The vCISO

Full Experience / Fractional Cost

Managing Cyber

A Threat Intelligence Briefing For Everyone

UNCLASSIFIED / For Official Use Only (FOUO)

Updated: July 2023
Version 3.7

On what topics are you prepared to brief us?

Briefing Purpose

The vCISO
Full Experience / Fractional Cost

- **What is Cybersecurity?**
- **Why Hackers Hack?**
- What threats do organizations face?
- Is this really happening?
- Why does this matter?
- Why does every organization need a Cyber Strategy?
- What is the single most important investment one can make?
- **What is the role of a CISO?**
- What are the most important things for SMBs
- What does a fully realized Cybersecurity program look like?
- **What might we be missing?**
- What if I can't do all that?
- What if I want a career in cyber?
- Where can I go for additional guidance and resources?

What is Cybersecurity?

Product Recalls

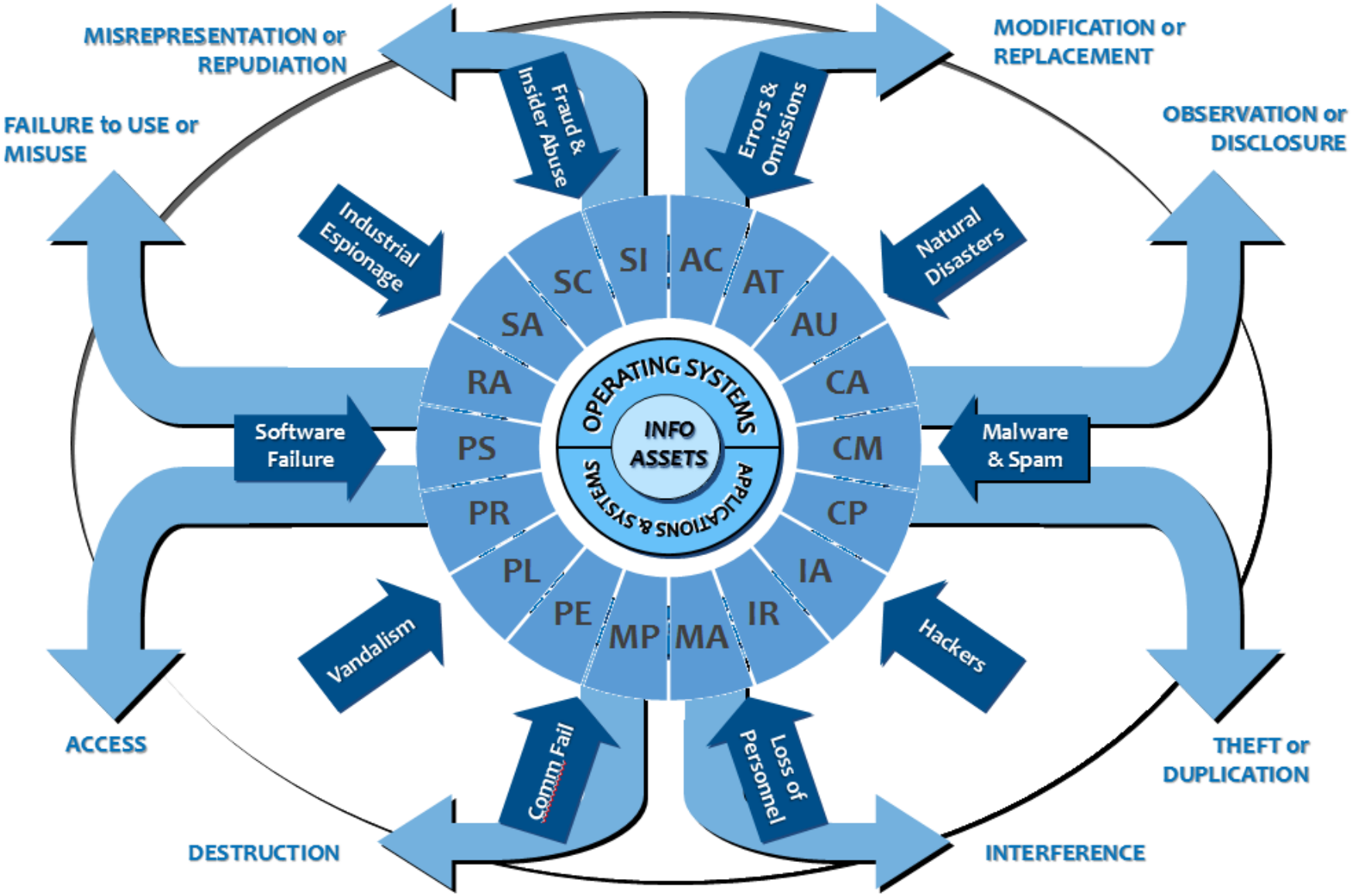
Crossing the Street

What is this all about?

Context

The vCISO

Full Experience / Fractional Cost

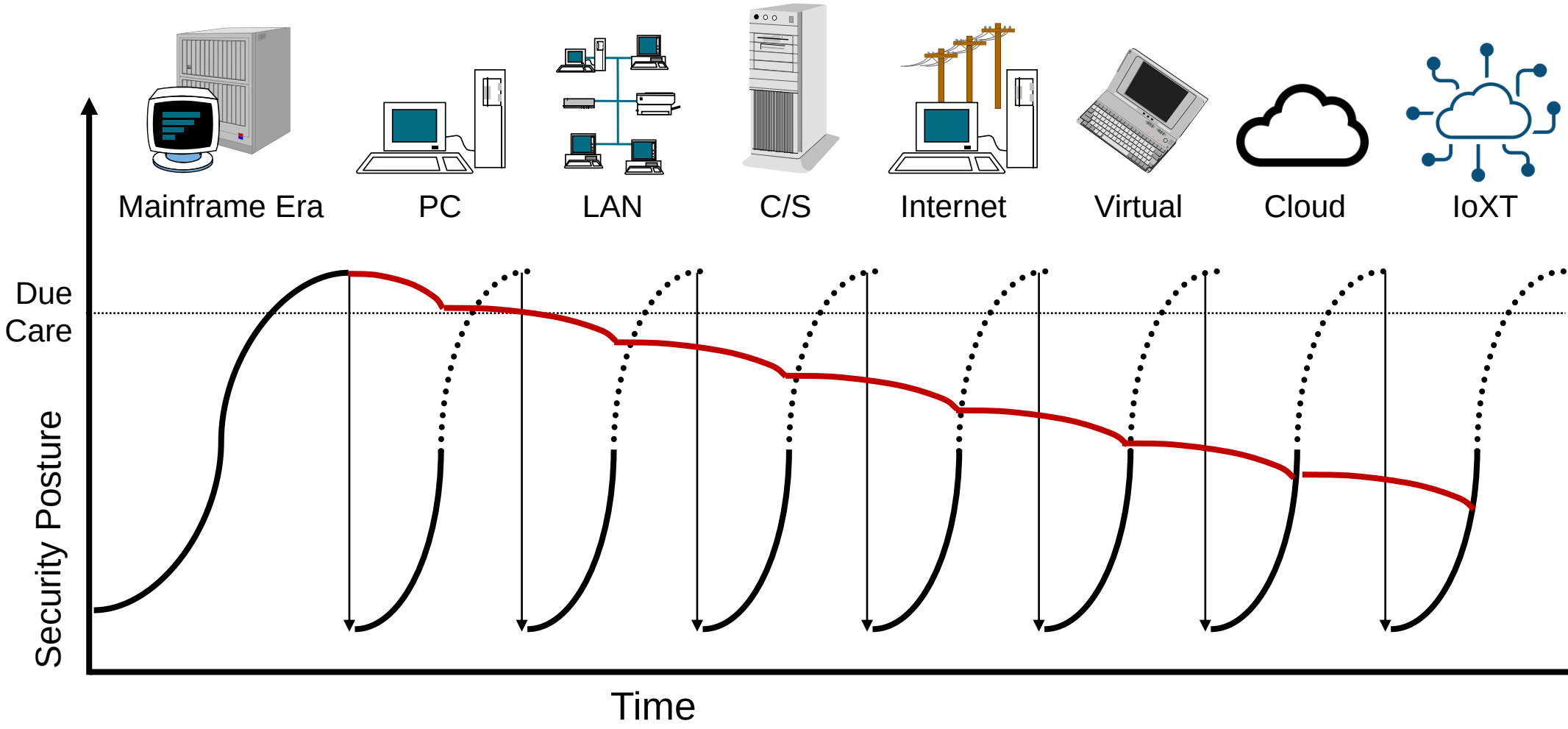


How did we get here?

