Cybercrime Business Models:

Developing an Approach for Effective Security against Better Organized Criminals

PTC Presentation | January 15, 2017
About the Authors

CHARLA GRIFFY-BROWN
Professor, Information Systems and Tech Mgt
Director, Center for Teaching & Learning Excellence
Graziadio School of Business and Management, Pepperdine University, USA

DEMETRIOS LAZARIKOS (LAZ)
CISA, CISM, CRISC, CSSLP, MBA, MCIS
IT Security Strategist and Two Time Former CISO
Blue Lava Consulting

MARK CHUN
Associate Professor,
Information Systems & Technology Management,
Graziadio School of Business and Management,
Pepperdine University, USA
Agenda

• Results and Methodology
• Evolution – How Did We Get Here?
• What Organizations Can Do - InfoSec Maturity Model
• Where Do We Go From Here?
By 2017, the global Cyber Security market is expected to skyrocket to $120.1 billion from $63.7 billion in 2011.

Motivations Behind Attacks
November 2016
- Cyber Crime: 82.7%
- Hacktivism: 9.3%
- Cyber Espionage: 4.0%
- Cyber Warfare: 2.7%
- N/A: 1.3%

Organization Drill Down
November 2016
- Non-Profit: 28.6%
- Trade Union and Professional: 14.3%
- Activism: 14.3%
- NGO: 14.3%
- Sport: 14.3%
- Politics: 14.3%

The estimated annual cost over global cybercrime is 100 BILLION

YEARLY CYBER CRIME VICTIM COUNT ESTIMATE
Collecting our Data

- Visited 27 cities throughout the world
- Meetings with 204 individuals in multiple verticals
- Total of 80 organizations
- Cross examination of reported incidents 1/15 - 8/16
- Business Model Evaluation by 70 business leaders across 11 verticals using NICE framework
- Top Items Emerged
  - The InfoSec Maturity Model
  - Majority of models involve ransomware
  - Business models with the highest scores demonstrated strong efficiency, complementarity and novelty
  - Modern cybercriminals are well organized, business savvy with advanced techniques for exploiting organizations
NICE Model

• **Novelty:** This refers to the renewal ability of the company. In essence, novelty refers to anything the company could be doing which represents a fresh new approach to the business previously unemployed in the industry or the market.

• **Lock-in:** Also known as switching costs, this criterion measures the company’s ability to create loyal repeat customers as well as partnerships that will not be dissolved in favor of the competition. Parties with a relationship with the company should remain with the company if ever the chance for making a choice arrives.

• **Complementarities:** This refers to how the various product lines of a single company and how complimentary are they to each other so that if a consumer is buying one, will he automatically feel the need to buy the second making his purchase more meaningful.

• **Efficiency:** This refers to transaction efficiency and proclaims that the more the volume of transactions, the less cost incurred by the company per transaction.

*Source: Amit and Zott (2012)*
## Evaluation and Scoring

<table>
<thead>
<tr>
<th>Business Model</th>
<th>Novelty</th>
<th>Lock-in</th>
<th>Complementarities</th>
<th>Efficiency</th>
<th>Average of All Scores</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distraction</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>Targeted Espionage</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>Market Manipulation</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>Algorithmically Coordinated Campaigns</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>Ransomware for causing Human Harm</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>Mass Mobile Injection</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>Source Code Injection</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>Adware Injection</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>Critical Asset Targeting</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>BIOS-Focused</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td><strong>Average Score</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Scale:** 1 = Very Weak; 2 = Weak; 3 = Viable; 4 = Strong; 5 = Very Strong
# Cyber Crime Models and Ratings

