

# 2010 Data Breach Investigations Report



© 2010 Verizon. All Rights Reserved. PTE14626 07/10

## Methodology

### Data Source

- Verizon Business Investigative Response Team
- **NEW:** United States Secret Service (USSS)

### Collection and Analysis

- VERIS framework used to collect data after investigation
  - USSS used internal application based on VERIS
- Case data anonymized and aggregated
- RISK Intelligence team provides analytics

### Data Sample

- Six years of forensic investigations (not internal Verizon incidents)
- >900 breaches, 900 million stolen records in combined dataset
  - Actual compromise rather than data-at-risk
  - Both disclosed and non-disclosed
  - Many of the largest breaches ever reported



## VERIS Framework

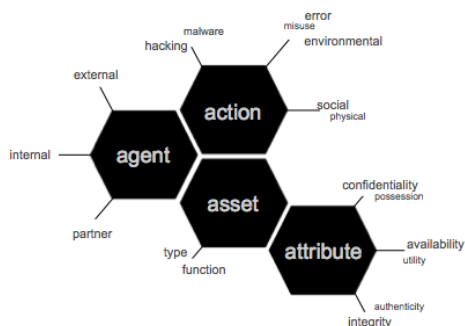
VERIS is a set of metrics designed to provide a **common language for describing security incidents** (or threats) in a structured and repeatable manner.

The overall goal is to create a foundation for data-driven **decision-making and risk management**.



## VERIS Framework

The Incident Classification section employs Verizon's **A<sup>4</sup> threat model**



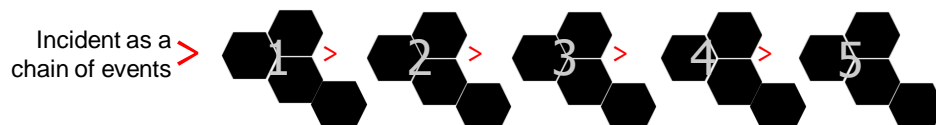
A security incident (or threat scenario) is modeled as a series of **events**. Every event is comprised of the following 4 A's:

**Agent:** Whose actions affected the asset

**Action:** What actions affected the asset

**Asset:** Which assets were affected

**Attribute:** How the asset was affected



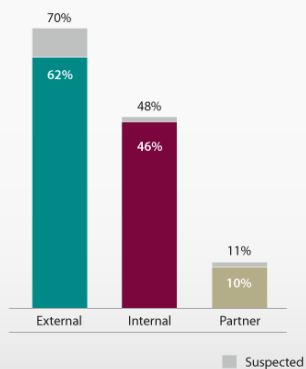


## 2010 Data Breach Investigations Report

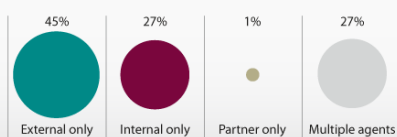
# RESULTS & ANALYSIS

### Threat Agents

Threat agents (inclusive) by percent of breaches



Threat agents (exclusive) by percent of breaches



Compromised records by threat agent, 2004-2009

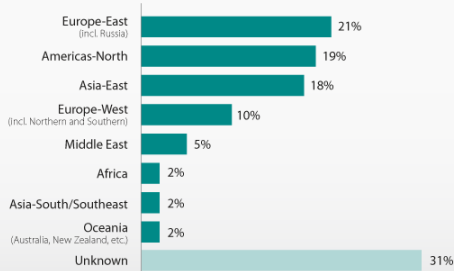


## External Agents

Table 1. Types of external agents by percent of breaches within External

Organized criminal group	24%
Unaffiliated person(s)	21%
External system(s) or site	3%
Activist group	2%
Former employee (no longer had access)	2%
Another organization (not partner or competitor)	1%
Competitor	1%
Customer (B2C)	1%
Unknown	45%

Origin of external agents by percent of breaches within External



9



## Internal Agents

Role of internal agents by percent of breaches within Internal



Types of internal agents by percent of breaches within Internal

Regular employee/end-user	51%
Finance/accounting staff	12%
System/network administrator	12%
Executive/upper management	7%
Helpdesk staff	4%
Software developer	3%
Auditor	1%
Unknown	9%

