NAAG Winter Meeting
Presidential Initiative Session

Andy Bonillo
Director – Cyber Security & Public Safety
February 24, 2015
2014 Data Breach Investigations Report

50 CONTRIBUTING GLOBAL ORGANIZATIONS

1,367 CONFIRMED SECURITY BREACHES

63,437 SECURITY INCIDENTS

95 COUNTRIES REPRESENTED
Data Breach Landscape

**OPPORTUNISTIC**

- Activists
- Hackers
- Organized Crime
- State-Affiliated

**TARGETED**

- Retail
- Financial Services
  - Online Media
  - Retail
  - Financial Services
  - Media
  - Shipment & Logistics
  - Technology
  - Entertainment
  - Unknown
  - Public Sector
  - Telecom
  - Utility
  - Media

*Number of records stolen as a result of each breach

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.
Breach Discovery

Breach discovery methods over time

- Fraud Detection
- Internal
- Law Enforcement
- Third Party
14 Victims
180 Million Cards Stolen
90 Billion Potential Loss
13 Indictments
+ 100 TB of Digital Evidence

A Cybercrime Scene
2014 Data Breach Investigations Report

Nine classification patterns covered the majority of security incidents.

In 2013, we analyzed over 63,000 security incidents and more than 1,300 confirmed breaches to provide new insight into your biggest threats and to help improve your defenses against them. This year's report identifies nine basic patterns that covered 92% of all the 100,000 security incidents we've looked at from the past 10 years.

- **Energy/Utilities**: Just two patterns—web app attacks and crimeware—covered 69% of all incidents.
- **Public Sector**: The most frequent incidents were errors (34%), insider misuse (24%), crimeware (21%) and lost/stolen assets (19%).
- **Healthcare**: Physical theft and loss of assets occurred most often in the office—not from personal vehicles or homes.
- **Travel/Hospitality**: Three-quarters of the attacks targeted POS devices and systems—a good argument for PCI compliance.

92% of all security incidents we analyzed over a ten-year period fit into nine basic patterns.
Top 3 Patterns Cover 72% of Incidents

ON AVERAGE 72% OF THE INCIDENTS IN AN INDUSTRY CAN BE DESCRIBED BY JUST THREE OF THE NINE PATTERNS.

In most industries, more than 50% of incidents are covered by just three of the nine patterns.
# Data Breach by Industry

<table>
<thead>
<tr>
<th>INDUSTRY</th>
<th>POS</th>
<th>WEB APP</th>
<th>INSIDER/PRIVLGE. MISUSE</th>
<th>LOST/STOLEN</th>
<th>MISC. ERROR</th>
<th>CRIMEWARE</th>
<th>PAYMENT CARD SKIMMER</th>
<th>DENIAL OF SERVICE</th>
<th>CYBER ESPIONAGE</th>
<th>EVERYTHING ELSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accommodation</td>
<td>85%</td>
<td>1%</td>
<td>8%</td>
<td>&lt;1%</td>
<td>1%</td>
<td>1%</td>
<td>&lt;1%</td>
<td>0%</td>
<td>0%</td>
<td>4%</td>
</tr>
<tr>
<td>Administrative</td>
<td>0%</td>
<td>8%</td>
<td>29%</td>
<td>8%</td>
<td>47%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
<td>6%</td>
</tr>
<tr>
<td>Construction</td>
<td>1%</td>
<td>20%</td>
<td>10%</td>
<td>7%</td>
<td>29%</td>
<td>3%</td>
<td>1%</td>
<td>0%</td>
<td>2%</td>
<td>27%</td>
</tr>
<tr>
<td>Education</td>
<td>14%</td>
<td>38%</td>
<td>10%</td>
<td>0%</td>
<td>24%</td>
<td>0%</td>
<td>5%</td>
<td>5%</td>
<td>0%</td>
<td>5%</td>
</tr>
<tr>
<td>Entertainment</td>
<td>&lt;1%</td>
<td>42%</td>
<td>8%</td>
<td>1%</td>
<td>6%</td>
<td>2%</td>
<td>34%</td>
<td>0%</td>
<td>&lt;1%</td>
<td>6%</td>
</tr>
<tr>
<td>Finance</td>
<td>22%</td>
<td>3%</td>
<td>32%</td>
<td>12%</td>
<td>18%</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>0%</td>
<td>1%</td>
<td>12%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>1%</td>
<td>46%</td>
<td>8%</td>
<td>3%</td>
<td>4%</td>
<td>4%</td>
<td>&lt;1%</td>
<td>&lt;1%</td>
<td>8%</td>
<td>25%</td>
</tr>
<tr>
<td>Information</td>
<td>0%</td>
<td>23%</td>
<td>13%</td>
<td>2%</td>
<td>4%</td>
<td>1%</td>
<td>0%</td>
<td>0%</td>
<td>43%</td>
<td>14%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>0%</td>
<td>33%</td>
<td>0%</td>
<td>0%</td>
<td>7%</td>
<td>0%</td>
<td>7%</td>
<td>0%</td>
<td>0%</td>
<td>53%</td>
</tr>
<tr>
<td>Mining</td>
<td>0%</td>
<td>16%</td>
<td>12%</td>
<td>2%</td>
<td>6%</td>
<td>3%</td>
<td>0%</td>
<td>0%</td>
<td>48%</td>
<td>12%</td>
</tr>
<tr>
<td>Professional</td>
<td>1%</td>
<td>3%</td>
<td>3%</td>
<td>1%</td>
<td>1%</td>
<td>3%</td>
<td>10%</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
</tr>
<tr>
<td>Public</td>
<td>0%</td>
<td>3%</td>
<td>3%</td>
<td>1%</td>
<td>1%</td>
<td>3%</td>
<td>10%</td>
<td>0%</td>
<td>0%</td>
<td>7%</td>
</tr>
<tr>
<td>Real Estate</td>
<td>0%</td>
<td>4%</td>
<td>6%</td>
<td>1%</td>
<td>1%</td>
<td>3%</td>
<td>10%</td>
<td>0%</td>
<td>0%</td>
<td>7%</td>
</tr>
<tr>
<td>Retail</td>
<td>8%</td>
<td>31%</td>
<td>8%</td>
<td>4%</td>
<td>12%</td>
<td>8%</td>
<td>4%</td>
<td>0%</td>
<td>0%</td>
<td>27%</td>
</tr>
<tr>
<td>Trade</td>
<td>0%</td>
<td>11%</td>
<td>23%</td>
<td>8%</td>
<td>5%</td>
<td>2%</td>
<td>6%</td>
<td>0%</td>
<td>39%</td>
<td>6%</td>
</tr>
<tr>
<td>Transportation</td>
<td>0%</td>
<td>72%</td>
<td>4%</td>
<td>1%</td>
<td>1%</td>
<td>3%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>12%</td>
</tr>
<tr>
<td>Utilities</td>
<td>2%</td>
<td>28%</td>
<td>22%</td>
<td>0%</td>
<td>17%</td>
<td>3%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>7%</td>
</tr>
</tbody>
</table>

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.
The Detection Gap Continues to Grow

Percent of breaches where time to compromise (red) and time to discovery (blue) was days or less

* Source: Verizon 2014 Data Breach Investigations Report

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.
Resources

- Download: www.verizonenterprise.com/dbir
- VERIS: www.veriscommunity.net
- Email: DBIR@verizon.com
- Twitter: @vzdbir and hashtag #dbir