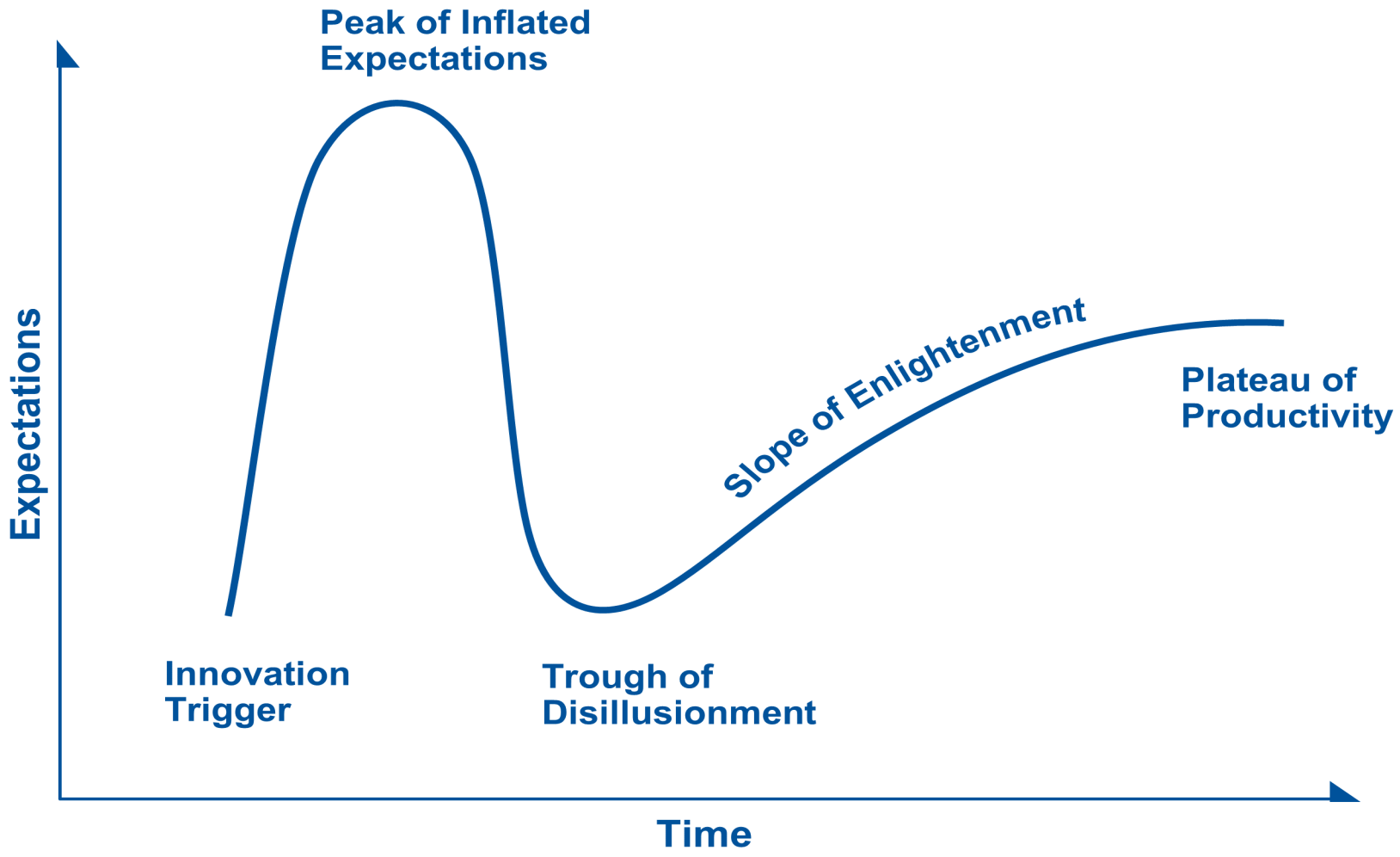
- ❑ Blockchain/Cryptocurrencies
- ❑ Internet of Things
- ❑ Drones
- ❑ Ransomware
- ❑ AI/Machine Learning
- ❑ Digital Transformation
- ❑ MFA and Privilege Restriction
- ❑ Automation/Orchestration
- ❑ Threat Intelligence Sharing
- ❑ DevSecOps
- ❑ Increased Cloud Migration

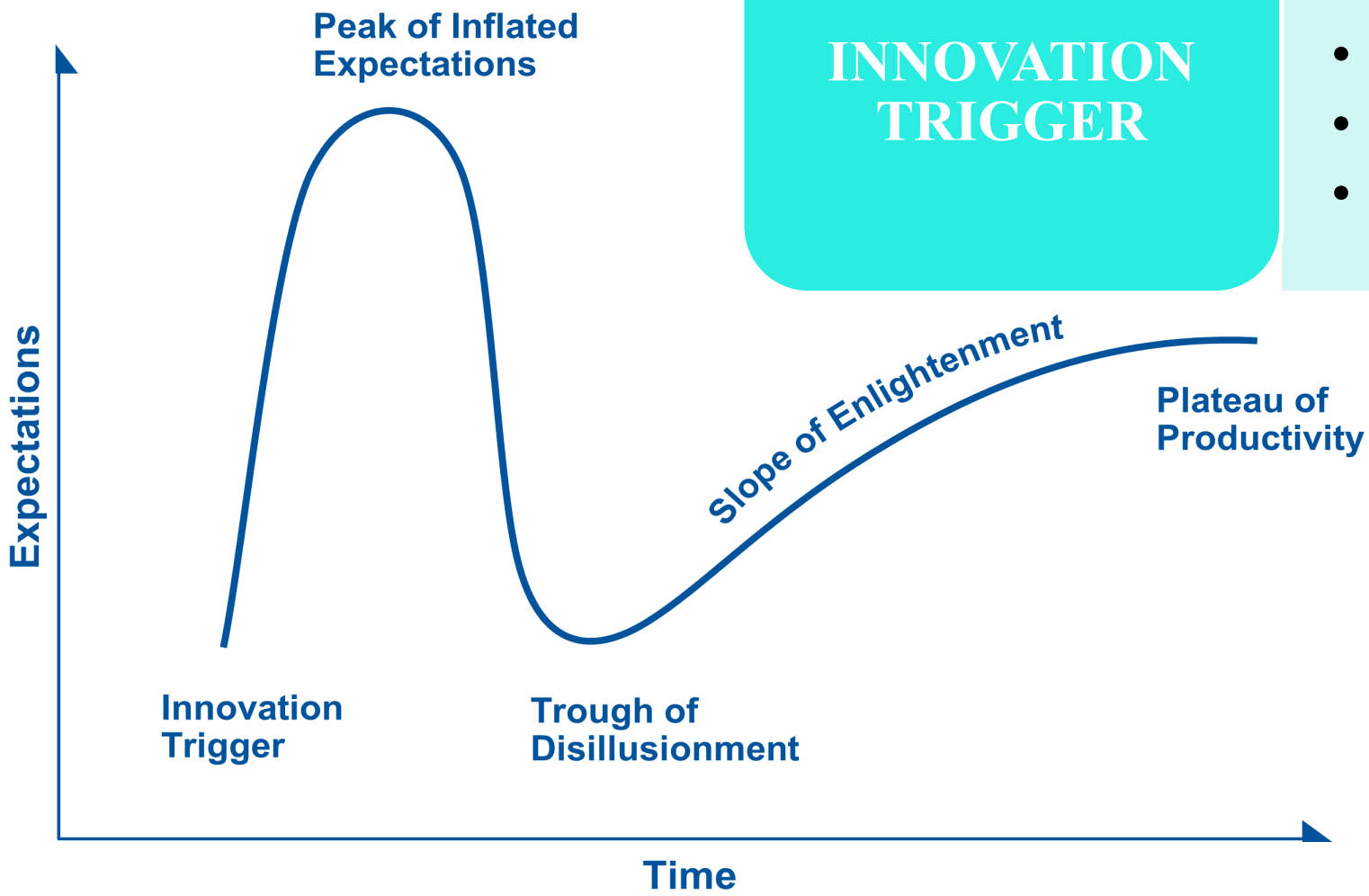


Multiple Forces Impact CISO Role and Strategy



Examine Emerging Technology Trends





INNOVATION TRIGGER

- Firewall as a Service
- Hardware-Based Security
- File Analysis
- Breach and Attack Simulation

Figure 4.2 *CISO COMPASS: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers (Auerbach, 2019)*, threat-facing technologies by hype cycle phase. (From Young, G., Hype Cycle for Threat-Facing Technologies, 2 0 17, G a r t n e r.)

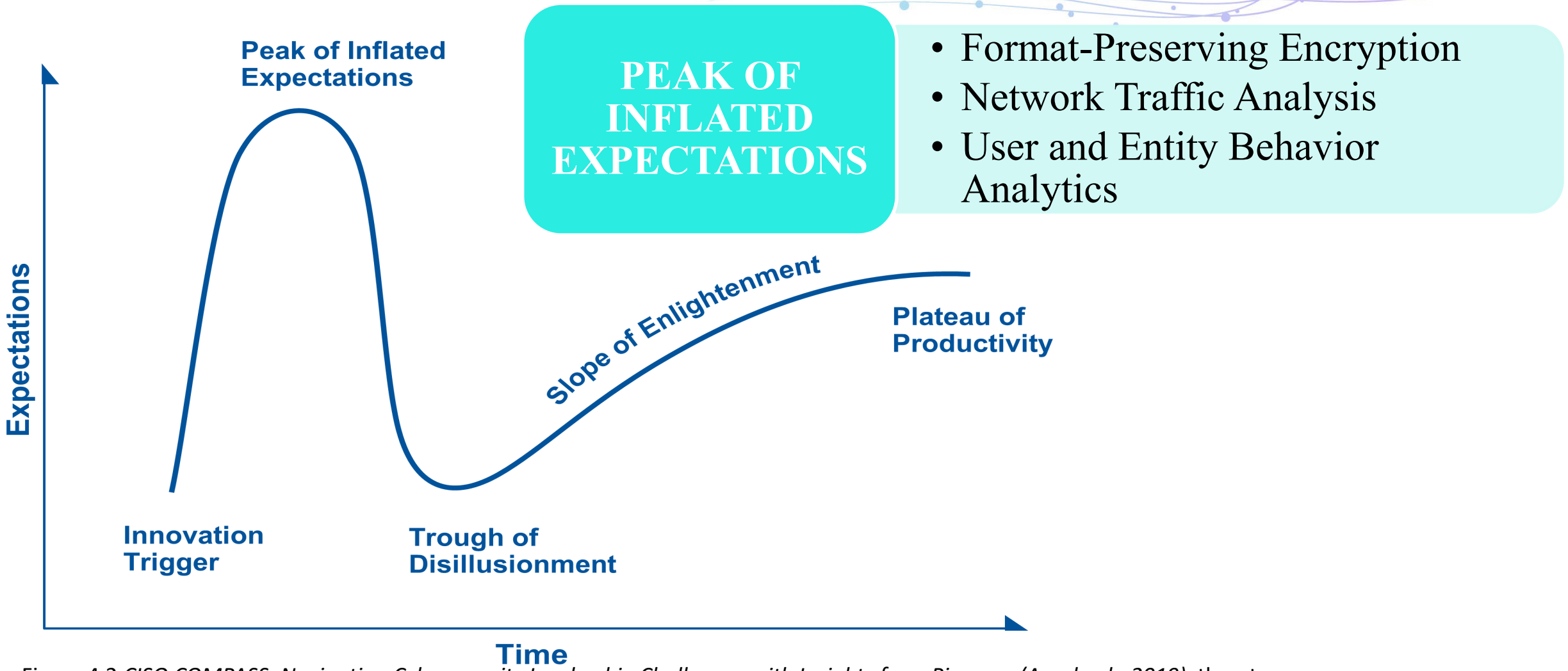
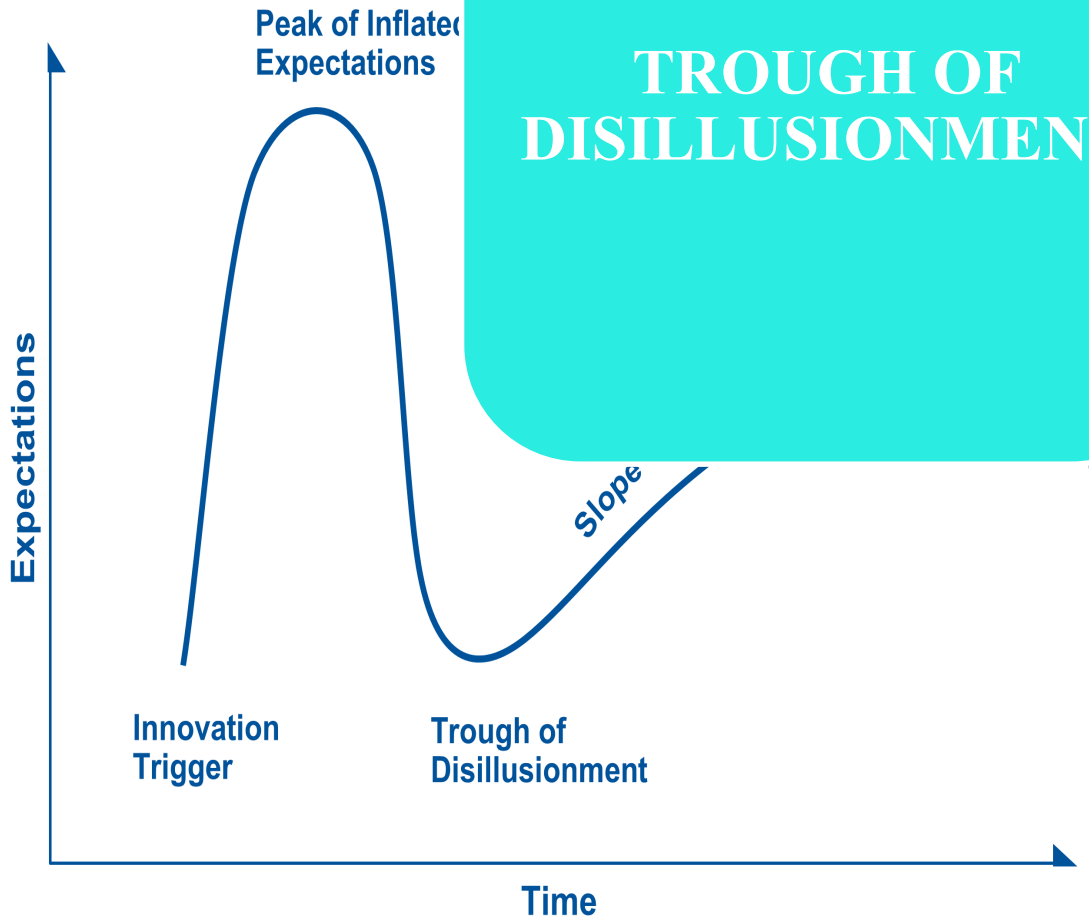


Figure 4.2 *CISO COMPASS: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers (Auerbach, 2019)*, threat-facing technologies by hype cycle phase. (From Young, G., Hype Cycle for Threat-Facing Technologies, 2 0 17, G a r t n e r.)

