Security, Compliance, and Quantum Entanglement

Wednesday October 25th, 2023
4-5pm ET

TABLE OF CONTENTS

01

Intros & ROE

Kevin Baker

CISO

MCPC & Fortress SRM

CISSP-ISSMP

CRob, n, adj, and v

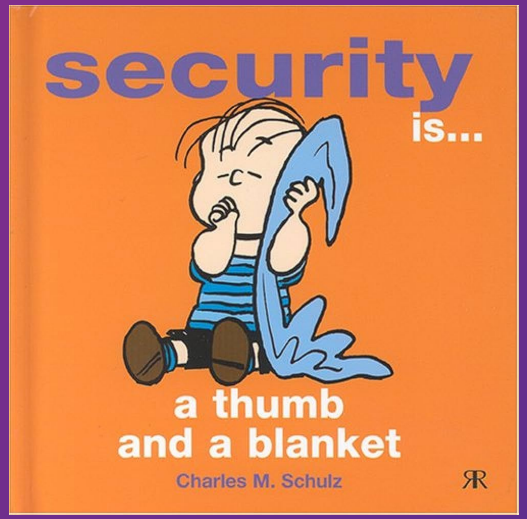
Pronunciation: U.S. (K-rowb)

43rd level Dungeon Master

26th level Securityologist

Pirate-enthusiast & hat-owner

What does “Security” mean?



“Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.”

- CISA -
https://www.cisa.gov/news-events/news/what-cybersecurity

Image source

What does “Compliance” mean?

Compliance - **noun -** com·pli·ance

“conformity in fulfilling official requirements.”

- Merrium-Webster - https://www.merriam-webster.com/dictionary/compliance

02

The Quandary

noun

a state of perplexity or uncertainty over what to do in a difficult situation.

A Tale as old as time....

Image Source

Let me tell you about my program...

Image Source

Quantum entanglement is when...

...two particles can be connected in such a way that a change to one is instantly reflected in the other- no matter how far apart they are.

Einstein called this “spooky action at a distance”

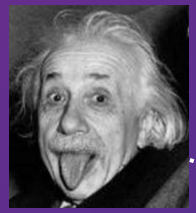


Image Source

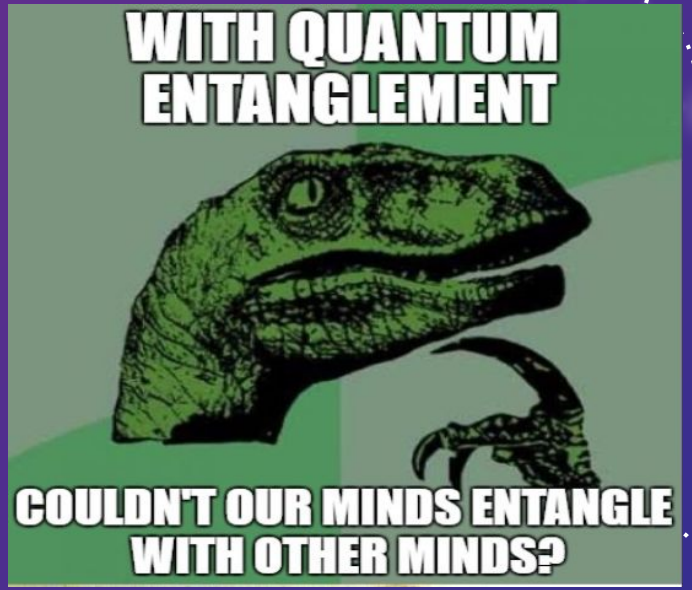


Image Source

We begin with two Programs separated by distinct differences

Compliance is an audit function

Security is ops-focused

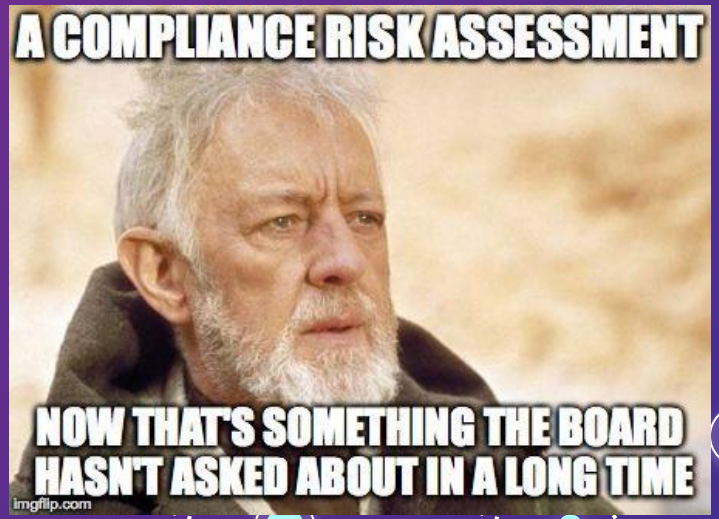


Image Source

Compliance ... has advantages?

Compliance has a voice

BUT...

It may not be saying the right thing

Image Source

Security has advantages too?

Image Source

Operations-focused ;

Works to “keep the lights on”

Security lives in the grey space

“it depends”

Though they are separated they are undeniably connected

Image Source

03

A Range of Possibilities

Factors to consider....

