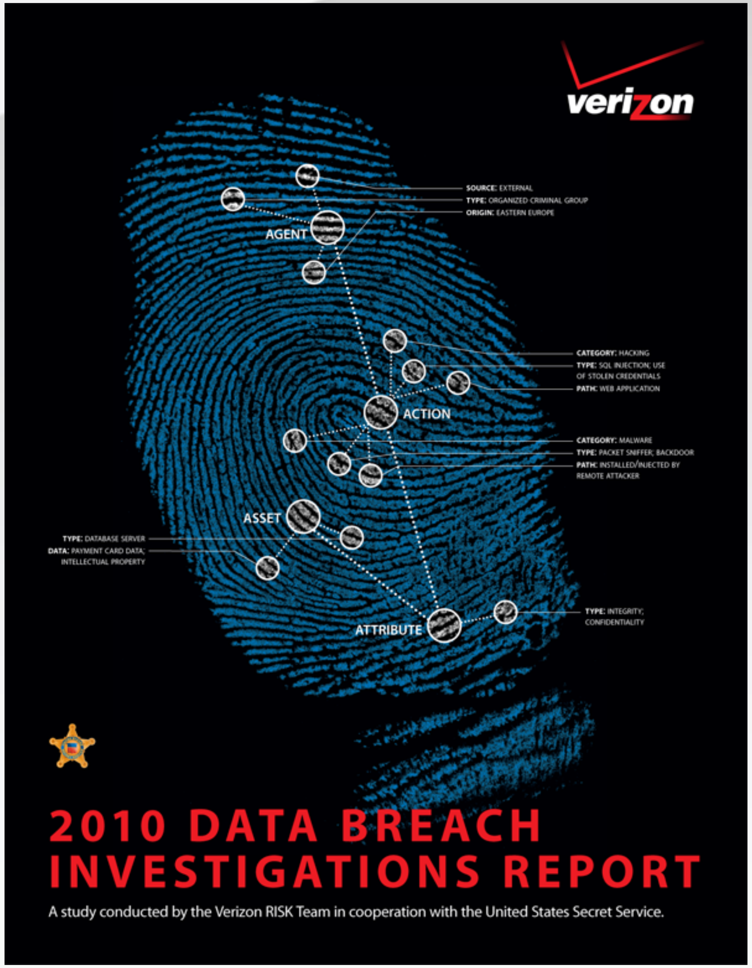
2010 Data Breach Investigations Report



verizon

AGENT
SOURCE: EXTERNAL
TYPE: ORGANIZED CRIMINAL GROUP
ORIGIN: EASTERN EUROPE
ACTION
CATEGORY: HACKING
TYPE: SQL INJECTION; USE OF STOLEN CREDENTIALS
PATH: WEB APPLICATION
CATEGORY: MALWARE
TYPE: PACKET SNIFFER; BACKDOOR
PATH: INSTALLED/INJECTED BY REMOTE ATTACKER
ASSET
TYPE: DATABASE SERVER
DATA: PAYMENT CARD DATA; INTELLECTUAL PROPERTY
ATTRIBUTE
TYPE: INTEGRITY; CONFIDENTIALITY

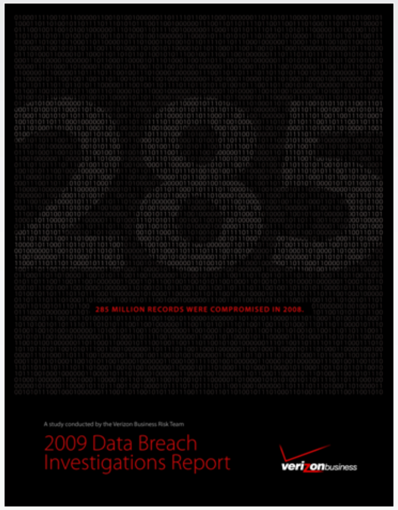
2010 DATA BREACH INVESTIGATIONS REPORT

A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service.

A *Study* CONDUCTED BY THE VERIZON BUSINESS RISK TEAM

2008 DATA BREACH INVESTIGATIONS REPORT

Four Years of Forensic Research. More than 500 Cases.
One Comprehensive Report



285 MILLION RECORDS WERE COMPROMISED IN 2008.

A study conducted by the Verizon Business Risk Team

2009 Data Breach Investigations Report

verizon business

Matthijs van de Wel
Managing Principal Forensics EMEA

PROPRIETARY STATEMENT

This document and any attached materials are the sole property of Verizon and are not to be used by you other than to evaluate Verizon's service.

This document and any attached materials are not to be disseminated, distributed, or otherwise conveyed throughout your organization to employees without a need for this information or to any third parties without the express written permission of Verizon.

A call for breach research

“…we will create a National Digital Security Board modeled on the National Transportation Safety Board. The NDSB will have the authority to **investigate information security breaches** reported by victim organizations. The NDSB will publish reports on its findings for the benefit of the public and other organizations, thereby **increasing transparency** in two respects. First, intrusions will have real costs beyond those directly associated with the incident, by bringing potentially poor security practices and software to the attention of the public. Second, other organizations will **learn how to avoid the mistakes** made by those who fall victim to intruders.”

--

Remarks by the president on securing our nation’s cyber infrastructure
May 29, 2009

http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

verizon

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

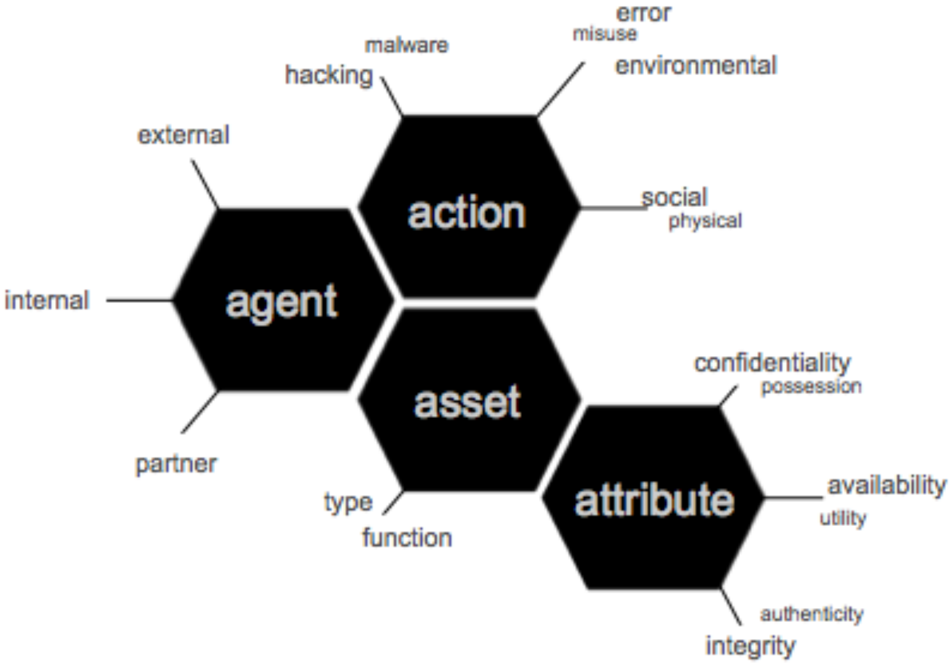
VERIS Framework

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^4 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:

