

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.

verizon

POLITIE
Korps landelijke politiediensten

Background: The VERIS framework

- 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/>

verizon

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>



2011 DBIR Contributors



Verizon



United States
Secret Service



Korps landelijke politiediensten
Dutch National High
Tech Crime Unit



Demographics

Figure 3. Industry groups represented by percent of breaches

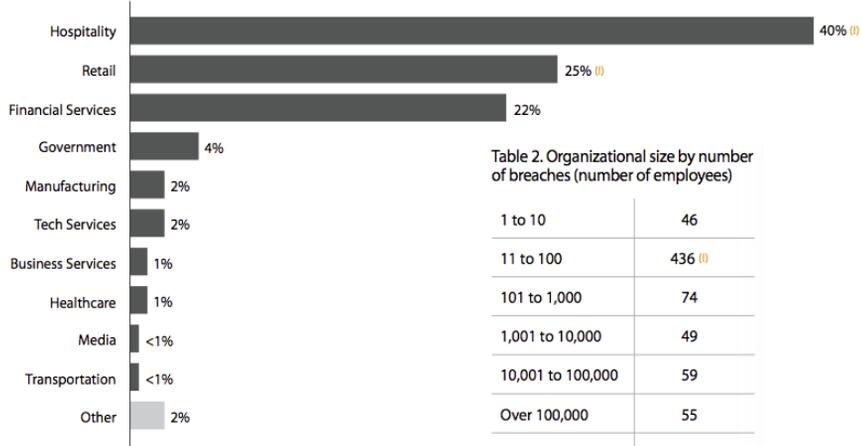


Table 2. Organizational size by number of breaches (number of employees)

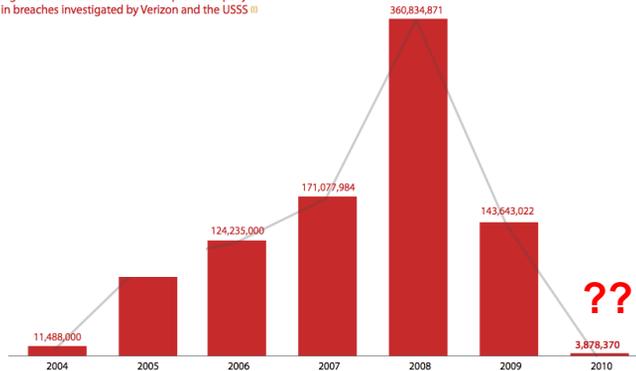
1 to 10	46
11 to 100	436
101 to 1,000	74
1,001 to 10,000	49
10,001 to 100,000	59
Over 100,000	55
Unknown	40



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**

Figure 33. Number of records compromised per year in breaches investigated by Verizon and the USSS



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



DBIR Executive Summary Facts and Figures

Who is behind data breaches?

92% stemmed from external agents (+22%)

17% implicated insiders (-31%)

<1% resulted from business partners (-10%)

9% involved multiple parties (-18%)



DBIR Executive Summary Facts and Figures

17% implicated insiders (-31%)
<1% resulted from business partners (-10%)

- **Perceived “drop” in insider activity**
 - 17% of 761 > 48% of 141
 - Decrease from a percentage is attributable to the explosion in the industrialized attack methods
- **Partners, nothing to worry about?**
 - Above reflects only when the Partner was the causal agent.
 - Partners contributed to conditional events that allowed attacks to continue in 22 percent of our caseload
 - Default passwords
 - Insecure web applications
 - Stolen partner credentials

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



DBIR Executive Summary Facts and Figures

How do breaches occur?

50% utilized some form of hacking (+10%)

49% incorporated malware (+11%)

29% involved physical attacks (+14%)

17% resulted from privilege misuse (-31%)

11% employed social tactics (-17%)

- Increase in organized ATM and gas pump skimming operations
- Decreases in Misuse and Social (as a percent of total cases) is also attributable to explosion of small, external attacks



Threat Action Category: Error

Table 11. Types of causal and contributory errors by number of breaches

	Causal	Contributory
Disposal error	1	0
Publishing error	1	0
Omission	0	192
Programming error	0	16
Misconfiguration	0	10
General user error	0	1



DBIR Executive Summary Facts and Figures

What commonalities exist?

83% of victims were targets of opportunity (<->)

92% of attacks were not highly difficult (+7%)

76% of all data was compromised from servers (-22%)

86% were discovered by a third party (+25%)

96% of breaches were avoidable through simple or intermediate controls (<->)

89% of victims subject to PCI-DSS had not achieved compliance (+10%)



Conclusions / Recommendations

Achieve essential, then worry about excellent

Access Control

- Change default credentials
- User account review
- Restrict and monitor privileged users

Network Management

- Secure remote access services
- Monitor and filter egress network traffic

Secure Development

- Application testing and code review

Log Management and Analysis

- Enable application and network witness logs and monitor them
- Define "suspicious" and "anomalous" (then look for whatever "it" is)




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

