RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **SEM-M01E**

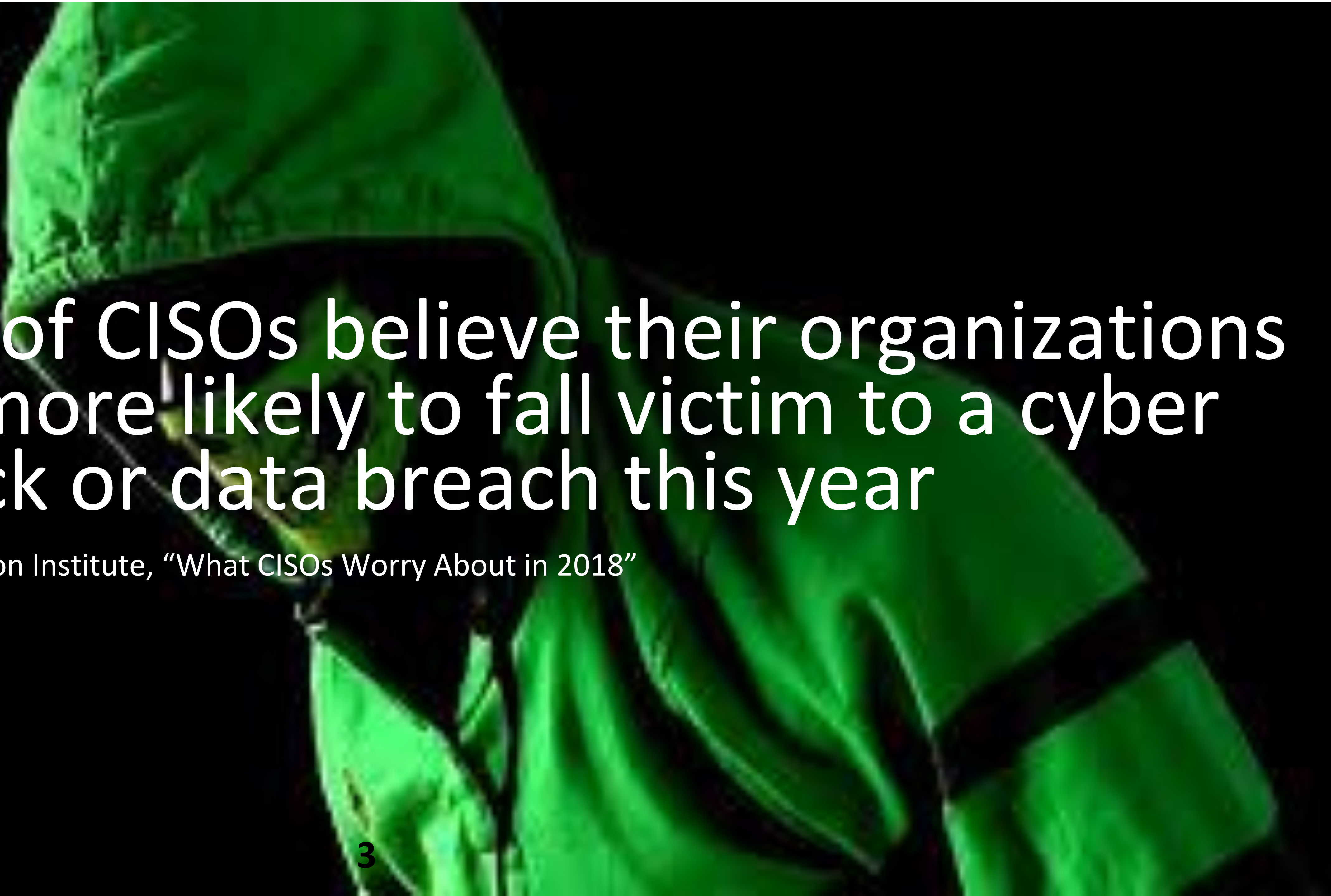
Transforming from Techie to Security Leader

Todd Fitzgerald

CISO, ***CISO COMPASS*** Cybersecurity Leadership Author
CISO SPOTLIGHT, LLC
EXECUTIVE IN RESIDENCE – Cybersecurity Collaborative
@securityfitz

Today's Objective:

1. The Evolution of the Cybersecurity Leader (CISO/VP/Dir/Mgr Information Security)
2. The Skills Required of this ~~guy~~ person
3. The Job Opportunity

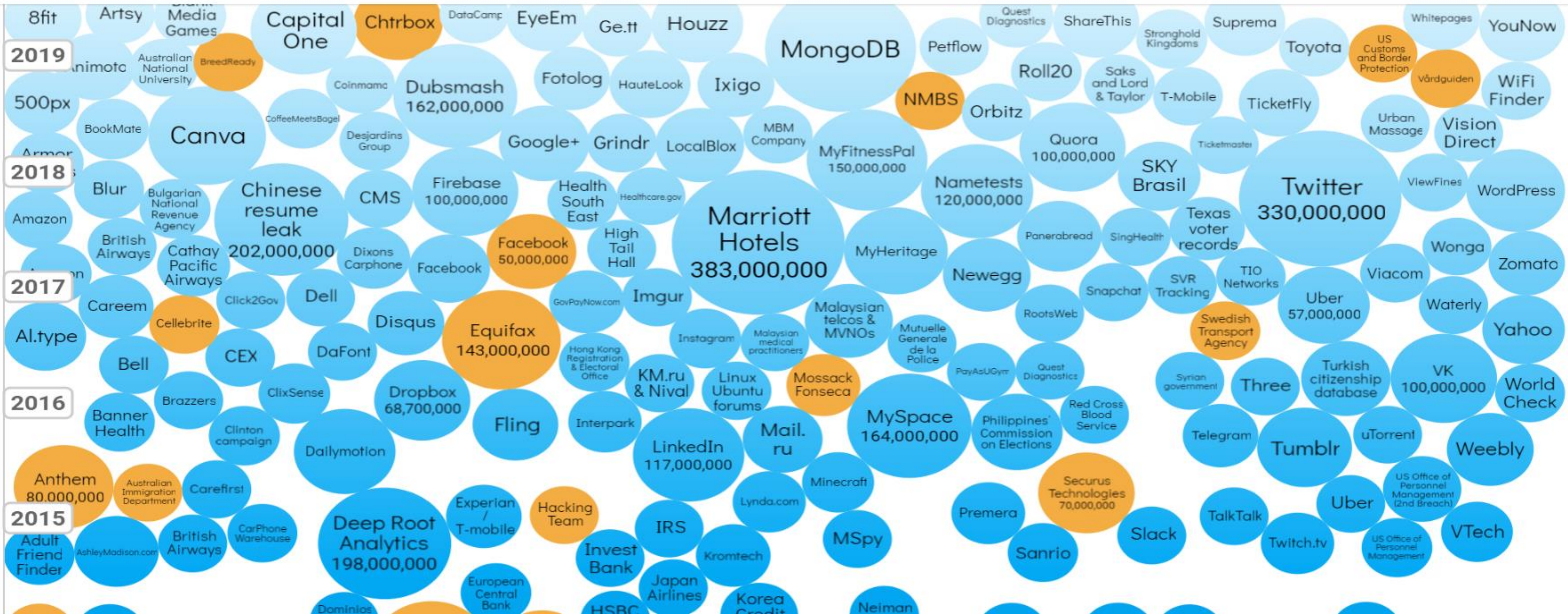


67% of CISOs believe their organizations are more likely to fall victim to a cyber attack or data breach this year

- Ponemon Institute, “What CISOs Worry About in 2018”

DATA BREACH

And That Includes Only The *Reported* Ones



Source: Informationisbeautiful.com

CISO SPOTLIGHT, LLC

Trusted Cybersecurity and Privacy Training

SOLUTION: We Recruit a

CISO

Chief Information Security Officer

CISO 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

Source: Actual CISO Job Description posted on Glassdoor (company name omitted)

Where Do CISOs Come From ?

