Inside the Cyber Trenches:
A vCISO's Perspective on Cyber Realities

Jim Ambrosini, CISA, CISSP, CRISC

Who's Jim?

- With over 25 years of experience in Information Security Consulting, Jim has worked with clients spanning the Middle-Market to the largest companies in the world performing a wide array of services from strategy to breach response.
- He currently works for CompassMSP, a leading security and IT provider, serving as a virtual CISO (vCISO) for multiple organizations. CompassMSP, an IT managed services provider, helps SMBs align technology with their business objectives to achieve growth.
- He has worked on several high-profile security breaches for NYPD and State Attorneys General, as well as established global security functions. His faithful dogs, Champ and Max, keep him company as he helps keep companies safe.

PART 1

Working as a vCISO

What is a vCISO?

Being a security leader
involves many types of skills:

- Business Executive
- Team Lead
- Project Manager
- Consultant
- and Coach





A Day In the Life of a vCISO

What I Think I Do

Saving the world through security governance and risk management.

What Friends & Family Think I Do

"Jim is like a cyber hacker or something"

What I Really Do

Research solutions.
Lead client meetings.
Drink lots of coffee.

A **virtual chief information security officer (vCISO)** performs the same duties and responsibilities as a traditional chief information security officer (CISO) who is employed full-time but works on a ***part-time*** basis.

Managing Multiple Clients

Simplify Everything

- Eliminate useless meetings
- Good enough is good enough
- Use project management tools (software, tasks, Scrum boards, etc.).

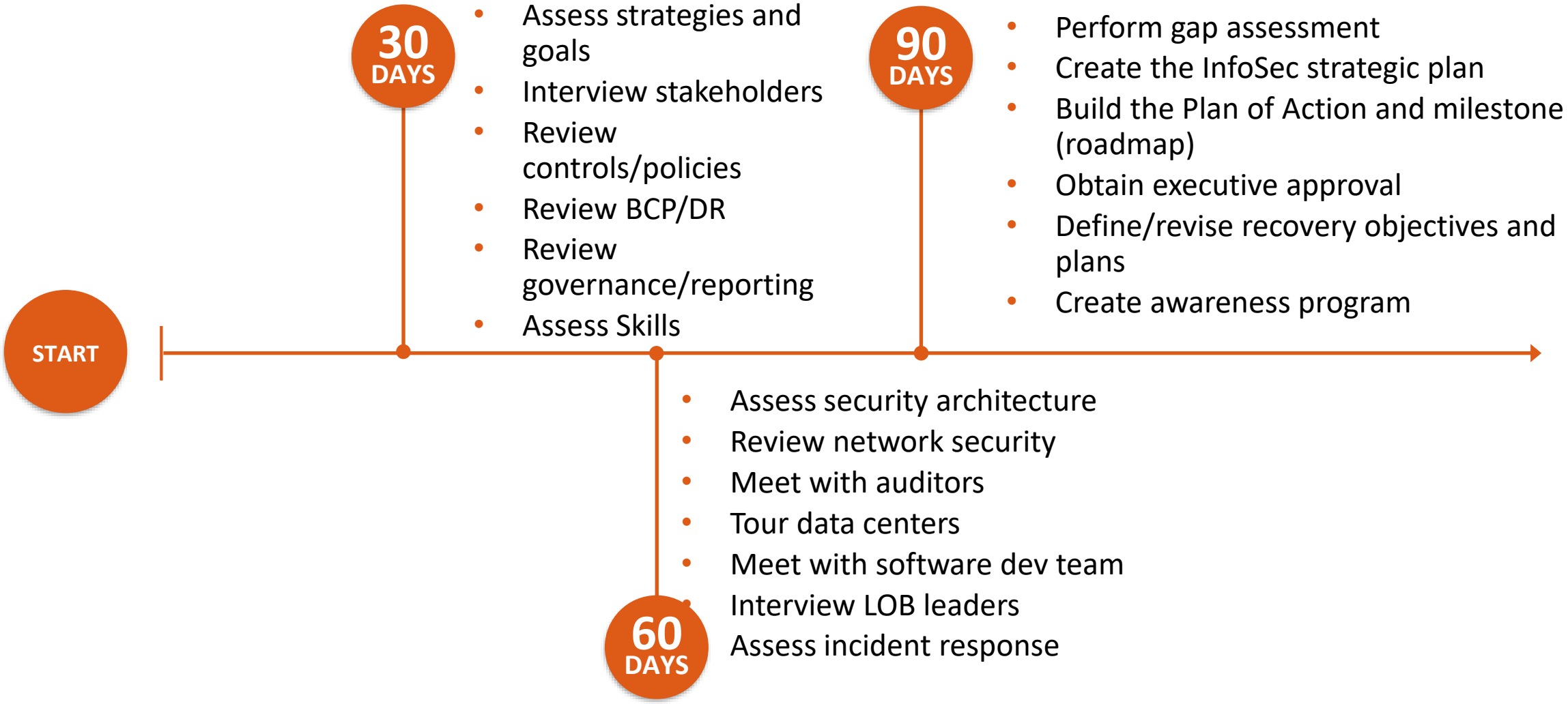
Reuse Everything

- Make templates
- Organize all previous work (frameworks, research papers, deliverables, etc.)
- Phone a colleague – leverage their knowledge

