



CISO

Chief Information Security Officer

**2020: The Threats and
Opportunities Facing Today's
Security Leaders**

OR

**The Job Sucks, But You Still
Want To Be A CISO, Don't You?**

DIFFERENCES IN THE CYBER THREAT LANDSCAPE

YEAH BABY....?

Chief Information Security Officer

[Methodology](#)

10016, New York, NY

Median Salary + Bonus **\$240,216**

10% \$148,513 25% \$192,215 75% \$306,708 90% \$367,245

? **Projected Salary Unknown**

Chief Information Security Officer

[Methodology](#)

San Francisco, CA

Median Salary + Bonus **\$248,773**

10% \$153,803 25% \$199,062 75% \$317,633 90% \$380,326

? **Projected Salary Unknown**



CHA-CHING



OG



Russian Central Bank Admits
\$6M SWIFT Attack

DDOS Attacks on
Top Banks

NYT, WSJ, and Washington Post
Claim to be Hacked

OPM Breach – Spies
in Government Data

DNC hacked, posted on
WikiLeaks

Criminal Ring Steals
Millions of Identities

Equifax, Uber and Target
all taken down by hackers



YOU'RE FIRED!



CISO

**The
Boss**

WE FEEL THE OFFICE SCAPEGOAT IS A
KEY COMPONENT OF TEAM-BUILDING,
AND YOU'RE A GREAT FIT FOR THE JOB.

**Today's Security
Leader/ CISO**



It sucks to be you....

**A HISTORY OF SECURITY THAT
LED US TO....**

...COMPLIANCE????!

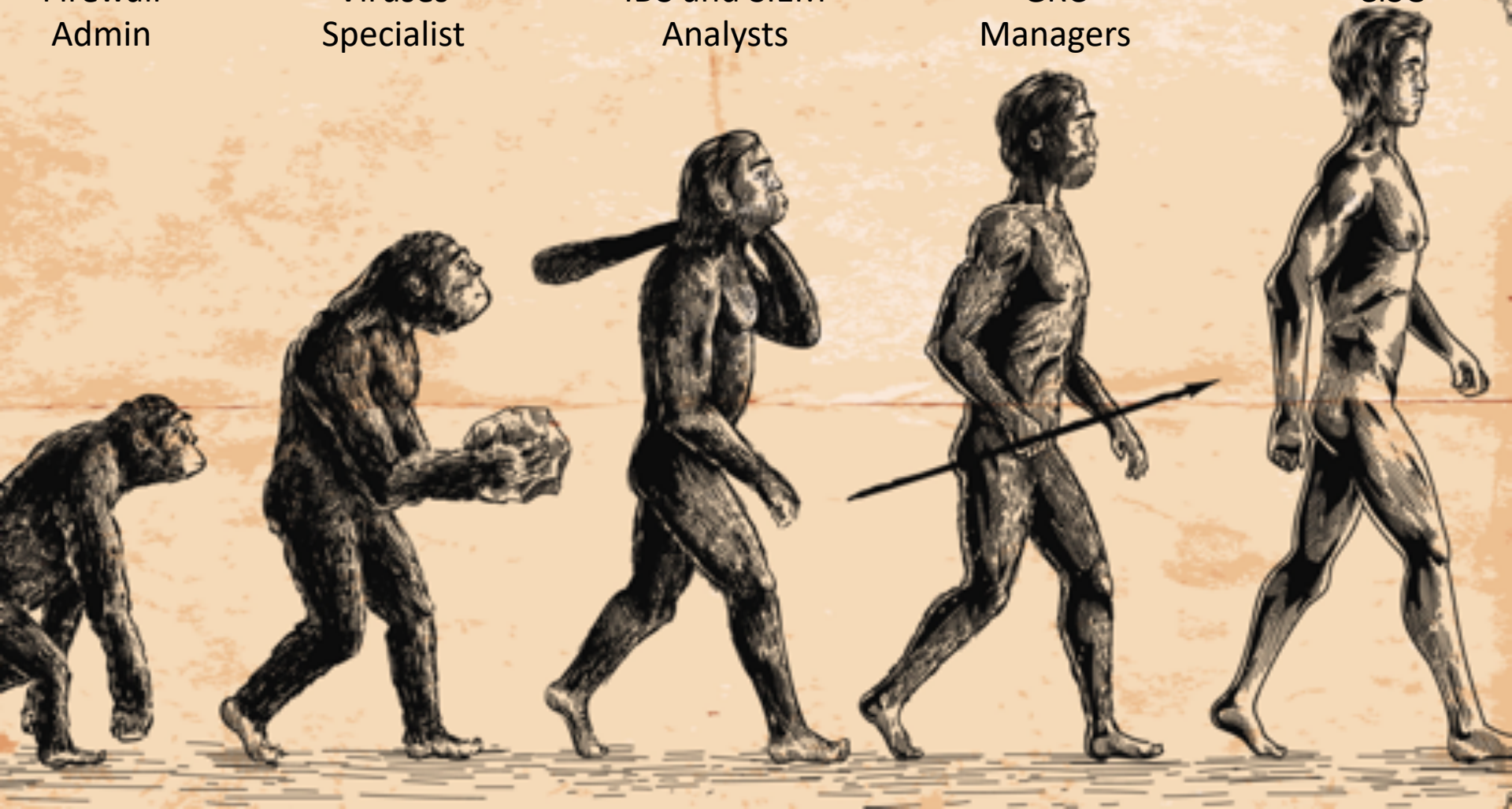
Firewall
Admin

Viruses
Specialist

IDS and SIEM
Analysts

GRC
Managers

CISO



Certified EU GDPR Foundation Online

C GDPR F

ACREDITED
IBITG

The **NEED** to **KNOWS**
for **SECURITY MANAGERS**

a 10 part series to securing your organization

[Subscribe Now](#)

ISO 17024:2012 certificated and IISP accredited



CC(GRC)P

Certified Cyber (Governance Risk and Compliance) Professional

From Technologies to Solutions

CISSP in 21 Days

Boost your confidence and get a competitive edge to crack the exam

M. L. Srinivasan

PACKT
PUBLISHING



Space Rogue
@spacerog

[Follow](#)

Social Media Security Professional? Is that the cert I need to be a security expert on twitter? is.gd/chKy9j via @attritionorg

[Reply](#) [Retweet](#) [Favorite](#)

Covers latest CISSP exam changes

CISSP
FOR
DUMMIES

So much better than clown school

CompTIA backs down; past certs remain valid for life

CompTIA has reversed course—existing holders of an A+, Network+, or Security+.



