The First Cyber Short

Lessons learned on the way to Wall Street.
Justine Bone, Brucon 2017
A market solution to product quality WTF?
Why are we talking about this?

We are in desperate need of cyber innovation:

Shoddy technologies, shoddy company practices, and an industry stuck in a rut of litigation battles, weak policies, and impending legislative battles.
Public markets are a new opportunity

A new way
- to hold companies accountable for the security (quality) of their products
- to fund vulnerability research

- Just as analysts examine company financial statements to help evaluate company integrity, so too can we examine a company’s technology to help evaluate product quality & security.

- This upsets those that have been relying on security by obscurity.

- Company products, not company infrastructure. For example:
Illustrating what a market-based cybersecurity solution is not:
Presentation Overview

- Financial markets as a new opportunity
- A market approach to product quality
- What that means
- How does it work?
- Why would I do that? Why now?
- What to expect, if you want to get involved.
Bio

• NYC and Miami-based entrepreneur (CEO MedSec, ex-CEO Immunity)
• Reformed vulnerability researcher (GCSB, ISS X-Force)
• A few stints as CSO, CISO, CTO (Bloomberg L.P, Dow Jones, startups)
• Board advisor (HP, Blackhat reviewer, POSHARE)
• Expat kiwi
• Ex-ballet dancer
• Mother of three. This list was not in order of importance.
Cybersecurity: A spotty history

• From the lab, to IT/engineering, the risk department, audit, and the boardroom, we’re taking this as far we as can.

- Still managing FUD, paranoia, denial, and mispaced trust:
  - Folks trust* hospitals to protect their data more than their credit card companies (wrong way around!)
  - Industry isn’t producing methodologies, tools, metrics, messaging, instead relying on niche expertise and skillsets, which doesn’t scale.

*Ponemon Study May 2017
People are starting to care?

Security incidents are going mainstream:

- Target, Home Depot, Stuxnet, OPM, etc
  - seen as affecting big business & government

- Jeep, Linked In, elections, home routers, Equifax, etc
  - Now its getting personal

... we are starting to see financial impact:

Brucon 9/22/17
Growing Financial Impact of Cybersecurity Events

Cybersecurity incidents and market valuations:

• *Harvard Business Review, Why Data Breaches Don’t Hurt Stock Prices, March 2015* ...
  but later that same year...

• *Data Breaches and Stock Prices* - “It’s pretty interesting to see the initial drops in stock and the patterns that affect all companies and all breaches regardless of how well it is handled”, *December 2015*

Specific events:

• Verizon/Yahoo acquisition (8%)
• Jeep recall (6%)
• Oxford/CGI study (2%)
• Ponemon (5%)
• Petya (trading halts - needs analysis)
• Equifax (40%)

Brucon 9/22/17
Hackers are inventors and risk takers

• .... but are we?
• Defensive security: a history of inefficacy
• Offensive security: increasingly costly, increasingly compliant, increasingly demotivating?
• Innovation = Creativity + Value*
• Is the security research community innovating?
• The security industry’s “directional thinking”* often has us following each other, without question.

Eg: Vulnerability Disclosure Policy

* The Medici Effect

Brucon 9/22/17
“Responsible Disclosure”

- Sponsored and coined by big tech (Microsoft) in the early 2000’s
- Compelled researchers to take work directly to the manufacturer/vendor
- Brilliant marketing, total win for the manufacturer and negative connotations for non-compliance

Previously the security research market was small to nonexistent, so most complied....

Resulting in:

- Security research under-valuations and a minimally sized market
- A closed, confidential conversation between manufacturer and researcher
- Power to act on the information in the hands of the manufacturer
- Negative connotations for those who didn’t comply
An improvement: “coordinated” disclosure

Rebranded “responsible” disclosure.

Bug bounties will sometimes bring a third party into the conversation, but be wary of compensation and action still being controlled by the manufacturer.

Disclosure Policies - why change!?

• A method by which negligent companies can give cybersecurity insufficient attention, while conveniently keeping outsiders (customers, investors, media, regulators) in the dark.

• An opportunity to mislead the public about product quality and company resiliency.
The case for more disclosure

Engaging with influencers and educators:

• Customers (opinion, trust)
• Media (content, customer opinion)
• Government (regulation, law, policy)
• Competitors (strategy, PR)
• Non-profits (strategy)
• Financial Analysts & Investors...
Public markets: A way to raise security standards

• Rarely is there a publication on investment strategy, active or passive, where there is NOT an opportunity for cybersecurity expertise

• Financial analysts examine company financial data, security analysts examine company software.