Security Exposure

The vCISO

Full Experience / Fractional Cost



Why Hackers Hack

Why do Hackers Hack?

Adversary Motivation

The vCISO
Full Experience / Fractional Cost

- **REASONS HACKERS HACK**
  - Nation / State Sponsored
  - Political Cause / Hactivism
  - Economic Gain
  - Dark Web Credibility

June 2020
Ransomware Halts Honda Production

EKANS Ransomware encrypted Industrial Control System files interrupting production lines.

May 2021
Colonial Pipeline Shut Down by Ransomware

DarkSide (using a RAAS) encrypted and stole 100G of data from company responsible for 45% of fuel consumed on east coast.

August 2021
John Deere Security Vulnerabilities Put Agriculture at Risk

John Deere's systems found to have security weaknesses that could allow remote code execution of the machines.

February 2022
Meta Pays $90M to settle privacy claim.

The parent company of Facebook, agreed to pay $90 million to settle a data privacy lawsuit over its use of cookies to track users' internet use even after they had logged off.

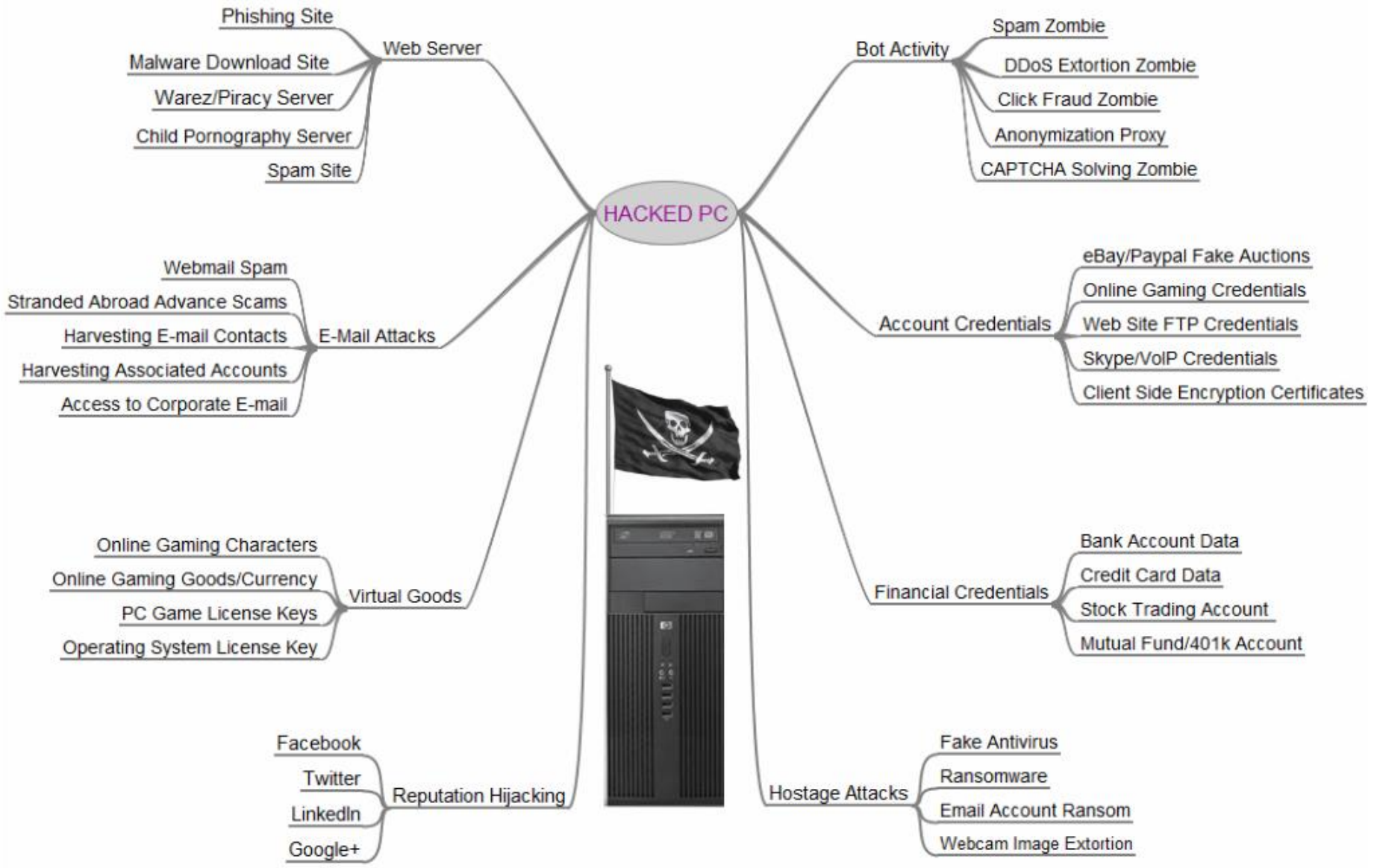
January 2023
Killnet Hacktivist Launch DDOS Campaign

Pro-Russian Hacktivist group launches DDOS campaign against German and US government, utility, and healthcare targets

Why do hackers hack?

