The Evolution of our Threatscape

6/28/2018

Office of the Chief Information Officer

U.S. Department of Education

Agenda

Introduction

Legacy theories and frameworks

Threatscape

People and the Present

Technologies

Questions

Introduction

Steven Hernandez

MBA, CISSP, CISA, CNSS, CSSLP, SSCP, CAP, ITIL

Co-Chair Federal CISO Council

Chief Information Security Officer (CISO)

US Department of Education

Government Chair

ACT-IAC Cybersecurity Community of Interest

Prior Roles:

Vice Chairman Board of Directors $(ISC)^2$

CISO HHS OIG

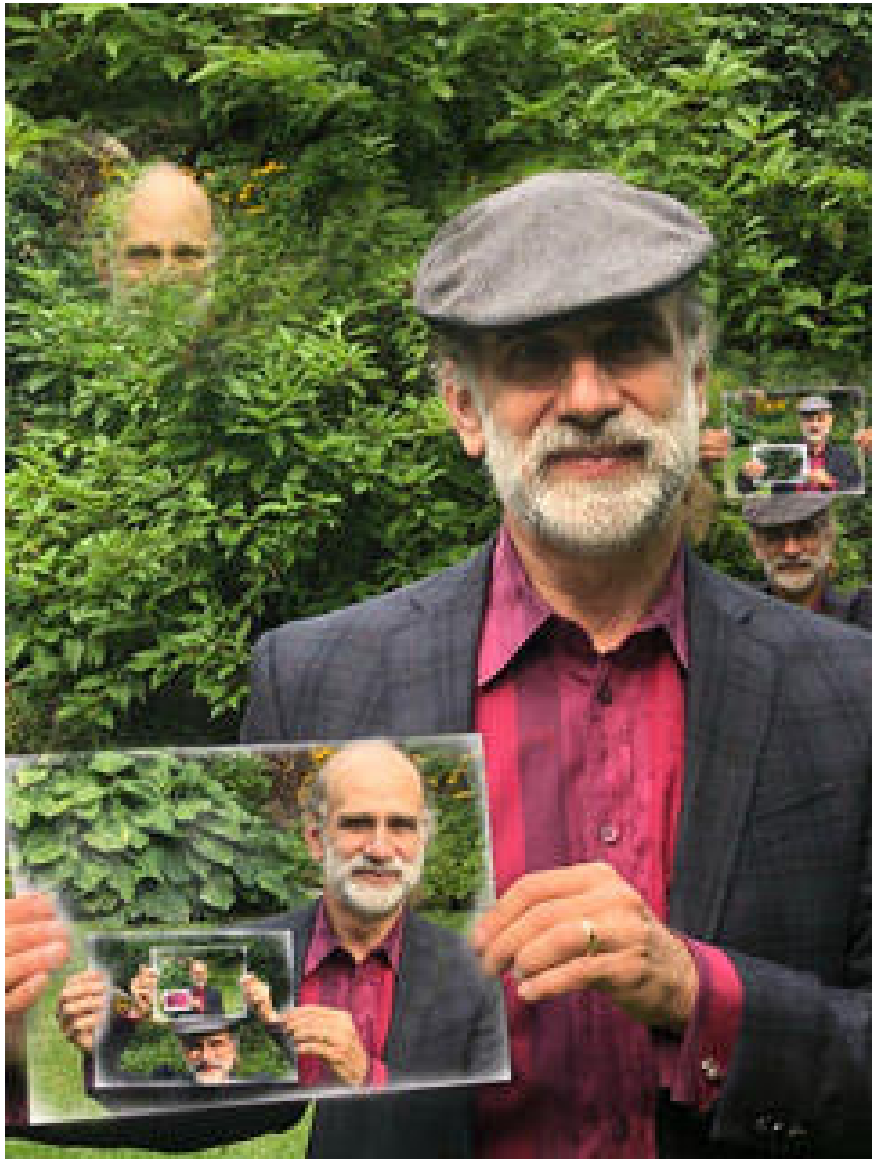
Senior Official for Privacy, HHS OIG

Perspectives

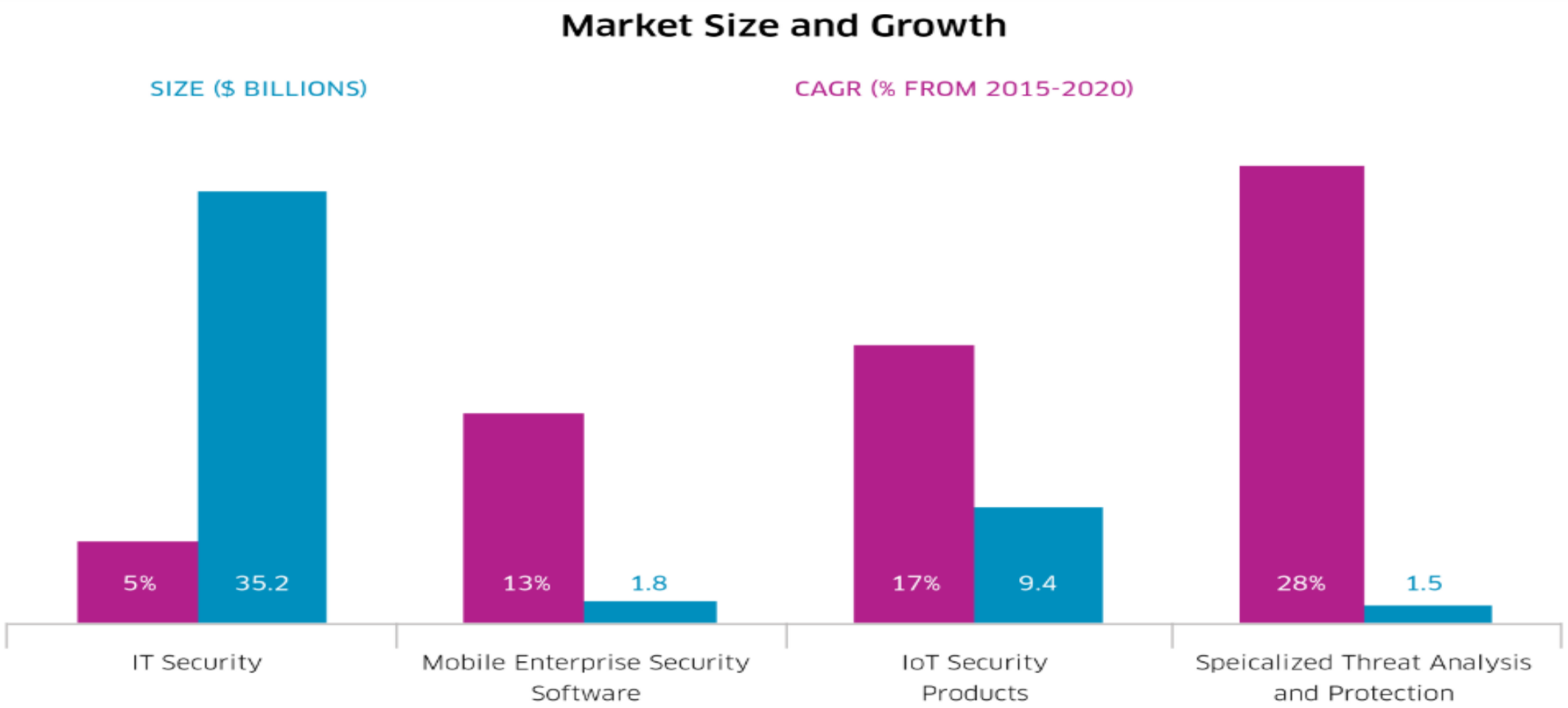
Bruce Schneier is an internationally renowned security technologist, called a "security guru" by *The Economist*. He is the author of over one dozen books--including his latest, *Click Here to Kill Everybody*--as well as hundreds of articles, essays, and academic papers. His influential newsletter "Crypto-Gram" and his blog "Schneier on Security" are read by over 250,000 people. He has testified before Congress, is a frequent guest on television and radio, has served on several government committees, and is regularly quoted in the press. Schneier is a fellow at the Berkman Klein Center for Internet & Society at Harvard University; a Lecturer in Public Policy at the Harvard Kennedy School; a board member of the Electronic Frontier Foundation, AccessNow, and the Tor Project; an Advisory Board Member of the Electronic Privacy Information Centerand VerifiedVoting.org; and a special advisor to IBM Security.

