On real data…
…and data not yet realized

MiniMetricon 3.5

Wade Baker
Alex Hutton
Chris Porter

Agenda

- ~~Preliminary Findings~~ Short overview of our data breach impact study
- Data & Discussion: The 2009 Data Breach Investigations Report
- Whaddaya think: Open DBIR case metrics?

Breach Impact Study

Plans

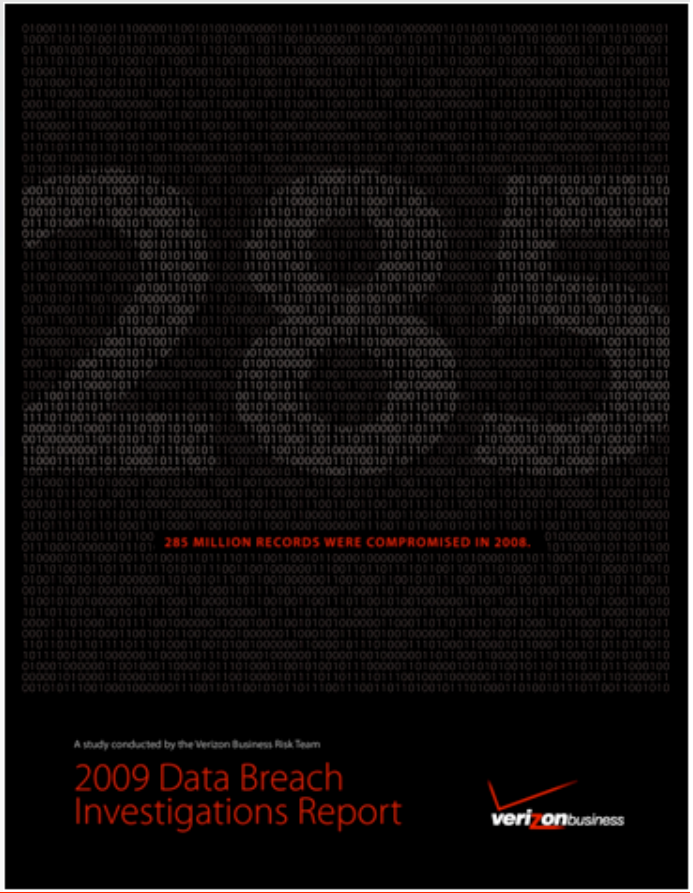
- Investigative Response has two types of clients:
  - Retainer
  - On-demand
- Preliminary study with retainer clients
  - This is what was supposed to be presented here
- Larger study with on-demand clients
  - We have yet to send out invitations
- Methodology not under discussion here
  - Worked with Doug Hubbard, author of “How to Measure Anything”
  - Perhaps more on this at a later date

Questions

- What are the + and – of extending study beyond our IR clients?
- Are the incentives sufficient? Would you participate?

2009 Data Breach Investigations Report

Wade H. Baker
Alex Hutton
C. David Hylender
Christopher Porter
Christopher Novak
Bryan Sartin
Peter Tippett
Andrew Valentine



IR Case Data

All data collected during cases worked by the Verizon Business Investigative Response team during 2008