Value of a "Pwned" Computer

The vCISO
Full Experience / Fractional Cost



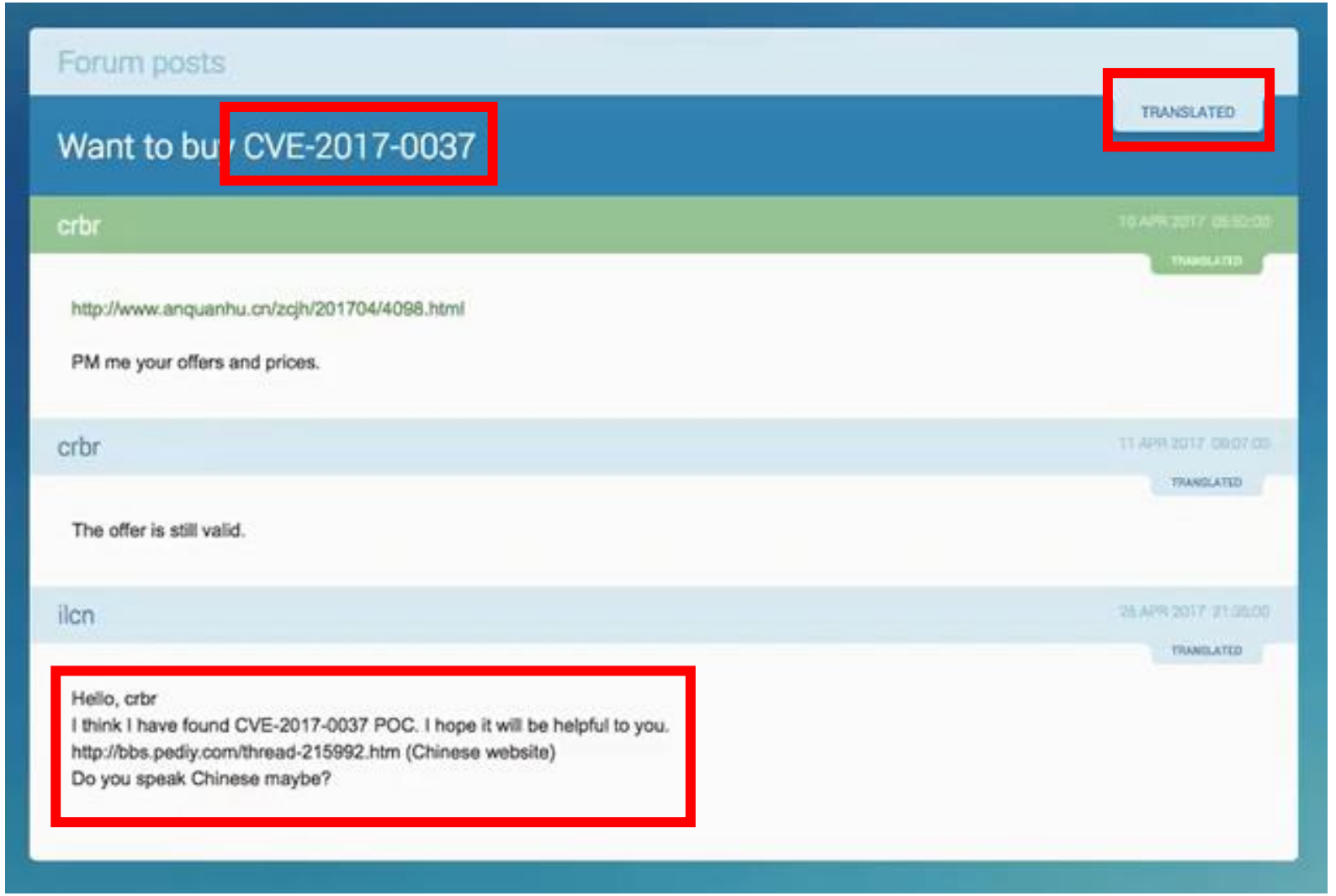
Source: Brian Krebs

And better still, what if you knew how they were going to break in?

Proactive Threat Intelligence

The vCISO

Full Experience / Fractional Cost

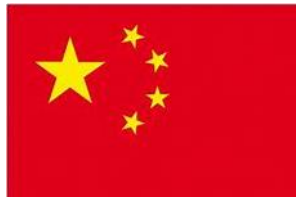


Can we stipulate that cybersecurity is a real threat facing your organization?

Context

The vCISO
Full Experience / Fractional Cost

- Presumed awareness of current realities:
  - Weapons Grade Attacks vs. Limited Budgets
  - Unrecognized Supply Chain and Third-Party Dependencies
  - Well equipped and financed Nation State and Organized Crime Actors
  - Increasingly Costly Breaches
  - Rapidly escalating customer demands
  - Risk driven allocation vs. 100% coverage
  - Solutions that hinder operations get disabled
  - Expanding Deep/Dark Web Economy.



Cybercrime To Cost The World $10.5 Trillion Annually By 2025

Special Report: Cyberwarfare In The C-Suite.

– *Steve Morgan, Editor-in-Chief*

Sausalito, Calif. – Nov. 13, 2020

If it were measured as a country, then cybercrime — which is predicted to inflict damages totaling $6 trillion USD globally in 2021 — would be the world's third-largest economy after the U.S. and China.

Why Cybersecurity Matters

What is it exactly that we're trying to do?

Managed Risk

The vCISO

Full Experience / Fractional Cost

- You can forget about the word "security", but you must acknowledge that:
  - We are in a global economy
  - Where organizations are competing with one another for a share of increasingly diminishing resources
  - Some players deem it fiscally prudent to take the R&D of a competitor rather than invest on their own
  - The laws of many nation states leave it to companies to protect themselves against hacking
- This translates directly into a need for organizations to:
  - Protect the value of their intellectual property
  - Preserve the integrity of data entrusted to them by customers and third parties
  - Prevent the theft and/or misuse of physical assets and other key resources
  - Obtain insurance coverage and do so at the lowest possible premiums
  - Fulfill due care obligations of the board and senior leadership team
  - Minimize the likelihood of active threats
  - Satisfy market demands
  - Avoid damage to our brand

"The CISO's job is to make it as easy as possible for customers to engage with us and for us to conduct business without putting ourselves or them at undue risk."

To what security requirements are Board of Directors and Senior Company Leadership obligated?

Fiduciary Liability

The vCISO
Full Experience / Fractional Cost

Of these questions however, THREE are most important and must remain top of mind:

1. **Where are we?**
2. **Where do we need to be?**
3. **How do we get there??**

The CISO is not just another title for “VP of Going to Jail.” If the CISO does the job correctly, it is the Board and Senior Leadership team who are collectively accountable for managing company cyber risk.

What is a CISO?

The vCISO

Full Experience / Fractional Cost

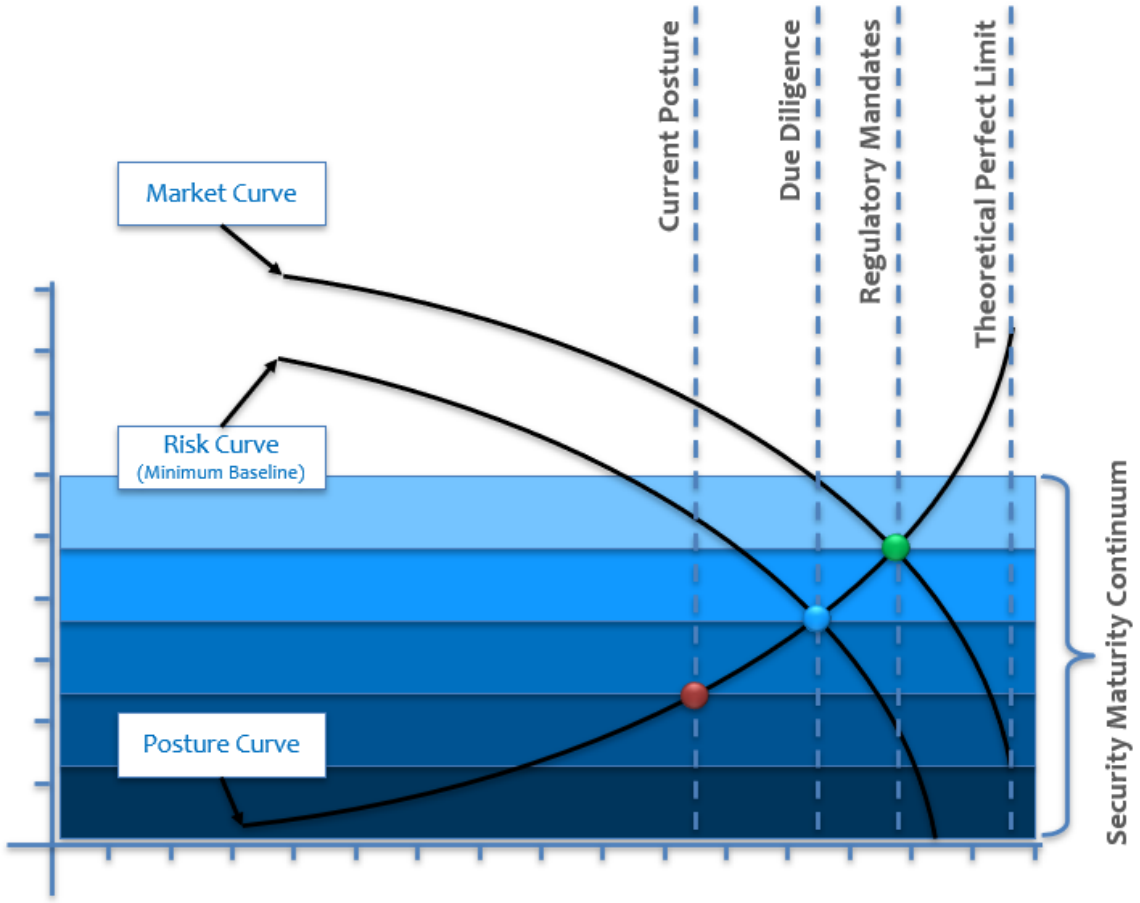
Great, another tax on operations…

The Role of a CISO

The vCISO

Full Experience / Fractional Cost

- **A good CISO is not just the Defensive Coach on a football team**
- **You also need an offensive playbook and someone to help move obstacles to success out of the way, engaging all aspects of the operation and enabling the business:**
  - Business Objectives>Business Strategy>IT Strategy>Security Overlay
  - Okay to accept risk of which you are aware and deem to fall within acceptable limits
  - It is NOT okay to accept risk by default because you lack awareness of its existence
  - Spend must be justified based on the risk reduction benefit (Econ 101).

