RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PROF-T09**

Making The Leap: Transform from Techie to CISO/Infosec Leader, Should You?

Todd Fitzgerald

CISO, Cybersecurity Leadership Author, CISO SPOTLIGHT, LLC
VP Cybersecurity Strategy, Cybersecurity Collaborative
@Securityfitz www.amazon.com/author/toddfitzgerald

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Several videos in this presentation are from personal collection of the late Eugene Schultz with permission, an unforgettable information security pioneer and frequent RSA presenter.

Todd Fitzgerald, CISO, Cybersecurity Leadership Author

Global Security Leadership Roles

Northwestern McCORMICK SCHOOL OF ENGINEERING — Adjunct Faculty

CYBERSECURITY COLLABORATIVE — VP, Cybersecurity Strategy

NORTHERN TRUST — SVP, CAO, Infosec and Tech Risk

Grant Thornton — Global CISO

ManpowerGroup

Anthem / National Government Services — Global CISO

Medicare SSO/External Audit Oversight

ZENECA syngenta

Prior IT Leadership Roles

imshealth NOW IQVIA — North and Latin America CISO

American Airlines

BlueCross BlueShield

CISO SPOTLIGHT, LLC
Trusted Cybersecurity and Privacy Training

Author Roles

2019,2020,2021 #1 BEST SELLER - Taylor & Francis (Publisher)

2020 CANON Cybersecurity Hall of Fame Inductee

Leadership Books Contributor to:

- ISC2 CISSP
- ISACA COBIT 5
- ISACA CSX
- E-C Council CCISO
- Dozen Other Books

Podcast

RSAConference2022

Today We Will Cover:

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

HOW CAN WE BE SURE

OF WHICH 

TO TAKE?

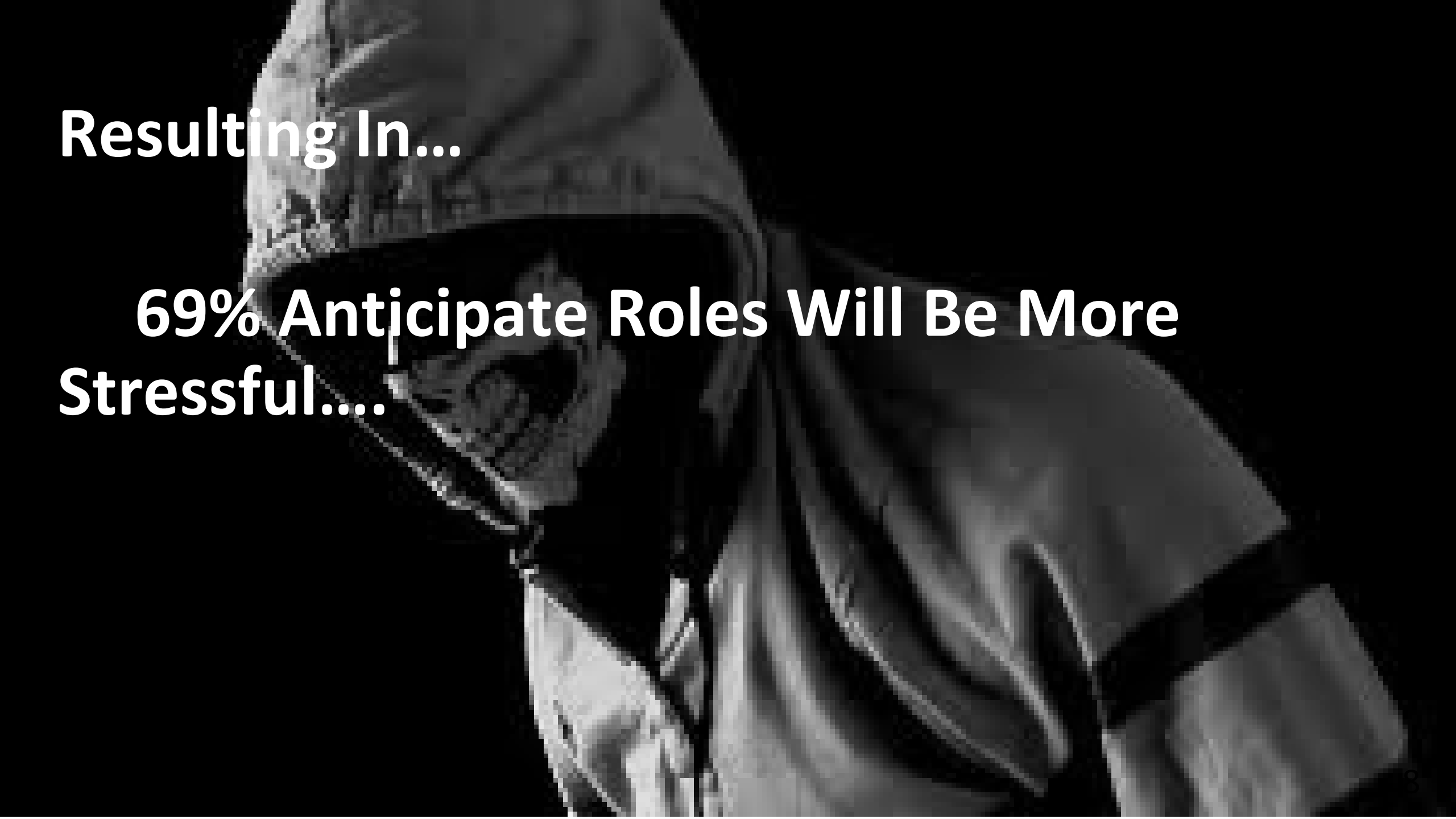
RSAConference2022

The Evolution of the Security Leader (CISO or Individual Leading Significant Security Aspects)

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

- Ponemon Institute

” Source: Ponemon Institute, “What CISOs Worry About in 2018



Resulting In…

69% Anticipate Roles Will Be More Stressful….