10



## Partner Agents

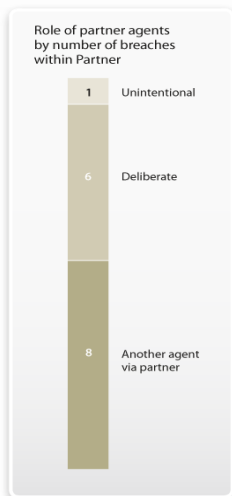


Table 3. Types of partner agents by percent of breaches within Partner

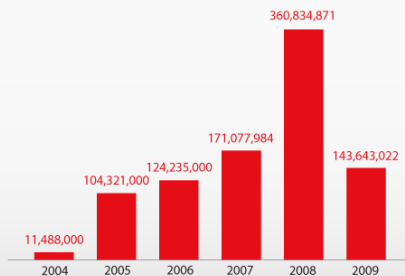
Remote IT management/support	7
Data processing and analysis	1
Hosting provider	1
Onsite IT management/support	1
Security services/consulting	1
Shipping/logistics provider	1
Unknown	3



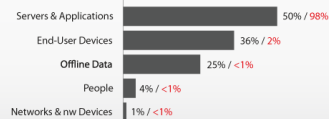
11

## Assets & Data

Number of records compromised per year in breaches investigated by Verizon and the United States Secret Service



Categories of compromised assets by percent of breaches and percent of records



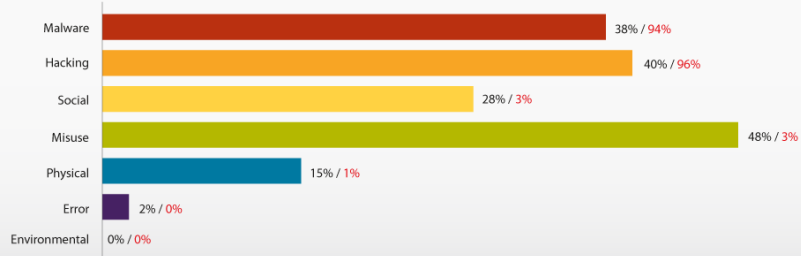
Compromised data types by percent of breaches and percent of records



12

## Threat Actions

Threat action categories by percent of breaches and records

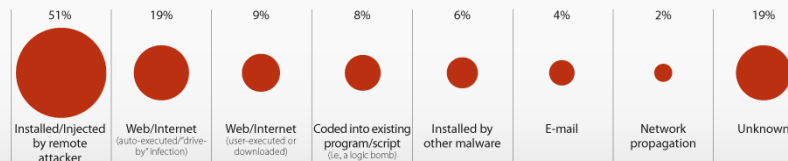


13



## Malware Infection Vector

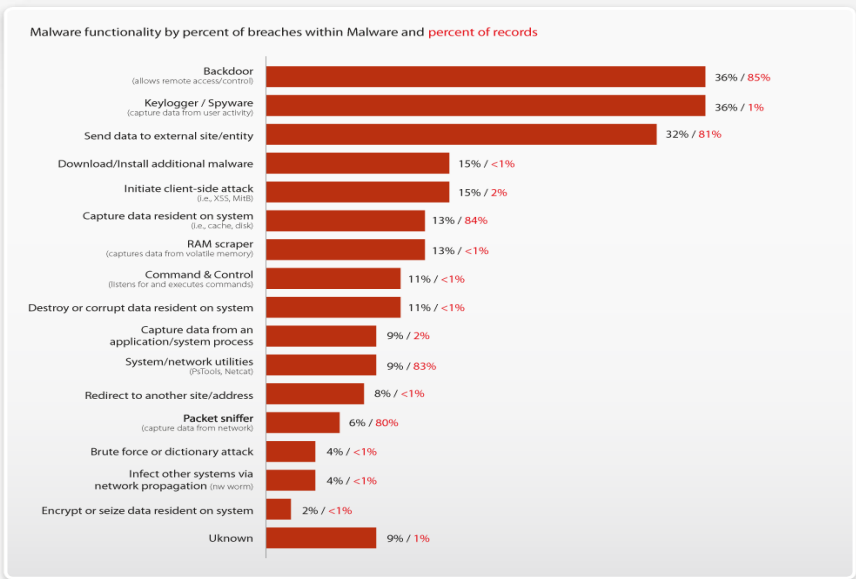
Malware infection vectors by percent of breaches within Malware