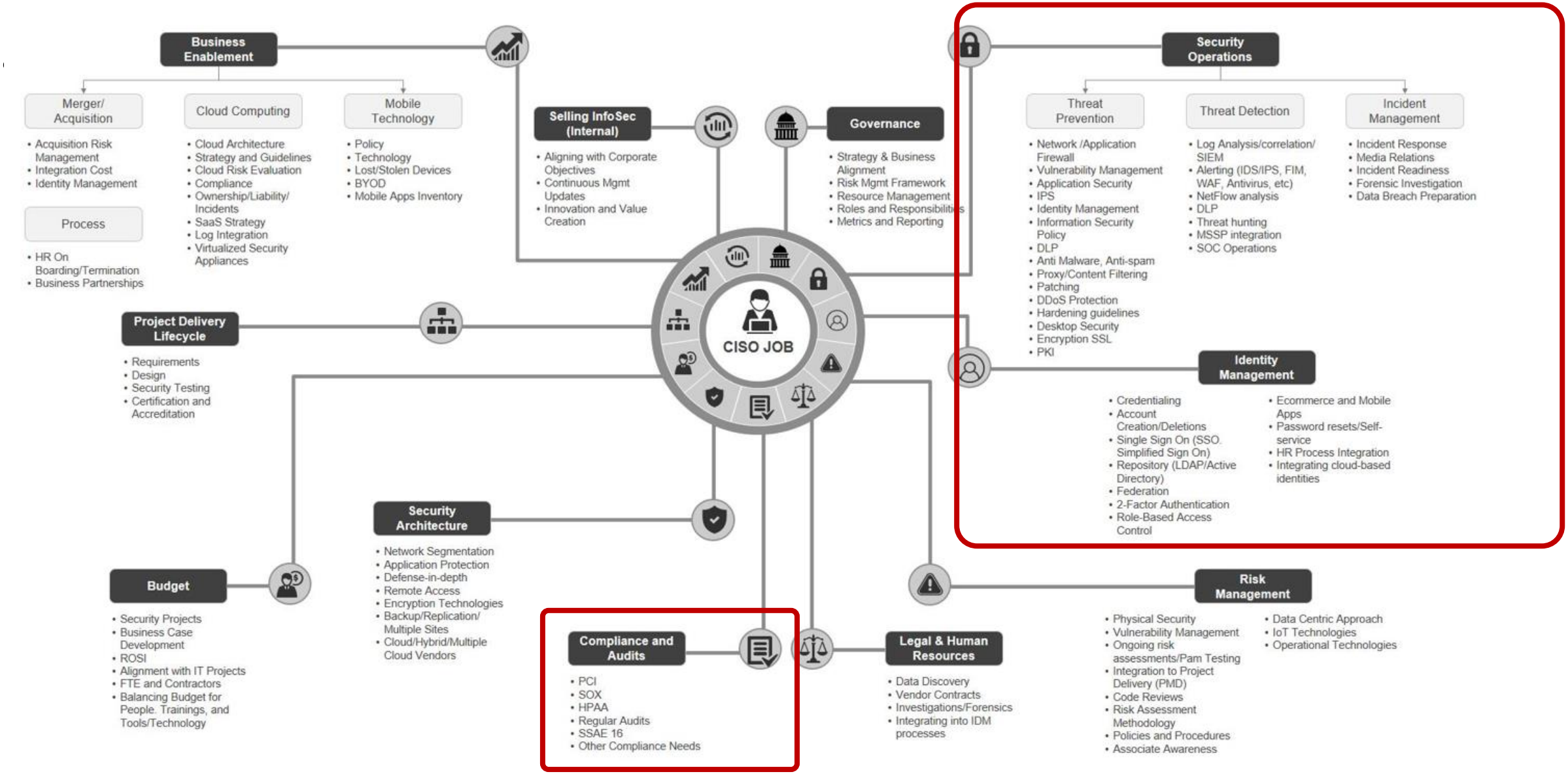


One person does all that?

Our Needs are Critical and Strategic

The vCISO

Full Experience / Fractional Cost



But when should I engage the CISO?

The CISO Partnership

The vCISO

Full Experience / Fractional Cost

- Engaging an IT service provider
- Leasing a new facility
- Hiring a cleaning crew
- Purchasing property
- Selling off all or part of our business
- Hiring a new employee or engaging a contract worker
- Entering into merger/acquisition conversation with another entity
- Purchasing software
- Returning leased equipment
- Developing a custom application
- Responding to a regulatory auditor's request for information
- Submitting a proposal to a customer
- Downloading and installing something on my computer
- Expanding into a new geographic market
- Engaging an insurance broker/underwriter for company policies
- Travelling to another country for business
- Allowing team members to work from home

ALL OF THEM!

What are we not thinking about?

A not so nice bakers dozen

Program Sufficiency

The vCISO

Full Experience / Fractional Cost

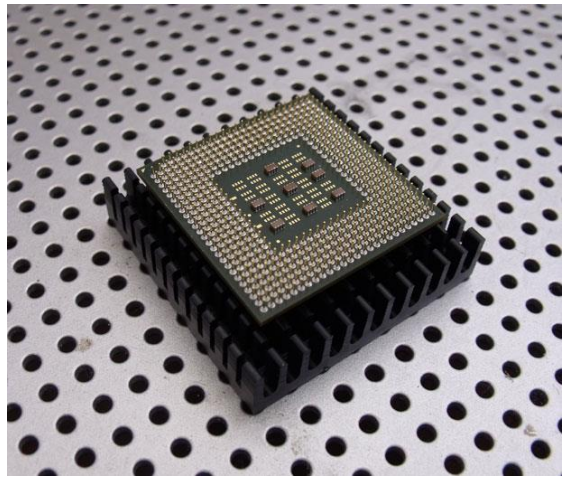
1. **Operations Technology (OT) & Internet of Things (IoT)**
2. **Artificial Intelligence & Machine Learning**
3. **Cloud Computing & Shared Public Infrastructure**
4. Quantum Computing
5. Blockchain Technology
6. 5G Networks / Smart City Infrastructure
7. **Return to Office (RTO)**
8. Augmented Reality / Virtual Reality
9. **Biometric Authentication**
10. Autonomous Vehicles
11. Wearable Technology
12. Drones
13. Smart Homes

There is no IT and there is no OT, there's just T!

Operations Technology (OT) & Internet of Things (IoT)

The vCISO
Full Experience / Fractional Cost

- **Vulnerabilities (and/or misconfigurations) exist everywhere:**
  - Traditional IT Stack
  - Operations Technology (OT)
  - Firmware
  - APIs.
- **What we're missing:**
  - Tools to scan everything that we install on our networks
  - Tools to scan anything to which we interconnect
  - Managed gateways for vendor support
  - OT Vendors typically do not offer patches
  - Security point products have little insight or analytics into OT traffic
  - We are not fully inspecting inbound assets as part of our supply chain
  - Default credentials
  - Chipmaker controls alert on change but fail to detect embedded malware

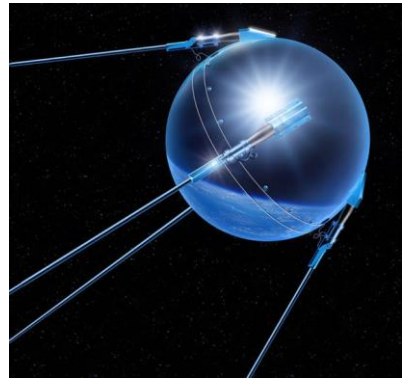


The fact that things work as well as they do as often as they do is nothing short of miraculous!