63% Believe Information Security Budgets to Decline or Remain Flat…

45% Even Fear Job Loss in the Event of A…

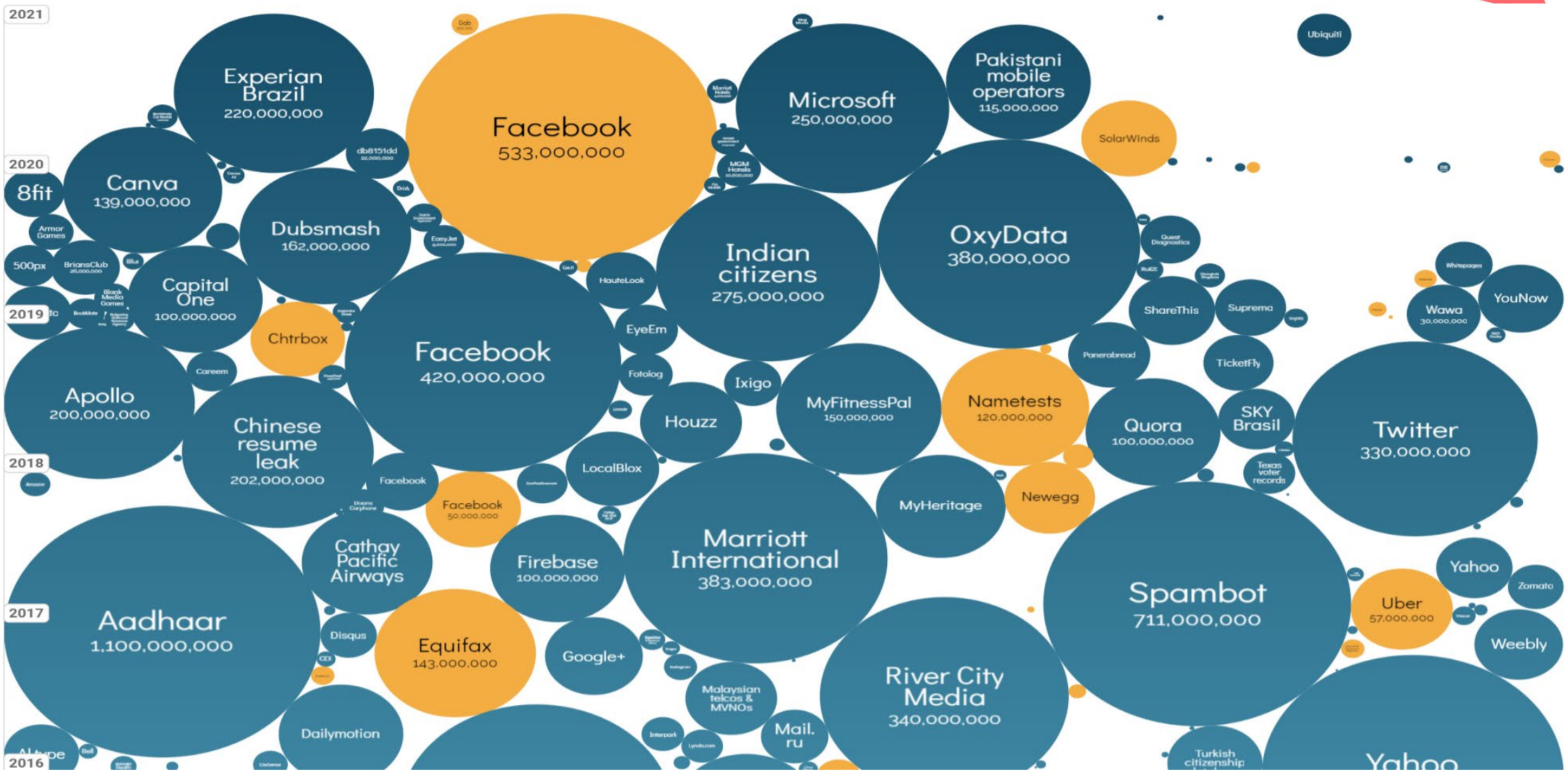
DATA BREACH

DATA BREACH

DATA BREACH

11.7 B Records Breached Since 2005

AND THAT INCLUDES JUST THE *REPORTED* ONES…



Source: Informationisbeautiful.com

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)

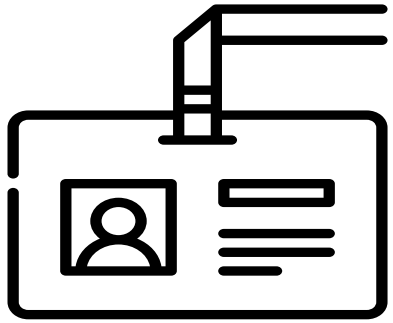
Where Do CISOs Come From ?

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)

THE FIRST SECURITY LEADERS….

THE FIRST SECURITY LEADERS….

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

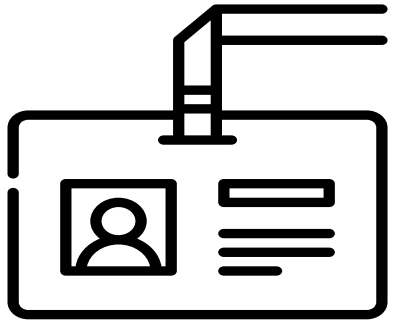
4 Threat-Aware Cybersecurity, Socially-Mobile-Cloud CISO

2008-2016

5 The Privacy and Data-Aware CISO

2016-2020's

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

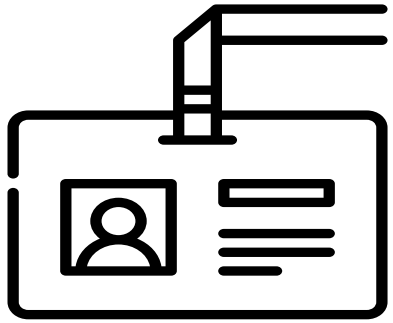
4 Threat-Aware Cybersecurity, Socially-Mobile-Cloud CISO

2008-2016

5 The Privacy and Data-Aware CISO

2016-2020's

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

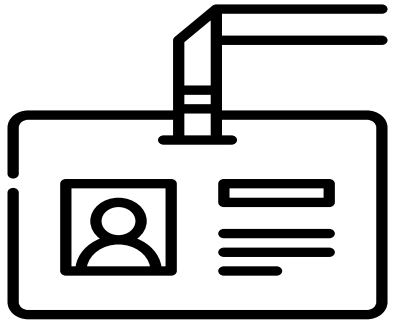
4 Threat-Aware Cybersecurity, Socially-Mobile-Cloud CISO

2008-2016

5 The Privacy and Data-Aware CISO

2016-2020's

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

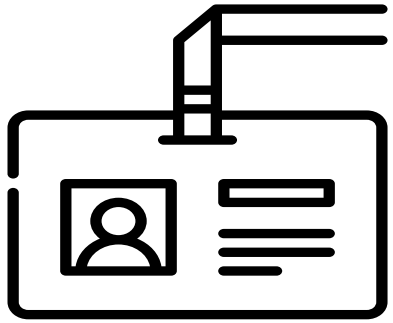
4 Threat-Aware Cybersecurity, Socially-Mobile-Cloud CISO

2008-2016

5 The Privacy and Data-Aware CISO

2016-2020's

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

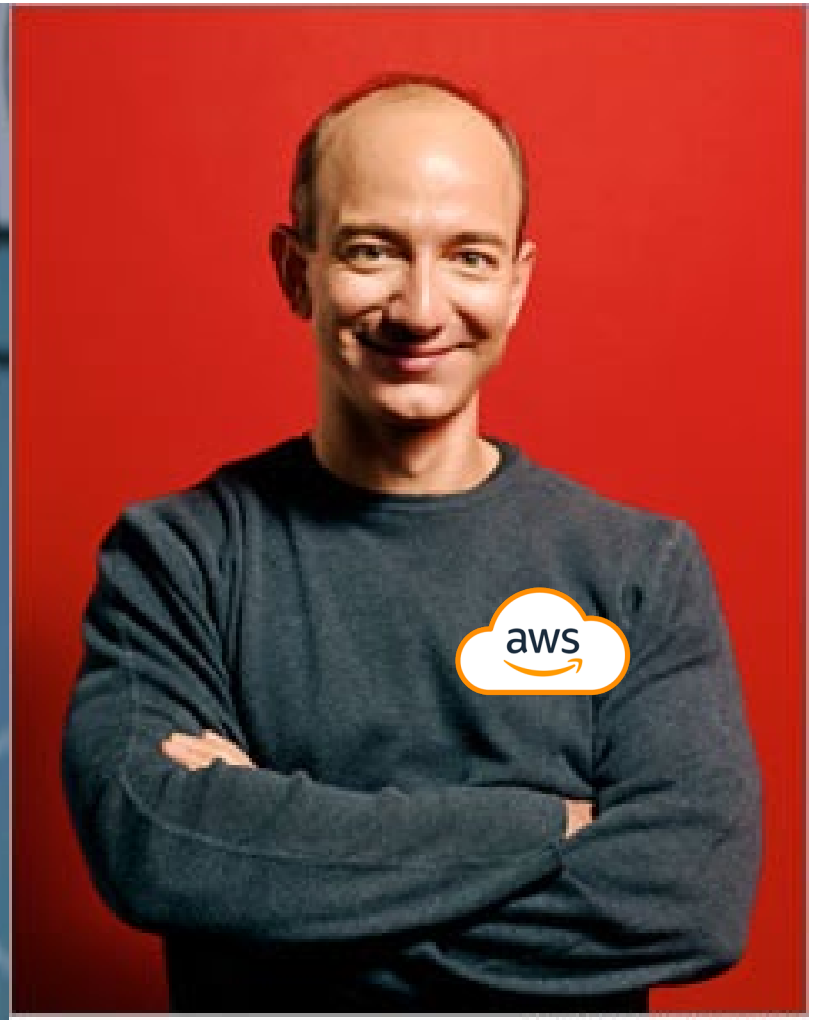
2004-2008

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

2008-2016

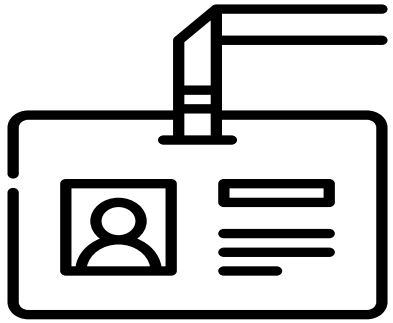
5 The Privacy and Data-Aware CISO

2016-2020's



COURTESY: AMAZON

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

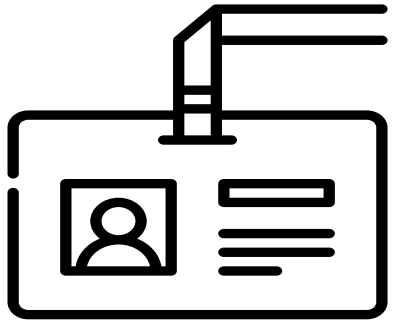
4 Threat-Aware Cybersecurity, Socially-Mobile-Cloud CISO