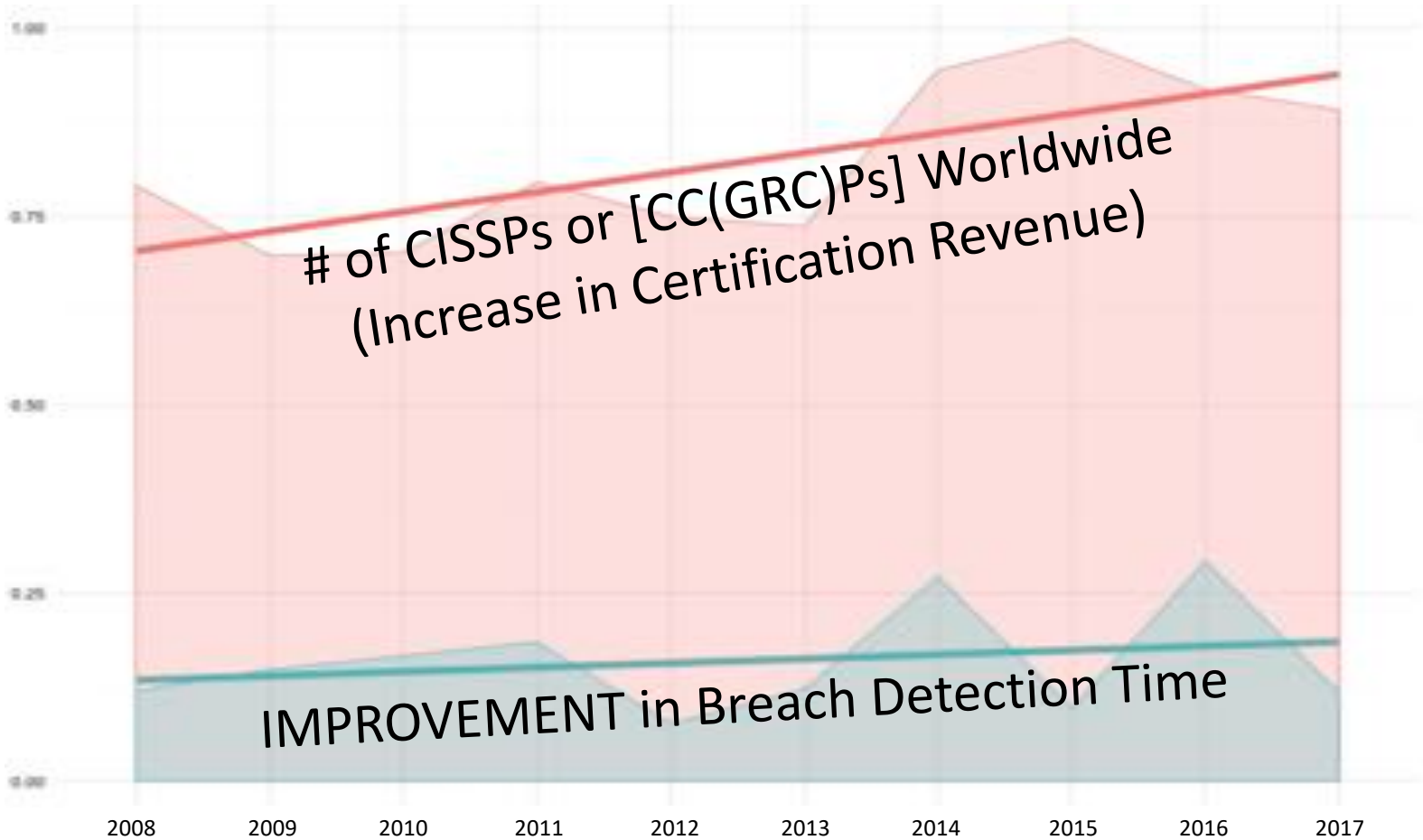
Want to be the best at what you do?
Just **Concentrate**.

View the CISSP Concentrations domain webcasts.

CISSP Architecture **CISSP** Engineering **CISSP** Management

[Watch](#)

2018 Big U.S. Telecom Company Breach Report



of CISSPs or [CC(GRC)Ps] Worldwide
(Increase in Certification Revenue)

IMPROVEMENT in Breach Detection Time



AUDIT CHECKLIST



Audit Satisfactory



**Nonconformances Found
Observations Made**





ISO
27001



....is to SECURITY



....is to BEING FUNNY

You have a funny costume, but there's no guarantee anyone's going to LAUGH...

Указ Президента Российской Федерации
от 05.12.2016 г. № 646

Об утверждении Доктрины информационной безопасности
Российской Федерации



FAIR
Factor Analysis
Information Risk



$$\text{Risk} = \text{Threats} \times \text{Assets} \times \text{Vulnerabilities}$$





IGNORANCE

Sometimes it's best just not to know.



COMPLIANCE

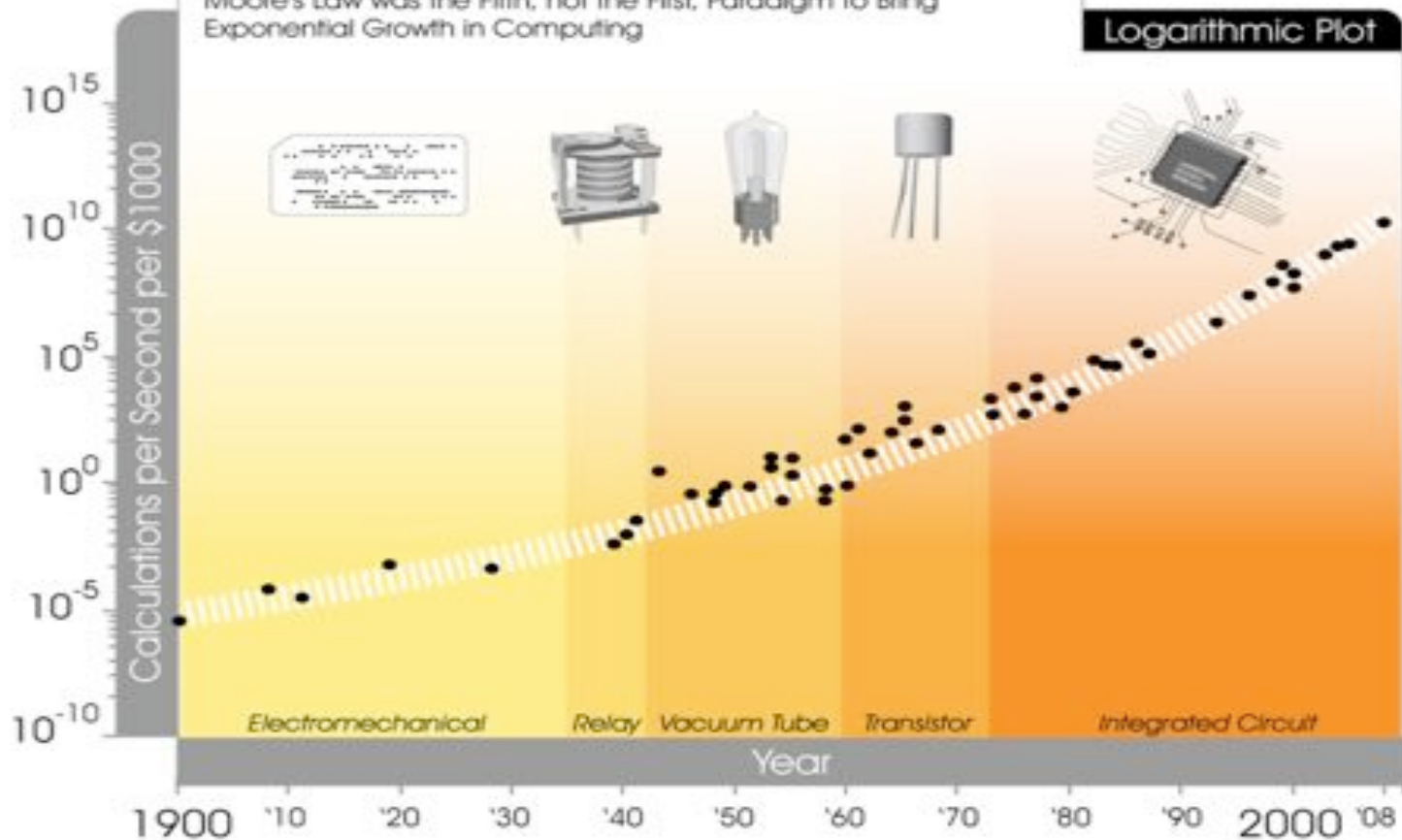
But What's REALLY Different?