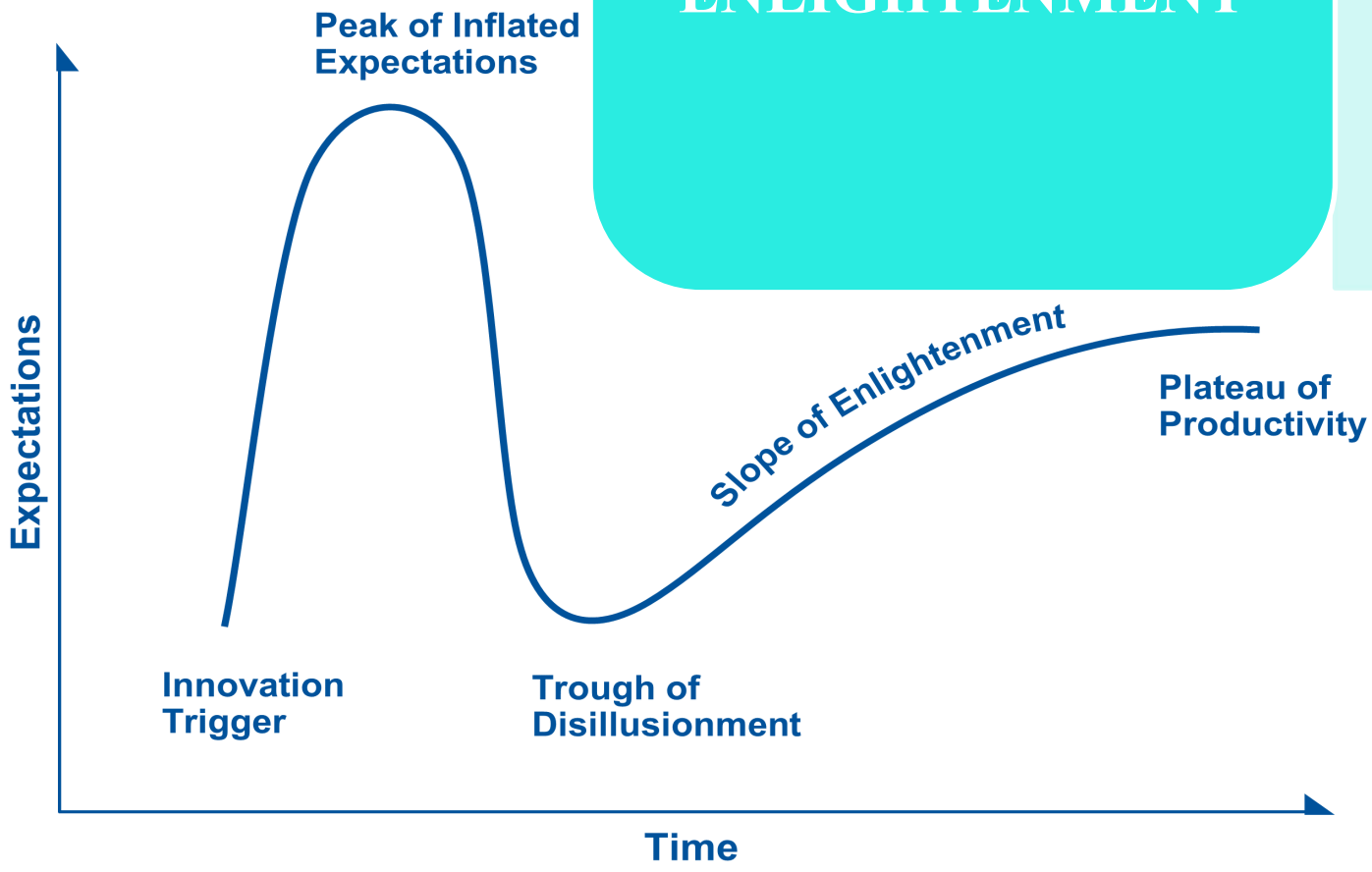


TROUGH OF DISILLUSIONMENT

- Threat Intelligence Platforms
- Security in the Switch
- Network Security Policy Management
- TLS Decryption Platform
- Enterprise Key Management
- Operational Technology Security
- Micro segmentation (Software- Defined)
- Secure Web Gateways

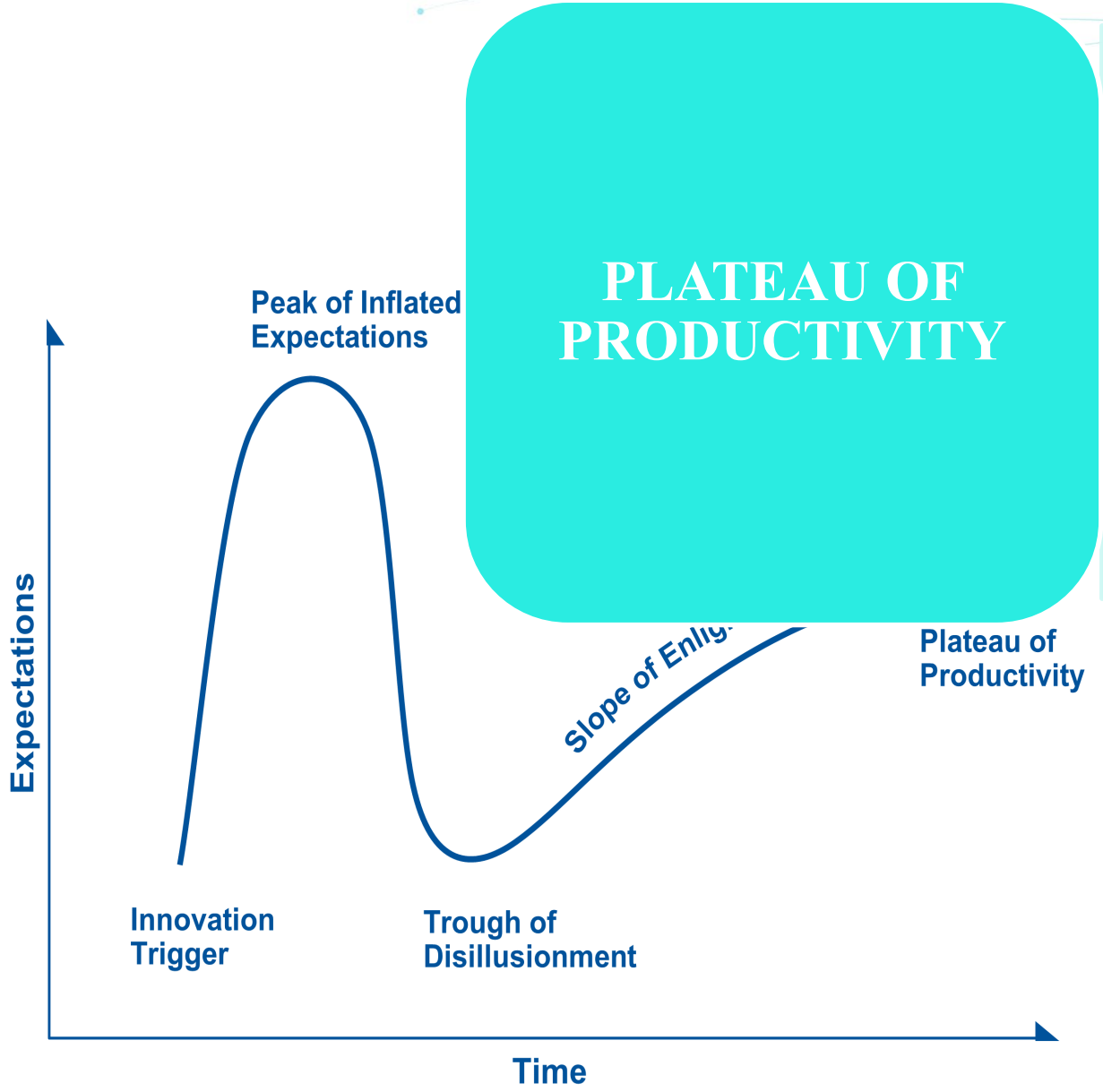
Figure 4.2 *CISO COMPASS: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers (Auerbach, 2019)*, threat-facing technologies by hype cycle phase. (From Young, G., Hype Cycle for Threat-Facing Technologies, 2 0 17, G a r t n e r.)

SLOPE OF ENLIGHTENMENT



- Network Sandboxing
- Network Access Control
- DDoS Defense
- Database Audit and Protection
- Web Application Firewalls
- NextGen Interoperable Storage Encryption
- NextGen IPS
- Database Encryption

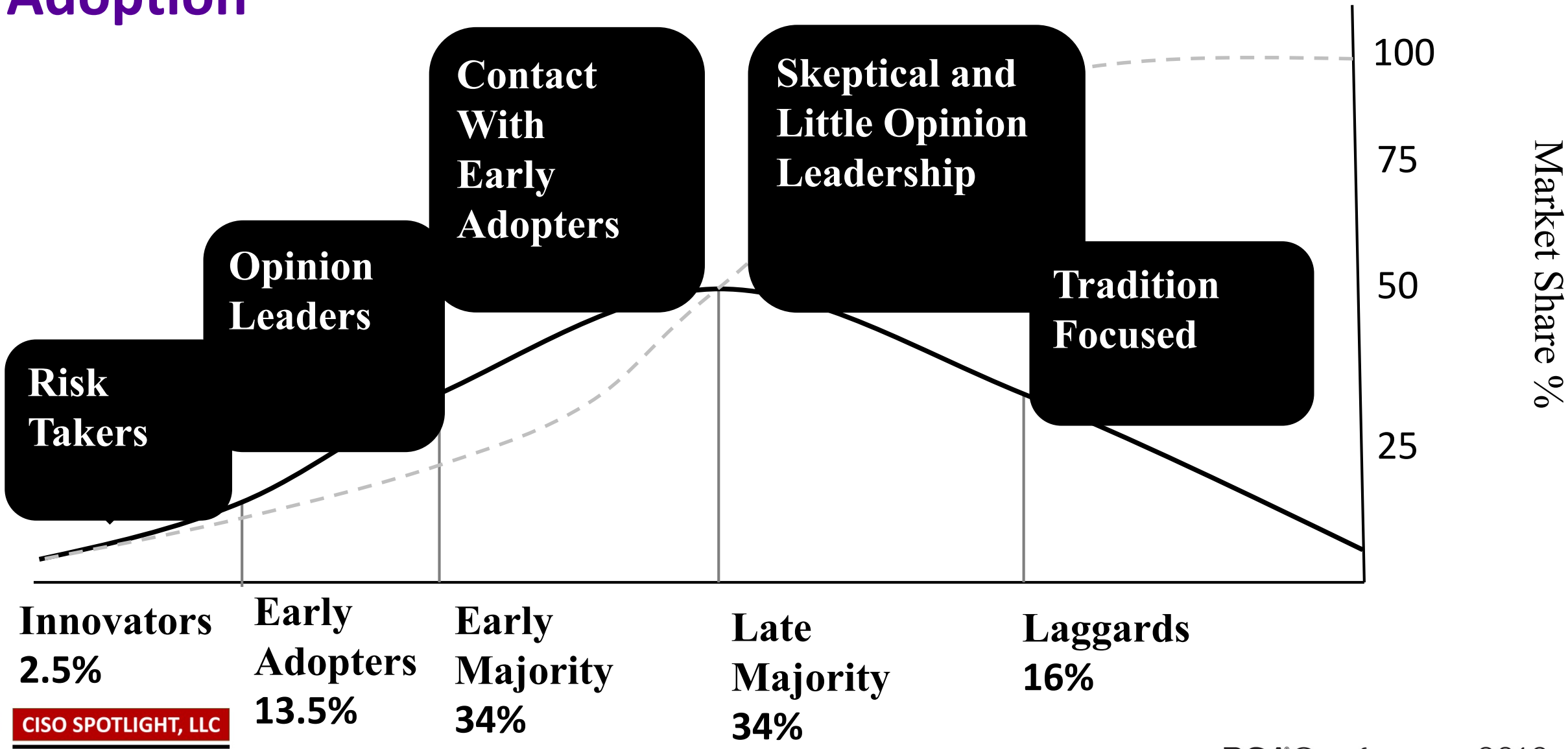
Figure 4.2 *CISO COMPASS: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers (Auerbach, 2019)*, threat-facing technologies by hype cycle phase. (From Young, G., Hype Cycle for Threat-Facing Technologies, 2 0 17, G a r t n e r.)



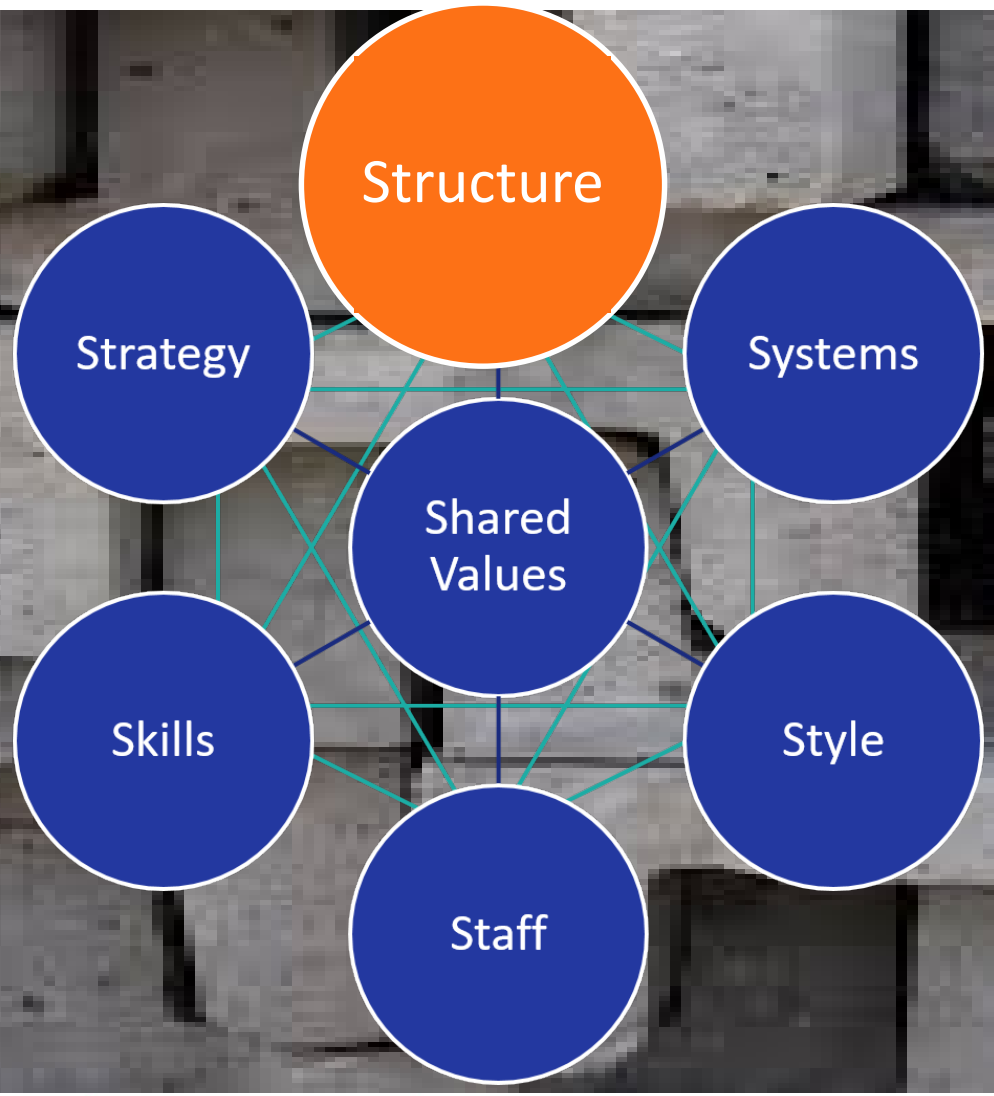
- High-Assurance Supervisors
- Network Penetration Testing Tools
- Enterprise (NextGen) Firewalls
- SIEM
- Application Control
- Vulnerability Assessment
- Mobile Data Protection for Workstations
- Network IPS
- Unified Threat Management

Figure 4.2 *CISO COMPASS: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers (Auerbach, 2019)*, threat-facing technologies by hype cycle phase. (From Young, G., Hype Cycle for Threat-Facing Technologies, 2 0 17, G a r t n e r.)

