EVIDENCE
Suspects implicated in security breach
First known victim
2011
Data Breach
Investigations Report
A study conducted by the Verizon RISK Team with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit.
POLITIE
Korps landelijke politiediensten
verizon

PROPRIETARY STATEMENT

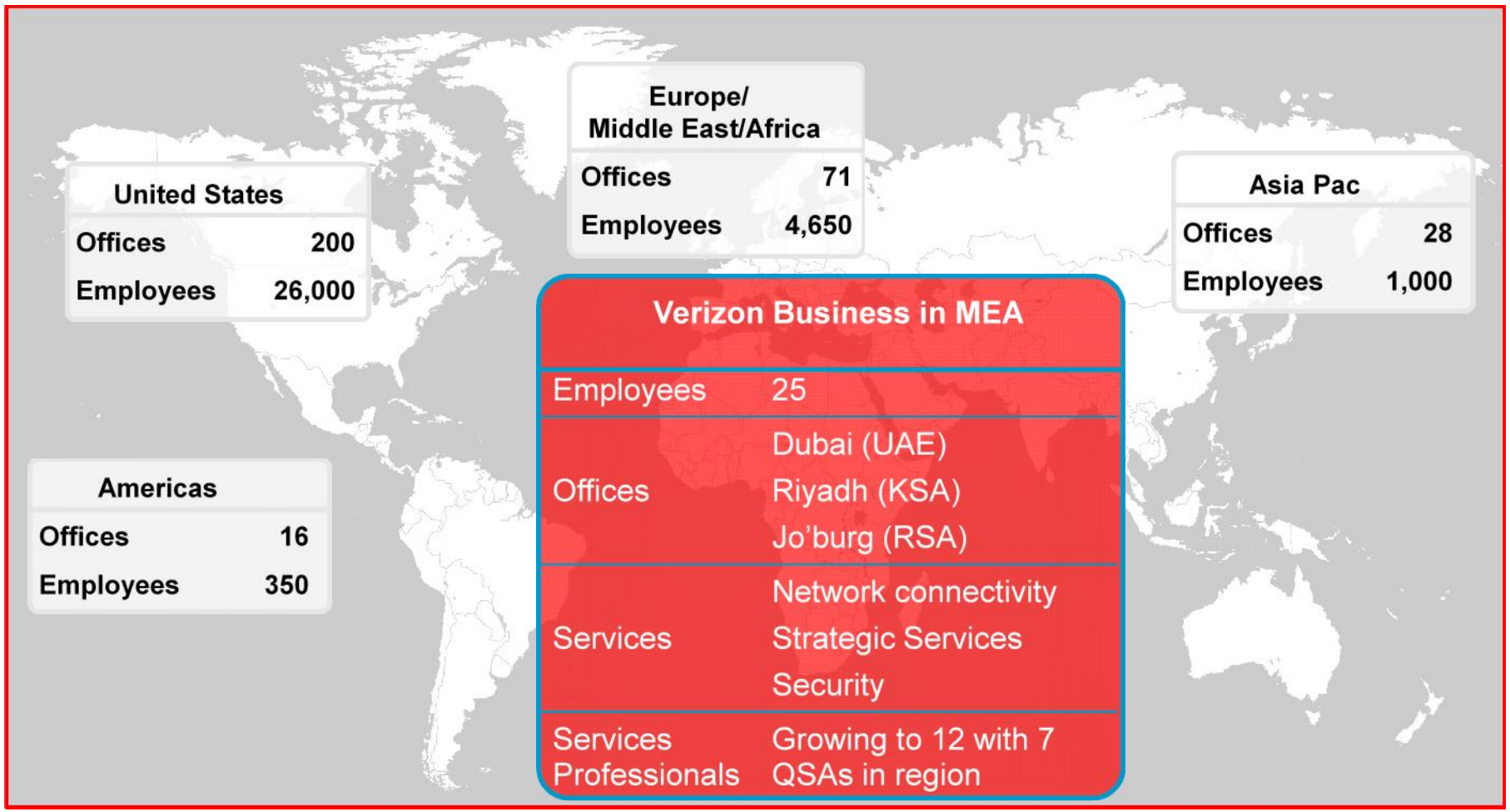
This document and any attached materials are the sole property of Verizon and are not to be used by you other than to evaluate Verizon's service.

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.

The Verizon and Verizon Business names and logos and all other names, logos, and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners.

Verizon Business
Global Resources to Meet Multinational Needs

Verizon Business, a unit of Verizon Communications (112 Billions revenues in 2010, 220 000 employees, part of the “DOW 30”), is a global leader in communications and IT solutions .



Data Breach Investigations Report (DBIR) series

An ongoing study into the world of cybercrime that analyzes forensic evidence to uncover how sensitive data is stolen from organizations, who's doing it, why they're doing it, and, of course, what might be done to prevent it.

Available at: http://verizonbusiness.com/databreach
Updates/Commentary: http://securityblog.verizonbusiness.com

verizon

2011 DBIR Contributors

Verizon

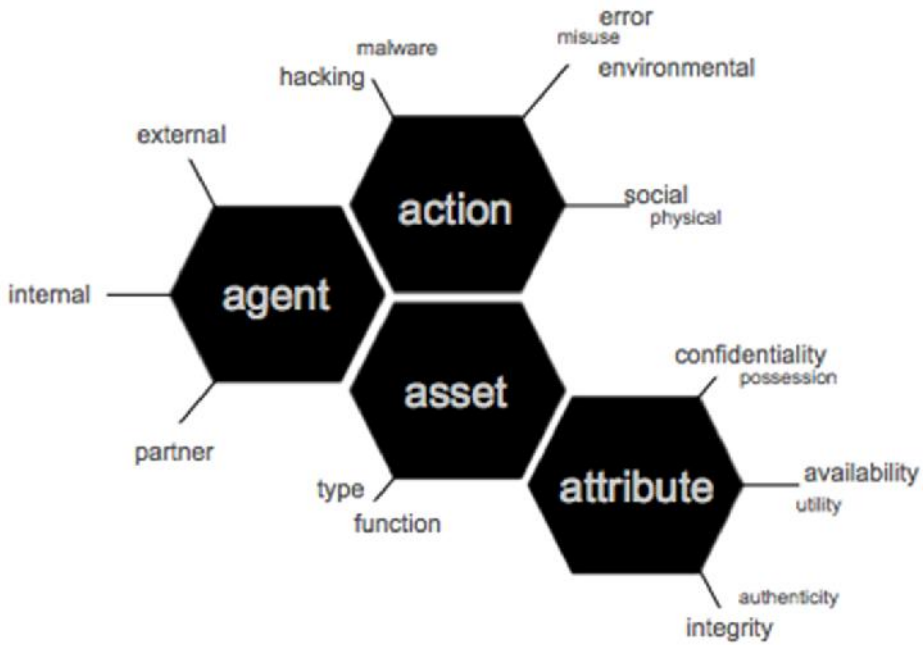
United States
Secret Service

Dutch National High
Tech Crime Unit

Methodology: Data Collection and Analysis

DBIR participants use the Verizon Enterprise Risk and Incident Sharing (VERIS) framework to collect and share data.

Enables case data to be shared anonymously to RISK Team for analysis



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

VERIS: https://verisframework.wiki.zoho.com/

How VERIS works

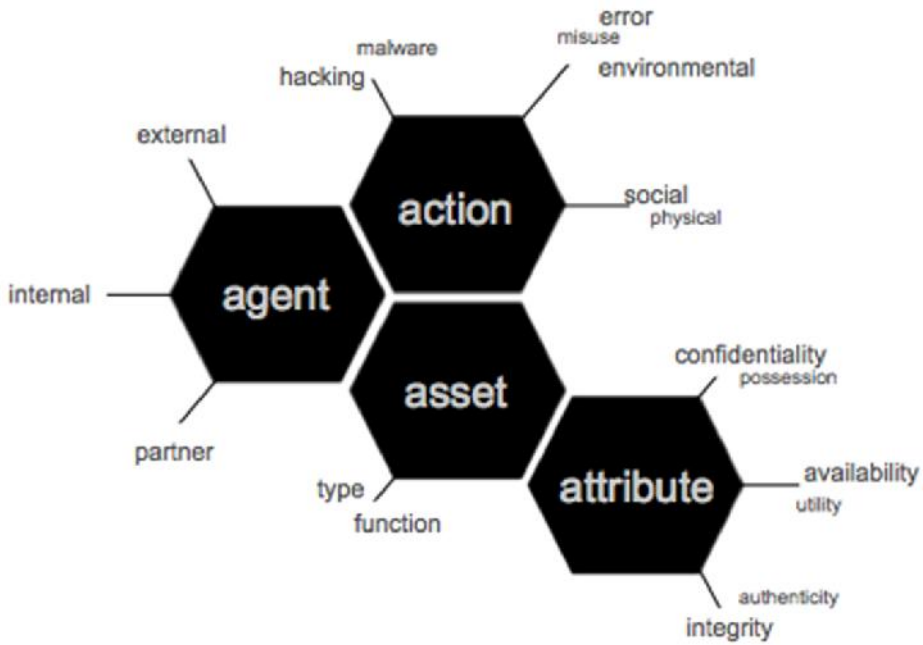
A security incident (or threat scenario) is modeled as a series of **events**. Every eve is comprised of the following 4 **A**'s:

Agent: Whose actions affected the asset

Action: What actions affected the asset

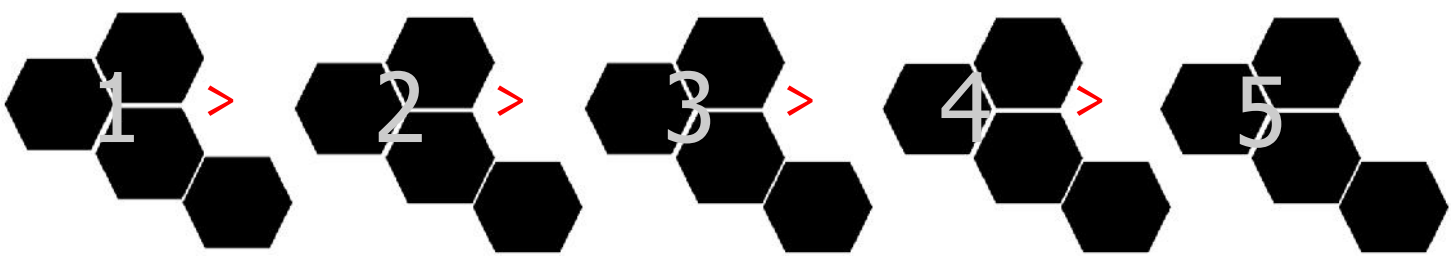
Asset: Which assets were affected

Attribute: How the asset was affected



The Incident Classification section employs Verizon's A4 threat model

Incident as a chain of events >



VERIS: https://verisframework.wiki.zoho.com/

How VERIS works

E1	E2	E3	CE1	E4
External agent sends a phishing e-mail that successfully lures an executive to open the attachment.	Malware infects the exec's laptop, creating a backdoor and installing a keylogger.	External agent accesses the exec's laptop via the backdoor, viewing e-mail and other sensitive data.	System administrator failed to enable proper authentication when building a new file server.	External agent accesses a mapped file server from the exec's laptop and steals intellectual property.
TE#553 External Social People Integrity	**TE#295** External Malware User Devices Integrity	**TE#256** External Hacking User Devices Confidentiality	**TE# 56** Internal Error Servers Integrity	**TE#4** External Hacking Servers Confidentiality

…and translates it to this…

verizon

Interpreting Charts and Tables

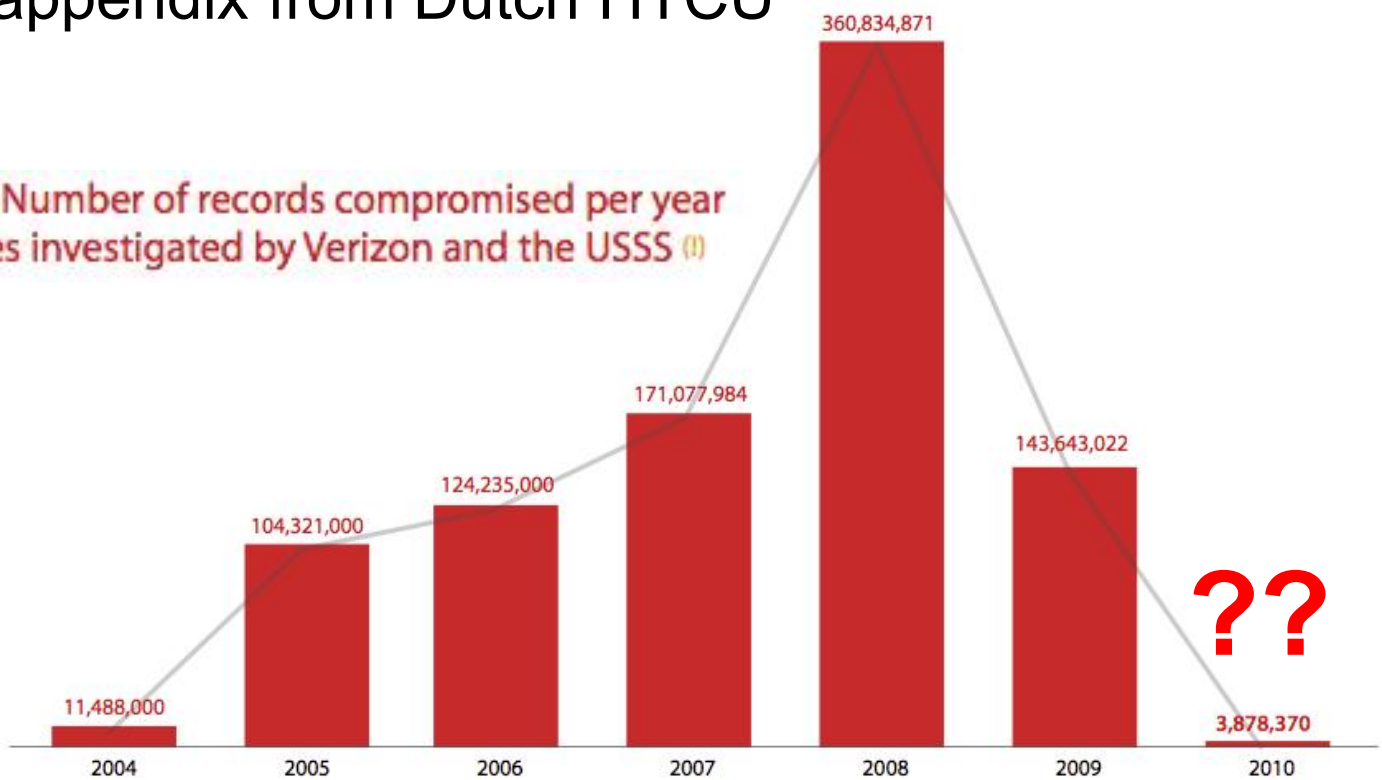
Table 1. Key for translating percents and numbers for 2009 and 2010 datasets

	2009 141 breaches	2010 761 breaches
3%	4	23
10%	14	76
25%	35	190
33%	47	251
50%	71	381
75%	106	571
100%	141	761

verizon

Overview – What's New?

- Over **750 new breaches** studied since the last report
  - Total for all years = 1700+
- Just under **4 million records** confirmed compromised
  - Total for all years = 900+ million
- Euro-centric appendix from Dutch HTCU



Drop in Data Loss – Our Leading Hypotheses

- ~~Random caseload variation~~
  - Unlikely; other external sources show similar results
- ~~Huge global improvement in security posture~~
  - Unlikely; Not enough time and doesn't explain rise in breaches
- Prosecution and incarceration of "Kingpins"
  - Deterrence and/or scrambling among criminal groups
- Change in criminal tactics
  - Away from massive breaches to smaller, less risky heists
  - Helps explain increase in breaches
- Market forces (law of supply and demand)
  - Oversupply of data in black market driving prices down
- Targeting different (non-bulk) data types
  - More IP, classified data, etc stolen
- They've gotten better at evading detection
  - Maybe; but doesn't seem to fully account for the drop

verizon

Demographics

Figure 3. Industry groups represented by percent of breaches

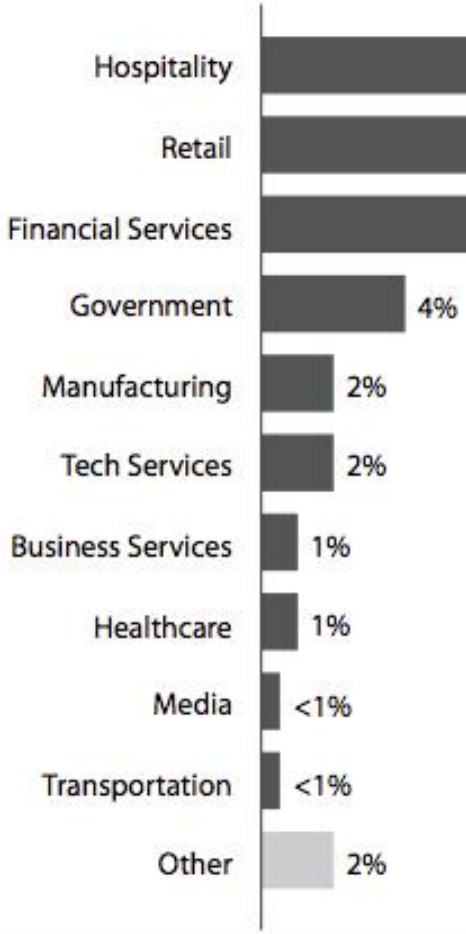


Table 2. Organizational size by number of breaches (number of employees)

1 to 10	46
11 to 100	436 (1)
101 to 1,000	74
1,001 to 10,000	49
10,001 to 100,000	59
Over 100,000	55
Unknown	40

verizon

Agents: Whose Actions Affected the Asset?