Exponential Business Impact!

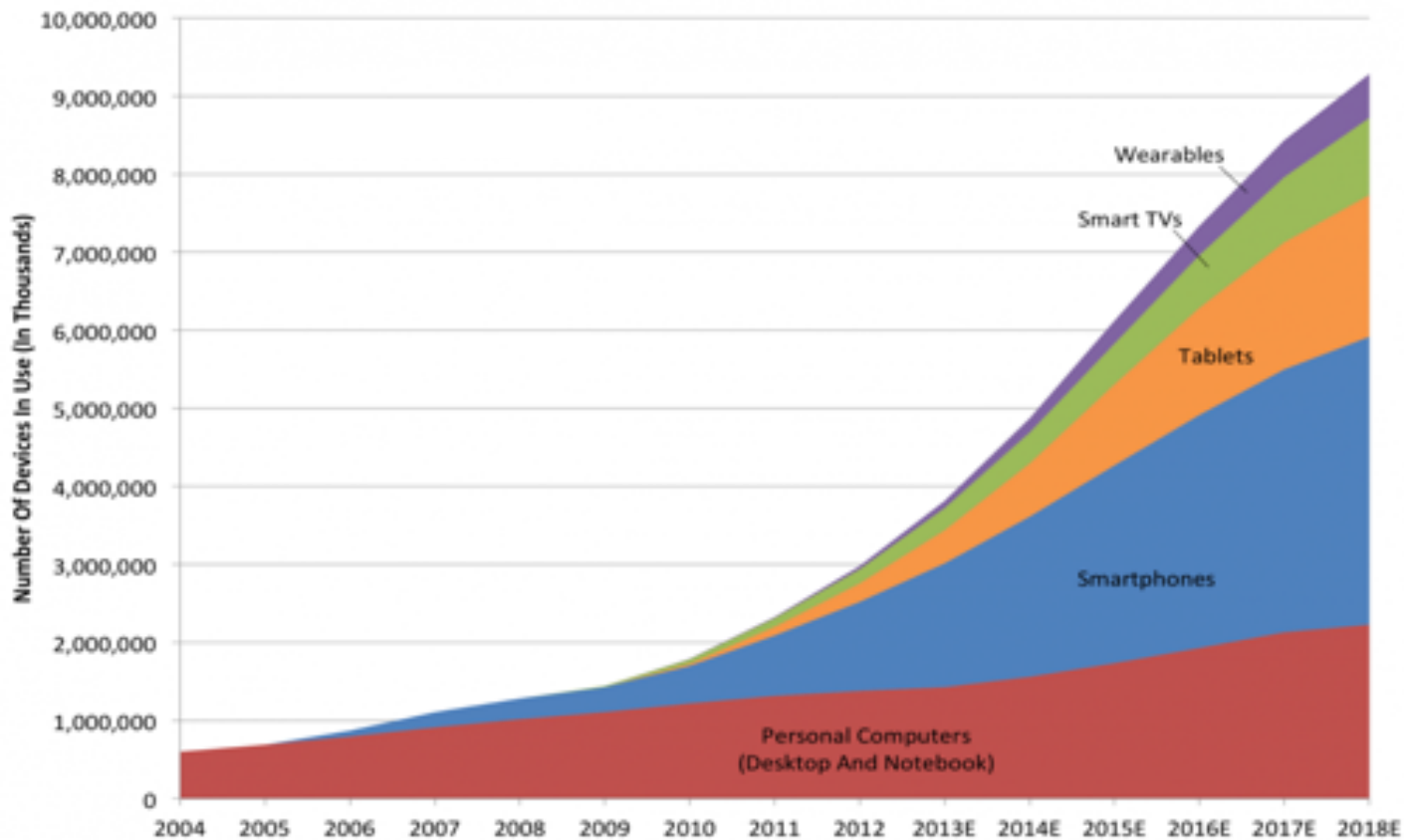
Exponential Growth of Computing for 110 Years

Moore's Law was the Fifth, not the First, Paradigm to Bring Exponential Growth in Computing