Firms Have Different Approaches To Technology Adoption

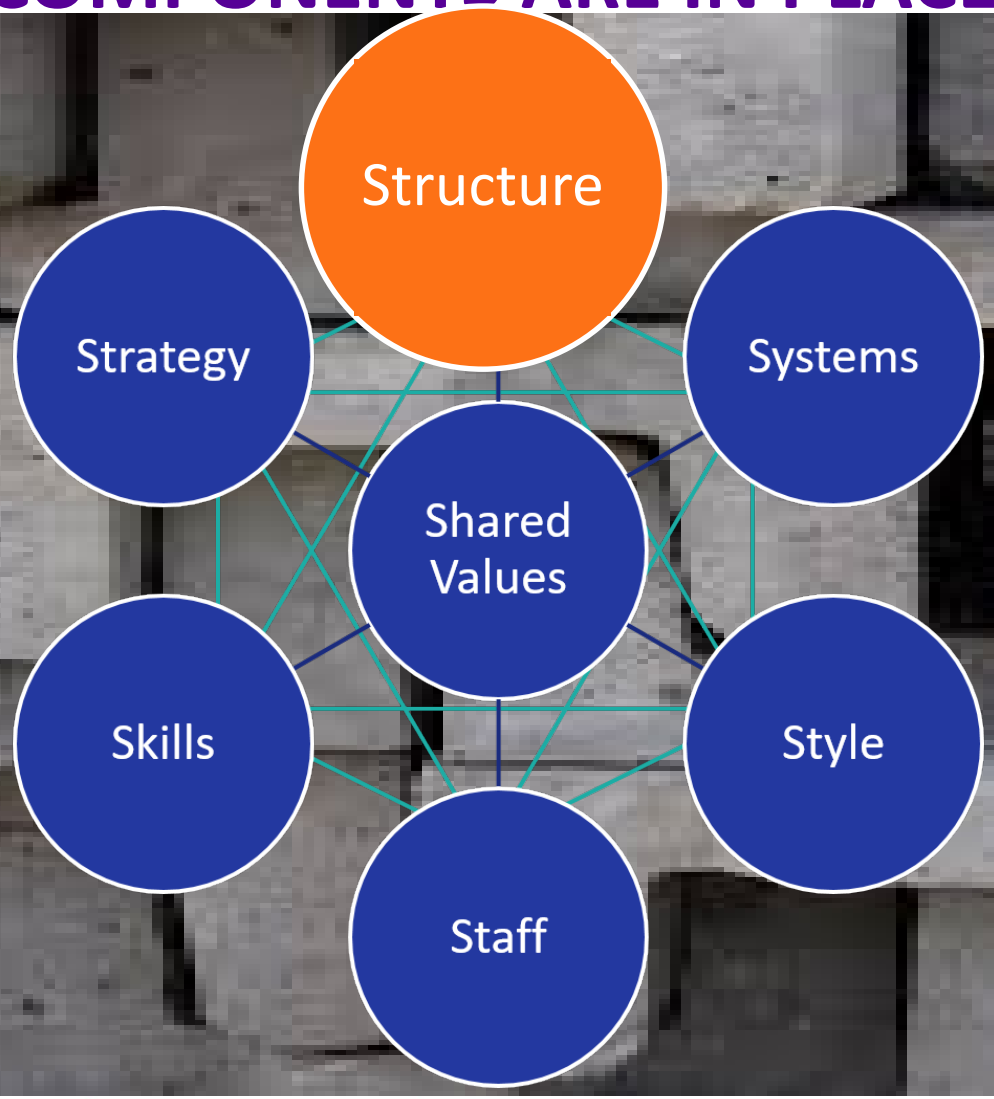


CYBERSECURITY STRUCTURE



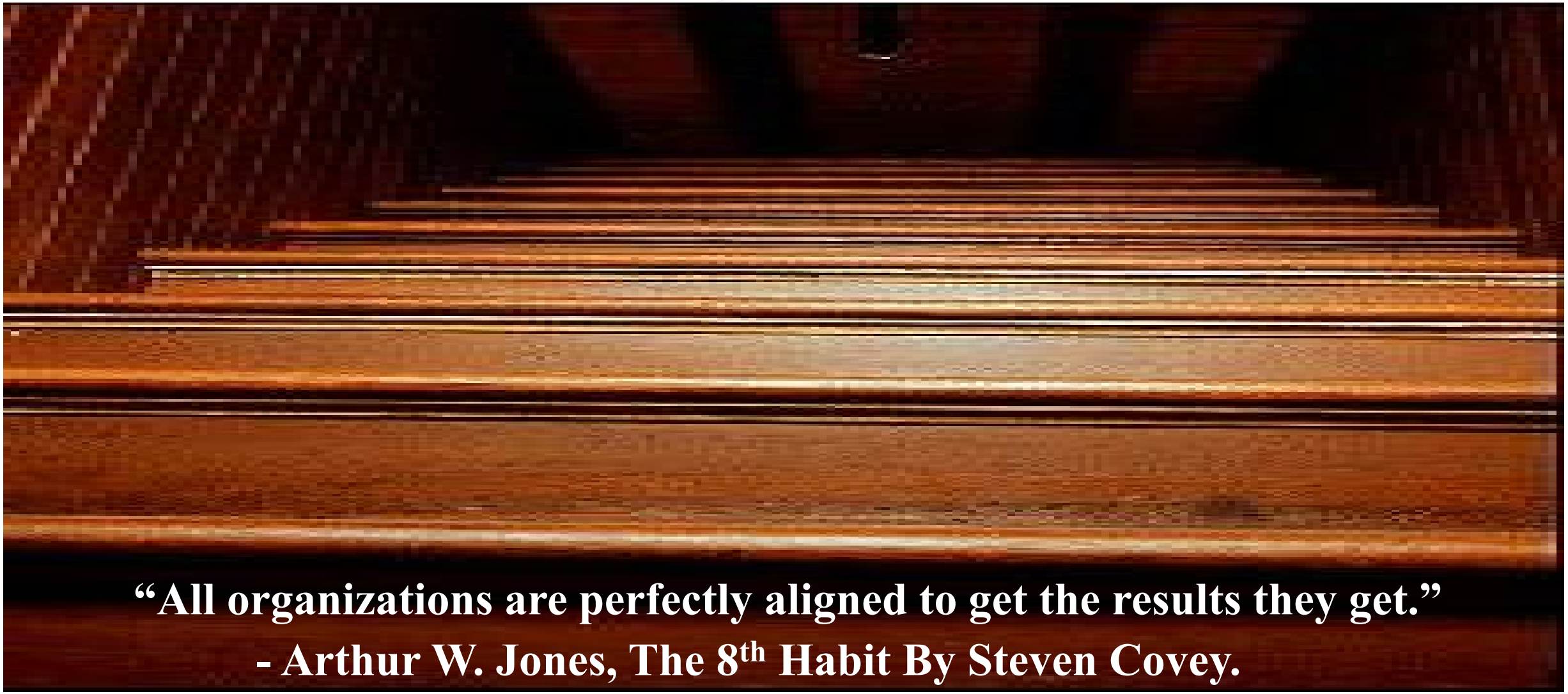
HOW DO WE BEST ORGANIZE THE CYBERSECURITY ORGANIZATON TO ADAPT TO THE NEEDS OF THE ORGANIZATION?

CYBERSECURITY ORGANIZATION STRUCTURE ENSURES RIGHT COMPONENTS ARE IN PLACE

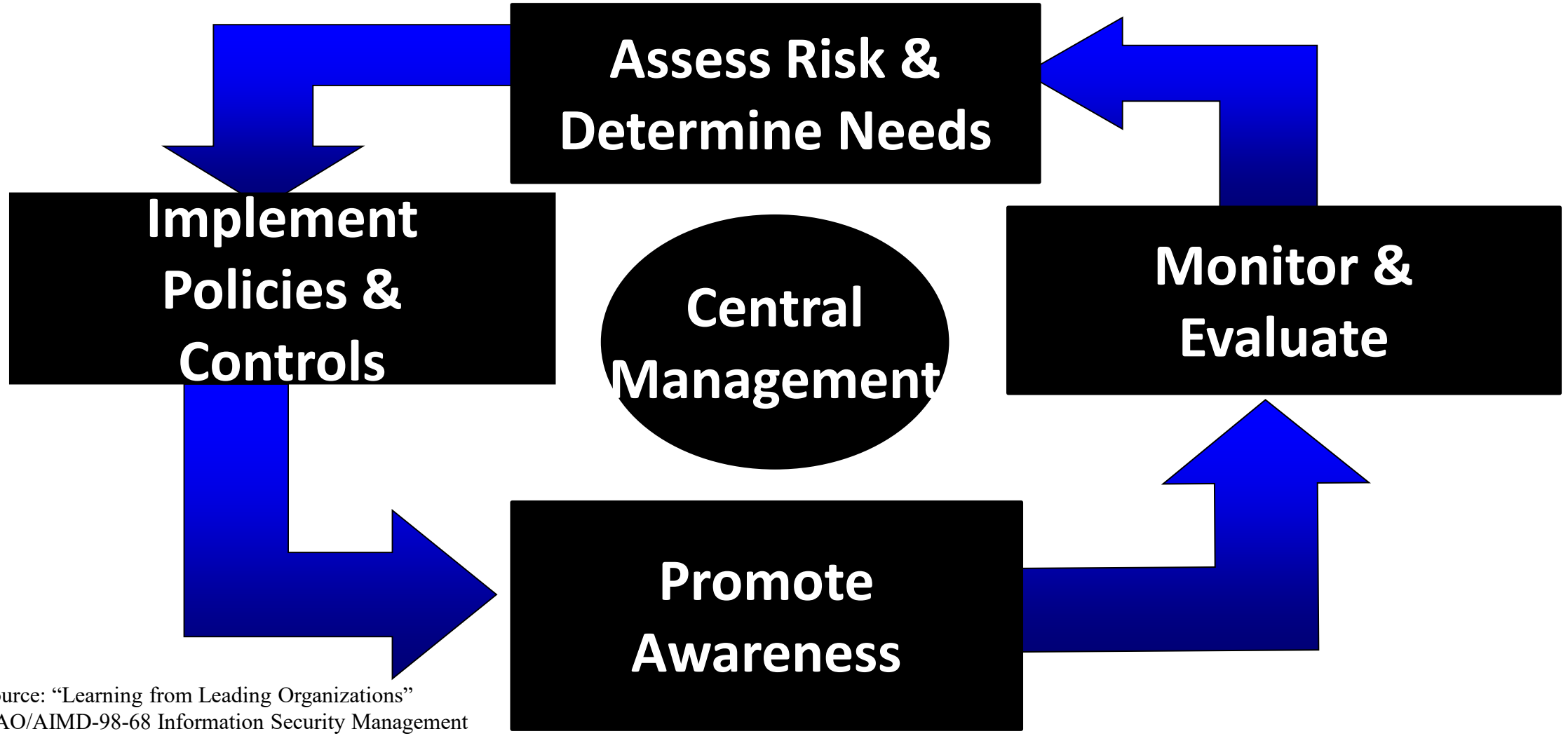


- ❑ What is the organizational hierarchy?
- ❑ Is decision-making centralized?
- ❑ What are the lines of communication?
- ❑ What are the informal/formal reporting relationships?