Figure 7. Threat agents (inclusive) by percent of breaches

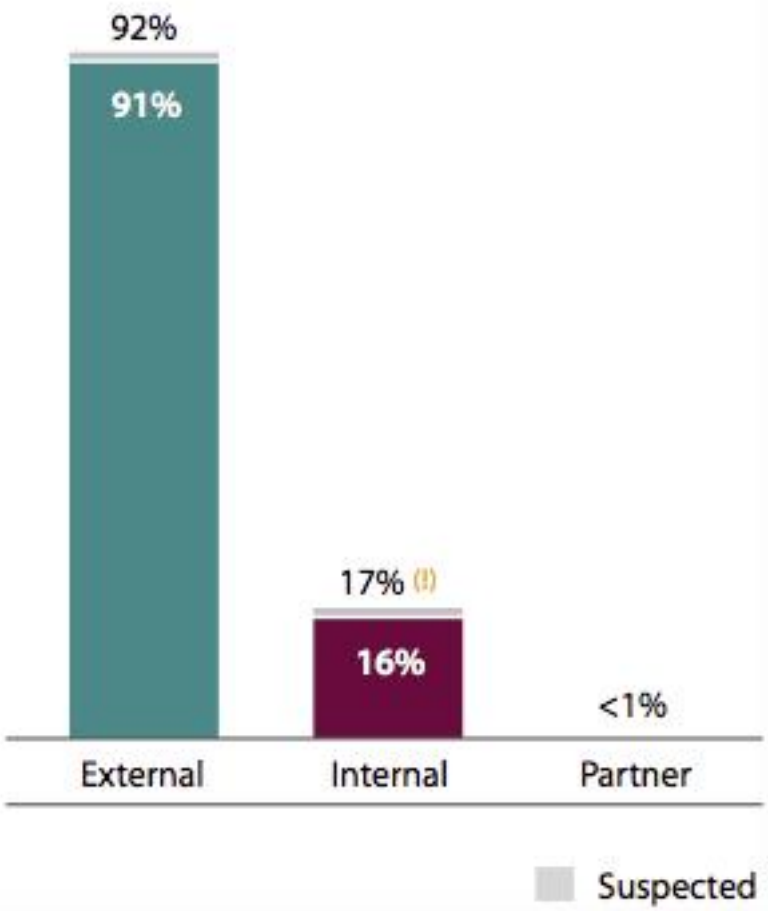
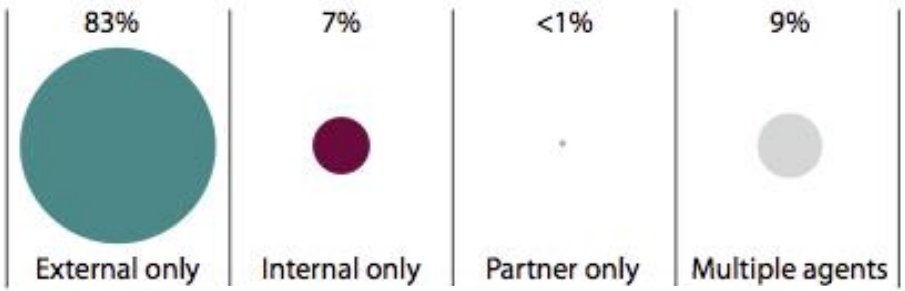


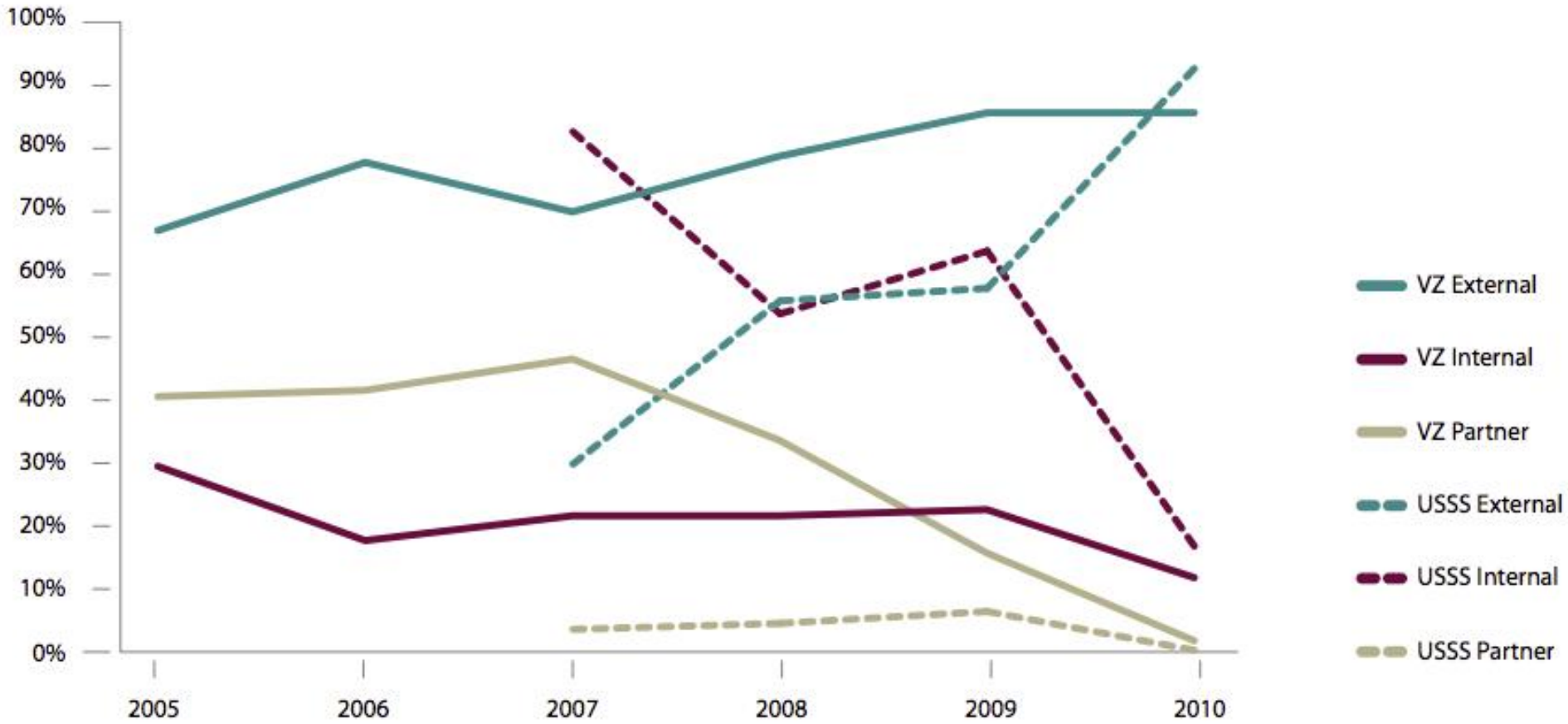
Figure 9. Threat agents (exclusive) by percent of breaches



VERIS Classification Note: If the agent's role in the breach is limited to a contributory error (see explanation in the Error sub-section under Threat Actions), the agent would not be included here. For example, if an insider's unintentional misconfiguration of an application left it vulnerable to attack, the insider would not be considered an agent if the application were successfully breached by another agent. An insider who deliberately steals data or whose inappropriate behavior (i.e., policy violations) facilitated the breach would be considered an agent in the breach.

Agents: Whose Actions Affected the Asset?

Figure 8. Threat agents over time by percent of breaches



verizon

Agents: Whose Actions Affected the Asset?

Figure 10. Compromised records by threat agent, 2010

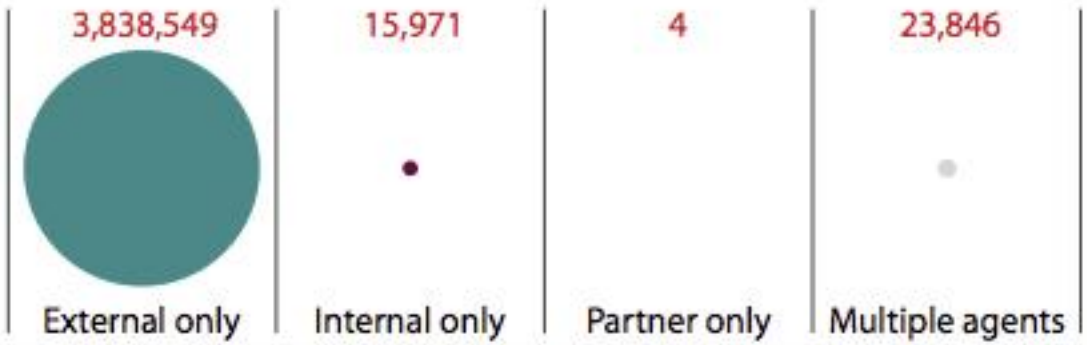


Figure 11. Compromised records by threat agent, 2004-2010

verizon

Agents: More about External Agents

Figure 13. Origin of external agents by percent of breaches within External

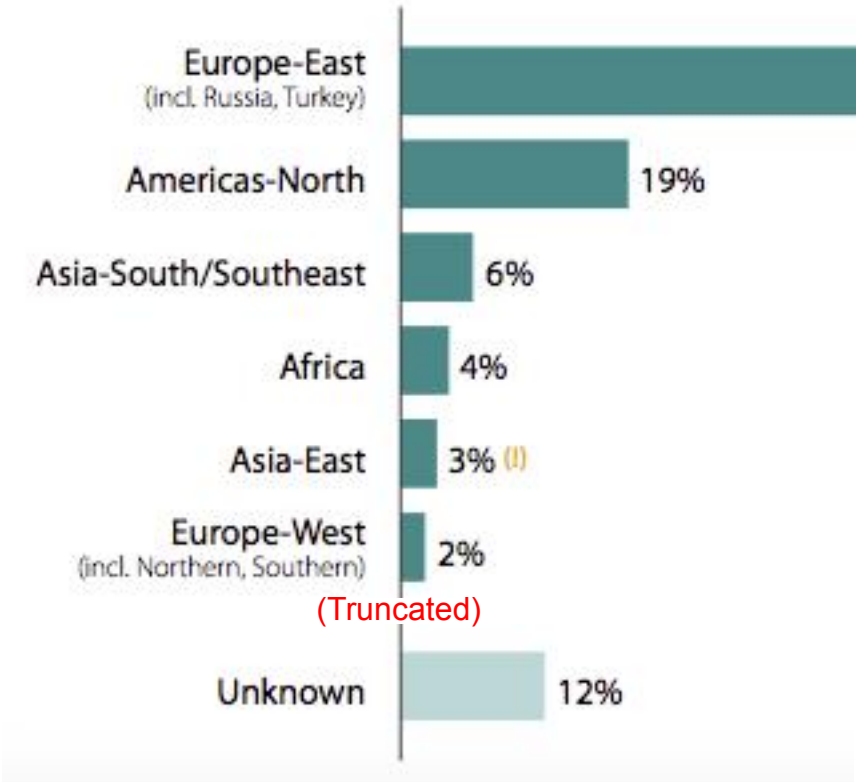


Table 6. Types of external agents by percent of breaches within External

Organized criminal group	58% (I)
Unaffiliated person(s)	40% (I)
Former employee (no longer had access)	2%
Competitor	1%
Unknown	14%
Other	<1%