A. Born as natural paranoid leaders

B. Raised their hand at the wrong time during a meeting

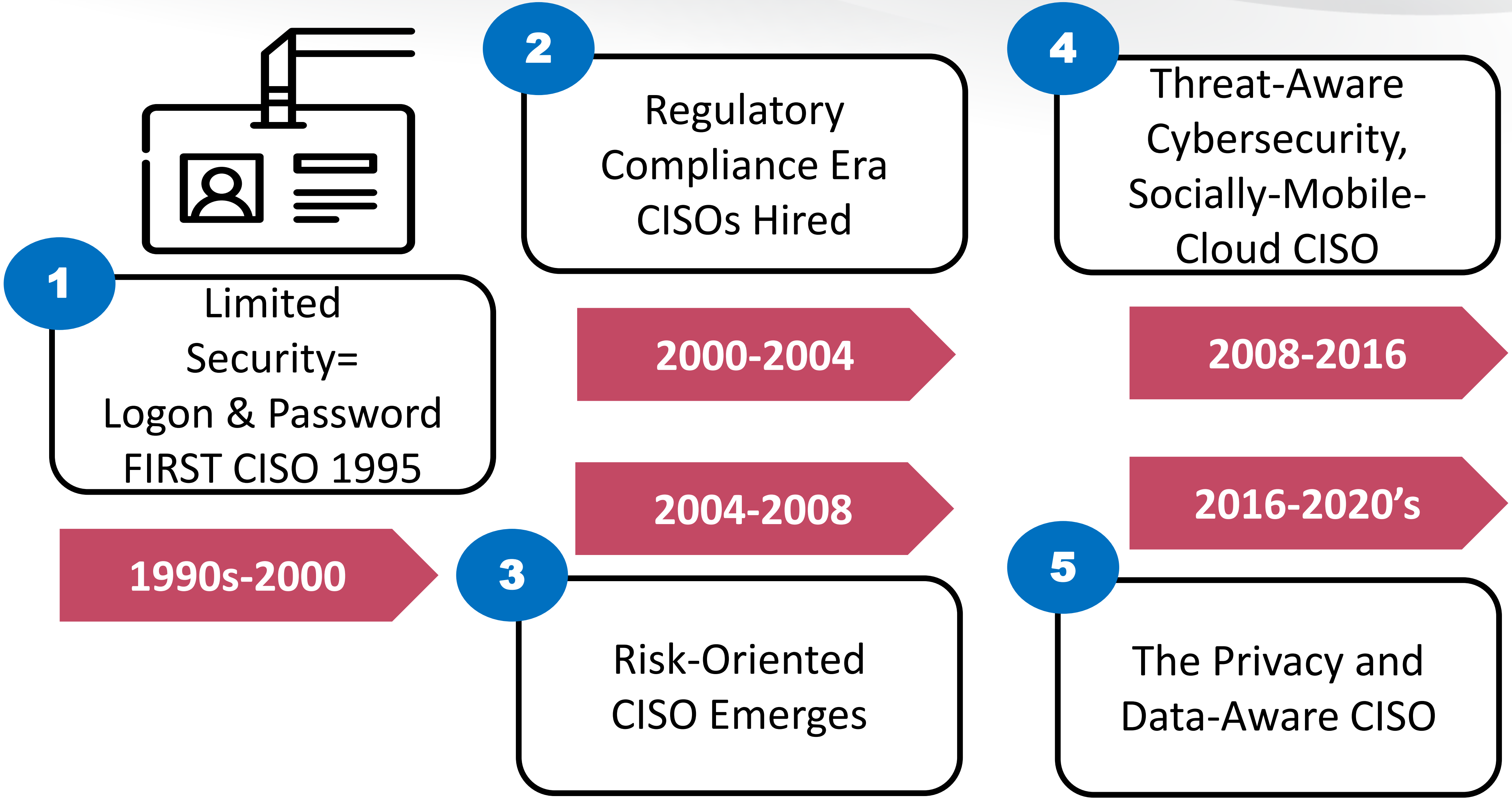
C. Didn’t attend the selection meeting

D. Last IT guy in the shop

E. Worked on compliance stuff

F. Chose this career (full deck should be checked)

5 STAGES OF CISO EVOLUTION 1995-2020'S



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

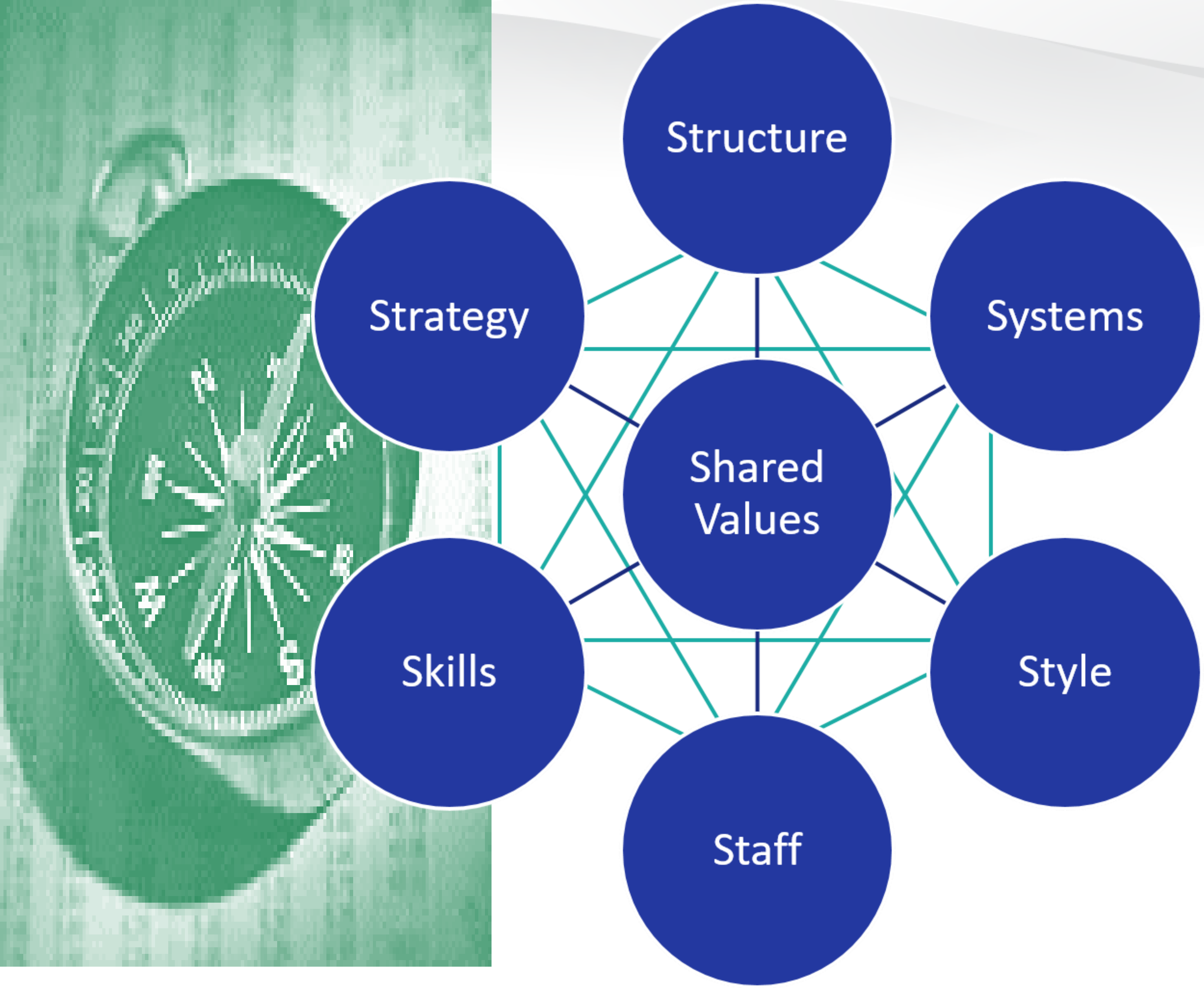
2016-2020's

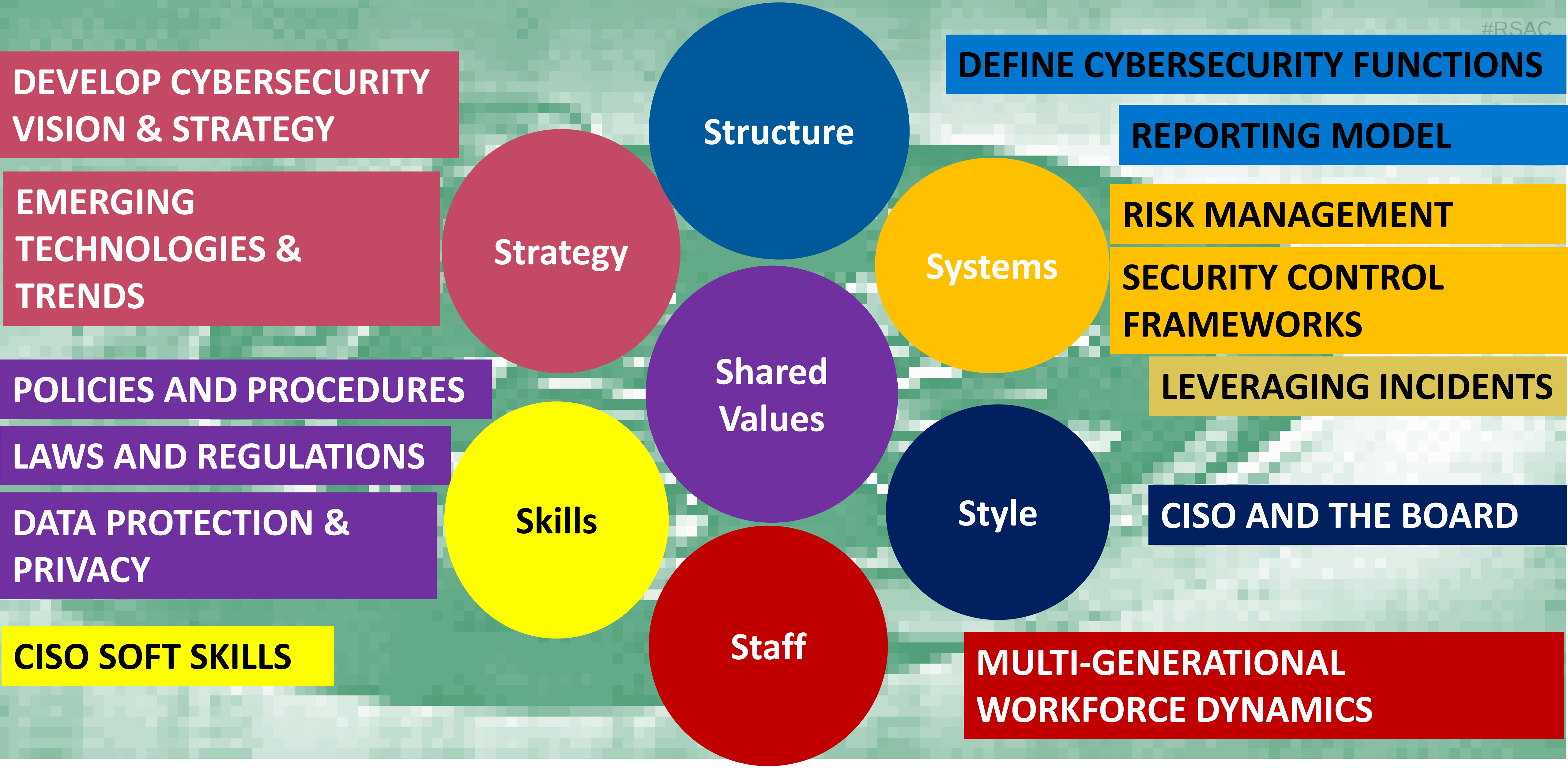
Increasingly Becoming a Global-Oriented Role

“The CISO is responsible for a **global organization** and will manage **teams** located **appropriately** across the globe.”

- Recent Job Posting Fortune Global 500 Company

The CISO's Ability To Realize a Cybersecurity Strategy Is Impacted By 7 Key Factors





Strategy

DEVELOP CYBERSECURITY VISION & STRATEGY

EMERGING TECHNOLOGIES & TRENDS

Structure

DEFINE CYBERSECURITY FUNCTIONS

REPORTING MODEL

Systems

RISK MANAGEMENT

SECURITY CONTROL FRAMEWORKS

LEVERAGING INCIDENTS

Shared Values

POLICIES AND PROCEDURES

LAWS AND REGULATIONS

DATA PROTECTION & PRIVACY

Skills

CISO SOFT SKILLS

Style

CISO AND THE BOARD

Staff

MULTI-GENERATIONAL WORKFORCE DYNAMICS

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

2020 CISO Managed Functions

Monitor

- Security Baseline Configuration Review
- Logging SIEM & Monitoring
- Vulnerability Assessment
- Managed Services
- Incident Response
- Forensic Analysis
- Threat Intelligence
- Security Analytics
- Insider Threat

Awareness

- End User Security Awareness
- Intranet Site and Policy Publication
- Targeted Awareness
- Phishing Programs
- Executive/Board Education and Advance Reporting

Risk

- Risk Assessment and Analysis
- Systems Security Plan
- Internal and External Penetration Testing
- Privacy
- Cyber Insurance
- 3rd Party Vendor Risk Management

Policy/Controls

- Security Policy
- Security Architecture
- Security Control Assessment
- Identity Access Management
- Bus Continuity & Disaster Recovery
- Control Framework Compliance
- Program Management