<table>
<thead>
<tr>
<th>Business Model</th>
<th>Description</th>
<th>Revenue Model</th>
<th>NICE score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distraction</td>
<td>Ransomware as a service attacks to distract authorities prior to a major planned events (such as major theft, social disruption or neighborhood/store robbery)</td>
<td>Ransomware is available as an on-demand service and payment is for a specific attack at a specified time purely as a distraction for another vector attack</td>
<td>4.5</td>
</tr>
<tr>
<td>Targeted Espionage</td>
<td>Ransomware asking not for payment in bitcoin but for passwords or other intellectual property. This was both large scale and smaller scale targeting individuals.</td>
<td>Business model is downstream payoff for other exploit leveraging the information gathered or selling the information gathered. For the attacker this model simplifies process and avoids the risk of block-chain/ledger being investigated down the road.</td>
<td>4.75</td>
</tr>
<tr>
<td>Market Manipulation</td>
<td>Using ransomware or electronic blackmail demand a CFO divulge financial performance data ahead of the next quarterly earnings and use the information to game the equities market.</td>
<td>Business model requires no payment, just a zipped spreadsheet. High costs for identification and tracking but high return with the right selection material.</td>
<td>4.74</td>
</tr>
<tr>
<td>Algorithmically Coordinated Campaigns</td>
<td>Algorithms can be used for evasion but also campaign efficiency based around the timing of coordinated campaigns. Algorithms have also been used to set-up and tear-down accounts, move bitcoins round and choose random fog networks for money retrieval. Algorithms have also been used to switch-up command and control communications.</td>
<td>Once written the core modules can scale indefinitely and be sold as a product or service.</td>
<td>4.8</td>
</tr>
<tr>
<td>Ransomware for causing Human Harm</td>
<td>Ransomware campaign that victimizes hospitals and medical centers worming through externally facing servers, deleting snapshot backups and encrypting an entire networks. This model could be applied to any critical infrastructure.</td>
<td>Backups are restored after ransom is paid.</td>
<td>4.7</td>
</tr>
</tbody>
</table>
## Cyber Crime Models and Ratings

<table>
<thead>
<tr>
<th>Business Model</th>
<th>Description</th>
<th>Revenue Model</th>
<th>NICE score</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mass Mobile Injection</strong></td>
<td>Gaining an Android or Apple footprint and using an automated set of text messages across a wide footprint installing ransomware. Could be applied to IoT (vehicles, etc).</td>
<td>Ransom demand to carriers or network operators.</td>
<td>4.45</td>
</tr>
<tr>
<td><strong>Source Code Injection</strong></td>
<td>Large open-source software distribution with ransomware attached.</td>
<td>Organization who use the software are asked to pay ransom.</td>
<td>4.6</td>
</tr>
<tr>
<td><strong>Adware Injection</strong></td>
<td>Adware/PUAs are used to auction off browser space of a compromised company. Sometimes combined with the ability worm, compromise credentials or target active directory.</td>
<td>Access to shell is sold to the winning bidder and used to upload whatever tools they want to target the host.</td>
<td>4.74</td>
</tr>
<tr>
<td><strong>Critical Asset Targeting</strong></td>
<td>Targeting a few critical assets and preventing restoration ahead of time. Large scale operations are most vulnerable.</td>
<td>Ransom of $1 less than the daily operations supported or halted by this attack.</td>
<td>4.4</td>
</tr>
<tr>
<td><strong>BIOS-Focused</strong></td>
<td>Using lower paid staff to stick in thumb drives that disable machines at the BIOS level. A link is sent after payment which restores your BIOS (but leaving a backdoor open for further exploit). Seen in hotels (delivered by cleaning staff).</td>
<td>Thumb drive distributors are paid per thumb drive and machine compromised. Ransom is multiplied and increased with each exploit.</td>
<td>4.37</td>
</tr>
</tbody>
</table>
RESULTS

• The majority of these models involve ransomware.

• Ransomware is a risk factor which needs to be more carefully noted amongst business leaders.

• The models with the highest score had the highest ratings in efficiency, complementarity and novelty.
How Did We Get Here?

Traffic

Third Party Vendor

FIREWALL POLICY

Web

FIREWALL POLICY

Apps

FIREWALL POLICY

DBs
Gartner estimates that East-West traffic will increase by 80% through 2016
The Big Switch?
What organizations can do:

• Current architecture in most firms is a “hot mess” lacking any perimeter BY DESIGN. Risk evaluation and governance is critical.

• Firms need a way to put together processes and tools for coordination and alignment to business to support hyper growth of emerging technologies and agile environments

• The InfoSec security model developed describes the companies examined but only a small percent are taking a risk-based approach and are therefore tied to a world with corporate “perimeters”

• Data Mining and Big Data Analytics for Leveraging User Behavioral Analytics - User Behavior Analytics have become more complicated leveraging machine learning with extreme context awareness capabilities built enabling pattern revelation and analysis (beyond threshold telling)

• Agile Development Striving for Continuous Integration and Continuous Delivery

• Evaluation of Cyberliability Insurance
InfoSec Maturity Model

Reactive

- Lack of Executive support
- Underfunded
- Understaffed
- Lack of metrics for reporting
- Set up for failure

Blocking & Tackling

Proactive

Compliance Driven

- Control-based security approach
- Align to mandatory regulations
  - ISO 2700x
  - FFIEC
  - PCI
  - HIPAA
  - EU/PII Data protection
  - NCUA

