Evidence Based Risk Management

When analysis is used to uncover how sensitive data is stolen from organizations, who’s doing it, why they’re doing it, and what might be done to prevent it

Seán Paul McGurk

January 24, 2013
<table>
<thead>
<tr>
<th>Research</th>
<th>Uncover the who, what, when, how and why behind computer security incidents.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigations</td>
<td>Study and understand the ever-changing risk and threat environment. It all starts here.</td>
</tr>
<tr>
<td>Solutions</td>
<td>Leverage lessons learned from “R” and “I” to create new products and enhance our existing portfolio.</td>
</tr>
<tr>
<td>Knowledge</td>
<td>Cultivate and disseminate our information resources to make our people, products, and brand smarter than the competition.</td>
</tr>
</tbody>
</table>

The RISK Team = Risk Intel + Investigative Response + eDiscovery
Approach: IT Investigative focus

Diverse Investigator Backgrounds

Licensed Private Investigators

Truly Global Coverage – 24x7x365
- Investigators based in 16 countries
- Forensic labs and evidence storage facilities in Americas, Europe, and Asia-Pacific

No Subcontractors

Global PFI Firm

Annual Data Breach Investigations Report

Service offerings:
- IT Investigative Support (On-demand)
- Guaranteed Response (Retainer-based)
- eDiscovery and Litigation Support
- PCI Forensic Investigations
- Electronic Data Recovery / Destruction
- Incident Response Training
- Mock-Incident Exercises
- Corporate IR Program Development

Verizon RISK team has handled 8 of the world’s 10 largest data compromise investigations! *

*Source: http://www.idtheftcenter.com/
# Seven Sources of Threat Intelligence

<table>
<thead>
<tr>
<th></th>
<th>Source Description</th>
</tr>
</thead>
</table>
| 1 | **Threat & Vulnerability Intel**  
Track and analyze new software vulnerabilities and related attacks |
| 2 | **Underground Intel**  
Watch discussions, code sharing, planning,... Historically BBS, then Usenet, now more IRC and Cons... |
| 3 | **ICSA Labs Intel**  
Security product testing and security consortia operations. 400+ products |
| 4 | **Forensics Intel**  
Data and Intel from forensics investigations (200+ cases per year). |
| 5 | **MSS Intel**  
Data from IDS, FW, IPS, Applications… Management & Monitoring SOC operations |
| 6 | **Net Intel**  
Data from backbone. Sensors on more than 1 Million VzB addresses. Netflow Honey nets, Honey Pots... |
| 7 | **Studies & Surveys**  
VZB Studies, surveys (10+/yr), Others published data to drive Risk Models, equations & methodology |
Knowledge improves operations

For over 10 years, the **Security Management Program** has looked after the deployment, configuration, and upkeep of thousands of client systems on an ongoing basis.

Our **Vulnerability Management Services** identify and track common vulnerabilities and weaknesses present across clients and applications.

The **RISK team** monitors criminal activity and collaborates with law enforcement to understand the motives and methods that drive cybercrime.

The **Penetration Testing** team provides visibility into the numerous ways malicious agents can subvert defenses to exploit information assets.

Our **Investigative Response** unit investigates hundreds of cases per year, providing quality metrics on the agents and actions that frequently contribute to security incidents.

**Sensors and systems** spread across Verizon’s vast network infrastructure collect data 24/7 to stay abreast of current and emerging threats.

Verizon’s **PCI-DSS consultants** work with hundreds of clients each year and provide assessment results for the body of controls required in that standard.

**ICSA Labs** continually tests the reliability and effectiveness of security products against an ever-changing threat environment.

As our **Governance, Risk, and Compliance** services work with clients to align security posture with risk tolerance, they gain perspective into how incidents affect organizations.

We track the growing number of **external reports on organizational losses** (i.e., corporate 10Ks) and studies that quantify the consequences of security incidents.

**Applied Asset Data**

The **RISK Intelligence** team tracks asset usage to help assess the criticality of published vulnerabilities and guide recommendations to our client base.