Get Creative

- Chat GPT
- Presentation Software
- Block out “Thinking Time”

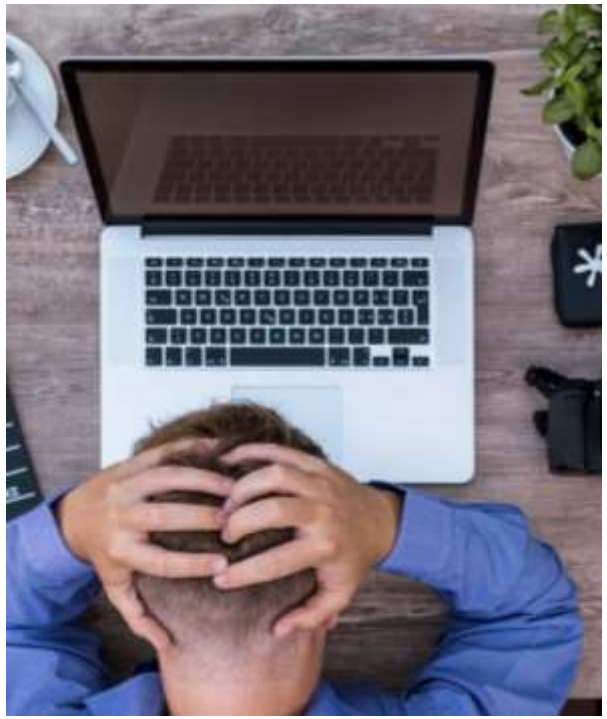
90 Day Plan: Provides an Actionable Roadmap



PART 2

Realities & Perspectives

CISO Burnout—a Very Real Phenomenon



52%

of cyber professionals feel burnt out in current job role[1]

↑

burnout rates are higher in cyber than many other industries[2]

69%

of cybserecurity professionals considered quitting due to burnout[3]

How to Handle

1. Warren Buffets 5/20 system (aka 'Big Rocks')
2. Leverage - what can I improve 10% that would yield the greatest impact?
3. Mindset and Perspective

[1]Source: Indeed, "Cybersecurity Trends - The Escalating Cyber Talent Gap".
[2]Source: NIST "Workforce Framework for Cybersecurity".
[3]ISSA and Enterprise Strategy Group: "The Life and Times of Cybersecurity Professionals"

What I'm Seeing - Lots of Careless Risk

Poor Controls

1. Weak passwords
2. No Defense in Depth
3. Lacking advanced solutions (EDR/ Threat Detection)
4. Fragmented solutions

Lack of Governance

1. No real way to monitor the success of IT
2. Lack of reporting / metrics
3. Outdated policies
4. Not checking if policies are followed

Do NOT Rely on Security Frameworks

It's Like Building an Airplane with the Pre-Flight Checklist

Cyber Frameworks Can't Do the Job

1. Not designed for dynamic socio-technical systems
2. Were based on inventory/accounting controls

Critical/Design Thinking is What's Needed

1. Adopt an engineer's mindset
2. Understand how the system actually works
3. Use Deeming's approach to quality control

Will They Love Me In September as They Did in May?

What to do when bad stuff DOESN'T Happen

Demonstrate Value and Inform

1. Board reporting
2. Prepare like your job depends on it—because it does
3. Always be assessing/testing

Link Cyber to Business

1. Key projects/growth initiatives
2. Safer for customers—how can we capitalize

What Really Happens after a Breach

A tale of a major print outsourcer that got hit with **Ransomware**

Avoid Becoming the CEO of Cyber: Chief EXCUSE Officer

1.

Risk-based analysis and budgeting

2.

Business alignment

3.

Use cyber insurance and customer requirements as leverage

4.

Create awareness

5.

Incorporate security early in the project lifecycle

6.

Be transparent

PART 3

Looking Forward

Predictions by Gartner, March 2023 Risk Conference

Looking Forward

2024

modern privacy regulations will blanket the majority of consumer data, but less than 10% of organizations are using privacy as a competitive advantage.

2025

half of all cybersecurity leaders will have changed jobs, 25% for different roles due to multiple work-related stress

2026

70% of boards will include one member with cybersecurity experience

2027

50% of CISOs will adopt human-centric design practices into their cybersecurity programs to minimize operational friction and maximize controls adoption

UBER—CISO Liability

Case Details

Joe Sullivan, the former security lead at Uber, has been found guilty on two counts related to the cover-up of a data breach that occurred in 2016. This marks what is believed to be the first instance of a company executive facing charges over a cyberattack. The breach impacted the personal data of over 57 million Uber riders and drivers. Sullivan was found guilty of obstructing a Federal Trade Commission (FTC) investigation and concealing a felony from authorities. The charges could lead to a potential prison sentence of up to 8 years.

Questions?