JUST LIKE THE WINCHESTER HOUSE…

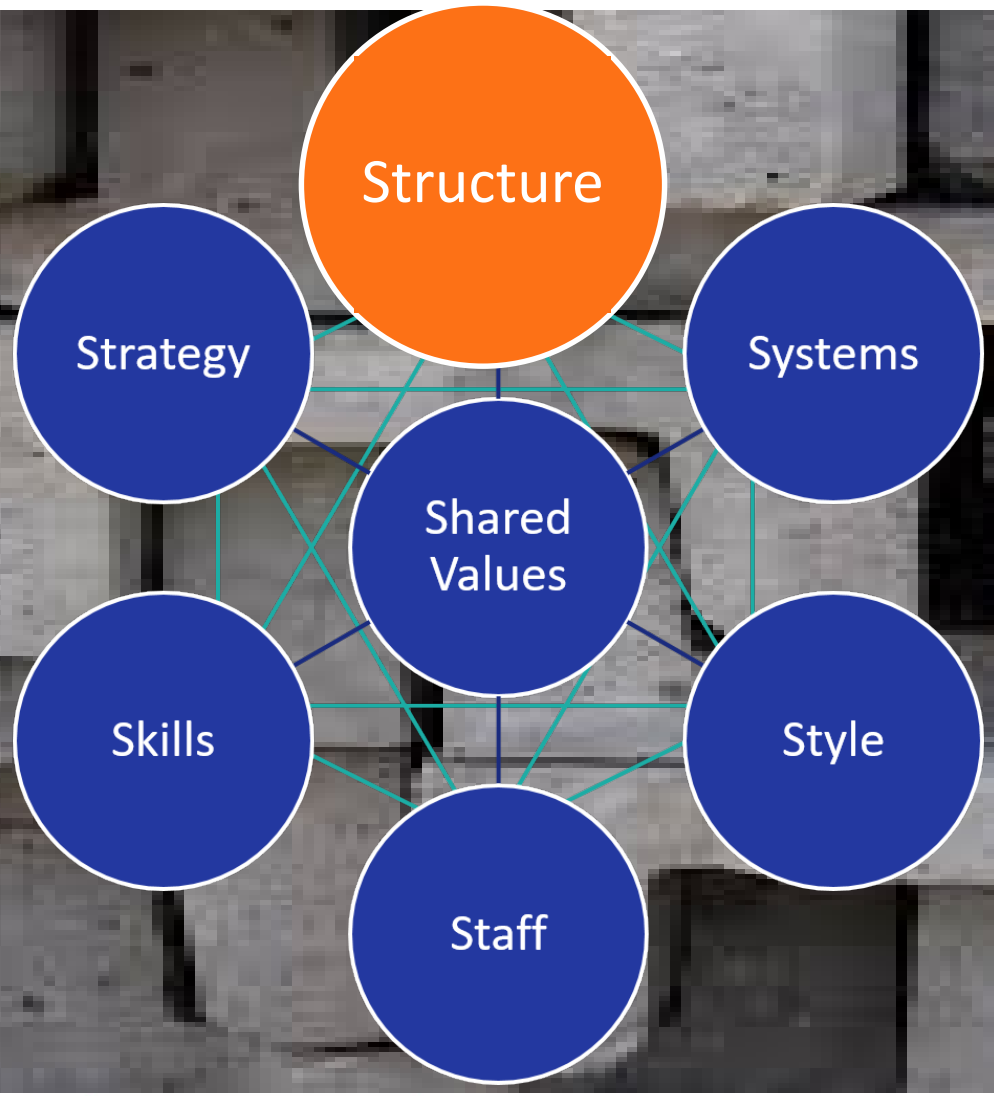


Successful Security Management Practices



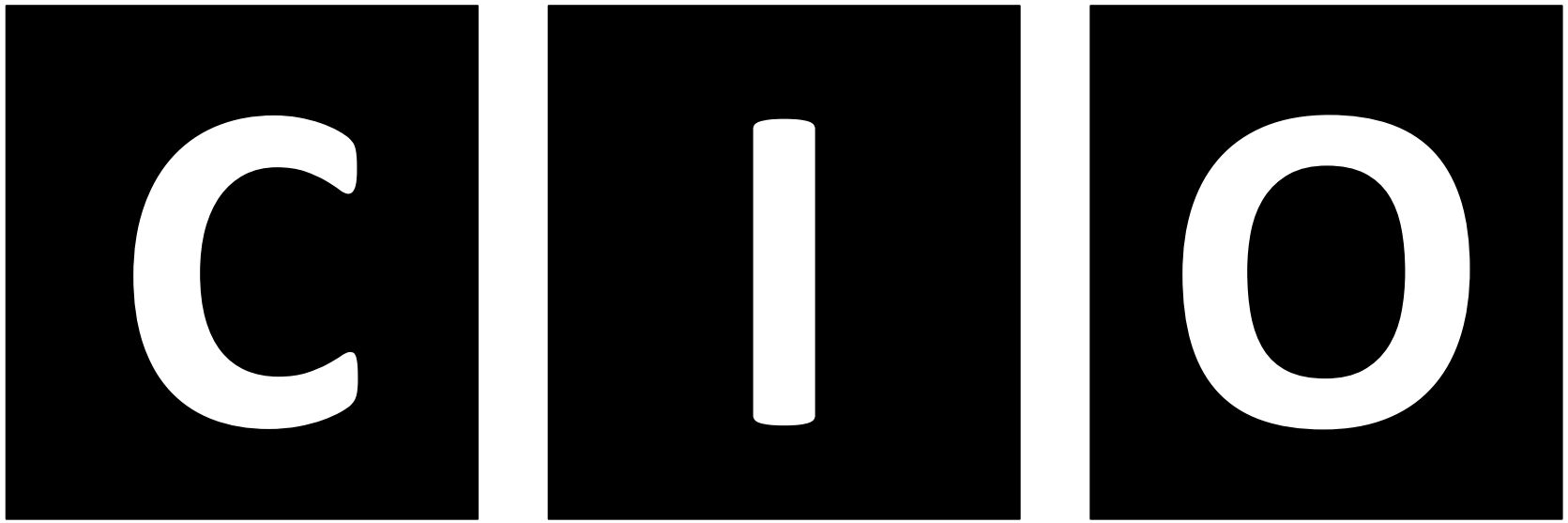
Source: "Learning from Leading Organizations"
GAO/AIMD-98-68 Information Security Management

REPORTING MODELS VARY BY ORGANIZATION AND INFLUENCE FORMAL AND INFORMAL DECISION-MAKING



- How is the team divided?
- What is the organizational hierarchy?
- Is decision-making centralized?
- What are the lines of communication?
- What are the informal/formal reporting relationships?

And While Changing, Most CISOs Still Report To…



56% of The Time

Source: CISO's Today: The good. bad and the ugly, CISO Summit, Larry Ponemon Dec 2013

OTHER OPTIONS FOR CISO TO REPORT

GENERAL COUNSEL

- Compliance focused
- Legal Expertise Access
- Lack of technical understanding
- Underestimation of costs

CEO

- Lack of time for security
- Raises visibility of security
- May provide aid short-term
- Too many details for CEO

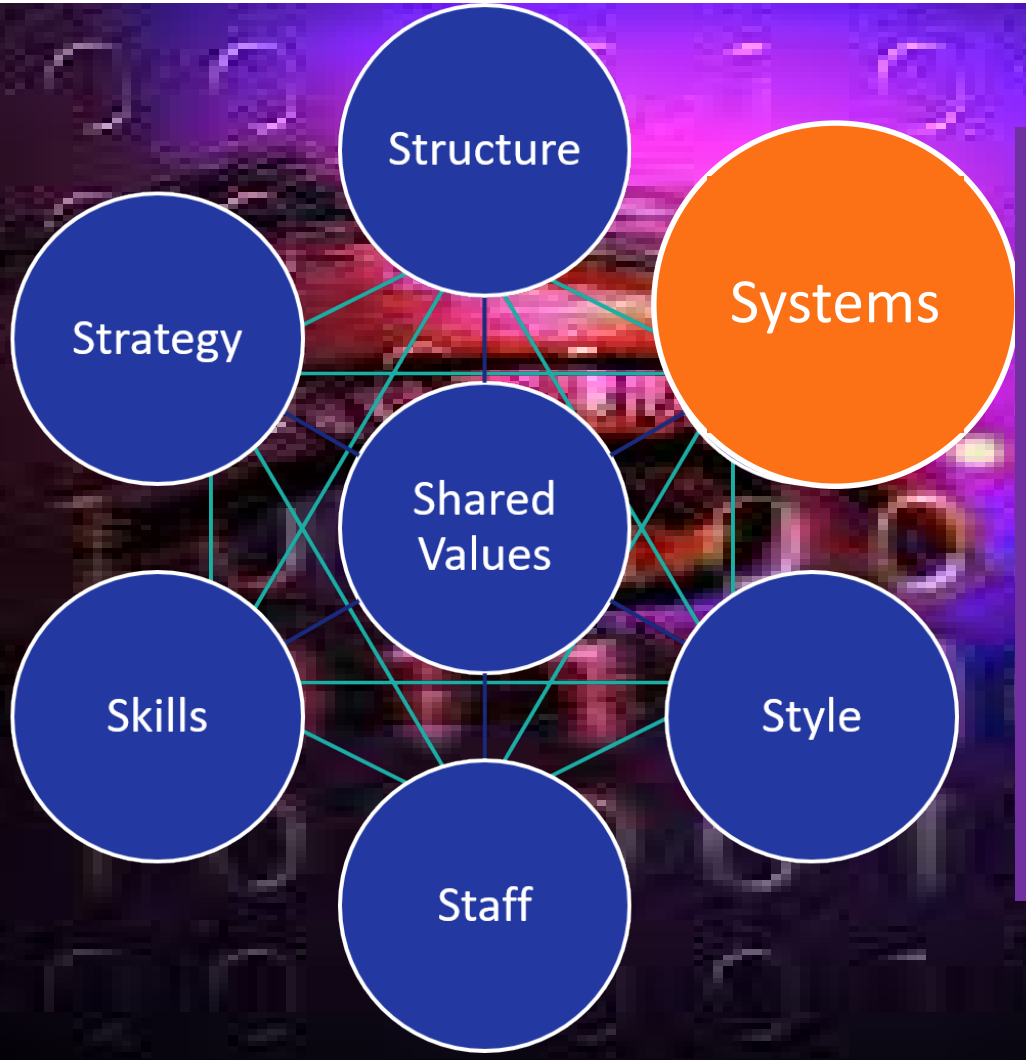
RISK OFFICER

- Risk advocate
- Security may not get attention
- Clout with senior management
- Lack of business metrics

PHYSICAL SECURITY

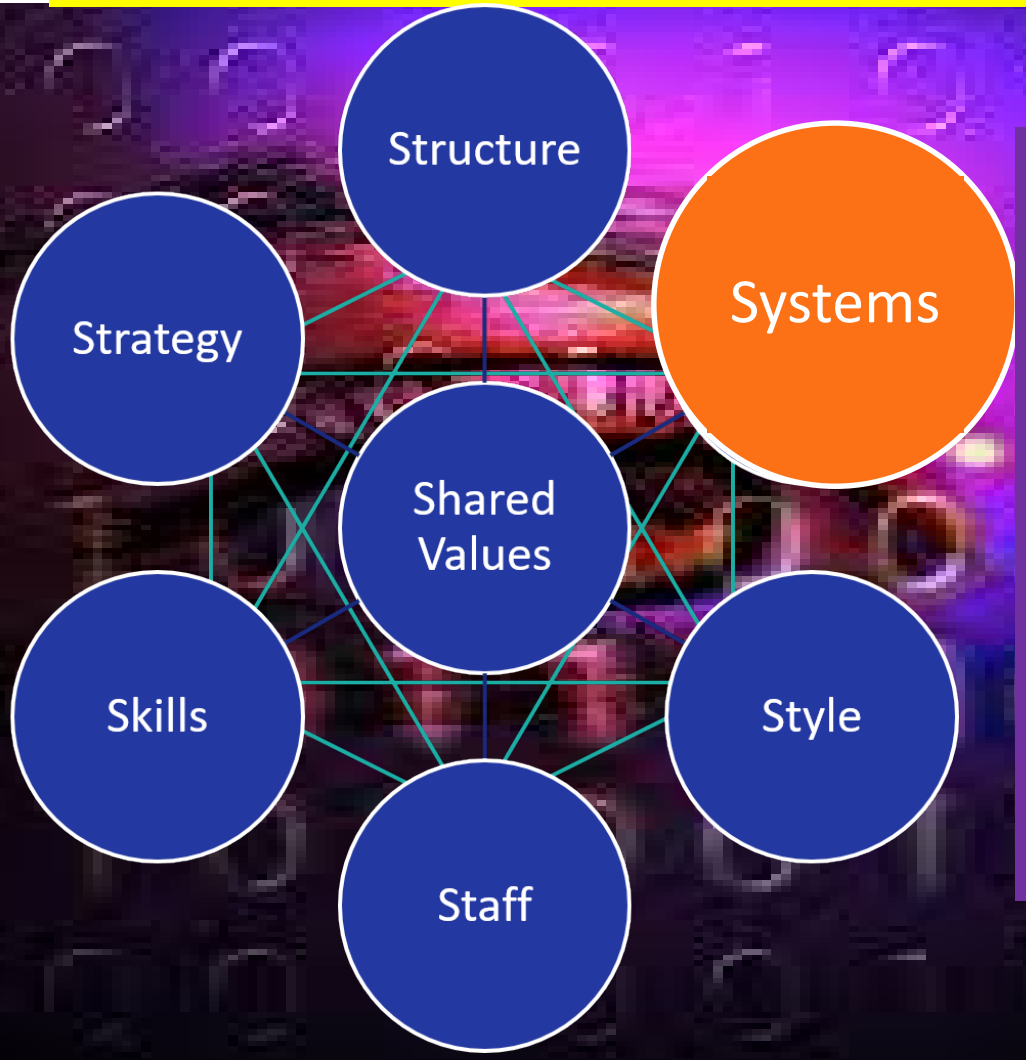
- Guns Guards vs IT culture Increased incident comms
- "Police Mentality"
- Law enforcement connections

SYSTEMS FOR THE CISO/SECURITY



WHAT PROCESSES AND ROUTINES DOES THE CISO LEVERAGE TO LEAD AND REDUCE THE CYBERSECURITY RISK TO THE ORGANIZATION?

LEVERAGING INCIDENTS



Recent High-Profile Breaches

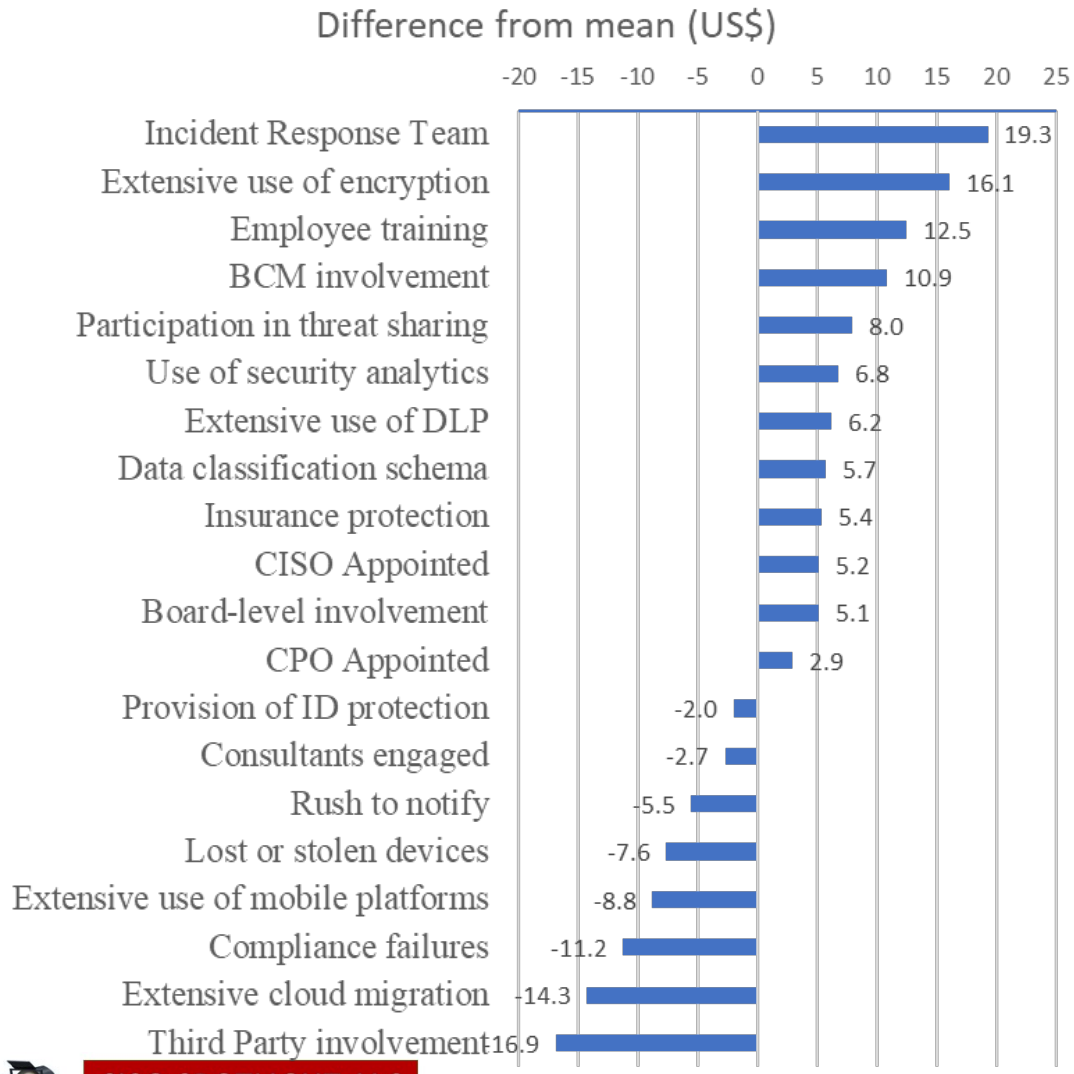
- ❑ Under Armour (2018)
- ❑ Facebook/Cambridge Analytica (2018)
- ❑ Equifax (2017)
- ❑ Spambot (2017)
- ❑ WannaCry, NotPetya (2017)
- ❑ Apple Vs FBI (2016)
- ❑ Anthem (2015)
- ❑ Target (2013)
- ❑ Yahoo (2013-16)