2008-2016

5 The Privacy and Data-Aware CISO

2016-2020's

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

Evolution of Security Leadership 1995-2020's

Dimension	Pre-2000	2000-2003	2004-2008	2008-2016 & 2016-2020's*
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

RSAConference2022

The Security Leader Skills

Resulting In …

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

- Job Posting Fortune Global 500 Company

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

Decision Point: Critical Differences in Thought Processes

TECHNICAL

- Technical Challenge
- Concrete, non-ambiguous solutions
- Task-Oriented
- Mastery of Technical Skill
- Hands-on Training Focus
- Documentation Aversion
- High Level of Individual Contribution
- Meetings are Distractions

Managerial Competencies Are Different

MANAGERIAL

- Embracing Ambiguity and Uncertainty
- Meetings, meetings and more meetings!
- Oral Communication At Various Levels
- Business Relationships
- People-Oriented/Conflict Resolution
- Consensus Building
- Many Presentations
- Influence
- Team Building

Skills: Leadership Skills Paramount for Today's CISO

- Plan a path away from operations
- Refine risk management processes to business language
- Widen vision to privacy, data management and compliance
- Build a support network for insights
- Leverage new business skills to create focus and attention of business leaders

Source: Forrester Research (Projection to 2018 CISO)

GARTNER : 6 STEPS A CISO CAN TAKE

1. Develop an **executive narrative** to reset perspectives on risk and cybersecurity
2. Formalize the **risk and security program**
3. Establish the risk and **security business service portfolio and catalog** and validate with the rest of the business
4. Determine **standard costs** for the risk and security business services
5. Enable the business units to choose **service levels** based on the cost-benefit and desire level of risk
6. Manage risk and security budget as a service of the selected service level and use chargeback or show back to **link to the budget to the business benefit**

Source: https://www.gartner.com/en/conferences/emea/security-risk-management-germany/featured-topics/leadership-and-strategy

… Remember the CISO Qualifications?

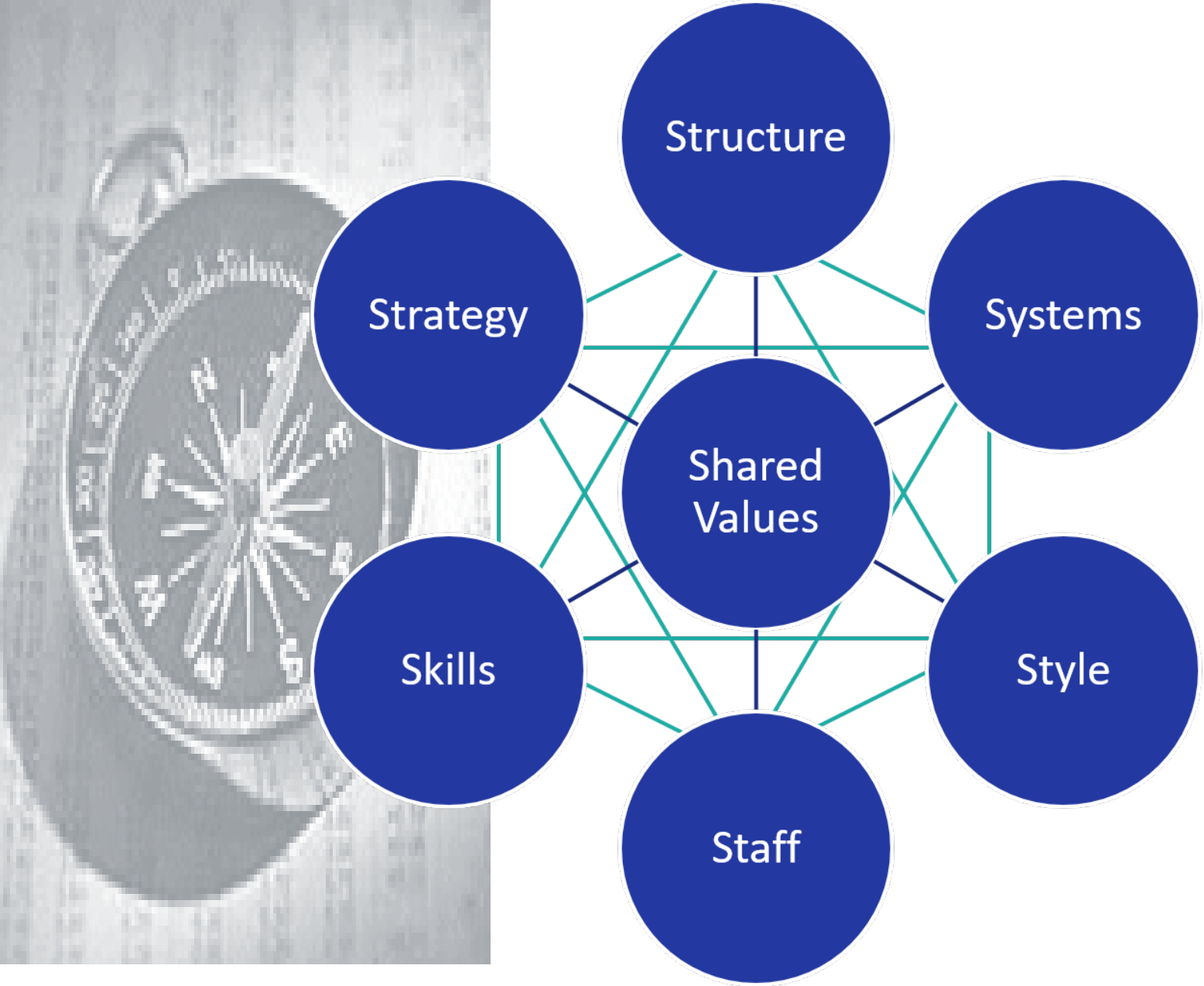
- Qualifications Bachelor's degree in a related field (Computer Science or related field).
- Advanced degree preferred.
- • 10-15 years of progressive IT Security experience, including cybersecurity and risk management, within a large corporate environment with at least 5 years in a management role• 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)

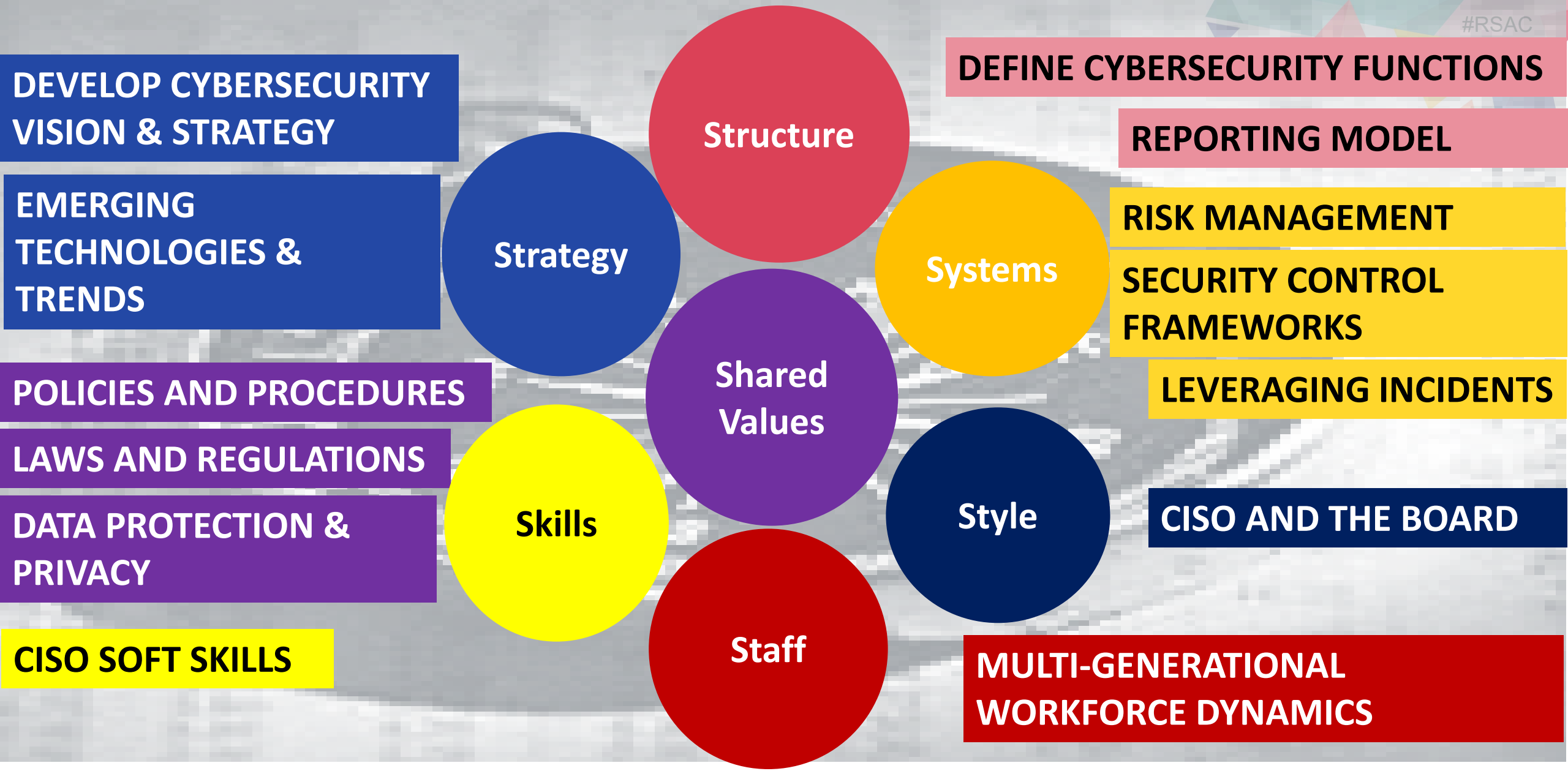
… Remember the CISO Qualifications?

