Addressing the Asymmetry Problem

Bob Cowles

bob.cowles@gmail.com

BrightLite Information Security

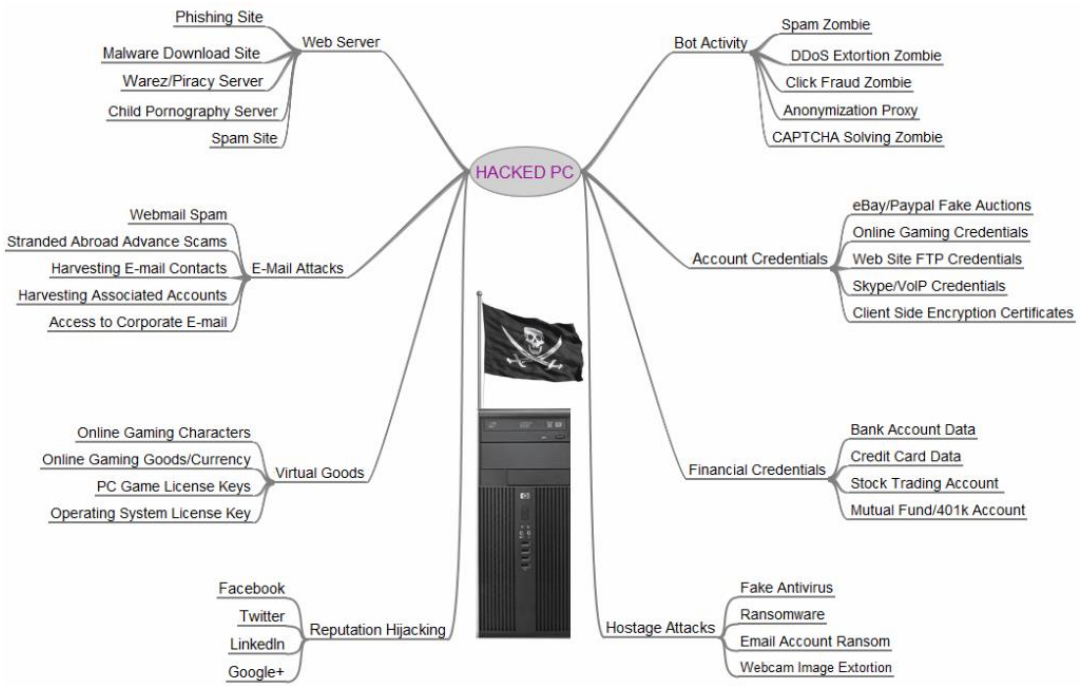
3 August 2016

QRS 2016 – CRE Workshop Panel Discussion

Vienna, Austria

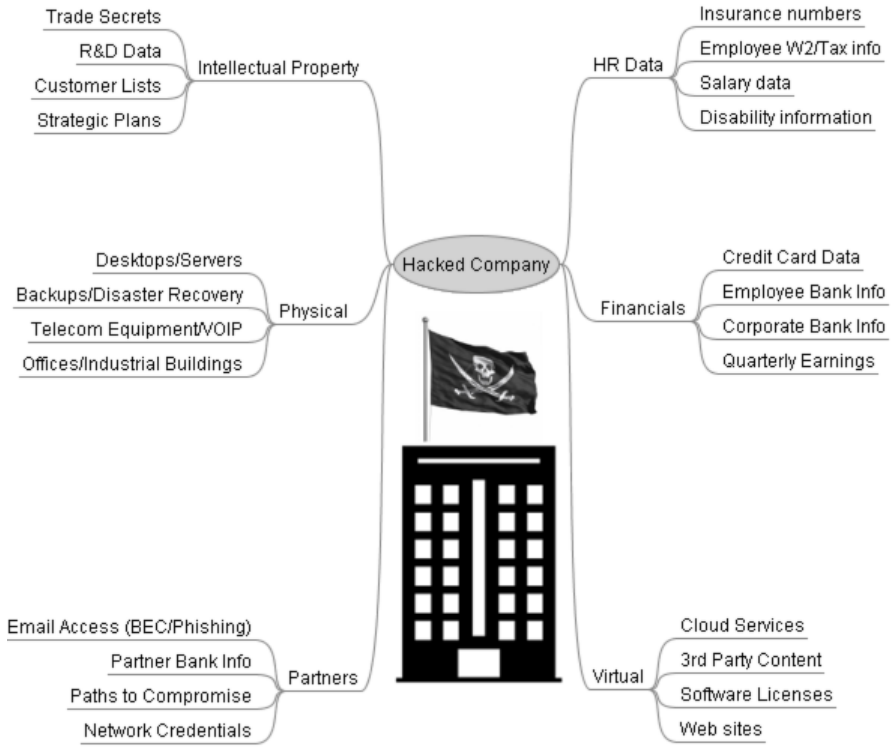
Value of a Hacked PC

http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/



Value of a hacked Company

http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/



Defense Economics (Ponemon-Jan2016)

https://www.paloaltonetworks.com/content/dam/creative-assets/campaigns/corporate/ponemon-report/web-assets/PAN_Ponemon_Report.pdf

