UNIVERSITY OF AGDER

NTNU
Norwegian University of Science and Technology

Strathmore UNIVERSITY

UNIVERSITY OF NEBRASKA OMAHA

How does the second economy influence trends in information security?

Jose J Gonzalez

josejg@uia.no

Professor
Faculty of Engineering and Science
Centre for Integrated Emergency Management
University of Agder
NO-4898 Grimstad, Norway

Content

- The threat landscape in the second economy
- Misaligned incentives
- Black markets for vulnerabilities and exploits
- Credit card exploits
- Ransomware
- Automation and the Internet of Things
- The asymmetric battle between black and white hats
- Unintended outcomes
- Defense opportunities

Guiding questions for trend identification

- How has the threat landscape changed over time and what is likely next?
- Where are preconceived security notions limiting successful outcomes for victims in the fight?
- What measures can organizations take to protect themselves?

Threat landscape (1)

- Cyber attacks become more and more sophisticated
- Attacks designed to be inconspicuous in nature
  - longer exploit time
  - greater damage to victim
  - higher financial reward for attacker
- Insider attacks
  - Ponemon Institute study: 35 percent of companies in 2015 suffered a cyberattack from a malicious insider

Threat landscape (2)

- External attackers often succeed by exploiting people as weakest link
- Attack on Target (international retailer with more than 340,000 employees) 2013
  - compromised bank accounts of ca. 40 million customers
  - exposed personally identifiable information for about 70 million more customers
  - Costs for Target
    - full-year profits down by more than one third
    - US$150 million in investigative costs
    - US$116 million in settlement costs with banks and consumers
    - loss of invaluable customer trust
  - Actual insider: small supplier with remote access to Target
    - Target's supplier portal listed suppliers with contact information
    - Attackers used social engineering

Threat landscape (3)

- Social engineering techniques, like phishing, are on the rise
  - multiple potential failures in people who collectively are connected to a particular company target
  - Asymmetric situation
    - For full protection, defenders must have zero exploitable vulnerabilities
    - attackers succeed if they identify and exploit one vulnerability

Threat landscape (4)

- Phishing statistics
  - Anti-Phishing Working Group found at least 123,972 unique phishing attacks worldwide in the second half of 2014
  - Verizon (2015)
    - more than one in five recipients open phishing messages
    - more than one in ten click on attachments
    - median time to first click came in at ca. 80 seconds
- Compare with companies' response:
  - more than ten hours to remove a phishing threat
    - despite average cost per phishing or social engineering incident at US$ 86,000

Bad incentives, bad security

- Quote from famous article that appeared 2006*:
  - *"Over the past 6 years, people have realized that security failure is caused at least as often by bad incentives as by bad design. Systems are particularly prone to failure when the person guarding them (the principal) is not the person who suffers when they fail."*
  - Ten years later the statement is more true than ever!
- Key questions:
  - Which categories of misaligned incentives exist?
  - How do misaligned incentives cause security failures?
  - How can proper incentives be implemented?

* R. Anderson & T. Moore, "The Economics of Information Security". Science **314** (5799), pp.610–613, 2006

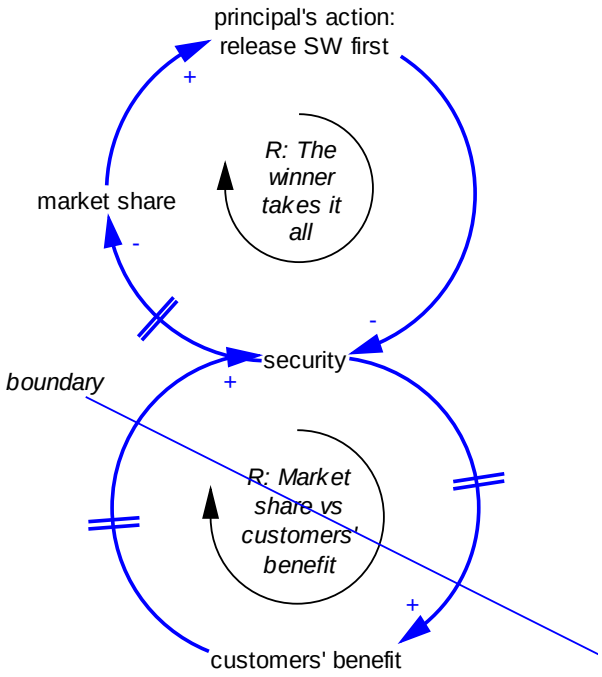
Overview of some common bad incentives

- Principal pushes responsibility on third parties
  - Paper presented in my NISlab lecture 2016
- Network externalities effects
- Asymmetric information
- Tragedy of the commons
- Odds on the black hat hackers

Network externalities effects

- Network externalities effects stimulate software producers to get on market as soon as possible to lock in the customer, increasing market share.
- Extensive security SW testing suffers.