Technology

“a mathematical utopia: algorithms that would keep your deepest secrets safe for millennia, protocols that could perform the most fantastical electronic interactions-unregulated gambling, undetectable authentication, anonymous cash-safely and securely. In my vision cryptography was the great technological equalizer; anyone with a cheap (and getting cheaper every year) computer could have the same security as the largest government. In the second edition of the same book, written two years later, I went so far as to write: "It is insufficient to protect ourselves with laws; we need to protect ourselves with mathematics.“”



Technology Spend



Source: Bloomberg Intelligence (Anurag Rana – Senior Industry Analyst), Sept. 22nd, 2016 and IDC

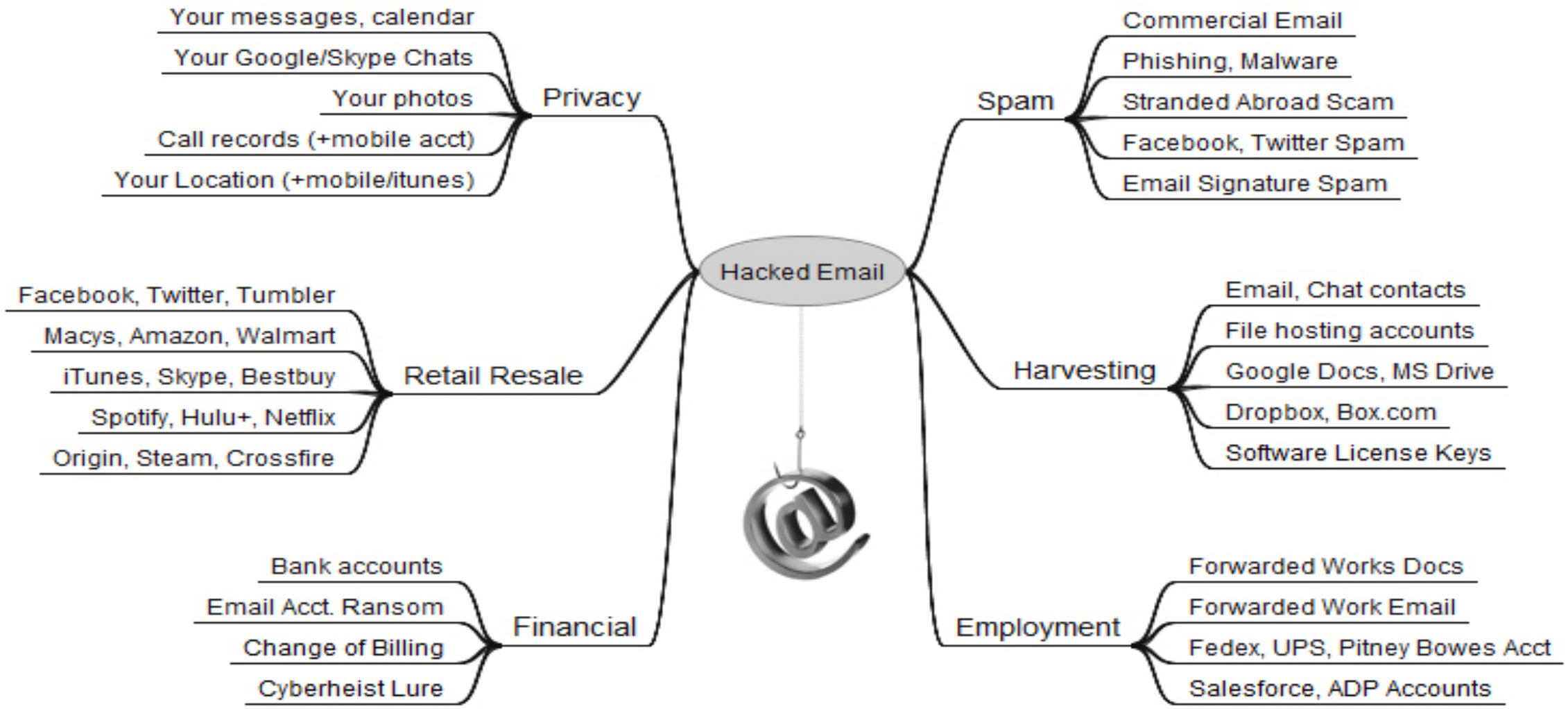
Kreb's Value of a Hacked PC

Bitcoin mining:

- Leveraging physical and cloud assets to mine cryptocurrency (cryptojacking)
- This turns any device or cloud infrastructure into a money mining machine
- The cost to you comes in terms of performance and in the cloud real cash.
- No real skill necessary, automated kits are available for ~$30