- 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)



Our Ability To Implement Cybersecurity Strategy Is Impacted By 7 Key Factors



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

2019 LEADING ORGANIZATION 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

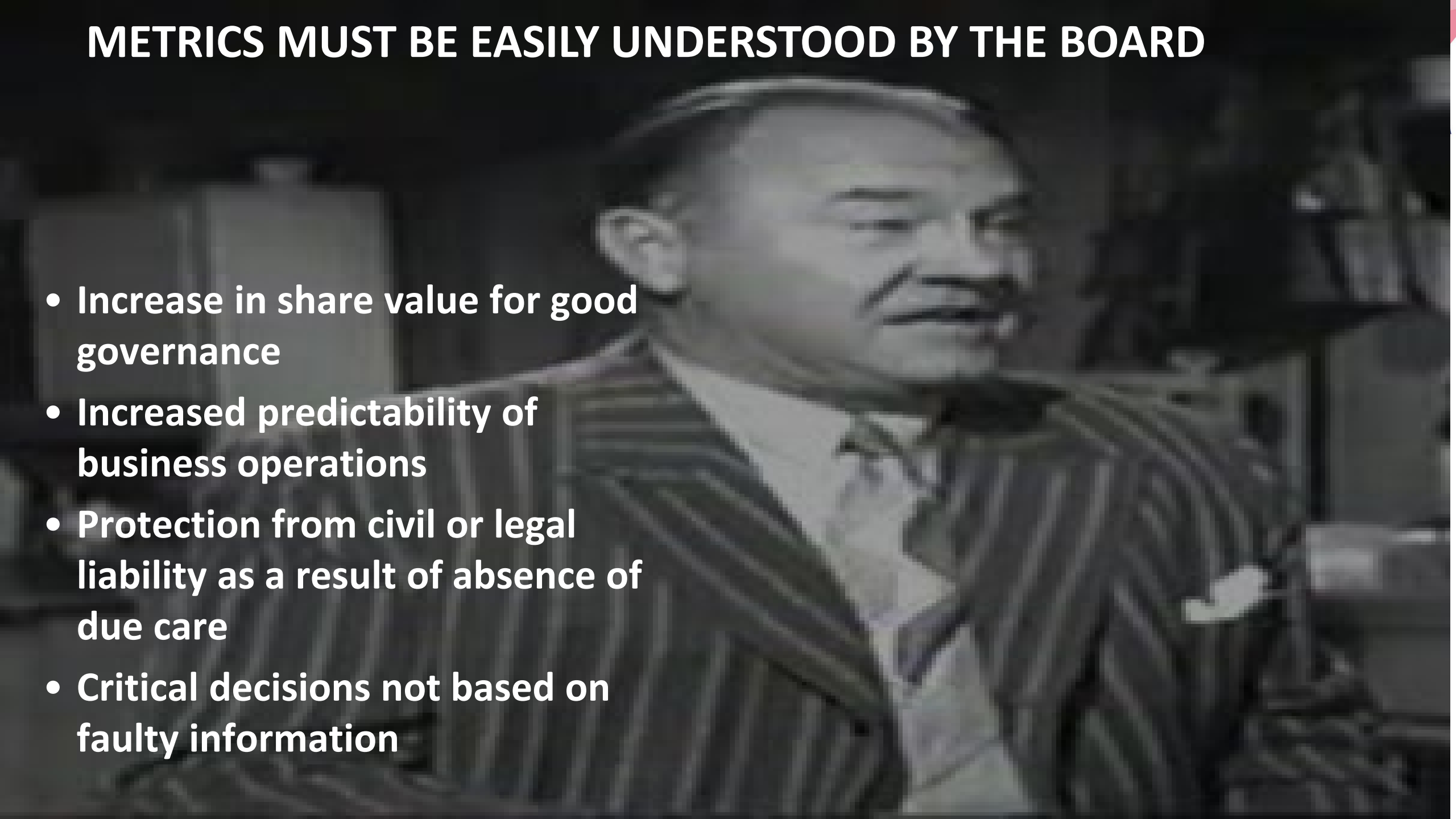
Policy/Controls

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

And While Changing, Most CISOs Still Report To …

Source: 2021 Global Chief Information Security Officer (CISO) Survey, Heidrick & Struggles
Source: CISO's Today: The good. bad and the ugly, CISO Summit, Larry Ponemon, 2013
Governance of Cybersecurity: 2015 Report, How Boards and Senior Executives are Managing Cyber Risks, Georgia Tech Information Security Center
CISO salary and job description- What's the role of the CISO, who should the CISO report to and how much does a CISO get paid?, 1/17/18 CIO UK

METRICS MUST BE EASILY UNDERSTOOD BY THE BOARD



- Increase in share value for good governance
- Increased predictability of business operations
- Protection from civil or legal liability as a result of absence of due care
- Critical decisions not based on faulty information

BOARD-LEVEL SKILLS THE CISO MUST HAVE TO *KEEP* THE POSITION

1. Use Analogies to explain complicated concepts
2. Understand the business goal-why is the CISO in the room?
3. Are we secure? Peers-Trends-Gaps-how to
4. Enterprise-wide risk management
5. How are you managing risk? Framework?
6. How is risk being mitigate
7. Risk posture most importa
8. Compliance maturity, inci
9. Must be 'business relevan
why', avoid security jargon
10. Credibility-share good ne
11. Share a story, don't drown them in metri
possible (have available if asked)
12. Compare with peers, industry, maturity s
13. Share incidents
14. Talk $$$ - budgets, cost of downtime
15.Efficiency – managing costs down
16. Effectiveness – oriented towards new business ops, new trends,

is viewed by the rest of the organization, be
business value

l and works up one level

he board

fenses (control oversight,

rnance

nvite regulators, government bodies, peers to

ress with a simple framework, deviation from

25. Explain the 'ideal' maturity level – risk appetite= difference from perfection and reality

26. What are the top 5 risks related to cybersecurity?

27. What are the actions in place to address these risks?

28. Are internal and external threats being examined?

29. Is the risk assessment holistic? Does it include vendors, suppliers– if not, could be 'willful neglect'

30. Carve program into security processes vs technology – such as threat management, incident response, vulnerability and patch management, security operations, security architecture, and risk management

31. Discuss how we would respond to an incident to educate the board that anyone could be vulnerable

32. 49% reporting on vulnerabilities to board, followed by 25% on incident response

33. Many CISOs grasp for topics to connect with the boards!!!

34. Do we think the board cares about lost laptops and website blocking?

35. Transparency on security risks new innovations carry

36. Prioritize assets, create common risk appetite with board to fuel business growth and innovation.

37. Implement security reporting discipline and engagement between CISO and board

38. Crowded board agenda, invisible payoff vs shareholder deliverables

39. "Not our problem" outside of military and financial services

40. Overinvested in wrong priorities (preventative controls vs detect/response)

41. Risk Posture – Not tactics, security architecture, operational issues

42. Be ready for questions – board expects you as the expert to know the answers

43. Listen to their reactions- highlight next time

Source: Research by T. Fitzgerald, First presented at COSAC, Naas, Ireland, *Are we boring the board*, October, 2017)