16

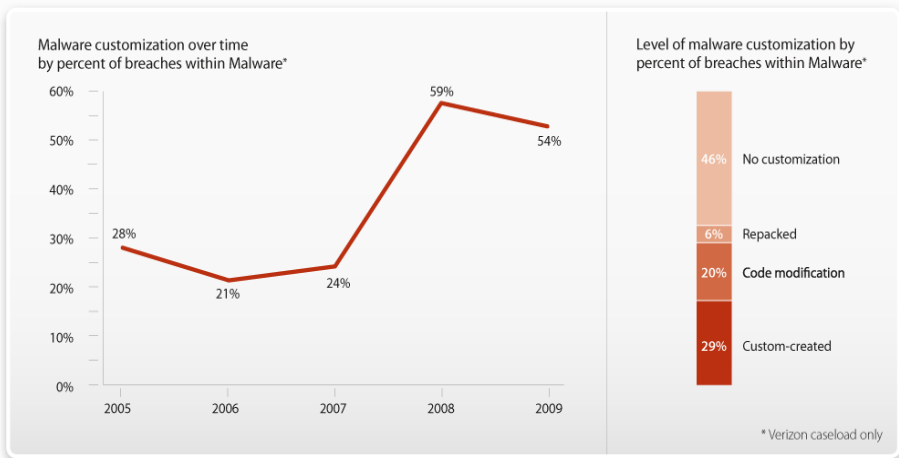


## Malware Functionality



17

## Malware Customization

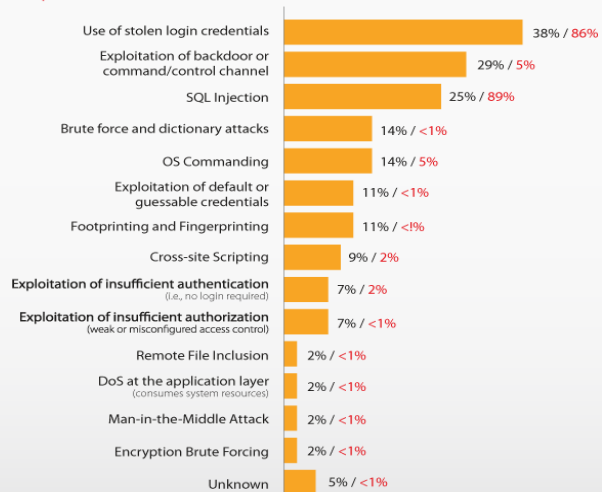


18



## Hacking Types

Types of hacking by percent of breaches within Hacking and percent of records

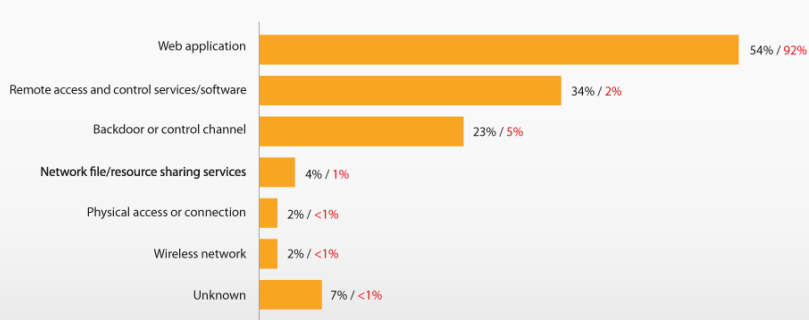


19



## Hacking Paths

Attack pathways by percent of breaches within Hacking and percent of records

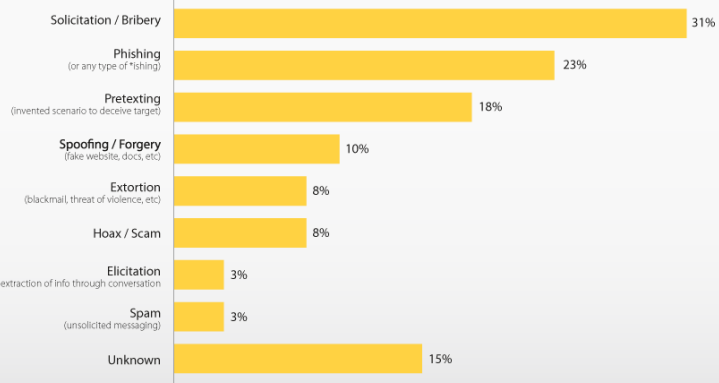


20 Patchable vulnerabilities: 0



## Social Types

Types of social tactics by percent of breaches within Social

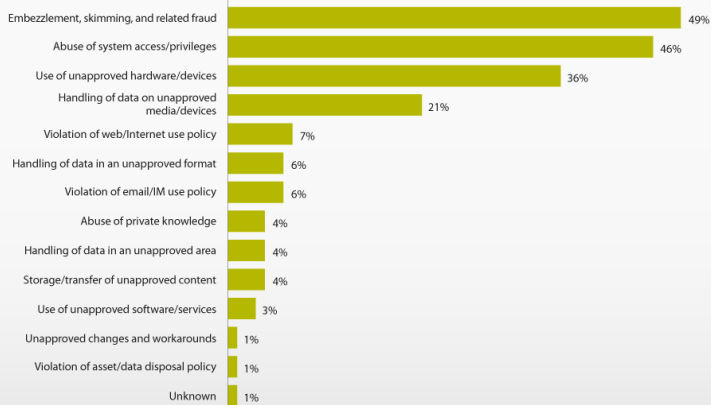


21



## Misuse Types

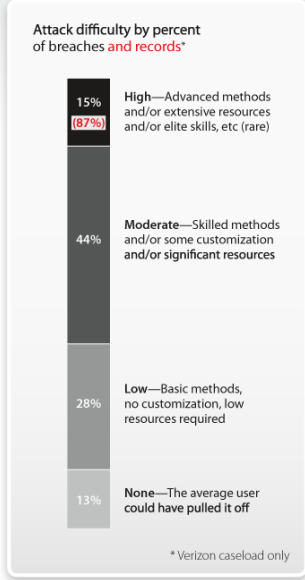
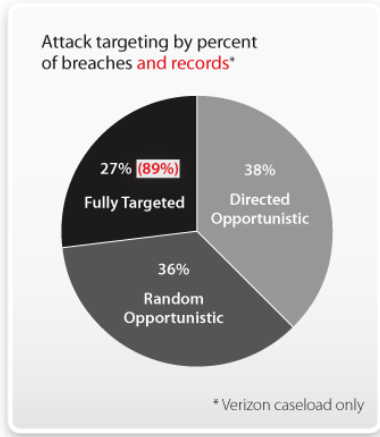
Types of misuse by percent of breaches within Misuse