CISO MUST REVIEW ATTACK PATTERNS OF HOW TO MINIMIZE RISK

ATTACK PATTERN	• HOW TO REDUCE RISK
Crimeware	• Software updates, macro-enabled document risk
Cyber-Espionage	• Security Awareness training, phishing exercises
Denial of Service	• Test DDOS mitigation services
Insider and Privilege Misuse	• Limit, log, monitor use, large data transfer and usb awareness
Miscellaneous Errors	• Disposal processes, 4-eye policy for publishing information
Payment Card Skimmers	• Train employees, monitor terminals with video, review tapes regularly
Physical Theft & Loss	• Encrypt where possible, corporate policy limiting printing sensitive data
Web Application Attacks	• Promote varying Passwords, 2FA, limit data in web-facing applications
Point of Sale Intrusions	• Review 3rd party POS vendors and remote access

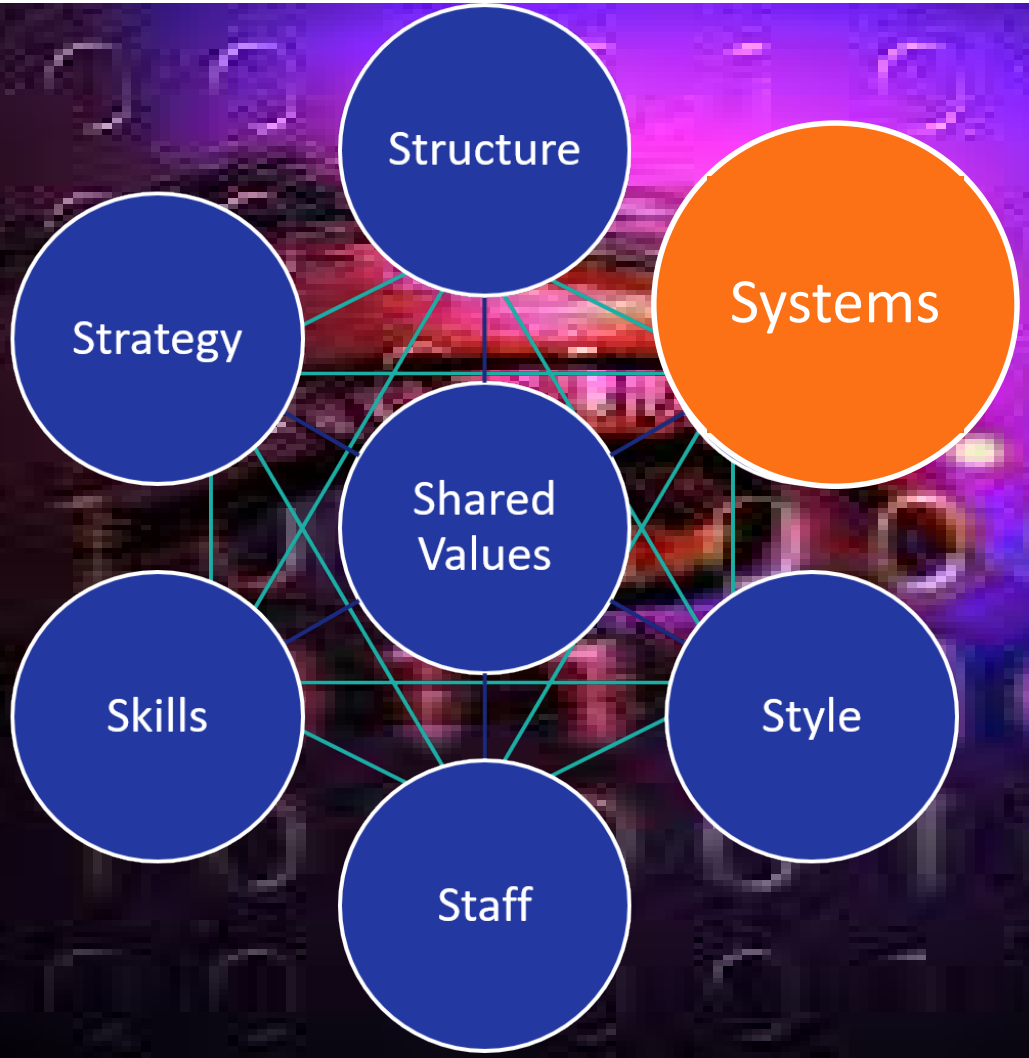
Source: (Adapted from *2017 Data Breach Investigations Report, 10th Edition*. 2017, Verizon).

Reducing Data Breach Costs



- Costs may be decreased or increased from $141 per capita cost per customer record
- Evaluate in terms of fixing the *process vs the incident*

NAVIGATING THE SECURITY CONTROL FRAMEWORK MAZE PROVIDES FOCUS



WHAT PROCESSES AND ROUTINES DOES THE CISO LEVERAGE TO LEAD AND REDUCE THE CYBERSECURITY RISK TO THE ORGANIZATION?

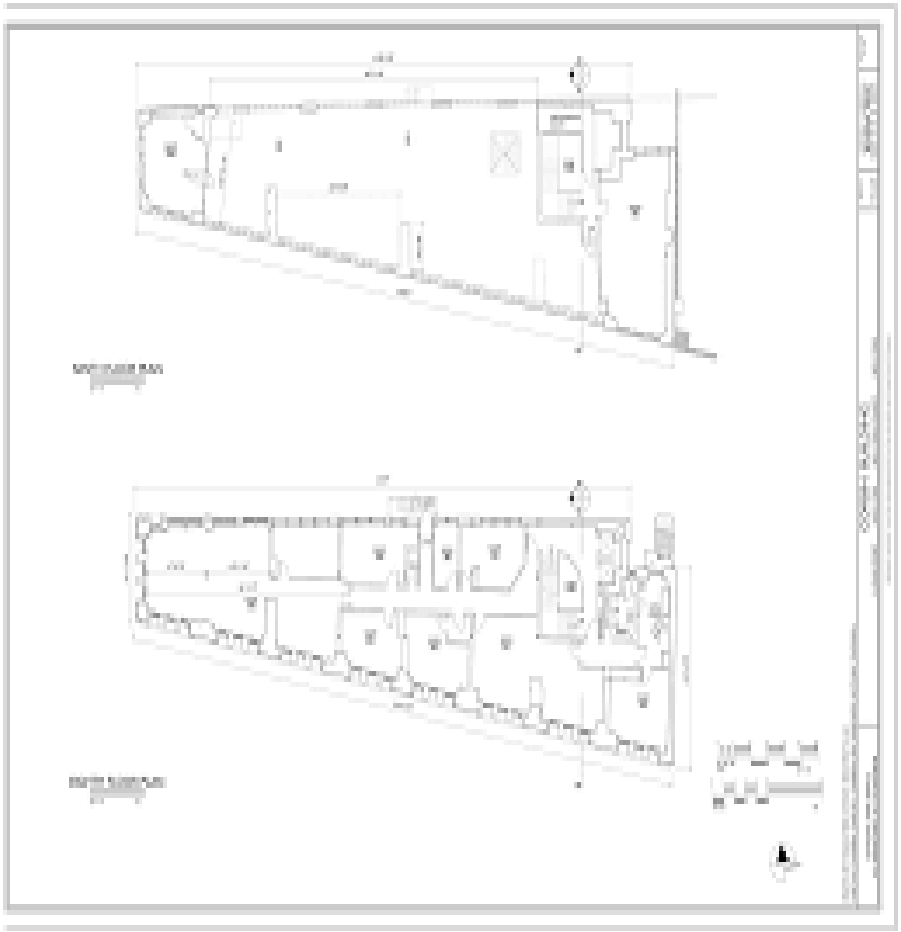
Executive Level Communication

- NIST Cybersecurity Framework
- Control Objectives for Information and related Technology (COBIT)

Overall Cybersecurity Frameworks

- ISO/IEC 27001:2013 Information Security Management System (ISMS)
- Health Insurance Portability and Accountability Act (HIPAA)
- CMMI Capability Maturity Model
- Cloud Security Alliance Cloud Controls Matrix
- ITIL (IT Security Management)
- Payment Card Industry Data Security Standard (PCI DSS)
- Information Security Forum (ISF) Standard of Good Practice
- NERC Critical Infrastructure Protection

DETAILED CONTROLS



Detail-Oriented Controls

- OWASP Top 10 Most Critical Web Application Security Risks
- HITRUST Common Security Framework
- Federal Financial Institutions Examination Council (FFEIC) IT Examination Handbook
- NIST 800-53 Controls
- Security Technical Implementation Guides (STIGS) and National Security Agency (NSA) Guides
- Center for Internet Security (CIS) Controls
- Federal Information Systems Controls Audit Manual (FISCAM)
- Vendor Implementation Guides

STRATEGY/SYSTEMS: Create 12mo, 24mo, 3-5 Year Plan

Function	Category	M	12 Mo	M	24 Mo	M	3-5 Year	M
Identify	Asset Management Business Environment Governance Risk Assessment Risk Management Strategy Supply Chain Risk Management							
Protect	Identity Management and Access Control Awareness & Training Data Security Information Protection Pr Protective Technology, M							
Detect	Anomalies and Events Security Continuous Moni Detection Processes							
Respond	Response Planning Communications Analysis Mitigation Improvements							
Recover	Recovery Planning Improvements Communications							

Actions to advance maturity

Actions to advance maturity

Actions to advance maturity

Could Use Colors (H,M,L) or

0=Nonexistent No Evident of practice or standard

1= Initial Ad-hoc or inconsistent

2=Repeatable consistent overall approach, but mostly undocumented

3=Defined documented approach, lacks enforcement or measurement

4=Managed regularly measures compliance and makes process improvements

5=Optimized refined compliance to best practice

Note: M=Maturity Level Using the NIST Cybersecurity Framework

Some of Us Take More Risks Than Others

CISO SPOTLIGHT, LLC
Trusted Cybersecurity
and Privacy Training

What Does Risk Look Like?

- Risk tolerance is different for different individuals
- Risk IS:
  - Issuing policies without management review
  - Accepting current state risk unknowingly
  - Failure to understand business impact
  - Lack of management support for implementation
  - Unfunded initiatives
  - Short term thinking
  - Inattention to security

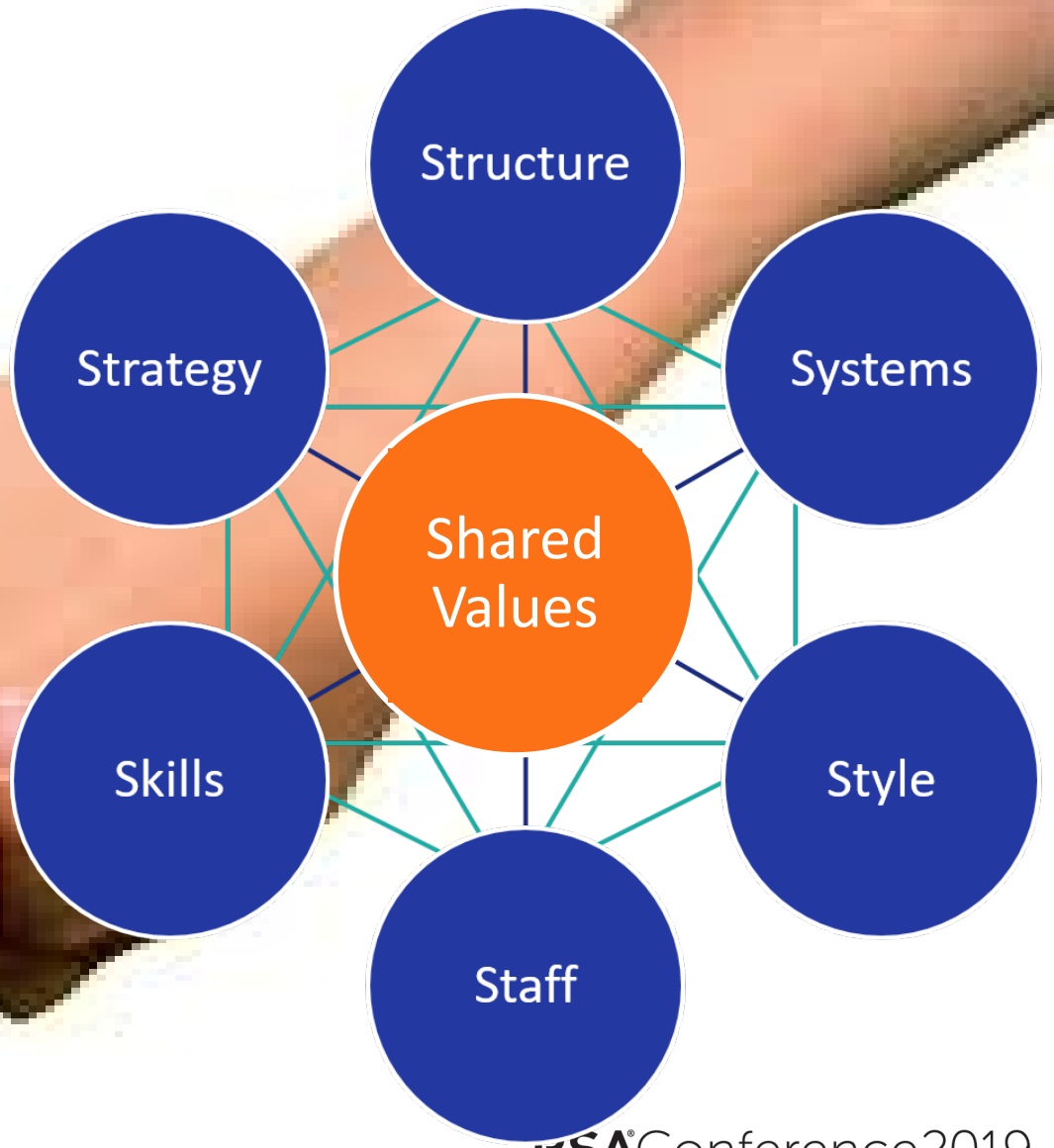
Threats to Our Systems Come From Many Sources

Environmental	Media Disposal Scavenging	Carelessness Accidental Events
Omissions	Procedural Violations	Theft Vandalism
Physical Intrusion	Unacceptable Use	Labor Unrest
Terrorism Riots	Natural Disaster	Data/System contamination
System Corruption Malicious Code	Eavesdropping System Intrusions	Misuse Software Weakness
Installation Errors Hardware Failure	Impersonation Shoulder Surfing	Use Abuse Fraud