Knowledge of prevalent vulnerabilities and related exploits guides our **Application Risk Assessment and SDLC training teams** in delivering more effective services.

**Applied Threat Data**

Our top-rated **Managed Security Services** incorporate intelligence on emerging threat sources and patterns to better protect client assets.

The **Virtual Discovery and Classification** service draws from intelligence around threat capabilities to better identify and classify suspicious network activity.

Verizon’s **PCI-DSS consultants** use lessons learned from our forensic investigators about financially-motivated crime to deliver more informed and relevant assessments.

The **Security Management Program** incorporates threat frequency data into the models that drive risk scoring and reporting to clients.

**Applied Control Data**

**Professional Services** teams utilize control usage data to drive baseline comparisons for clients and enhance the value of deliverables.

**Quantitative Risk Management (QRM)** service leverages control effectiveness data to prioritize security initiatives and provide managerial decision support.

**Applied Impact Data**

A new **Incident Analytics Service** leverages the VERIS impact model as well as loss data collected by RISK Intel to create unique and powerful metrics.

The **Governance, Risk, and Compliance** group uses historical impact data to improve the accuracy of risk assessments and better counsel clients.
• Malicious cyber activity is routinely directed at the U.S. Government, private sector, and academia
  – Growing more sophisticated, targeted, and prevalent
  – Nature and source of the threat is diverse
  – Designed to
    • Exploit data gathered from information systems or networks (computer network exploitation)
    • Disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves (computer network attack)
• We have insight on intrusions into private sector networks, but are becoming more aware of U.S. information infrastructure vulnerabilities to cyber attacks
  – Key factors: dynamic business environment, reliance on open systems and COTS, management/enterprise networks’ Internet connections
  – Key challenges: Your sensitive data isn’t just on your network, it is on your vendors networks, consultants networks, suppliers networks, etc.
Cyber Security Consequences

- The Intelligence Community has information from multiple sources of cyber intrusions followed by extortion demands
  - Encrypting corporate data/demanding money to decrypt the data
- Theft of sensitive corporate data
  - Industrial espionage costs US businesses up to $250 billion per year
  - 98% of breaches were attributed to external agents
- Theft of personal data
  - Attacker/there is typically motivated by profits (value is approximately $8 per record)
  - 855 investigated incidents with over 174 million records compromised
- Cyber attacks have been used to disrupt critical services in several regions outside the U.S.
Cyber Threat Vectors

### Threat Level 1
**“Garden Variety”**
- Inexperienced
- Limited funding
- Opportunistic behavior
- Target known vulnerabilities
- Use viruses, worms, rudimentary trojans, bots
- Acting for thrills, bragging rights
- Easily detected

### Threat Level 2
**“Mercenary”**
- Higher-order skills
- Well-financed
- Targeted activity
- Target known vulnerabilities
- Use viruses, worms, trojans, bots as means to introduce more sophisticated tools
- Target and exploit valuable data
- Detectable, but hard to attribute

### Threat Level 3
**“Nation State”**
- Very sophisticated tradecraft
- Foreign intel agencies
- Very well financed
- Target technology as well as info
- Use wide range of tradecraft
- Establish covert presence on sensitive networks
- Difficult to detect
- Supply interdiction/hardware implants

Confidential and proprietary materials for authorized Verizon personnel and outside agencies only. Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement.
8 years of investigations and research
2000+ confirmed data breach cases
More than 1 billion stolen records
Figure x. Countries represented in combined caseload

Countries in which a breach was confirmed

- Australia
- Austria
- Bahamas
- Belgium
- Brazil
- Bulgaria
- Canada
- Denmark
- France
- Germany
- Ghana
- Greece
- India
- Ireland
- Israel
- Japan
- Jordan
- Kuwait
- Lebanon
- Luxembourg
- Mexico
- Netherlands
- New Zealand
- Philippines
- Poland
- Romania
- Russian Federation
- South Africa
- Spain
- Taiwan
- Taiwan, Province of China
- Thailand
- Turkey
- United Arab Emirates
- Ukraine
- United Kingdom
- United States
Figure 8. VERIS A4 Grid depicting the frequency of high-level threat events

