national fintech
CYBER SECURITY SUMMIT

Why is Collaboration the Future of Cyber Security for Fintech?

Ron Moritz
Founding Partner, TrueBit Cyber Partners
Venture Partner, Cyber Security, OurCrowd

national fintech
CYBER SECURITY SUMMIT

Cyber Security

*Learning something that makes you dumber

- Layered security works but …
  - Are we getting dumber with each layer we add?
- We can't seem to stop consuming sec-tech
  - How many layers can we possibly have?
- There aren't enough good guys to go around
  - More tech means more experts we don't have
- So we must find ways to help the good guys
  - Strength in numbers?

Balancing Limited Cyber Resources

- Marginal returns from enterprise security model
  - Ever-evolving endpoint security and monitoring tech
  - Sifting through a myriad of data and alerts
- This model (like the AV industry) will not scale
  - Severity and number of successful attacks will ↑
  - PwC: detected incidents 38% YoY ↑ 2014 to 2015
  - Verizon: confirmed breaches 55% YoY ↑ 2014 to 2015
- Security teams are at a disadvantage
  - Security teams lack information (to use or share)
  - Need look-back on attacks that have happened and also need to have insight about those in progress

Carbanak

- APT-style phishing-based attack
  - Began in 2013
  - $1B+ over 2 years
- Multiple breaches
  - 100+ banks, 30+ countries
- Failure of existing enterprise security model
  - Bad guys executing well-coordinated attacks

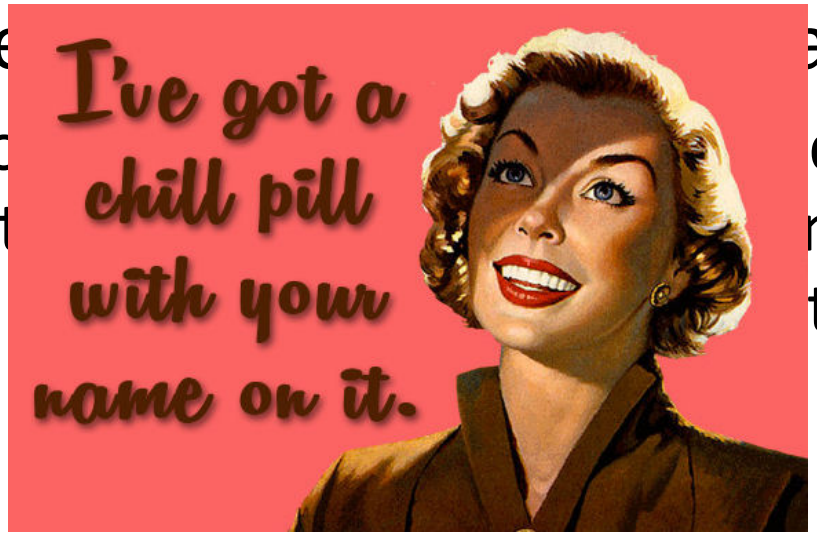
The Opposition is Better Organized

- Bad guys share vulnerability info freely, quickly
  - Good guys dig a hole, bury their heads in the sand
    - Partially driven by legal department anti-trust concerns
- Attacks: spread in hours, undetected for months
  - According to Risk Analytics, 75% of attacks spread from victim zero to victim one within 24 hours*
    - 40% of those (30% of all) spread within the first hour
  - A growing attacker/defender detection deficit
    - Median days threats are present before detection is 205
    - Median days between exploit and remediation is 120

*Verizon 2015 Data Breach Investigation Report (DBIR)

Better Living Through Collaboration

- The practice of taking meds (drugs) to make life more enjoyable:
  - "Wow, Jenny was always so depressed, but now that she takes a bottle of Prozac in the morning and washes it down with vodka, she seems really relaxed and happy." http://urbandictionary .com
- Better cybe aboration
  - The lack c d collaborat nd experts is the bane try



What Do Cybersecurity Teams Need?