Logarithmic Plot



Global Internet Device Installed Base Forecast

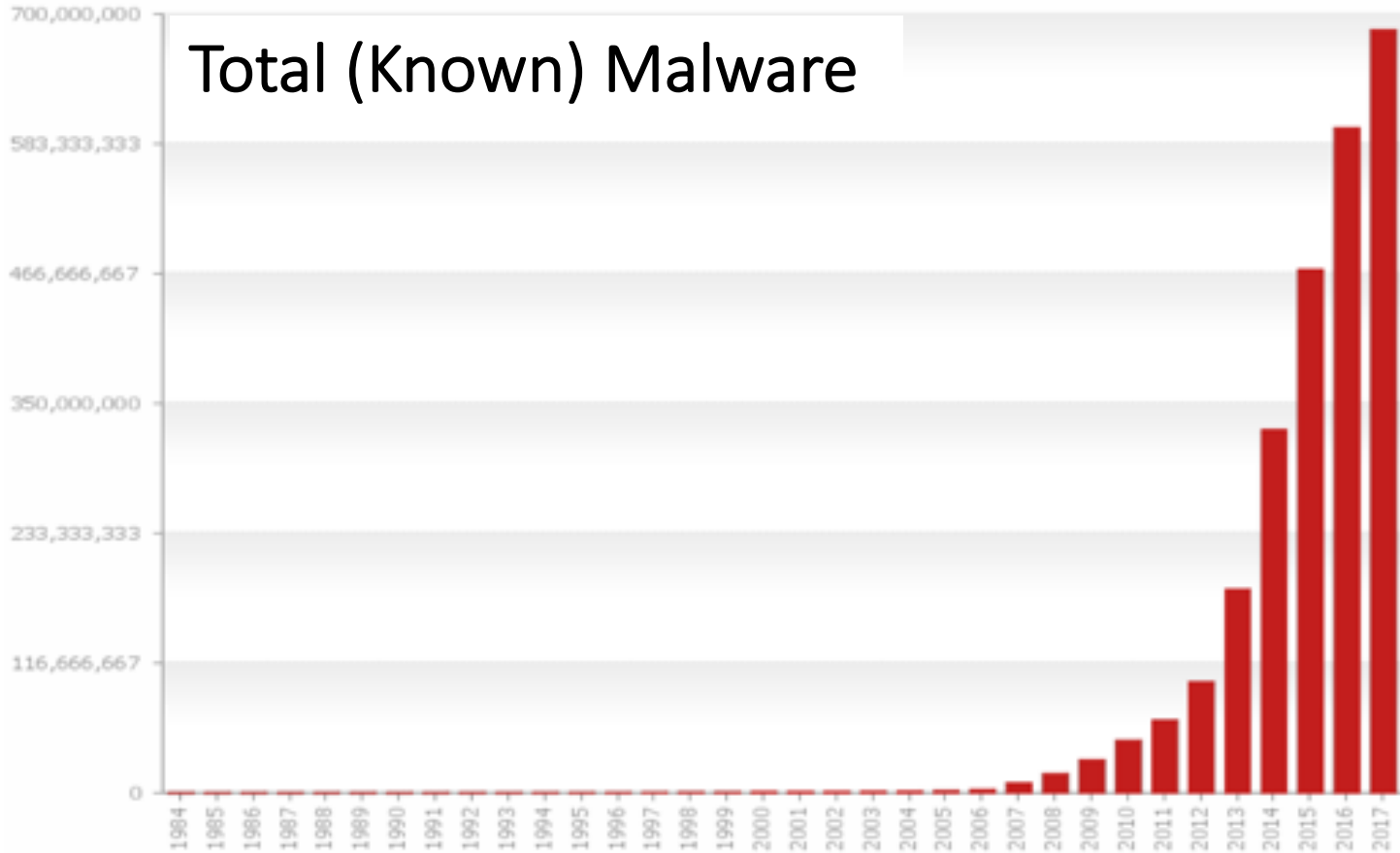


Source: BI Intelligence Estimates

$\mathcal{L} = \oint E \cdot t$
 $f(\omega) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i x \omega} dx \frac{dt}{d\theta}$
 $\nabla \cdot E = 0$
 $\nabla \times E = -\frac{1}{c} \frac{\partial H}{\partial t}$
 $\nabla \cdot H = 0$
 $\nabla \times H = \frac{1}{c} \frac{\partial E}{\partial t}$
 $i \hbar \frac{\partial}{\partial t} \Psi = H \Psi$
 $\rho \left(\frac{\partial v}{\partial t} + v \cdot \nabla v \right) = -\nabla p + \nabla \cdot T + f$
 $H = -\sum p(x) \log p(x)$
 $+ \sum_{i=1}^n \frac{q_i}{2} H_i^M + C_s \frac{D}{Q} + C_0 D + \frac{Q(p-D)}{2p} H^M + F_0 N + F_0 N + \sum_{i=1}^n D_i \cdot w_i \cdot d_i \cdot \left(\frac{1+w_i}{F_r} \right)$
 $\frac{1}{2} G^2 S^2 \frac{\partial^2 v}{\partial s^2} + S \frac{\partial v}{\partial s} + 2v$
 $TC(Q, q_i, m_i) = \sum_{i=1}^n \left[\frac{1}{m_i} S_i + C_s D_i + \frac{1}{2} \left(m_i \left(1 - \frac{1}{p_i} \right) - 1 + 2 \frac{D_i}{T_i} \right) \right]$
 $\cos(2.5 \sin(\theta)) \cos(\theta)$
 $\frac{d \Delta p(s, \phi)}{d \phi} = \begin{bmatrix} \gamma & -\beta \\ -\beta & 0 \end{bmatrix} \begin{bmatrix} \Delta p(s, \phi) \\ \Delta M(s, \phi) \end{bmatrix}$
 $\int_0^{\pi/2} (\log \sin x)^2 dx = \int_0^{\pi/2} (\log \cos x)^2 dx = \frac{\pi}{2} \left\{ \frac{\pi^2}{12} + (\log 2)^2 \right\}$