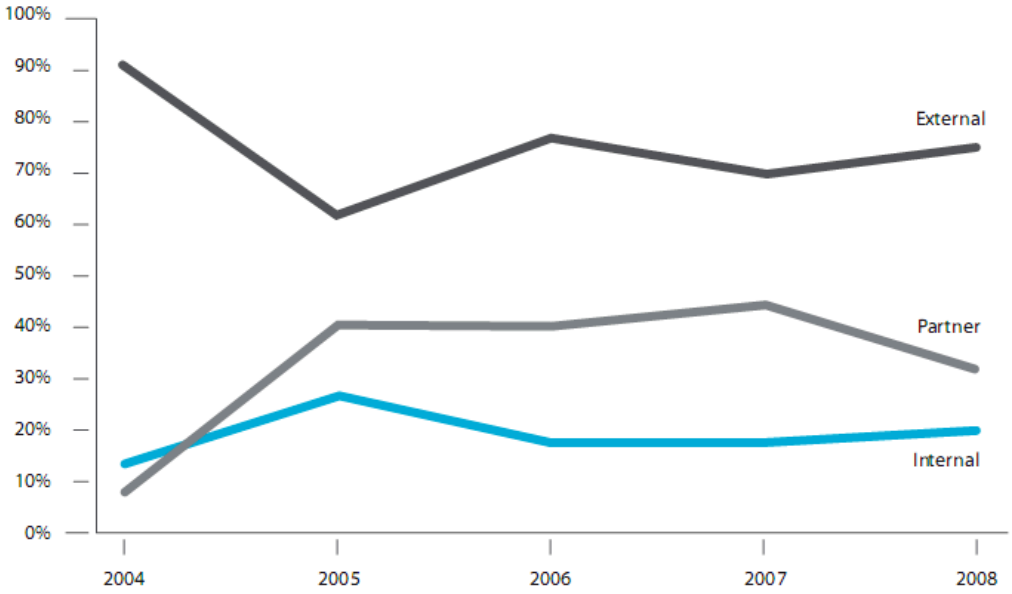
- Objective, credible, first-hand information on actual breaches

2008 Caseload:

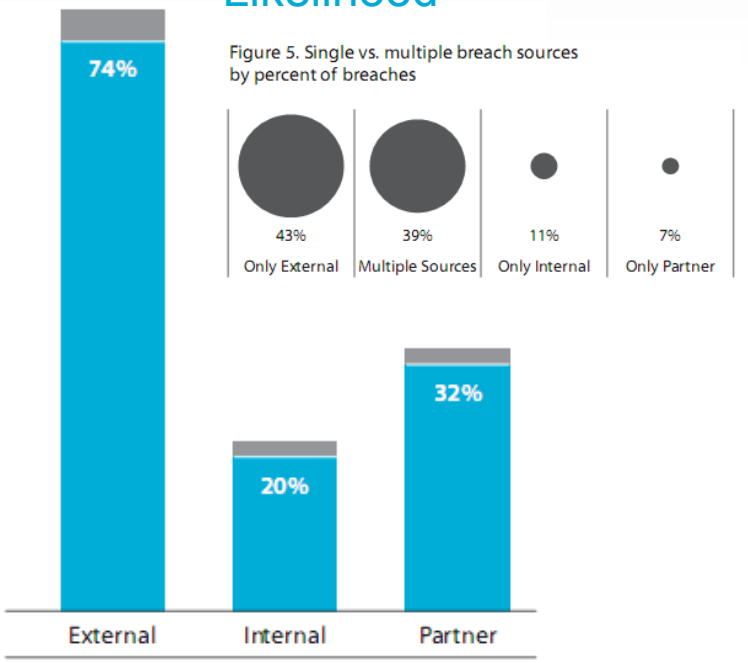
- 90 confirmed breaches (>150 total engagements)
- 285 million compromised records (confirmed – not “data-at-risk”)
- 1/3 of these cases have been publicly disclosed (so far)
- About 50% of caseload comprised of sets of interrelated incidents
  - Same attacker(s), shared connections, identical circumstances, etc
- 15 arrests (and counting)
- 31% Retail, 30% Financial, 14% Food&Bev, Remaining mixed
- Over 1/3 of investigations conducted outside the US

Breach Sources

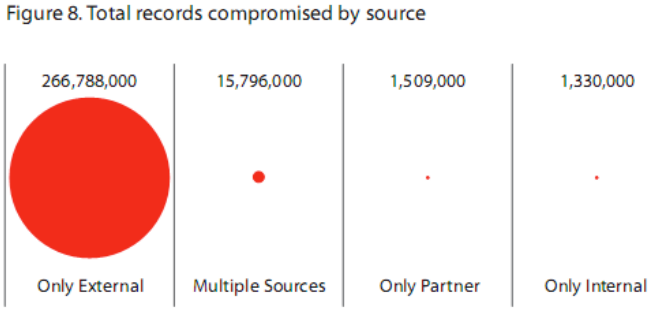
- External sources
  - Most breaches, nearly all records
  - 90+% of breached records attributed to organized crime activity
- Internal sources
  - Roughly equal between end-users and admins
- Partner sources
  - Mostly hijacked third-party accounts/connections



