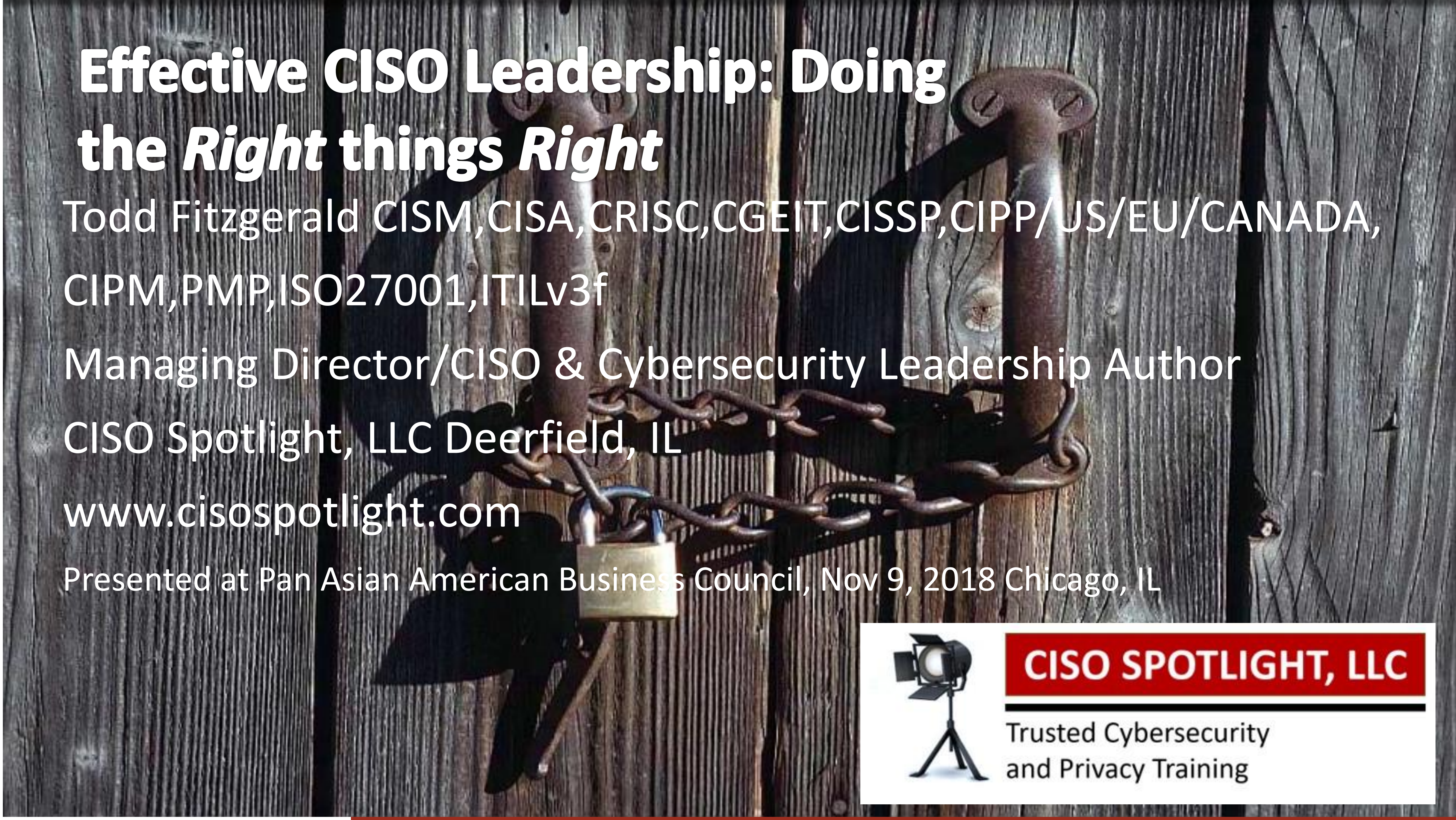


Effective CISO Leadership: Doing the *Right* things *Right*

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

Managing Director/CISO & Cybersecurity Leadership Author

CISO Spotlight, LLC Deerfield, IL

www.cisospotlight.com

Presented at Pan Asian American Business Council, Nov 9, 2018 Chicago, IL

CISO SPOTLIGHT, LLC

Trusted Cybersecurity
and Privacy Training

67% of CISOs believe their organizations are more likely to fall victim to a cyber attack or data breach in 2018

- 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

WHAT IS THE QUESTION?

