Cybersecurity 2018:

Looking Back, Looking Ahead, or Just Looking Around?

Tony Sager
Senior Vice President & Chief Evangelist

December 2018

CIS: the Center for Internet Security

non-profit, global, volunteer-powered

- **Security Best Practices**
  - CIS Controls
  - CIS Benchmarks
  - CIS Hardened Images
- **The Multi-State ISAC (Info Sharing and Analysis Center)**
  - Elections Infrastructure ISAC
  - CIS Marketplace
  - CIS Services

<www.cisecurity.org>

The Cybersecurity Problem

- Every type of victim: country, sector, size, individual…
- Every motivation: financial and IP theft, extortion, social control, political statements, notoriety, influence operations, “false flags”, “prep of the battlespace”….
- Attackers are efficient: information sharing, automation, very large scaling, specialization, a marketplace… (4K ransomware attacks/day)
- threat of cyber a “top 3 disruption” (World Economic Forum)
- Cyber threats greater than physical threats (DHS Secretary Nielsen)
- Worldwide cybercrime costs $600B/year (McAfee, CSIS)
- Expect $100B in defensive spending in 2020 (IDC)

Y2K - with real impact, and without the deadline

Attacks

- information (even about attacks) is beautiful
- **Incidents *and* Campaigns**
  - Marriott, “Operation Sharpshooter”, “BEC”
- **Deep *and* Wide**
  - SPECTRE/MELTDOWN, VPN Filter, NotPetya (2017)
- **Old *and* New**
  - Cloud infrastructure, SaaS, outsourcing
  - Criminality as a distributed, industrial-scale enterprise

Targets

- **Criminal**
  - Ransomware, ID theft
- **Espionage**
  - IP theft, “prep of the battlespace”, influence operations
- **Political/Social**
  - Elections, Campaign staffs, social media
- **Small/Medium**
  - small dollar, large scale; dispersed solution opportunities

"Anyone in organized crime who is not getting into this (cyber) ought to be sued for malpractice."

-- Shawn Henry

President of Crowdstrike Services

former Deputy Director for Cyber, FBI

Political/Social

- **Legislative**
  - Sharing; “hygiene”; use of commercial standards
  - Privacy, Protection “Push-of-War”; encryption
- **Executive**
  - Role of Federal Regulatory Agencies
- **Marketplace**
  - Compliance, Supply Chain, the “Multi-Framework Era”
  - Scoring, Assessment
  - ”mainstreaming” of Cybersecurity in Executive Decision-making; Cyber as a “social expectation”
  - Role of non-profits

Some General Interest References

- **Verizon Data Breach Incident Report**
  https://www.verizonenterprise.com/verizon-insights-lab/dbir/
- **Krebs on Security**
  https://krebsonsecurity.com/
- **Center for Strategic & International Studies Cyber Incident List**
  https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity
- **National Academy of Sciences: At The Nexus of Cybersecurity and Public Policy**
  https://www.nap.edu/catalog/18749/at-the-nexus-of-cybersecurity-and-public-policy-some-basic

Small Businesses and Cyber

- 29 million small businesses - less than 500 employees (SBA)
- Half of all attacks target them (NCSA, Symantec, DBIR, etc.)
- Over half of them report an attack or data breach in prior year
- Half have no budget allocated for risk mitigation
- Most of the data breaches are from small businesses (the Hill)
- Typical cost between $84k and $148K (UPS Capital)
- Half identified root cause as “negligent employee or contractor”