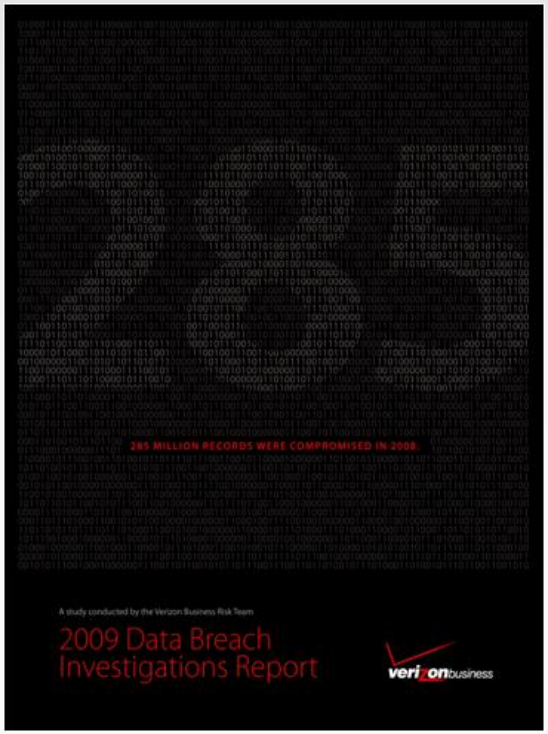
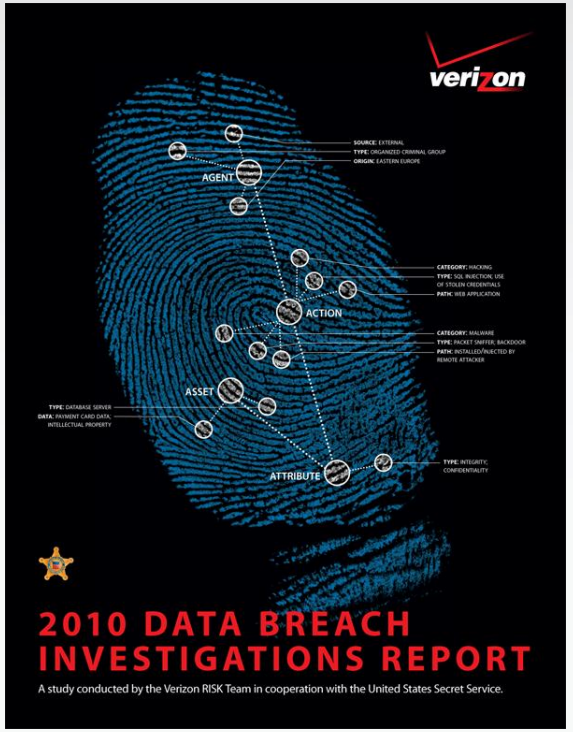
2010 Data Breach Investigations Report





Why Publish These Reports?

"…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 U.S. president on securing the US' 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

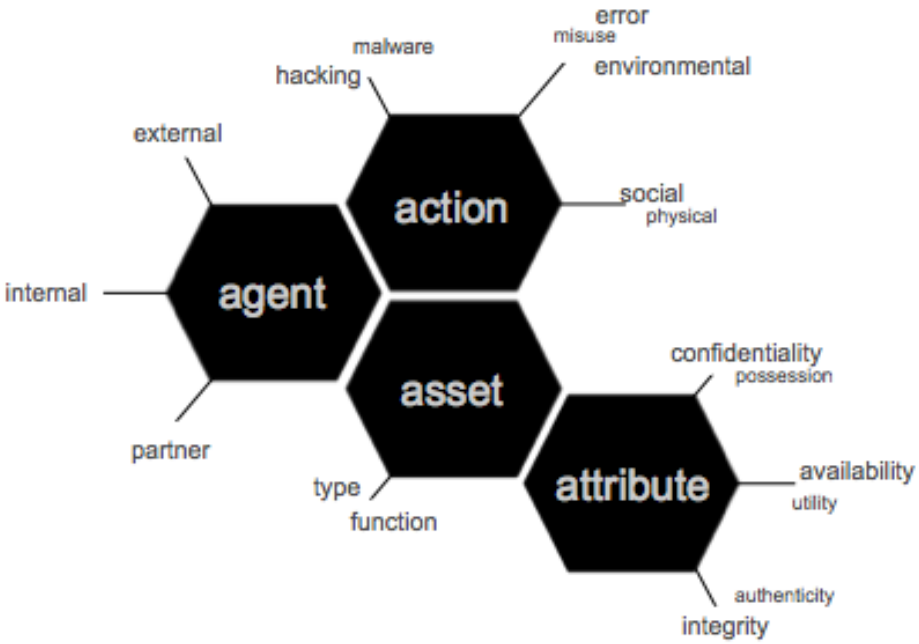
- VERIS framework used to collect data after investigation
- Case data anonymized and aggregated
- RISK Intelligence team provides analytics

Data Sample

- 6 years of forensic investigations (not internal Verizon incidents)
- >900 breaches, 900 million stolen records in combined dataset

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:

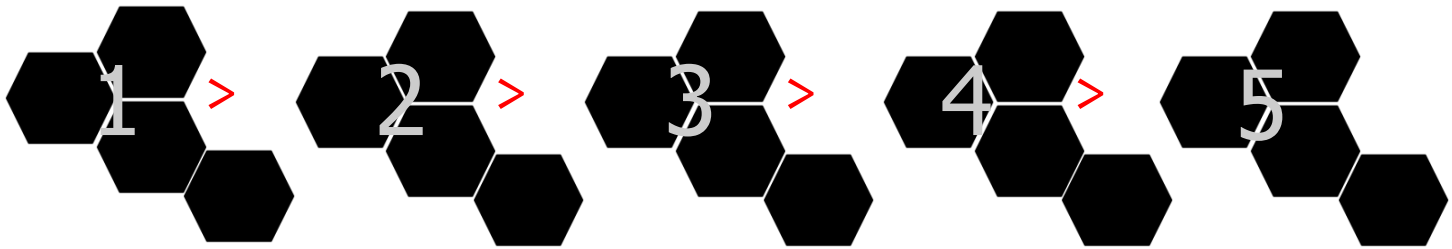
Agent: Whose actions affected the asset

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

Assets & Data

Figure 29. Number of records compromised per year in breaches investigated by Verizon and the United States Secret Service

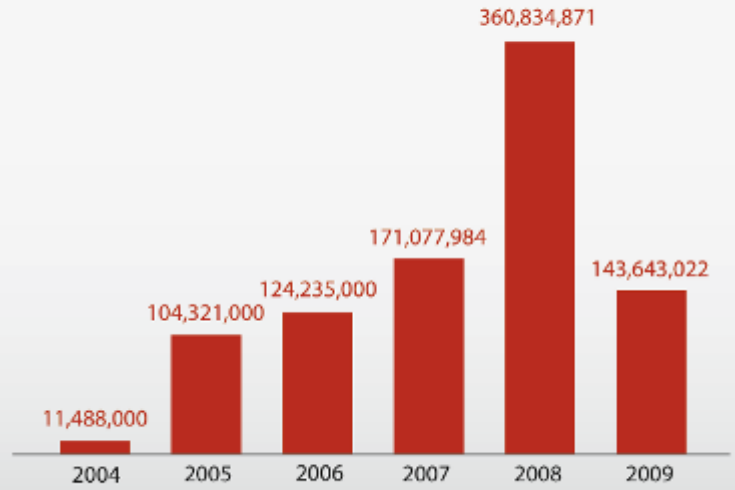


Figure 27. Categories of compromised assets by percent of breaches and percent of records

