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....?
Russian Central Bank Admits $6M SWIFT Attack

OPM Breach – Spies in Government Data

DDOS Attacks on Top Banks

NYT, WSJ, and Washington Post Claim to be Hacked

DNC hacked, posted on WikiLeaks

Criminal Ring Steals Millions of Identities

Equifax, Uber and Target all taken down by hackers
YOU’RE FIRED!
We feel the office scapegoat is a key component of team-building, and you're a great fit for the job.

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
So much better than clown school.
Audit Checklist

- Audit Satisfactory
- Nonconformances Found
- Observations Made
You have a funny costume, but there’s no guarantee anyone’s going to LAUGH...

....is to SECURITY

....is to BEING FUNNY
Risk = Threats x Assets x Vulnerabilities
IGNORANCE
Sometimes it's best just not to know.
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

Calculations per Second per $1000

Year

1900  '10  '20  '30  '40  '50  '60  '70  '80  '90  2000 '08

Electromechanical  Relay  Vacuum Tube  Transistor  Integrated Circuit
Global Internet Device Installed Base Forecast

Number Of Devices In Use (in Thousands)

Source: BI Intelligence Estimates
= 31 billion by 2020
Total (Known) Malware
Total (Known)
Android Malware

- Malware Applications Overall
- New Malware Applications

January 2013

February 2017
Exponential Vendor **Bucks!!!**
ISO Class 5 Cleanroom Facilities Exclusively Used
Physical Impacts as the Result of Cyber Efforts...

...Exponential Impacts
SEEING BEYOND VENDOR HYPE
a.k.a.: pwnd by sales & procurement people
Enter the KILL CHAIN, etc.
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

FAIL!
THREAT INTELLIGENCE

Don’t Leave Home Without It
Good Intelligence is Good if You Can Get It!
Tracking my cookies?

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

WhatsApp 419MM
Facebook 145MM
Gmail 123MM
Twitter 54MM
Skype 52MM

Source: comScore Media Metrix, census, media, and company filings. News and company filings in addition to estimates derived from these sources.
Data Sources

Format, Prepare, Classify & Store

Level 1 Analysis

Level 2 Analysis

Machine Learning, AI, Blah Blah... (You Can’t Do it Yet...!)

Level 3 Analysis

Human Analysis
(You Can Do It If You Have The People...)

Dissemination

Reporting & Distribution
Finished Intel
Sharing Communities ISACs
APIs
Orchestration

ETL
Level 1 Analysis
Level 2 Analysis
Level 3 Analysis
FROM HACKER TO CISO

How to Speak the Language of Business...
POP QUIZ!
Good Luck
Evolution of the CISO to the CIRO

- CISO: Securing the Organization
- CIRO:
  - Information Security
  - Third-Party Risk Management
  - Regulatory Compliance Management
  - Business Acumen

- Secure the internal organization
- Manage the risk of third parties
- Manage regulatory risks
- Communicate current status and risks to board
“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.”
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, Yes, and No.
MAYBE WE ONLY JUST NEED MORE CISSPs!!
CISSP Test Question #27: 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/