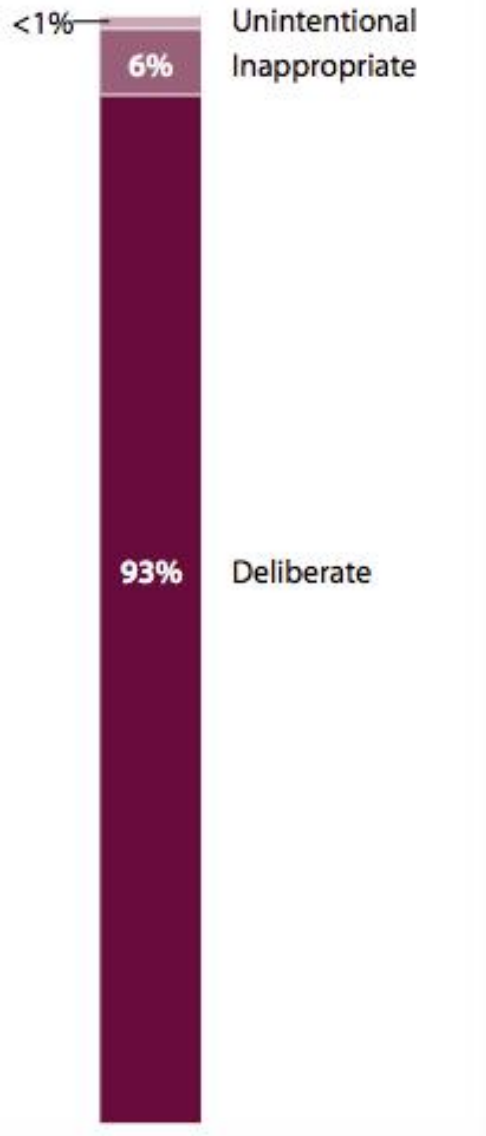
verizon

Agents: More about Internal Agents

Table 7. Types of internal agents by percent of breaches within Internal

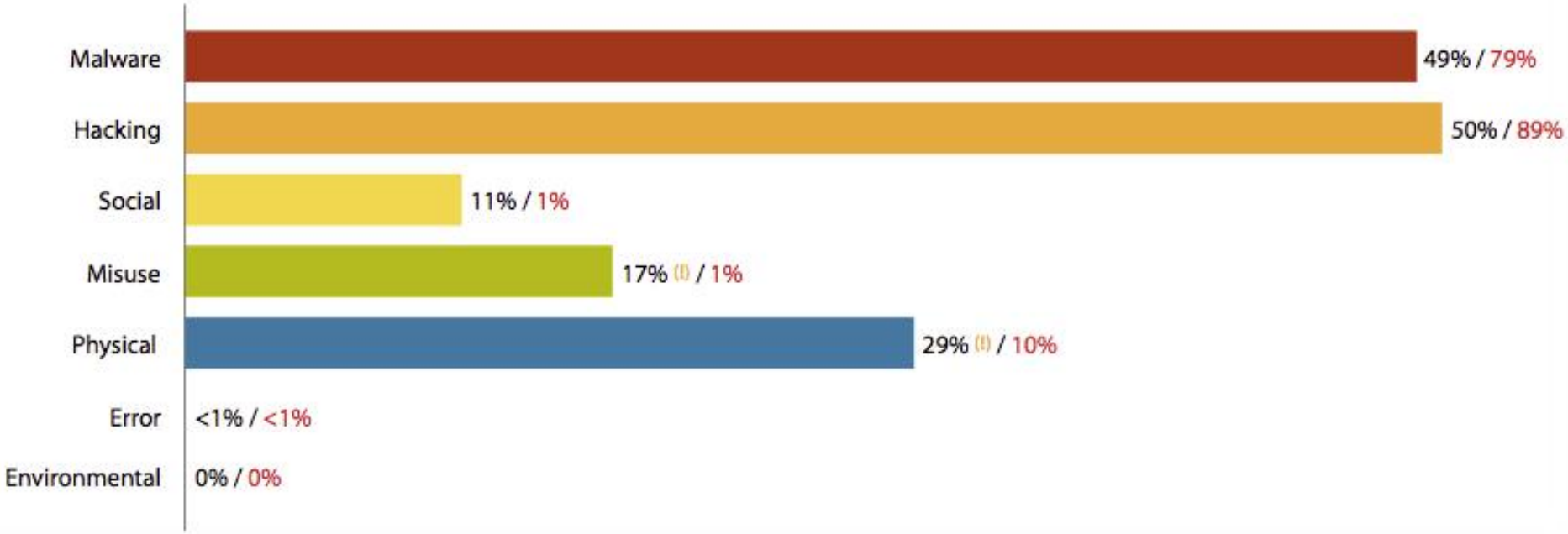
Regular employee/end-user	85% (1)
Finance/accounting staff	22%
Executive/upper management	11%
Helpdesk staff	4%
System/network administrator	3%
Software developer	2%
Unknown	1%
Other(s)	1%

Figure 14. Role of internal agents by percent of breaches within Internal



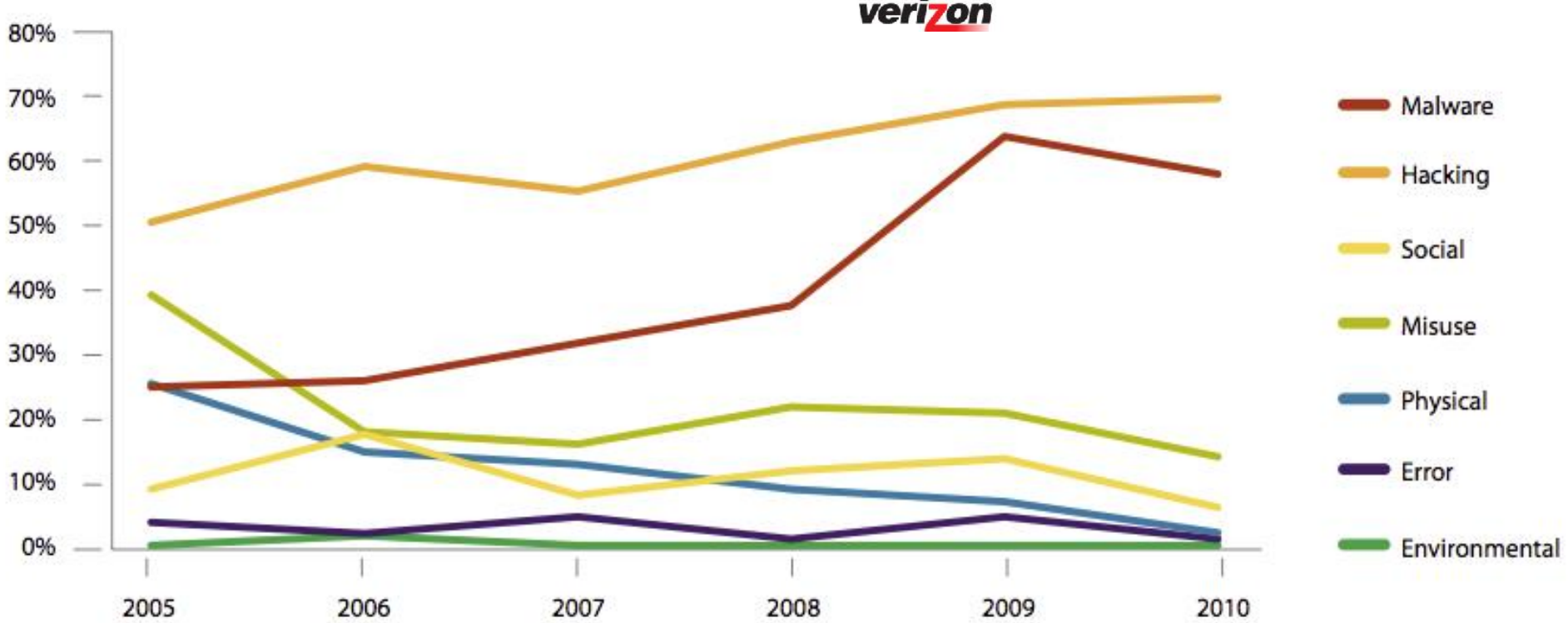
Actions: What Actions Affected the Asset?