A. 11 BILLION

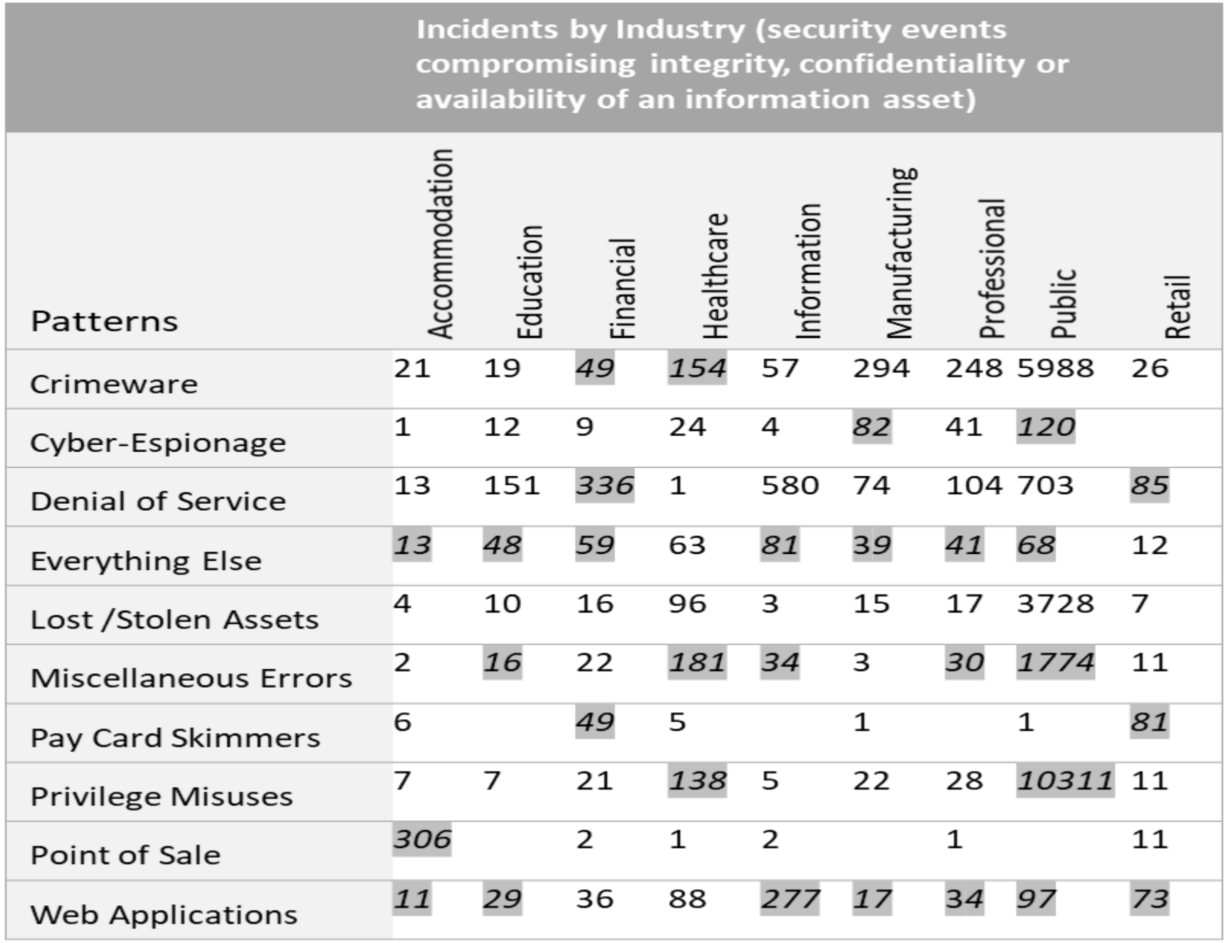
B. 1.9 BILLION

C. 500 MILLION

D. 8,229

Source: 2015 Verizon Data Breach Investigations Report

INCIDENT PATTERNS BY INDUSTRY AND TOP PATTERNS FOR BREACHES



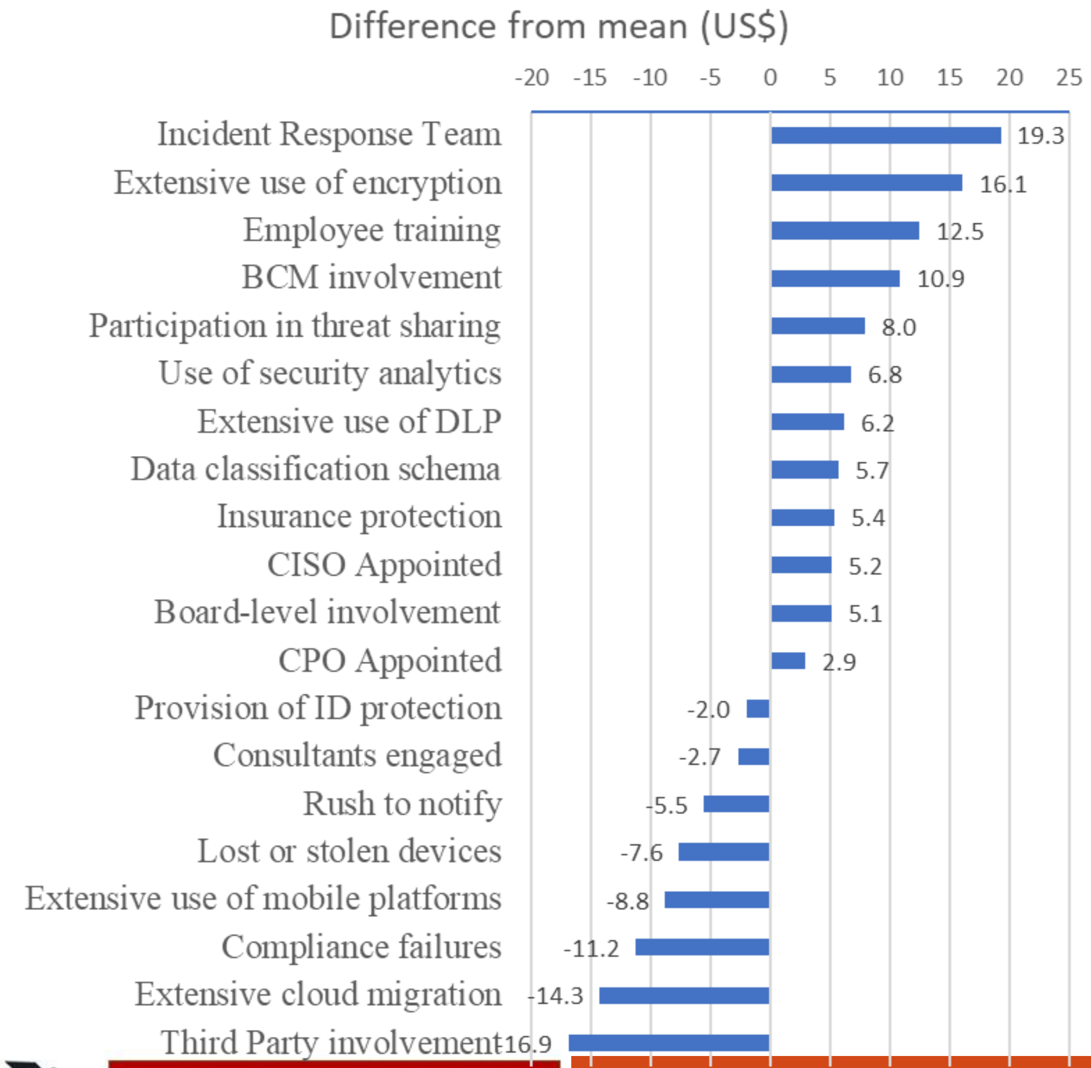
Incidents by Industry (security events compromising integrity, confidentiality or availability of an information asset)

Patterns	Accommodation	Education	Financial	Healthcare	Information	Manufacturing	Professional	Public	Retail
Crimeware	21	19	*49*	*154*	57	294	248	5988	26
Cyber-Espionage	1	12	9	24	4	*82*	41	*120*	
Denial of Service	13	151	*336*	1	580	74	104	703	*85*
Everything Else	*13*	*48*	*59*	63	*81*	*39*	*41*	*68*	12
Lost /Stolen Assets	4	10	16	96	3	15	17	3728	7
Miscellaneous Errors	2	*16*	22	*181*	*34*	3	*30*	*1774*	11
Pay Card Skimmers	6		*49*	5		1		1	*81*
Privilege Misuses	7	7	21	*138*	5	22	28	*10311*	11
Point of Sale	*306*		2	1	2		1		11
Web Applications	*11*	*29*	36	88	*277*	*17*	*34*	*97*	*73*

▨ Shaded box = Top patterns accounting for breaches by industry (confirmed disclosure to an unauthorized party)

Source: (Adapted from *2018 Data Breach Investigations Report, 11th Edition*. 2018, 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*

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).

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

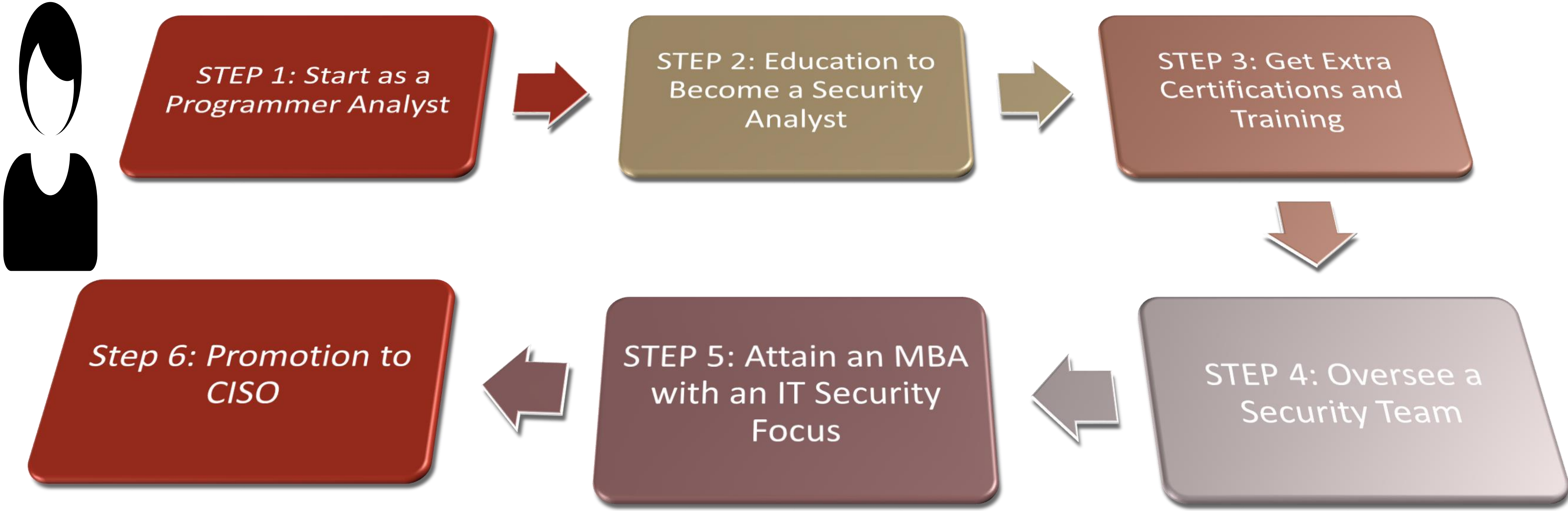
- Leadership qualities, and proven experience as an effective manager and influencer of people

- 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

Source: Actual CISO Job Description posted 7/19/18 on Glassdoor (company name omitted)

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

WHERE DO THE CISOS COME FROM?