<table>
<thead>
<tr>
<th></th>
<th>Malware</th>
<th>Hacking</th>
<th>Social</th>
<th>Misuse</th>
<th>Physical</th>
<th>Error</th>
<th>Environmental</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ext</td>
<td>Int</td>
<td>Prt</td>
<td>Ext</td>
<td>Int</td>
<td>Prt</td>
<td>Ext</td>
</tr>
<tr>
<td>Servers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality &amp; Possession</td>
<td>381</td>
<td>518</td>
<td>1</td>
<td></td>
<td>9</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>Integrity &amp; Authenticity</td>
<td>397</td>
<td>422</td>
<td>1</td>
<td></td>
<td>6</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Availability &amp; Utility</td>
<td>2</td>
<td>6</td>
<td></td>
<td></td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality &amp; Possession</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity &amp; Authenticity</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability &amp; Utility</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality &amp; Possession</td>
<td>356</td>
<td>419</td>
<td>1</td>
<td></td>
<td>1</td>
<td>86</td>
<td></td>
</tr>
<tr>
<td>Integrity &amp; Authenticity</td>
<td>355</td>
<td>355</td>
<td>1</td>
<td>1</td>
<td>86</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability &amp; Utility</td>
<td>1</td>
<td></td>
<td></td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Offline Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality &amp; Possession</td>
<td>23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity &amp; Authenticity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability &amp; Utility</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>People</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidentiality &amp; Possession</td>
<td>30</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity &amp; Authenticity</td>
<td>59</td>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability &amp; Utility</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Figure 10: Threat agents over time by percent of breaches

- 2004-2007: 70% External, 33% Internal, 11% Partner
- 2008: 78% External, 39% Internal, 6% Partner
- 2009: 72% External, 48% Internal, 6% Partner
- 2010: 86% External, 12% Internal, 2% Partner
- 2011: 98% External, 4% Internal, <1% Partner
Figure 15: Motive of external agents by percent of breaches within external

<table>
<thead>
<tr>
<th>Motive of External Agents</th>
<th>All Orgs</th>
<th>Larger Orgs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial or personal gain</td>
<td>71%</td>
<td>96%</td>
</tr>
<tr>
<td>Disagreement or protest</td>
<td>25%</td>
<td></td>
</tr>
<tr>
<td>Fun, curiosity, or pride</td>
<td>23%</td>
<td></td>
</tr>
<tr>
<td>Grudge or personal offense</td>
<td>2%</td>
<td></td>
</tr>
</tbody>
</table>

Table 5: Varieties of external agents by percent of breaches within External and percent of records

<table>
<thead>
<tr>
<th>Type of Agent</th>
<th>All Orgs</th>
<th>Larger Orgs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organized criminal group</td>
<td>83%</td>
<td>35%</td>
</tr>
<tr>
<td>Unknown</td>
<td>10%</td>
<td>31%</td>
</tr>
<tr>
<td>Unaffiliated person(s)</td>
<td>4%</td>
<td>10%</td>
</tr>
<tr>
<td>Activist group</td>
<td>2%</td>
<td>21%</td>
</tr>
<tr>
<td>Former employee (no longer had access)</td>
<td>1%</td>
<td>6%</td>
</tr>
<tr>
<td>Relative or acquaintance of employee</td>
<td>0%</td>
<td>2%</td>
</tr>
</tbody>
</table>
Figure 17. Threat action categories over time by percent of breaches and percent of records

<table>
<thead>
<tr>
<th>Year</th>
<th>Category</th>
<th>2010</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Malware</td>
<td>17%</td>
<td>69%</td>
</tr>
<tr>
<td></td>
<td>Hacking</td>
<td>50%</td>
<td>81%</td>
</tr>
<tr>
<td></td>
<td>Social</td>
<td>11%</td>
<td>7%</td>
</tr>
<tr>
<td></td>
<td>Misuse</td>
<td>0%</td>
<td>5%</td>
</tr>
<tr>
<td></td>
<td>Physical</td>
<td>29%</td>
<td>/&lt;1%</td>
</tr>
<tr>
<td></td>
<td>Error</td>
<td>&lt;1%</td>
<td>1%</td>
</tr>
<tr>
<td></td>
<td>Environmental</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>
## Table 7. Top 10 Threat Action Types by number of breaches and records