THE CYBERSECURITY TONE IS LIVED THROUGH SHARED VALUES

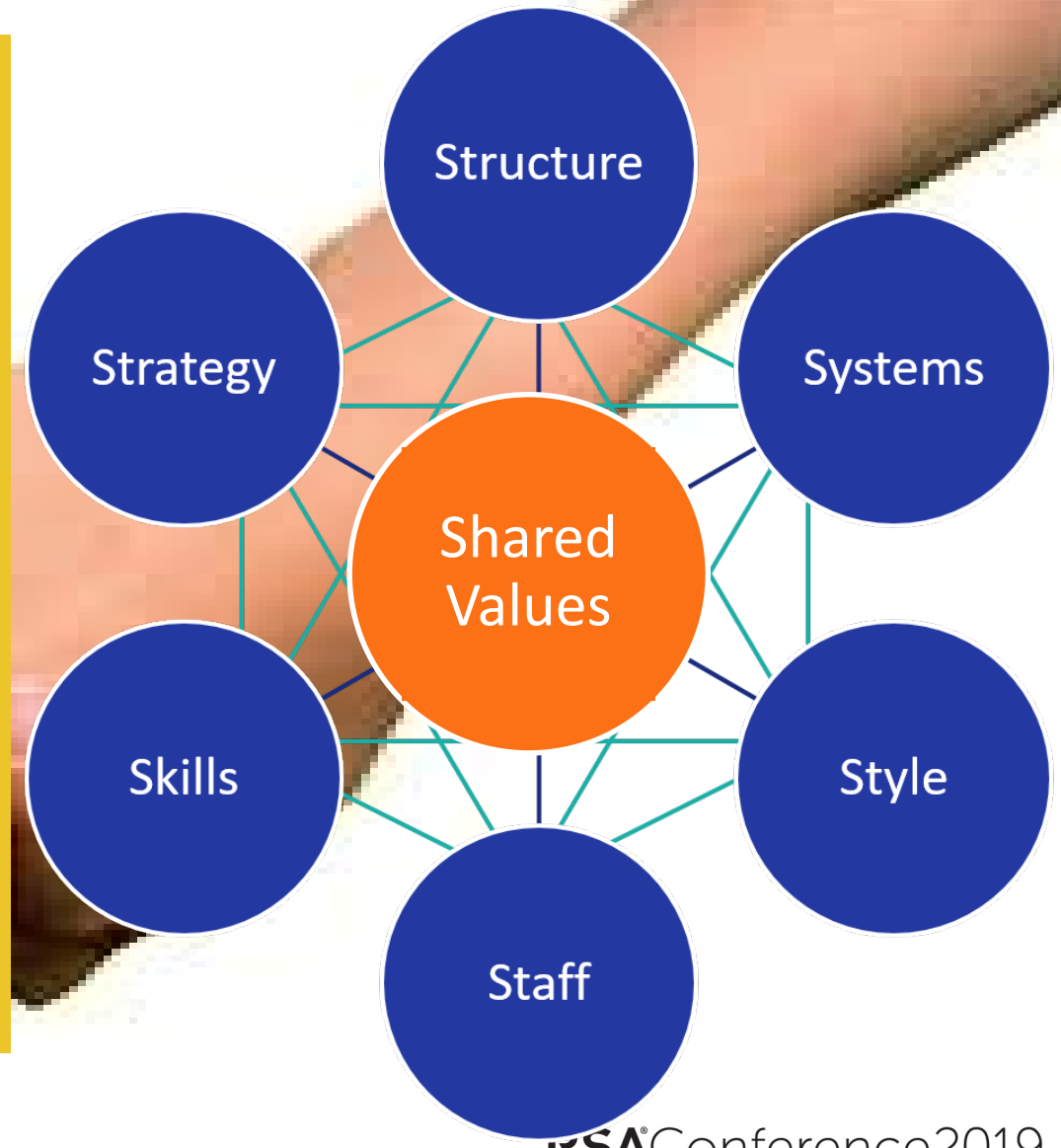
#RSAC

WHAT ARE THE CORE CYBERSECURITY VALUES SHARED ACROSS THE ORGANIZATION (LAWS & REGULATIONS, DATA PROTECTION AND PRIVACY, POLICIES AND PROCEDURES). HOW STRONG ARE THESE VALUES?



LAWS AND REGULATIONS SET THE DESIRED 'MUST' WE NEED TO ACHIEVE FOR *COMPLIANCE*

- ❑ Electronic Communications Privacy Act of 1986
- ❑ Computer Security Act of 1987
- ❑ Sarbanes-Oxley Act of 2002 (SOX)
- ❑ Gramm-Leach-Bliley Act (GLBA)
- ❑ Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- ❑ Health Information Technology for Economic and Clinical Health Act
- ❑ Federal Information Security Management Act of 2002
- ❑ Cybersecurity Information Sharing Act of 2015 (CISA)
- ❑ 2017 Executive Order 13800
- ❑ 2017 New York State Cybersecurity Requirements for Financial Services Companies
- ❑ International Cybersecurity Laws



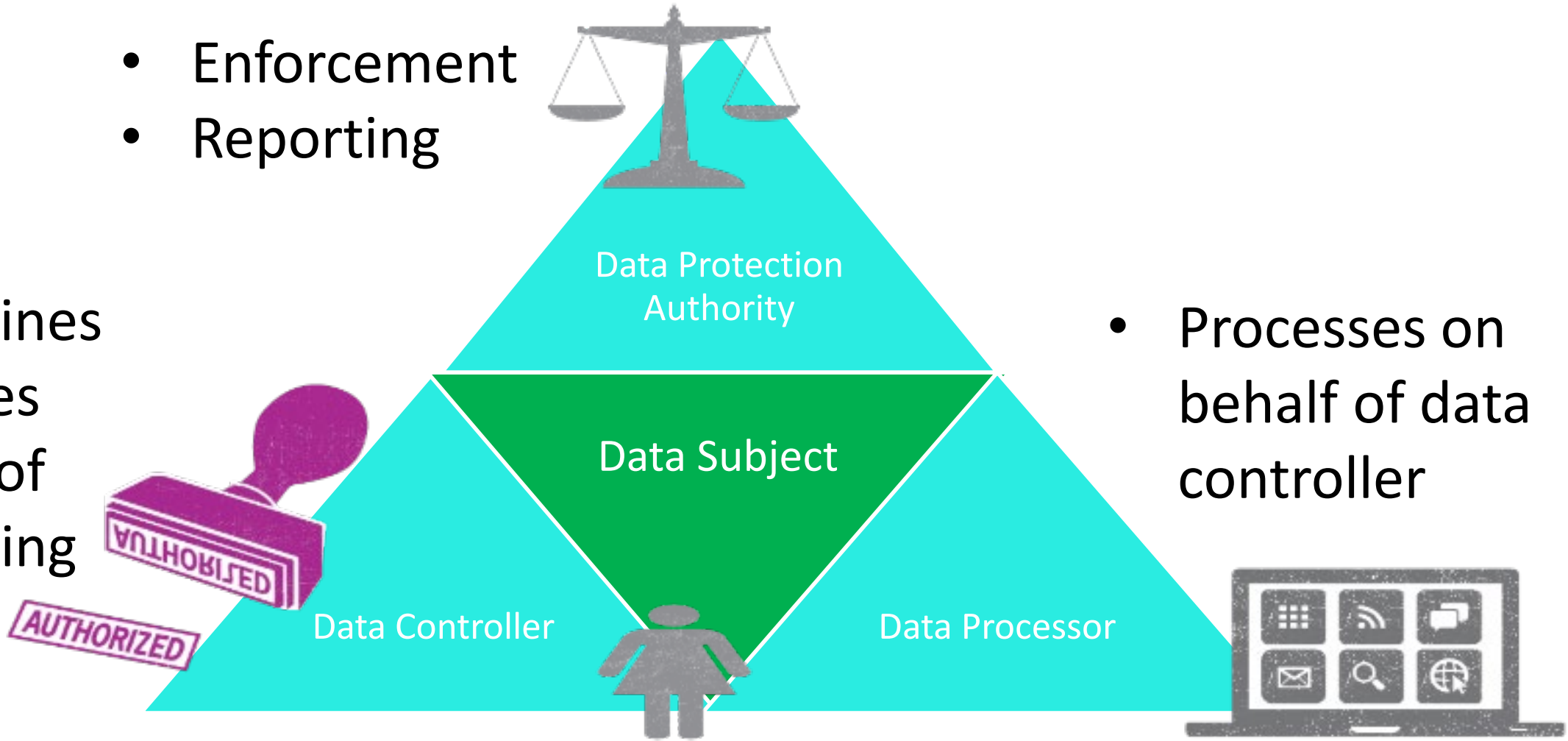
DATA PROTECTION AND PRIVACY PROTECTS WHAT WE 'SHOULD' BE DOING WITH THE DATA

Organization for Economic Co-operation and Development (OECD) 8 Privacy Principles

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability

Data Protection Roles

- Enforcement
- Reporting



- Determines purposes
- Means of processing

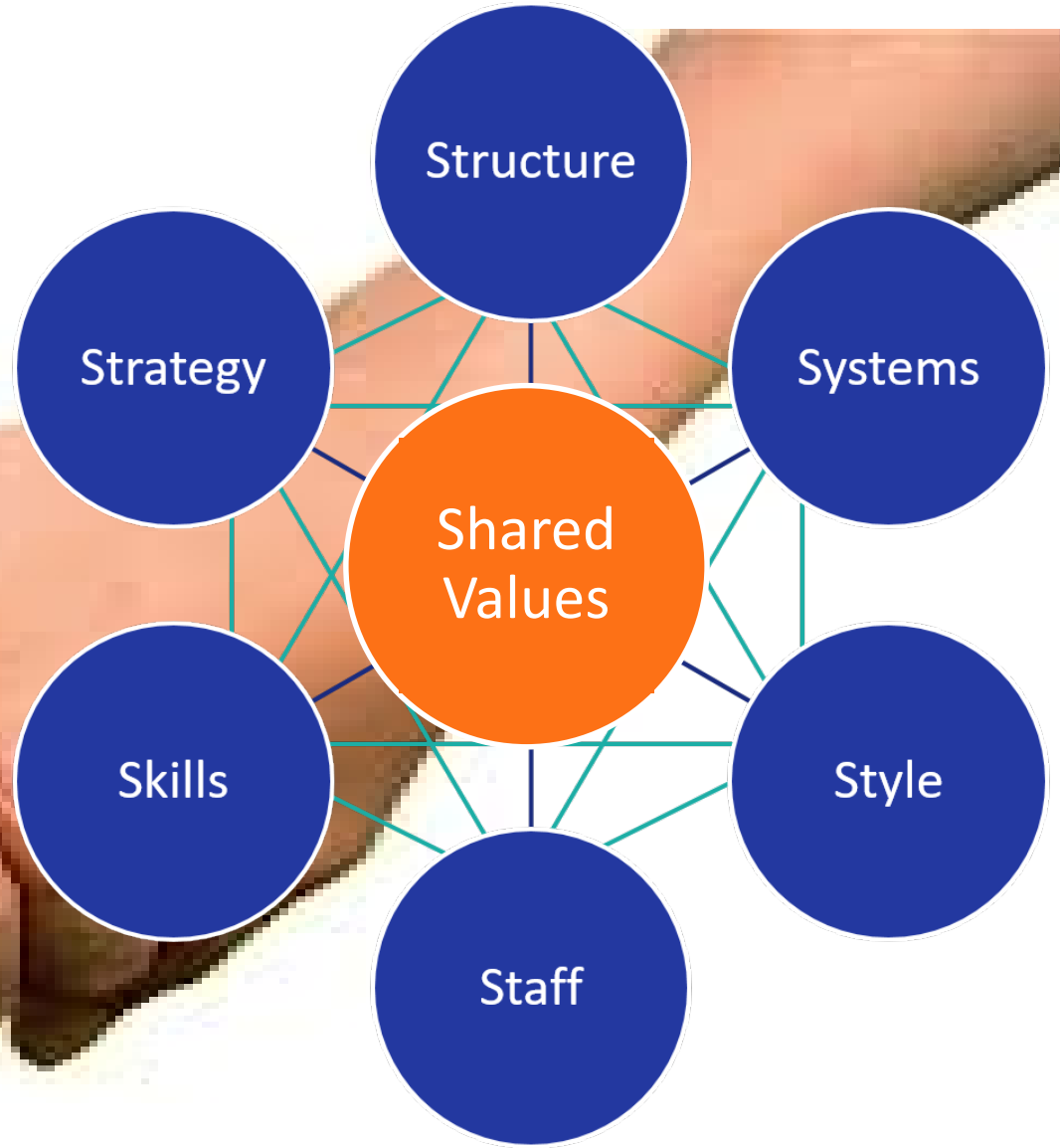
- Processes on behalf of data controller

Privacy By Design – 7 Principles

1. Proactive/ Preventive
2. Privacy By Default
3. Embedded In Design
4. Positive-Sum Not Zero-Sum
5. End-End Lifecycle Protection
6. Visibility/Transparency
7. Respect for Users

MEANINGFUL POLICIES AND PROCEDURES CODIFY OUR ORGANIZATION'S EXPECTATIONS

- **Relevant, up-to-date and accessible:**
  - Policies
  - Procedures
  - Standards
  - Guidelines



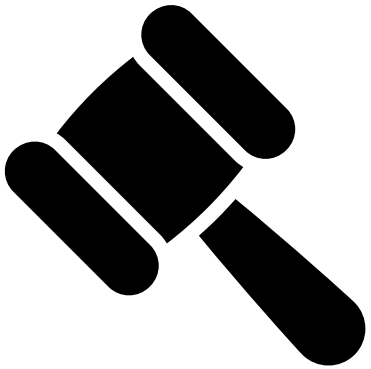
Policies, Procedures, Standards, Guidelines, Baselines – What is the Difference?

Laws, Regulations, Requirements,
Organizational Goals, Objectives

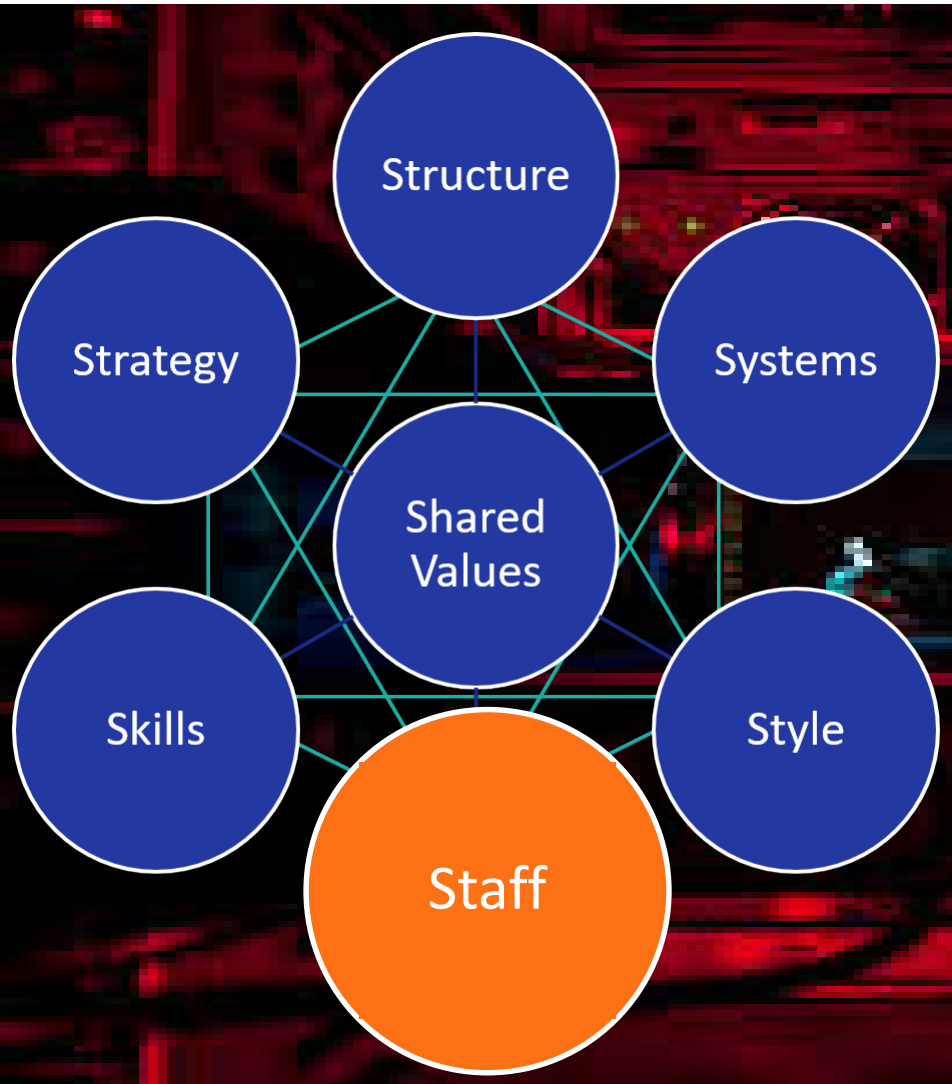
General Organizational (Information Security) Policy
Representing Management Directives