A. The are born as natural paranoid leaders

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

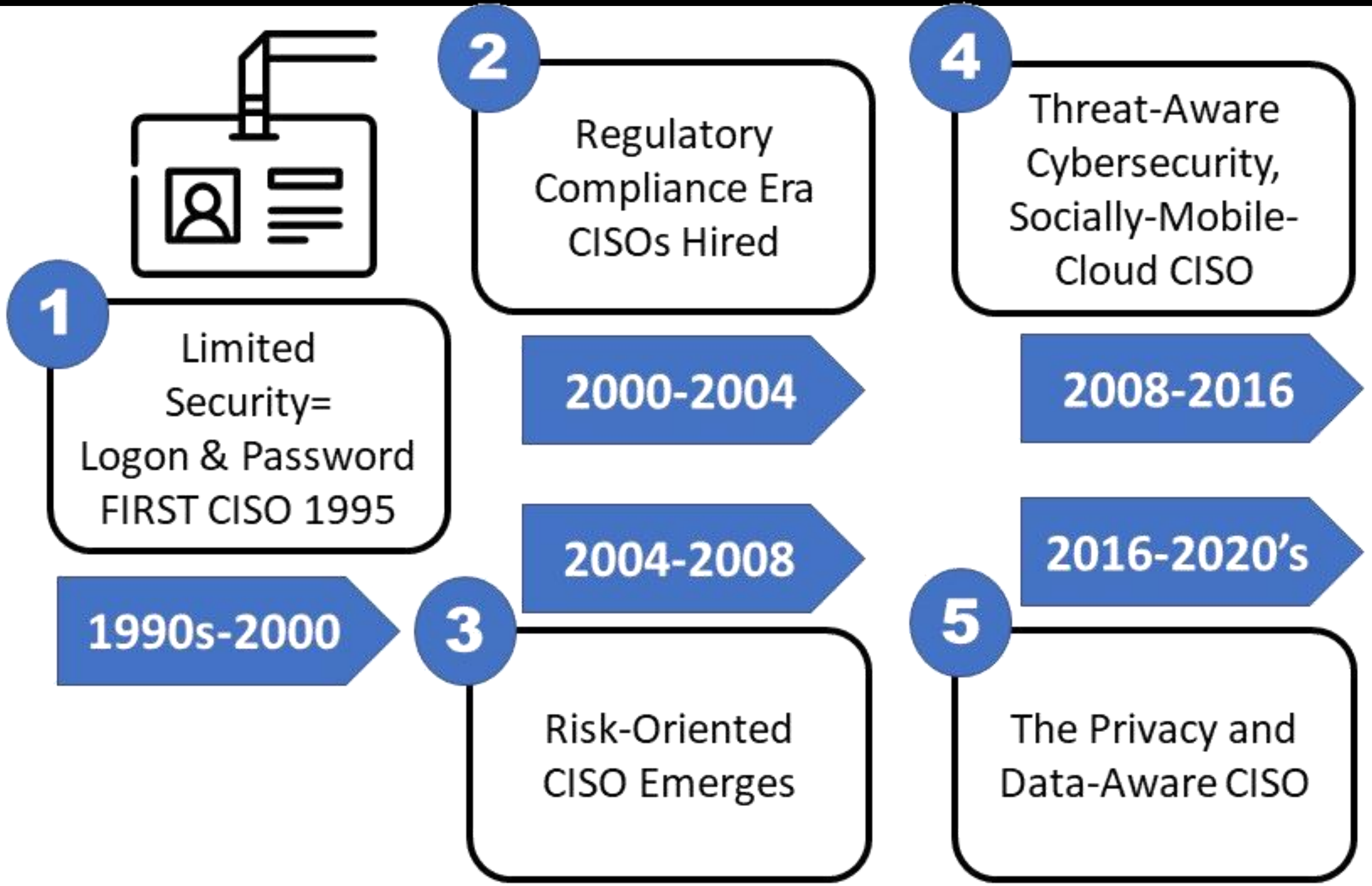
C. Didn’t attend the selection meeting

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

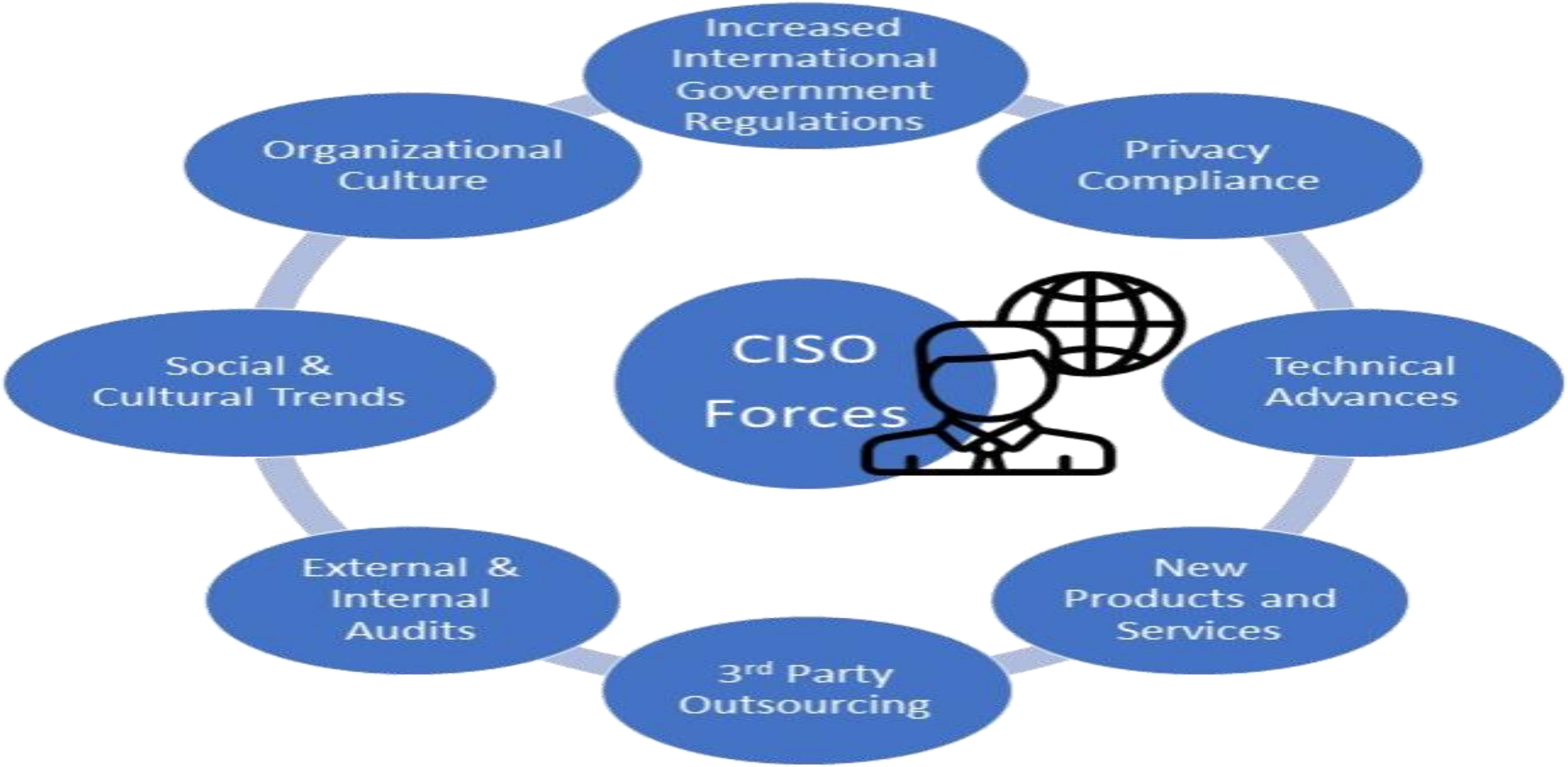
2008-2016

5 The Privacy and Data-Aware CISO

2016-2020's

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

FORCES IMPACTING THE SECURITY ORGANIZATION



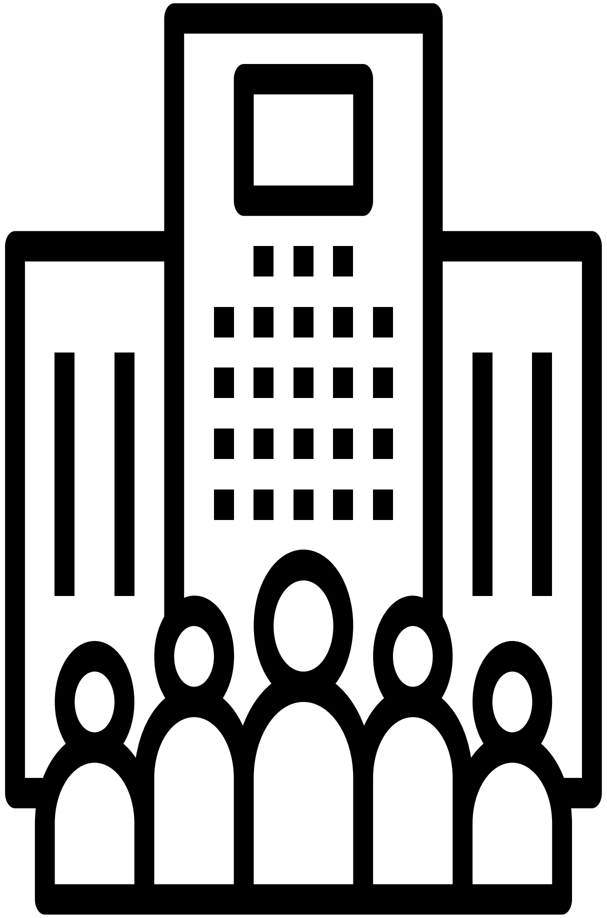
EVOLUTION OF THE CISO ROLE PRE-2000 to Present

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

DO CISOS GET PROMOTED FROM WITHIIN?

59%
Fortune 500
CISOs
External
Hires

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



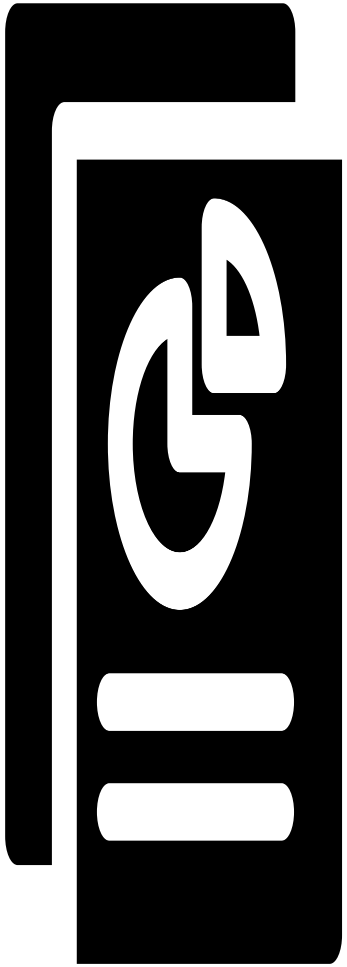
F500 CISOs
average
tenure 4.5
years

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

CISO SPOTLIGHT, LLC
Trusted Cybersecurity
and Privacy Training

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

GARTNER SAYS…



- ✓ 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

EXECUTE THE ESSENTIALS FOR A LEADING SECURITY PROGRAM

"We are on the verge of a revolution that is just as profound as the change in the economy that came with the industrial revolution. Soon electronic networks will allow people to transcend the barriers of time and distance and take advantage of global markets and business opportunities not even imaginable today, opening up a new world of economic possibility and progress."

- Vice President Al Gore, Jr., July 1997, A Framework for Global Electronic Commerce

2018

1998

1998 – "The Good Ol' Days"