The Security Leader Skills Required of This ~~Guy~~ Person

Decision Point: Critical Differences in Thought Processes

Technology Challenge

Concrete Task-Oriented

Hands-On, Mastery of Skill

High Individual Contribution

Meetings, Documentation=AVOID

TECHNICAL

Managerial Competencies Are Different

Embrace Ambiguity

Oral Communications Up, Down, Across

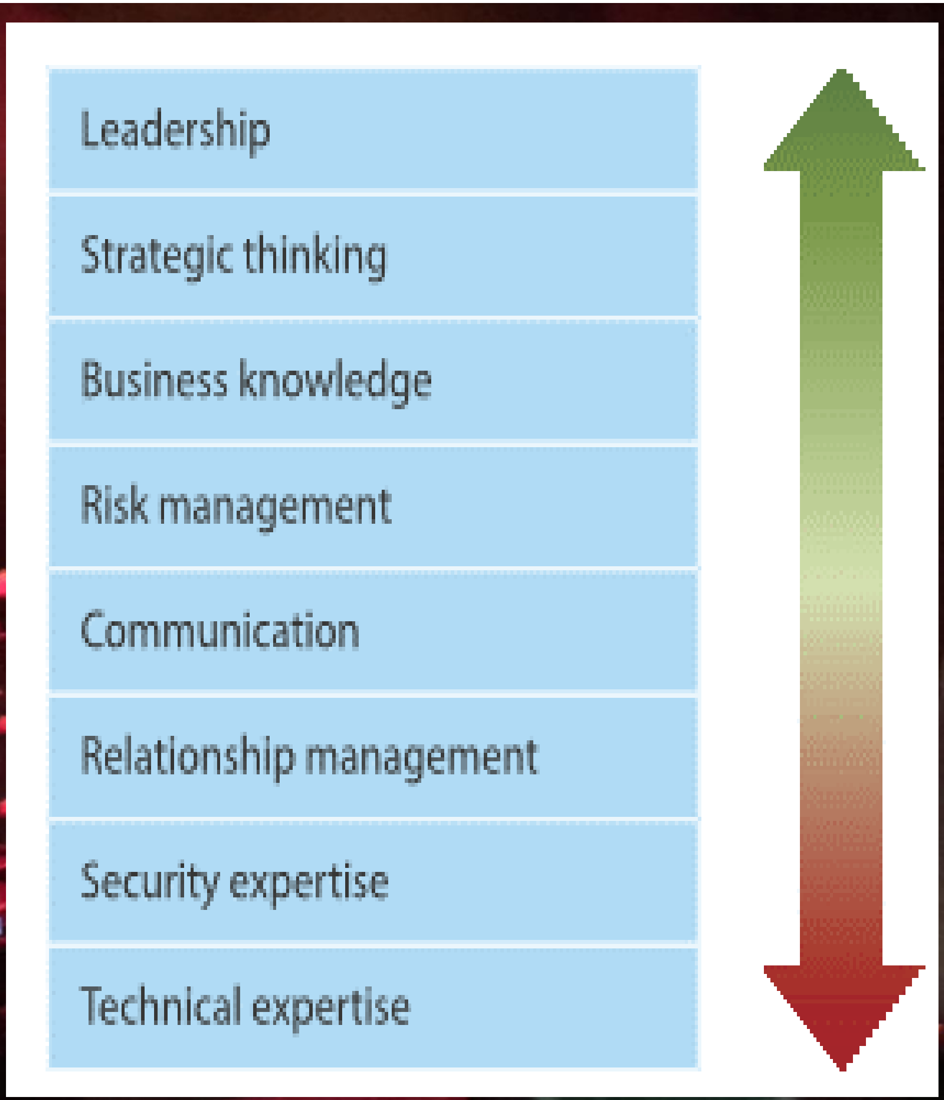
People-Oriented Conflict Resolution

Influence Consensus Building

Multi-Generational Team Building

MANAGERIAL

Skills: Leadership Skills Paramount for Today’s CISO



Leadership

Strategic thinking

Business knowledge

Risk management

Communication

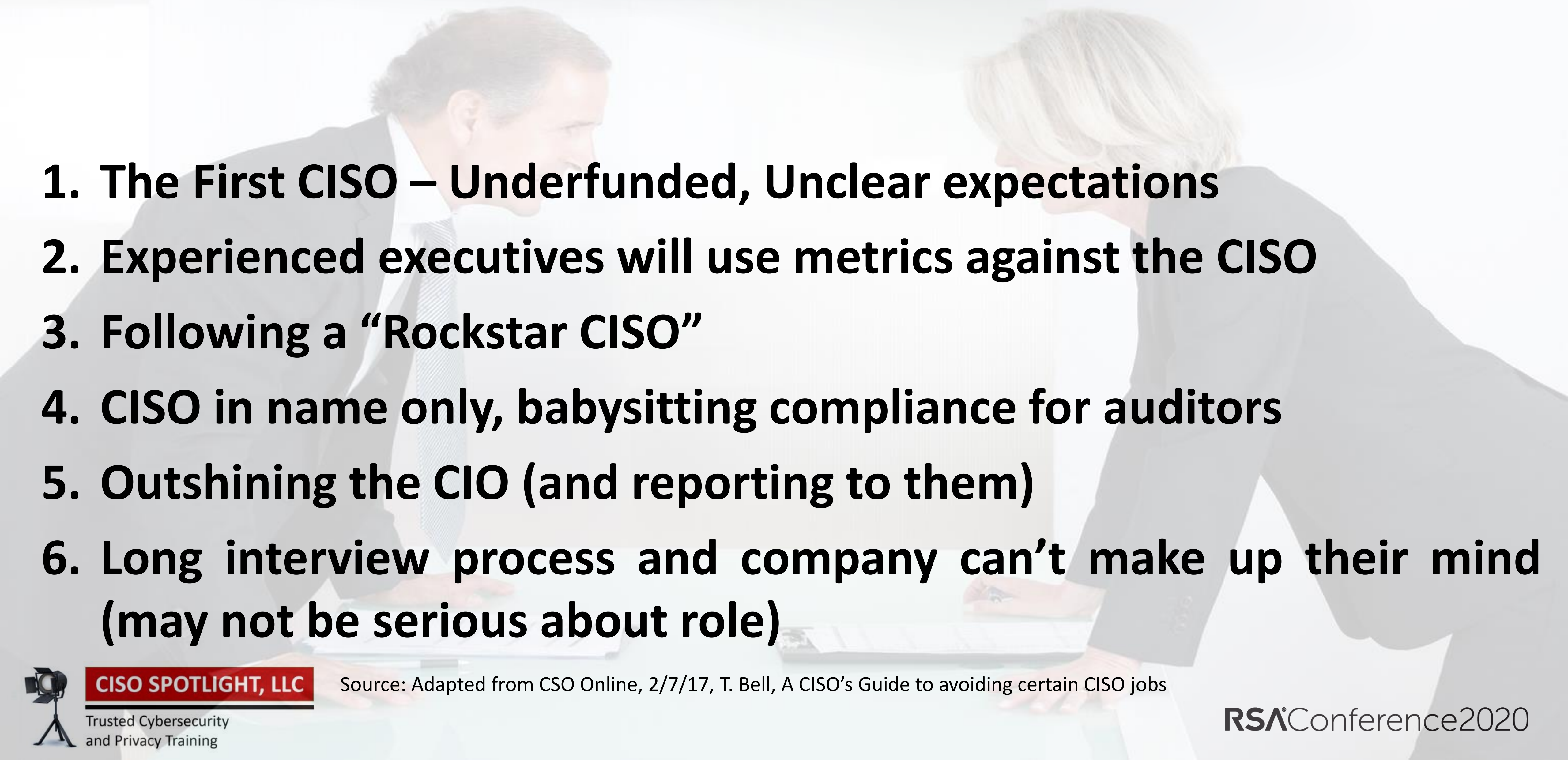
Relationship management

Security expertise

Technical expertise

Source: Forrester Research (Projection to 2018 CISO)

Avoid CISO "Pitfalls"



1. The First CISO – Underfunded, Unclear expectations
2. Experienced executives will use metrics against the CISO
3. Following a "Rockstar CISO"
4. CISO in name only, babysitting compliance for auditors
5. Outshining the CIO (and reporting to them)
6. Long interview process and company can't make up their mind (may not be serious about role)

Source: Adapted from CSO Online, 2/7/17, T. Bell, A CISO's Guide to avoiding certain CISO jobs