Functional Area Implemented Policies

Baselines (Required, Consistency)	Guidelines (Recommended, but Optional)	Procedures (Step By Step)	Standards Specific Hardware/ & Software

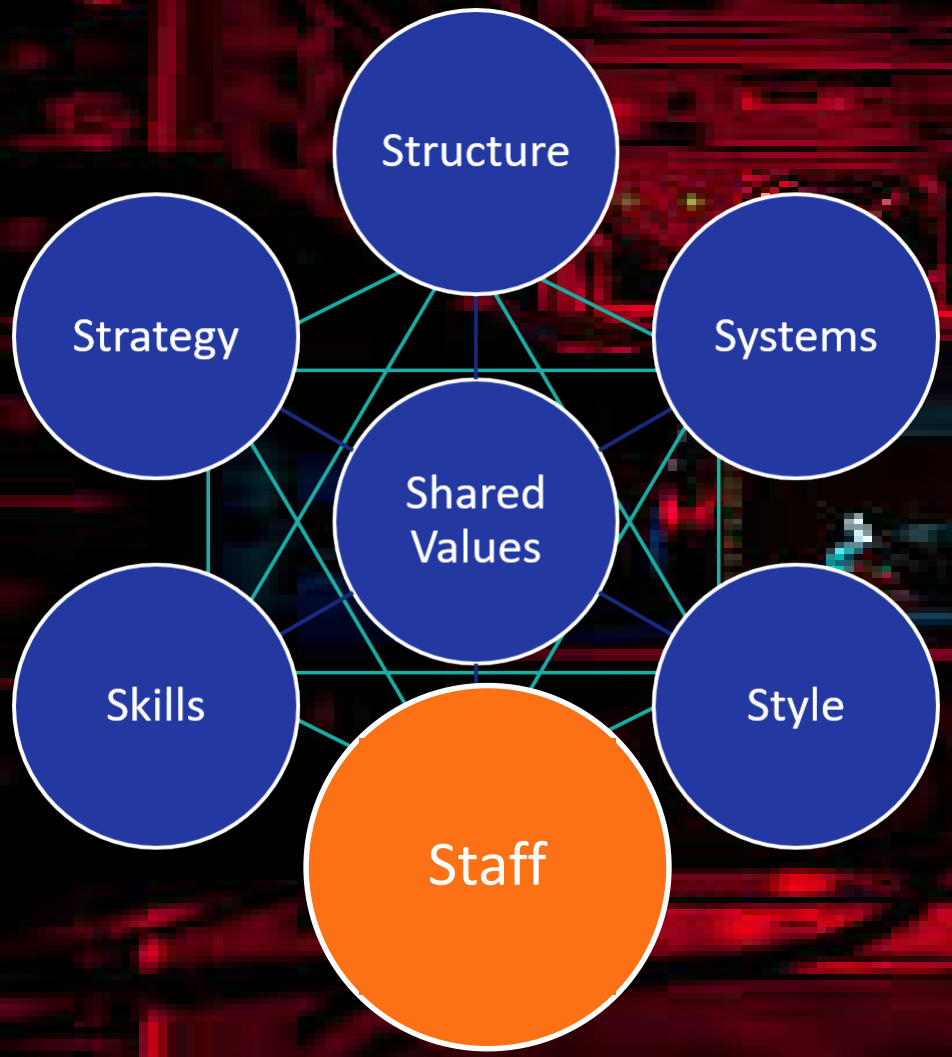


OBTAINING THE RIGHT STAFF CAN MAKE OR BREAK THE CYBERSECURITY ORGANIZATION



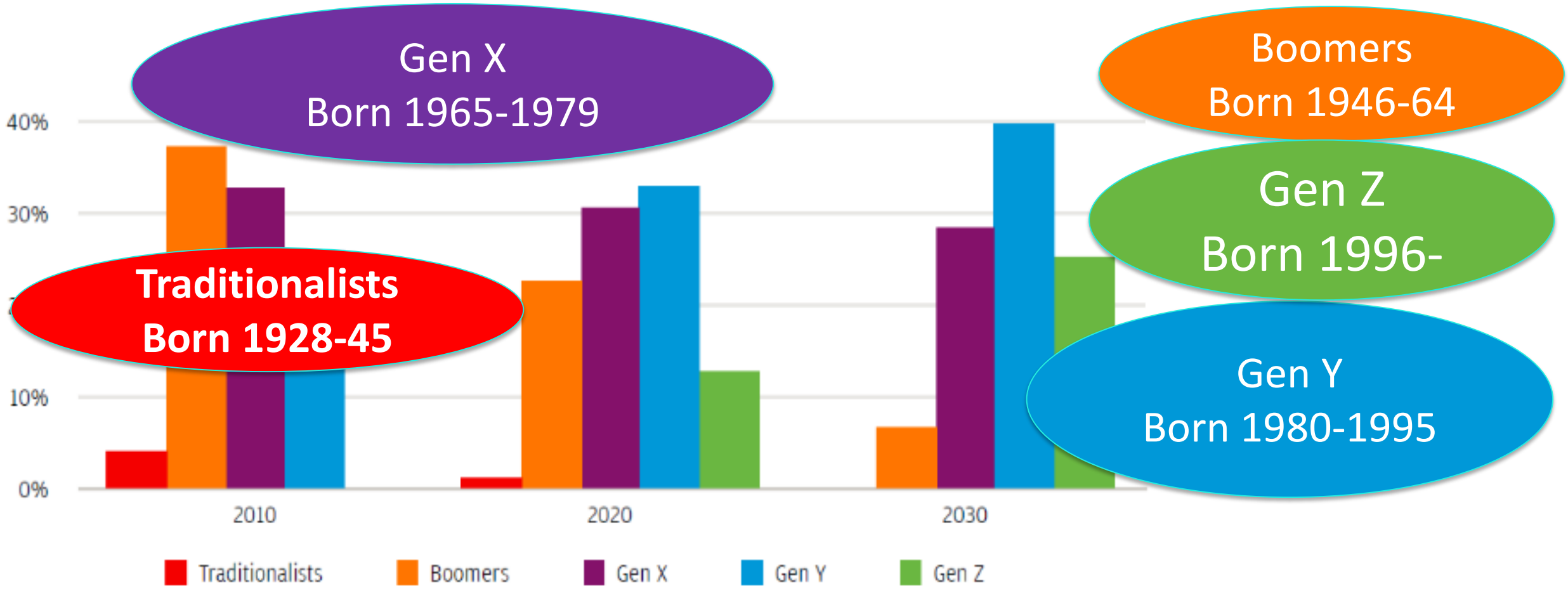
STAFF ARE VIEWED IN HARD TERMS (Salaries, Performance, formal training) and SOFT TERMS (morale, attitude motivation, and behaviors)

GREATER STAFF INSIGHTS VIA MANAGING MULTI-GENERATIONAL WORKFORCE DYNAMICS



- What are the differences between the generations and how foes that impact teams?
- What are the individual personality preferences?

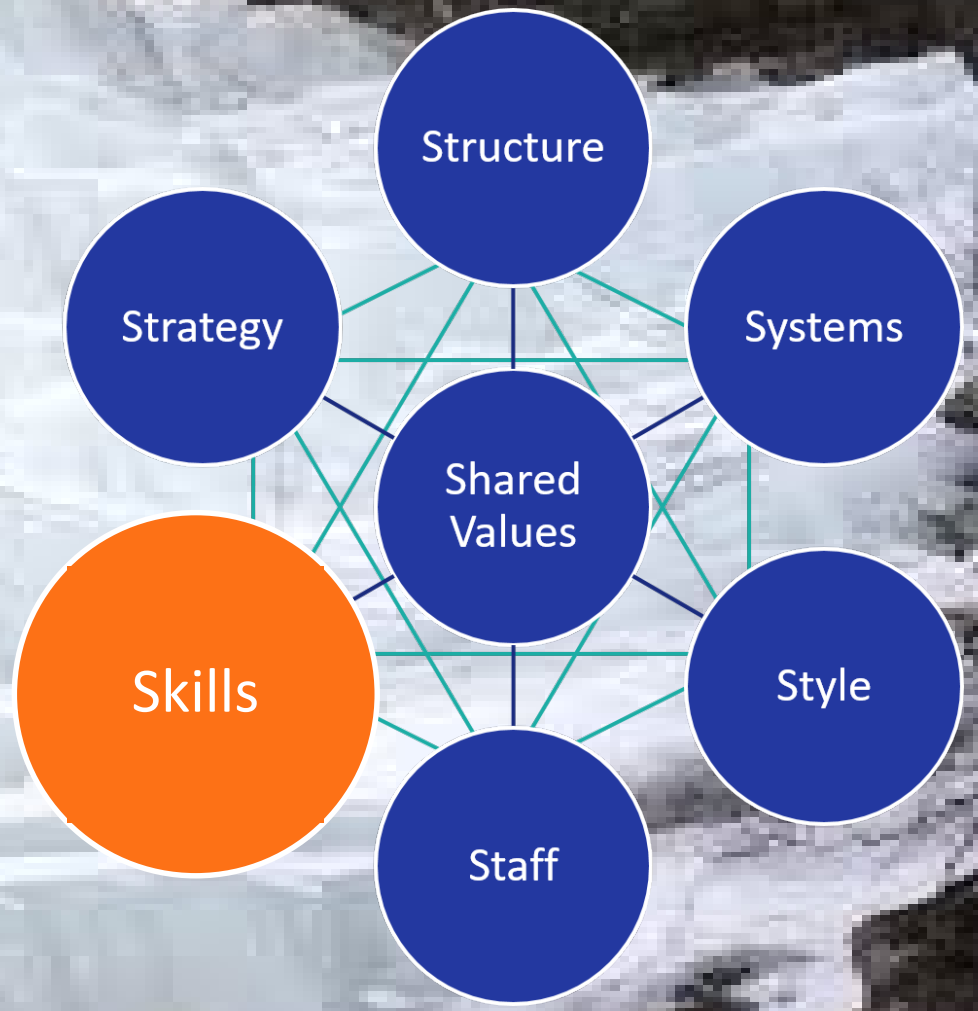
The Workforce Is Changing Dramatically



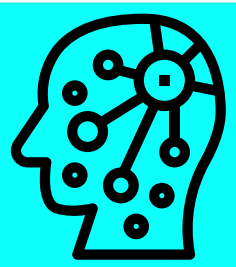
Source: Deloitte Research/UN Population Division, It's 2008: Do You Know Where Your Talent Is?

CISO/SECURITY LEADER SKILLS DON'T HAPPEN BY BIRTH OR ACCIDENT

WHAT SKILLS (TECHNICAL, BUSINESS, SOFT) DOES THE CISO NEED TO BE SUCCESSFUL?



“Techie” Core Competencies



Analytical Problem Solving
Best Practices
Innovations
Process Orientation

Tool Expertise
Industry Standards
Emerging Technologies

Team Work
Crisis Management
Provide Technical Assistance

Leadership Competencies

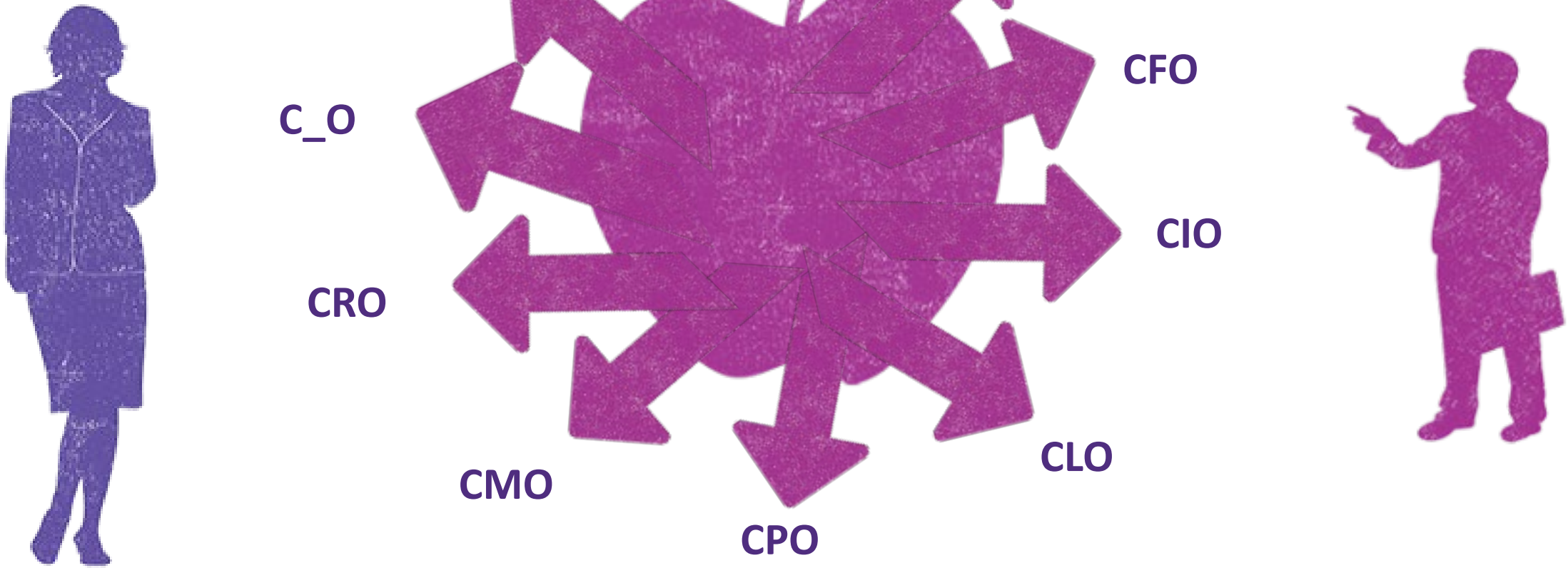
Self-Control	Interpersonal Awareness	Adapability
Perseverance	Results-Oriented Flexibility	Thoroughness
Self-Development Orientation	Critical Information Seeking	Efficiency Seeking

SKILLS: Soft Skills

- ✓ Operational, technical, business and leadership skills
- ✓ Certifications helpful but not mandatory
- ✓ 10-20+ years experience to train for CISO (operations, engineering, architecture and business
- ✓ Vertical and Industry experience helpful, but not requirement; especially from large tech to small co.
- ✓ Business/risk-based backgrounds need to gain tech knowledge first

Source: Gartner, Feb 2017, A Step-by-Step Guide to Becoming a CISO

Form Relationships with All CXO Stakeholders



And Various Oversight Committees

- LEGAL
- RISK
- COMPLIANCE
- HUMAN RESOURCES
- FINANCE
- PHYSICAL SECURITY/FACILITIES
- BUSINESS UNITS
- MARKETING
- INFORMATION TECHNOLOGY

The relationship between the CISO and senior leadership CONVEYS *STYLE*

HOW EFFECTIVE IS THE CISO WITH THE OTHER EXECUTIVES AND THE BOARD OF DIRECTORS?