Risk-Based Approach

- Multi-layered security and risk-based approach
- Using behavior analytics
- Linking events across multiple disciplines
- Using dynamic InfoSec and IT Audit controls in the environment*

Source: Blue Lava Consulting
Results

Source: Blue Lava Consulting
What Organizations Are Doing

• Board of Directors and Executives are more involved with Information Security and IT Audit – budgets are approved faster

• Embracing multiple InfoSec and monitoring solutions for Internet of Things (IoT)

• Moving towards agile frameworks with exit criteria embedded through the idea, development, and support processes

• Investing in Big Data and User Behavior Analytics (UBA) solutions

• Evaluating cyber liability insurance

There is no silver-bullet to solving these complex issues
Addressing the Issues

Gartner estimates that East-West traffic will increase by 80% through 2016
# Aligning Information Security with the Business and PMO

<table>
<thead>
<tr>
<th>Stage</th>
<th>Activities</th>
</tr>
</thead>
</table>
| **Idea** | • What data will this application store, process, or transmit?  
• Is this a mobile or Internet-facing application? |
| **Dev** | • Security framework and standards review  
• Peer review / source code review* |
| **Test** | • Internal scans 24x7x365 (network, OS, and application)* |
| **Prod** | • External scans 24x7x365 (network, OS, and application)* |
| **Maint** | • What new functionality will be supported?  
• How will monitoring (external and internal) be incorporated?* |

*Using dynamic InfoSec and IT Audit controls in the environment
Dashboards and Reporting

• Create an inventory of issues and solutions within your environment

• Identify the risks, gaps, observations, and what you need to be successful with your program

• Generate reports in terms the business understands

Build relationships with internal stakeholders to achieve these goals
<table>
<thead>
<tr>
<th>Threat Vector</th>
<th>Problem Statement</th>
<th>Tools Implemented</th>
<th>Current Observations, Risks, and Gaps</th>
</tr>
</thead>
</table>
| **Application Security**      | Web application vulnerabilities lead to significant issues when P1s aren’t resolved with current SLAs. | 1. Training for developers (internal and third parties)  
2. External and internal scans 24x7x365 (WhiteHat)  
3. Penetration testing (3rd party quarterly tests)  
4. Source code analysis (WhiteHat SCA)  
5. Behavior analytics (RSA and Shape Security)  
6. WAF (Integrate with WhiteHat rules) | 1. There is 14% attrition with the developers.  
2. P1 appsec vulns are increasing by 12% a week.  
3. Integrate WhiteHat vulns with the WAF for automation. |
| **Innovation**                | Automobles  
Cloud (third party integration)  
IoT (eg. Wearables, Appliances, HVAC, Garage Doors)  
Virtualization | 1. Partner with manufacturers – insert InfoSec legal requirements into contract agreements  
2. Application scanning 24x7x365 (WhiteHat)  
3. Cloud integration (vArmour)  
4. IoT (WhiteHat and vArmour)  
5. Physical and virtualized management (vArmour) | 1. System of systems* will be in scope for PCI, HIPAA, GLBA, PII, Privacy, EU Data Protection. |
| **Network/OS/Systems**        | PCI 3.0 states that virtualized environments are in scope.  
The company needs to meet agile business requirements.  
The company needs to detect laterally moving traffic between the data centers, zones, supporting networks, and cloud integration. | 1. Elasticity and agility to spin up/down environments (vArmour)  
2. Network and OS scanner (Nessus)  
3. PCI 3.0 management of physical and virtualized environments (vArmour)  
4. File integrity monitoring (OSSEC agents)  
5. Monitoring internal (east/west) malicious traffic (vArmour) | 1. PCI 3.0 states that all virtualized environments that store, process, and transmit cardholder data are in scope.  
2. vArmour allows you to manage both physical and virtual PCI environments under one policy and one enterprise software solution.  
3. OSSEC agents are not being used and configured properly. |
| **Emerging Threats (Internal)** | The company needs a ways to identify, monitor, and combat emerging threats once cyber criminals break the perimeter. | 1. Monitoring ‘east / west traffic’ (vArmour) | 1. Internal traffic anomalies are increasing by 15% per month. Anomalous traffic patterns are moving between Zone X and Y and four data centers at 2:21am daily. |
| **External Mobile Security Applications** | Mobile device usage is increasing by 54% year over year. 15 mobile applications are being developed by external teams that are out of corporate compliance and do not meet mandatory industry regulations. | 1. Behavior analytics software (RSA)  
2. Monitoring mobile app stores (Risk I/Q)  
3. WhiteHat source code analysis (SCA)  
4. Cyber threat research (FOX-IT) | 1. Mobile source code being developed by third party organizations is not compliant with corporate InfoSec policies and industry regulations. |
| **Mobile Security (Internal/BYOD)** | The company needs to support the BYOD policy. | 1. Access controls (LDAP/AD)  
2. MDM (Good Technology) | 1. Need to determine how the MDM solution will scale over the next 12 months. |