<table>
<thead>
<tr>
<th>Rank</th>
<th>Variety</th>
<th>Category</th>
<th>Breaches</th>
<th>Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Keylogger/Form-grabber/Spyware (capture data from user activity)</td>
<td>Malware</td>
<td>48%</td>
<td>35%</td>
</tr>
<tr>
<td>2</td>
<td>Exploitation of default or guessable credentials</td>
<td>Hacking</td>
<td>44%</td>
<td>1%</td>
</tr>
<tr>
<td>3</td>
<td>Use of stolen login credentials</td>
<td>Hacking</td>
<td>32%</td>
<td>82%</td>
</tr>
<tr>
<td>4</td>
<td>Send data to external site/entity</td>
<td>Malware</td>
<td>30%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>5</td>
<td>Brute force and dictionary attacks</td>
<td>Hacking</td>
<td>23%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>6</td>
<td>Backdoor (allows remote access/control)</td>
<td>Malware</td>
<td>20%</td>
<td>49%</td>
</tr>
<tr>
<td>7</td>
<td>Exploitation of backdoor or command and control channel</td>
<td>Hacking</td>
<td>20%</td>
<td>49%</td>
</tr>
<tr>
<td>8</td>
<td>Disable or interfere with security controls</td>
<td>Malware</td>
<td>18%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>9</td>
<td>Tampering</td>
<td>Physical</td>
<td>10%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>10</td>
<td>Exploitation of insufficient authentication (e.g., no login required)</td>
<td>Hacking</td>
<td>5%</td>
<td>&lt;1%</td>
</tr>
</tbody>
</table>
## Top Threat Actions: Larger Orgs

### Table 8. Top 10 Threat Action Types by number of breaches and records - LARGER ORGS

<table>
<thead>
<tr>
<th>Rank</th>
<th>Overall Rank</th>
<th>Variety</th>
<th>Category</th>
<th>Breaches</th>
<th>Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>Use of stolen login credentials</td>
<td>Hacking</td>
<td>30%</td>
<td>84%</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>Backdoor <em>(allows remote access/control)</em></td>
<td>Malware</td>
<td>18%</td>
<td>51%</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>Exploitation of backdoor or command and control channel</td>
<td>Hacking</td>
<td>17%</td>
<td>51%</td>
</tr>
<tr>
<td>4</td>
<td>9</td>
<td>Tampering</td>
<td>Physical</td>
<td>17%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>Keylogger/Form-grabber/Spyware <em>(capture data from user activity)</em></td>
<td>Malware</td>
<td>13%</td>
<td>36%</td>
</tr>
<tr>
<td>6</td>
<td>11</td>
<td>Pretexting <em>(classic Social Engineering)</em></td>
<td>Social</td>
<td>12%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>Brute force and dictionary attacks</td>
<td>Hacking</td>
<td>8%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>8</td>
<td>15</td>
<td>SQL Injection</td>
<td>Hacking</td>
<td>8%</td>
<td>1%</td>
</tr>
<tr>
<td>9</td>
<td>20</td>
<td>Phishing *(or any type of &quot;fishing&quot;)</td>
<td>Social</td>
<td>8%</td>
<td>38%</td>
</tr>
<tr>
<td>10</td>
<td>22</td>
<td>Command and Control <em>(listens for and executes commands)</em></td>
<td>Malware</td>
<td>8%</td>
<td>36%</td>
</tr>
</tbody>
</table>
Figure 26. Categories of compromised assets by percent of breaches and percent of records

- Servers: 64% / 94%
- User Devices: 60% / 35%
- People: 7% / 34%
- Offline data: 3% / <1%
- Network infrastructure: <1% / <1%
- Unknown: 1% / 1%

Figure 27. Categories of compromised assets by percent of breaches and percent of records – LARGER ORGS