Presenting to the Board

5 Principles for the Board

National Association of Corporate Directors (NACD)	
Principle 1	Directors need to understand and approach cybersecurity as an **enterprisewide risk management** issue, not just an IT issue.
Principle 2	Directors should understand the **legal implications of cyber risks** as they relate to their company's specific circumstances.
Principle 3	Boards should have **adequate access to cybersecurity expertise**, and discussions about cyber-risk management should be given **regular and adequate time** on the board meeting agenda.
Principle 4	Directors should set the expectation that management will establish an **enterprisewide cyber-risk management framework**.
Principle 5	Board-management discussion of cyber risks should include **identification of which risks to avoid, which to accept, and which to mitigate or transfer** through insurance, as well as specific plans associated with each approach.

Source: Cyber-Risk Oversight Executive Summary, Director's Handbook Series 2014 Edition (National Association of Corporate Directors (NACD) in collaboration with AIG and Internet Security Alliance (ISA)

5 PRINCIPLES FOR THE BOARD

National Association of Corporate Directors (NACD)	
Principle 1	Directors need to understand and approach cybersecurity as an **enterprisewide risk management** issue, not just an IT issue.

PRINCIPLE 1: Directors need to understand and approach cybersecurity as an enterprise wide risk management issue, not just an IT issue.

Source: Cyber-Risk Oversight Executive Summary, Director's Handbook Series 2014 Edition (National Association of Corporate Directors (NACD) in collaboration with AIG and Internet Security Alliance (ISA)

5 PRINCIPLES FOR THE BOARD

National Association of Corporate Directors (NACD)	
Principle 1	Directors need to understand and approach cybersecurity as an **enterprisewide risk management** issue, not just an IT issue.

PRINCIPLE 2:Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

Source: Cyber-Risk Oversight Executive Summary, Director's Handbook Series 2014 Edition (National Association of Corporate Directors (NACD) in collaboration with AIG and Internet Security Alliance (ISA)

5 PRINCIPLES FOR THE BOARD

National Association of Corporate Directors (NACD)

PRINCIPLE 3:Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.

Source: Cyber-Risk Oversight Executive Summary, Director's Handbook Series 2014 Edition (National Association of Corporate Directors (NACD) in collaboration with AIG and Internet Security Alliance (ISA)

5 PRINCIPLES FOR THE BOARD

National Association of Corporate Directors (NACD)	
Principle 1	Directors need to understand and approach cybersecurity as an **enterprisewide risk management** issue, not just an IT issue.

PRINCIPLE 4:Directors should set the expectation that management will establish an enterprise wide cyber-risk management framework.

Source: Cyber-Risk Oversight Executive Summary, Director's Handbook Series 2014 Edition (National Association of Corporate Directors (NACD) in collaboration with AIG and Internet Security Alliance (ISA)

5 PRINCIPLES FOR THE BOARD

National Association of Corporate Directors (NACD)	
Principle 1	Directors need to understand and approach cybersecurity as an **enterprisewide**

PRINCIPLE 5:Board-management discussion of cyber risks should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

Source: Cyber-Risk Oversight Executive Summary, Director's Handbook Series 2014 Edition (National Association of Corporate Directors (NACD) in collaboration with AIG and Internet Security Alliance (ISA)

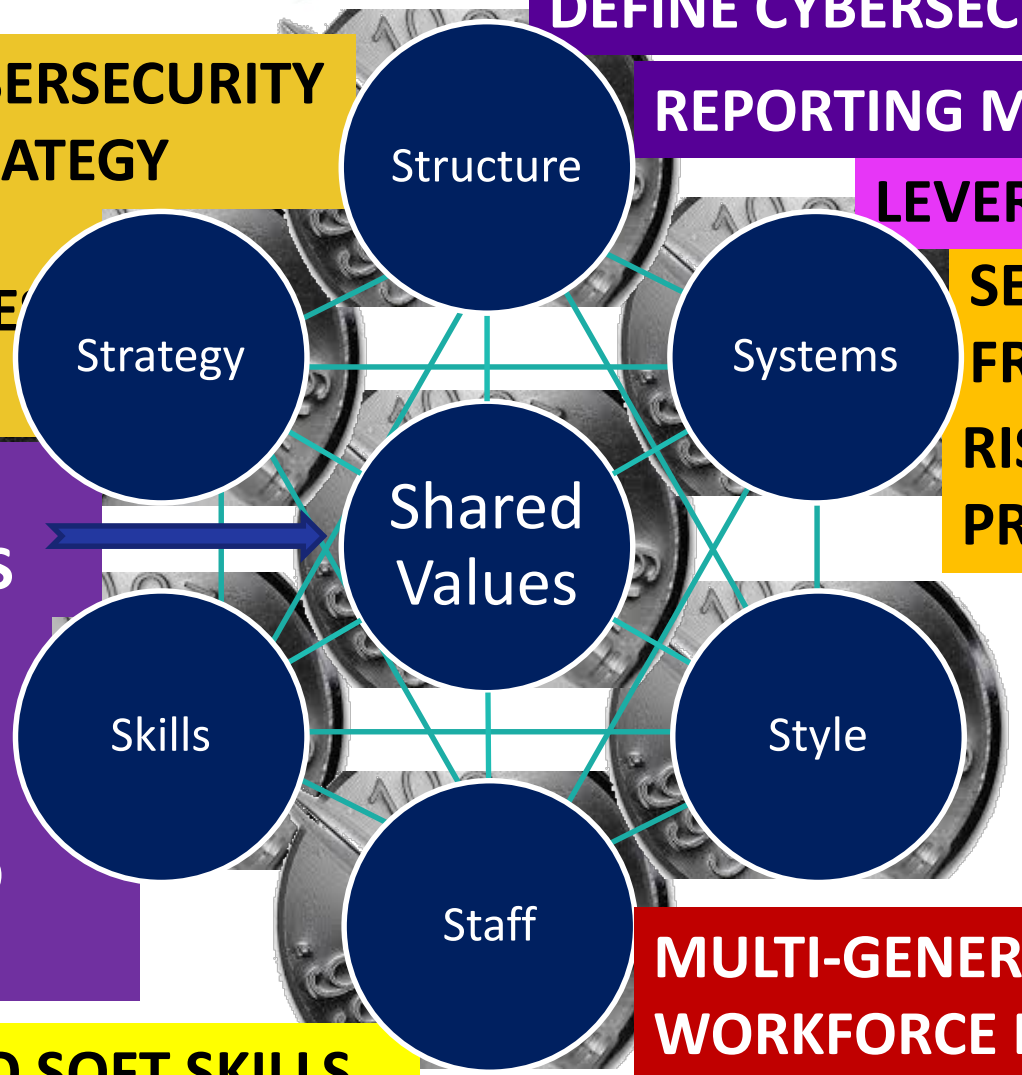
You are the CISO of a major healthcare institution, here is the situation:

1. It is 1 Month before the 04/30/19 annual board update
2. 12 months ago, a IOT Healthcare provider suffered a breach from web app vulnerability (150M Records, impact still unknown)
3. Your company's merger efforts are in trouble, costing millions more than anticipated, stock price down 15% last quarter, still up 20% for year
4. Re-imaging of machines due to ransomware is running 20% a month
5. Big 4 assessment indicated 2.6 program maturity on 5pt scale
6. Oh… you are presenting: What are you going to say?

THE CISO SECRET SAUCE

1. ADD A CISO
2. ADD THE RIGHT THINGS (7-S FRAMEWORK)
3. DO THEM RIGHT

7-S MODEL APPLIED TO CYBERSECURITY LEADERSHIP



DEFINE CYBERSECURITY FUNCTIONS

REPORTING MODEL

LEVERAGING INCIDENTS

SECURITY CONTROL FRAMEWORKS

RISK MANAGEMENT PRACTICES

CISO AND THE BOARD

MULTI-GENERATIONAL WORKFORCE DYNAMICS

CISO SOFT SKILLS

POLICIES AND PROCEDURES

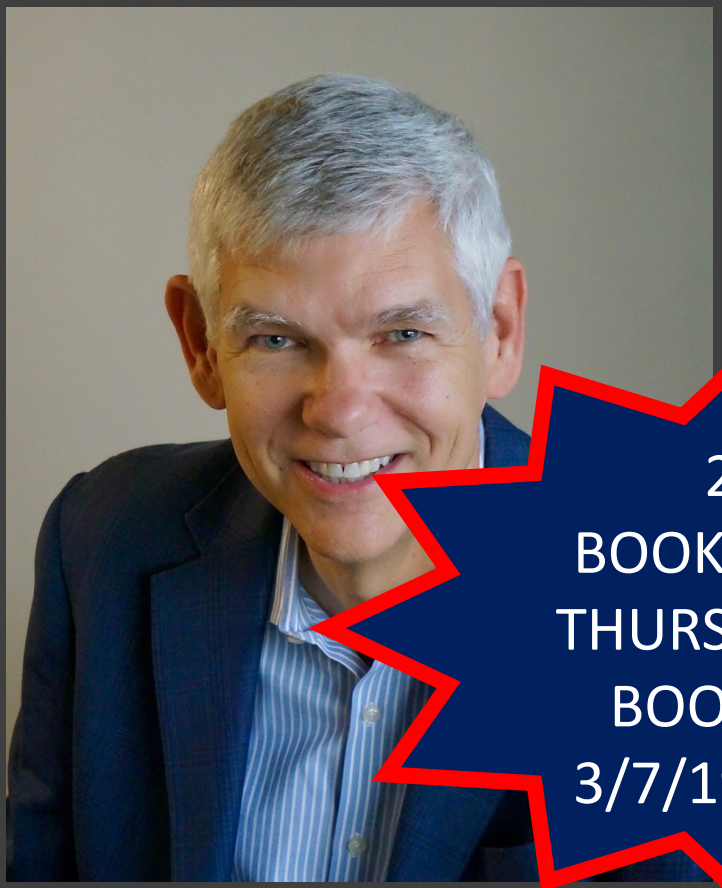
LAWS AND REGULATIONS DATA PROTECTION & PRIVACY

DEVELOP CYBERSECURITY VISION & STRATEGY EMERGING TECHNOLOGIES & TRENDS

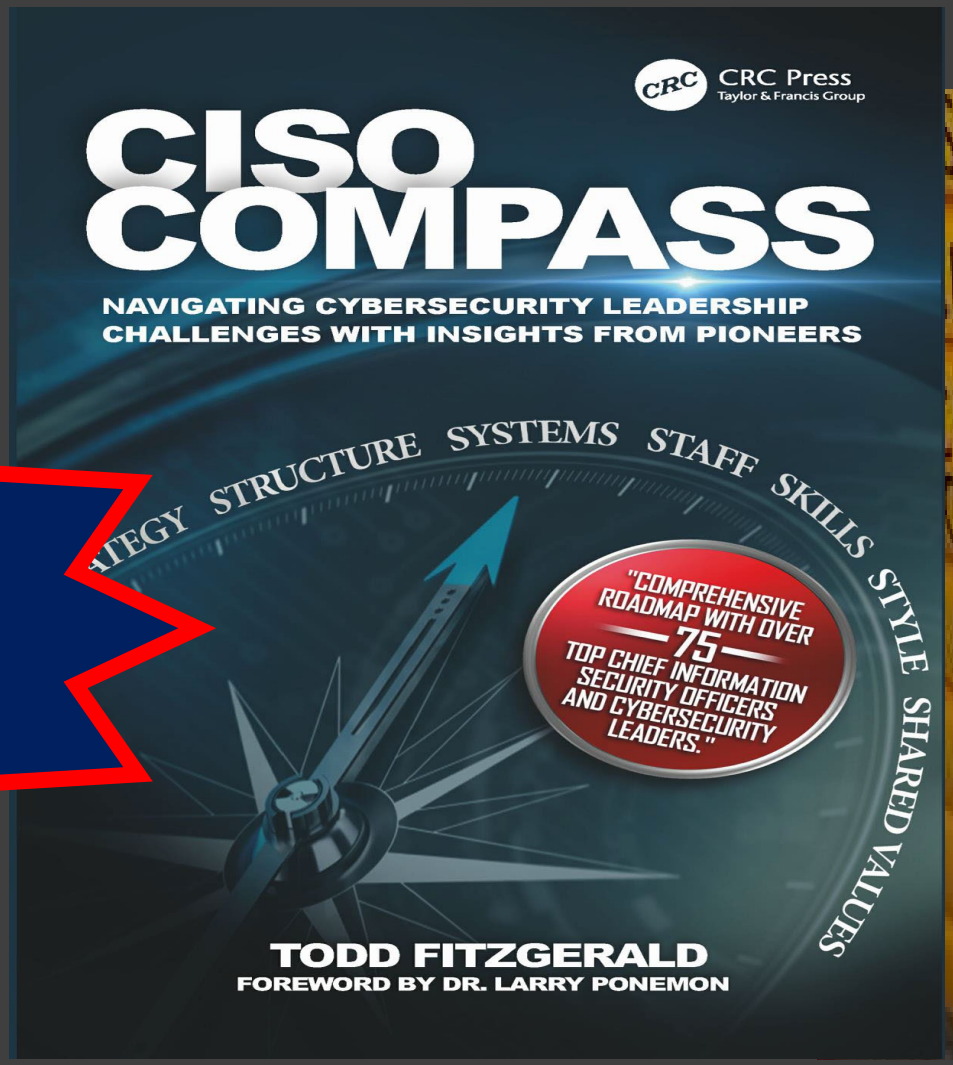
Source: T. Fitzgerald, *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers* (2019, Auerbach Publications)

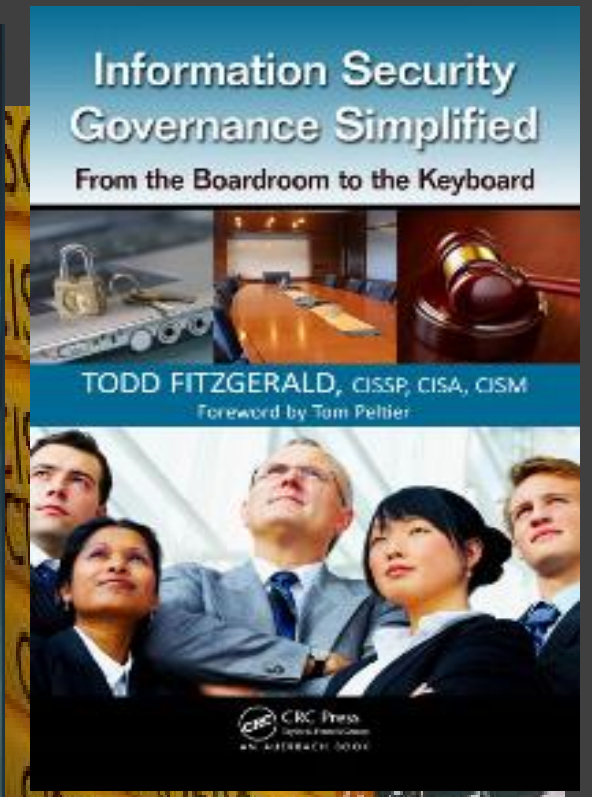
THANK YOU!!! ANY QUESTIONS?

#RSAC



2019
BOOK SIGNING
THURSDAY RSAC
BOOKSTORE
3/7/19 12:30-1





LINKEDIN.COM/IN/TODDFITZGERALD

CISO SPOTLIGHT, LLC

Trusted Cybersecurity
and Privacy Training

AMAZON.COM/AUTHOR/TODDFITZGERALD

RSAConference2019