Source: Blue Lava Consulting  
*Blue Lava Consulting ‘System of Systems’ research will be made available in Q1, 2015
Risk Frameworks

- CMM
- COBIT
- CVSS
- Home Grown
- ISO
- NIST
- OCTAVE
- RiskCalibrator
- RiskIT
- TARA

Ensure risk frameworks can be dynamic in your environment
Reporting in Business Terms

How much annualized web application cyber-risk does your organization have overall?

<table>
<thead>
<tr>
<th></th>
<th>Maximum</th>
<th>90th %</th>
<th>Average</th>
<th>10th %</th>
<th>Minimum</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0 - $2M</td>
<td>$10,054,932</td>
<td>$7,063,547</td>
<td>$5,530,918</td>
<td>$4,077,686</td>
<td>$1,701,978</td>
</tr>
<tr>
<td>$2.01 - $4M</td>
<td>$10,054,932</td>
<td>$7,063,547</td>
<td>$5,530,918</td>
<td>$4,077,686</td>
<td>$1,701,978</td>
</tr>
<tr>
<td>$4.01 - $6M</td>
<td>$10,054,932</td>
<td>$7,063,547</td>
<td>$5,530,918</td>
<td>$4,077,686</td>
<td>$1,701,978</td>
</tr>
<tr>
<td>$6.01 - $8M</td>
<td>$10,054,932</td>
<td>$7,063,547</td>
<td>$5,530,918</td>
<td>$4,077,686</td>
<td>$1,701,978</td>
</tr>
<tr>
<td>$8.01 - $10M</td>
<td>$10,054,932</td>
<td>$7,063,547</td>
<td>$5,530,918</td>
<td>$4,077,686</td>
<td>$1,701,978</td>
</tr>
</tbody>
</table>

Source: CXOWare, WhiteHat Security, and Blue Lava Consulting
User Behavior Analytics

• Deviation of a compromised user (or entity’s) behavior from its past or its peers

• Indicators of compromise but must be pattern woven together to distinguish a threat

• Behavior of entities can be mined to reveal anomalies

• Capture the footprint of the threat of actors as they traverse enterprise, cloud and mobile environments

• UBA uses advanced machine learning algorithms to baseline and detect anomalies

• Aberrations are then stitched into meaningful sequences over time revealing a kill chain (sequence of malicious events in each stage of the larger sequence)

• Unlike known thresholds the behavior based detection approach uses machine learning with extreme context awareness
(Internal) Sample Threats Detected UBA

- **Privileged Account Abuse**—inappropriate usage of access permissions
- **Privilege Escalation**—transformation of identity and access credentials
- **Data Exfiltration**—the act of stealing private, confidential and sensitive data within an organization by malware or an attacker
- **Unusual Activity**—accessing external domains, remotely accessing high privileged assets, and unusual login duration, time or location
- **Credential Compromise**—stealthy takeover of accounts for malicious purposes
External Sample Threats Detected Using a UBA

- **Account Takeover (ATO)** – compromise of privileged and regular accounts by external, malicious entity
- **Lateral Movement** – navigation of malware within a network
- **Command and Control Activity** – periodic beaoning activity by malware to communicate with CnC infrastructure
- **Data Exfiltration** – the act of stealing private, confidential and sensitive data within an organization by malware or an attacker
- **Browser Exploits and Malware Activity** – infection discovery of polymorphic attacks and advanced persistent threats (APTs)
Where Do We Go from Here

• Information Security must be part of the culture – driven by the Board of Directors and Executives throughout the organization

• Cyber criminals are evolving – we must as well

• It’s not *if* the cyber criminal will access your environment – it’s *when* – invest in current technologies and have a plan to address the issue

• User behavior analytics (UBA) is critical

• Evaluate your InfoSec and IT Audit programs frequently – ensure part of the program is to evaluate emerging technology

• Be flexible – introduce dynamic InfoSec and IT Audit controls in the environment
Questions:

Email: cbrown@pepperdine.edu
Phone: +1-310-420-2524