Figure 15. Threat action categories by percent of breaches and percent of records



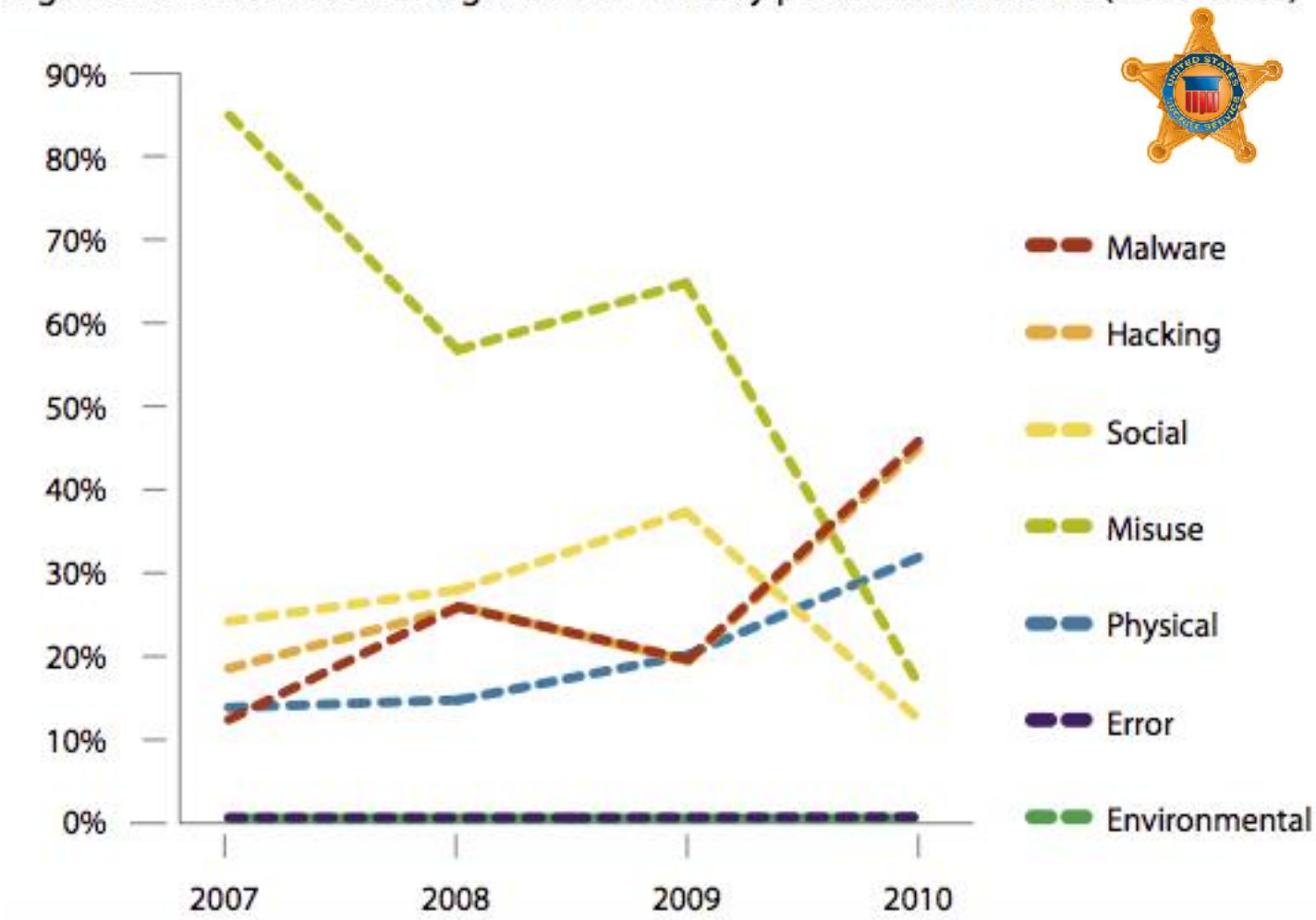
Actions: What Actions Affected the Asset?

Figure 16. Threat action categories over time by percent of breaches (Verizon cases)



Actions: What Actions Affected the Asset?

Figure 17. Threat action categories over time by percent of breaches (USSS cases)



verizon

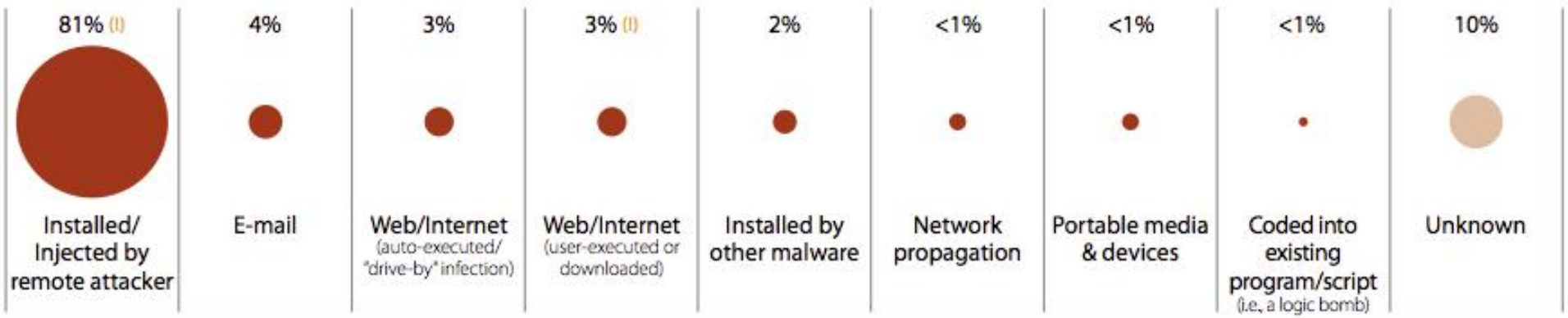
Top 15 Threat Actions

Table 8. Top 15 Threat Action Types by number of breaches and number of records

	Category	Threat Action Type	Short Name	Breaches	Records
1	Malware	Send data to external site/entity	SNDATA	297	1,729,719
2	Malware	Backdoor (allows remote access / control)	MALBAK	294	2,065,001
3	Hacking	Exploitation of backdoor or command and control channel	HAKBAK	279	1,751,530
4	Hacking	Exploitation of default or guessable credentials	DFCRED	257	1,169,300
5	Malware	Keylogger/Form-grabber/Spyware (capture data from user activity)	KEYLOG	250	1,538,680
6	Physical	Tampering	TAMPER	216	371,470
7	Hacking	Brute force and dictionary attacks	BRUTE	200	1,316,588
8	Malware	Disable or interfere with security controls	DISABL	189	736,884
9	Hacking	Footprinting and Fingerprinting	FTPRNT	185	720,129
10	Malware	System/network utilities (PsTools, Netcat)	UTILITY	121	1,098,643
11	Misuse	Embezzlement, skimming, and related fraud	EMBZZL	100	37,229
12	Malware	RAM scraper (captures data from volatile memory)	RAMSCR	95	606,354
13	Hacking	Use of stolen login credentials	STLCRED	79	817,159
14	Misuse	Abuse of system access/privileges	ABUSE	65	22,364
15	Social	Solicitation/Bribery	BRIBE	59	23,361
		Honorable Mention at #16			
16	Hacking	SQL Injection	SQLINJ	54	933,157

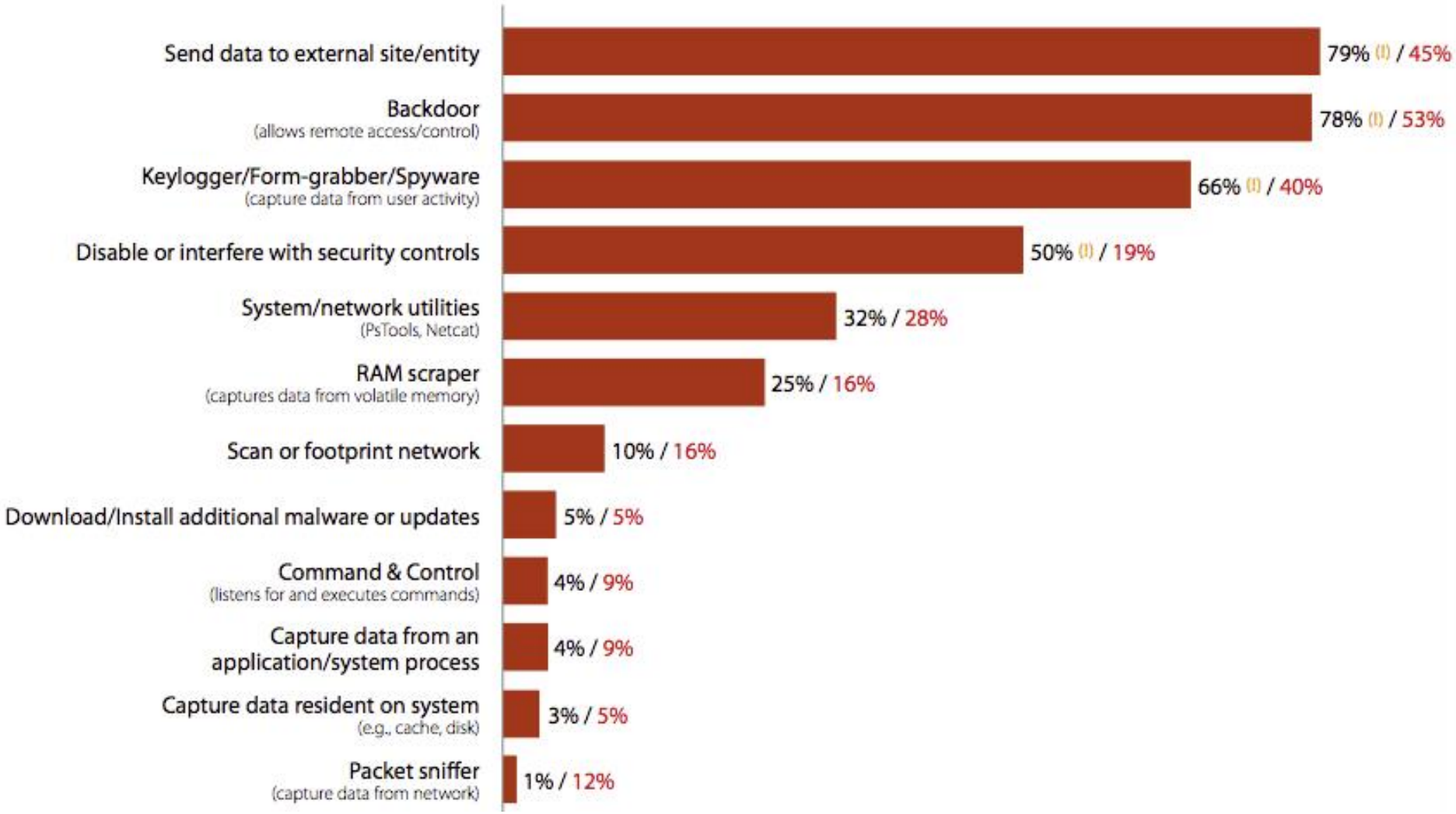
Actions: More on Malware (49% of breaches)