- Visibility into incident info from peers
  - May be same attack methods or different
- Ability to effectively exchange information
  - Not dump raw but add qualified, enriched content
- Ability to effectively collaborate
  - Joint problem solving via shared expertise
- Share our experts and share our pain
  - Ability to open the kimono (sharing economy)

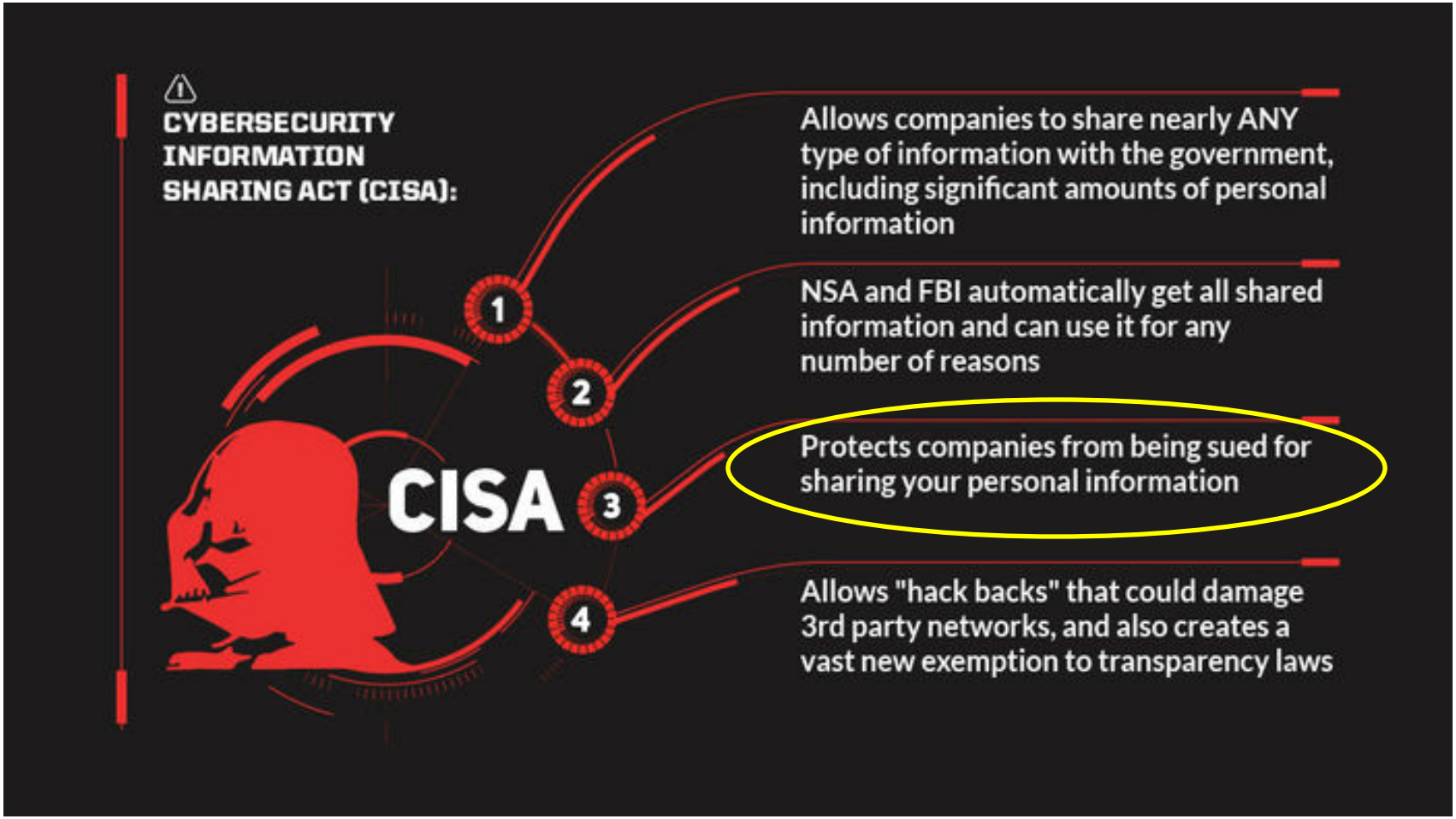
Other Good Guys Who Collaborate

- Counter Terrorism (National + International)
  - U.S. DHS Fusion Centers
    - "A collaborative effort of two or more agencies that provide resources, expertise and information with the goal of maximizing the ability to ***detect, prevent, investigate, and respond*** to criminal and terrorist activity."
- Scientists and Solving Hard Problems
  - Multi-sectoral collaboration to solve HIV/AIDS
  - Manhattan Project during WWII
  - Team of Rival Scientists Come Together to Fight Zika
    - New York Times, 30-Mar-2016

So Why Don't We Share?

- Business risks slow information sharing
  - Legal / Government Concerns
    - Disclosing PII, IP, CCI (liability issues)
    - Anti-trust violations
    - Flagged as "in bed with" the government
  - Market / Financial Risks
    - Brand reputation
    - Cost of disclosing breach
- Some help from safe harbor legislation
  - U.S. Cybersecurity [Information Sharing] Act (12/2015)
    - Removes legal and government concerns **but …**
    - Leaves market and financial risks **and …**

CISA is not Perfect



Overcoming Sharing Limitations

- Without incentives to share quickly
  - Threat data is recycled (has limited value)
  - Relationships are ad-hoc (untrusted)
  - Incident data is outdated (yesterday's news)
- Basic algebraic equation: { VI ↑ → TE↓ }
  - As the value of the info exchanged increases the time to exchange decreases
- We need platforms to support and facilitate the rapid exchange of high-value information
  - Must share incident info of value faster

Many Years of Talk

- Underground Sharing Scene (informal yet seminal)
  - Computer Anti-Virus Research Organization (CARO)
    - Intimate, informal, and thumbing noses at legal
  - Maybe supplanted by the Cyber Threat Alliance (CTA)
    - Suffers from underlying competitive challenges