No Facebook

Phones

Wired

VCR

No Ipods or Ipads

No USB Sticks

Blockbuster

50 inch flat screen

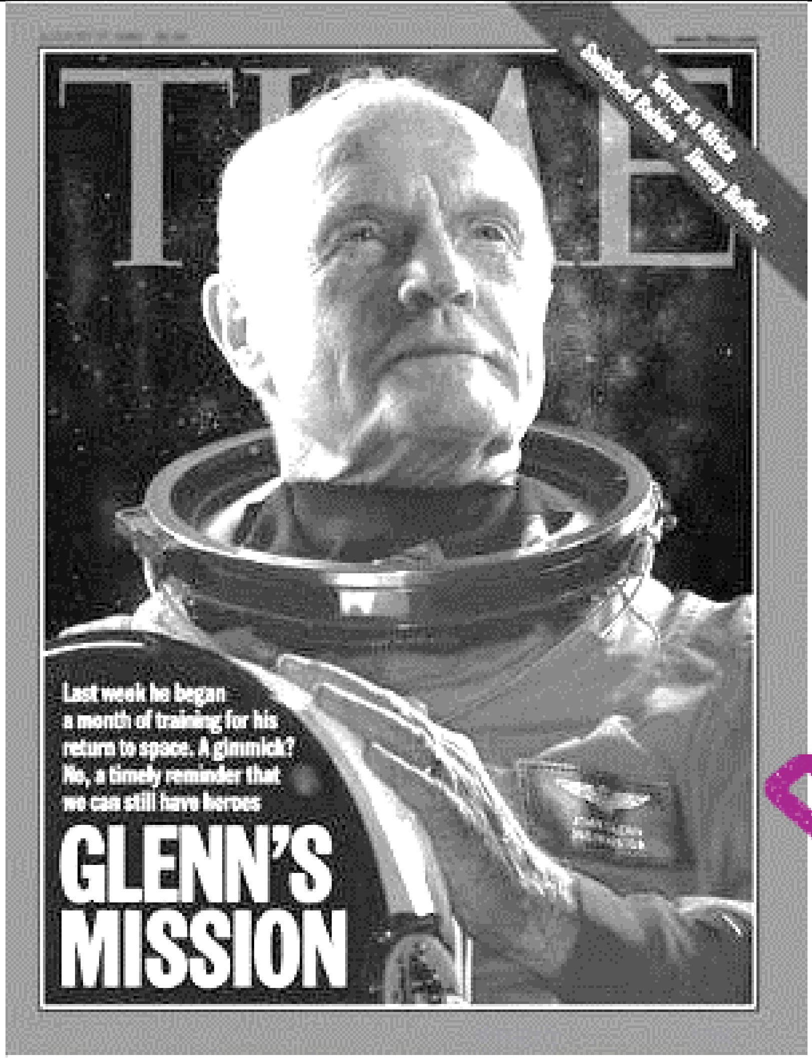
$9K

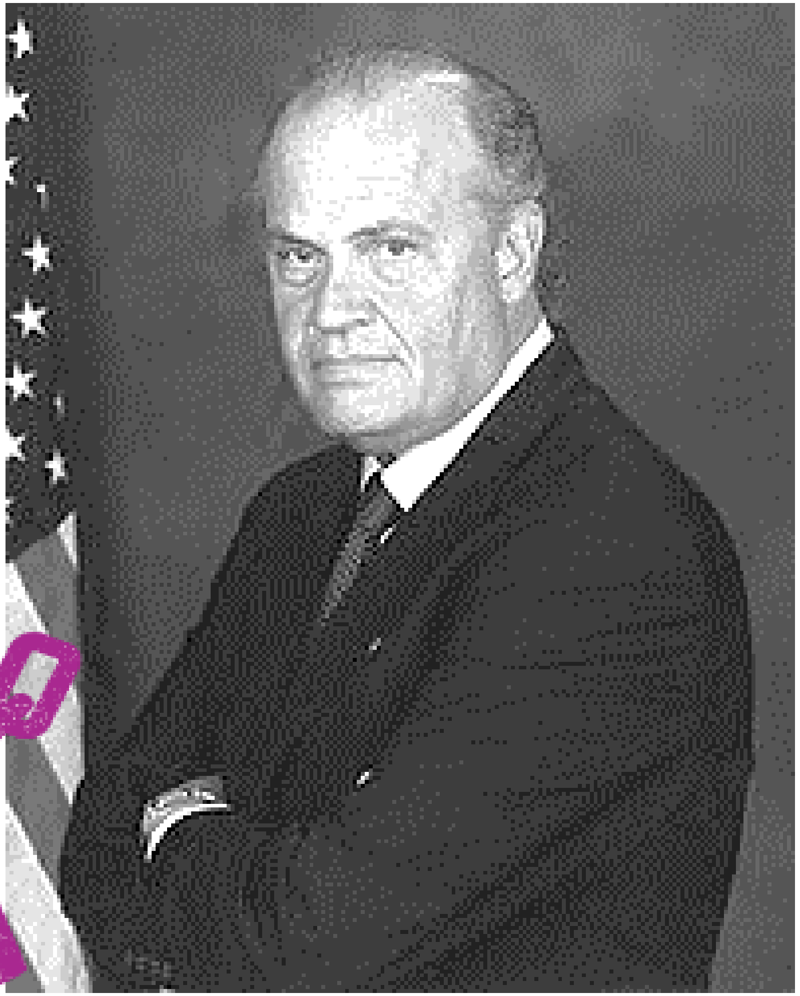
Y2k

Paper Maps

Gas $1.06 gal
ER Top TV
Saving Private Ryan
Backstreet Boys
M. Jordan MVP
Monica Lewinsky
Furby, Rugrats
Teletubbies
Final Seinfeld Show

Circa 1997-1998, There These Two Men….

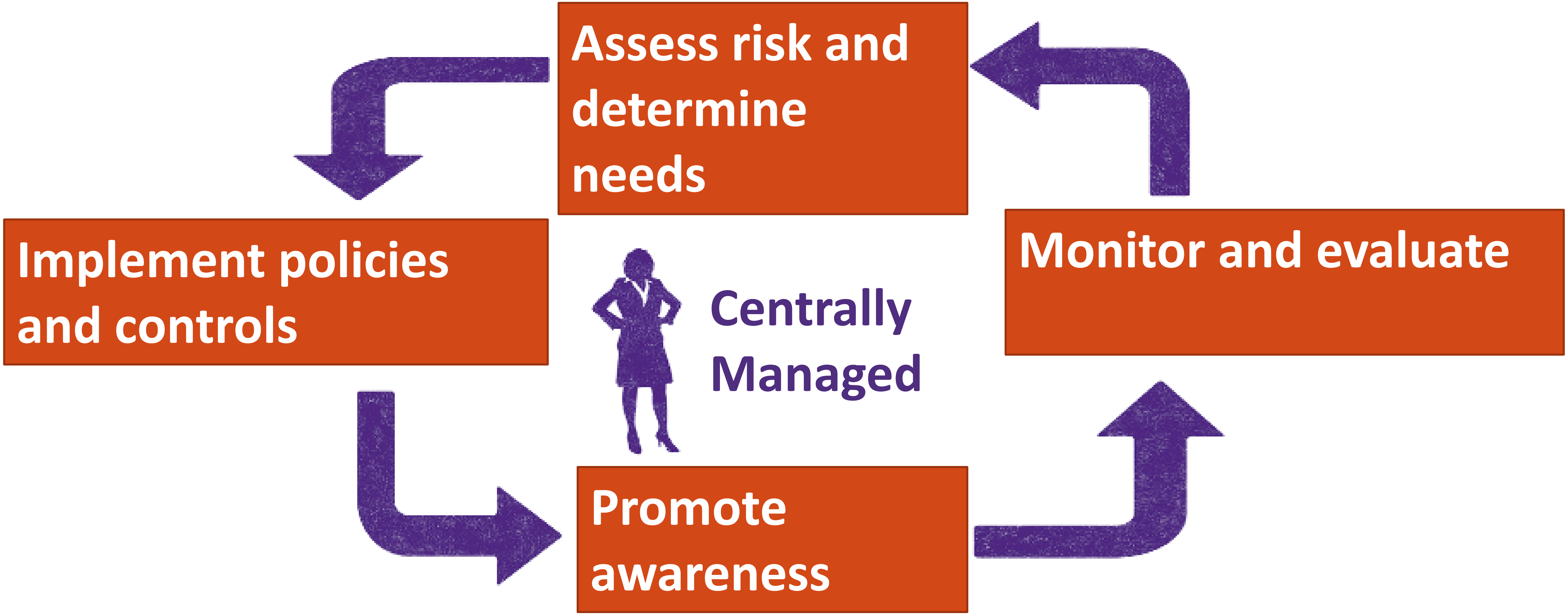

TIME
Terror in Africa
Jimmy Buffett
Last week he began a month of training for his return to space. A gimmick? No, a timely reminder that we can still have heroes
GLENN'S MISSION