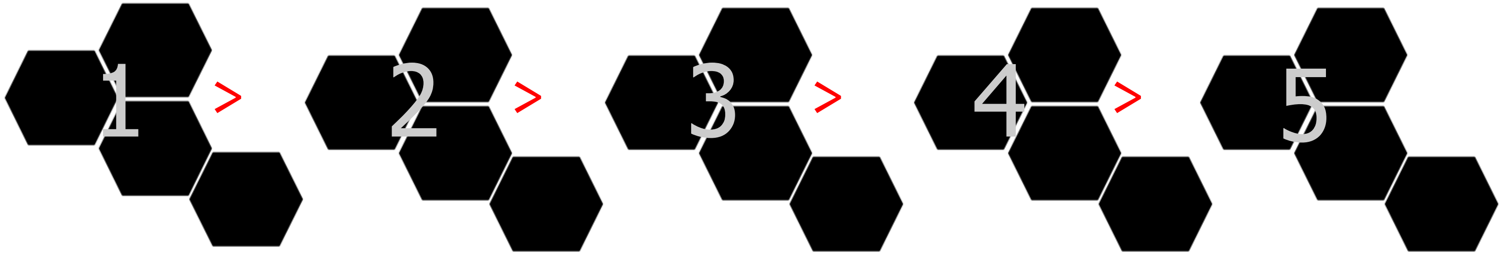
Agent: Whose actions affected the asset

Action: What actions affected the asset

Asset: Which assets were affected

Attribute: How the asset was affected

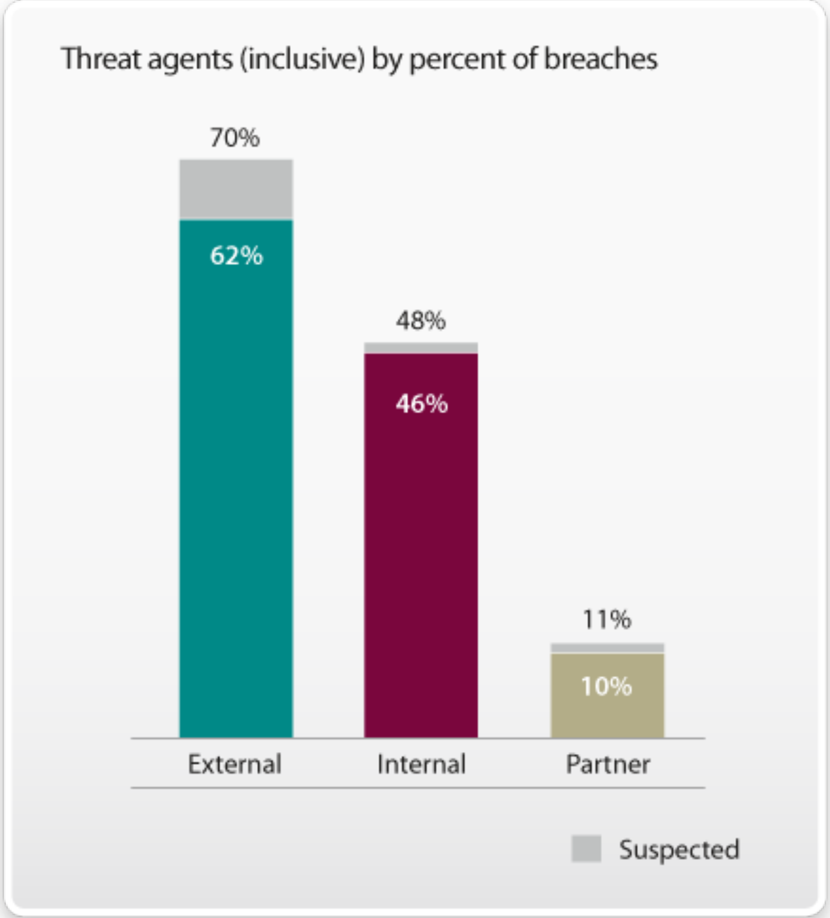
Incident as a chain of events >

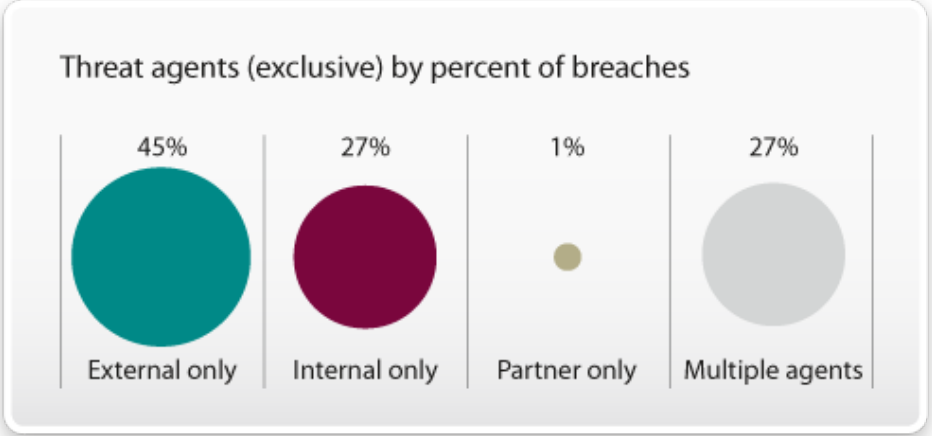


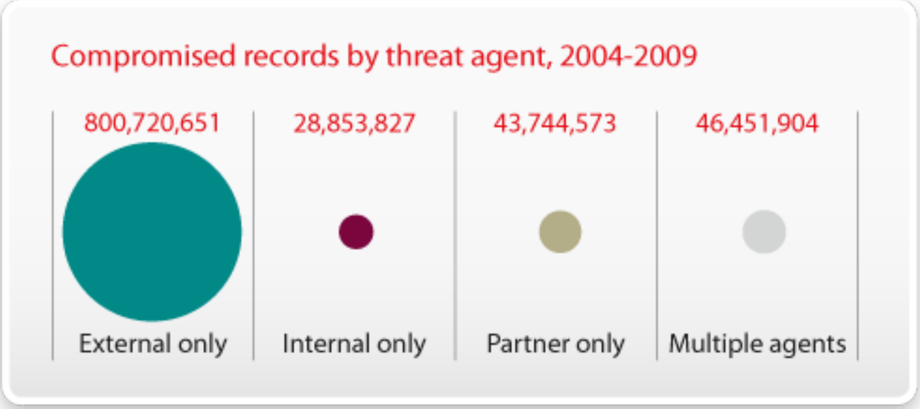
2010 Data Breach Investigations Report

RESULTS & ANALYSIS

Threat Agents

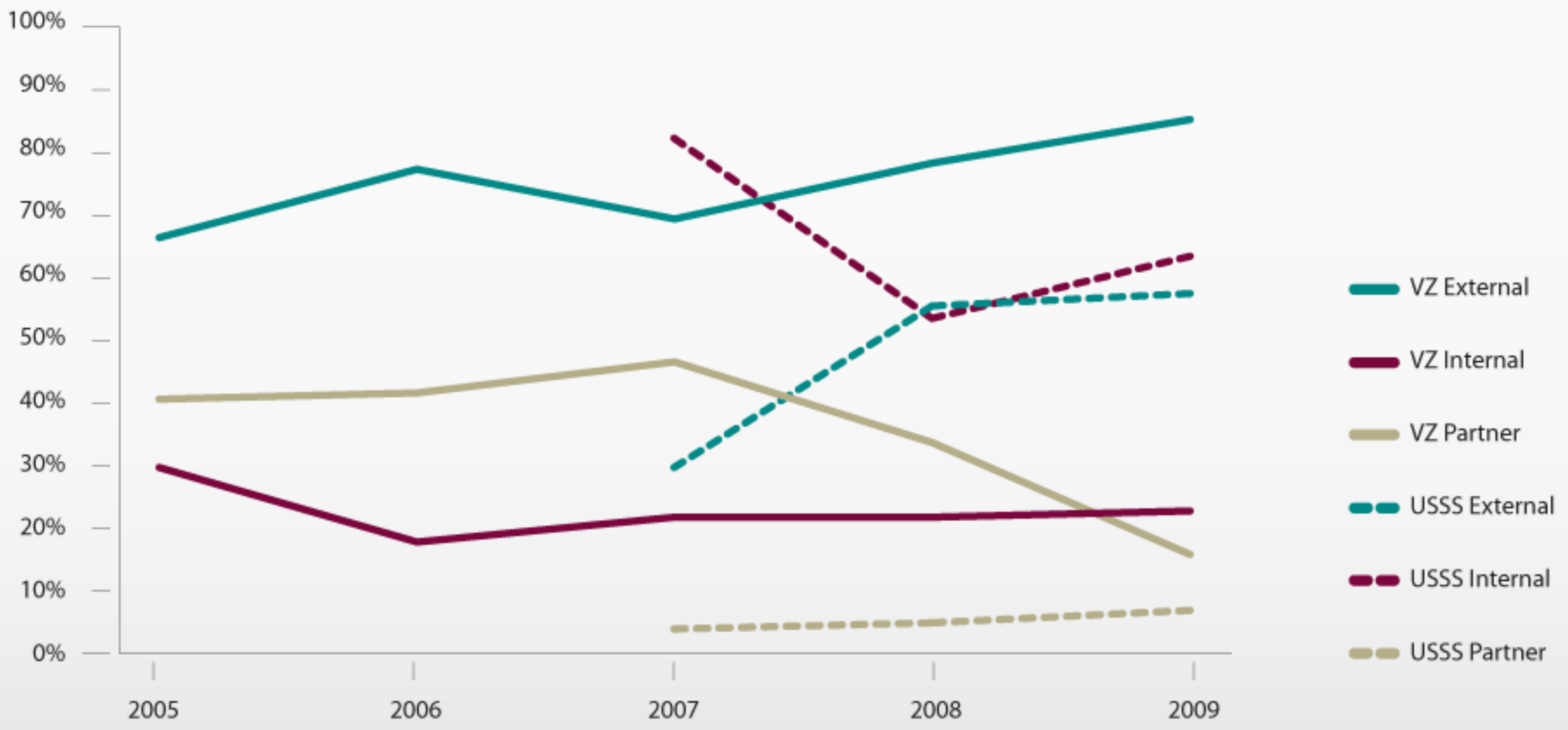






Threat Agents

Threat agents over time by percent of breaches

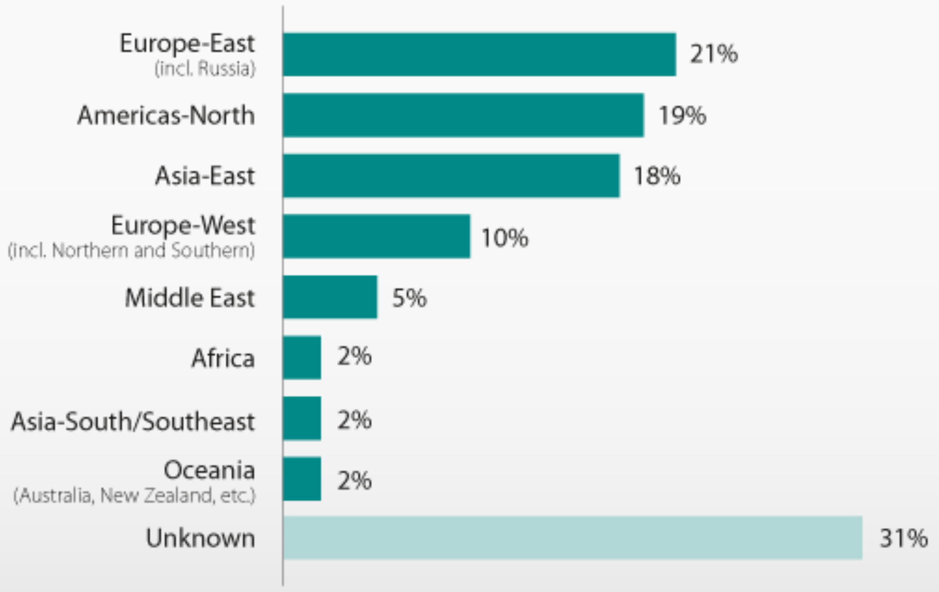


External Agents

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

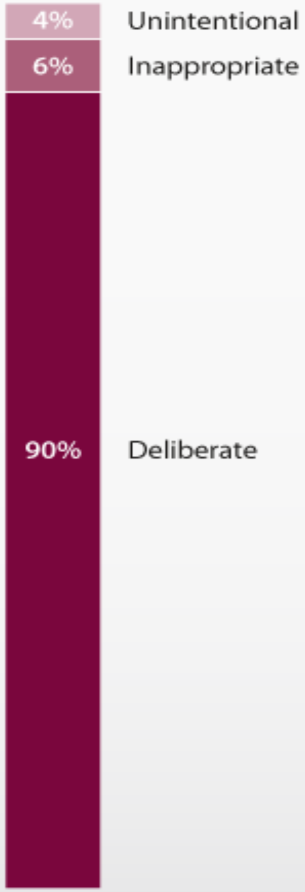
Organized criminal group	24%
Unaffiliated person(s)	21%
External system(s) or site	3%
Activist group	2%
Former employee (no longer had access)	2%
Another organization (not partner or competitor)	1%
Competitor	1%
Customer (B2C)	1%
Unknown	45%