= 31 billion by 2020

Total (Known) Malware



Last update: 10-20-2017 06:21

Copyright © AV-TEST GmbH, www.av-test.org

Total (Known) Android Malware

- Malware Applications Overall
- New Malware Applications

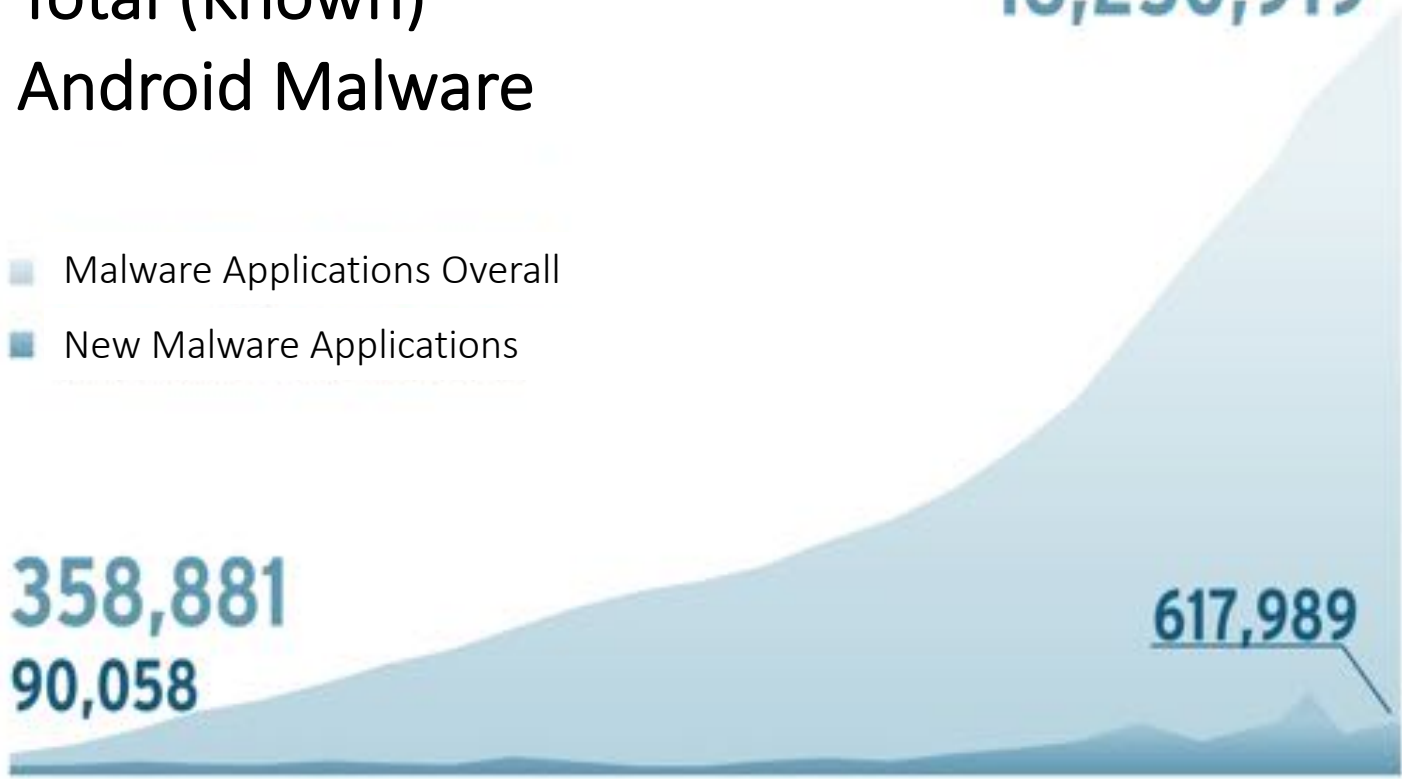
358,881
90,058

January 2013

18,250,919

617,989

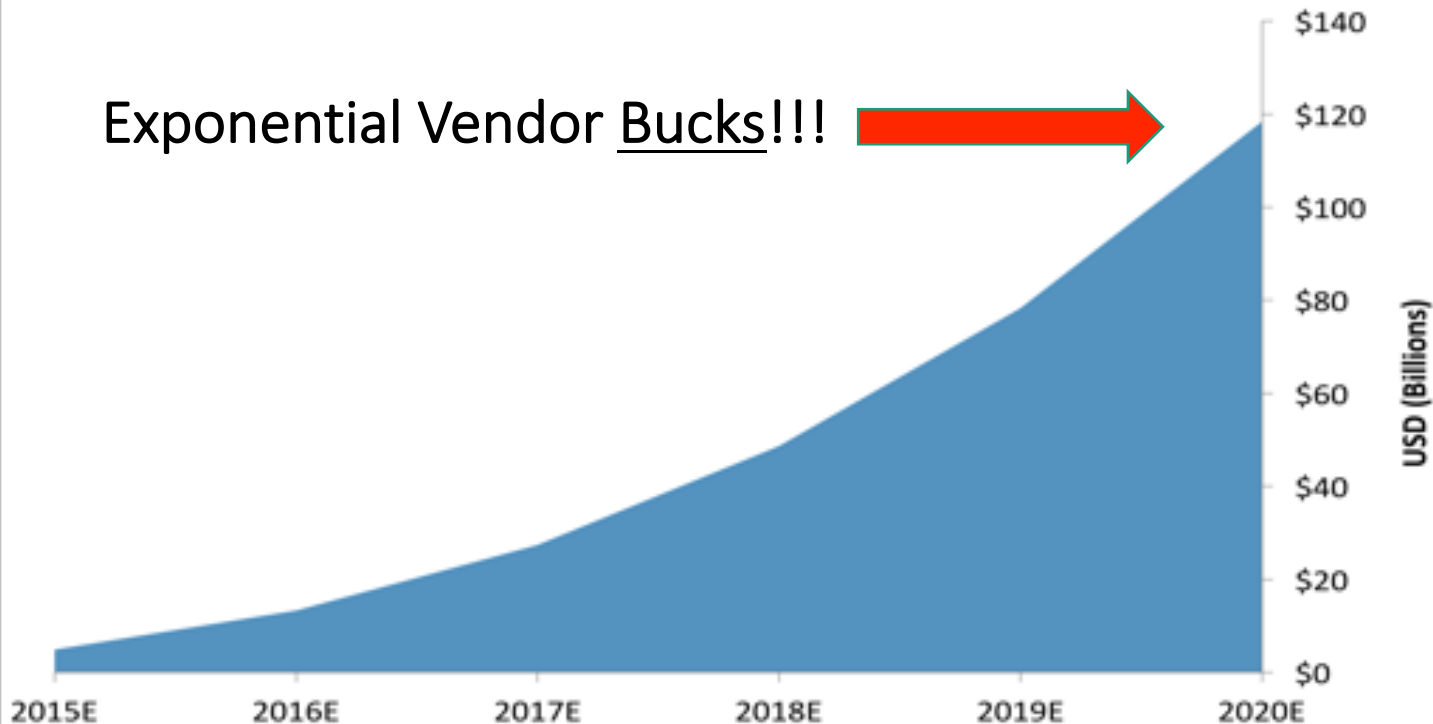
February 2017



Estimated Internet Of Things Cybersecurity Market

Global compounded (2015-2020)

Exponential Vendor Bucks!!!



Source: BI Intelligence Estimates, 2015



**ISO Class 5 Cleanroom Facilities
Exclusively Used**

Ukrainian blackout caused by hackers that attacked media company, researchers say

Power company suffered a major attack that led to blackouts across western Ukraine, after an attack on a Ukrainian media company



☒ Smokestacks in Dniprodzershynsk, Ukraine. Photograph: John Mcconnico/AP

Four Cyber Attacks On UK Railways In A Year

A security experts says the hackers could create "real disaster related to train safety".



Video: Sky News has learned that the UK railway network has suffered at least four major cyber attacks over the last year alone.



Massive flaw could give hackers full control of critical infrastructure

Physical Impacts as the Result of Cyber Efforts...