Network externalities effects



'Relative achievement archetype'

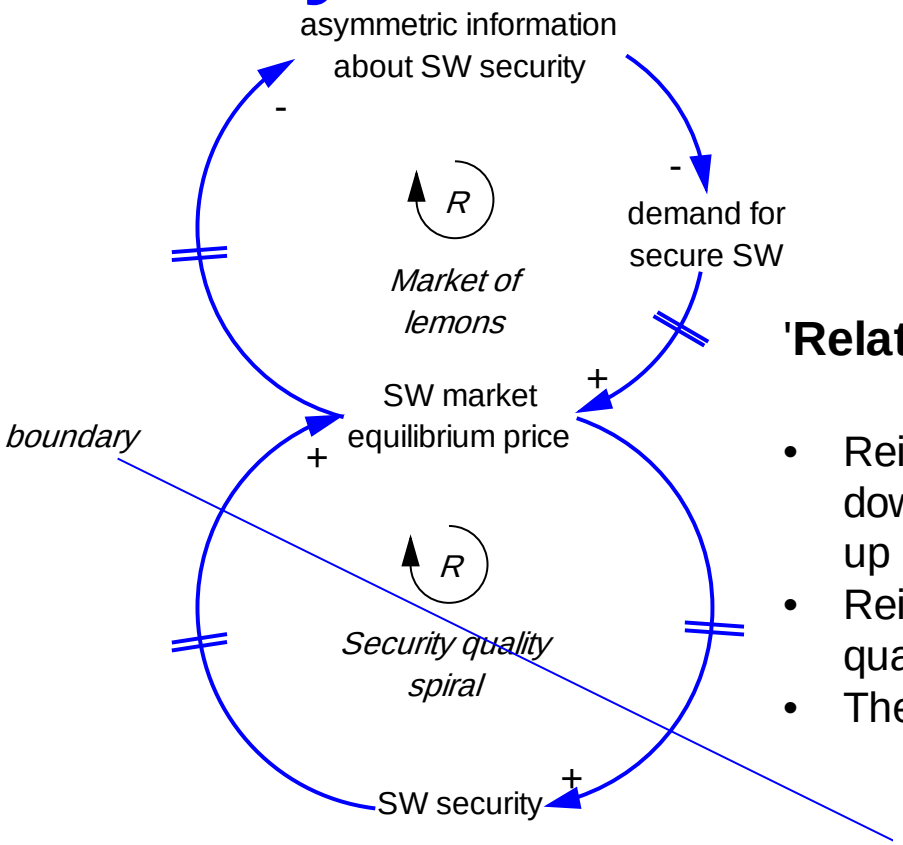
- Reinforcing feedback (the winner takes it all») benefits the SW developer
- Reinforcing feedback («Market share vs customers' benefit») hits customers and further erodes security.
- There are not satisfactory solutions yet

Network externalities effects stimulate software producers to get on market as soon as possible to lock in the customer, increasing market share. Extensive security SW testing suffers.

Asymmetric information

- “Market of lemons” was Akerlof’s paper about the impact of asymmetric information on demand for quality products
- The paper led to his being awarded the 2001 Nobel Memorial Prize in Economic Sciences