Origin of external agents by percent of breaches within External



Internal Agents

Role of internal agents by percent of breaches within Internal

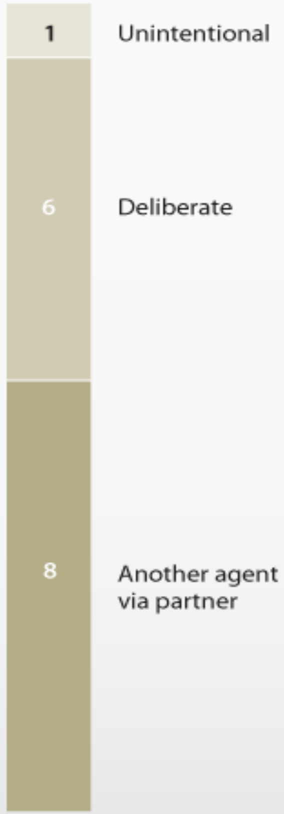


Types of internal agents by percent of breaches within Internal

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%

Partner Agents

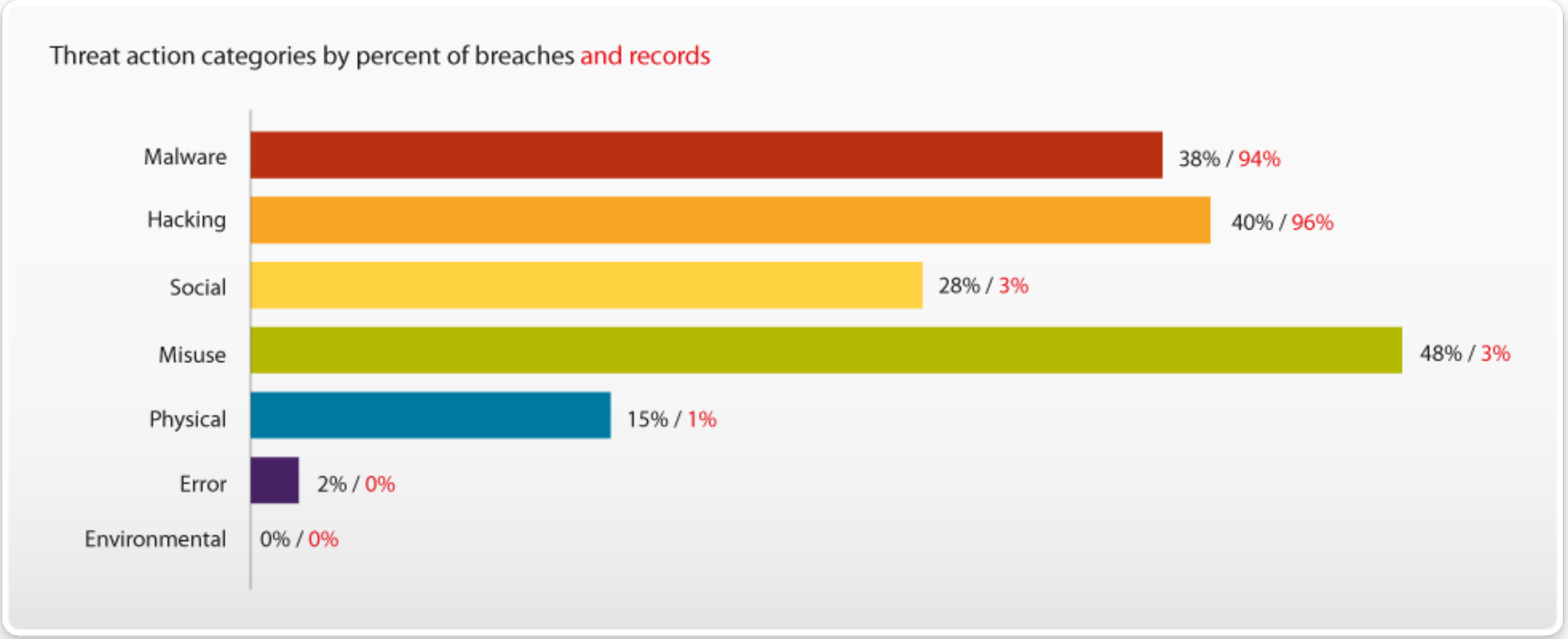
Role of partner agents by number of breaches within Partner



Types of internal agents by percent of breaches within Internal

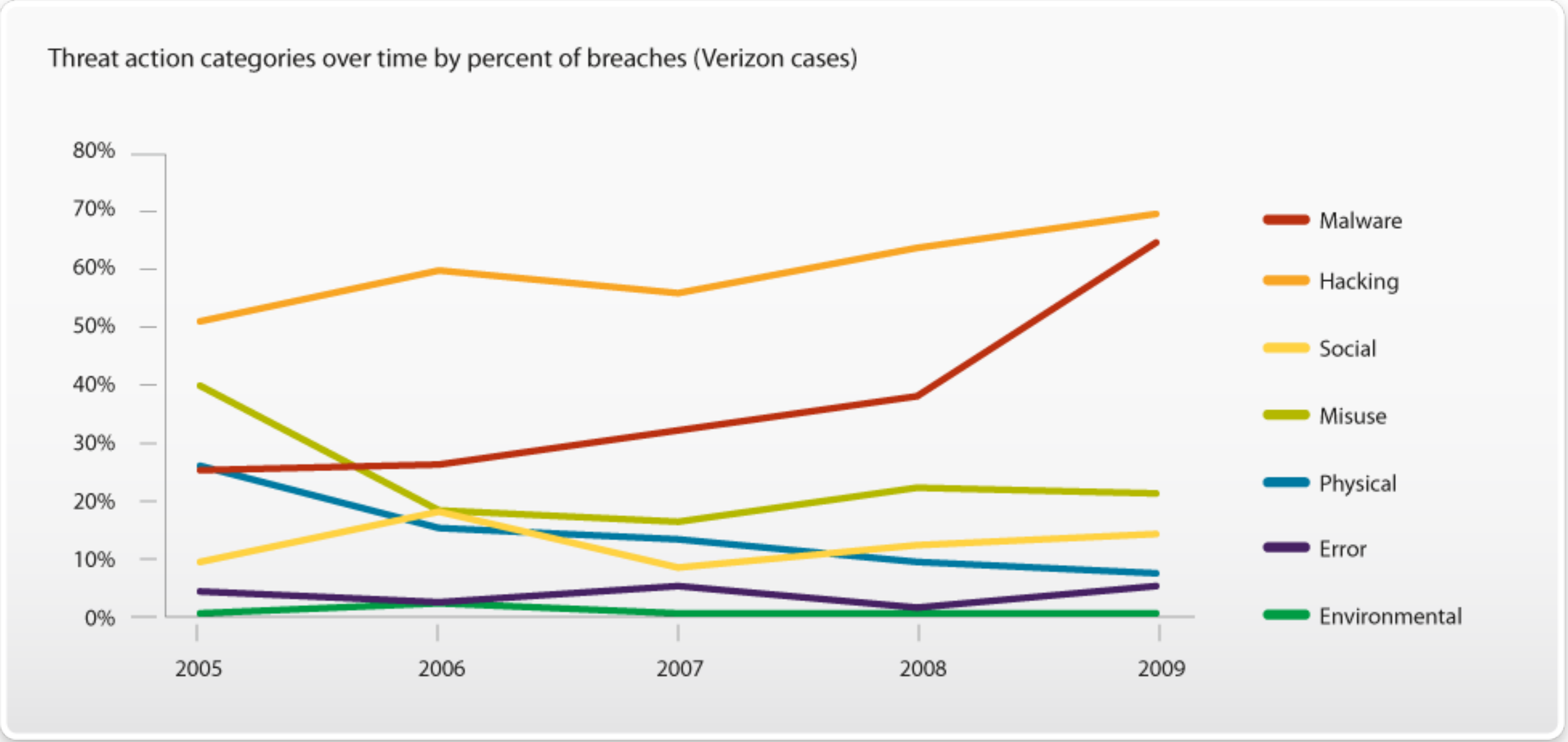
Regular employee/end-user	51%
Finance/accounting staff	12%
System/network administrator	12%
Executive/upper management	7%
Helpdesk staff	4%
Software developer	3%
Auditor	1%
Unknown	9%