RSAConference2020

The Opportunity

What Degrees Do 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

CISO SPOTLIGHT, LLC
Trusted Cybersecurity
and Privacy Training

Challenge Conventional Thinking Where CISOs Come From

CONSULTING

□ <1 in 1000 Big Four security consultants become CISOs

LAW ENFORCEMENT

□ < 4% come from this background

MILITARY

□ <11% Fortune 500 CISOS have military background

TECH COMPANY

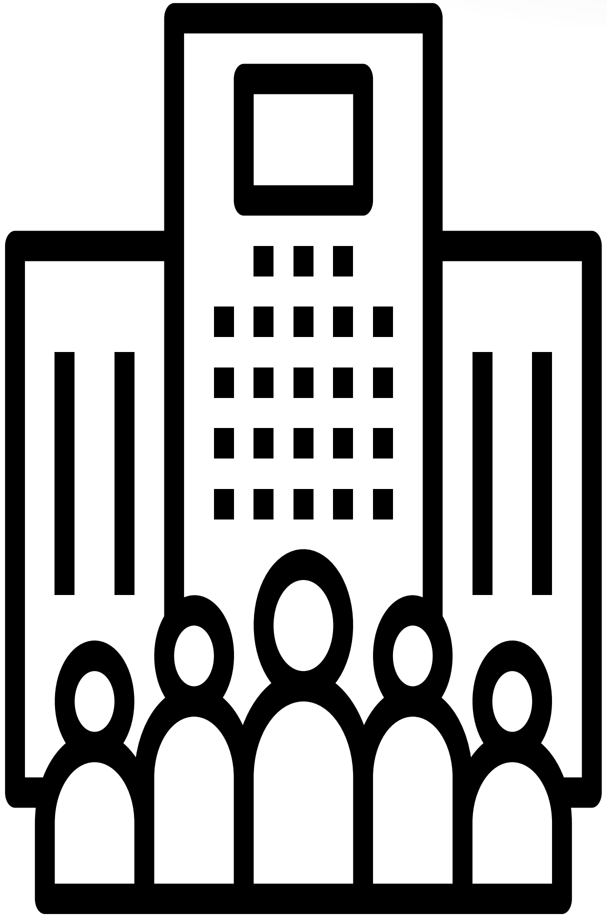
□ 25% worked for security vendor/service provider, few hired directly to CISO role

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

Do CISOs Get Promoted From Within?

59% Fortune 500 CISOs External Hires

4% CISOs have SVP title



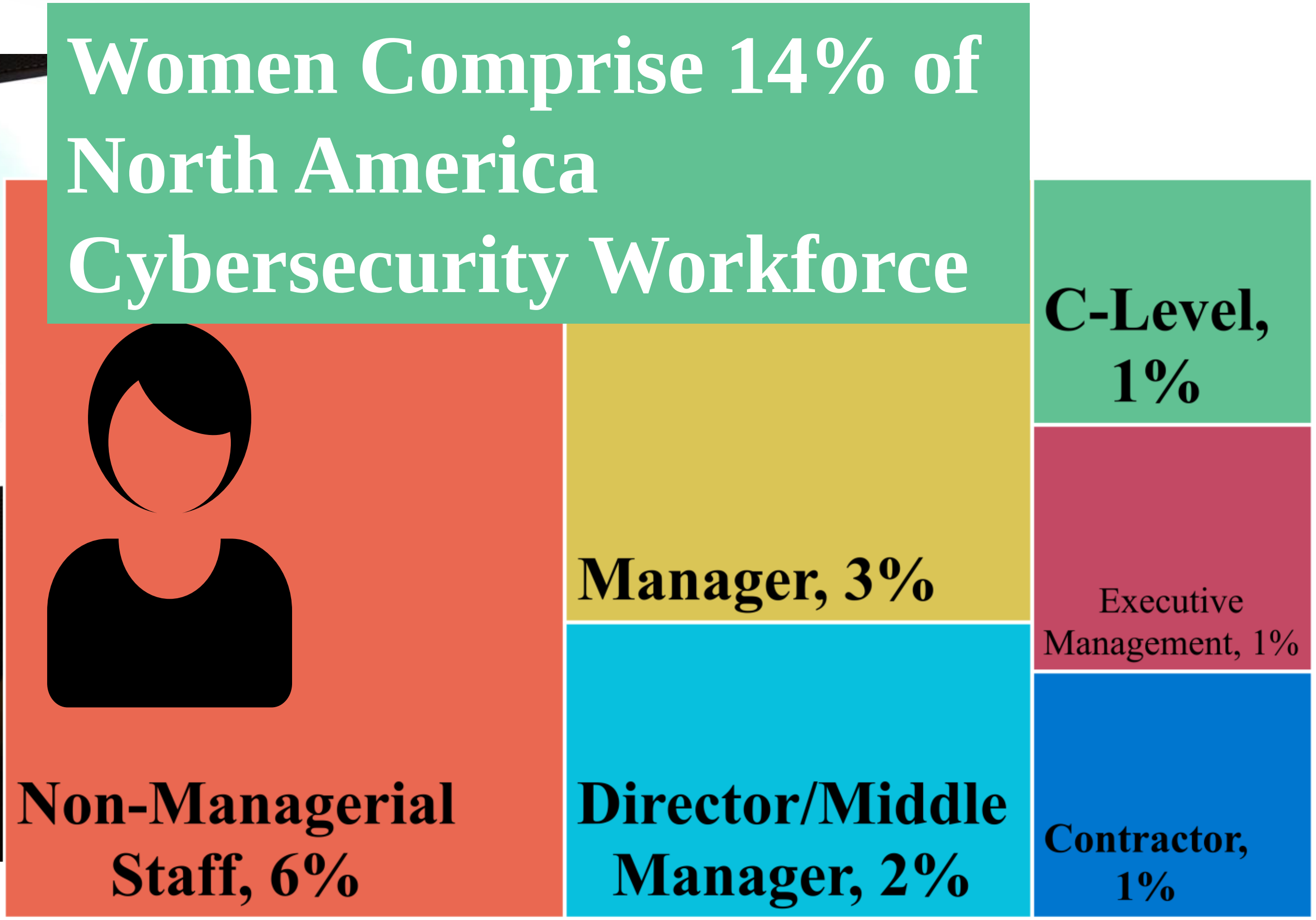
Few F100 hired first-time CISO; rest of F500 ok with that

F500 CISOs average tenure 4.5 years

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

Cybersecurity Leadership Demographics Are Changing

Source: ISACA SheLeadsTech Panel, Dublin, Ireland 2018, www.dogpatchlabs.com



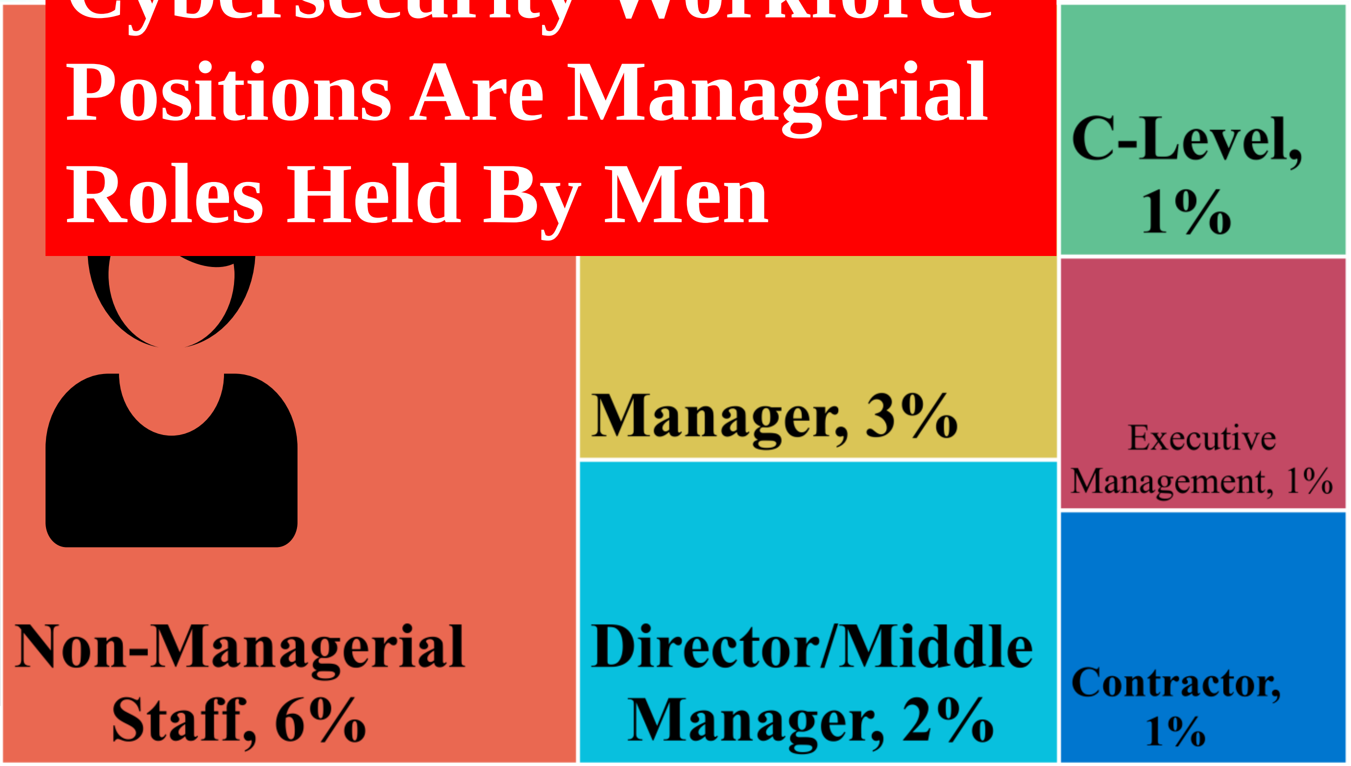
Women Comprise 14% of North America Cybersecurity Workforce