Asymmetric information



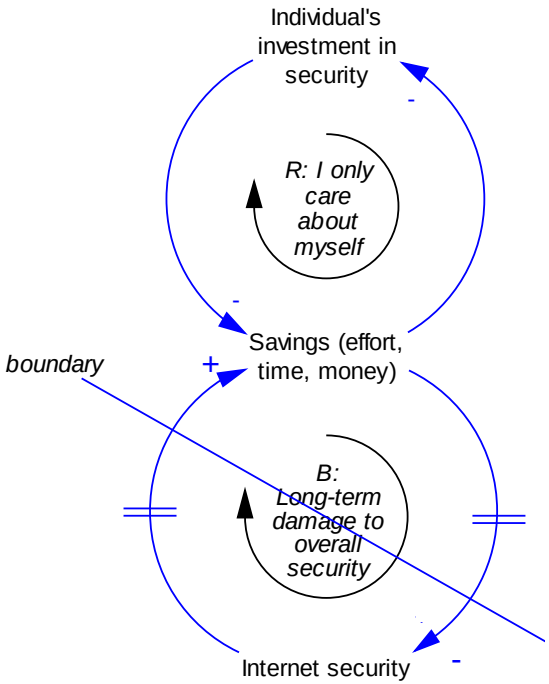
Problem archetype

'Relative achievement archetype'

- Reinforcing feedback drives price down and asymmetric information up ('market of lemons')
- Reinforcing feedback drives SW security quality spiral downward
- There are not satisfactory solutions yet

"Market of lemons" was Akerlof's paper about the impact of asymmetric information on demand for quality products that led to his being awarded the 2001 Nobel Memorial Prize in Economic Sciences

Tragedy of the commons



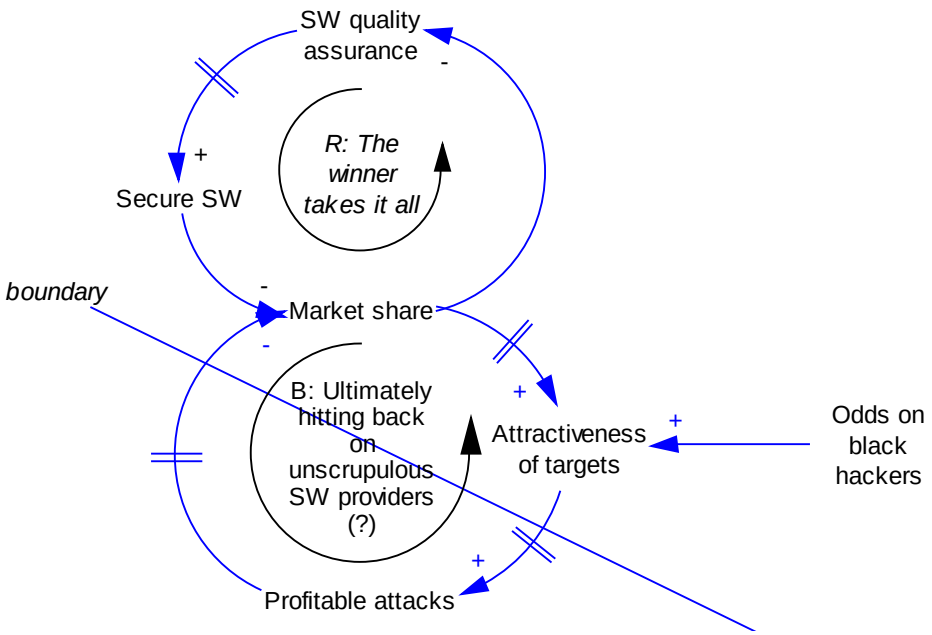
Problem archetype

Underachievement archetype'

- Reinforcing feedback drives an egoistic attitude (saving on security – letting others spend)
- Balancing feedback drives overall security downward to the long-term detriment of all
- There are not satisfactory solutions yet

Users are not motivated to spend on security, since who suffers most from bad security are third parties, when computers are used for spam or denial of service attacks

Odds on the black hat hackers



Underachievement archetype'

- Reinforcing feedback drives being first to the marked
- Balancing feedback will possibly compromises the market share in the very long-term
- There are not satisfactory solutions yet

Problem archetype

Owing to insufficient quality assurance, in part because users do not sufficiently appreciate security, the number of undiscovered SW vulnerabilities is huge – the odds are on the side of the black hat hacker to discover zero-days vulnerabilities that white hat hackers would not find in advance

Black market for small transactions

- Targeting big heist from wealthy people in the second economy presents risk
  - Long preparations with social engineering give the criminals much time, but only until they have taken the money
  - When big quantities are pocketed, cybercriminals face a time disadvantage, viz. to spend or to hide the money while remaining under the radar
  - Hence, big heists are becoming rarer as cybercriminals favour economy of scale:
    - Plenty of small thefts from everyday people
    - Hence, cybercriminals infiltrate databases of proprietary customer and employee information