• Both are valid approaches for assessing company health and serving investors.

In an article for Bloomberg View last week titled “Why It’s Smart to Worry About ETFs”, Noah Smith wrote the following prescient truth: “No one knows the basic laws that govern asset markets, so there’s a tendency to use new technologies until they fail, then start over.” As we explored in WILTW June 1, 2017, algorithmic accountability has become a rising concern among technologists as we stand at the precipice of the machine-learning age. For more than a decade, blind faith in the impartiality of math has suppressed proper accounting for the inevitable biases and vulnerabilities baked into the algorithms that dominate the Digital Age. In no sector could this faith prove more costly than finance.
Meet the customer: Investors

- Institutional as opposed to individual*
- Active as opposed to passive*
- Activist as opposed to active*

*for now
Activist investors

• Change agents, often highlighting fraudulent or negligent behavior

• Not always about a trading position, some are looking for takeovers, change of control, board seats, etc

• Extremely experienced and sophisticated extended teams of analysts, traders, bankers, lawyers, experts, private investigators, and PR firms

• Produce research papers addressing management, operations, capital structure/business and strategy, criticizing past decisions and functions that are not considered best practice.

• The process is a mirror of ours, and something we can learn from
  • Traditional cyber: research noisily (think fuzzer presentations at BH!), disclose behind closed doors
  • Traditional finance: secret research then disclosure with impact
Short sellers

• Subset of activist investors that take short positions to highlight deficiencies

• What is short selling?
Short sellers

- Subset of activist investors that take short positions to highlight deficiencies

- What is short selling?
A few clarifications

• Short selling is not illegal, but it is regulated and sometimes (usually temporarily) banned
• Short selling doesn’t rely on inside information
• Short selling has been shown to:
  • highlight deficiencies in company practice
  • correct market prices
  • increase liquidity
  • limit upward market manipulation
Activist investor/short seller research

- Invest in significant diligence and third-party consulting services to analyze the target’s business, AND, TECHNOLOGY
- Relatively new, contributing to short positions for now
- Potential future opportunities?
  - long positions
  - M&A activity
  - Optimizations for algorithmic trading
  - etc
Cybersecurity as contributing research

- Bugs as an indicator of low quality (insecure) product
- One bug isn’t enough – we are highlighting ongoing inattention to product security
- POC’s are nowhere near useful. Need at least a couple of exploits.
- Exploits need to be repeatable & reliable.
- A certain amount of work upfront (pre engagement)
- Hardware beats firmware beats software
Non-technical aspects

• Be prepared to open the kimono
• From sharing source code to workplace inspections through to extensive background checks for all involved.
• Research integrity needs to be verified, and that includes the folks behind it
• Communications are critical
  • Documentation in understandable language
  • Demonstrations. Over and over.
  • Explanation. Depending on the project this may include media, financial analysts, regulators, etc.
• Our contributions at this early stage are limited. Your work will probably be part of a bigger picture, eg
  • Company history of incompetence?
  • Staffing issues?
  • Misrepresentations, lack of transparency etc
Even when it all lines up, there still may be no trade

Other factors:

- Material significance of the technology (company revenue linked to the technology)
- Understandability of the problems, especially for those who matter (investors, analysts, media, customers)
- Company track history, including likely handling of incident, past problems, litigation
- Regulator influence
- Difficulty to fix the problems (hardware issues will have more impact)
- Trading specs, including liquidity, volume, trading cost
Risk

- Short sellers are expert at risk evaluation
- No limit to downside (the stock can continue to rise indefinitely), so research is extremely thorough
- Litigation readiness is a cost of doing business
- Managing aggressive responses (target companies have their own extensive PR and lobbying machines)
Cyber Shorts: An Innovation

Creativity (highlighting deficiencies by pulling together multiple perspectives) plus value (alternative revenue for researchers!)

Red teaming that actually brings change to company behaviour

• Raising standards by highlighting inadequacy
• Enforced accountability
• Increased transparency
• Improved operations
• Improved (customer) trust
Takeaways

• We’ve made it to the boardroom, but we’re still seeing inattention.

• A bug probably won’t influence company behaviour, but it can educate the market, and the market will influence company behavior.

• You have options other than “coordinated disclosure” or full disclosure

• Short selling: Don’t try it at home.
"I'm not critical because I'm short; I'm short because I'm critical" - David Einhorn

Thank you, BruCon

Email justinembone@gmail.com
Cell +1 305 301 1831
Twitter @justinembone