Cloud Computing & Shared Public Infrastructure

The vCISO
Full Experience / Fractional Cost

- **Context:**
  - Cloud has been around in one form or another since the 1960s
  - Widely adopted in the 2000's and now ubiquitous
  - Great benefit in terms of economies of scale
  - Solid solution for many companies, particularly SMBs.



- **What we may be missing:**
  - Lessons of history. Why did we invent the internet?
  - Accountability gaps between reality and sanctioned shared responsibility models
  - Data Localization
  - Backup immutability
  - DR/BCP protocols (meaning downtime procedures) must now be ON-PREM!
  - Flawed presumption about the resiliency of the public network, power, and communication satellites.

Return to Office (RTO)

- **Context:**
  - Secondary to COVID WFH response companies are implementing Return to Office (RTO)
  - Percentage of staff are unable or unwilling to comply
- **Issues:**
  - The Genie was already out. COVID was NOT our first pandemic
  - Lack of hardening standards/requirements and/or access controls (MFA) for home infrastructure
  - Little/no training / guidance on working remotely
  - Is refusal to comply tantamount to a resignation?
  - Staffing shortages / loss of valuable personnel and/or corporate memory
  - Wrongful/unfair dismissal allegations
  - Return of computing assets
  - Cannot withhold paychecks
  - Asset sanitization
  - Software Licensing/Piracy

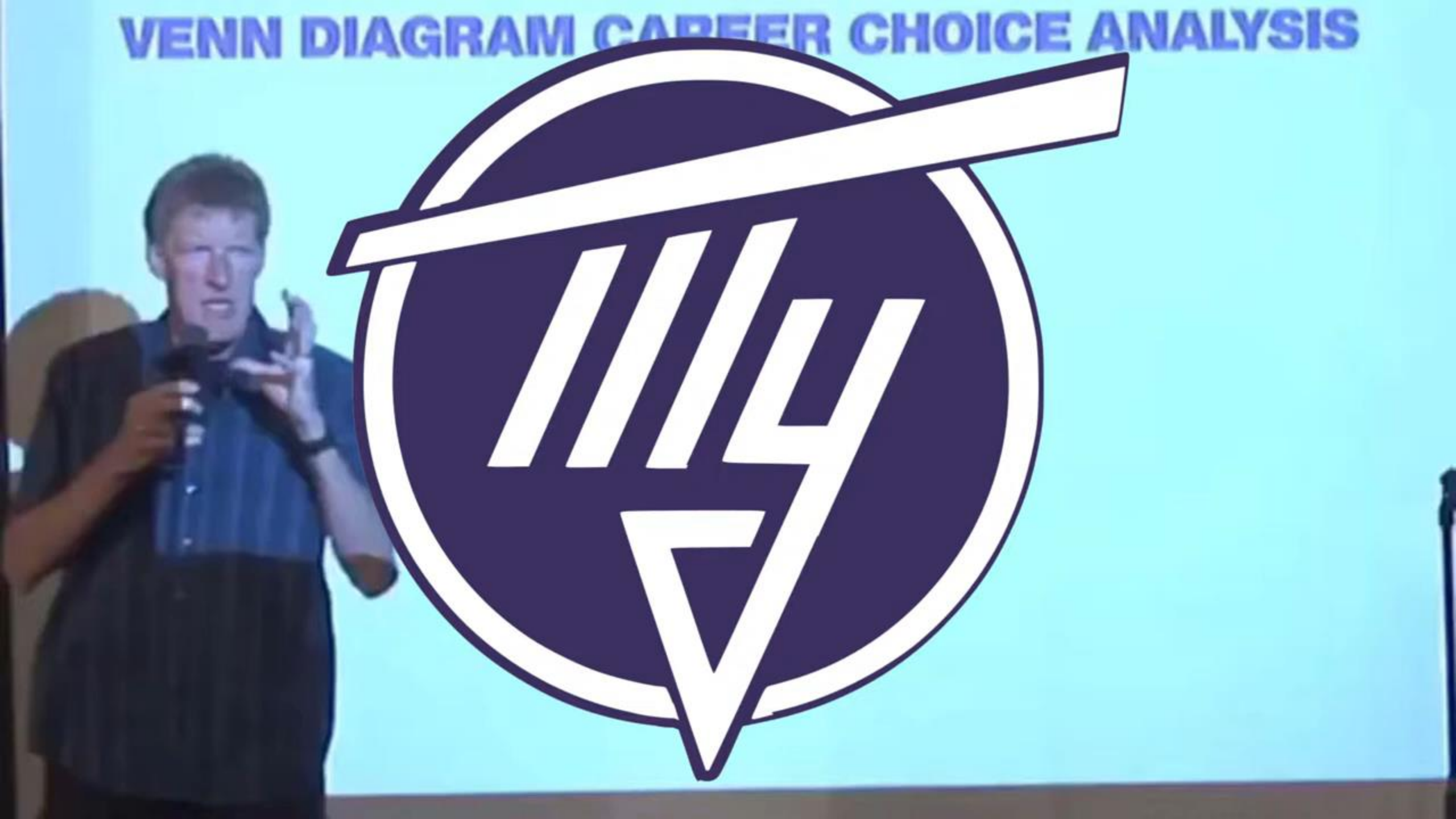
Biometric Authentication

- **Context:**
  - Verification of purported identity based on unique physical or behavioral characteristics
  - Traditional approaches calculate a value for comparison to a stored reference value
  - Eliminates the need to remember passwords or possess physical tokens
  - Access grants are contingent upon having a low likelihood that a match does not exist
  - Technology has been around and successfully used for decades.
- **What we're doing wrong:**
  - Reinventing the wheel
  - Lack of policies on the collection, use, and storage
  - Not obtaining explicit user consent
  - Alternatives for those who decline to provide consent
  - Improper/incomplete/invalid identity vetting
  - Storing the actual biometric vs. a derived value
  - Not encrypting these values at rest or in transmission
  - Not having defense in depth and/or not using in combination with another factor
  - Little to no response plans for irrevocable nature of biometric breach