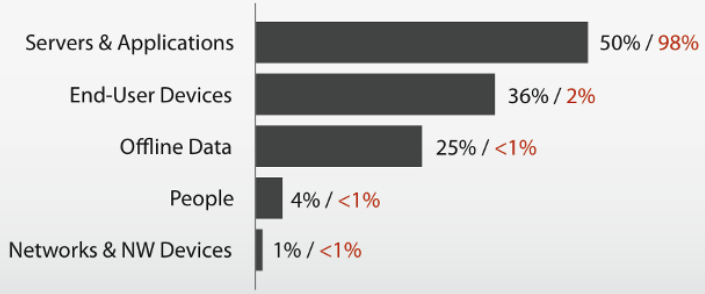
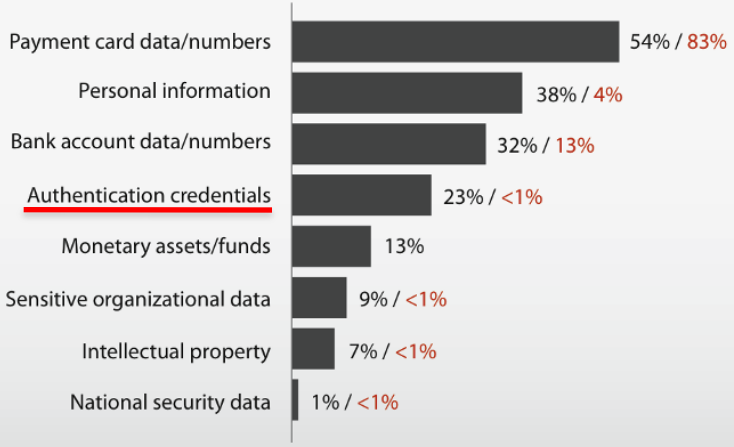
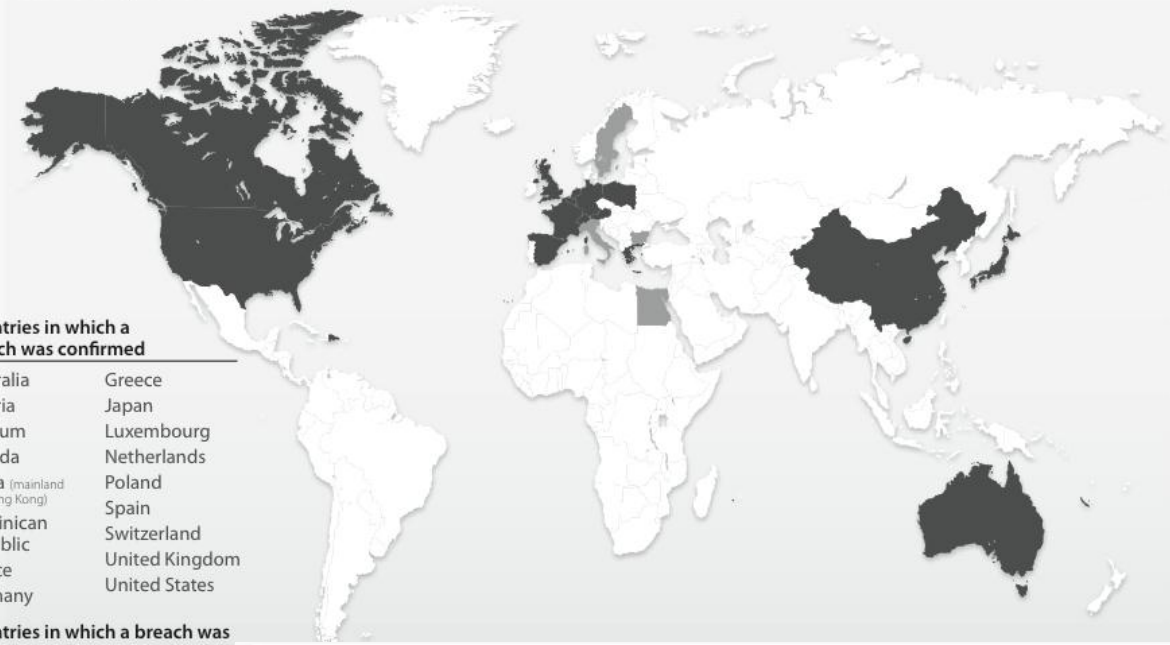


Figure 31. Compromised data types by percent of breaches and percent of records



Demographics

Figure 3. Countries represented



Countries in which a breach was confirmed

Australia
Austria
Belgium
Canada
China (mainland and Hong Kong)
Dominican Republic
France
Germany
Greece
Japan
Luxembourg
Netherlands
Poland
Spain
Switzerland
United Kingdom
United States

Countries in which a breach was investigated but not confirmed

Bulgaria
Egypt
Italy
Singapore
Sweden

Figure 2. Compromised records by industry group

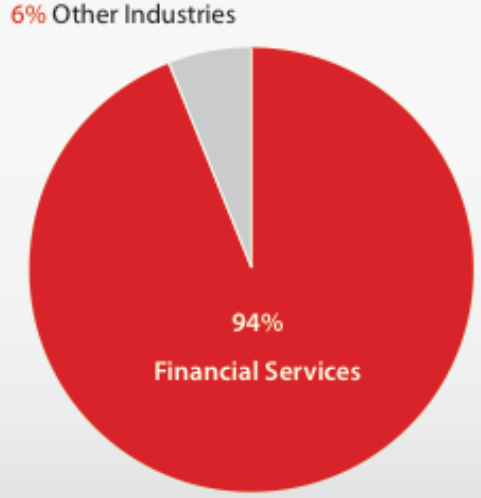
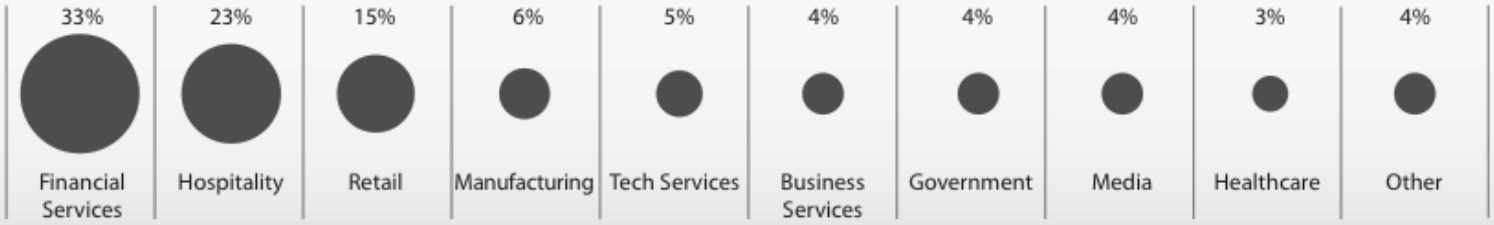