Note: Women n=2,134, Men n=16,679, percentages may not total 100% due to rounding, Source: T. Fitzgerald, *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers, Figure 13.2,* (2019, Auerbach Publications)

Cybersecurity Leadership Demographics Are Changing

Source: ISACA SheLeadsTech Panel, Dublin, Ireland 2018, www.dogpatchlabs.com

42% of North America Cybersecurity Workforce Positions Are Managerial Roles Held By Men



Note: Women n=2,134, Men n=16,679, percentages may not total 100% due to rounding, Source: T. Fitzgerald, *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers, Figure 13.2,* (2019, Auerbach Publications)

CISO SPOTLIGHT, LLC
Trusted Cybersecurity and Privacy Training

"Employment of information security analysts is projected to grow 32 percent from 2018 to 2028, much faster than the average for all occupations."

- U.S. Dept of Labor

Key Certifications To Invest In

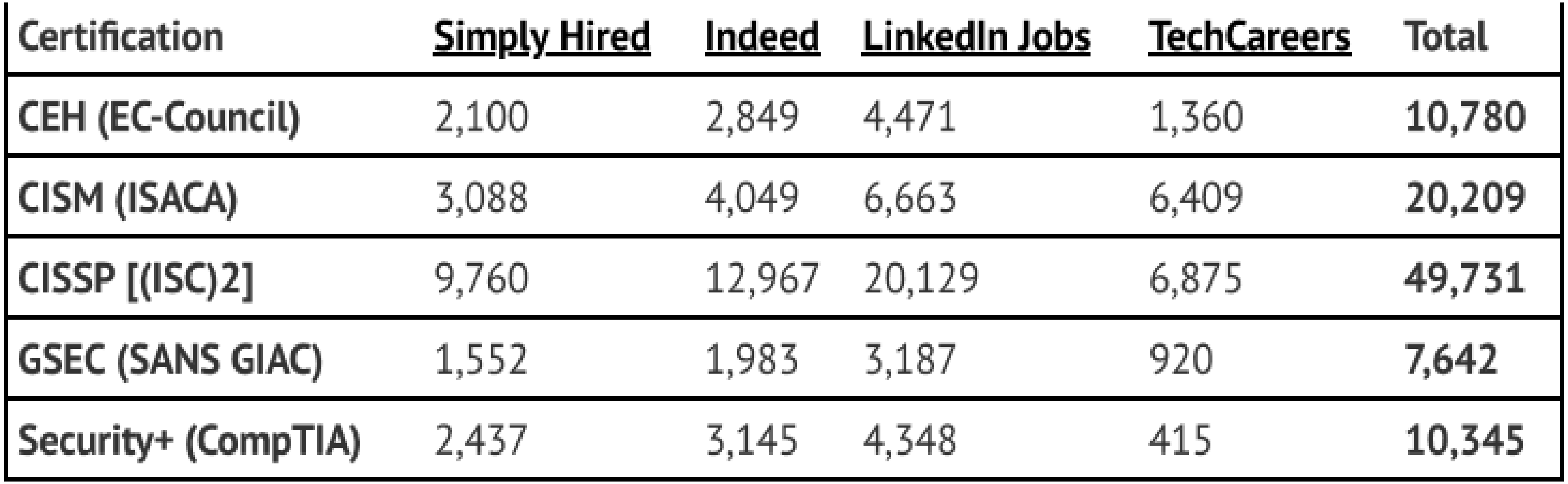
CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL CISSP® 132K

CISA® CERTIFIED INFORMATION SYSTEMS AUDITOR 115K

Certified Information Privacy Professional CIPP iapp >50K

CISM® CERTIFIED INFORMATION SECURITY MANAGER® 27K

PMI Project Management Professional >1M



Certification	Simply Hired	Indeed	LinkedIn Jobs	TechCareers	Total
CEH (EC-Council)	2,100	2,849	4,471	1,360	**10,780**
CISM (ISACA)	3,088	4,049	6,663	6,409	**20,209**
CISSP [(ISC)2]	9,760	12,967	20,129	6,875	**49,731**
GSEC (SANS GIAC)	1,552	1,983	3,187	920	**7,642**
Security+ (CompTIA)	2,437	3,145	4,348	415	**10,345**

Source: Business News Daily, 11/29/18 Best Information Security Certifications 2019