Threat Actions



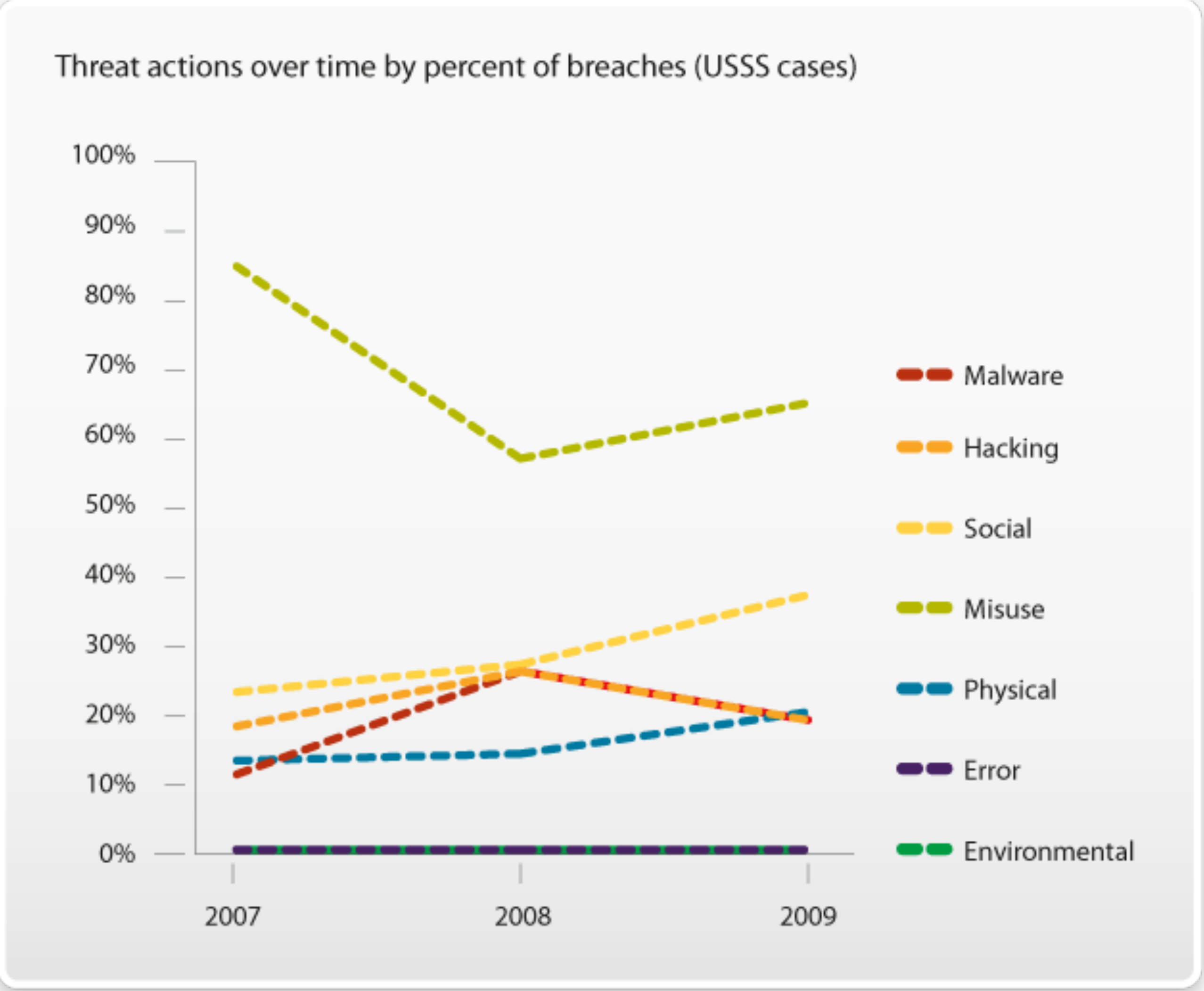
Threat Actions

Verizon



Threat Actions

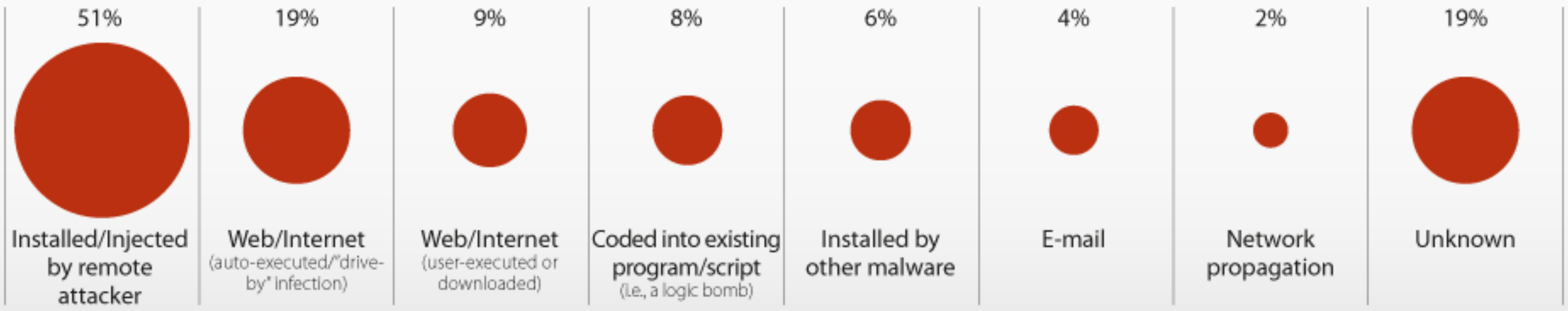
USSS



Malware

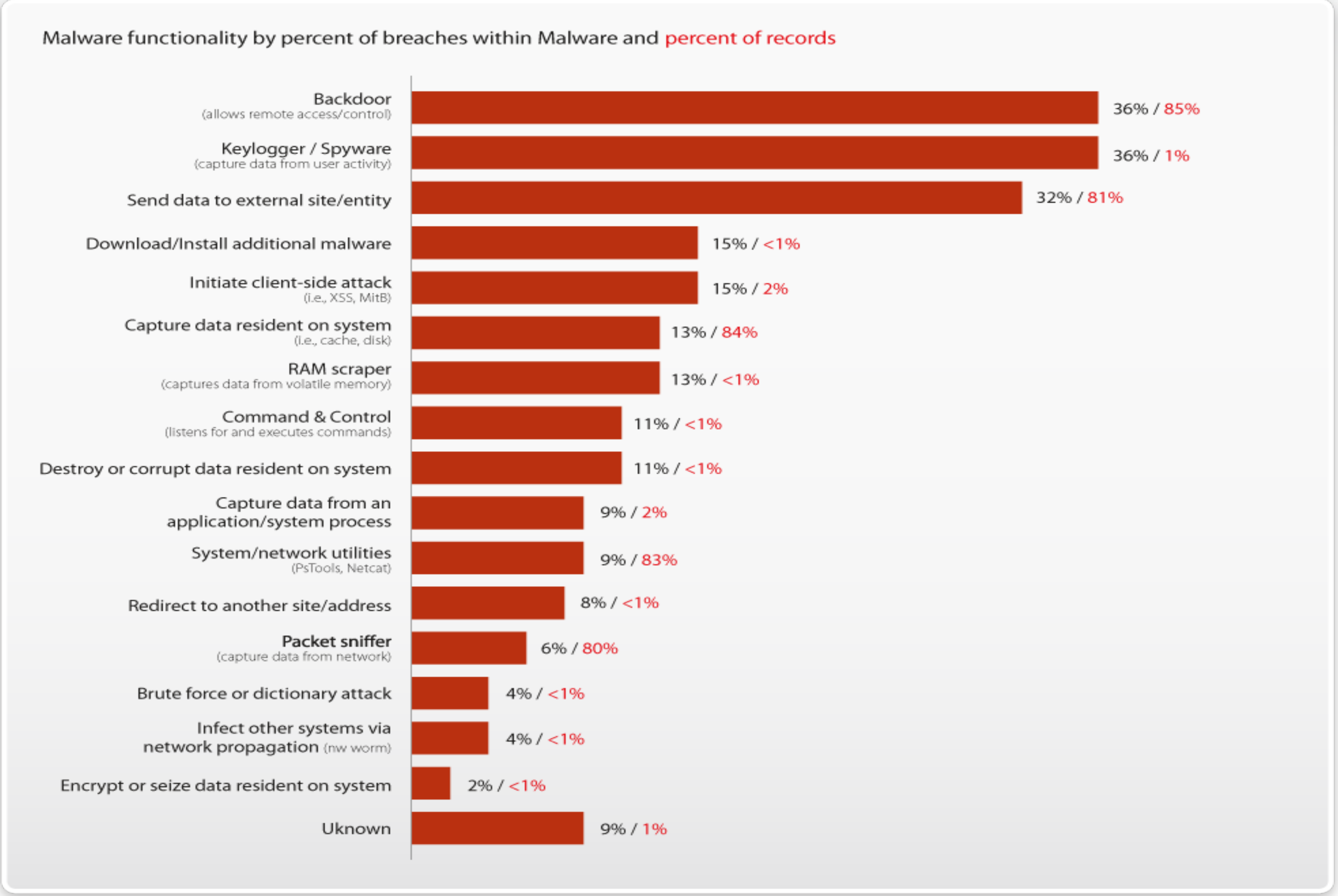
Infection Vector

Malware infection vectors by percent of breaches within Malware



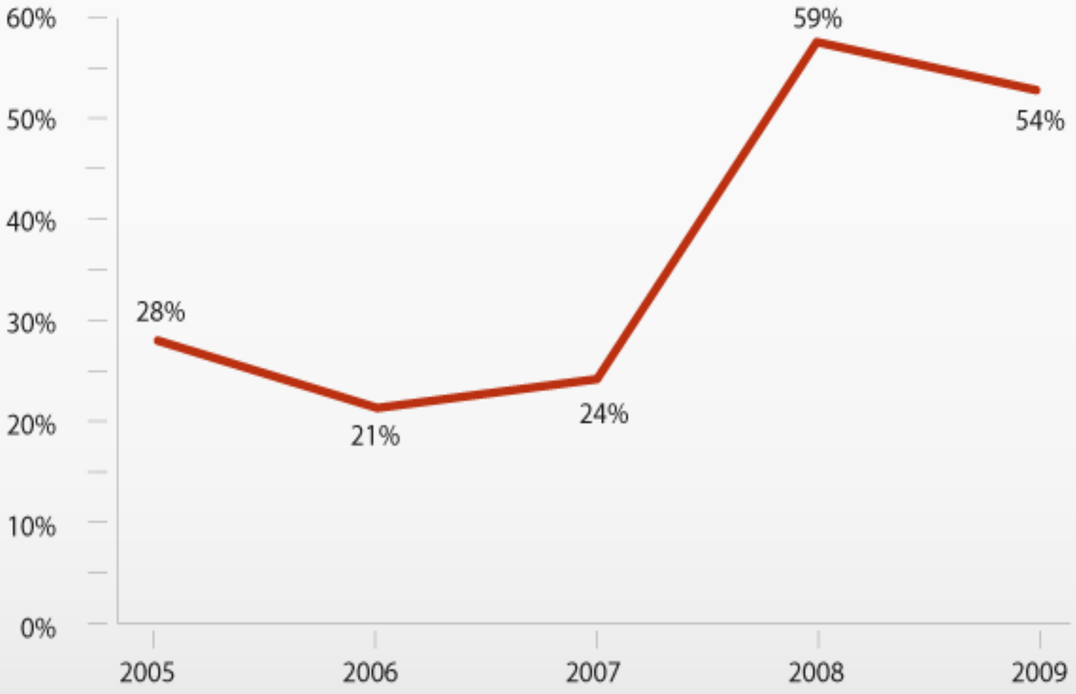
Malware

Functionality

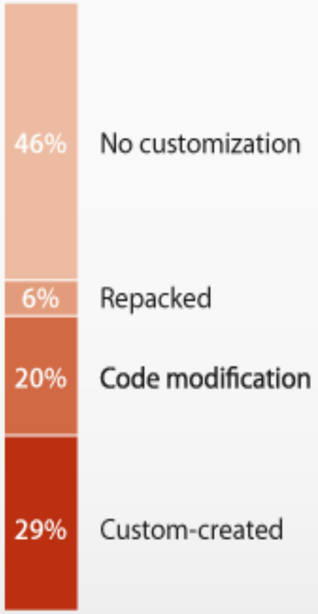


Malware
Customization

Malware customization over time
by percent of breaches within Malware*



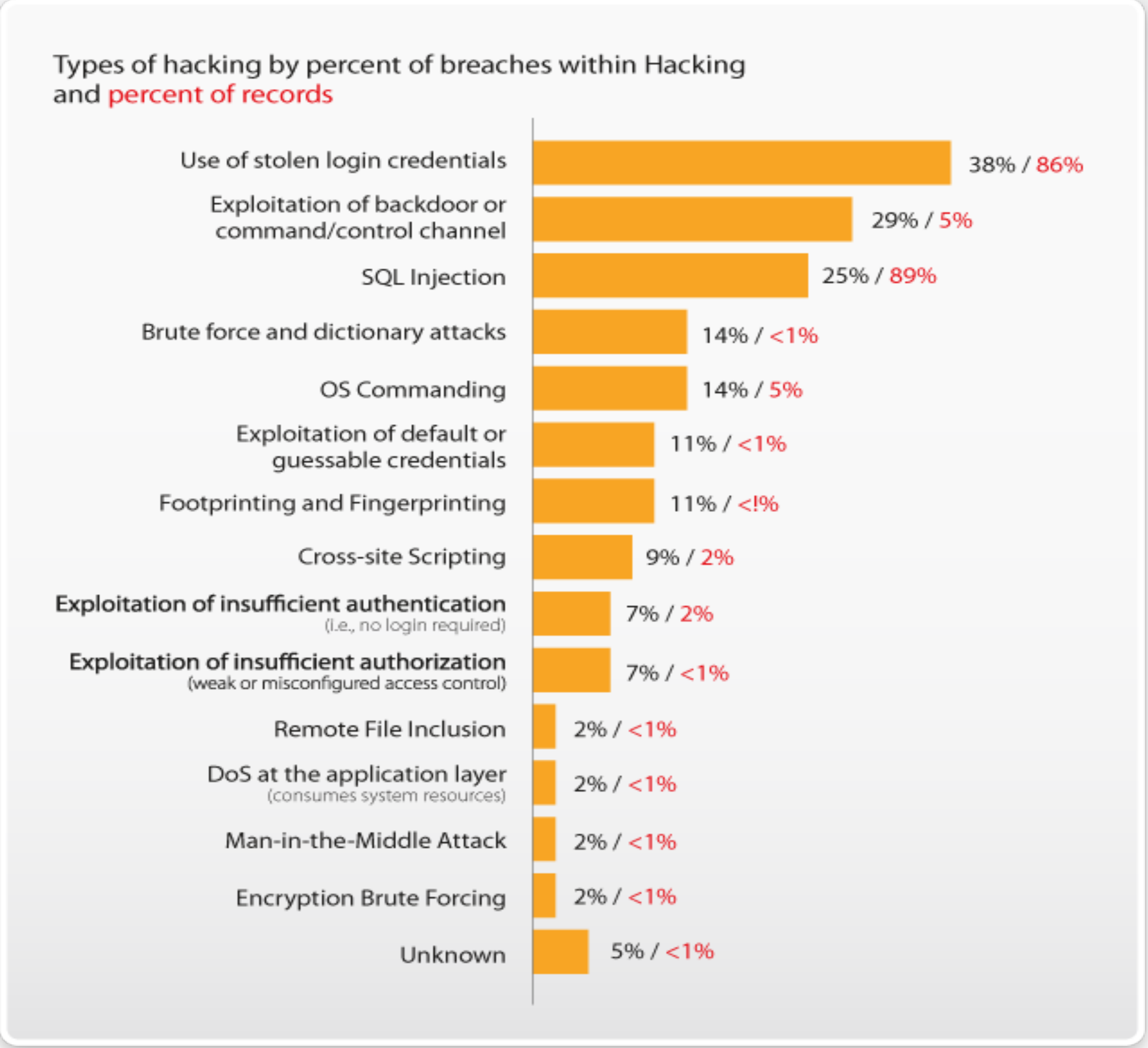
Level of malware customization by
percent of breaches within Malware*