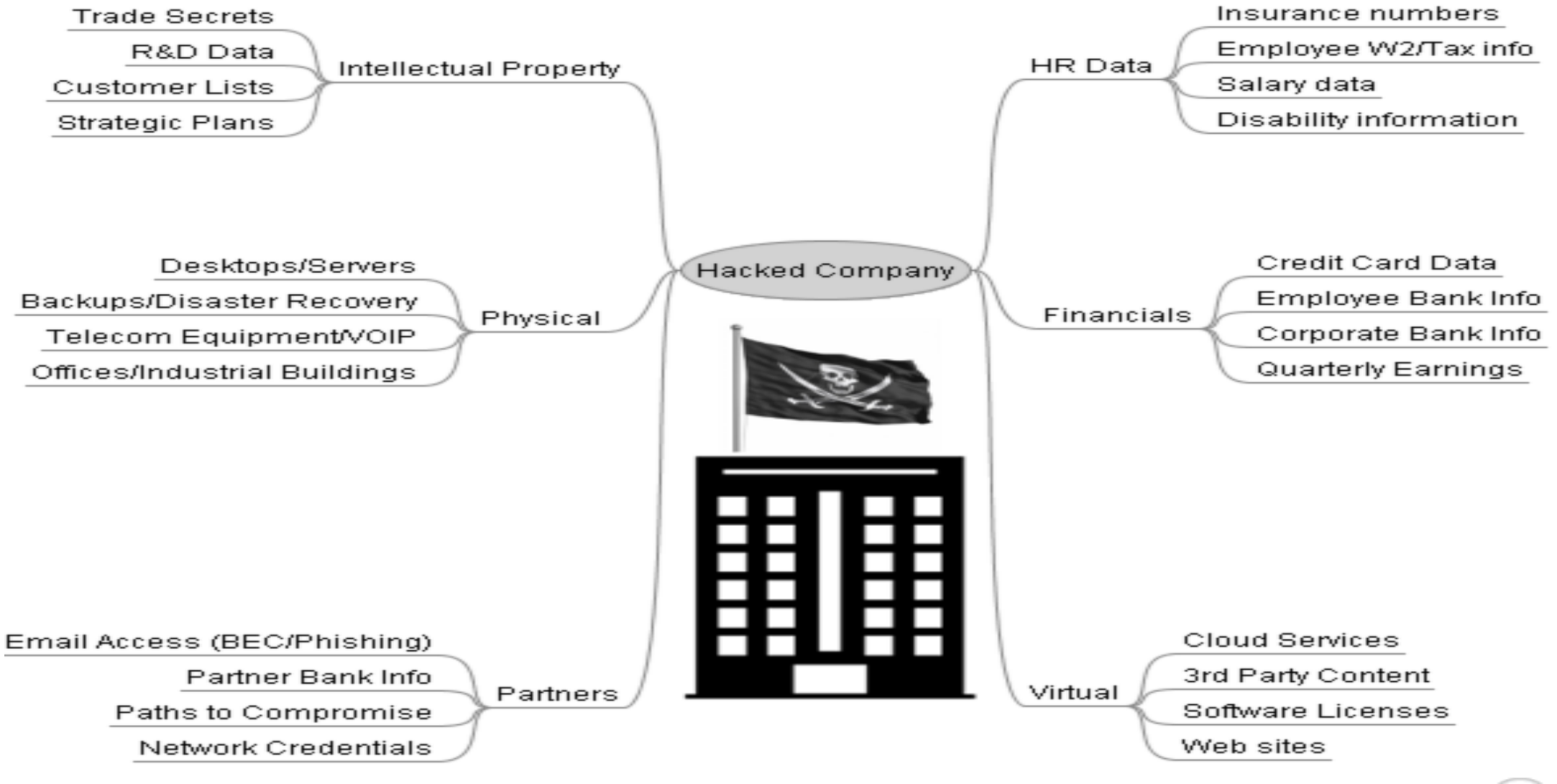
Unsecured AWS led to cryptojacking attack on LA Times, Tesla and Others. Insecure cloud resources, infested code and poor administrative control led to the attack.