CISO SPOTLIGHT, LLC

Trusted Cybersecurity
and Privacy Training

…Resulting in 'Security Leadership In Leading Organizations- 1998 Style



Assess risk and determine needs

Implement policies and controls

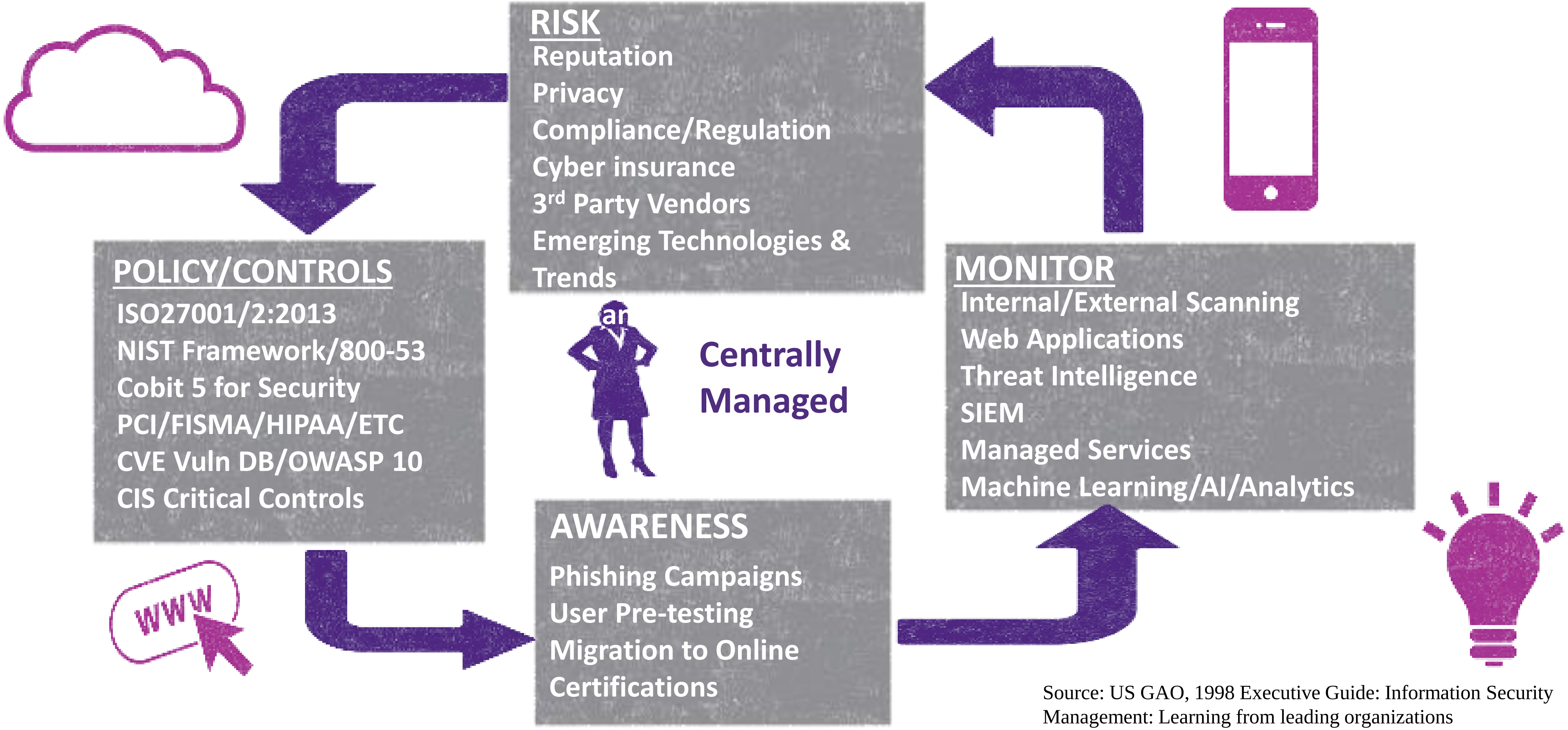
Promote awareness

Monitor and evaluate

Centrally Managed

Source: US GAO, 1998 Executive Guide: Information Security Management: Learning from leading organizations

Security Leadership In Leading Organizations- 2018 Style



RISK

Reputation
Privacy
Compliance/Regulation
Cyber insurance
3rd Party Vendors
Emerging Technologies & Trends

POLICY/CONTROLS

ISO27001/2:2013
NIST Framework/800-53
Cobit 5 for Security
PCI/FISMA/HIPAA/ETC
CVE Vuln DB/OWASP 10
CIS Critical Controls

Centrally Managed

MONITOR

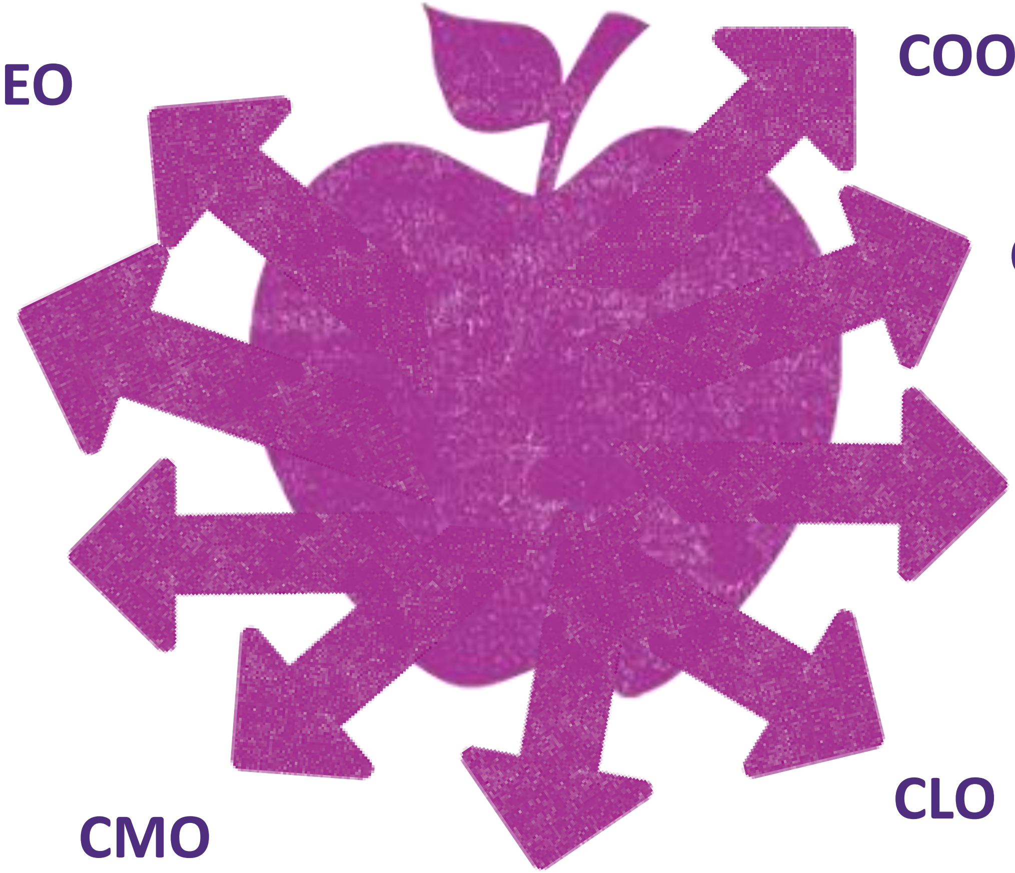
Internal/External Scanning
Web Applications
Threat Intelligence
SIEM
Managed Services
Machine Learning/AI/Analytics

AWARENESS

Phishing Campaigns
User Pre-testing
Migration to Online
Certifications

Source: US GAO, 1998 Executive Guide: Information Security Management: Learning from leading organizations

