Risky Business: Essential skills for pivoting security resources

* What do attacks today look like?
  + Custom tailored for your organization
  + Asynchronous - cat and mouse game
  + The rise of Advanced Persistan Threat (APT)
* Why have they been so successful lately?
  + Social engineering and social media
* Specific strategies
  + Social engineering
  + Malware/Malicious Ads
  + Newer Modalities - AI?
  + Email - has web component, macro based office docs, multi stage attacks
* Seasonality - during budget time we use different tools and those get targeted
* Small organizations are at risk because many of them have not built up their security
  + Cost of an average data breach is $4 million, including lost revenue due to recovery time, damage to reputation, etc.

Dissecting the APT

* What do they look like?
  + Consistently advanced; polymorphic in nature (md5 hashes change).
  + Borough through a network
  + Exfiltrate data; command and control traffic, filters out data
  + Network-centrism: people on mobile phones, cloud, etc, once they access dmz they can access everything.
    - Instead of only securing network, secure the applications as well. Coconut analogy: hard outer shell (DMZ) soft inside.
* How do they compromise our business processes?
  + "Low and slow" approach: find a weak point to pivot from (box in a DMZ)
  + Sample Timelines
* Who perpetrates them the most?
* What do you look for specifically?
  + Behavioral metrics, baselines

What is at stake here?

* The value of your company
  + Loss of assets
    - Intellectual property
      * Stolen
      * Destroyed
      * Altered
    - Organizational reputation
    - Customer priivacy
  + Financial impact on the organization
    - Value of specific assets
    - Ability to operate
  + Safety of employees/people in the field

Key challenges

* Existing business processes
* Understanding today's end points
* Configuration management
  + Managing patch level
  + A few realities
* Backup solutions
* Business process management: what data does the business value? Risk management key
* Creating enterprise level solutions
  + Cloud-based
  + Installed/traditional
  + Hybrid

Risk management yesterday and today

* Moving beyond pointing fingers
  + What are we doing wrong? Take on too much risk without beefing up security
    - What can we do right?
    - What do businesses need to do differently?
  + Business process management
  + Risk management
    - Essential concepts
    - Best practices
* Risk management - beyond basics
  + Risk management involved the proper use of one or more of the following, per asset in your network:
    - Mitigation: reduce the impact of an occurrence
    - Avoidance: reduce the likelihood of a occurrence
    - Transfer: move the impact to another party - insurance
    - Acceptance: state and indicate that you will simply allow the impact to happen. Accepting a risk is different from ignoring risk. They have evaluated the impact of the risk.
  + But, everyone needs to be on the same page
  + Is everyone on the same page?
  + How do you make that happen?

What has changed in risk management?

* Old school vs new school
  + Compliance vs pivoting resources
  + Analytics
  + Business practices
* What the Equifax attack - or any other attack - told us about risk management?
  + Importance of process
  + Impact of inadequate communication and return on investment (ROI) discussions
  + Applying and customizing frameworks

Pivoting resources - how that happens

* Laws and best practices
  + What laws do you need to know?
  + Privacy impact assessment
  + Privacy threshold assessment
* Data security and privacy practices
  + Labeling data
  + Burning data
  + Shredding data
  + Degaussing
* Additional practices and issues

Marketable skills

* Talk in multiple languages
* Understanding of risk management
* Pragmatism
* Honesty - admit when you don't know something
* Willingness to learn