Figure 1. Industry groups represented by percent of breaches



Threat Agents

Figure 5. Threat agents (inclusive) by percent of breaches

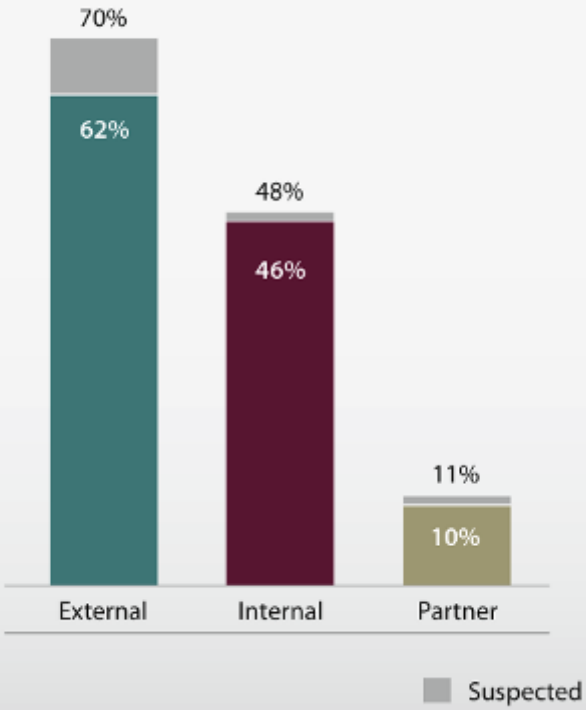


Figure 7. Threat agents (exclusive) by percent of breaches

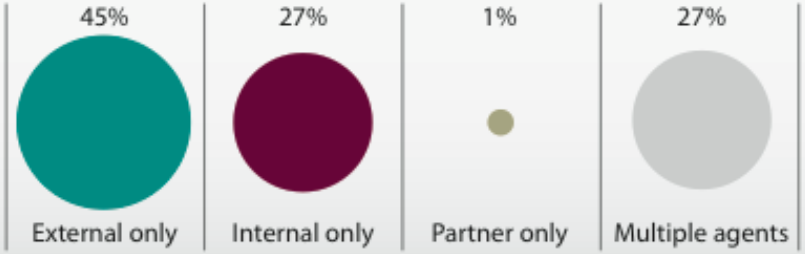


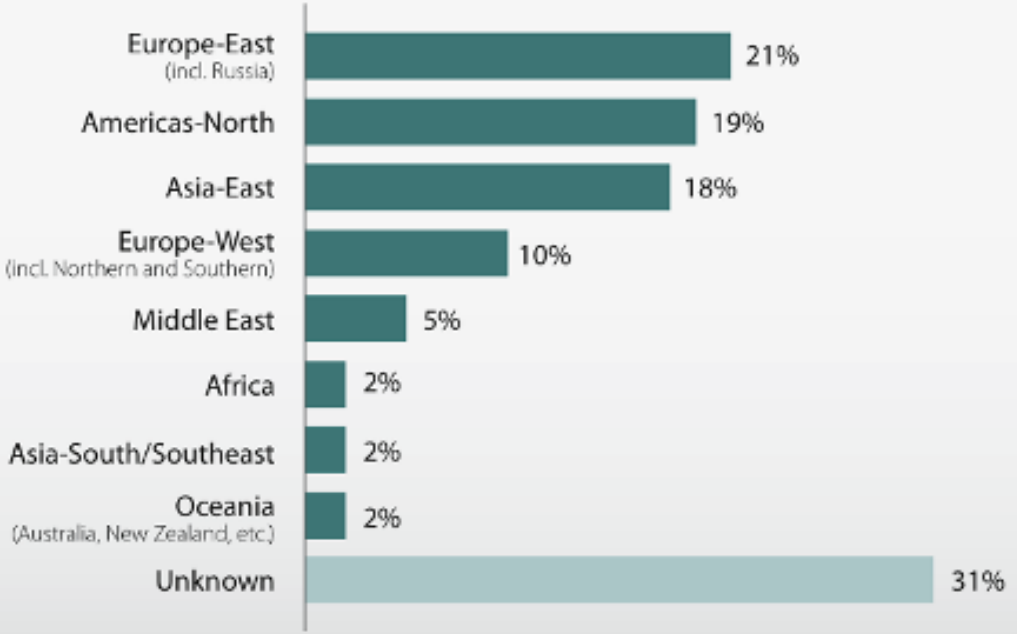
Figure 8. Compromised records by threat agent, 2009

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%

Figure 11. Origin of external agents by percent of breaches within External



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%

Figure 11. Origin of external agents by percent of breaches within External

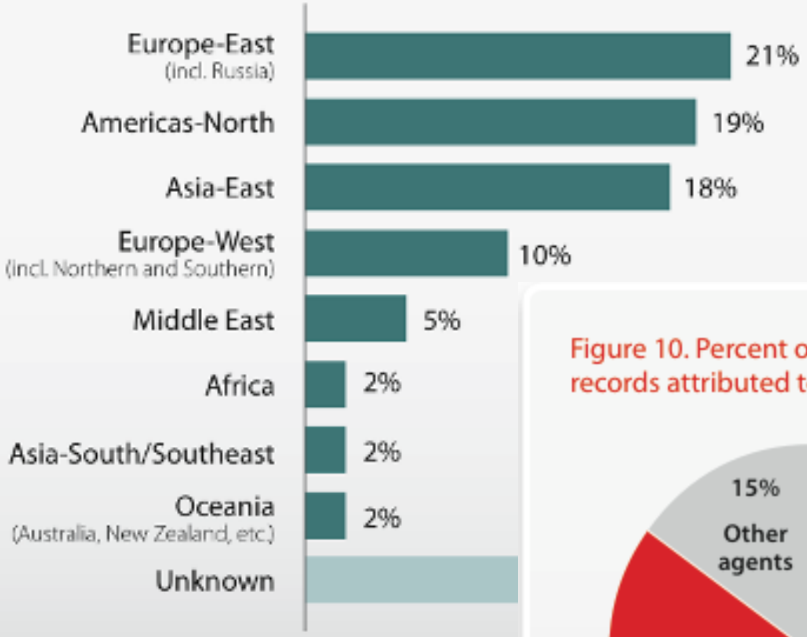
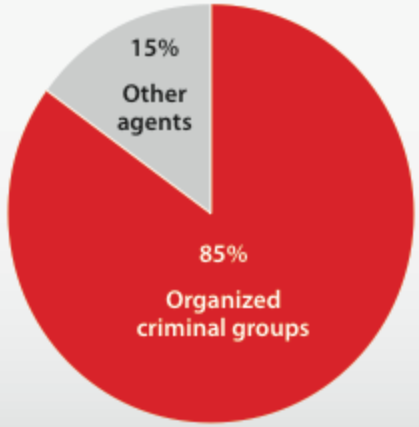


Figure 10. Percent of compromised records attributed to organized crime



Internal Agents

Figure 12. Role of internal agents by percent of breaches within Internal

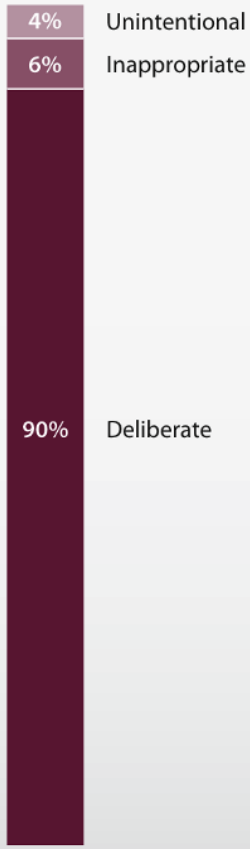


Table 2. Types of internal agents by percent of breaches within Internal

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

Figure 13. Role of partner agents by percent of breaches within Partner

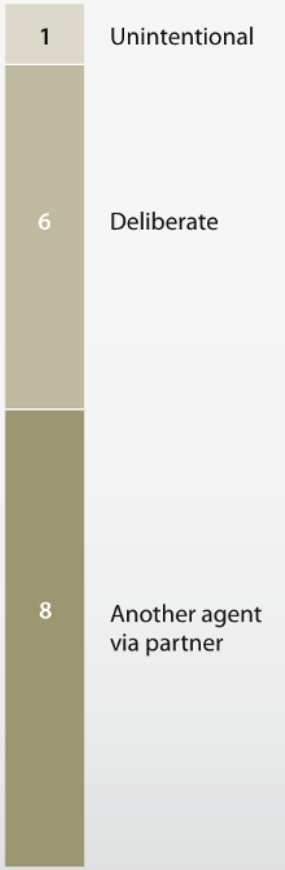
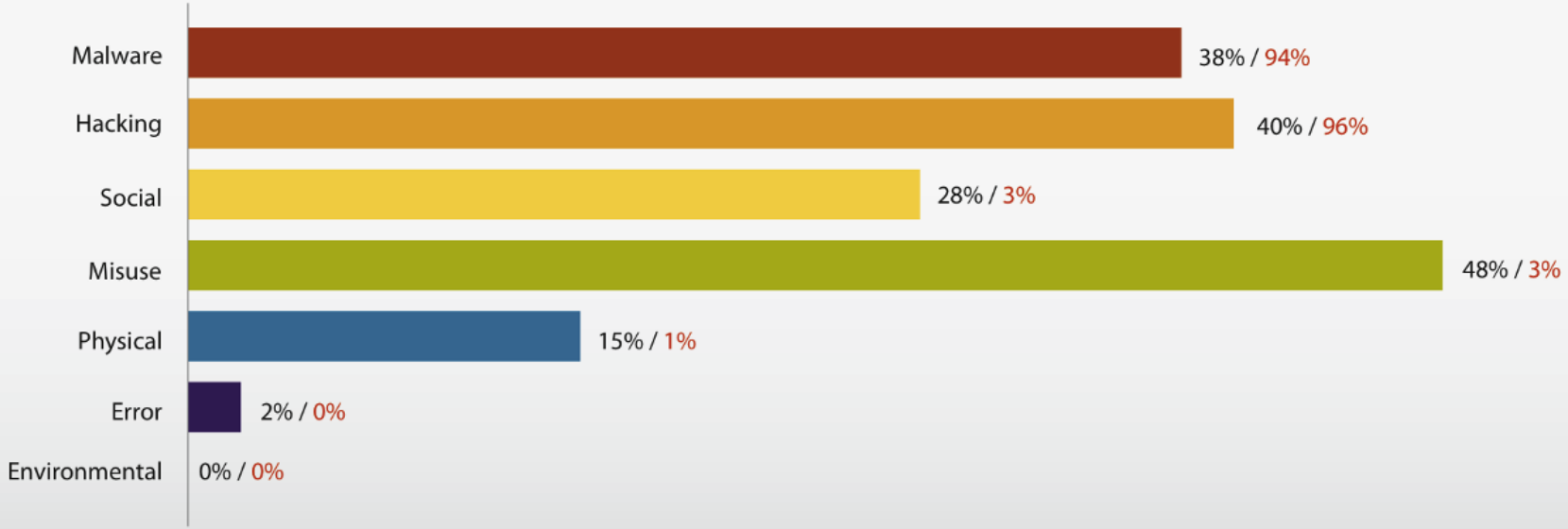