Cybersecurity Careers

The vCISO

Full Experience / Fractional Cost


VENN DIAGRAM CAREER CHOICE ANALYSIS

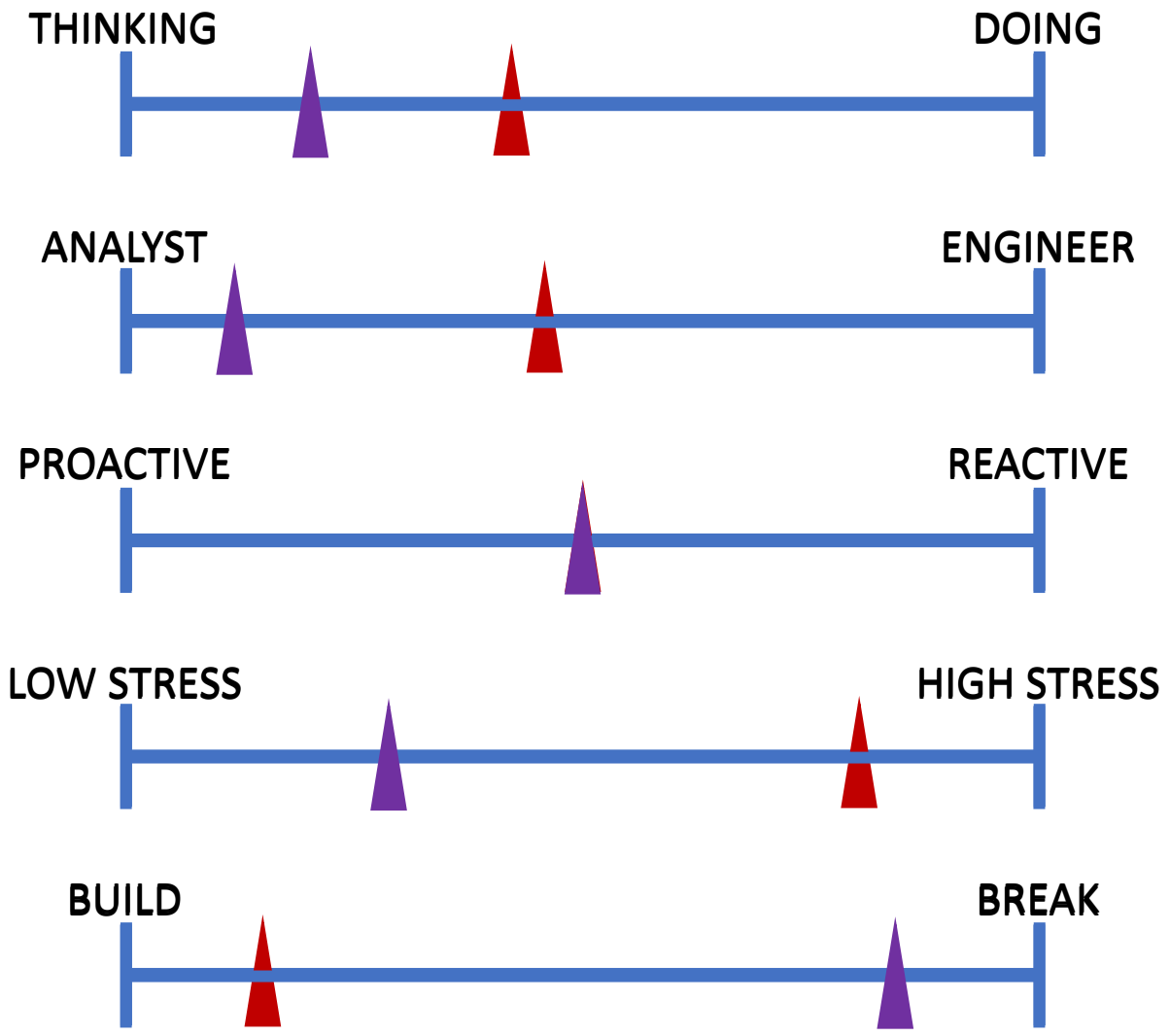
What types of jobs are in this field?

Cybersecurity Positions

The vCISO

Full Experience / Fractional Cost

- Auditor
- Assessor
- Business Analyst
- Data Analytics / Visualization
- Solutions Architect
- Designer/Developer
- Systems Integrator
- Security Engineer
- Systems Administrator
- Incident Response
- Disaster Recovery
- Risk Management
- Tester
- “Hacker”
- Forensics
- CISO



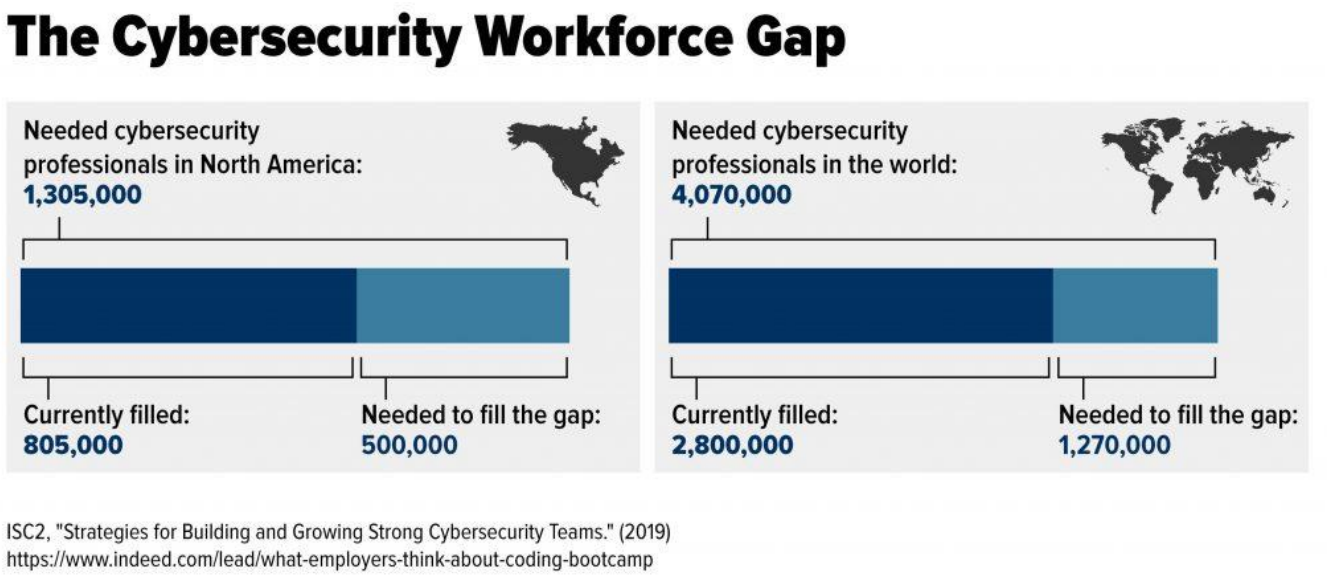
Are the open positions?

Demand Has Rarely Been Stronger

The vCISO

Full Experience / Fractional Cost

- **Market forces present substantial challenges (employers) or opportunities (professionals):**
  - Cyber workforce deficit stands at 3 Million workers worldwide.
  - This issue is being tracked by the NSC as an issue of national security
  - NIST/NICE and others are issuing millions in grants to address the issue
  - The cybersecurity gap will remain largely unchanged through 2025



ISC2, "Strategies for Building and Growing Strong Cybersecurity Teams." (2019)
https://www.indeed.com/lead/what-employers-think-about-coding-bootcamp

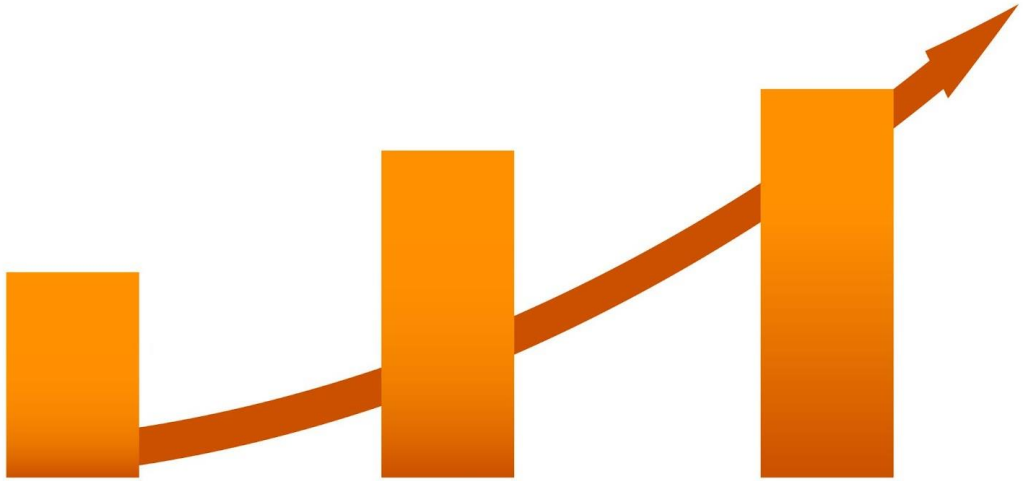
Make a difference and earn a good living...