Black market for credit card accounts

- In the Internet's black markets you can buy all kind of information from credit card accounts for different price depending on country
  - Credit card account with card verification value for 5 – 30 US$
  - The same plus bank account number: 15 – 30 US$
  - Date of birth too: Add 5-15 US$
  - All this plus full name, billing address, card expiration date, PIN, social security number, etc: Add 15 – 30 US$
  - The victim's shopping patterns, so that the cybercriminal's transactions look normal: Add more US$
  - *Emerging defence: credit card numbers with dynamic tokens that change with every purchase*
  - Also, since there are risks in monetizing the payoff, cybercriminals look for a less risky activity

Ransom in the First Economy

- Ransom means the price or payment for the release of property or a person who has been kidnapped.
- Kidnapping is risky business for the criminals
  - The act of kidnapping presents risks in detection
  - The hostage may have arms or bodyguards
  - Contacting the victim's relatives to ask for ransom may get the police involved
  - The ransom drop presents risks in detection, and - even if one is not caught - the bills delivered may have been marked or may even be forged, i.e., worthless

Ransom in the 2nd Economy

- Criminals are moving to ransomware exploiting the opportunities of the Second Economy.
  - The ransomware malware locks systems by encrypting files and demanding ransom to obtain the decryption key
    - The victim is put under very strong time pressure: “pay soon a certain quantity in bitcoins or else you will never get access to your files (they will be destroyed)”
  - Ransom less risky for the criminal than in the first economy:
    - Virtually impossible to track the cybercriminal, whether attack preparation, attack itself, or tracking the payment in bitcoins
  - Cybercriminals can target anybody, not only rich people.
    - They can take much less ransom per incident, providing huge increase in targets (anybody can be a target), while scaling up to huge aggregate profits.
    - Perversely: the “success” of software like CryptoLocker generates trust among victims that paying ransom will release their files

Ransom in the 2nd Economy: Critical Infrastructure

- Critical Infrastructure (CI):
  - assets that are essential for the functioning of a society and economy (such as public health, transportation systems, energy generation and distribution, financial systems, telecommunication)
- Cybercriminals locking critical files in CI can put enormous pressure and demand high ransom
- Examples show they can:
  - February 5, 2016, Hollywood Presbyterian Medical Center (HPMC) in California: ransom payment US$ 17,000 in bitcoins
  - In the weeks after, several hospitals across USA suffered ransomware attacks
- Emerging trend: More and bigger attacks on CI?

Trend: Automation

- More automation, many more targets!
  - systems once isolated and mechanically driven are increasingly networked and automated or controlled remotely via Internet, often wirelessly
  - great expansion of the targets and types of cyberattacks
- As with software, automation developers target “first to market” strategy
  - Security is sacrificed
  - devices in the “Internet of Things” are easily vulnerable to hacking
- The Internet of Things – see next slide

Trend: Internet of Things (IoT)

- The Internet of things (IoT):
  - inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity
  - IoT allows objects to be sensed or controlled remotely across existing network infrastructure
  - direct integration of the physical world into computer-based systems
    - Target: improved efficiency, accuracy and economic benefit in addition to reduced human intervention.
    - complex labyrinth uniting physical and virtual worlds.
    - each connected thing must now be secured, lest it provides an open door through which the adversary can enter to cripple infrastructures once quarantined from the virtual realm.
- IoT estimate: 30 billion objects by 2020

Ransom in the 2nd Economy: Internet of Things

- Enormous opportunities for cybercriminals
  - Plenty of targets where life is at stake, e.g. self-driving vehicles
    - Five Lessons On The 'Security Of Things' From The Jeep Cherokee Hack
    - A connected car uses software with ca. 100 million lines of code
      - Android operating system has 12 million lines of code
    - Hackers could ransom **all** vehicles with a particular software vulnerability and demand, say US$ 100 in bitcoins for ignition to start
    - Drivers would be under enormous time pressure and would pay ransom – volume of scale, low ransom acceptable
  - Plenty of targets within the Critical Infrastructure
    - Hospitals, energy grids, banks, …