...Exponential Impacts

SEEING BEYOND VENDOR HYPE

**a.k.a.: pwnd by sales &
procurement people**

FEAR



UNCERTAINTY



DOUBT





OG

FAIL





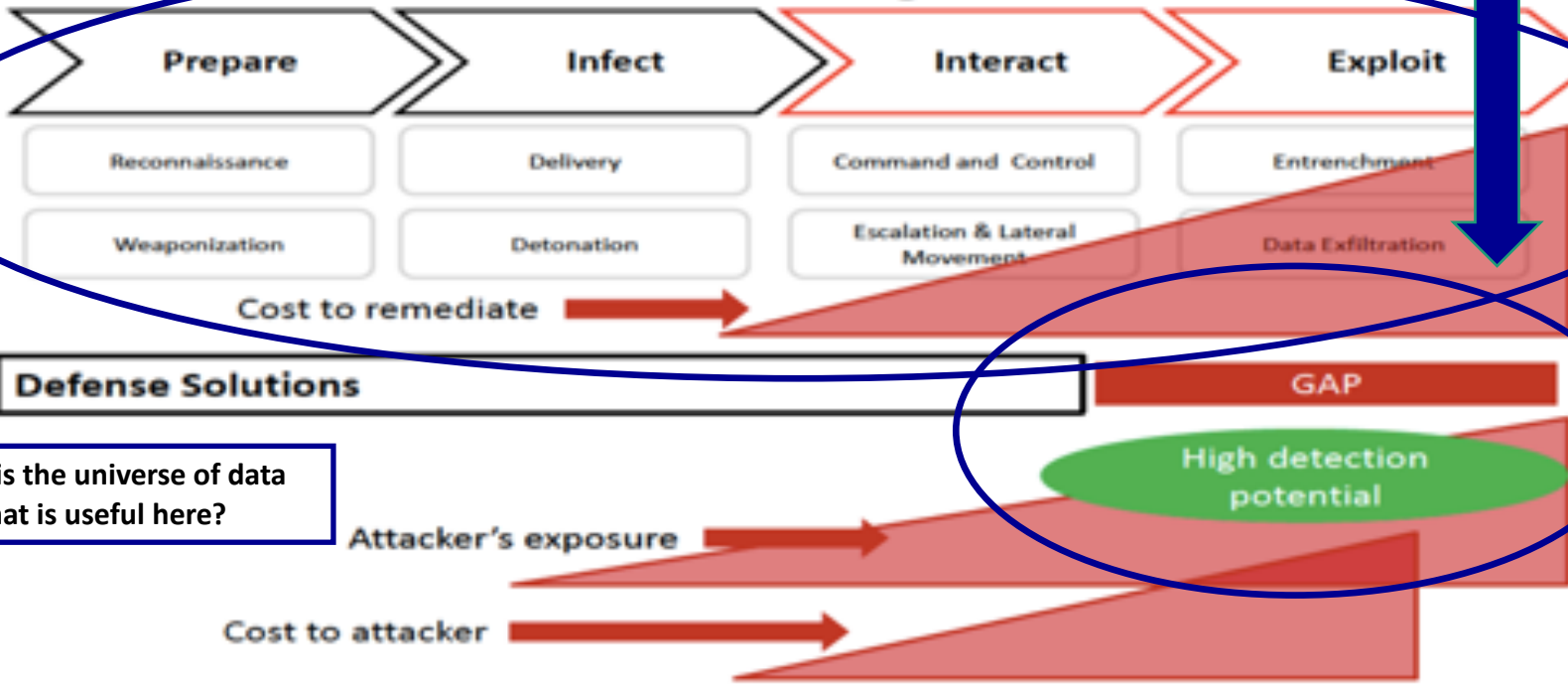
f





Enter the KILL CHAIN, etc.

APT Attack Progression



What level of resources belongs RIGHT HERE??

What is the universe of data that is useful here?

Artificial Intelligence DRIVEN Security

Key Constraints of AI Historically in Cyber Security:

- Costs of Storage
- Limits of Computing Power
- No HUMANS to Figure Out the Use Cases / Code

Opportunities for Growth in AI:

- Costs of Storage Are Exponentially Decreasing (Collect)
- Computing Power is Exponentially Increasing (Analyze)
- Extensive interest in China and the US



One Page 2018 Report to Global CISOs from the CEO Committee Studying Corporate Security Team Metrics Relative to Data Breach Prevention



THREAT INTELLIGENCE

Don't Leave Home Without It



Good Intelligence is Good if You Can Get It!

Tracking my cookies?

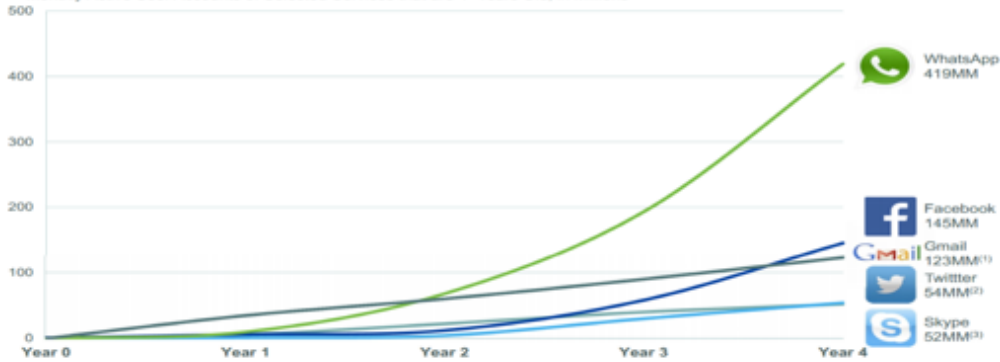
An elderly woman with short, curly white hair and glasses is sitting at a desk. She is looking intently at a laptop screen, with her right hand raised to her forehead in a gesture of concern or suspicion. She is wearing a light blue patterned blouse. The background is a plain, light-colored wall.

**They will never get my
recipe!**

WhatsApp Extraordinary Growth in Users

First Four Years Growth after Launch

Monthly Active User Accounts of Selected Services that are 4+Years Old, in Millions

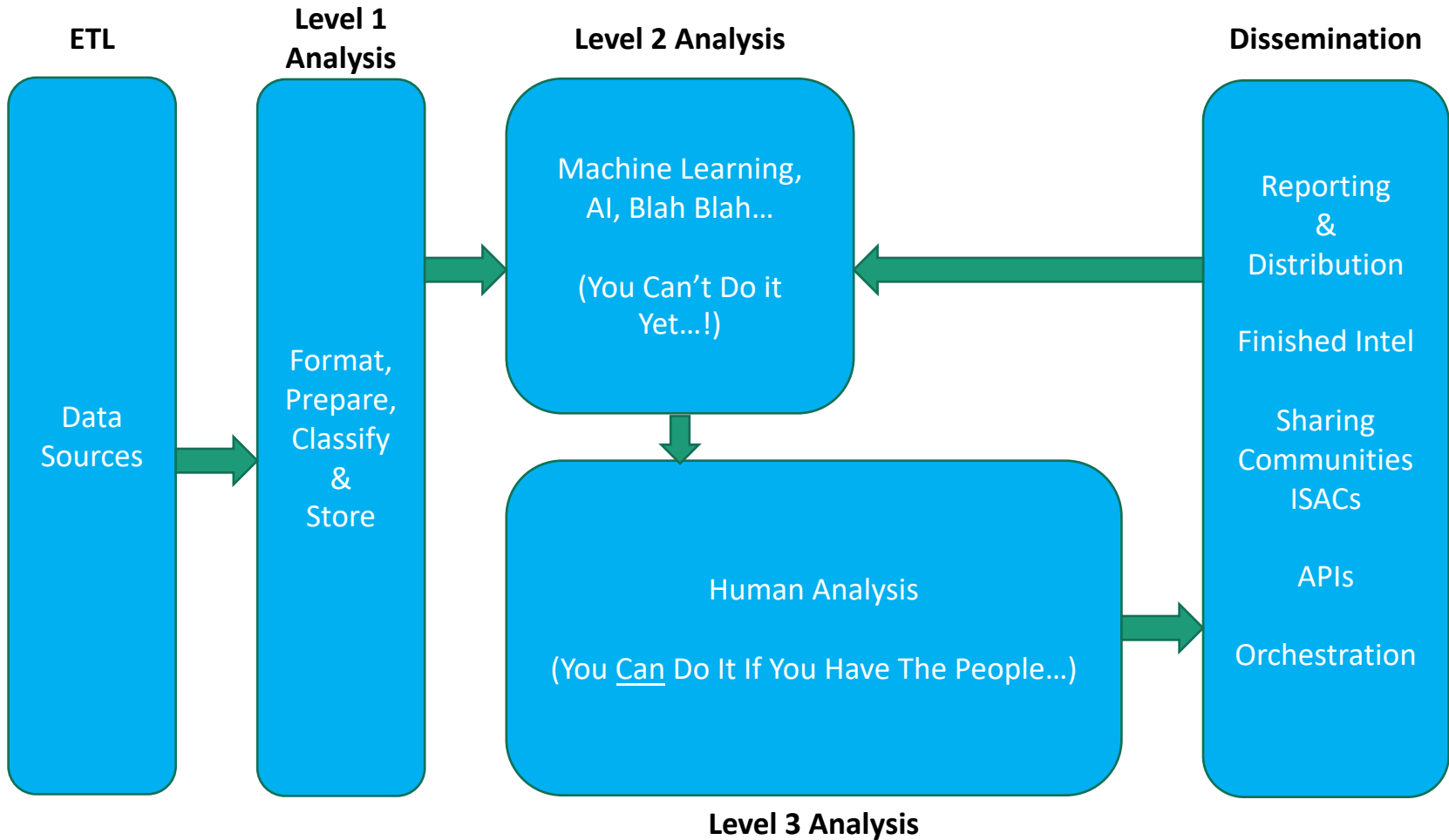


Source: (1) comScore Media Matrix
(2) comScore Media Matrix, news, and company filings
(3) News and company filings in addition to estimates derived from these sources

WhatsApp

facebook





FROM HACKER TO CISO

How to Speak the Language of
Business...