Table 3. Types of partner agents by percent of breaches within Partner

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

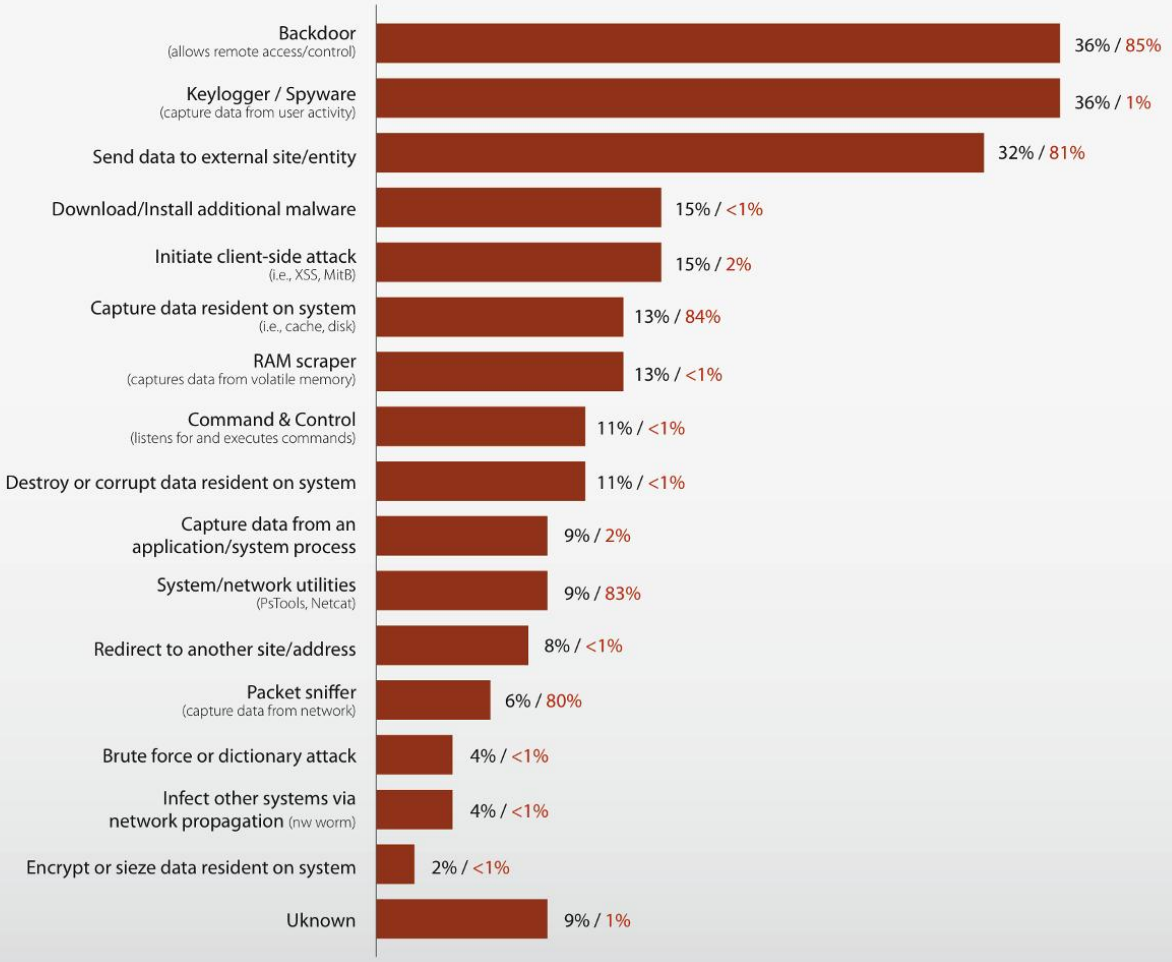
Threat Actions

Figure 14. Threat action categories by percent of breaches and records



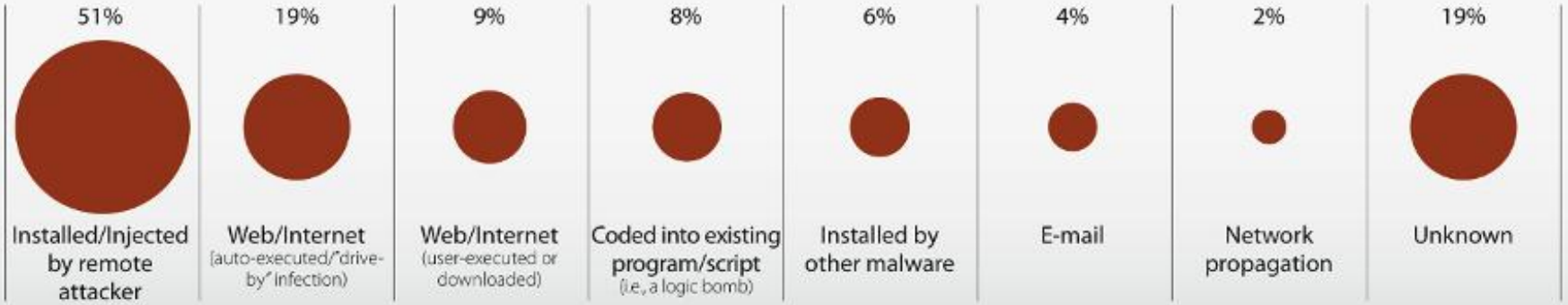
Malware
Functionality

Figure 19. Malware functionality by percent of breaches within Malware and percent of records