Kreb's Value of Hacked Email (BEC)



https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/

Kreb's Value of a Hacked Company (Organization)



Education Sector

Electronic Frontier Foundation did aa study titled "**Spying on Students: School-Issued Devices and Student Privacy"**

- In Summary the EFF concludes ed tech suffers from:
  - **Lack of transparency.** Schools issued devices to students without their parents' knowledge and consent. Parents were kept in the dark about what apps their kids were required to use and what data was being collected.
  - **Investigative burdens.** With no notice or help from schools, the investigative burden fell on parents and even students to understand the privacy implications of the technology they were using.
  - **Data concerns.** Parents had extensive concerns about student data collection, retention, and sharing. We investigated the 152 ed tech services that survey respondents reported were in use in classrooms in their community, and found that their privacy policies were lacking in encryption, data retention, and data sharing policies.
  - **Lack of choice.** Parents who sought to opt their children out of device or software use faced many hurdles, particularly those without the resources to provide their own alternatives.
  - **Overreliance on "privacy by policy."** School staff generally relied on the privacy policies of ed tech companies to ensure student data protection. Parents and students, on the other hand, wanted concrete evidence that student data was protected in practice as well as in policy.
  - **Need for digital privacy training and education.** Both students and teachers voiced a desire for better training in privacy-conscious technology use.

Value of the SEA/LEA information

The information, technology and access to students has tremendous value to an attacker:

- Student PII and PHI is often untouched in terms of prior breaches.
  - A ripe target for collection and maturing for use later
- Ed tech can provide a conduit for predators to profile, stalk or harass victims.

Value of the SEA/LEA information

- TheDarkLord:
  - “We Are Savage Creatures”
  - https://gizmodo.com/hackers-lock-down-entire-school-district-with-threats-1818542996
- https://ifap.ed.gov/eannouncements/101617ALERTCyberAdvisoryNewTypeCyberExtortionThreat.html
- https://www.desmoinesregister.com/story/news/crime-and-courts/2017/10/05/dark-overlord-hacker-johnston-schools-threats/735950001/

Threatscape

- Ransomware
- Business E-mail Compromise
- Data Exfiltration/Breach
- Crytpojacking
- Moving down the Value Chain

Business Email Compromise (BEC)

- Business E-mail Compromise (BEC)/E-mail Account Compromise (EAC) is a sophisticated scam targeting both businesses and individuals performing wire transfer payments.
- The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.
- The scam may not always be associated with a request for transfer of funds. A variation of the scam involves compromising legitimate business e-mail accounts and requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees.[1]

https://www.ic3.gov/media/2018/180712.aspx

Business Email Compromise (BEC)

- The BEC/EAC scam continues to grow and evolve, targeting small, medium, and large business and personal transactions. Between December 2016 and May 2018, there was a 136% increase in identified global exposed losses[2]. The scam has been reported in all 50 states and in 150 countries. Victim complaints filed with the IC3 and financial sources indicate fraudulent transfers have been sent to 115 countries.

- Based on the financial data, Asian banks located in China and Hong Kong remain the primary destinations of fraudulent funds; however, financial institutions in the United Kingdom, Mexico and Turkey have also been identified recently as prominent destinations.

Business Email Compromise (BEC)

The following BEC/EAC statistics were reported to the IC3 and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between **October 2013 and May 2018:**

Domestic and international incidents:	78,617
Domestic and international exposed dollar loss:	$12,536,948,299

The following BEC/EAC statistics were reported in victim complaints where a country was identified to the IC3 from **October 2013 to May 2018:**

Total U.S. victims:	41,058
Total U.S. victims:	$2,935,161,457
Total non-U.S. victims:	2,565
Total non-U.S. exposed dollar loss:	$671,915,009

Business Email Compromise (BEC)

Even the best get hit by this one:

"On Thursday, March 16, the CEO of **Defense Point Security, LLC** — a Virginia company that bills itself as "the choice provider of cyber security services to the federal government" — told all employees that their W-2 tax data was handed directly to fraudsters after someone inside the company got caught in a phisher's net."

"I want to alert you that a Defense Point Security (DPS) team member was the victim of a targeted spear phishing email that resulted in the external release of IRS W-2 Forms for individuals who DPS employed in 2016," Defense Point CEO George McKenzie wrote in the email alert to employees. "Unfortunately, your W-2 was among those released outside of DPS."

https://krebsonsecurity.com/2017/03/govt-cybersecurity-contractor-hit-in-w-2-phishing-scam/

Preventing BEC

Be mindful of phone conversations. Many victims have reported receiving phone calls from BEC/EAC actors requesting personal information for verification purposes. Financial institutions report phone calls acknowledging a change in payment type and/or location. Some victims report they were unable to distinguish the fraudulent phone conversation from legitimate conversations. One way to counter act this fraudulent activity, is to establish code phrases that would only be known to the two legitimate parties or call the business/requester back at a validated good number.