- U.S. Information Sharing & Analysis Centers
  - FS-ISAC most advanced but limited effectiveness vis-à-vis reducing time (insufficient early warning) and not global
- Attack/Event Threat Intelligence Hub/Repository
  - Bulletin-board like services to consume and post info
  - Primarily for intelligence and research staff
- Threat Intelligence Hype (since about 2013)

Problems with Threat Intelligence

- Info overload – data too raw or generic
  - Threat intel vendors selling unrefined data scraped from web, collected via sensors and honeypots and no sector relevance
- Lack of anonymity
  - How do you contribute while protecting enterprise secrets?
- Unqualified data and sources, no consistent engagement
  - Challenge of garbage-in, garbage-out
- No standards or common exchange infrastructure
  - Challenge of sharing data and extracting meaningful value
- Lack of context or filters
  - Many indicators of compromise but what's relevant to me?
  - Should I worry about a spear-phishing attack on aviation sector?

Clarifying Our Goal

- Enrich cyber incident information while minimizing risk of exposing sensitive info
  - Reduce reputational risk
    - Redaction control
    - Anonymity in sharing
  - Improve detection / incident response speed
    - Incident reports correlated with threat intel feeds
  - Increase sharing of threat / incident info
    - Real-time sharing results in faster detection / response

Building Blocks Needed

- Trust
  - Must establish a way to build a trusted community (or communities) and maintain trust
- Connectivity and Productivity
  - Must incorporate into the workflow and business of cybersecurity (processes) inside the enterprise
- Regulation and Compliance
  - CISA enables sharing of cybersecurity information between companies and government
- Vendor Independence

Human Intelligence in Cyber Security

- Establish a Single Point of Truth
  - Dealing with The "Fog of More" (Tony Sager)
- Digest and correlate information
  - Aggregate into event threads
  - Enrich with related context
- Enable and promote collaboration
  - Bank A wants to know that Bank B is under attack
    - What are the attack details?
    - How can the attack effect Bank A?
    - How can Bank A work to help Bank B solve the problem?