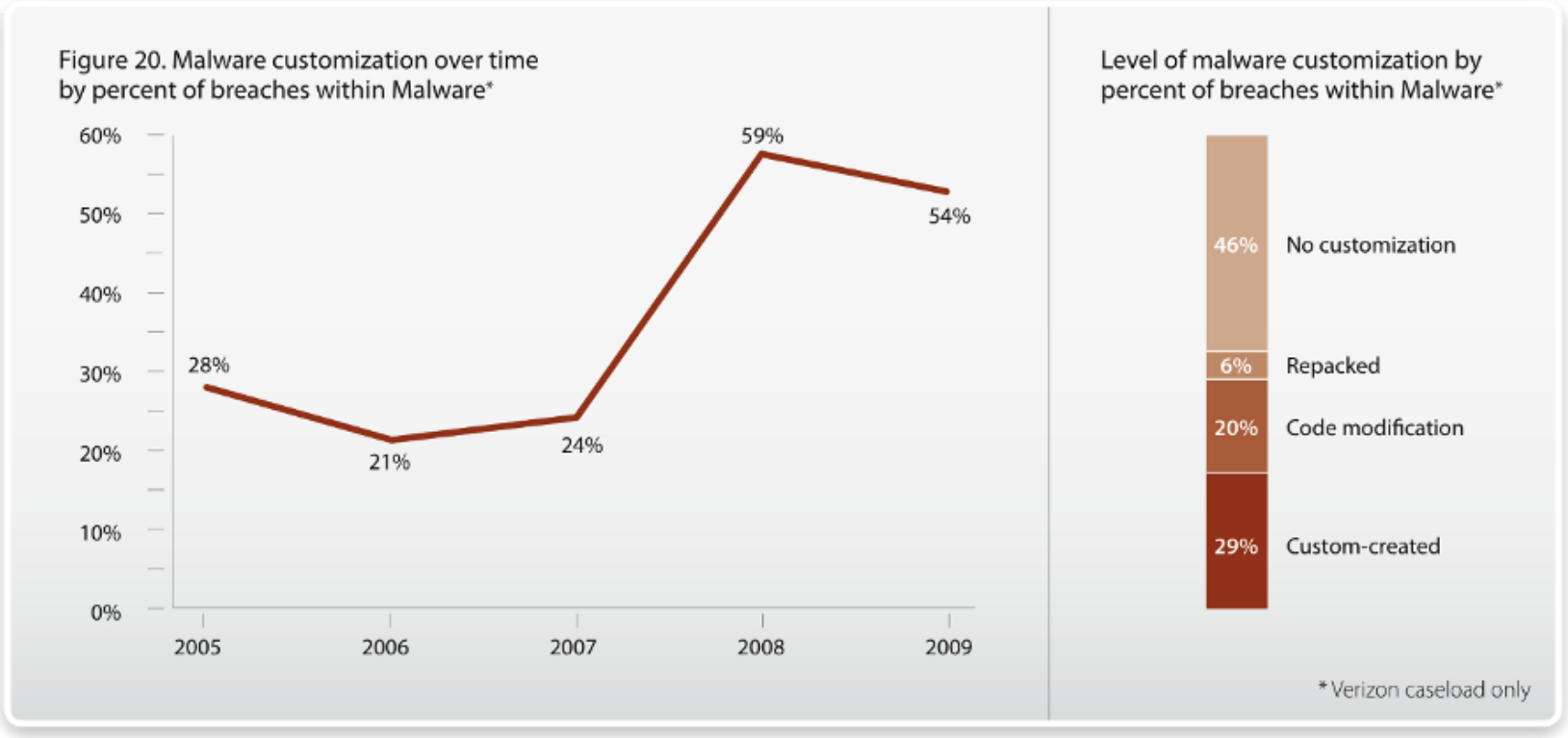


Malware
Infection Vector

Figure 18. Malware infection vectors by percent of breaches within Malware



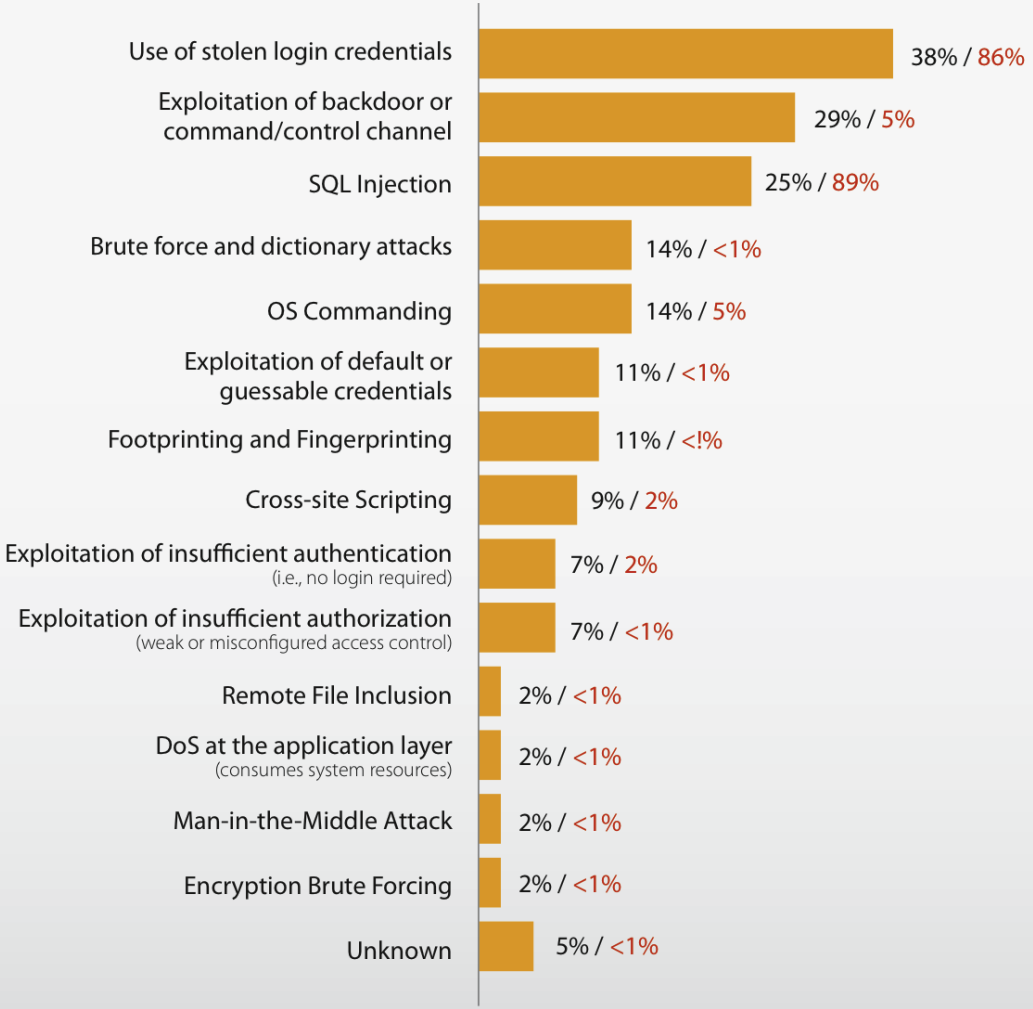
Malware
Customization



An incredible 97% of the 140+ million records were compromised through customized malware across the Verizon-USSS caseload.

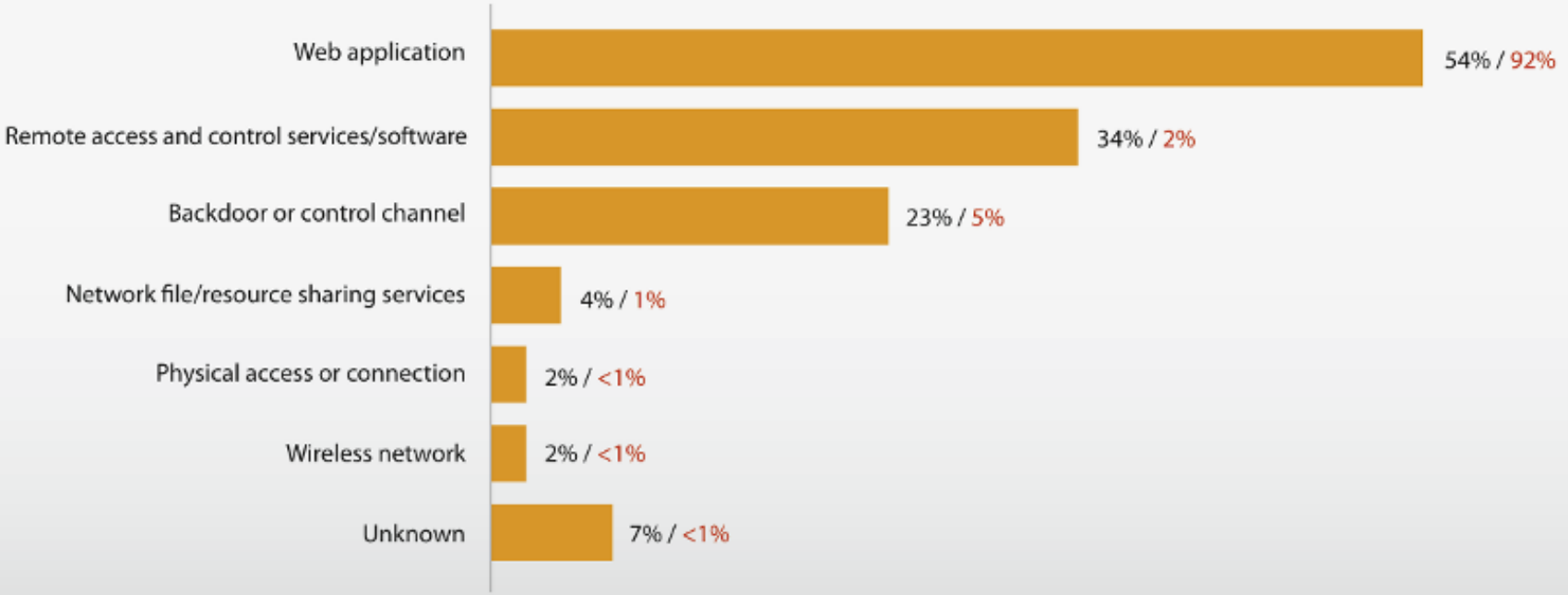
Hacking
Types

Figure 21. Types of hacking by percent of breaches within Hacking and percent of records