Preventing BEC

If you discover a fraudulent transfer, time is of the essence. First, contact your financial institution and request a recall of the funds. Different financial institutions have varying policies; it is important to know what assistance your financial institution will provide when attempting to recover funds. Second, contact your local FBI office and report the fraudulent transfer. Law enforcement may be able to assist the financial institution in recovering funds. Finally, regardless of dollar loss, file a complaint with www.ic3.gov or, for BEC/EAC victims, bec.ic3.gov. The IC3 will be able to assist both the financial institutions and law enforcement in the recovery efforts.

Post-Secondary Education

- The Department of Education through its Federal Student Aid Office Issues over 80 Billion dollars in Student Aid every year.

- The Department relies on institutions to receive these funds and ensure school bills are paid and the balances are disbursed to the students

Post-Secondary Education

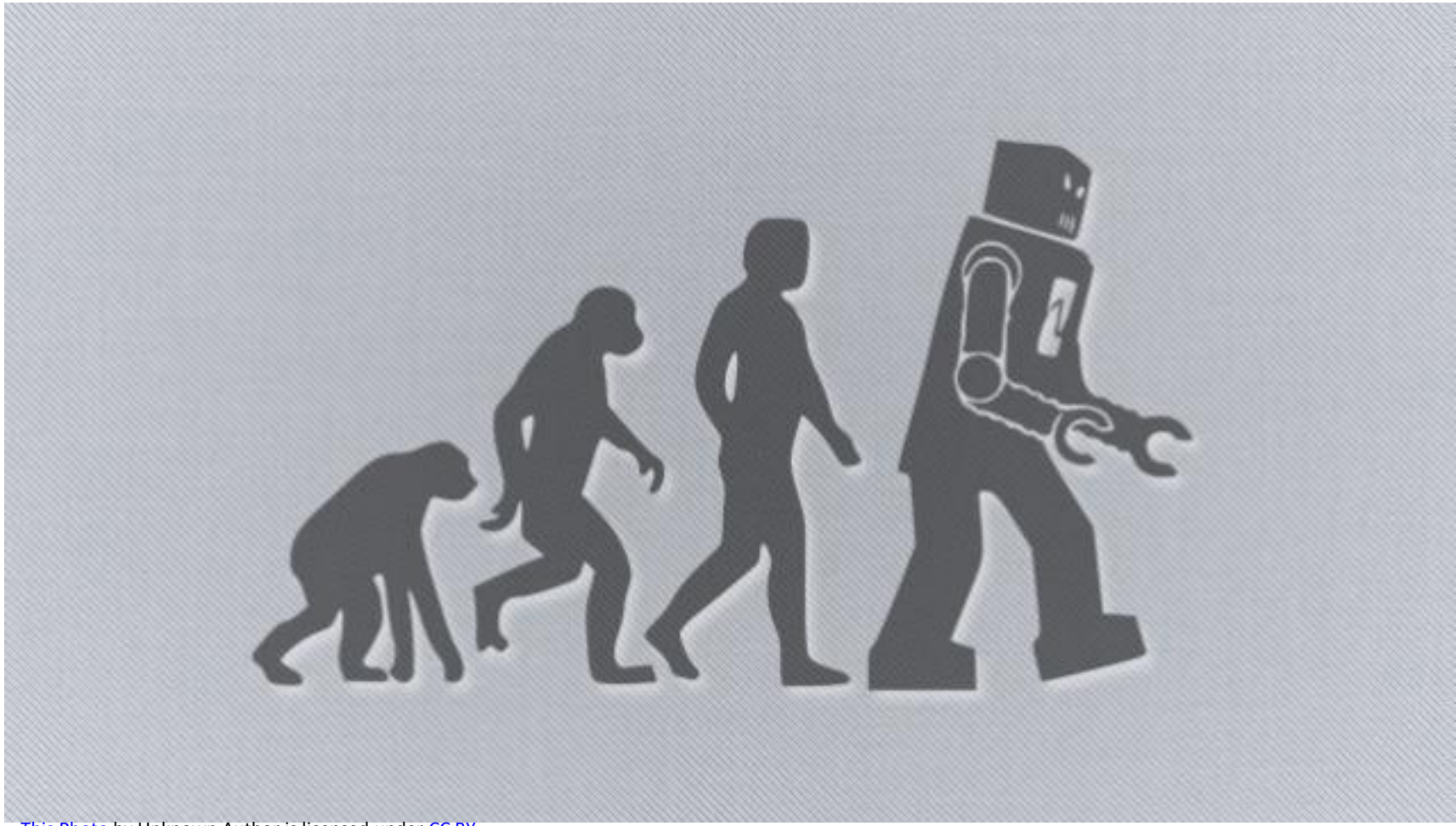
- Criminal elements want a slice of this 80 Billion dollar pie.
- They have tried for years to attack the Department's disbursement systems
- While they have had immaterial success, they continue to learn about the value chain and the business.