* Verizon caseload only

Hacking

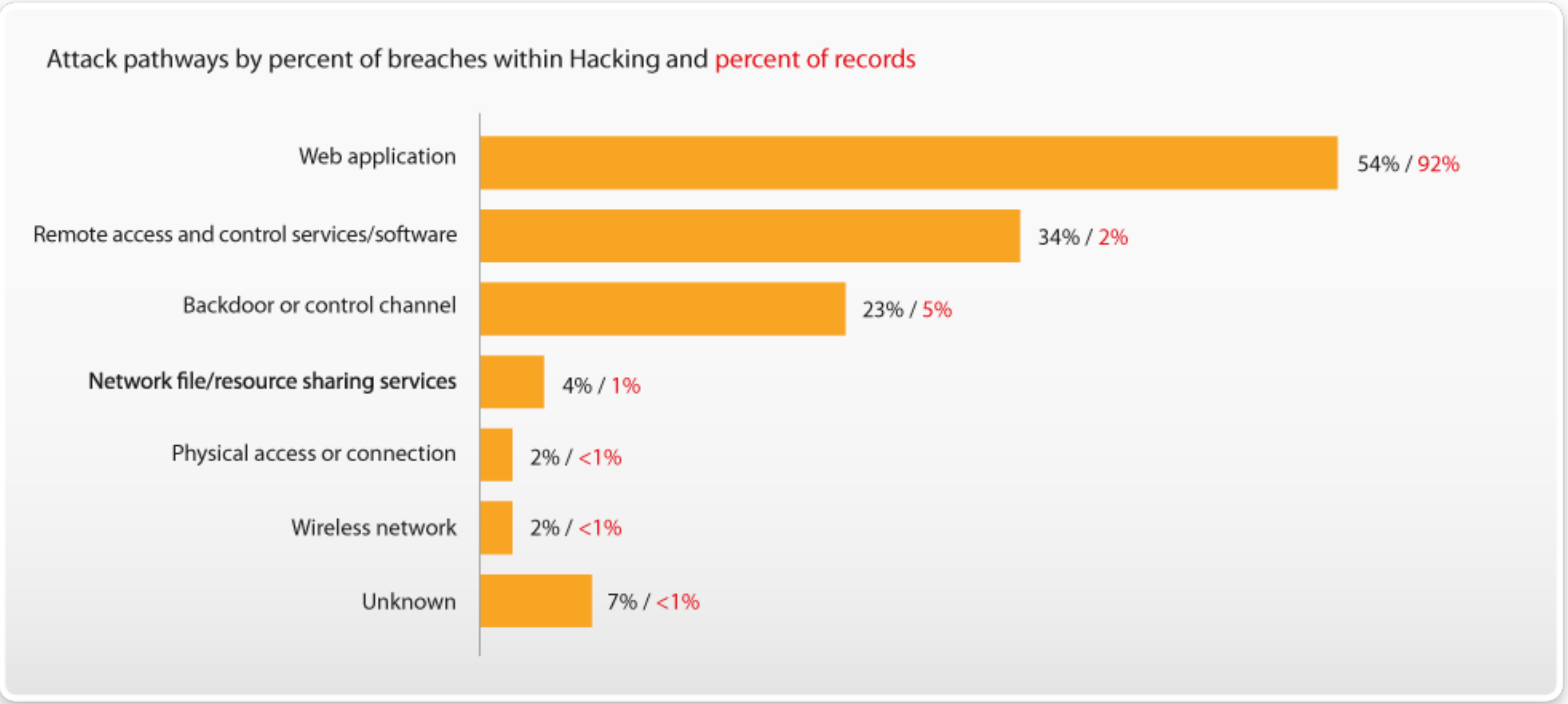
Types



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

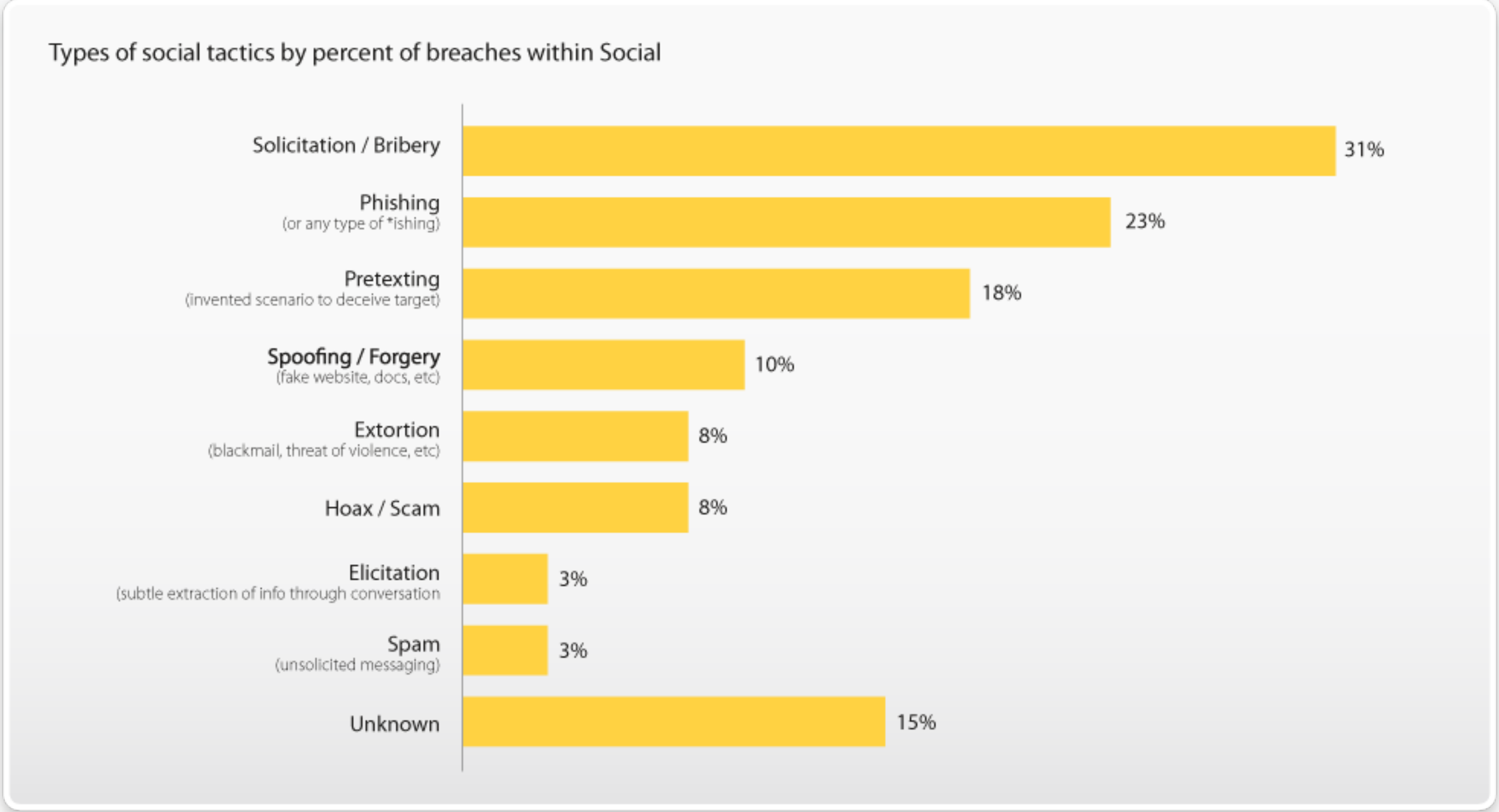
Hacking

Paths

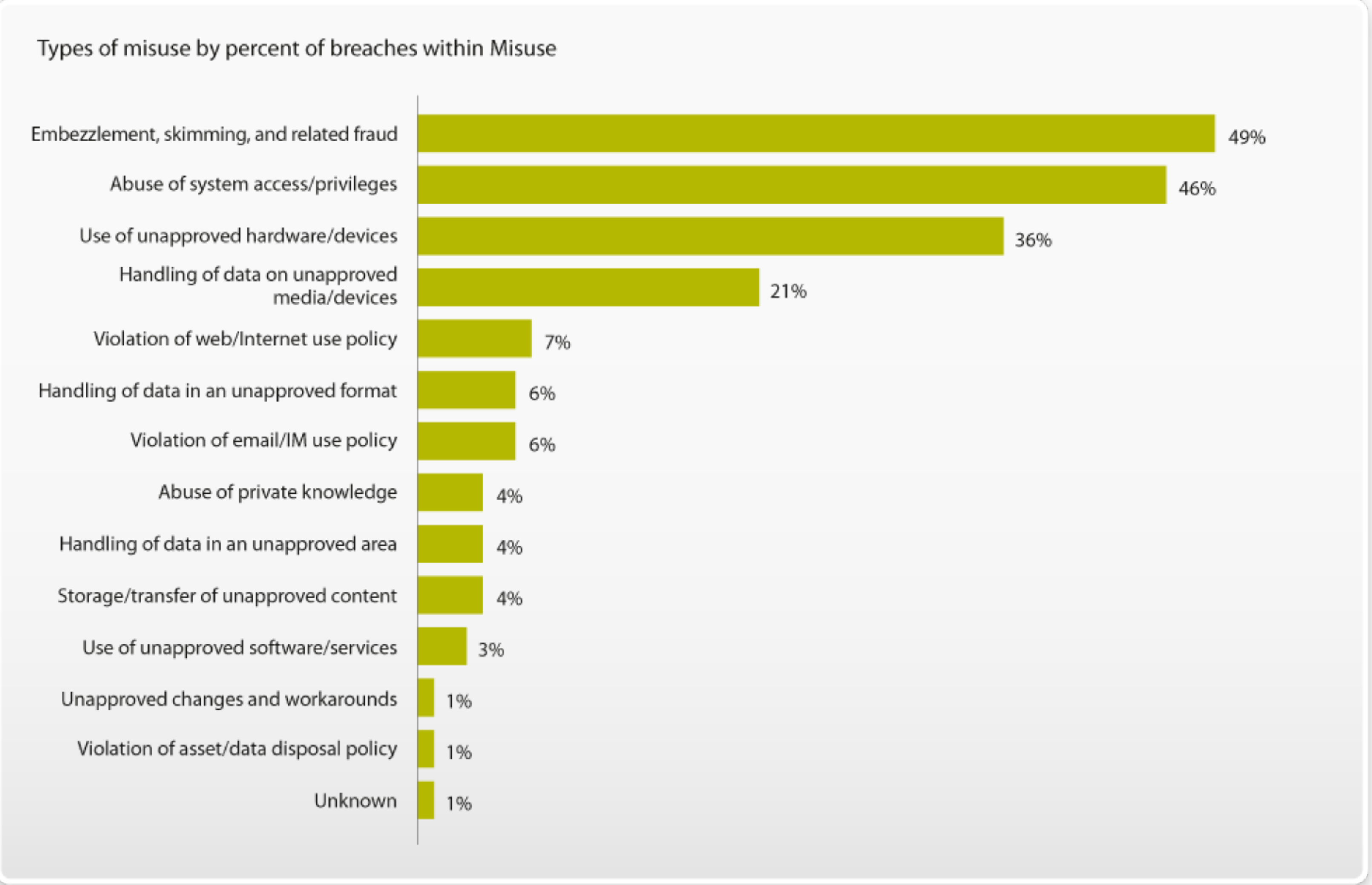


Patchable vulnerabilities: 0

Social
Types

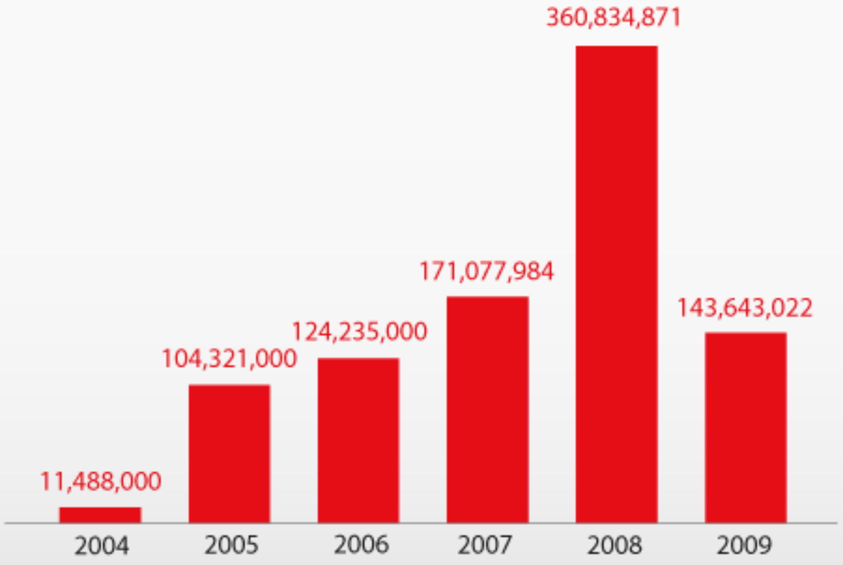


Misuse
Types