CISO SPOTLIGHT, LLC
Trusted Cybersecurity and Privacy Training

1. Use Analogies to explain complicated concepts

2. Understand the business goal-why is the CISO in the room?

3. Are we secure? Peers-Trends-Gaps-how to fill

4. Enterprise-wide risk management

5. How are you managing risk? Framework?

6. How is risk being mitigated, a

7. Risk posture most important

8. Compliance maturity, incider

9. Must be 'business relevant', talk about 'who would target us and why', avoid security jargon

10. Credibility-share good news and bad and what you don't know

11. Share a story, don't drown them in metrics, talk in $$$ where possible (have available if asked)

12. Compare with peers, industry, maturity status, risks

13. Share incidents

14. Talk $$$ - budgets, cost of downtime

15.Efficiency – managing costs down

16. Effectiveness – oriented towards new business ops, new trends, threats, technology

17. Determine how security is viewed by the rest of the organization, be relentless in demonstrating business value

rd level and works up one level

g to the board

s of defenses (control oversight,

21. Position board with their responsibility

22. Communicates clear organizational governance

23. Communicate trends – invite regulators, government bodies, peers to present at add credibility

24. Communicate plan progress with a simple framework, deviation from industry standards

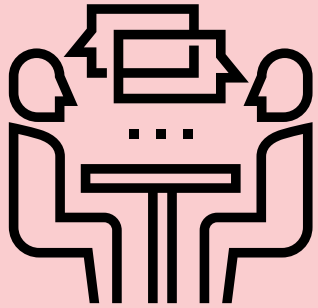
25. Explain the 'ideal' maturity level – risk appetite= difference from perfection and reality

ALWAYS SHOW VALUE

RSAConference2022

The Opportunity

Challenge Conventional Thinking Where CISOs Come From

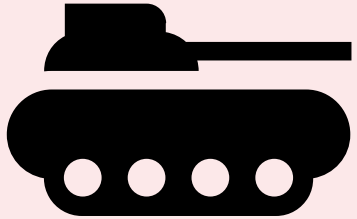


CONSULTING

- ❑ <1 in 1000 Big Four security consultants become CISOs

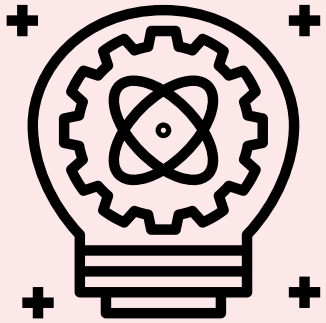
LAW ENFORCEMENT

- ❑ < 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

What Degrees Do Fortune 500 CISOs Prefer ?

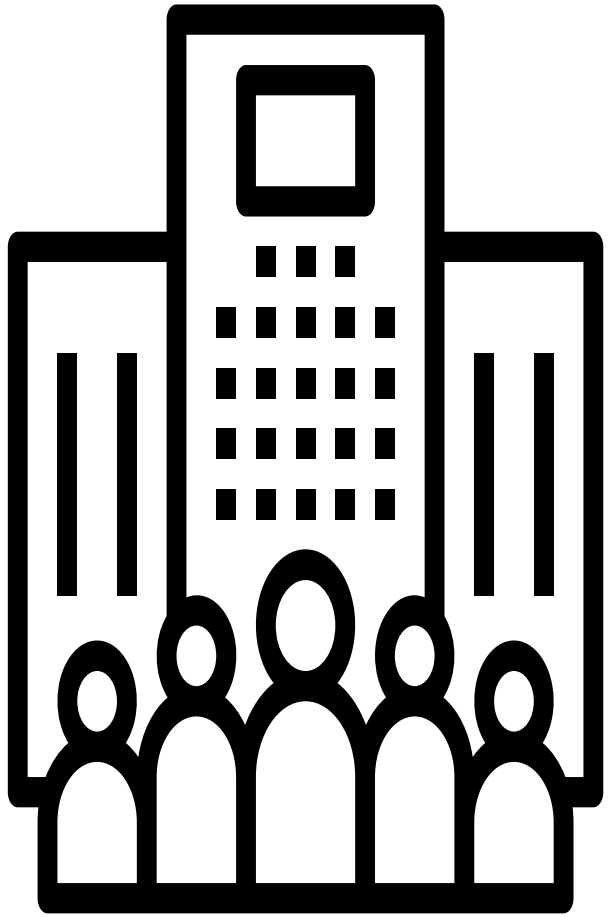
UNDERGRADUATE	GRADUATE
Computer Science 18.4%	MBA 44.8%
Business 9.2%	Computer Science 7.7%
Management Information Systems 8.9%	Management Information Systems 5.0%

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

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

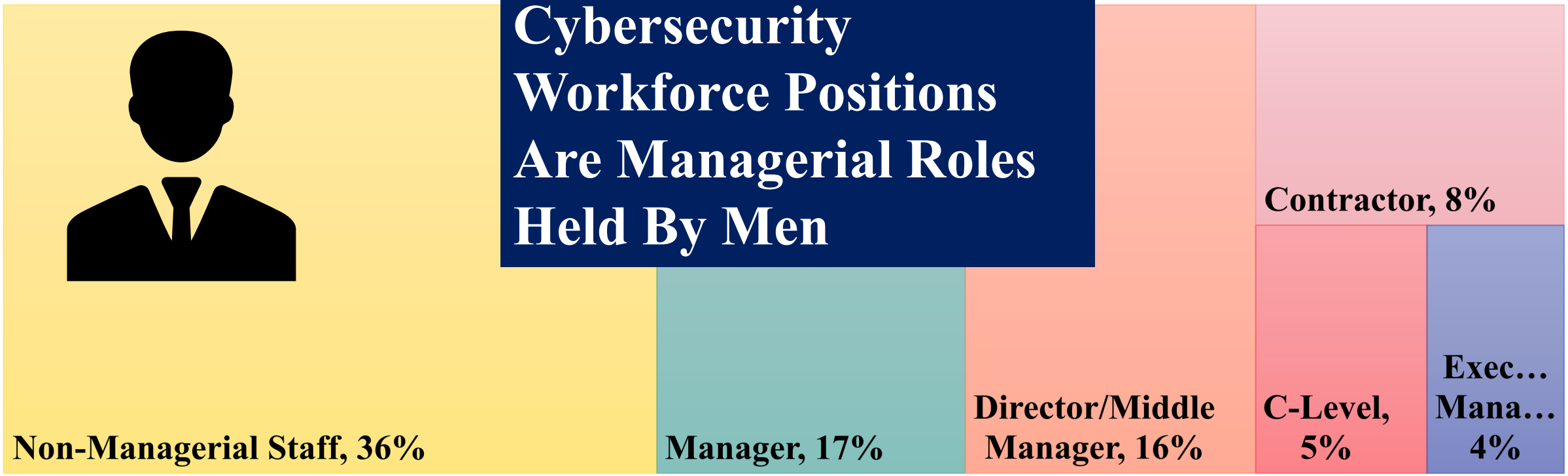
Source: ISACA SheLeadsTech Panel, Dublin, Ireland 2018, www.dogpatchlabs.com

Women Comprise 14% of North America Cybersecurity Workforce

- Non-Managerial Staff, 6%
- Manager, 3%
- Director/Middle Manager, 2%
- C-Level, 1%
- Executive Management, 1%
- Contractor, 1%

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)

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)