Figure 19. Malware infection vectors by percent of breaches within Malware



Actions: More on Malware (49% of breaches)

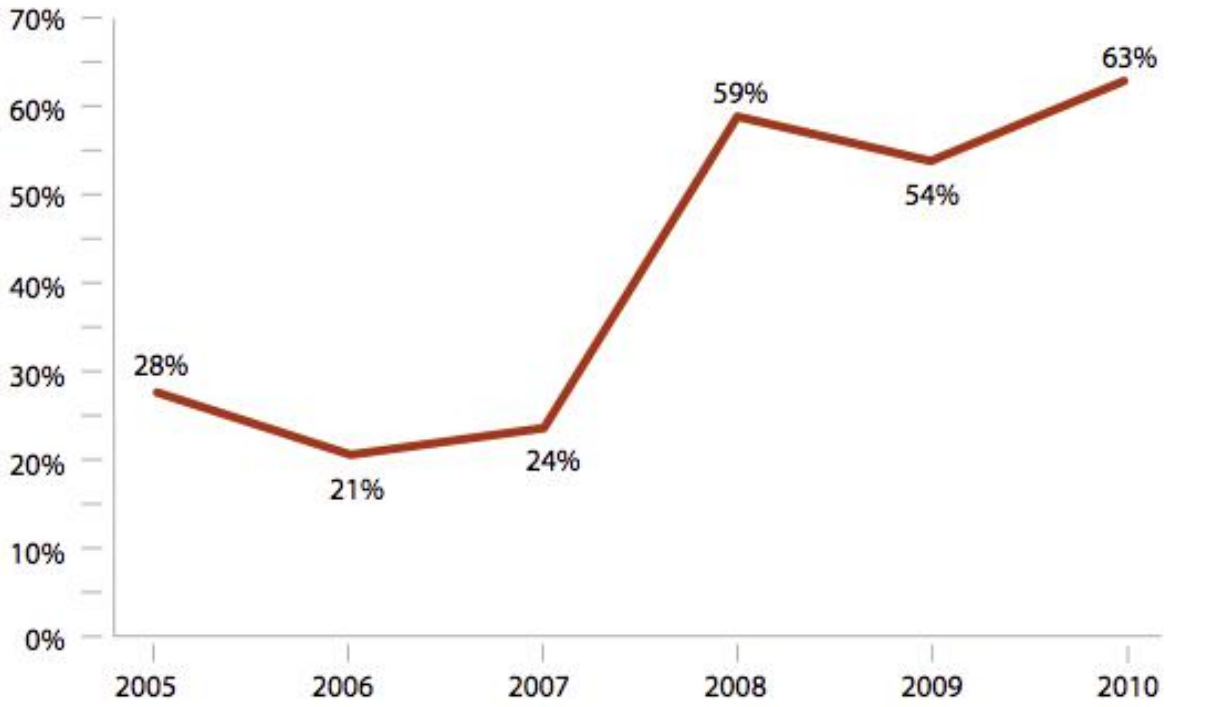
Figure 20. Malware functionality by percent of breaches within Malware and percent of records



(Truncated)

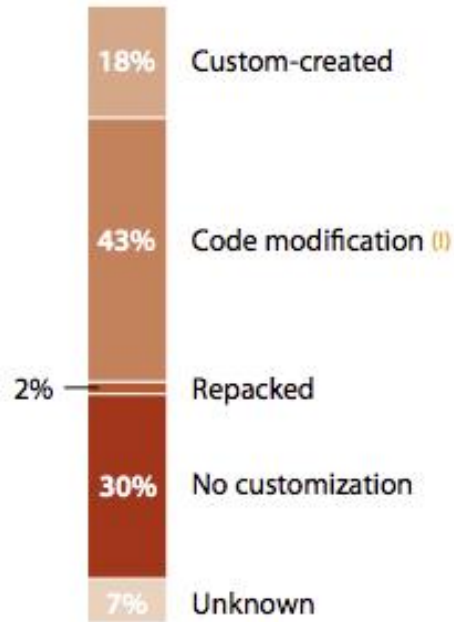
Actions: More on Malware (49% of breaches)

Figure 21. Malware customization over time by percent of breaches within Malware*



* Verizon caseload only

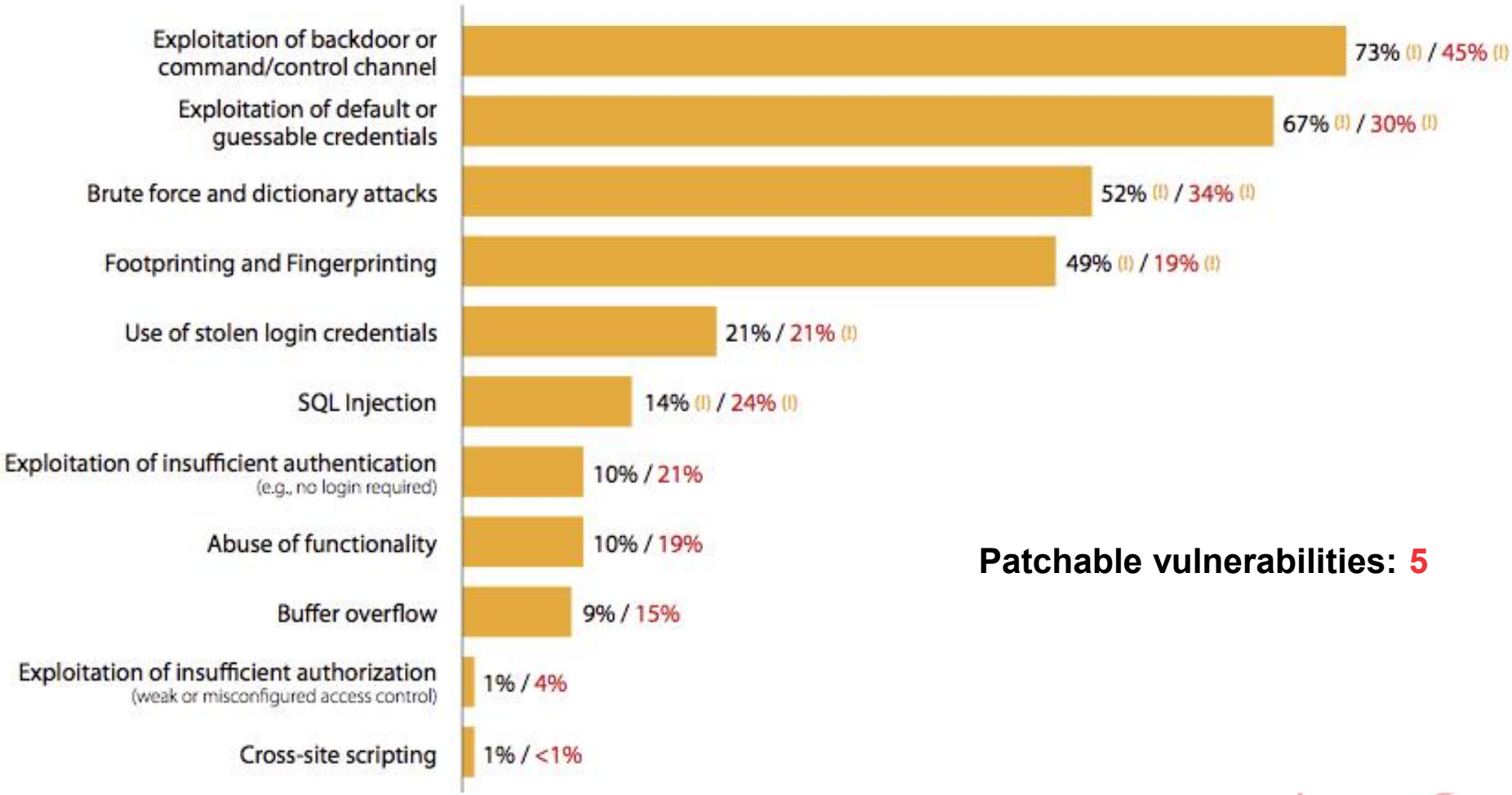
Level of malware customization by percent of breaches within Malware*



* Verizon caseload only

Hacking – What was the Type Used?