22

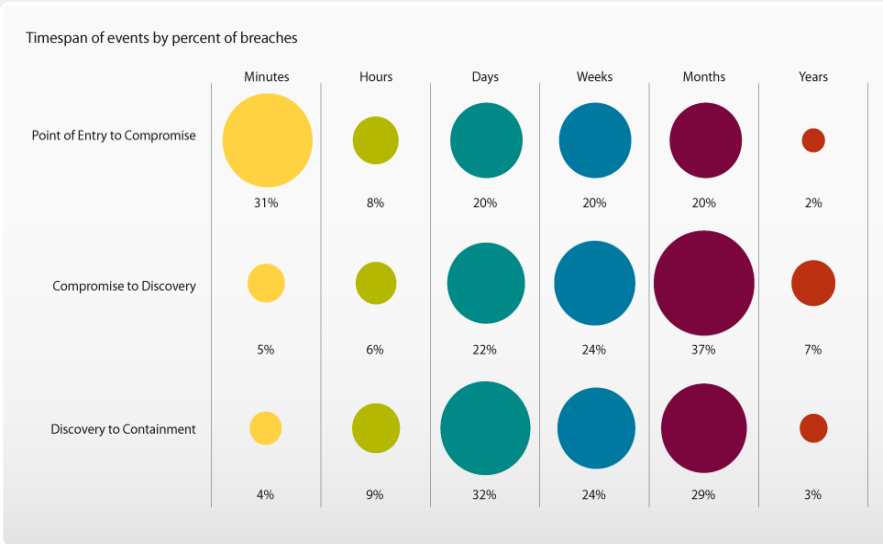


## Attack Difficulty & Targeting



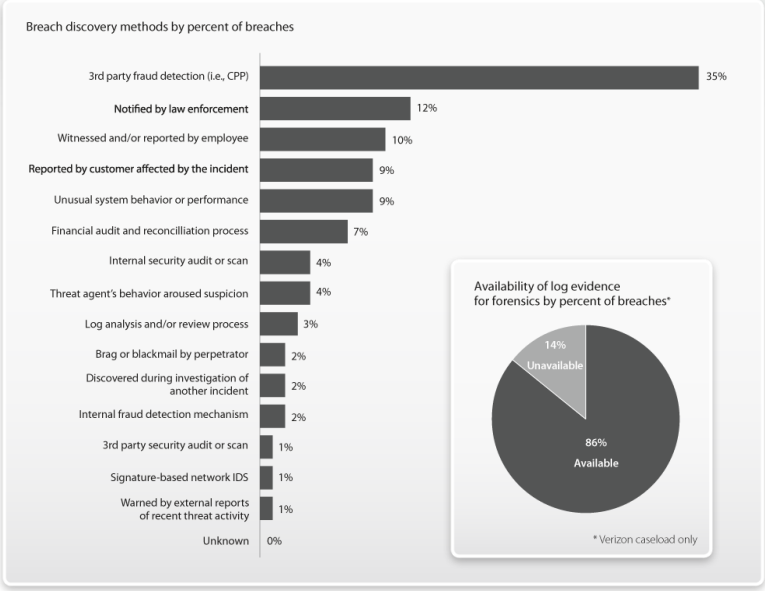
23

## Time Span of Events



24

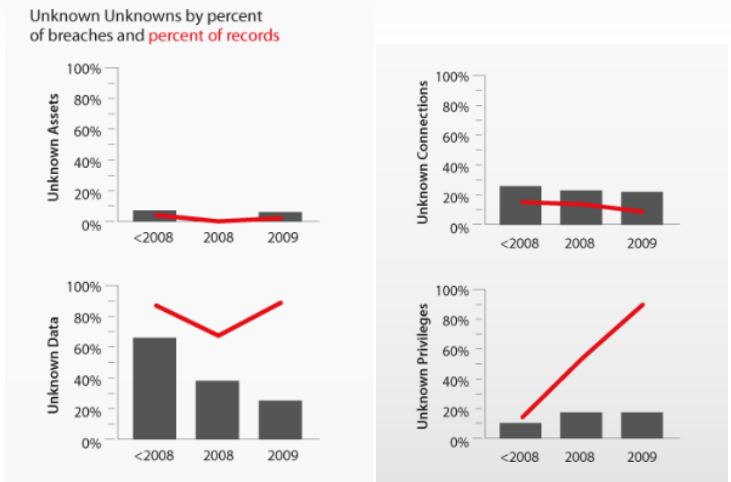
## Discovery Methods



25



## Unknown Unknowns



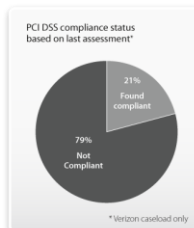
26



## PCI DSS

Percent of relevant organizations in compliance with PCI DSS requirements based on post-breach reviews conducted by Verizon IR team\*

	2008	2009
<b>Build and Maintain a Secure Network</b>		
Requirement 1: Install and maintain a firewall configuration to protect data	30%	35%
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	49%	30%
<b>Protect Cardholder Data</b>		
Requirement 3: Protect Stored Data	11%	30%
Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks	68%	90%
<b>Maintain a Vulnerability Management Program</b>		
Requirement 5: Use and regularly update anti-virus software	62%	53%
Requirement 6: Develop and maintain secure systems and applications	5%	21%
<b>Implement Strong Access Control Measures</b>		
Requirement 7: Restrict access to data by business need-to-know	24%	30%
Requirement 8: Assign a unique ID to each person with computer access	19%	35%
Requirement 9: Restrict physical access to cardholder data	43%	58%
<b>Regularly Monitor and Test Networks</b>		
Requirement 10: Track and monitor all access to network resources and cardholder data	5%	30%
Requirement 11: Regularly test security systems and processes	14%	25%
<b>Maintain an Information Security Policy</b>		
Requirement 12: Maintain a policy that addresses information security	14%	40%



\* Verizon caseload only



27