- Attacker motivation is typically monetary gain; hoping for big payout
- Significant improvements in tools make attacks easier and quicker
- Many attackers (60%) will quit if not successful in 40 hours
- A good IT infrastructure will keep out most attackers
- Organizations should focus on:
  - People: Security awareness including combating phishing attacks
  - Process: Integration of security; incident response; clear policies
  - Technology: Threat intelligence sharing; integrated security platforms

Data Breach Costs (Ponemon-Jun2016)

https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

- Global average cost of $158 per record
  - Cost is double in healthcare and financial industries
  - Cost lower in research and public sector
- Approx 48% caused by external or internal malicious activity
- Significant part of cost due to lost customers / business
- "In addition to cost data, our global study looks at the likelihood of a company having one or more data breach occurrences in the next 24 months. We estimate a 26 percent probability of a material data breach involving 10,000 lost or stolen records."
- $158 x 10,000 = $1.58M … x 0.26 ~ $400K 2year expected loss
- A cybersecurity program won't necessarily prevent this!!!!

What should NOT be a Cybersecurity Cost?

- Good business to have good cybersecurity
  - Effective policies including personnel policies
  - Business procedures have integrated security
  - Engaged senior management and business process owners
- Effective IT infrastructure is good cybersecurity
  - Configuration management and patch management
  - Identity management and access controls
  - Event tracking, and log collection and maintenance
  - Backups and disaster recovery

What is left for "Cybersecurity"?

- Monitoring (network and log analysis)
  - External attacks
  - Internal suspicious behavior
- Threats seen by peers ("threat intelligence")
- Incident Response
  - Investigate (Is there a problem?)
  - Curtail
  - Investigate (What happened?)
  - Approve restoration plan
  - Insure Remediation
  - Reporting

Cybersecurity Expenditures – Case Study

- Study of US Department of Energy open science labs
- Used publicly available data on budgets for lab, IT, and cybersecurity
- Six Office of Science labs: varying size, varying mission
- Size matters: Larger labs spend less as % of total budget (~0.5%)
- Mission matters: Unclassified labs spend ~9-10% of IT budget
- Issues: What counts as IT? What counts as cybersecurity?

Cybersecurity Costs: DOE Open Science Labs

FY2017 Total	Cyber Funding	
46832	843	1.80%
76882	816	1.06%
125574	1119	0.89%
394639	2560	0.65%
543072	2458	0.45%
643886	2940	0.46%

Total IT	Cyber Funding	
3020	843	27.91%
6866	816	11.88%
10820	1119	10.34%
30729	2560	8.33%
25467	2458	9.65%
31801	2940	9.24%

Cost Asymmetry to Large to Overcome

- Defense gets harder; attack tools make attacks easier
- Potential for “the big score” helps motivate attackers
  - Like buying a lottery ticket
- Costs/sizes of data breaches continually increase
  - More organizations are storing more data
- Economies of scale beyond reach of most organizations
  - ~ $500M Total budget
  - ~ $25M IT Budget
- Targeted organizations need to spend even more
- Attacker costs: Phishing emails or a few flash drives in the parking lot

Solution: Change the Calculation

- Defender
  - Decrease costs through economies of scale
  - Decrease financial exposure / liability
- Attacker
  - Increase the cost of attack
  - Decrease the value of a successful attack

Defense: Cost(decrease)/ Liability(decrease)

- Outsource cybersecurity to external or parent organization
  - Leverage economies of scale to reduce costs
- Use cloud services (with care)
  - Again, capture economies of scale
  - Outsources infrastructure and cybersecurity
- Insurance (tread very carefully)
  - Move the liability
- Reduce data breach cost
  - Encrypt sensitive data in motion and at rest
  - Eliminate unnecessary data

Attack: Cost (increase)/ Reward (decrease)

- Effective IT infrastructure
- Educate staff in good security practices, policies, and procedures
- Reward those who responsibly report security issues
  - Staff
  - White hats
- Reduce value (to attacker) of stored information
  - Encrypt sensitive data in motion and at rest
  - Eliminate unnecessary data

Vielen Dank!

Bob Cowles

 bob.cowles@gmail.com

 @CowlesBob