FORM RELATIONSHIPS WITH ALL CXO STAKEHOLDERS…



CEO

COO

C_O

CFO

CIO

CRO

CLO

CMO

CPO

… And Various Oversight Committees

LEGAL

RISK

COMPLIANCE

HUMAN RESOURCES

FINANCE

PHYSICAL SECURITY/FACILITIES

BUSINESS UNITS

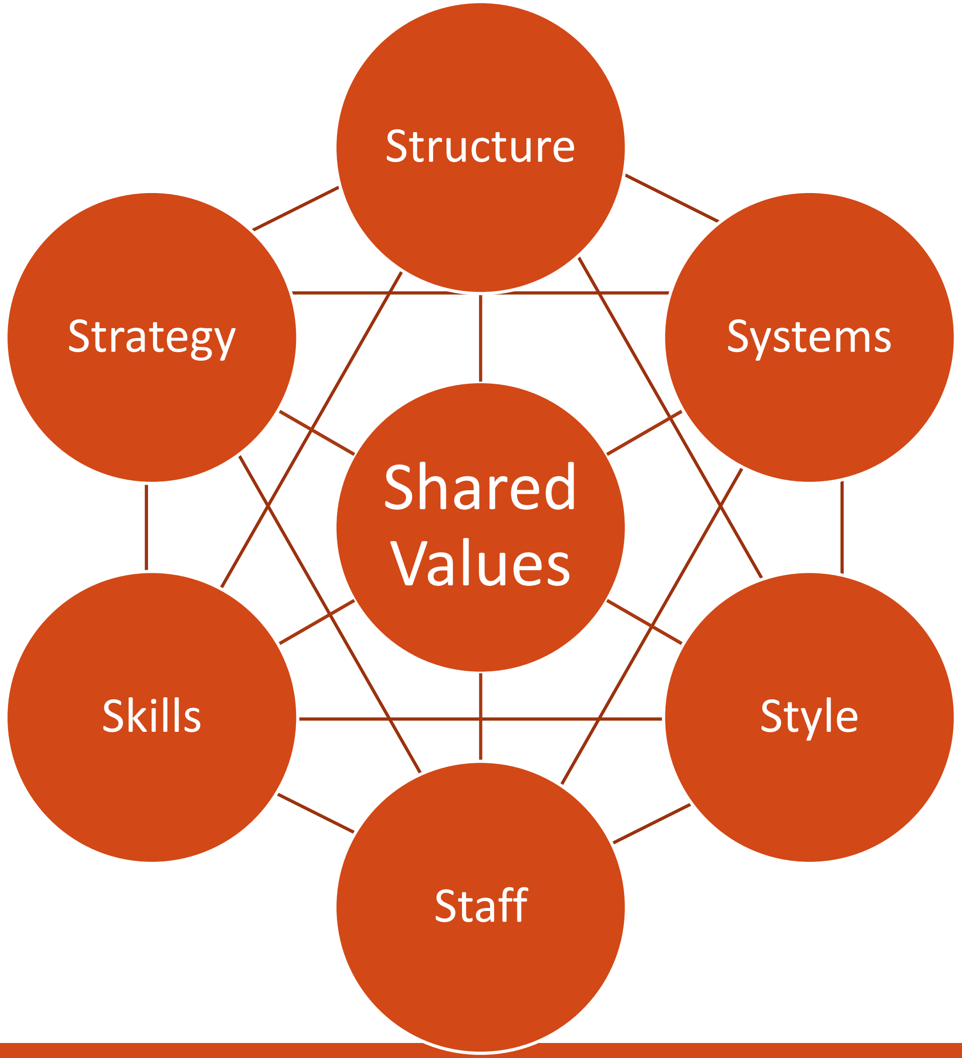
MARKETING

INFORMATION TECHNOLOGY

BOARDS ARE BECOMING MORE SAVVY AND NEED MORE INFORMATION ON SECURITY RISKS AND RISK REDUCTION

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.

CISO ORGANIZATIONAL EFFECTIVENESS: APPLYING THE MCKINSEY 7S FRAMEWORK TO CYBERSECURITY LEADERSHIP

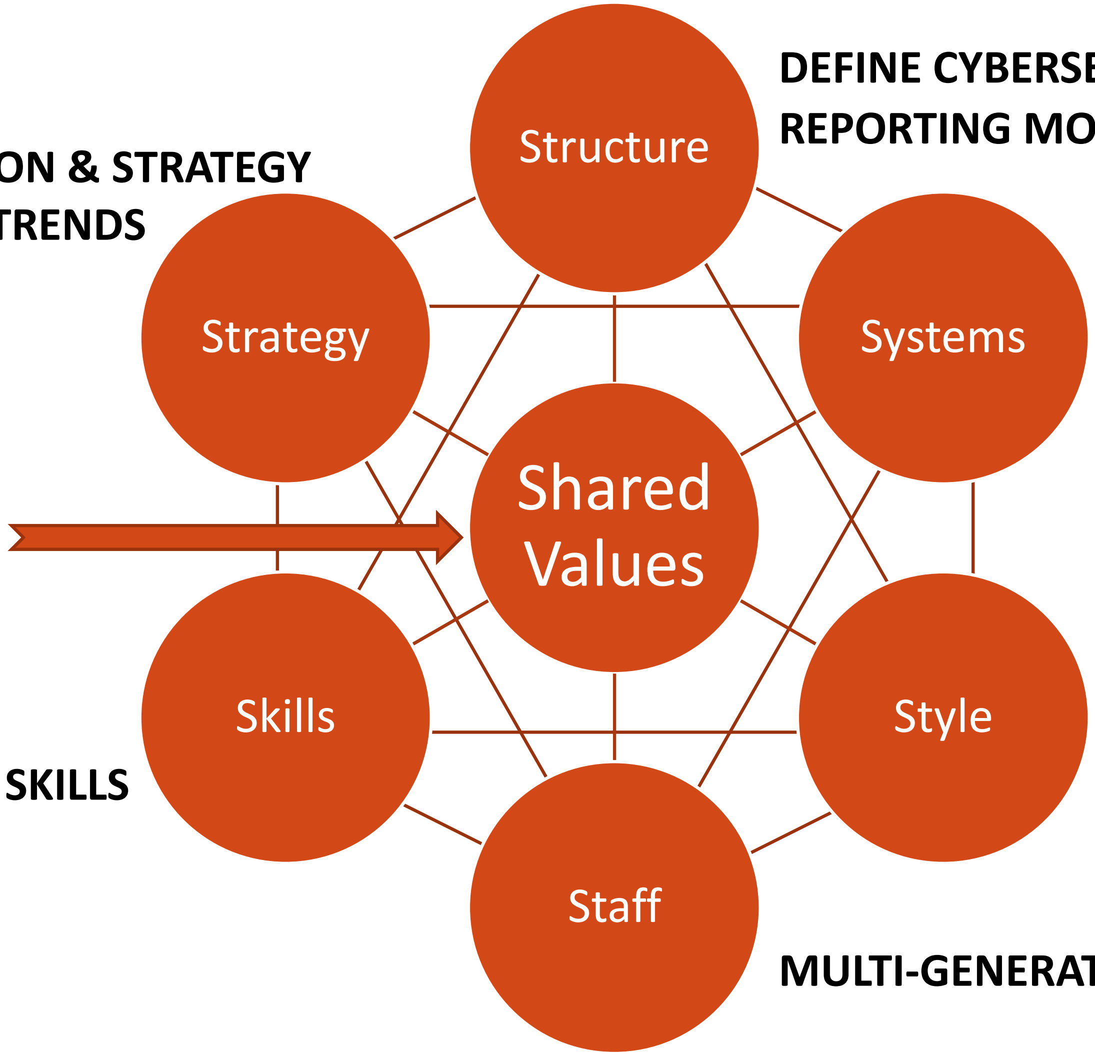


DEFINE CYBERSECURITY FUNCTIONS
REPORTING MODEL

DEVELOP CYBERSECURITY VISION & STRATEGY
EMERGING TECHNOLOGIES & TRENDS

LEVERAGING INCIDENTS
SECURITY CONTROL FRAMEWORKS
RISK MANAGEMENT PRACTICES

LAWS AND REGULATIONS
DATA PROTECTION & PRIVACY
POLICIES AND PROCEDURES



CISO AND THE BOARD

CISO SOFT SKILLS

MULTI-GENERATIONAL WORKFORCE DYNAMICS

"Security Language" may not be easily understood by the C-suite and the Board"