Faster

- FBI Roundtable – not scalable or continuous
  - Not trusted (not auditable or compliant)
  - Disruptive (leave the office for in-person meeting)
  - Typically post-mortem (not real-time)
- Social-Media (Sharing Economy) Engagement
  - Always-on discussions around an event
    - P2P, vetted group, un-vetted groups, public
  - Share structured and unstructured data
    - Complete or redacted
  - Correlated and enriched content, digestible feeds

What's App/Slack for Cyber Security?

- What's App Groups
  - Primarily text with photo/video enrichment
  - Recently added P2P but no group crypto
- Slack: "Team Communication for 21st Century"
  - Open and Private Channels and P2P Messaging
  - Drag/Drop/Share Files
  - Connectivity to Key Apps (like Salesforce) for more complete contextual search, content enrichment

Emerging InfoSharing Ideas

- Create optics around issues and reach a wide audience
  - If “X” gets attacked by Ransomware, who needs to know?
    - Other teams inside the enterprise? Peers at other enterprises?
- Can enterprise security operators (secops) cut their dependence on specific solution or service providers by working together?
- Thanks to CISA, private enterprises (in US) can begin working together on cyber security problems without anti-trust issues
  - But how can you add value to those who share while still including the little guys who may have less to share?
  - What about those outside the US?

Emerging InfoSharing Ideas

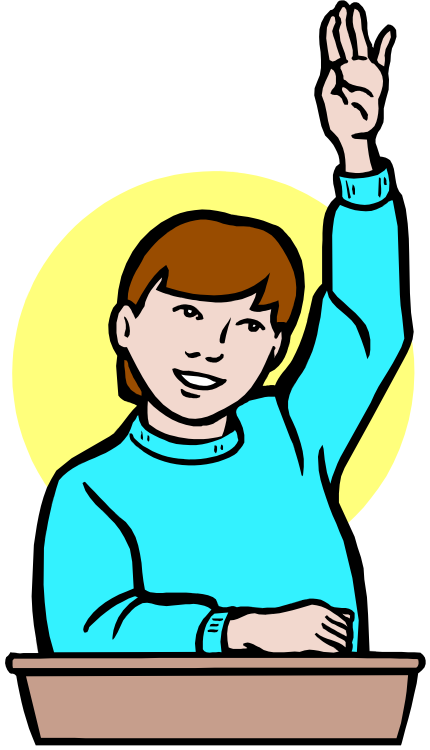
- Need anonymity and privacy protection
  - Mechanisms to protect the enterprise by redacting content (like PII or names) before it is shared
- Digest and correlate events in real time
  - Incident data from both cyber security and other enterprise tools
  - feeds from threat exchanges and open-source reporting
- Must feed into SIEM and workflow managers
- Must present information of value to the collaborator (by role or objective)

Emerging InfoSharing Ideas

- Must enable secops collaborating on an event to look at and work on the same data together
- The power of collaboration requires that many people are engaged in feeding and consuming
- Supplement event data with security infrastructure data to score product impact
  - Vendor performance against specific problems

Sample Vendors

- Early Threat Intelligence Innovators:
  - ThreatConnect (threat intelligence platform)
  - Anomoli (was ThreatStream)
  - ThreatMetrix (cybercrime/fraud)
- Big (vendor-centric consume-and-post clouds):
  - IBM X-Force Exchange
  - Check Point ThreatCloud IntelliStore
  - FireEye / iSight Threat Intelligence
- Emerging Innovators (the watch list):
  - Comilion
  - TruStar



Why is Collaboration the Future of Cyber Security for Fintech?

Sydney, New South Wales, Australia

Ron Moritz

Founding Partner, TrueBit Cyber Partners

Cybersecurity Venture Partner, OurCrowd

Israel: +972 54 625 6597 / U.S. +1 650 665 9560

Ron.Moritz@TrueBitCyber.com

@RonMoritz

http://www.il.linkedin.com/in/ronmoritz/

national fintech CYBER SECURITY SUMMIT