Culture

Does the org provide constructs where these convos can happen? ....or is this left up to ICs “just figuring it out”

Image Source

Personalities

Navigating the many strong personalities within your org and negotiating solutions can be challenging

Image Source

Career paths

People come into these careers from many different origins, experiences, and perspectives

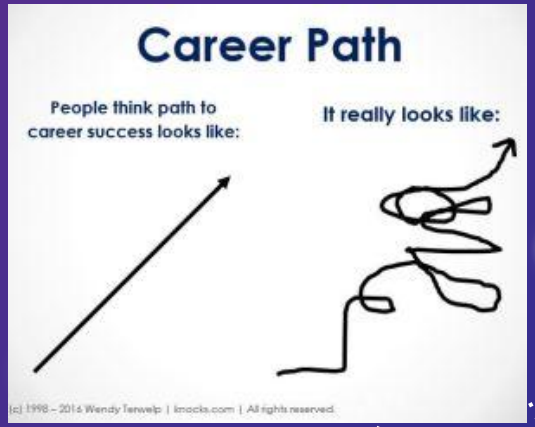


Image Source

But there is one more factor to consider

Security hat + compliance hat

...you still just have one head

Image Source

Image Source

Image Source

Our common mission: FOCUS ON THE RISK

We all can agree that MANAGING RISK IS THE BEST

Stay in YOUR lane - aka let the expert be the expert (which we know is hard to do, especially when your lane may not be defined!)

Image Source

How can COMPLIANCE help us be more SECURE

Comply with this simple advice

- Typically has a seat at the Boardroom table, while Security may not. Armed with good data, Compliance can be a powerful voice to “the Business” to help manage risk
- Typically has a feel for the current state of Regulations & reporting requirements

How can SECURITY help us be more COMPLIANT

Secure your spot for success

- Risk Management & Risk Ranking can help target specific things before they become problems
- Documentation (esp. Processes & Policy/Standard/Guidelines) + Logs/evidence = <3
- Security is more in tune with current threats, and can inform of potential new areas for forthcoming compliance
- Typically will know “where the bodies are buried” (aka - where controls or practices may be weaker) and can partner with teams like I.A. to focus in and improve on those areas before they become problems

Tangled together

Image Source

Because you can’t see it or totally understand it does not mean it is not true

You can’t do it alone

04

The Questions

And some answers!

Thanks!

Q&A

kbaker@fortresssrm.com

Kevin linkedin

CRob_at_Intel_dot_com

~~@SecurityCRob~~

@SecurityCRob@infosec.exchange

https://github.com/SecurityCRob

The Security Unhappy Hour, Chips & Salsa

https://www.linkedin.com/in/darthcrob/

05

Resources

The Problem....

Image Source

Some “fun” facts...

- Nearly 1 billion emails were exposed in a single year, affecting 1 in 5 internet users.
- Data breaches cost businesses an average of $4.35 million in 2022.
- Around 236.1 million ransomware attacks occurred globally in the first half of 2022.
- 1 in 2 American internet users had their accounts breached in 2021.
- 39% of UK businesses reported suffering a cyber attack in 2022.
- Around 1 in 10 US organisations have no insurance against cyber attacks.
- 53.35 million US citizens were affected by cyber crime in the first half of 2022.
- In 2020, malware attacks increased by 358% compared to 2019.
- The most common cyber threat facing businesses and individuals is phishing.
- A hacker accessed and attempted (unsuccessfully) to poison the water supply in Oldsmar, Florida, in February 2021. (Wired, 2021)
- The first reported death by ransomware occurred in September 2020, when a ransomware attack caused IT failure at a hospital in Düsseldorf, Germany. (Associated Press, 2020)

Sources - AAG & Norton

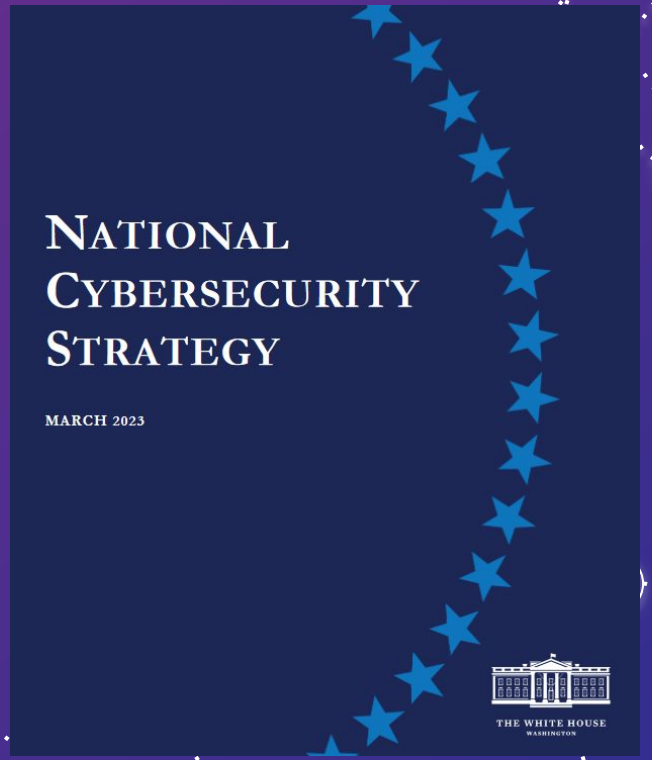
Security is AWESOME because...

Focused on Detecting, Preventing, and Remediating Threats

- Practically unlimited growth potential - the learning never stops (yay?)
- Plenty of variety - 50 cybersec job titles
- Ability to solve puzzles (aka complex business problems)
- Job has REAL impact - Protecting people & organizations is hugely rewarding (personally in addition to financially!)

More than 755,743 cybersec job openings in the US alone(as of Feb2023)
That number rises to over 3.5 Million Global openings (April 2023)

Source: TechBeacon



Do you recall seeing a "National Compliance Strategy?"

Communication technique is key

← talk different languages →

Compliance audience: *Business/Regulators*

Technical jargon is a determinant here, have to stay conceptual

Slow and steady (Laws & Regs infrequently change)

Security audience: *Technical*

Conceptual level a start, but focuses on specifics of implementation

Fast pace, balance of strategy and tactical agility to react

Image Source

Image Source