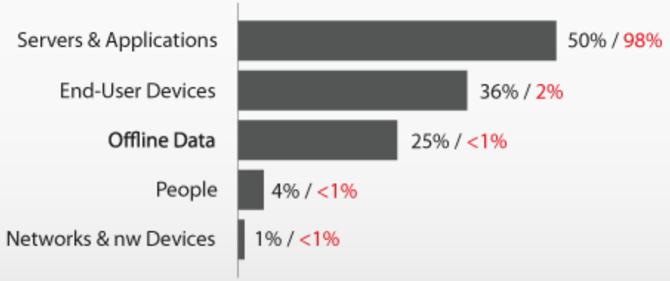


Assets & Data

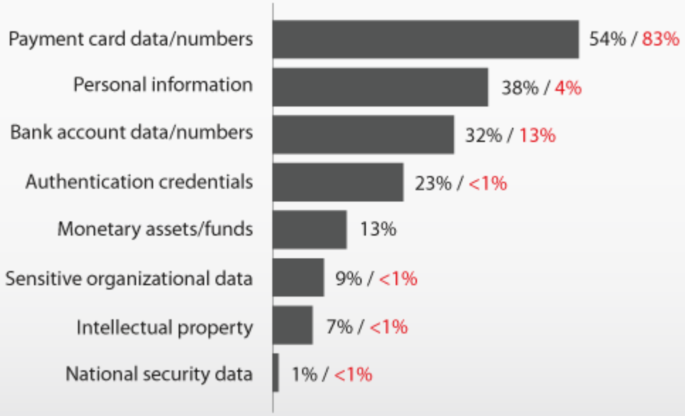
Number of records compromised per year in breaches investigated by Verizon and the United States Secret Service



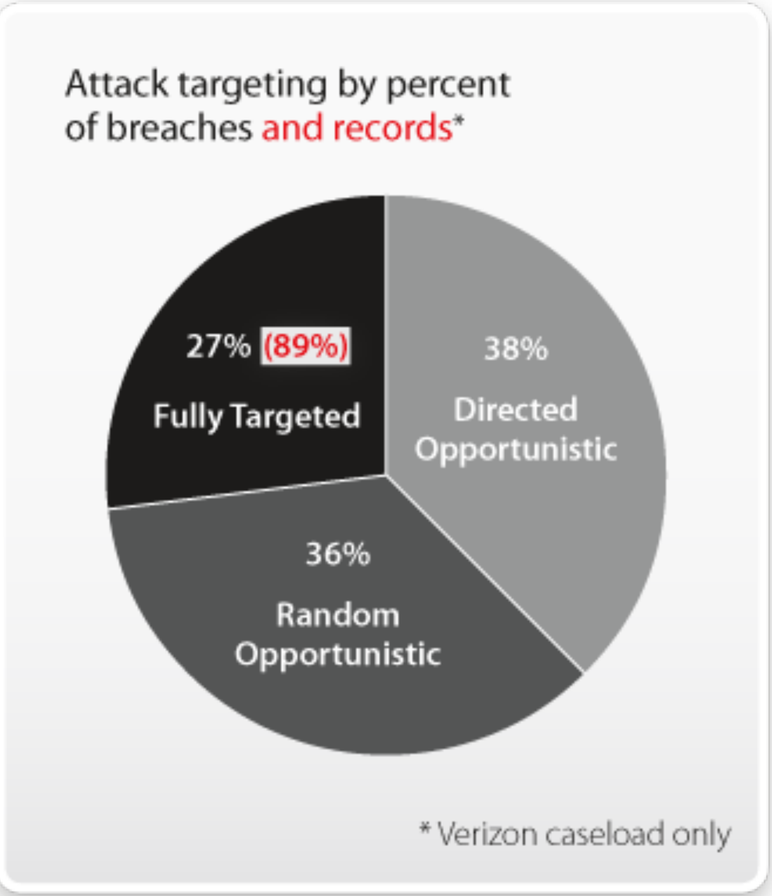
Categories of compromised assets by percent of breaches and percent of records



