Nardello & Co.
WE FIND OUT

HCCA Atlanta Regional Compliance Conference
January 25, 2019

The current state of cybersecurity: by the numbers

Average cost of a major data breach — **$11.7M**

Percentage increase in cost from previous year — **22.7%**

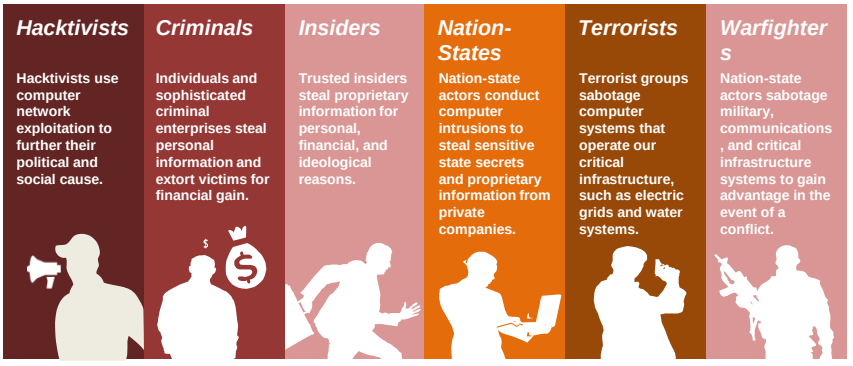
Average number of major security breaches each year — **130**

Percentage increase of major security breaches — **27.4%**

Cybercrime damages by 2021 — **$7 Trillion**

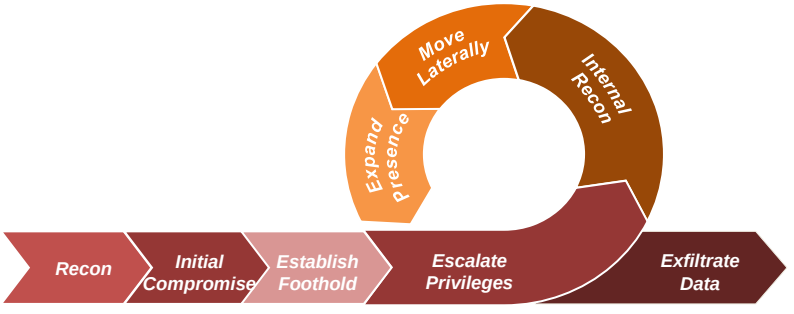
*Ponemon Institute (2017). "Cost of Cybercrime Study"

Who They Are: The Cyber Threat Landscape



How They Do It

The anatomy of a sophisticated cyber attack is complex, and on average, can take place over the course of 6 months to a year.



How They Do It: The Information Supply Chain

Attacks are increasingly originating from 3rd party providers such as contractors, partners, vendors.

Who has access to your data?

- Acquisitions/Mergers
- Travel agencies
- Law firms
- Vendors
- Customers
- Contractors
- Partners

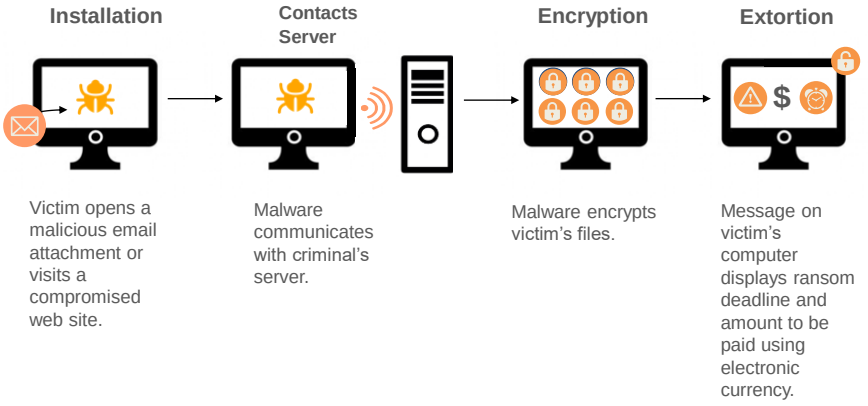
Major Threat: Email Compromises

- Simple, yet effective cybercrime scam.
- Carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques.
- Results in stolen information, unauthorized transfers, or larger data breaches.

Exposed Dollar Loss (USD):
(Oct 2013 – May 2018)

$12.5 Billion

Ransomware - A New Breed of Attack



Healthcare: A target-rich environment for attackers

- Healthcare organizations are the perfect target for attackers: highly valuable and sensitive data.
- Countless endpoints running various operating systems and applications with varying degrees of security.
- Information supply chain: Numerous vendors, business associates, etc.
- Higher per-record value on criminal underground than financial records.
- Ransomware: Preying on the life-and-death decisions of hospitals.

Tips for Securing your Digital Life

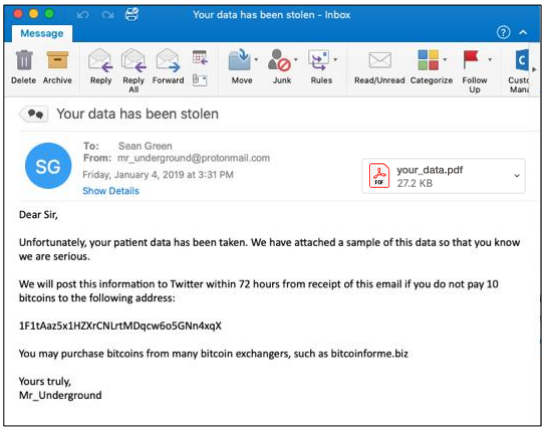
- Know that you are the target.
- Keep software up to date.
- Use strong passwords….and not the same one everywhere!
- Beware of suspicious emails or phone calls.
- Be careful of what you share on social networking sites.
- Use two-factor authentication when possible.
- Use public wifi and hot-spots carefully.
- Backup your data.
- Teach your kids about the internet and online safety.
- Be a good steward of your personal data.

Simulation Exercise

Healthcare Data Breach
Simulation Exercise

Simulation Exercise – Move 1

On Friday, Sean Green, CEO of Acme Healthcare, receives an email from an anonymous source who claims to have stolen a large amount of patient data from Acme's systems. The person attached a sample of the stolen data in the email, which Acme's IT team confirmed was an exact match of actual Acme patients.



Simulation Exercise – Move 2

The following Wednesday, several hospitals and doctor's offices in Acme's network begin receiving phone calls from patients stating that they have been receiving strange emails from someone claiming to be with the collections department at Acme.

Several weeks after the incident, Rachel Smith, Acme's CCO, receives a phone call from Michael Wilson from HHS. Wilson states that HHS is investigating reports of a data breach at Acme Heathcare, and requests Acme's full cooperation in the matter.

Takeaways: Have a Plan

Mistakes

- Lack of preparation
- Delayed response
- Over-communicating (externally)
- Under-communicating (internally)
- Making assumptions
- Proper assessment: Is this an ice cube or an iceberg?

Tips

- Have an offline plan in place
- Have legal/forensics/PR on call
- Have a decision framework in place
- Preserve evidence
- Notify insurance carrier early
- Get out ahead of media (if public breach)
- Review agreements
- Pre-establish relationships with law enforcement, regulators, etc.