Post-Secondary Education

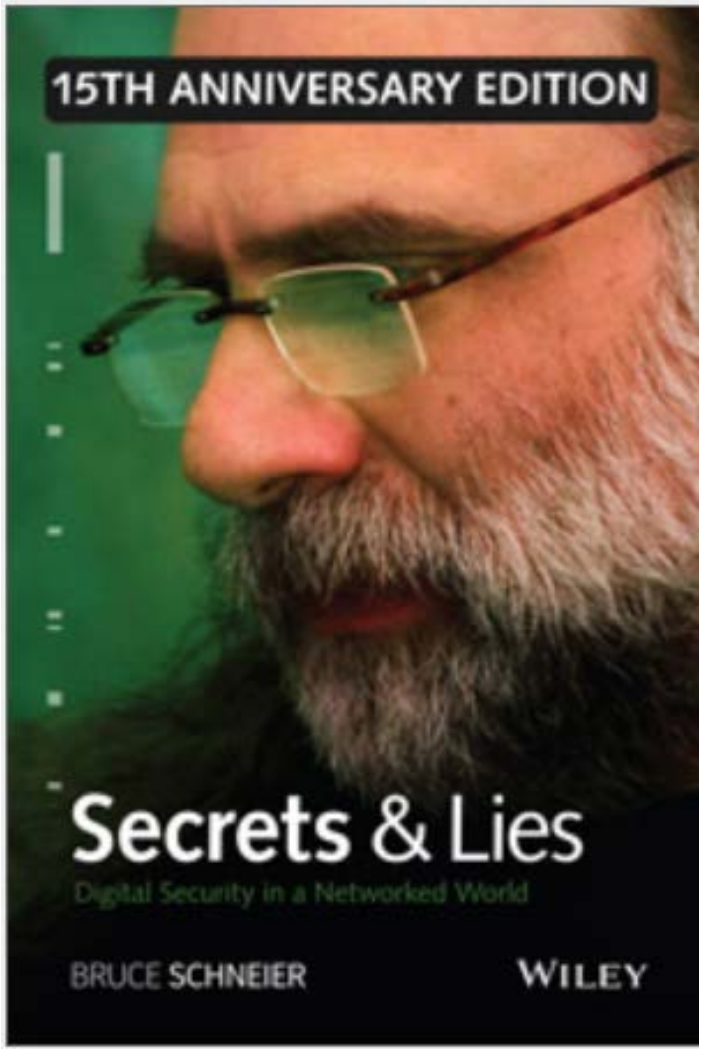
- Department hardened our systems.
- Criminals moved down the value chain
- Started to exploit the students
  - Phishing
  - Automation
  - Coordination

Post-Secondary Education

- Evolution
- Criminals adapted
- Laundering



Back to Bruce



It's just not true. Cryptography can't do any of that. It's not that cryptography has gotten weaker since 1994, or that the things I described in that book are no longer true; it's that cryptography doesn't exist in a vacuum. Cryptography is a branch of mathematics. And like all mathematics, it involves numbers, equations, and logic. **Security, palpable security that you or I might find useful in our lives, involves people: things people know, relationships between people, people and how they relate to machines.** Digital security involves computers: complex, unstable, buggy computers.

People are the problem….

- And also the solution!!
- We can only leverage the tools we understand how to use.
- Training, awareness and education must remain on the forefront of our risk management strategies.
- The behavior of people and individuals is becoming the key differentiator between those organizations that can survive and those who can thrive.
- Our threats are human, only humans will defeat them.

THANKS!!!!

Questions??

Contact me:

Steven G Hernandez

Steven.Hernandez@ed.gov