Cybersecurity Compensation

The vCISO

Full Experience / Fractional Cost

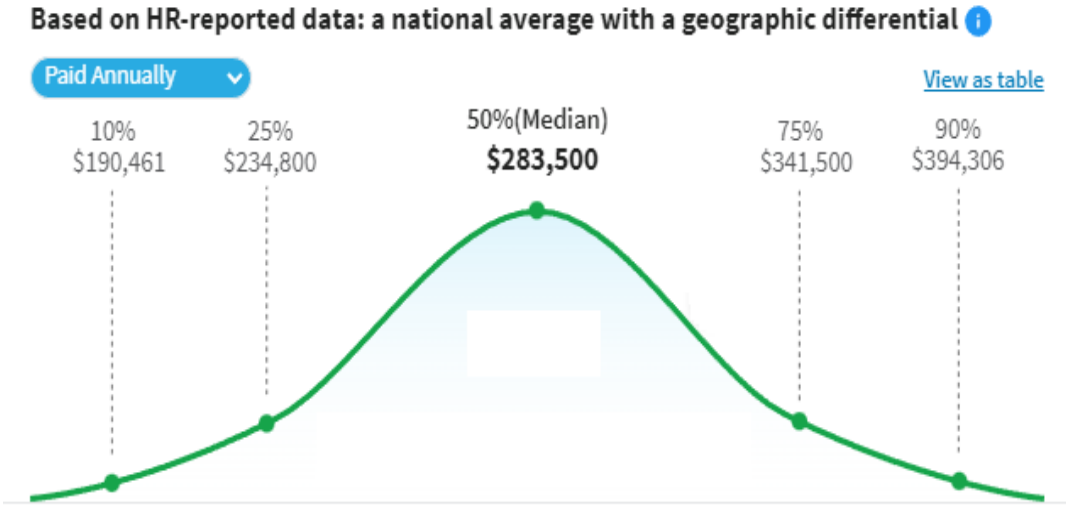
Cyber Security Annual Median Salaries



Network and Computer Systems Administrator:	Information Security Analysts:	Quality Assurance Analysts and Testers:
$84,810	$103,590	$110,140

U.S. Bureau of Labor Statistics, "Occupational Outlook Handbook" (2021)
https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-1

Chief Information Security Officer Salary

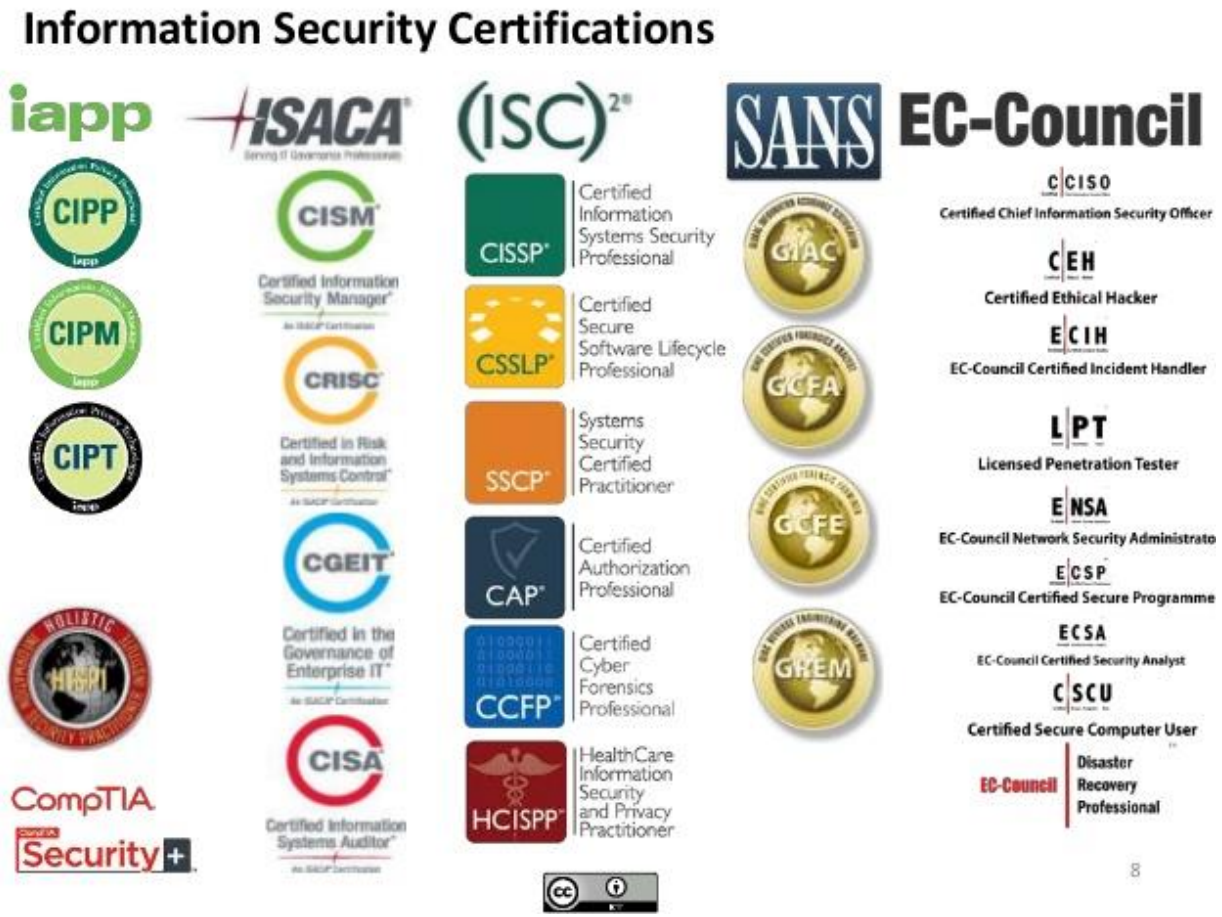


Source: Salary.com Salary Wizard- Do you know what you're worth? | Salary-Calculator | Salary.com

* Holding an active security clearance typically commands an additional 10-20%

Certification

- **Certification Benefits:**
  - Worthwhile
  - Provides needed credibility
  - Meaningful employment selection differentiator
  - Demonstrates proficiency with a body of knowledge
  - Many require practical skills as well
  - Typically required for cyber positions
  - Often provide a pay premium.



CLEARED CYBERSECURITY PAY IN WASHINGTON D.C. METRO

ClearanceJobs.com
A Dice Service

$110,936
Average total compensation

BY CLEARANCE LEVEL

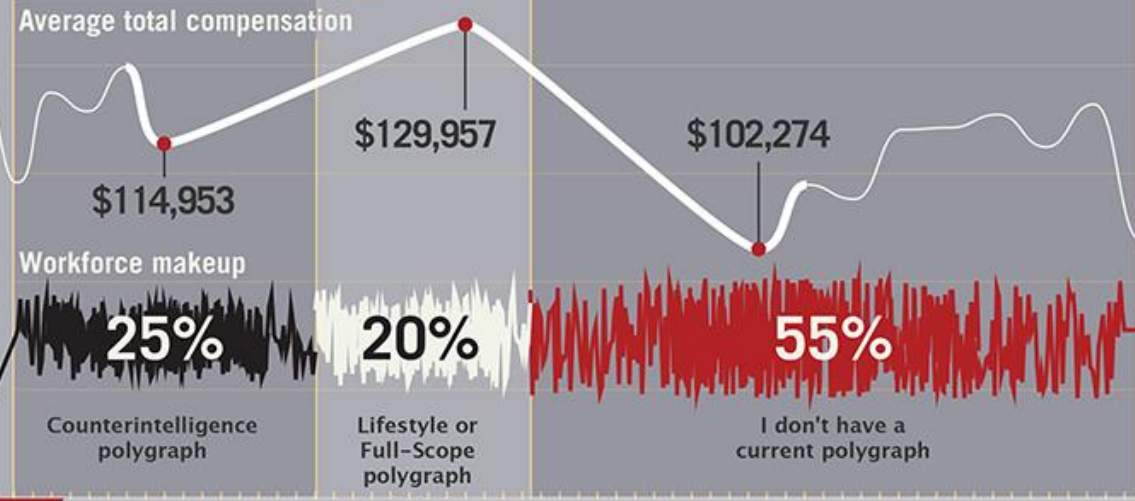
Department of Defense Secret	$86,313
Department of Defense Top Secret	$105,938
Department of Defense Top Secret/SCI	$108,487
Intelligence Agency	$136,246

BY LEVEL OF EXPERIENCE

Average total compensation

BY POLYGRAPH LEVEL

Average total compensation



BY GENDER, AGE AND EDUCATION

Average total compensation

GENDER

AGE

EDUCATION

SOME COLLEGE (2-YEAR)
$94,102 · 19%

STAY OR GO?