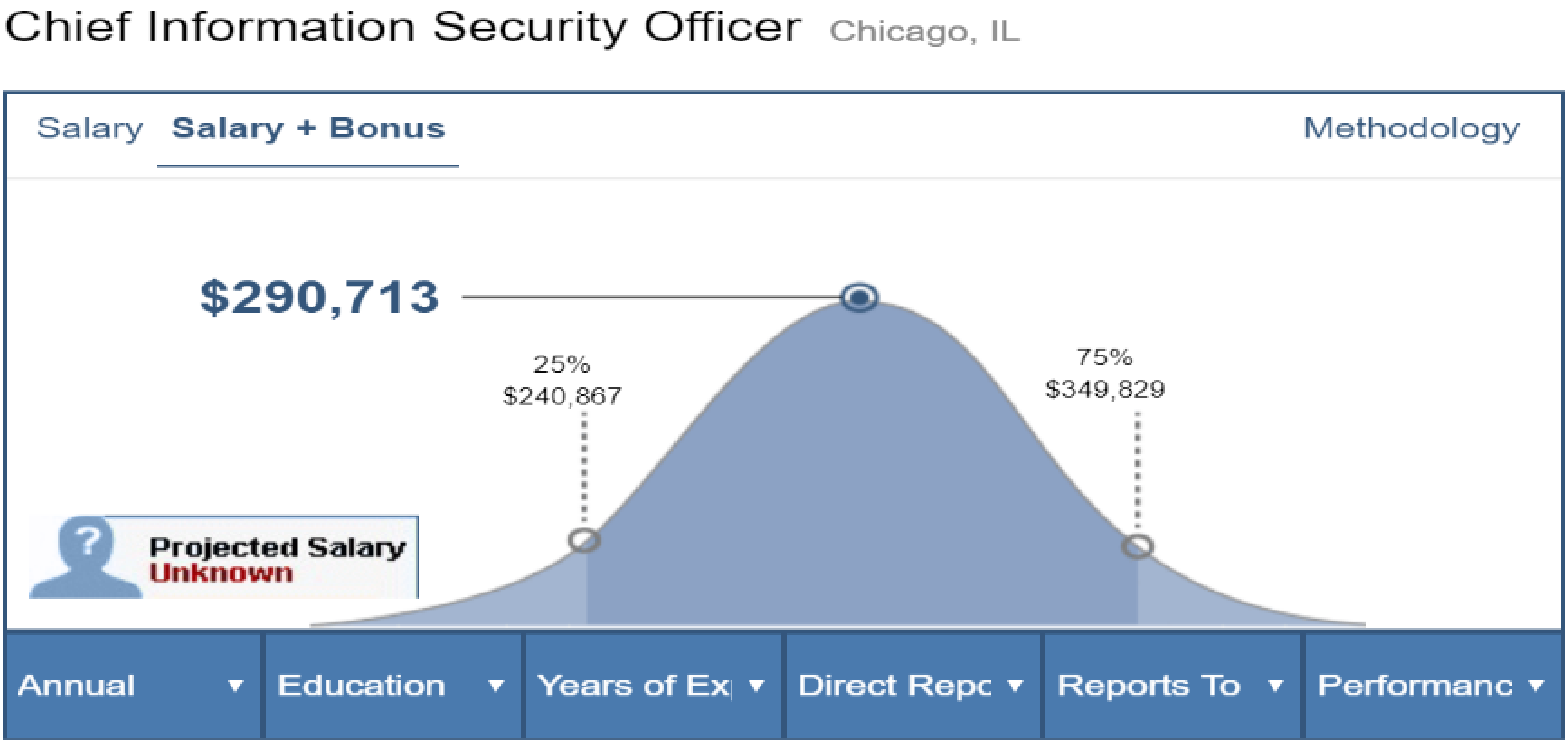
Top Paying Certifications

1. Google Certified Professional Cloud Architect - $139,529
2. **PMP® - Project Management Professional - $135,798**
3. Certified ScrumMaster® - $135,441
4. AWS Certified Solutions Architect - Associate - $132,840
5. AWS Certified Developer – Associate - $130,369
6. Microsoft Certified Solutions Expert (MCSE): Server Infrastructure - $121,288
7. ITIL® Foundation - $120,566
8. **CISM - Certified Information Security Manager - $118,412**
9. **CRISC - Certified in Risk and Information Systems Control - $117,395**
10. **CISSP - Certified Information Systems Security Professional - $116,900**
11. **CEH - Certified Ethical Hacker - $116,306**
12. Citrix Certified Associate - Virtualization (CCA-V) - $113,442
13. **CompTIA Security+ - $110,321**
14. CompTIA Network+ - $107,143
15. Cisco Certified Networking Professional (CCNP) Routing/Switching - $107K

CISSP MOST POPULAR

Source (July, 2019) https://www.globalknowledge.com/us-en/resources/resource-library/articles/top-paying-certifications/

Average CISO Salary+Bonus $290-350K (Large City Chicago, IL)



Chief Information Security Officer Chicago, IL

CISO SPOTLIGHT, LLC
Trusted Cybersecurity
and Privacy Training

Source: Salary.com, Chief Information Security Officer Job Title, 12/31/19

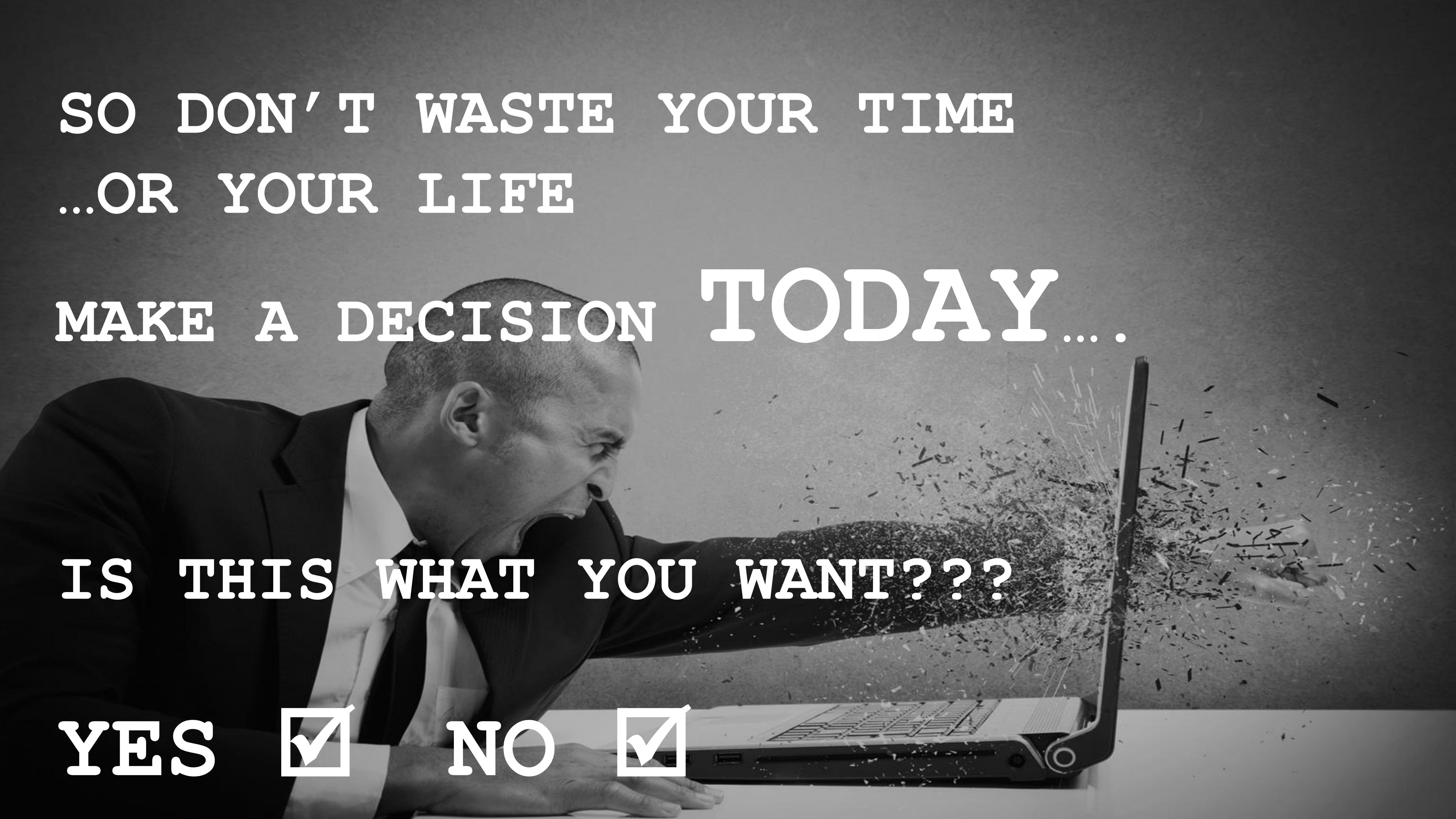
Choice of Money?

Happiness?

Both?

Today we Covered

1. The **Evolution** of the Cybersecurity Leader (CISO/VP/Dir/Mgr Information Security)
2. The **Skills** Required of this ~~guy~~ person
3. The Job **Opportunity**



SO DON'T WASTE YOUR TIME
…OR YOUR LIFE

MAKE A DECISION **TODAY**….

IS THIS WHAT YOU WANT???