White vs Black Hats (1)

- In cybersecurity, black hats determine the R&D agenda
  - R&D advancements serve black hats to launch a strike
    - White hats are taken by surprise, not knowing the timing, origin, or nature of the attack
- In cybersecurity, time is a white hat's enemy
  - In normal conditions, software engineers run test cycles at off-peak hours to not disrupt the business
  - When a cyberattack occurs, white hats must act at peak hours under huge time pressure
- Productivity trumps security
  - If employees must choose between security and productivity, the latter mostly wins
    - Lots of studies document this

White vs Black Hats (2)

- Cybersecurity return on investment (ROI) is fuzzy
  - ROI calculations depend on proving increase in productivity or other organizational advantages
    - How prove the worth of white hats?
      - They get kudos if nothing happens!
    - How document the costs saved in a diverted attack ?
- Cybersecurity has a back-office existence
  - 2016 study: 82 percent of board members were concerned about cybersecurity
    - only one in seven CISOs reported directly to the CEO and most were left completely off the board.
- Traditional IT professionals need only understand the product, not the motivations of its developer
  - White hats must understand both the product and the motivation of the attacker

White Hats Must Specialise

- Skills needed
  - Security architects : *“How may the enemy infiltrate?”*
  - Security operators: *“How is the enemy infiltrating?”*
  - Incident responders: *“How do I respond, now that the enemy has infiltrated?”*
- Different skills – different priorities
- Finger pointing when tension is high
  - Incident responders blame security operators
  - Security operators blame security architects
  - Security architects blame incident responders and security operators

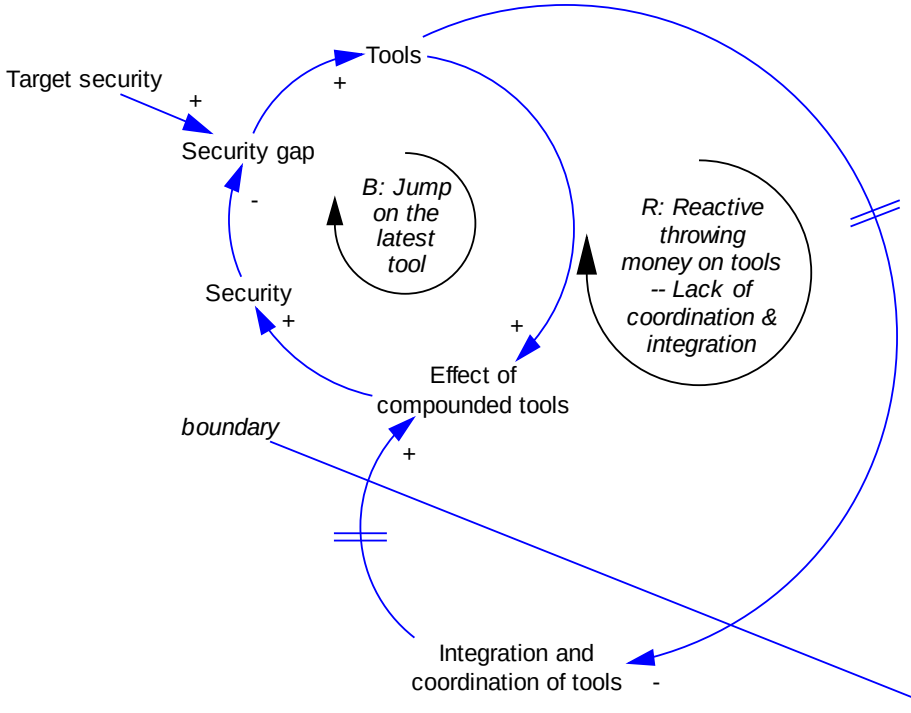
White hats: Belief in Technology

- Deploying ever more sophisticated technologies
  - Hoping for the silver bullet
    - Result:
      - Complexity
      - Lack of coordination and integration
- Cybersecurity software vendors:
  - Act as “arms dealers”
  - Exploit the anxiety of white hats
    - More than half of IT executives state: “they would still jump at the chance to purchase new, improved security software”
    - one in four say there is no limit to what they would pay for something more effective and reliable