“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

132,000

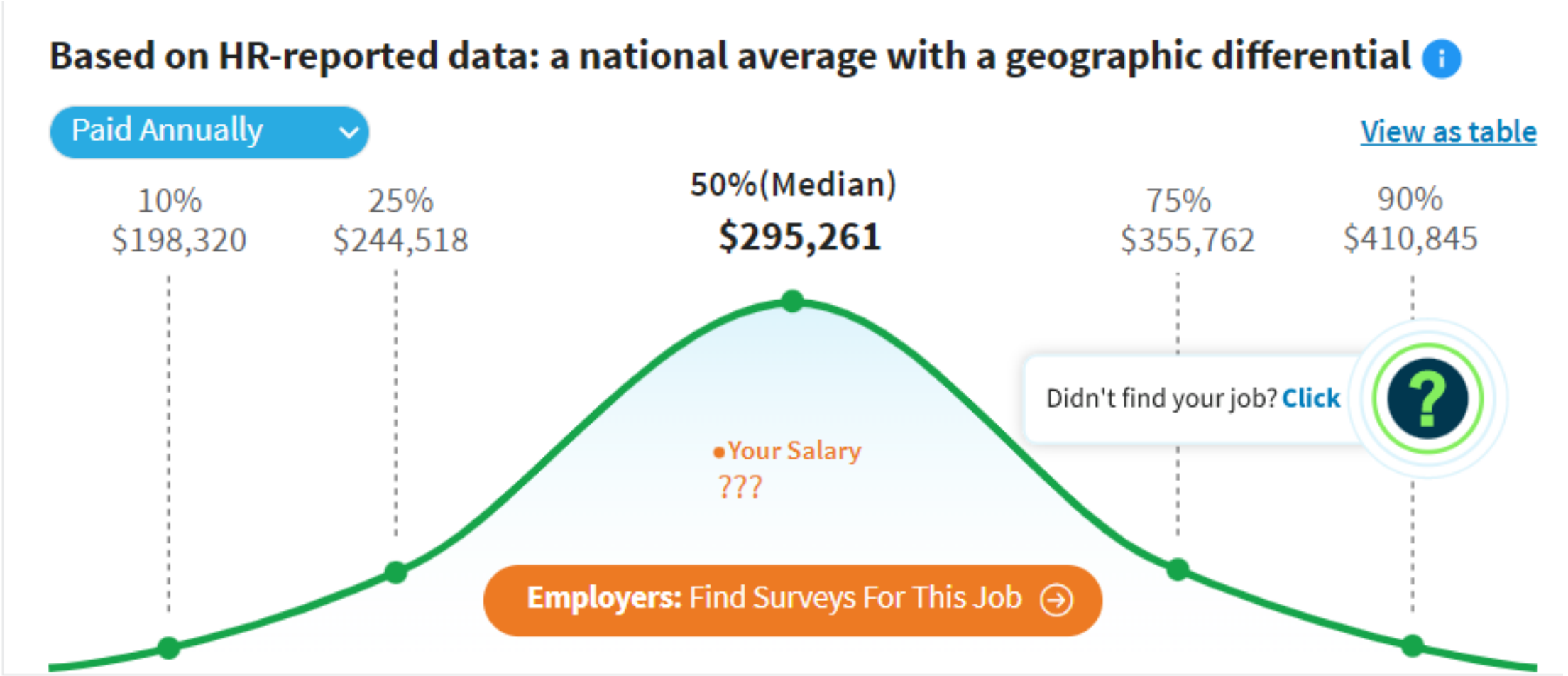
> 50,000

115,000

27,000

> 1M

Average CISO Salary+Bonus 50-90% Percentile $295-411K (Large City Chicago, IL)



Source: Salary.com, Chief Information Security Officer Job Title, Q1-2022

CISO "Risky Business" Pitfalls To Watch

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

Choice of Money?

Happiness?

Both?