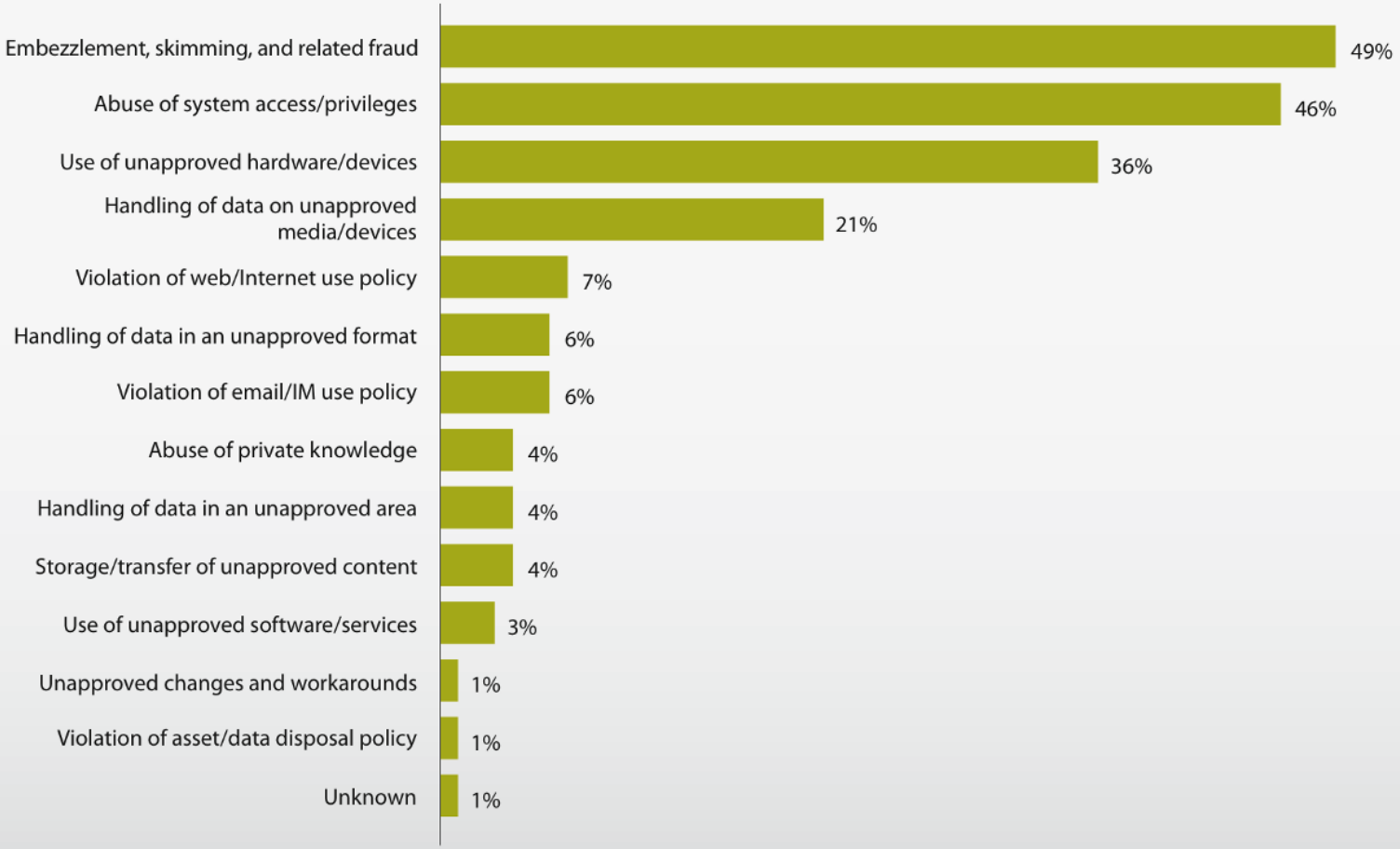
Hacking
Pathways

Figure 22. Attack pathways by percent of breaches within Hacking and percent of records