*Securing Solaris, Mac OS X,
Linux & FreeBSD*

3rd Edition
Essentially Revised
Over 250,000 copies in print

Practical Unix & Internet Security



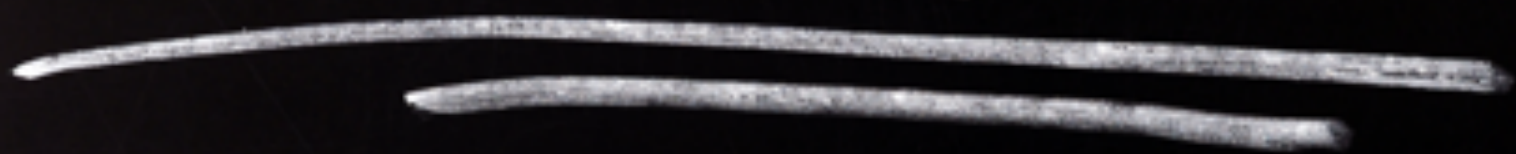
O'REILLY

Simson Garfinkel, Gene Spafford & Alan Schwartz

OG

POP

QUIZ!





Good Luck

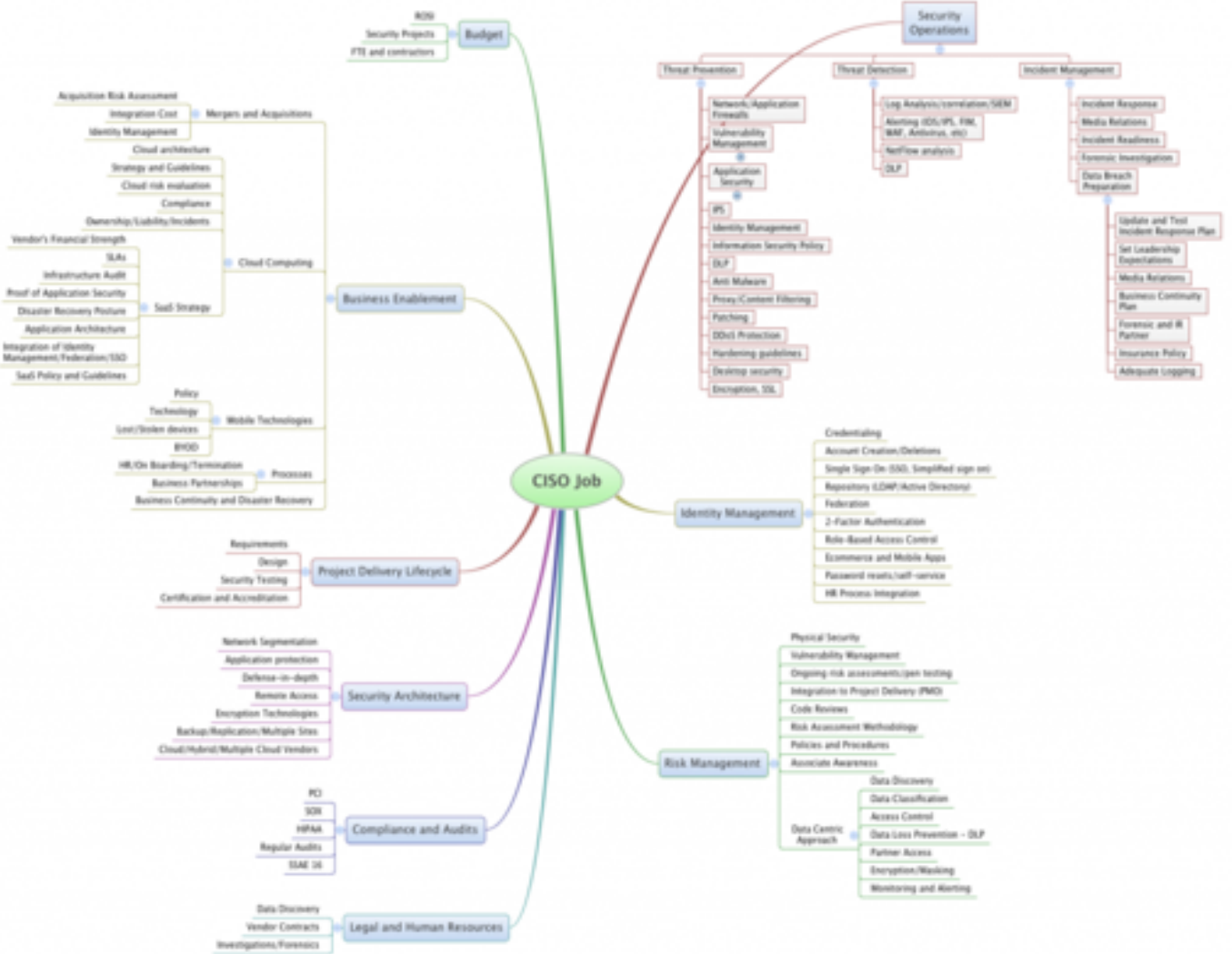


\$

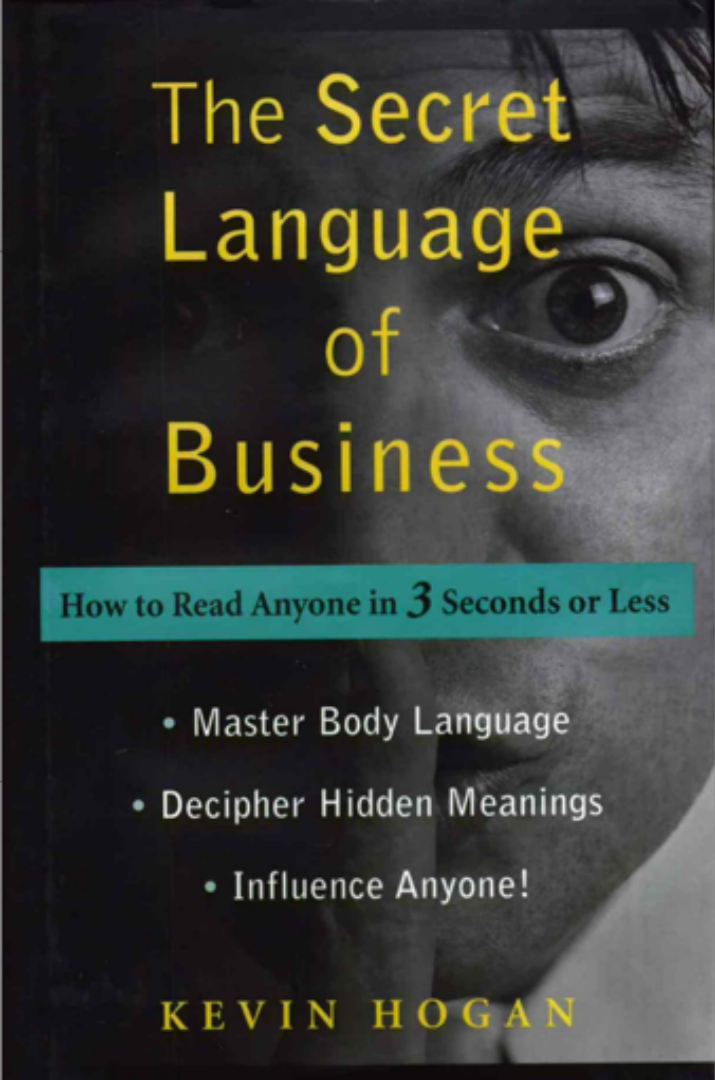
\$\$\$\$\$

Evolution of the CISO to the CIRO





“ Too frequently, infosec professionals speak in terms of threats or vulnerabilities or technology. They need to learn to speak in terms that business leaders understand, and the one thing they understand is risk. ”



The Secret Language of Business

How to Read Anyone in 3 Seconds or Less

- Master Body Language
- Decipher Hidden Meanings
 - Influence Anyone!

KEVIN HOGAN



Your Cyber
Security Program

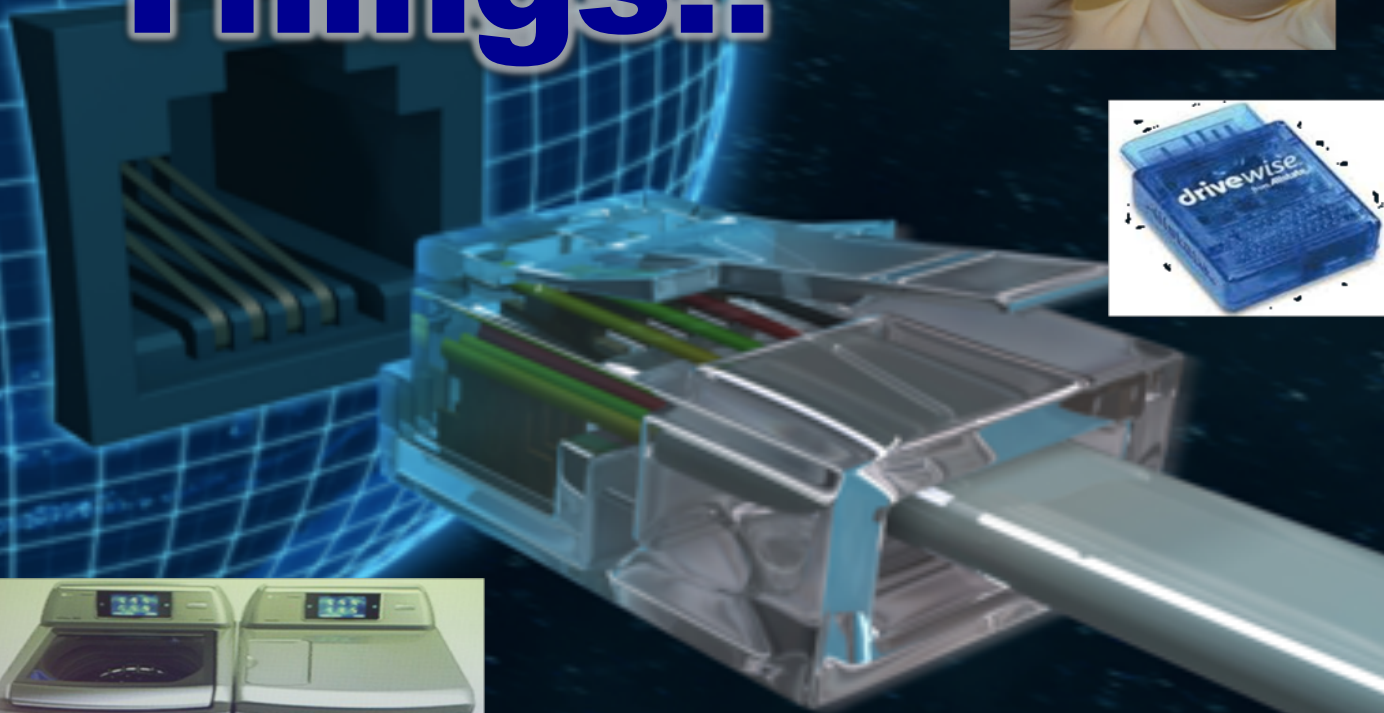
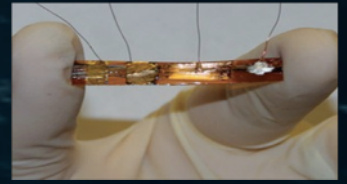
Business Goals
IT Plans, Threats,
Vulnerabilities



The Cloud and IoT

... Need A LOT of Security Too!

The Internet of Things!!



windows has been detected and your computer has been shut down to prevent damage to your brain.

DRIVER_JIM_NOT_LESS_OR_EQUAL_WHATEVER_THAT_MAY_MEAN

If this is the first time you have seen this stop error screen, get used to it. You'll probably be seeing it quite a few times in the coming months. (especially windows 9x users). If you think it'll help, you can try this:

Check to make sure the kettle is on. Tea or coffee should be served ASAP. If this is a new installation, ask your hardware or software manufacturer why they sold you the dodgy products, and if possible, get your money back.

If problems persist, take the cover off your computer and poke various boards with a sharp metal stick. Disable BIOS settings at random, and keep your fingers crossed. You may want to press f8 and enter Safe Mode, but there's no guarantee that'll work either. If all else fails, headbutt the monitor, and run around like a headless chicken.

Below is some unintelligible code, you can go to Microsoft.com and search for the strings but I doubt you'll find anything useful there.

Technical Information:

***STOP: 0x00000001 (0xFC10003F,0x00000002, 0x00000001, 0xf870f80a)

***PatMgr.sys - Address F870F90A base at F870F000, DateStamp 3B7DC5A7

HAVE A NICE DAY:FOXHOUND, NEMESIS:

THE FUTURE!!

AI, Blockchain, Hacks, Flying Cars, &
More Certs!!!

Well...Yes, Yes, Yes, Yes, and No.



**MAYBE WE ONLY
JUST NEED MORE
CISSPs!!**

CISSP Test Question #101: True or False:
Risk = Threats x Assets x Vulnerabilities

Not an
Equation

Risk =

- Prioritized, Assets You Really Need to, and Can Protect
- Situational Awareness of Your Real Attack Surface (Vulns)
- Mapping the Capabilities of the Adversaries (Threats) that Want Those Assets

Security Leaders in 2020

- Aligned with the business
- Focus on what matters most
- More automation and ML
- More intel sharing
- Better humans
- Vacation now and then



Thanks!

@eddieschwartz

www.linkedin.com/in/eddieschwartz/