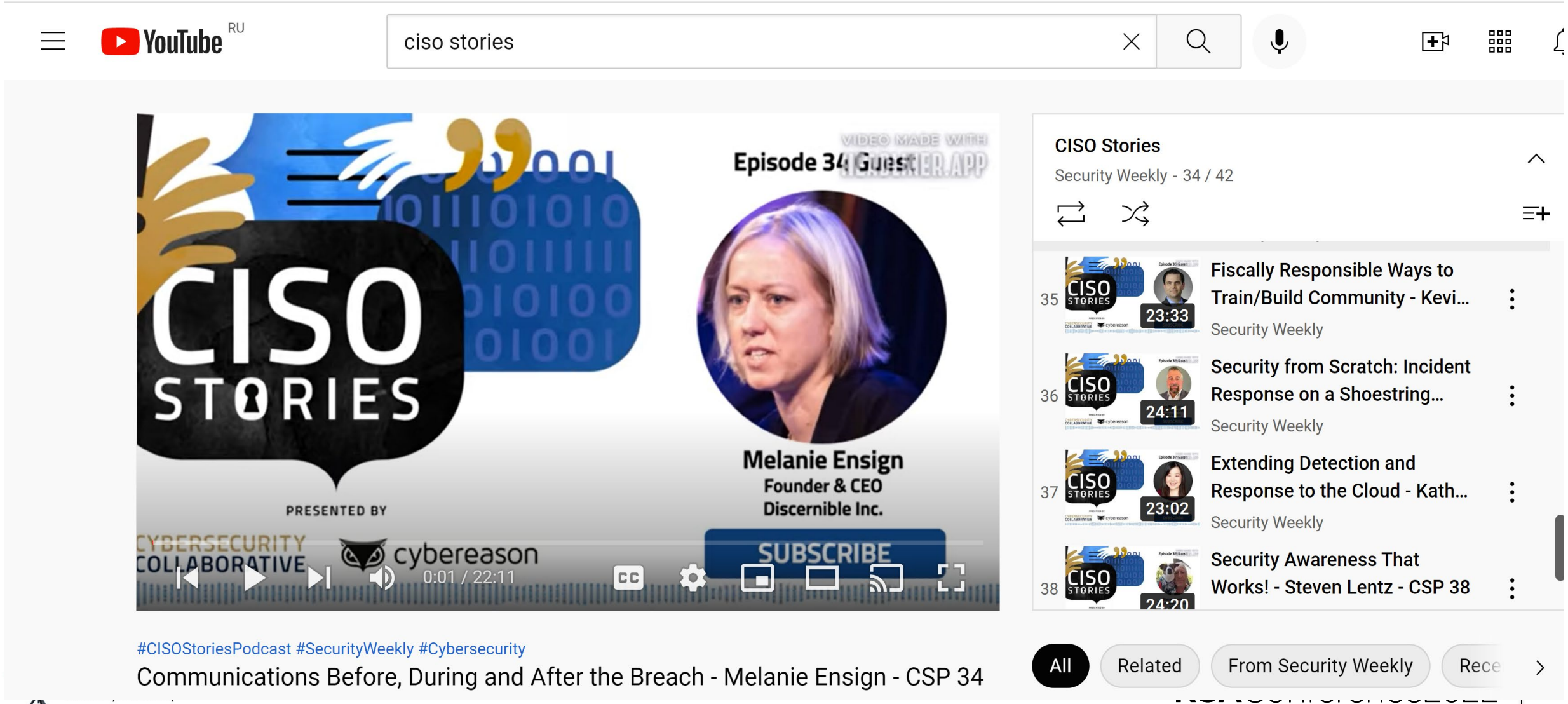
RSAConference2022

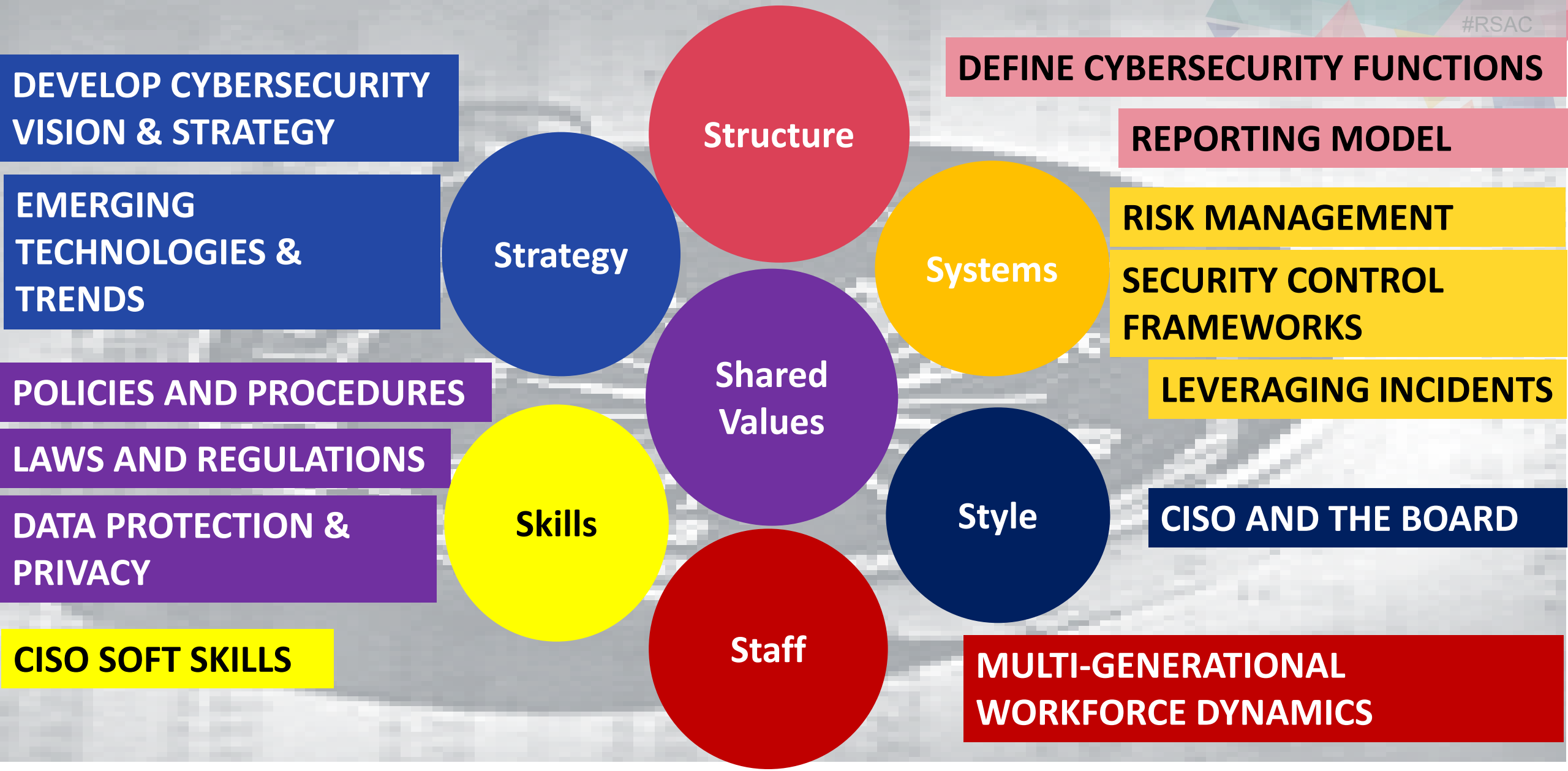
Today we Covered

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

Additional Resources – Listen To Other CISOs Problems! (CISO STORIES WEEKLY PODCAST)

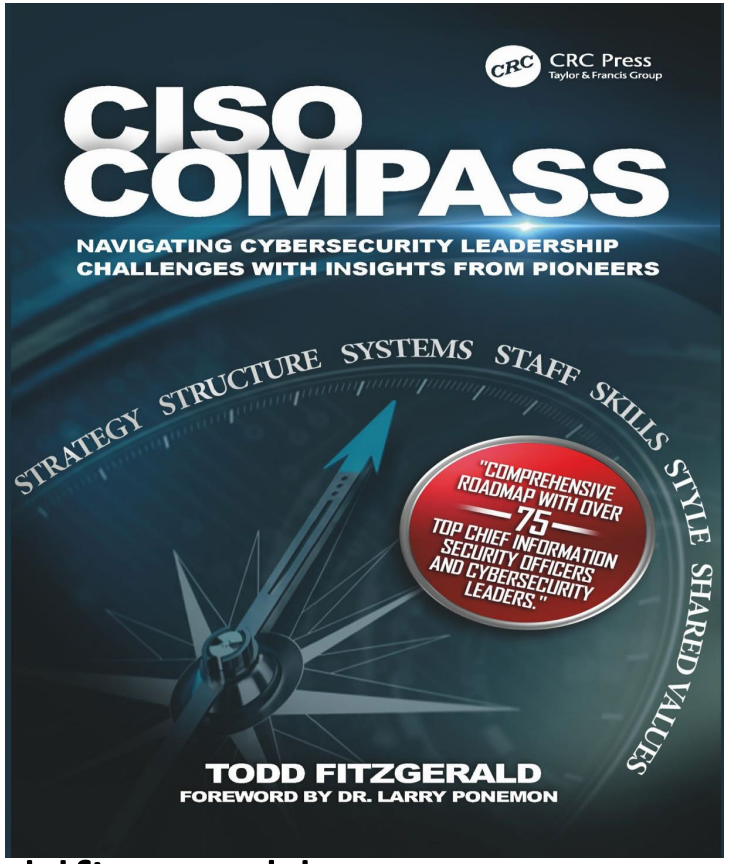
Apple, Spotify, Google play, Twitch, YouTube, securityweekly.com, etc.

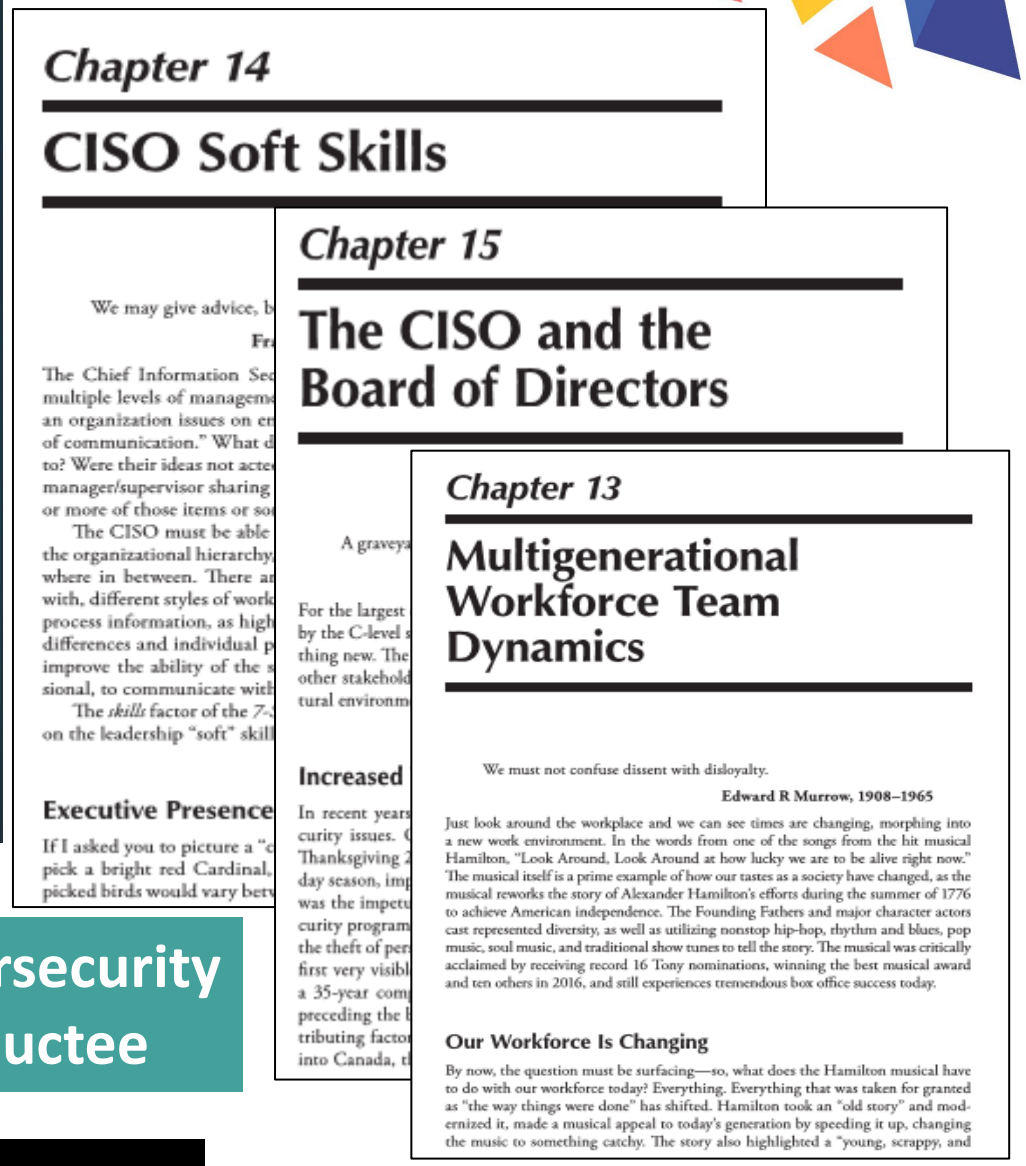




Source: T. Fitzgerald, *CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers* (2019, Auerbach Publications)

Additional Resources for the Journey…





www.amazon.com/author/toddfitzgerald

2019,2020, 2021 #1 BEST SELLER
- Taylor & Francis (Publisher)

2020 CANON Cybersecurity Hall of Fame Inductee

CISO SPOTLIGHT, LLC
Trusted Cybersecurity and Privacy Training

BOOK SIGNING IN RSA BOOKSTORE

Final Thoughts

- Both technical and leadership security jobs will be in demand
- Be honest with yourself and get EXCITED!!!
- Explore lateral/broad security experiences (technical)
- Immerse yourself in leadership literature (managerial/leadership)
- Build social networks and learn from each other
- Nothing is permanent, Nothing is wasted

Apply What You Have Learned Today

- Next week you should:
  - Review these slides again, ask yourself, “what activities do I like most?”
- In the first three months following this presentation you should:
  - Identify skills gap for techie or CISO career path
  - Talk with at least 1-2 senior security professionals and 1-2 CISO/Senior Leaders about their jobs
- Within six months you should:
  - Study and schedule additional certification
  - Develop a 2-3 year plan to obtain additional experiences

RSAConference2022

Thanks for Your Time!!