Figure 22. Types of hacking by percent of breaches within Hacking and percent of records



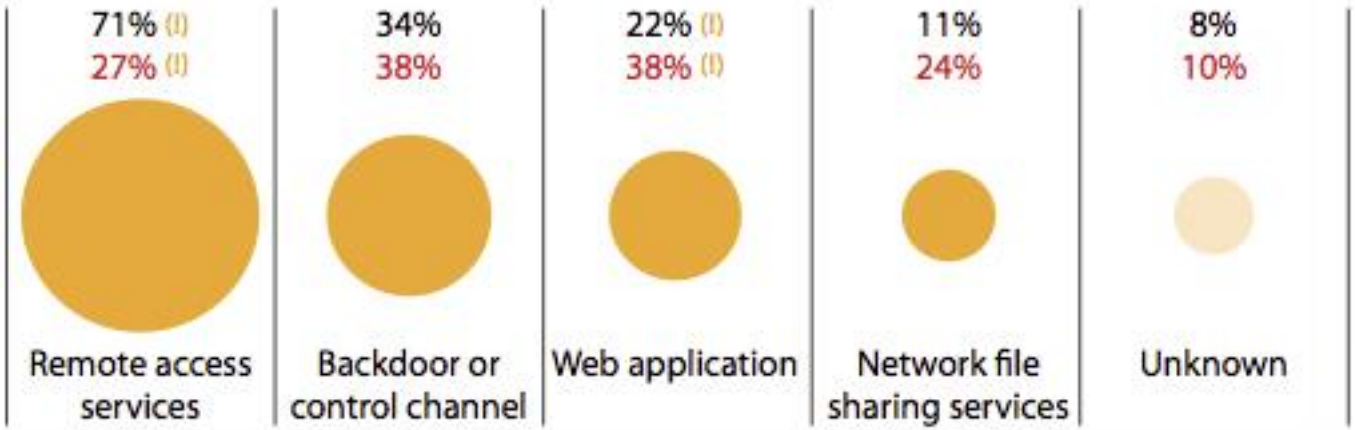
(Truncated)

Patchable vulnerabilities: 5

verizon

Actions: More on Hacking (50% of breaches)

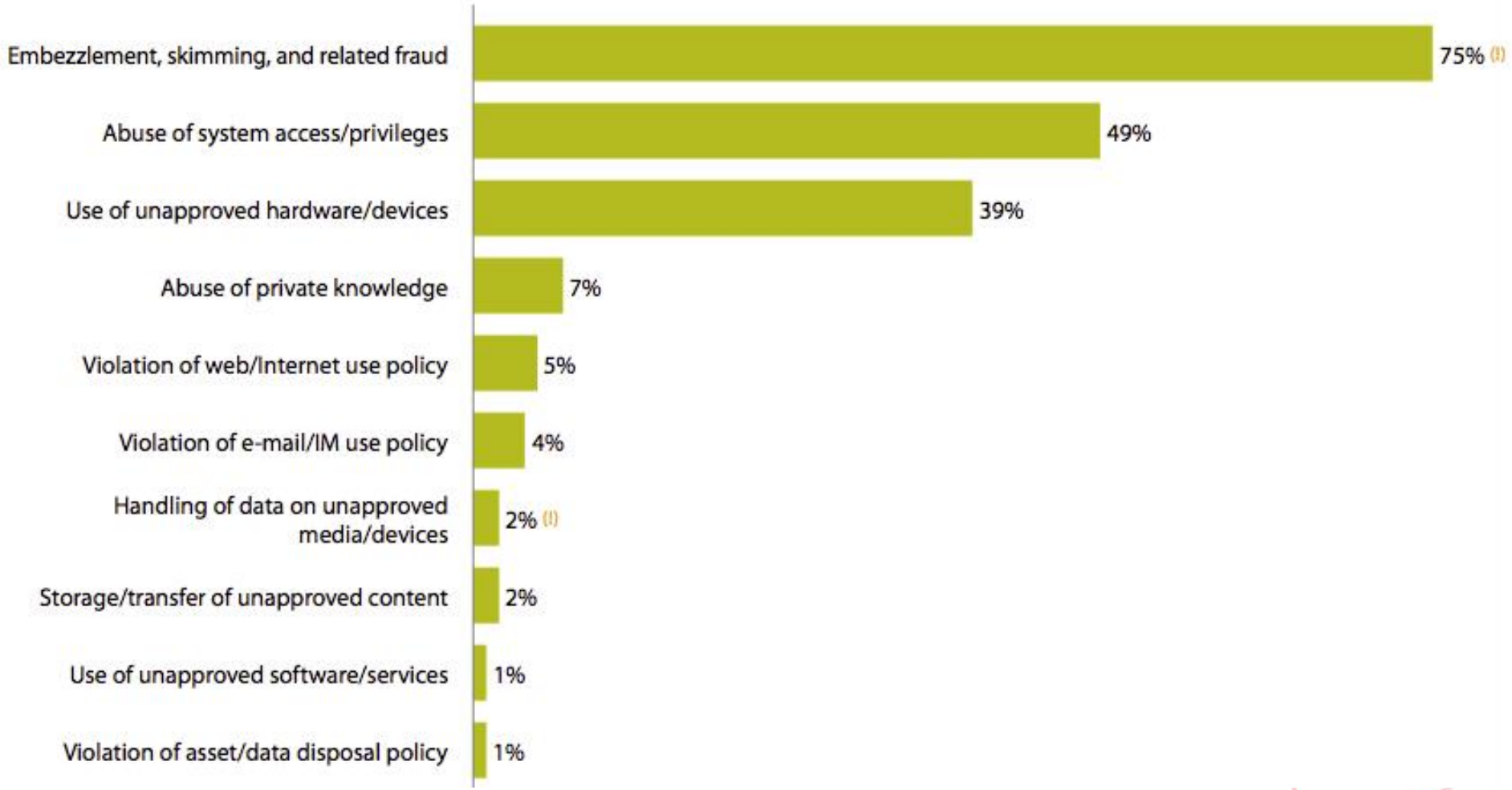
Figure 23. Attack pathways by percent of breaches within Hacking and percent of records



Local remote screen sharing (e.g., RDP, PCAnywhere)	64%	24%
Online session screen sharing (e.g., Go2Assist, LogMeIn, NetViewer)	5%	13%
Remote Shell (e.g., ssh, telnet, rsh)	2%	1%
Web-based terminal services (e.g., Citrix, MS Terminal Services)	2%	12%
VPN	1%	<1%

Actions: More on Misuse (17% of breaches)

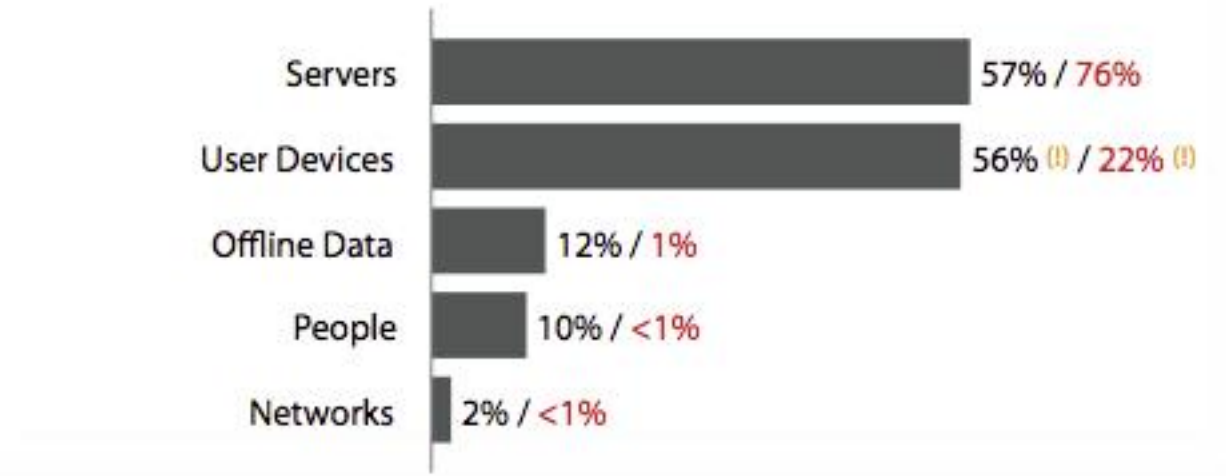
Figure 26. Types of misuse by percent of breaches within Misuse



verizon

Which Assets were Affected?

Figure 28. Categories of affected assets by percent of breaches and percent of records



verizon

Which Assets were Affected?

Table 12. Types of compromised assets by percent of breaches and percent of records*

Type	Category	% of Breaches	% of Records
POS server (store controller)	Servers	36% (I)	28% (I)
POS terminal	User Devices	21% (I)	13% (I)
Pay at the pump terminal	User Devices	18% (I)	<1%
Database server	Servers	14%	15% (I)
Web app/server	Servers	9%	24%
Regular employee/end-user	People	8%	0%
Automated teller machine (ATM)	User Devices	8%	9%
Desktop/workstation	User Devices	8%	0%
Payment card (credit, debit, etc)	Offline Data	7%	1%
File server	Servers	4%	<1%
Documents	Offline Data	4%	<1%
Finance/accounting staff	People	4%	0%
Human resources staff	People	3%	0%

What Security Attributes were Affected?

Table 13. Security attributes affected by percent of breaches

Attributes affected	Definition	Breaches
Confidentiality	Limited access, observation, and disclosure	100%
Possession	Exclusive (or intended) possession and control (and ability to prove it)	0%
Integrity	Complete and unchanged from original state	90%
Authenticity	Validity, conformance, and genuineness	5%
Availability	Present and ready for use when needed	1%
Utility	Usefulness or fitness for a purpose	0%

verizon

How Much Data was Stolen?

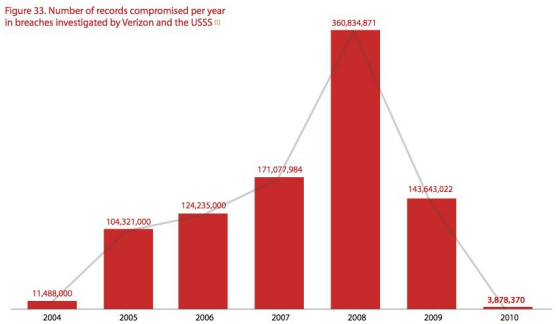


Table 14. Descriptive statistics on records compromised, 2004-2010

	2004-2009	2010	All-Time ('04-'10)
Total records	915,599,877	3,878,370	919,478,247
Mean	1,963,230	6,687	878,850
Median	20,000	221	775
Standard deviation	13,141,644	32,854	8,868,990
Percentiles			
10th	12	8	10
25th	360	10	40
50th	20,000	221	775
75th	200,000	2,401	19,221
90th	1,200,001	4,826	250,000
99th	60,720,000	157,695	10,000,001

What types of data were stolen?