## Conclusion & Recommendations

### Overall

- USSS cases afforded more complete picture of breaches
  - Further confirmation on what we already observed
  - New insight from pieces of the picture we were missing

### Agents

- External small majority of breaches, dominates overall data loss
  - Largely due to organized crime
- Internal up because of USSS cases
- Partner down again in both datasets

### Actions

- Two most-common scenarios
  - Exploit error, gain access to network/systems, install malware (External)
  - Exploit privilege, abuse access and/or embezzle funds/data (Internal)
  - Still not highly difficult or targeted though slightly more than before



28

## Conclusion & Recommendations

### Assets

- Most data compromised from servers & apps
- Desktops/laptops increasing; related to stolen credentials
- Most criminals interested in cashable forms of data

### Discovery & Response

- Discovery still takes a long time and is largely due to third parties
- Response and containment slow and prone to mishap

### Mitigation

- The basics – if done consistently – are sufficient in most cases
- Keep outsiders out; they are increasingly difficult to control once in
- Restrict and monitor insiders; disable access when they leave
- Maintain adequate resources for detection; make better use of logs
- Plan, prepare, train, and test for a timely and effective response

29



DBIR: [www.verizonbusiness.com/databreach](http://www.verizonbusiness.com/databreach)  
 VERIS: <https://verisframework.wiki.zoho.com/>  
 Blog: [securityblog.verizonbusiness.com](http://securityblog.verizonbusiness.com)  
 Email: [dbir@verizonbusiness.com](mailto:dbir@verizonbusiness.com)