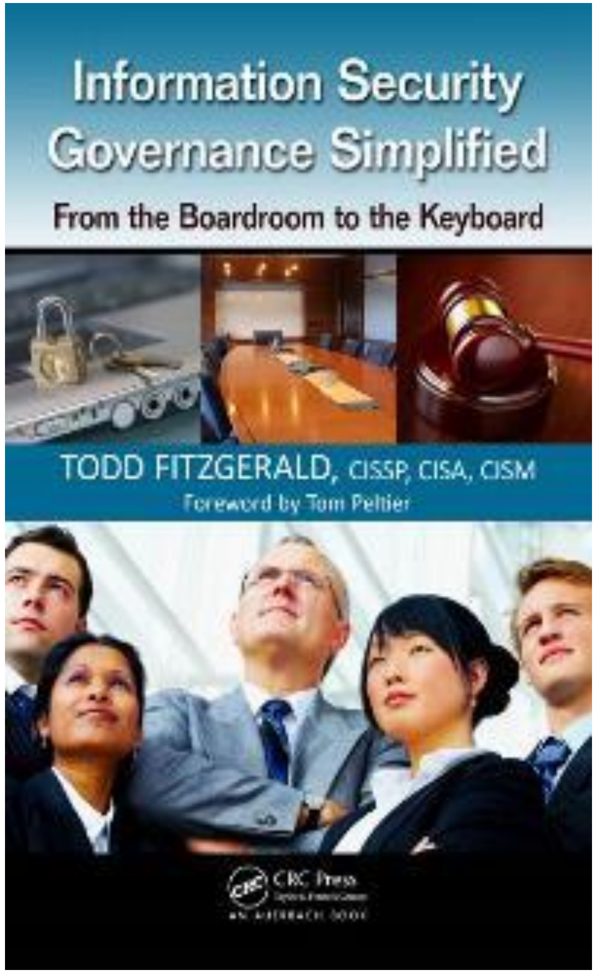
- Increase in share value for good governance
- Increased predictability of business operations
- Protection from civil or legal liability as a result of absence of due care
- Critical decisions not based on faulty information

Source: Several videos in this presentation from personal collection of Eugene Schultz, an unforgettable information security pioneer.

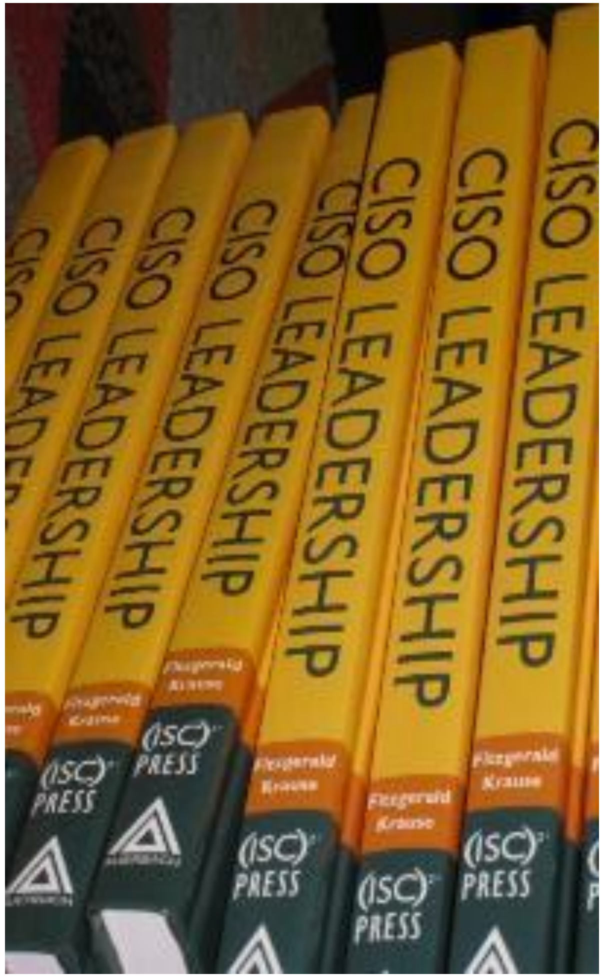
Source: Several videos in this presentation from personal collection of Eugene Schultz, an unforgettable information security pioneer.

3 BOOKS TO BUILD, LEAD, AND SUSTAIN CYBERSECURITY PROGRAM

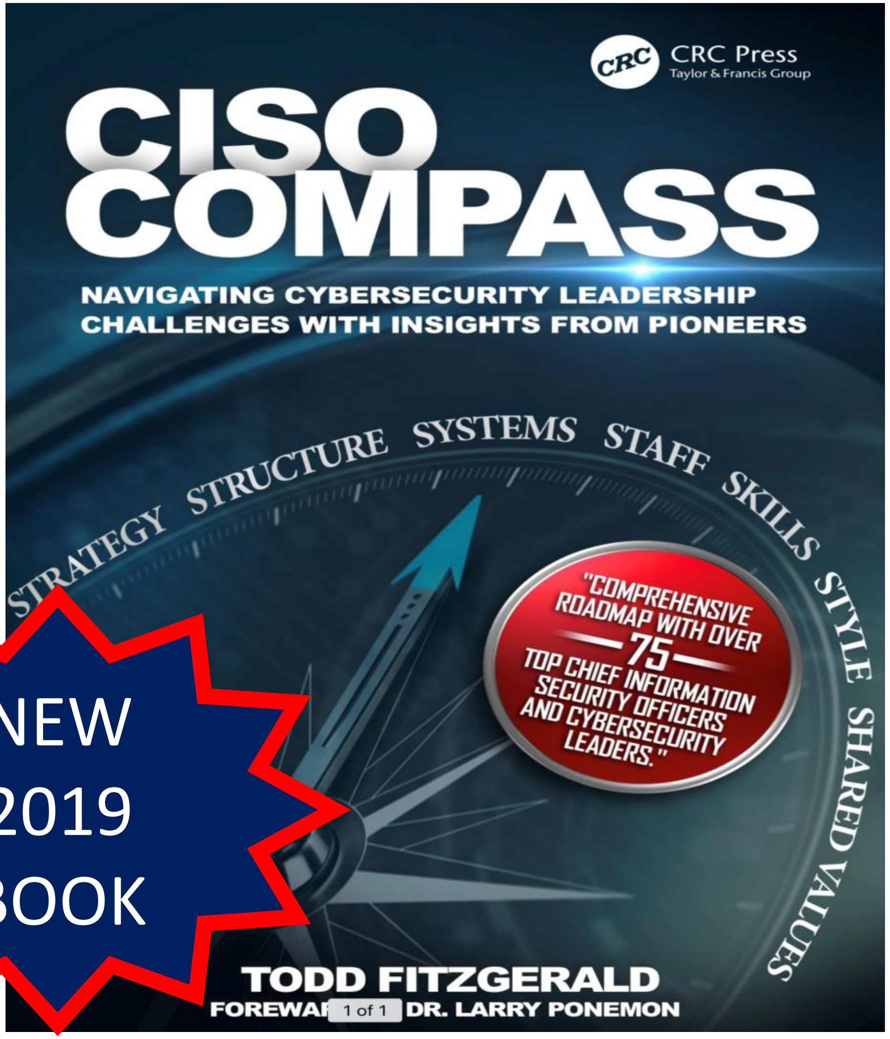
BUILD PROGRAM


Information Security Governance Simplified
From the Boardroom to the Keyboard
TODD FITZGERALD, CISSP, CISA, CISM
Foreword by Tom Peltier
CRC Press

LEAD PROGRAM



CISO ROADMAP


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
FOREWA[RD BY] DR. LARRY PONEMON

NEW 2019 BOOK

CISO SPOTLIGHT, LLC

Trusted Cybersecurity and Privacy Training

THANK YOU VERY MUCH!!!

CISO SPOTLIGHT, LLC

Trusted Cybersecurity
and Privacy Training

Todd Fitzgerald, CISSP, CISM, CISA, CGEIT, CRISC CIPP/US/E/C, CIPM, PMI ISO27001, ITILv3f

Managing Director/CISO

Security Leadership Author, Keynote Speaker, Advisor, CISO Trainer

CISO Spotlight, LLC

Deerfield, IL USA

Linkedin.com/in/toddfitzgerald

tfitzgerald@cisospotlight.com