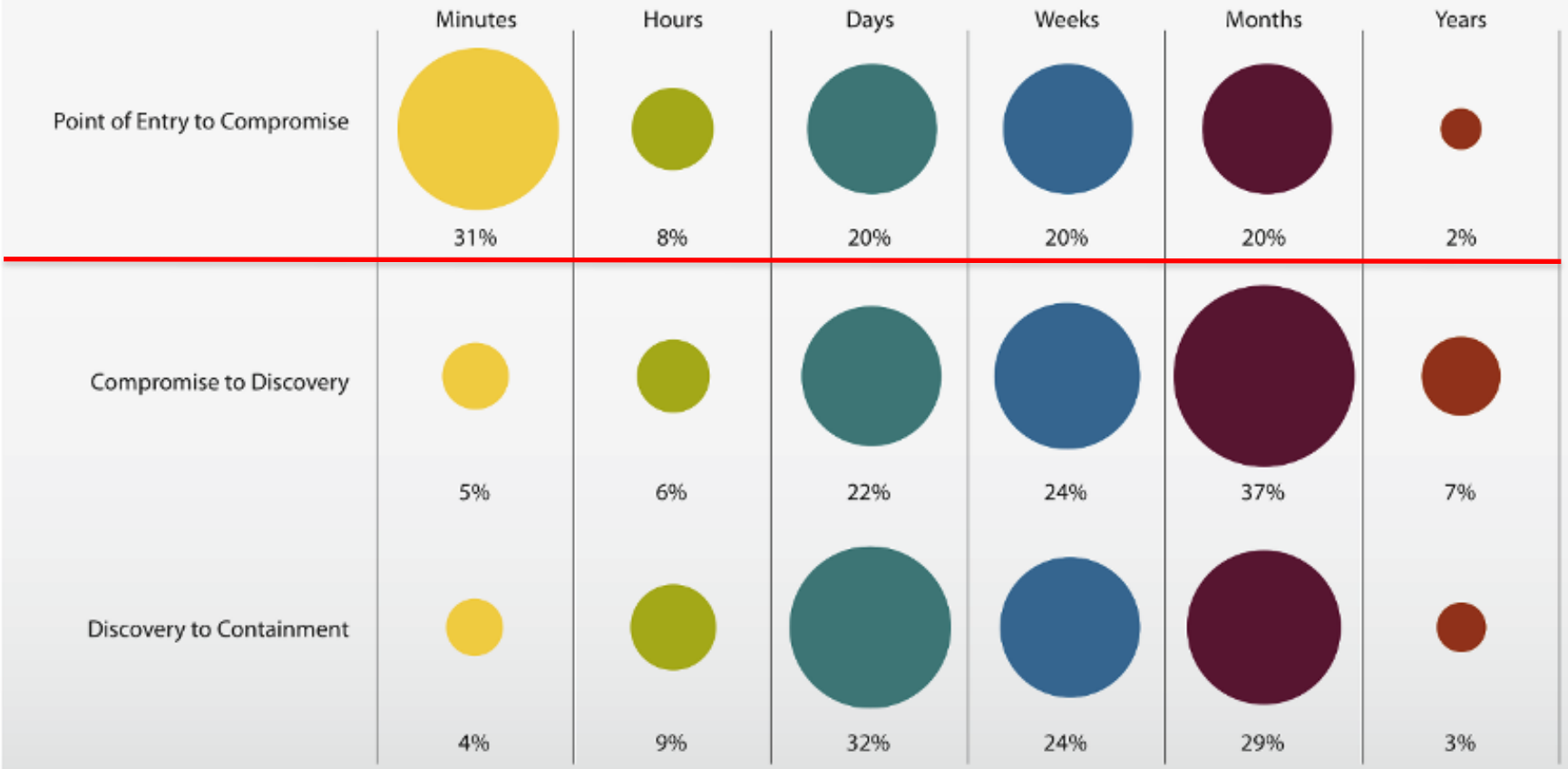
Misuse
Types

Figure 25. Types of misuse by percent of breaches within Misuse



Timeline of Events

Figure 35. Timespan of events by percent of breaches



Discovery Methods

Figure 38. Breach discovery methods by percent of breaches

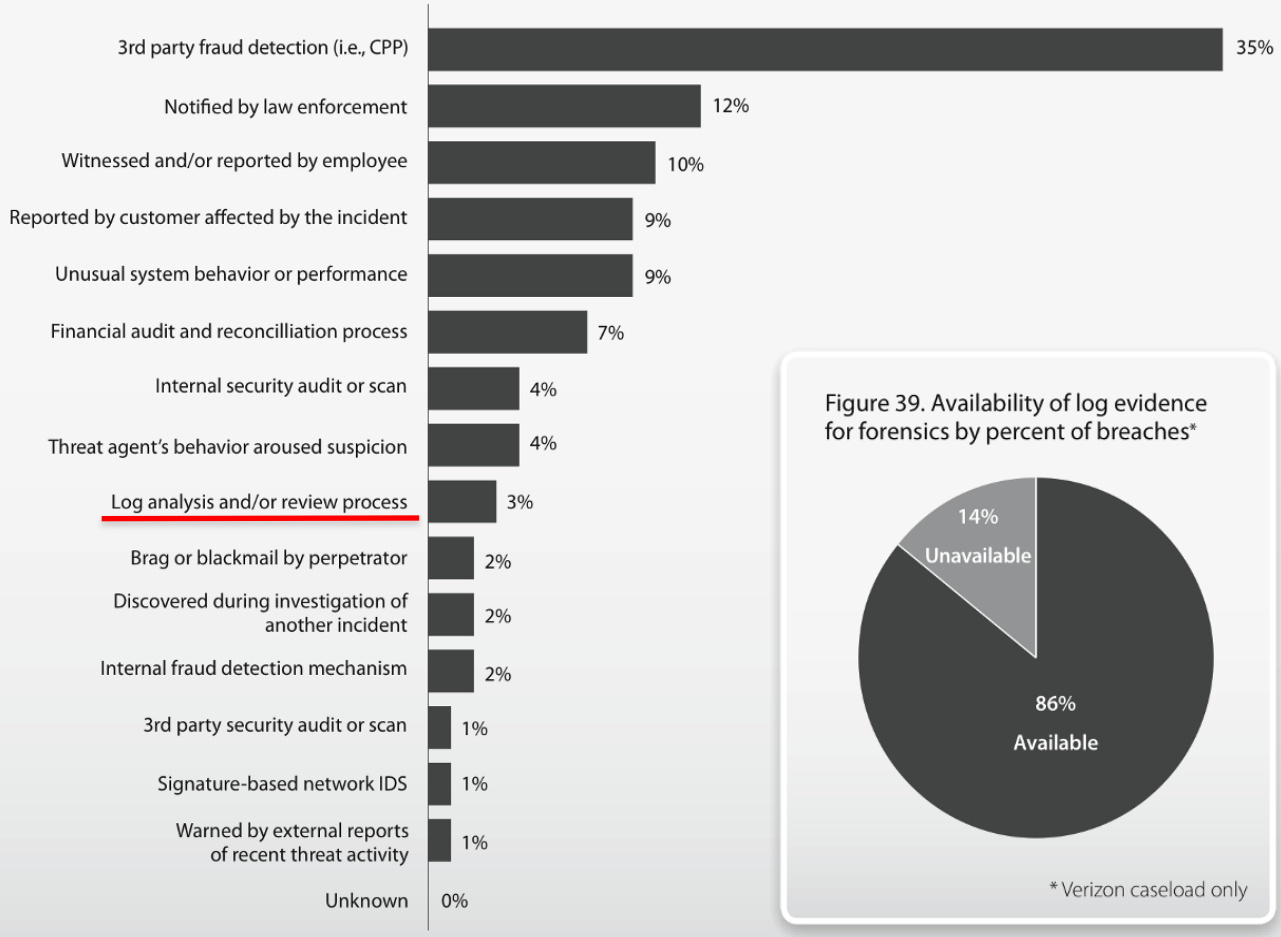
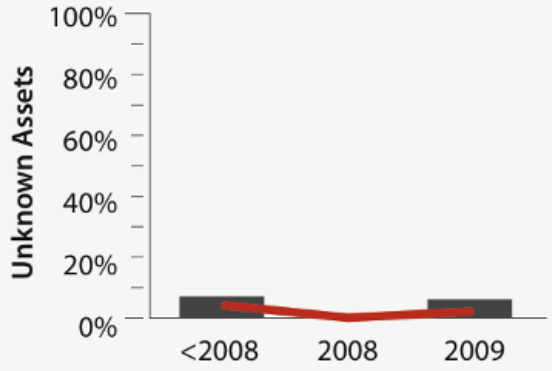


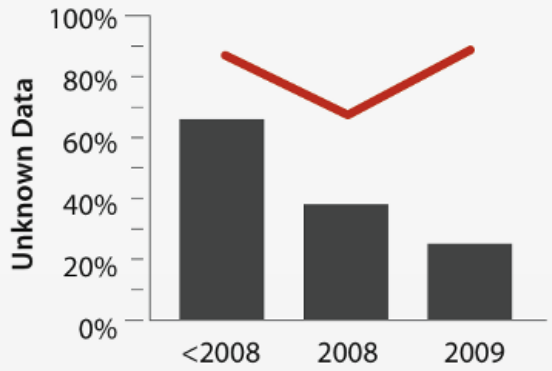
Figure 39. Availability of log evidence for forensics by percent of breaches*

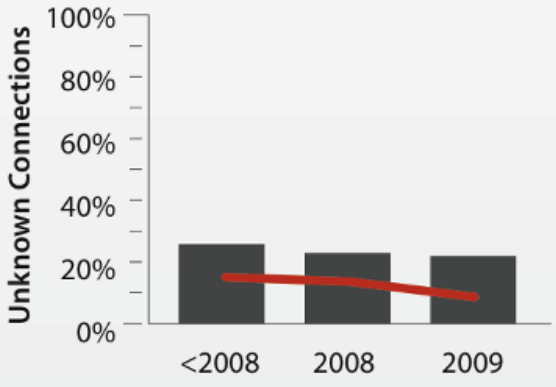
* Verizon caseload only

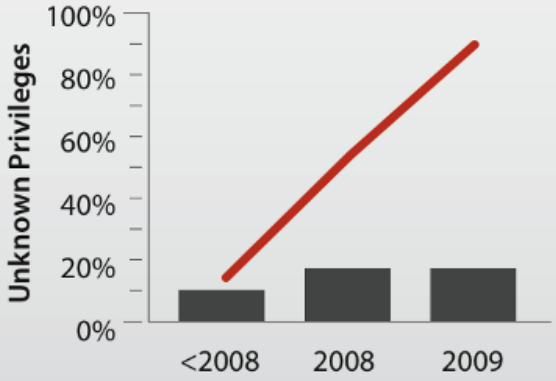
Unknown Unknows

Figure 34. Unknown Unknowns by percent of breaches and percent of records







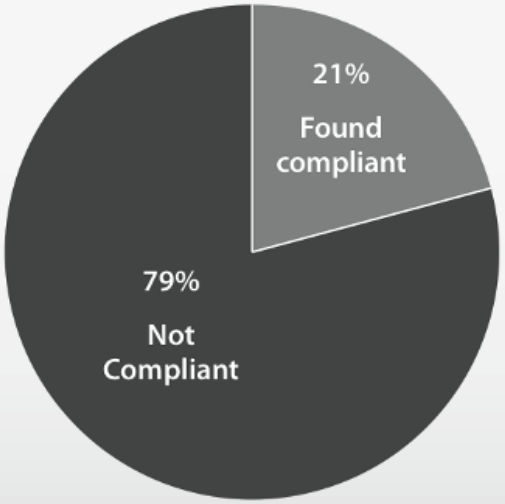


Assets & Data

Table 9. 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%
op and maintain secure systems and applications	5%	21%
Access Control Measures		
t access to data by business need-to-know	24%	30%
a unique ID to each person with computer access	19%	35%
t physical access to cardholder data	43%	58%
and Test Networks		
and monitor all access to network resources and cardholder data	5%	30%
larly test security systems and processes	14%	25%
ation Security Policy		
ain a policy that addresses information security	14%	40%