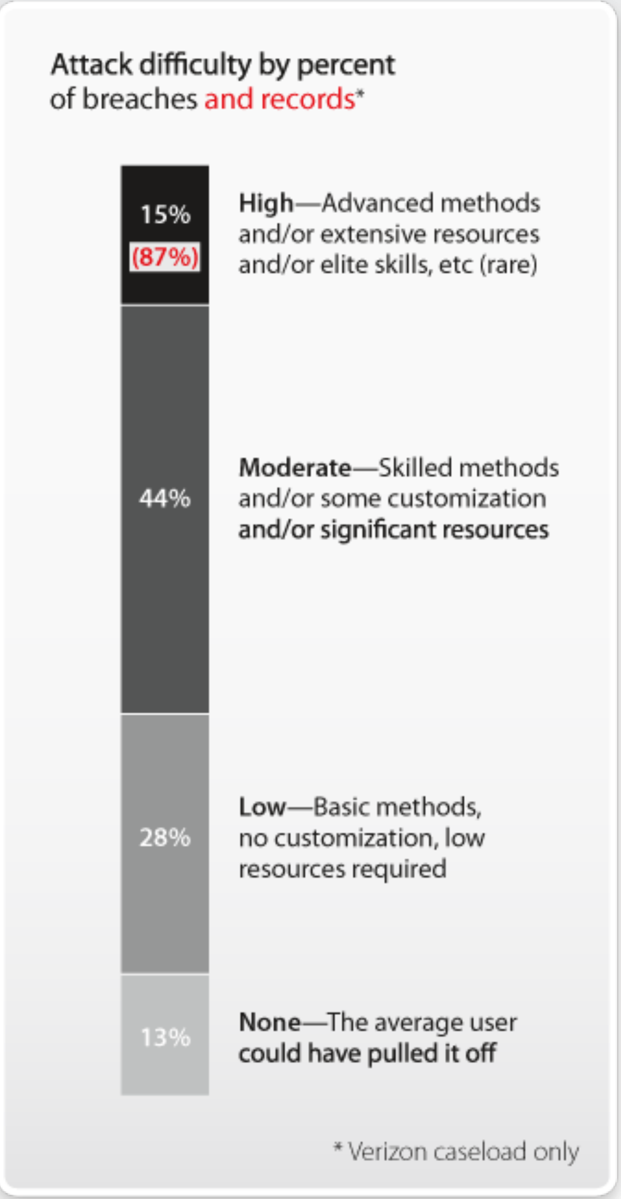
Compromised data types by percent of breaches and percent of records



Attack Difficulty & Targeting



* Verizon caseload only



High—Advanced methods and/or extensive resources and/or elite skills, etc (rare)

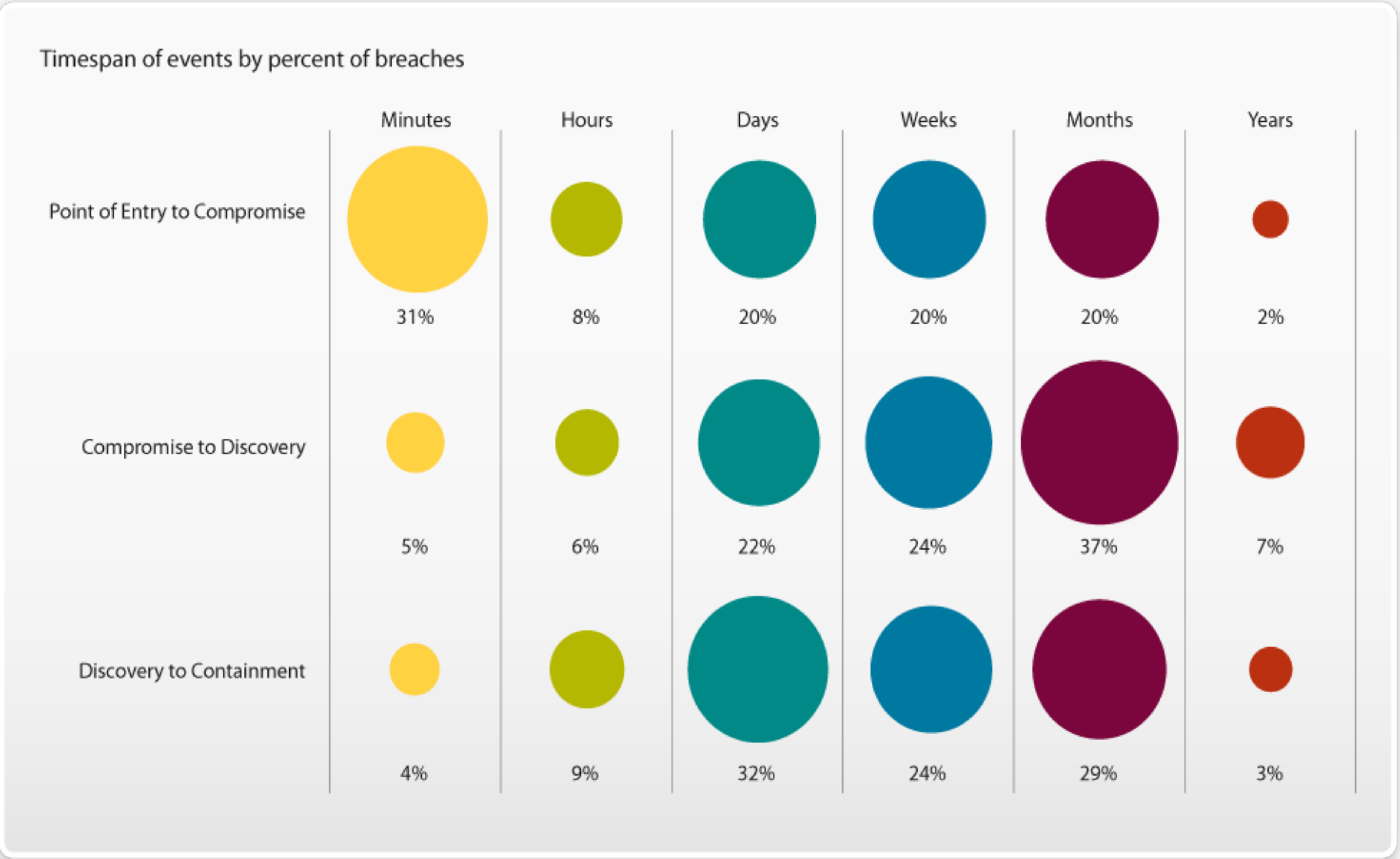
Moderate—Skilled methods and/or some customization and/or significant resources