Any Questions?

www.amazon.com/author/toddfitzgerald

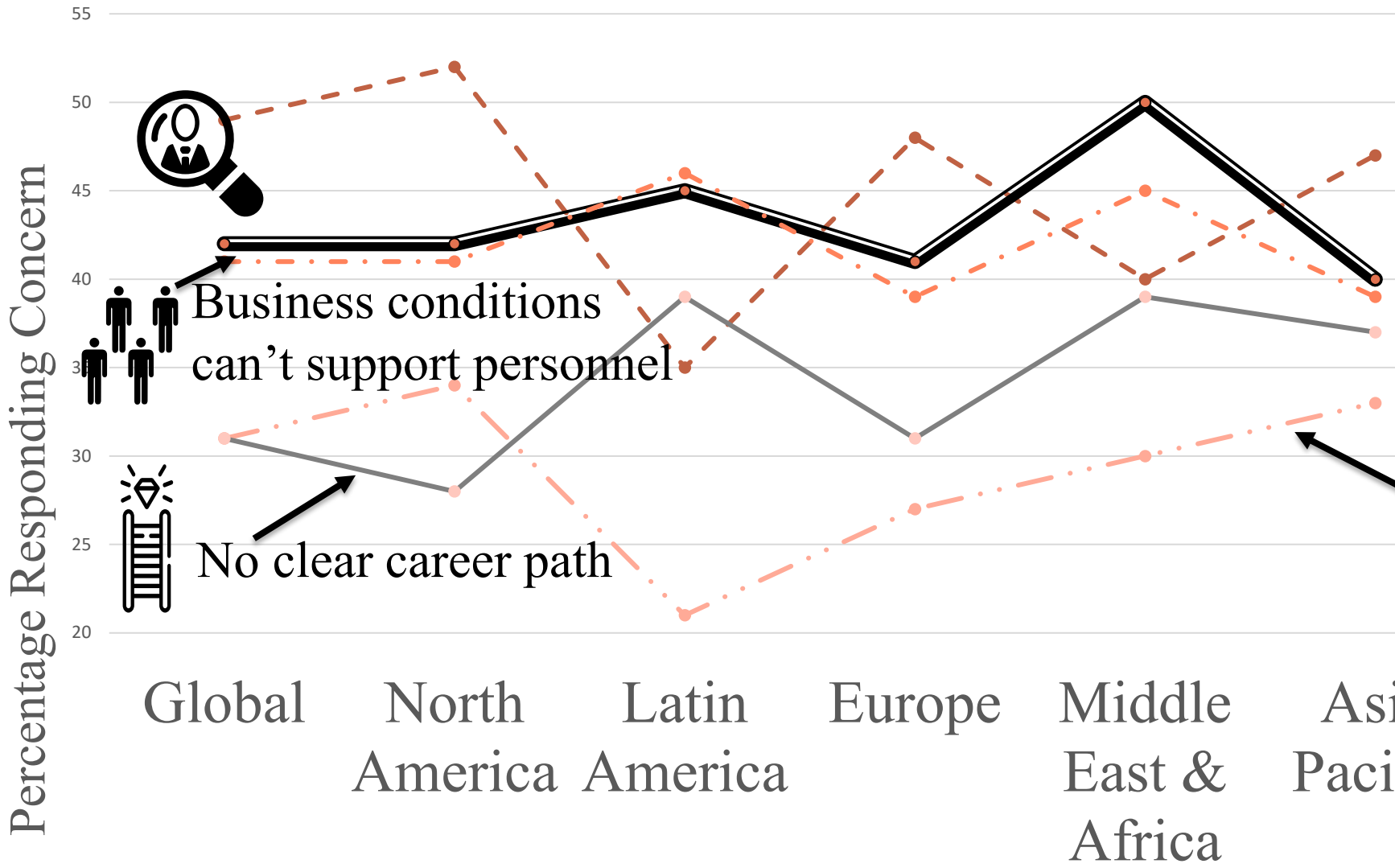
CISO SPOTLIGHT, LLC
Trusted Cybersecurity and Privacy Training

CYBERSECURITY COLLABORATIVE

RSAConference2022

Additional Reference Material

Qualified Personnel Are Difficult To Find



Requirements not understood by leadership

Workers hard to retain

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 13.1,* (2019, Auerbach Publications)

Popularity of Certifications Varies

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: https://www.globalknowledge.com/us-en/resources/resource-library/articles/top-paying-certifications/

SIGNIFICANT JUMP TO 2020 SALARIES WORLDWIDE

1. Google Certified Professional Cloud Architect — $175,761
2. AWS Certified Solutions Architect – Associate — $149,446
3. CISM – Certified Information Security Manager — $148,622
4. CRISC – Certified in Risk and Information Systems Control — $146,480
5. PMP® – Project Management Professional — $143,493
6. CISSP – Certified Information Systems Security Professional — $141,452
7. CISA – Certified Information Systems Auditor — $132,278
8. AWS Certified Cloud Practitioner — $131,465
9. VCP6-DCV: VMware Certified Professional 6 – Data Center Virtualization — $130,226
10. ITIL® Foundation — $129,402
11. Microsoft Certified: Azure Fundamentals — $126,653
12. Microsoft Certified: Azure Administrator Associate — $125,993
13. CCA-N: Citrix Certified Associate – Networking — $125,264
14. CCNP Routing and Switching — $119,178
15. CCP-V: Citrix Certified Professional – Virtualization — $117,069

CISM HIGHEST PAID SECURITY CERT

Source: https://www.globalknowledge.com/us-en/resources/resource-library/articles/top-paying-certifications/

STILL CLIMBING IN 2021 (RELEASED AUG 17, 2021)

CRISC HIGHEST PAID 2021 SECURITY CERT

1. Google Certified Professional Data Engineer — $171,749
2. Google Certified Professional Cloud Architect — $169,029
3. AWS Certified Solutions Architect - Associate — $159,033
4. CRISC - Certified in Risk and Information Systems Control — $151,995
5. CISSP - Certified Information Systems Security Professional — $151,853
6. CISM – Certified Information Security Manager — $149,246
7. PMP® - Project Management Professional — $148,906
8. NCP-MCI - Nutanix Certified Professional - Multicloud Infrastructure — $142,810
9. CISA - Certified Information Systems Auditor — $134,460
10. VCP-DVC - VMware Certified Professional - Data Center Virtualization 2020 — $132,947
11. MCSE: Windows Server — $125,980
12. Microsoft Certified: Azure Administrator Associate — $121,420
13. CCNP Enterprise - Cisco Certified Network Professional - Enterprise — $118,911
14. CCA-V - Citrix Certified Associate - Virtualization — $115,308
15. CompTIA Security+ — $110,974

https://www.globalknowledge.com/us-en/resources/resource-library/articles/top-paying-certifications/#10

15 MOST IN-DEMAND CERTIFICATIONS IN 2021

- AWS Certified Solutions Architect – Professional
- Certified Cloud Security Professional (CCSP)
- **Certified Data Privacy Solutions Engineer (CDPSE)**
- Certified Data Professional (CDP)
- Certified Ethical Hacker (CEH)
- **Certified Information Security manager (CISM)**
- Certified Information Systems Security Professional (CISSP)
- Cisco Certified Internetwork Expert (CCIE)
- Cisco Certified Network Associate (CCNA)
- Cisco Certified Professional Network Professional (CCNP)
- Microsoft Certified Azure Solutions Architect
- Microsoft Certified Solutions Associate (MCSA)
- Oracle Certified MySQL Database Administrator (CMDBA)
- Project Management Professional (PMP)
- Salesforce Certified Development Lifecycle and Deployment Designer

https://www.cio.com/article/3562331/top-15-it-certifications-in-demand-for-2021.html

And More CISO Leadership Skills

- Talking vs Listening
- Influencing/Negotiating
- Written Communication
- Networking
- Certification
- Presentation
- Budgeting
- Technical Excellence
- Team Dynamics (Personality Preferences)
- Generational Differences