- Servers: 68% / 97%
- User Devices: 32% / 36%
- People: 20% / 36%
- Offline data: 3% / <1%
- Network infrastructure: 2% / 0%
- Unknown: 5% / <1%
Figure 33. Role of organization size in type of record compromise

- Trade secrets
- Sensitive organizational data
- System information
- Personal information
- Bank account numbers/data
- Classified information
- Medical records
- Copyrighted/Trademarked material
- Authentication credentials
- Payment card numbers/data

Percent of incidents

- All Orgs
- Larger Orgs
## Timespan of events

### Figure 40. Timespan of events by percent of breaches

<table>
<thead>
<tr>
<th></th>
<th>Seconds</th>
<th>Minutes</th>
<th>Hours</th>
<th>Days</th>
<th>Weeks</th>
<th>Months</th>
<th>Years</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initial Attack to Initial Compromise</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10%</td>
<td></td>
<td>75%</td>
<td>12%</td>
<td>2%</td>
<td>0%</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td><strong>Initial Compromise to Data Exfiltration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8%</td>
<td></td>
<td>38%</td>
<td>14%</td>
<td>25%</td>
<td>8%</td>
<td>8%</td>
<td>0%</td>
</tr>
<tr>
<td><strong>Initial Compromise to Discovery</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0%</td>
<td></td>
<td>0%</td>
<td>2%</td>
<td>13%</td>
<td>29%</td>
<td>54%+</td>
<td>2%</td>
</tr>
<tr>
<td><strong>Discovery to Containment/Restoration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0%</td>
<td></td>
<td>1%</td>
<td>9%</td>
<td>32%</td>
<td>38%</td>
<td>17%</td>
<td>4%</td>
</tr>
</tbody>
</table>
Figure 44. Simplified breach discovery methods by percent of breaches

ALL ORGS
- 92% External party
- 2% Internal active
- 4% Internal passive
- 2% Unknown

LARGER ORGS
- 49% External party
- 16% Internal active
- 28% Internal passive
- 7% Unknown

Graph showing the trend from 2008 to 2011:
- Pre-2008: 75%
- 2008: 69%
- 2009: 61%
- 2010: 86%
- 2011: 92%
Figure 45. Breach discovery methods by percent of breaches

<table>
<thead>
<tr>
<th>Method</th>
<th>All Orgs</th>
<th>Larger Orgs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notified by law enforcement</td>
<td>10%</td>
<td>59%+</td>
</tr>
<tr>
<td>Third-party fraud detection (e.g., CPP)</td>
<td>8%</td>
<td>26%−</td>
</tr>
<tr>
<td>Reported by customer/partner affected by the incident</td>
<td>4%</td>
<td>5%</td>
</tr>
<tr>
<td>Brag or blackmail by perpetrator</td>
<td>3%</td>
<td>21%</td>
</tr>
<tr>
<td>Witnessed and/or reported by employee</td>
<td>2%</td>
<td>16%</td>
</tr>
<tr>
<td>Unusual system behavior or performance</td>
<td>1%</td>
<td>7%</td>
</tr>
<tr>
<td>Log analysis and/or review process</td>
<td>1%</td>
<td>8%</td>
</tr>
<tr>
<td>Financial audit and reconciliation process</td>
<td>1%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Internal fraud detection mechanism</td>
<td>1%</td>
<td>5%</td>
</tr>
<tr>
<td>Other(s)</td>
<td>2%</td>
<td>13%</td>
</tr>
<tr>
<td>Unknown</td>
<td>2%</td>
<td>7%</td>
</tr>
</tbody>
</table>
Collective Intelligence Framework

Artifacts or Indicators (IOCs)

- VERIS metrics
- Inference signatures
- Watchlist IP addresses
- Malcode hash patterns
- Text strings
- Breach notifications
- Attribution tables

Collective Intelligence Framework (CIF)

- RISK Team
  - Investigations, Research
- Verizon
  - Backbone, VzW, Terremark, Vz Federal, Internal security
- Trusted Sources
  - DHS, Intelligence and Law Enforcement Communities
- Other 3rd parties
  - VERIS Community, ISACs, OSINT