Belief in new technology

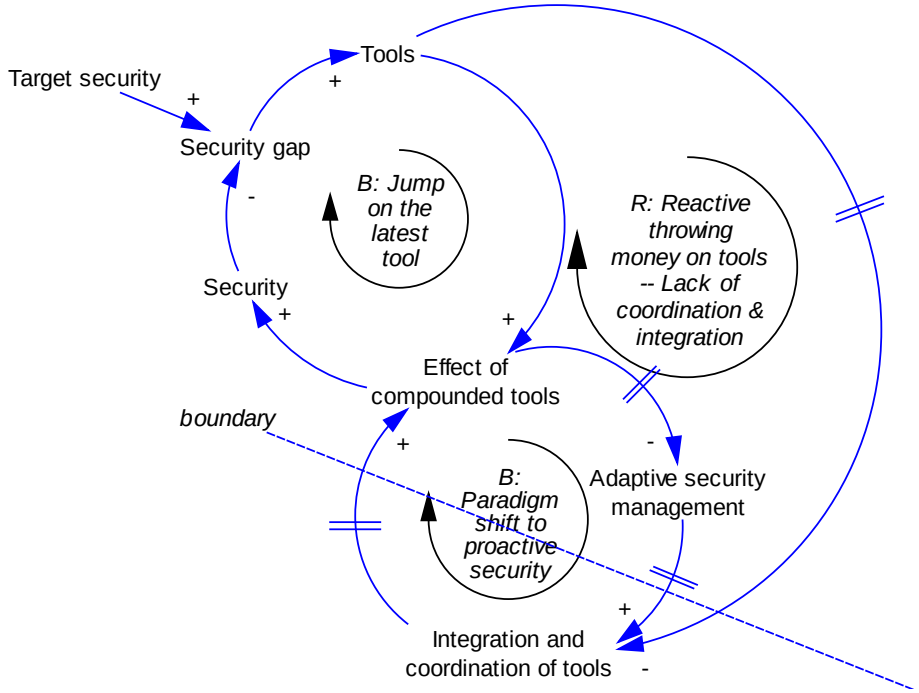
- Organizations are throwing money at the problem
  - Investing in the latest tools in the market, without proper strategy, integration and coordination
    - See archetype on next slide
  - Needed:
    - thorough change in the organization, from the boardroom to security operations, to successfully address current threats and prepare for future ones
    - moving from a siloed and reactive approach to an adaptive, aggressive, and proactive strategy

Problem archetype: Throwing money on tools



The unintended reinforcing feedback loops increases the dependence on tools with short time effects on security

Solution archetype: Paradigm shift to proactive security management



The solution requires thorough understanding of the formidable challenge of reshaping the organisational culture

White and Black Hats' Incentives

- Black hats: Clarity of incentives
  - They know what they are after
  - They can balance risk and reward when considering their opportunity
  - Black hats' incentive is linked to their ultimate goal
    - Consistent behaviour among the black hats community
- White hats: Unclear incentives
  - Torn between different priorities
  - Inconsistent behaviour among the white hats community
  - Limited budget and support from senior management
  - Growing number of adversaries
  - Employees aid black hats through poor security hygiene
  - *Worst: Misled by wrong incentives ("do something!")*

Asymmetric Battle (1)

- The adversary needs to succeed once while the defender must be right 100 percent of the time
- Defenders are overwhelmed
  - Only 26 percent of US organizations have capable staff to address cyber risks on implementation of new technologies
  - 2014: 50,000 postings for Certified Information Systems Security Professionals (CISSPs)
    - USA has about 65,000 CISSPs in total!!!
  - need for at least 9,000 and up to 29,000 more
  - 2015: more than 209,000 cybersecurity positions in USA unfilled, with postings up nearly 75 percent over the past five years

Asymmetric Battle (2)

- Demand for cybersecurity professionals is expected to rise to 6 million globally by 2019, with a projected shortfall of 1.5 million going unfilled by that time
  - more than one-fifth of jobs requiring ten or more years' experience sit vacant for at least a year
- Security managers in North America, Europe, the Middle East, and Africa:
  - significant obstacles against desired security projects
    - lack of staff expertise and inadequate staffing
    - less than one-quarter of enterprises have 24/7 monitoring in place using internal resources

Rules of the Cybersecurity Game (1)