Figure 41. PCI DSS compliance status based on last assessment*



* Verizon caseload only

Assets & Data

Table 9. 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%

Figure 41. PCI DSS compliance stat
based on last assessment*

* Verizon caseload

Conclusions & Recommendations

Figure 43. Categorization of recommended mitigation measures by percent of breaches*

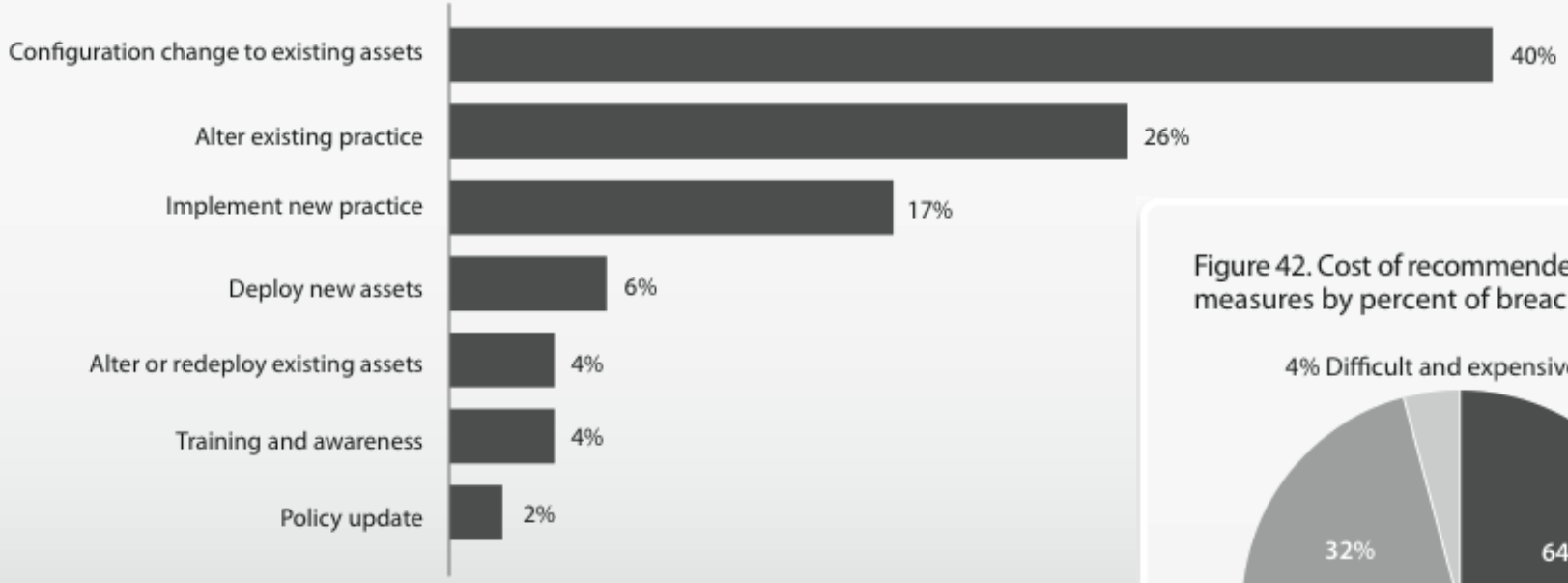
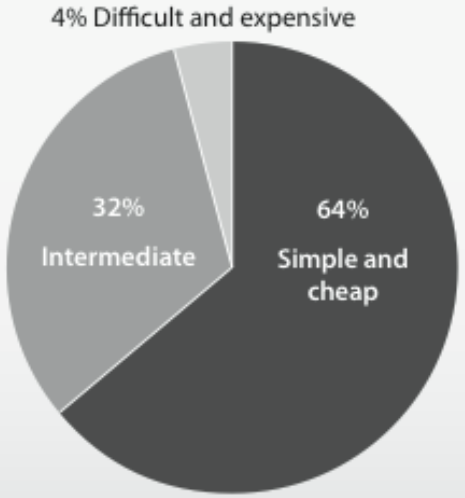


Figure 42. Cost of recommended preventive measures by percent of breaches*



* Verizon caseload only

Conclusions & 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

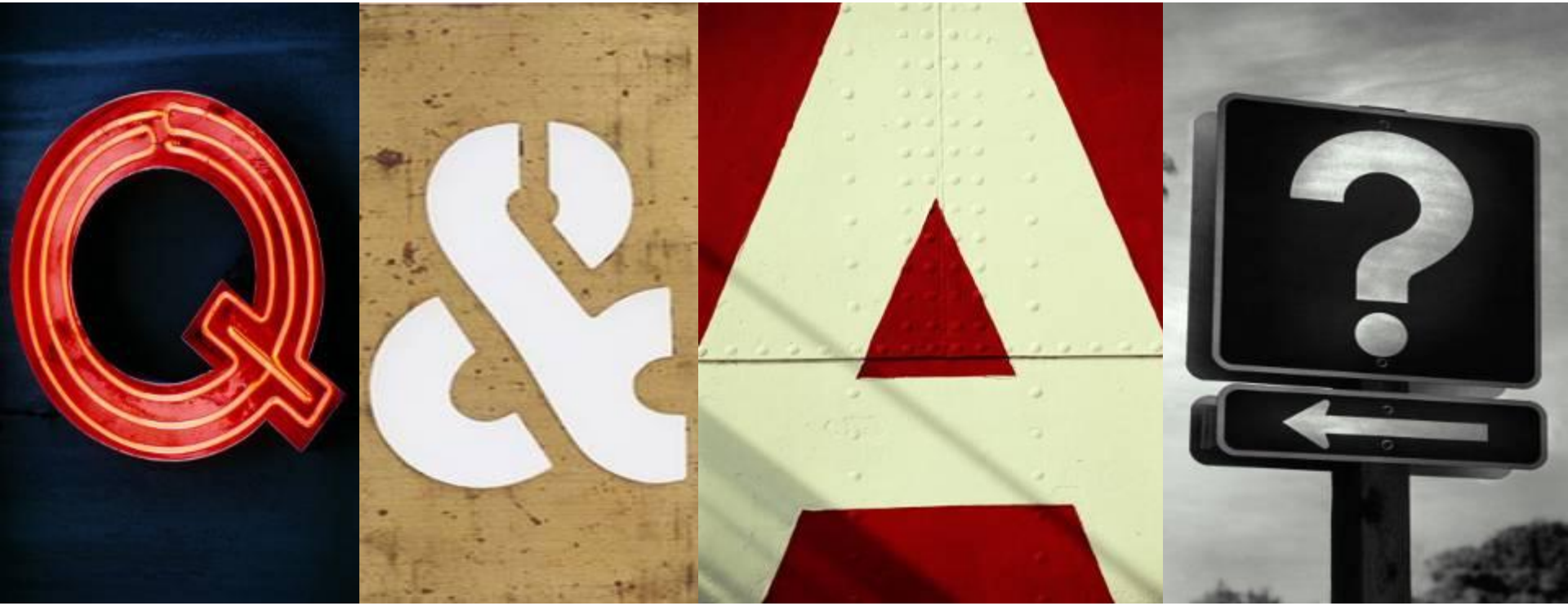
Keep outsiders out; they are increasingly difficult to control once in

Restrict and monitor insiders; disable access when they leave

In monitoring events: lookout for haystacks – not needles

Plan, prepare, train, and test for a timely and effective response

verizon



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

verizon