Are cybersecurity workers satisfied with their pay?

Survey respondents who expect to change jobs (and/or) employers within the next year

Survey respondents who say they're willing to relocate

A LOOK AT THE AGENCIES

Top five agencies for cybersecurity:

- Department of Defense
- National Security Agency
- Department of Homeland Security

What is the current employment picture?

Who Is Hiring?

The vCISO

Full Experience / Fractional Cost

- Corporations of all types in all sectors across all geographies
- Government Agencies at all levels
- Standards and Regulatory Bodies
- Feds/Eds/Meds & Other Highly Regulated businesses
- Energy, Manufacturing, Agriculture and other top consumers of IoXT
- Industry 4.0 / Digital Transformation Companies
- IT & Security Service Providers (MSPs, MSSPs, CSPs)
- Software Companies
- Assessors / Audit Firms
- Forensics / Incident Responses

What career path advice can you share?

Many Journeys

The vCISO
Full Experience / Fractional Cost

- **Accumulate a Strong Foundation in IT:**
  - Be a power User of PCs, Mobile Devices, Office Suites, Apps, Internet, etc.
  - Networking basics
  - Basic 3rd and 4th generation coder
  - Vocabulary.
- **Understand the Business:**
  - Fluency in business (Ops, revenue cycle, BD, etc.)
  - Industry Expertise
  - Project Management
  - People & Process.
- **Provide Value:**
  - Area of expertise
  - Connections (both up and down)
  - Integrity.
- **Real World Experience:**
  - Projects
  - Model Success / Lessons Learned
  - Regulations
  - Delivery Accountability.

TACTICS TO CONSIDER

- Seek a Mentor
- Network with Peers
- Reverse Interviews
- Resume Reviews
- Emphasize Skills
- Promote Right Brain Abilities
- Don't Overlook USA Jobs/CISA
- End Around On Web Submissions
- Use LinkedIn
- Build an App
- Create your own startup

Cybersecurity Resources

The vCISO

Full Experience / Fractional Cost

What about on a personal level?

Other Recommendations

The vCISO
Full Experience / Fractional Cost

- Proprietors who rely on the same computer for both business and personal use should give serious consideration to the following recommendations:
  - Use a **Password Manager** such as Last Pass or Keeper, which comes in both free and premium versions ($3/account/month). Password crackability is now and has always been about entropy (a measure of how difficult a password is to compromise) and this software makes it easier to use longer passphrases that would otherwise be difficult to remember. https://www.lastpass.com/
  - Stop using Google, Bing, Yahoo, or anything like that as your primary search engine and instead download and only use **Duck Duck Go** which neither tracks your activity nor steals your data for their monetization purposes. https://duckduckgo.com/
  - Consider **ProtonMail** instead of Gmail or Exchange. Because these transmissions have full end to end encryption, they cannot be seen by anyone other than the intended recipient(s). https://protonmail.com/
  - Use **The Onion Router (TOR) browser** instead of either Edge or Safari which blocks all sorts of mobile code and plugins that can otherwise be used to compromise devices and transmitted data. You can also install this on mobile phones. https://www.torproject.org/download/

Where can I get more information?

Resources

The vCISO

Full Experience / Fractional Cost

- Ted Talk: Where is Cybercrime really coming from?
  - https://www.ted.com/talks/caleb_barlow_where_is_cybercrime_really_coming_from?referrer=playlist-what_to_know_about_cybercrime
- Ted Talk: Cybersecurity Starts with Honesty and Accountability
  - https://www.ted.com/talks/nadya_bartol_better_cybersecurity_starts_with_honesty_and_accountability
- Cyber Hygiene 101 for SMBs
  - https://www.fdd.org/wp-content/uploads/2021/07/Cyber-Hygiene-101-for-Small-and-Medium-Sized-Businesses.pdf
- SBA: Stay Safe From Cybersecurity Threats
  - https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats
- FTC: Cybersecurity for Small Business
  - https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity
- Securing Your Home Network
  - Beware of Uninvited Holiday Guests (On your Network) (cisecurity.org)

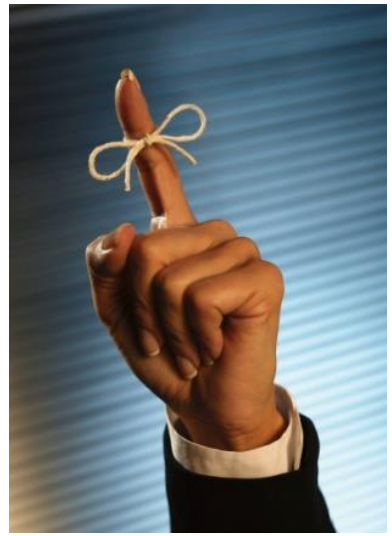
Summary & Conclusion

The vCISO

Full Experience / Fractional Cost

Quiz

- **What is our most important asset?**
  - Information
  - Office furniture
  - Company SWAG
  - Teddy the wonder lizard.
- **What is the objective of a good security program?**
  - To satisfy auditors
  - To manage the risk to which our information is exposed
  - To make it hard for personnel to do their jobs
  - To cause headaches and frustration.
- **Upon what does our security posture depend most for success?**
  - Management Commitment
  - Proper alignment of the stars
  - Each and every member of the team
  - Luck.
- **Who should you engage for assistance?**
  - Dear Abby
  - Ghostbusters
  - Magic Eight Ball
  - Your manager, IT/Security, or your CISO.



What are your qualifications to serve?

The vCISO

The vCISO

Full Experience / Fractional Cost

Jason Taule

CCSFP, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPSE, CDPS, NSA-IAM

PRAGMATIC CULTURALLY ATTUNED PROVEN **INFORMATION SECURITY LEADERSHIP**

Jason Taule is an information assurance and cybersecurity industry executive with a record of success who has worked in both the intelligence community and commercial sectors first consulting to Federal agencies and then serving as inside Chief Information Security Officer / Chief Privacy Officer both within Government and at large systems integrators like General Dynamics and CSC.

Mr. Taule's leadership contributions have advanced the science and practice of information security and risk management. With passion and integrity, his communication/interpersonal skills and numerous accomplishments have earned him recognition as Industry Luminary. Ever mindful of the need to balance security with utility, he has successfully adapted security controls in countless real-world implementations; this pragmatism cause many to consider him a voice of reason. His unique background enables him to incorporate both business and technical perspectives in integrated solutions. For example, Mr. Taule helped create the US-CERT, authored various State Data Privacy Laws, led a multi-million dollar global cyber security practice for a large international consulting firm, ran the team responsible for HIPAA complaint investigations for OCR for 3 years, for the last two decades has been a luminary in the US Health IT space supporting numerous OpDivs in DHHS, served as the CISO & VP of Standards for HITRUST, and more recently has been supporting organizations in all industries and geographies grapple with these issues delivering CISO services on a fractional basis.

LinkedIn profile

Mr. Taule is a graduate of the FBI Citizen's Academy, is member of the Homeland Security Preparation and Response Team, Chairs the Advisory Council of the Maryland Innovation Center, is the driving force behind the Maryland Innovation Center's CISO-In-Residence program, sat on the US Health IT Standards Committee's Transport and Security Workgroup and was a White House invitee to the Security Policy Roundtable for the President's Precision Medicine Initiative.

Developed By:

The vCISO
Full Experience / Fractional Cost

The vCISO appreciates the opportunity to partner with you and welcomes any questions you may have.

The vCISO

20 Windflower Court
Reisterstown, MD 21136
(410) 340-5385
Jason.taule@comcast.net