- Black hats initiate
  - Ongoing challenges for white hats:
    - Where will the next threat vector emerge?
    - How could the organization be vulnerable?
- Black hats don’t play fair and act unconstrained
  - As opposed to white hats who should and are constrained
- Black hats change frequently the parameters of the game
  - Such as polymorphic viruses to obfuscate signature collection or sandbox evasion techniques
  - While white hats are confined by IT environments targeting stability

Rules of the Cybersecurity Game (2)

- Black hats have easy access to white hats defences
  - Cybersecurity defences are commercially available and can be analysed and reverse engineered
  - While white hats must first fall victim to get hold on the attack vector
- Black hats need only score once
  - While white hats must defend against all possible attacks
- Black hats leverage time to their advantage
  - Such as stealthily infiltration of the victim's fortress lingering undetected for as long time as possible
  - or leveraging time with ransomware to force victim to pay ransom

Rules of the Cybersecurity Game (3)

- Black hats have clear incentives
  - Whether for profit, ideology or enmity threat actors have clear incentives guiding their next move
  - Whereas white hats´ incentives are determined by superiors (political pressure) or circumstances (pressure to do something)
    - Misaligned incentives lead to wrong behaviour

Unintended Outcomes (1)

- Gartner:
  - by 2018, 25% of corporate data traffic will bypass perimeter security and flow directly from mobile devices to the cloud
- Two-thirds of cybersecurity professionals worried about “tool sprawl”
  - unintended consequence of deploying multiple disintegrated security technologies across one’s environment
    - counteracts productivity
    - disintegrated management and communications platforms are spiraling out of control for many cybersecurity first responders,
    - more difficult to detect threats or creating sufficient confusion to overestimate risk

Unintended Outcomes (2)

- Ca. 80 percent of company board members indicate they are concerned with cybersecurity
  - But caring about cybersecurity and aligning the correct incentives toward its acceptable outcome is not one and the same
  - Typically, organizations are chasing meaningless alerts in a tsunami of data that overwhelms their ability to properly diagnose an impending serious threat
  - Many organizations are being lulled to sleep by their own metrics, which may indicate cybersecurity “success,” all the while concealing an incapacity to respond to a disastrous black-swan attack
  - Cybersecurity professionals are indirectly encouraged to practice behaviors contrary to that which will improve a company’s security posture

Recommendations Against Unintended Outcomes (1)

- Kill hidden incentives misaligned to effective cybersecurity outcomes. Why?
  - CISOs, often indirectly encourage the adoption of the latest cybersecurity tool designed to cure what ails them
    - Outcome: “tool sprawl”
    - Current cybersecurity environments lack an integrated cybersecurity platform for fast implementation of the latest technologies avoiding multiplying operational complexity for already overburdened fast responders
- Acknowledge loss of effectiveness with adoption
  - A cybersecurity defense mechanism will greatly lose effectiveness once it has been widely adopted in market
    - The more adopters, the more incentives for to develop countermeasures
  - Defender must eliminate outdated solutions to reduce burden

Recommendations Against Unintended Outcomes (2)

- Change the scorecard
  - Organizations use scorecards measuring the number of incidents captured and responded to in given period of time
    - They assess large volumes of alerts that are largely untargeted in their nature
  - Instead, organizations should reevaluate the nature of threats to determine the probabilistic nature of any as part of a highly targeted campaign
- Are false positives a concern?
  - White hats are more concerned about false negatives (disregarding a real threat) than about false positives (alarms about something that is not a real threat)
    - False positives consume precious time…
    - And skillful adversaries use them to deceive by raising the noise level

References

- S. Grobman & A. Cerra. "*The Second Economy: The Race for Trust, Treasure and Time in the Cybersecurity War*". Apress Media LLC: NY. 2016
- R. Anderson & T. Moore, "The Economics of Information Security". Science 314 (5799), pp.610–613, 2006
- Gonzalez, J. J. & K. Lenchik (2016). The economics of cybersecurity: Boomerang effects from misaligned incentives. International Conference of the System Dynamics Society, Delft, The Netherlands.
- Gonzalez, J. J. & D. Trcek (2017). "Proper Incentives for Proper IT Security Management – A System Dynamics Approach." Proceedings of the Annual Hawaii International Conference on System Sciences 2017: 2388-2397