YES ☑ NO ☑

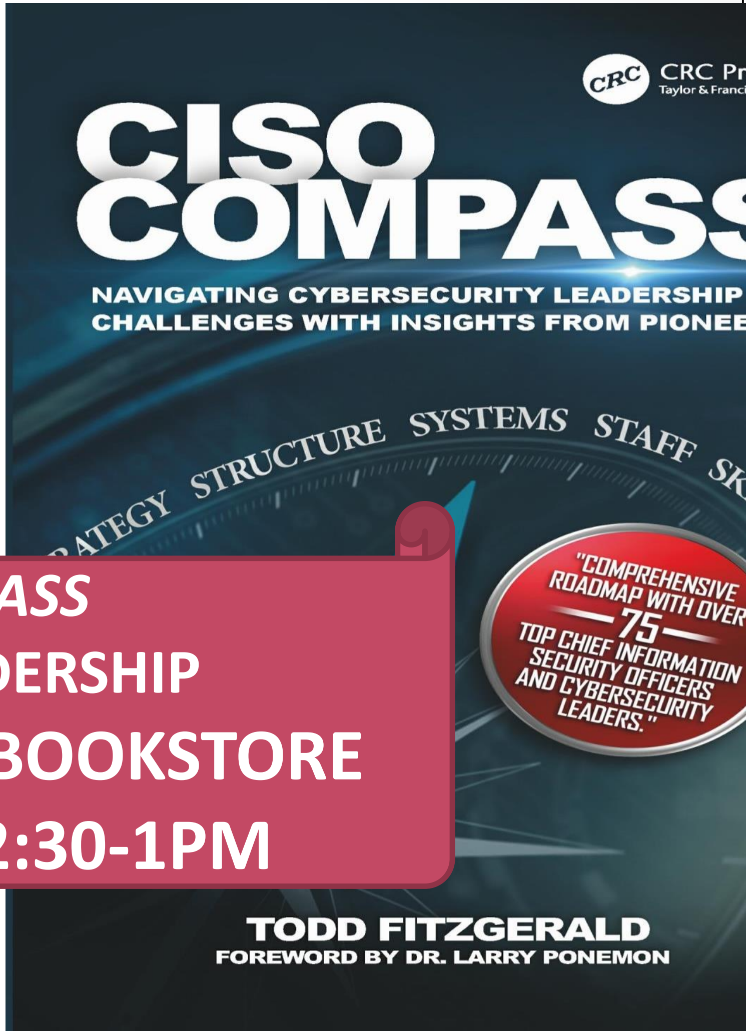
Additional Resources for the Journey… Thank You! Any Questions?

NEW *CISO COMPASS*

CYBERSECURITY LEADERSHIP

BOOK SIGNING IN RSA BOOKSTORE

THURSDAY FEB 27 12:30-1PM



CRC Press
Taylor & Francis Group

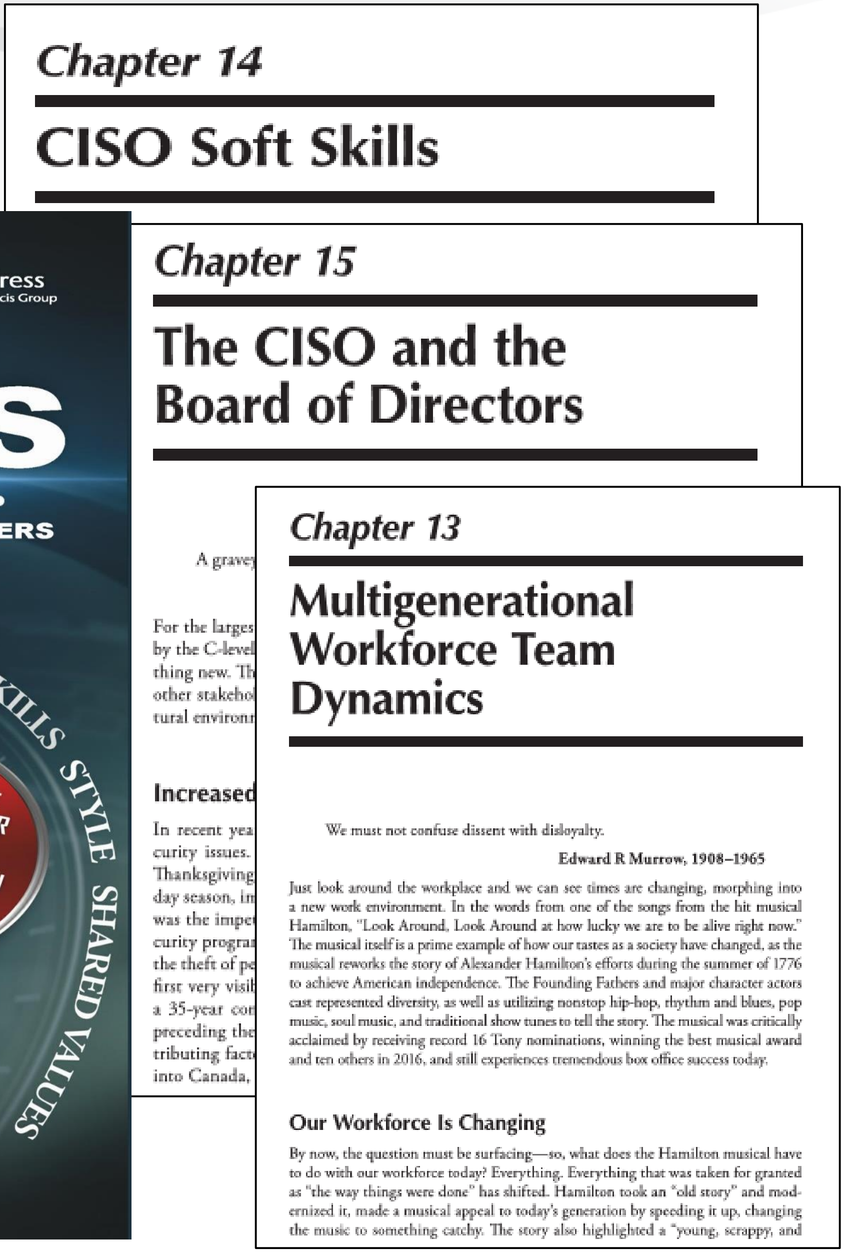
CISO COMPASS

NAVIGATING CYBERSECURITY LEADERSHIP CHALLENGES WITH INSIGHTS FROM PIONEERS

STRATEGY STRUCTURE SYSTEMS STAFF SKILLS STYLE SHARED VALUES
"COMPREHENSIVE ROADMAP WITH OVER —75— TOP CHIEF INFORMATION SECURITY OFFICERS AND CYBERSECURITY LEADERS."

TODD FITZGERALD

FOREWORD BY DR. LARRY PONEMON



Chapter 14

CISO Soft Skills

Chapter 15

The CISO and the Board of Directors

A gravey

For the larges by the C-level thing new. Th other stakehol tural environm

Increased

In recent yea curity issues. Thanksgiving day season, im was the impet curity progra the theft of pe first very visib a 35-year con preceding the tributing fact into Canada,

Chapter 13

Multigenerational Workforce Team Dynamics

We must not confuse dissent with disloyalty.

Edward R Murrow, 1908–1965

Just look around the workplace and we can see times are changing, morphing into a new work environment. In the words from one of the songs from the hit musical Hamilton, "Look Around, Look Around at how lucky we are to be alive right now." The musical itself is a prime example of how our tastes as a society have changed, as the musical reworks the story of Alexander Hamilton's efforts during the summer of 1776 to achieve American independence. The Founding Fathers and major character actors cast represented diversity, as well as utilizing nonstop hip-hop, rhythm and blues, pop music, soul music, and traditional show tunes to tell the story. The musical was critically acclaimed by receiving record 16 Tony nominations, winning the best musical award and ten others in 2016, and still experiences tremendous box office success today.

Our Workforce Is Changing

By now, the question must be surfacing—so, what does the Hamilton musical have to do with our workforce today? Everything. Everything that was taken for granted as "the way things were done" has shifted. Hamilton took an "old story" and modernized it, made a musical appeal to today's generation by speeding it up, changing the music to something catchy. The story also highlighted a "young, scrappy, and

CISO SPOTLIGHT, LLC

Trusted Cybersecurity and Privacy Training