Low—Basic methods, no customization, low resources required

None—The average user could have pulled it off

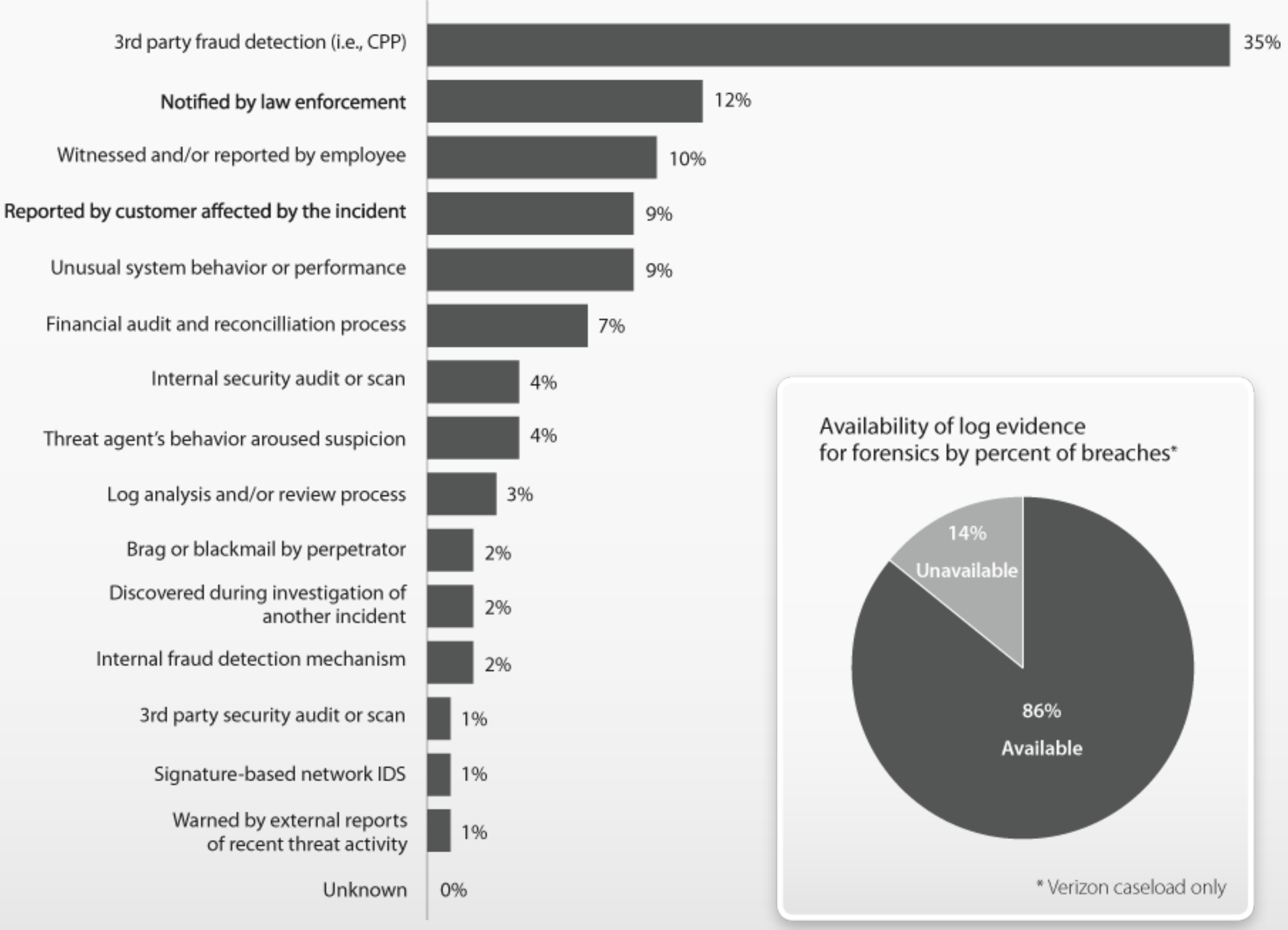
* Verizon caseload only

Time Span of Events

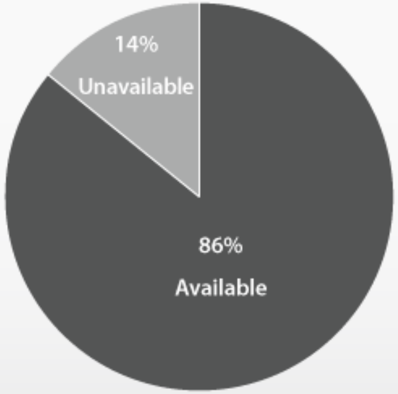


Discovery Methods

Breach discovery methods by percent of breaches

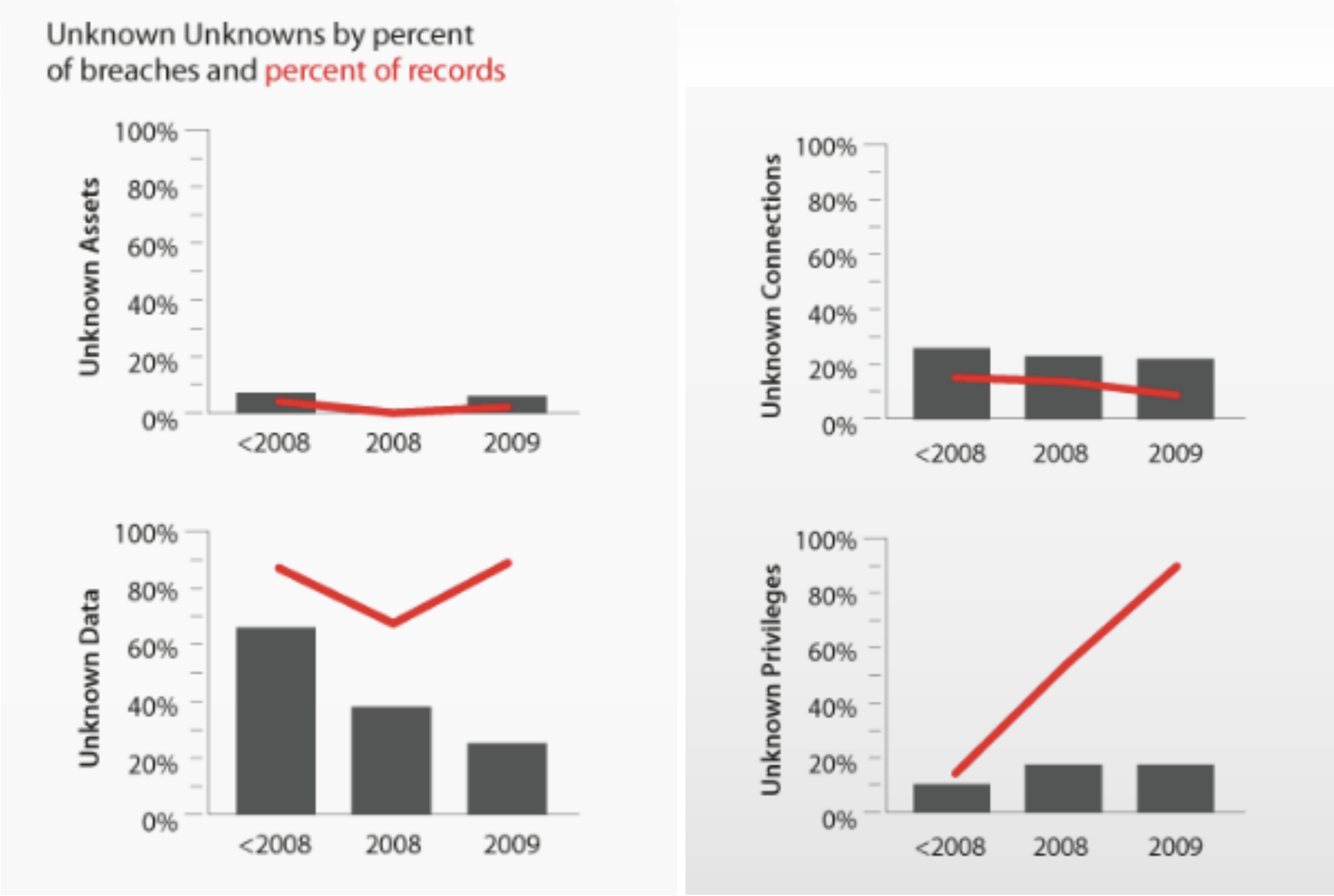


Availability of log evidence for forensics by percent of breaches*



* Verizon caseload only

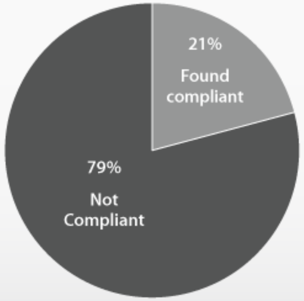
Unknown Unknowns



Unknown Unknowns by percent of breaches and percent of records

PCI DSS

PCI DSS compliance status based on last assessment*



* Verizon caseload only

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

Build and Maintain a Secure Network	2008	2009
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%
Protect Cardholder Data		
Requirement 3: Protect Stored Data	11%	30%
Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks	68%	90%
Maintain a Vulnerability Management Program		
Requirement 5: Use and regularly update anti-virus software	62%	53%
Requirement 6: Develop and maintain secure systems and applications	5%	21%
Implement Strong Access Control Measures		
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%
Regularly Monitor and Test Networks		
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%
Maintain an Information Security Policy		
Requirement 12: Maintain a policy that addresses information security	14%	40%

* Verizon caseload only

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

Conclusion & Recommendations

Assets

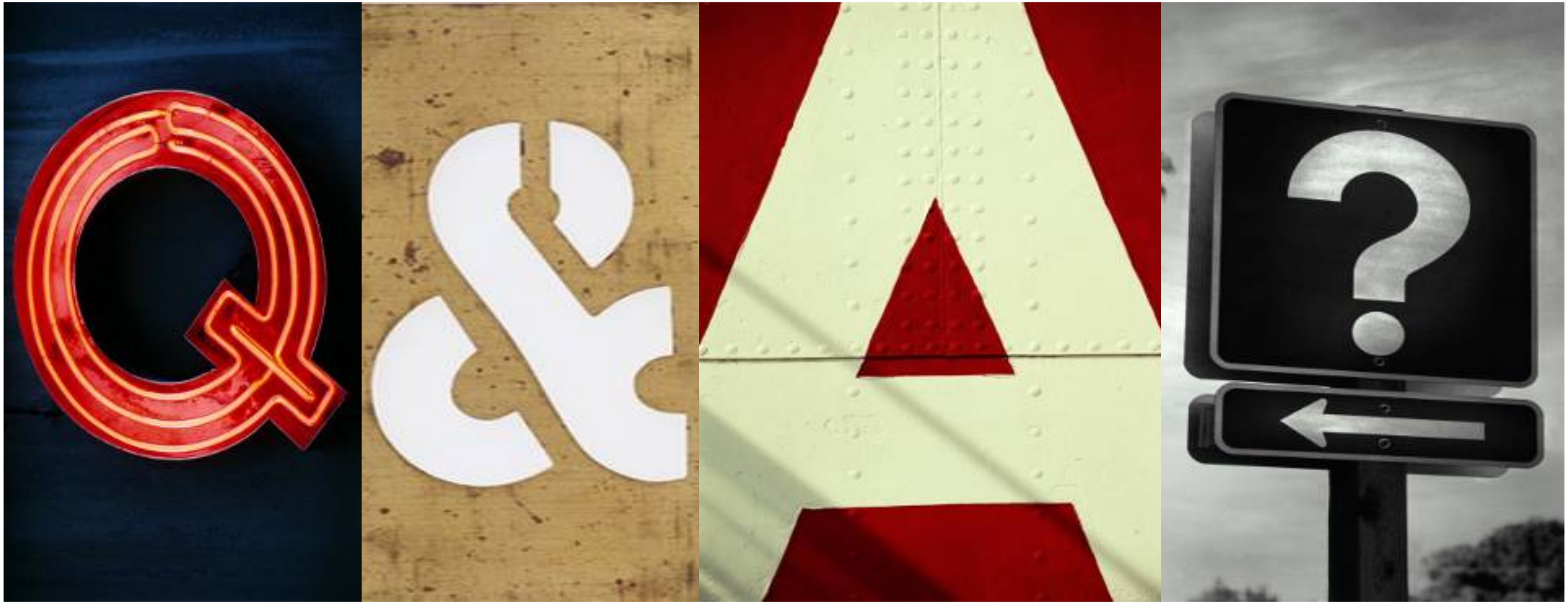
- Most data compromised from servers & apps
- Desktops/laptops increasing; related to stolen credentials
- Most criminals interested in cashable forms of data

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



DBIR	http://www.verizonbusiness.com/databreach
VERIS	https://verisframework.wiki.zoho.com/
Blog	http://securityblog.verizonbusiness.com
Email	dbir@verizonbusiness.com
Thijs Bosschert	thijs.bosschert@verizonbusiness.com