Table 15. Compromised data types by number and percent of breaches and percent of records

	Number of incidents	Percent of incidents	Percent of records
Payment card numbers/data	593	78%	96%
Authentication credentials (usernames, pwds, etc)	339	45%	3%
Personal Information (Name, SS#, Addr, etc)	111	15%	1%
Sensitive organizational data (reports, plans, etc)	81	11%	0%
Bank account numbers/data	64	8%	<1%
Intellectual property	41	5%	<1%
System information (config, svcs, sw, etc)	41	5%	unknown
Classified information	20	3%	unknown

verizon

How difficult and targeted were these attacks?

Figure 34. Attack difficulty by percent of breaches and percent of records*

* Verizon caseload only

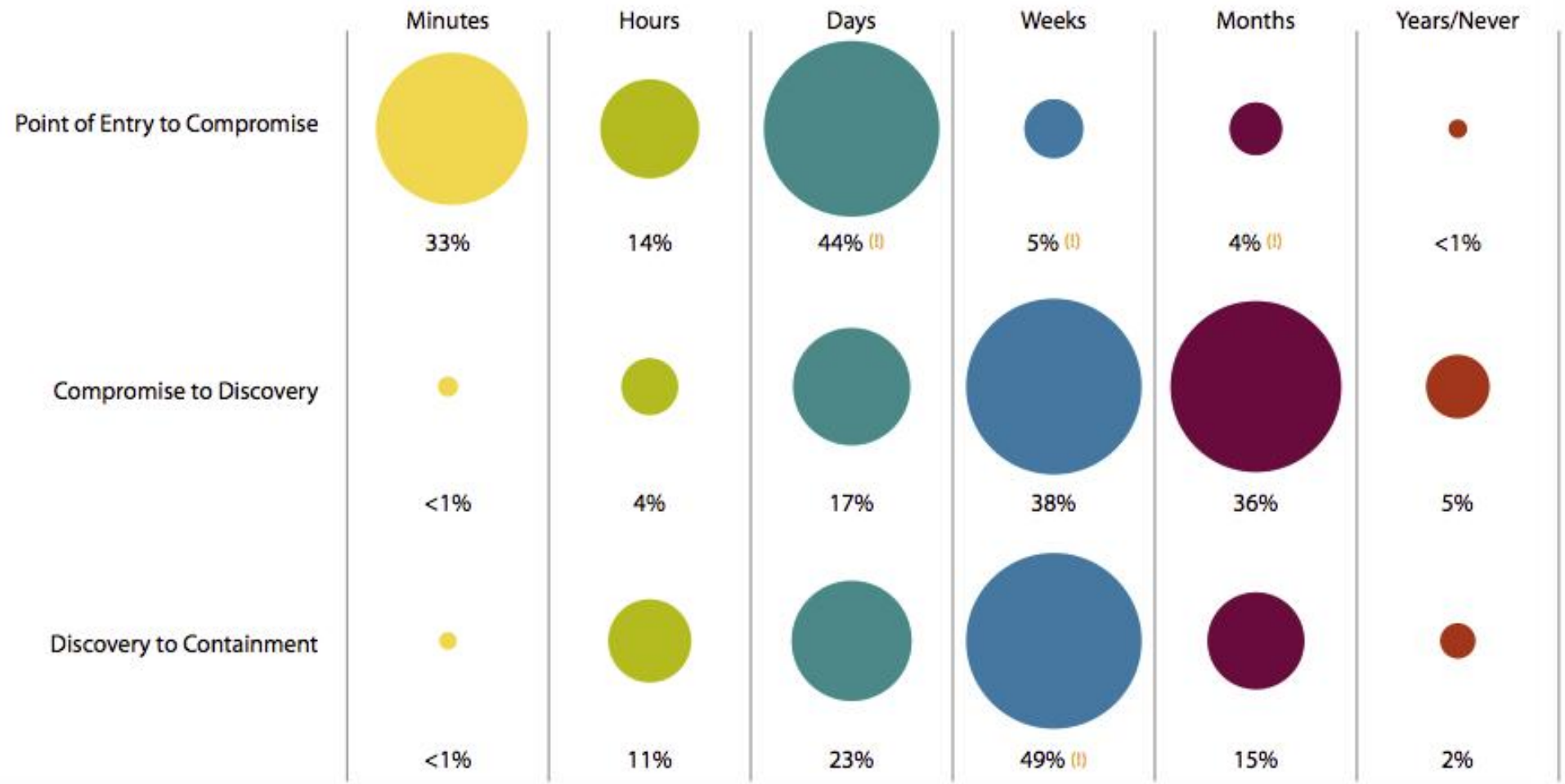
Figure 35. Attack targeting by percent of breaches and percent of records*

* Verizon caseload only

verizon

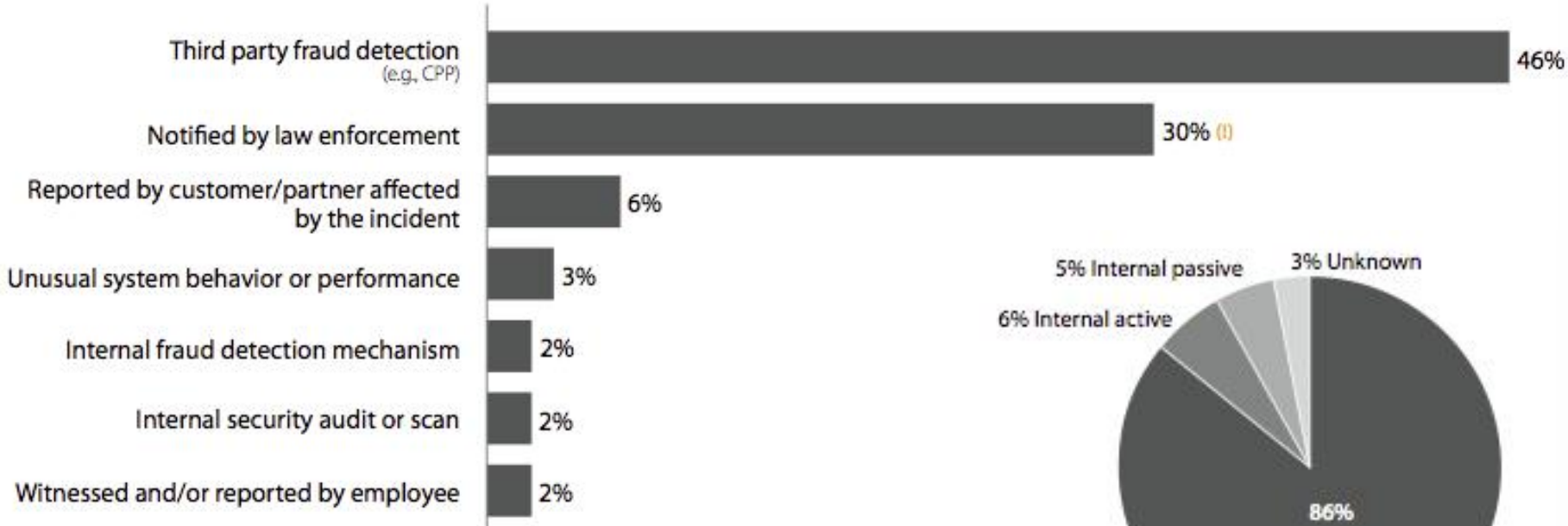
Timespan of events in breach scenarios

Figure 37. Timespan of events by percent of breaches

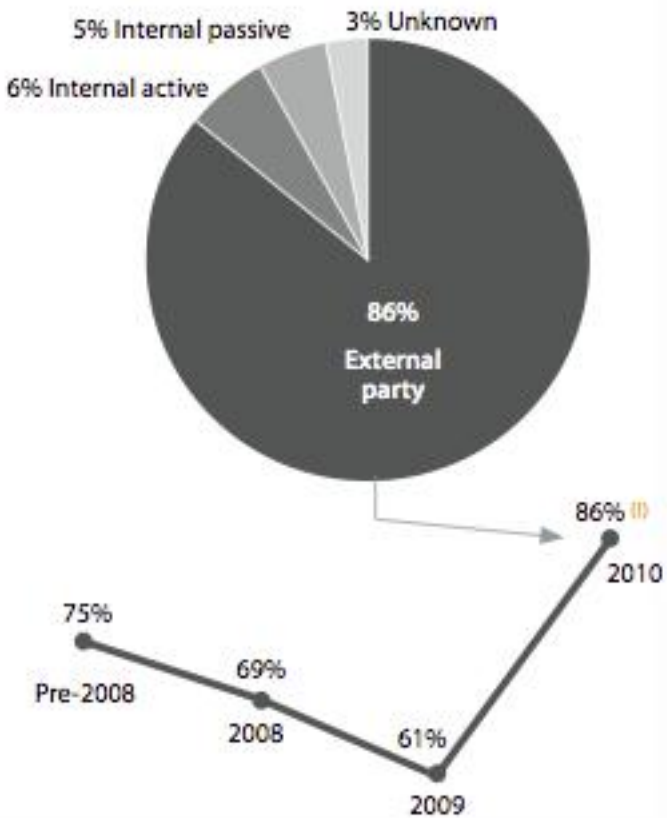


How did the victim discover the breach?

Figure 40. Breach discovery methods by percent of breaches



Anti-virus (1%)
IDS (<1%)
Log review (0%)



DBIR: www.verizonbusiness.com/databreach
VERIS: https://verisframework.wiki.zoho.com/
Blog: securityblog.verizonbusiness.com
Email: dbir@verizonbusiness.com

verizon

Figure 6. A⁴ Grid depicting the frequency of VERIS Threat Events across 2010 caseload