Likelihood

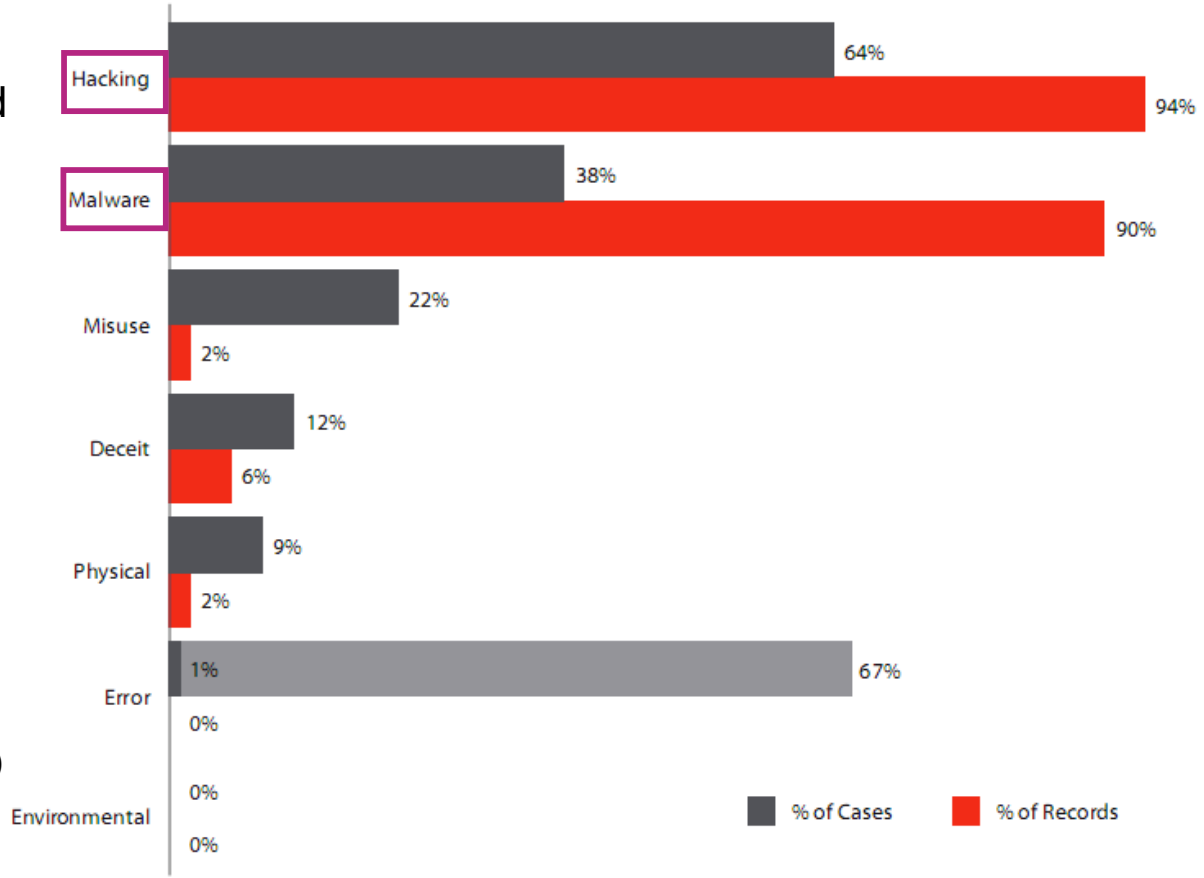


Impact



Threats and Attacks

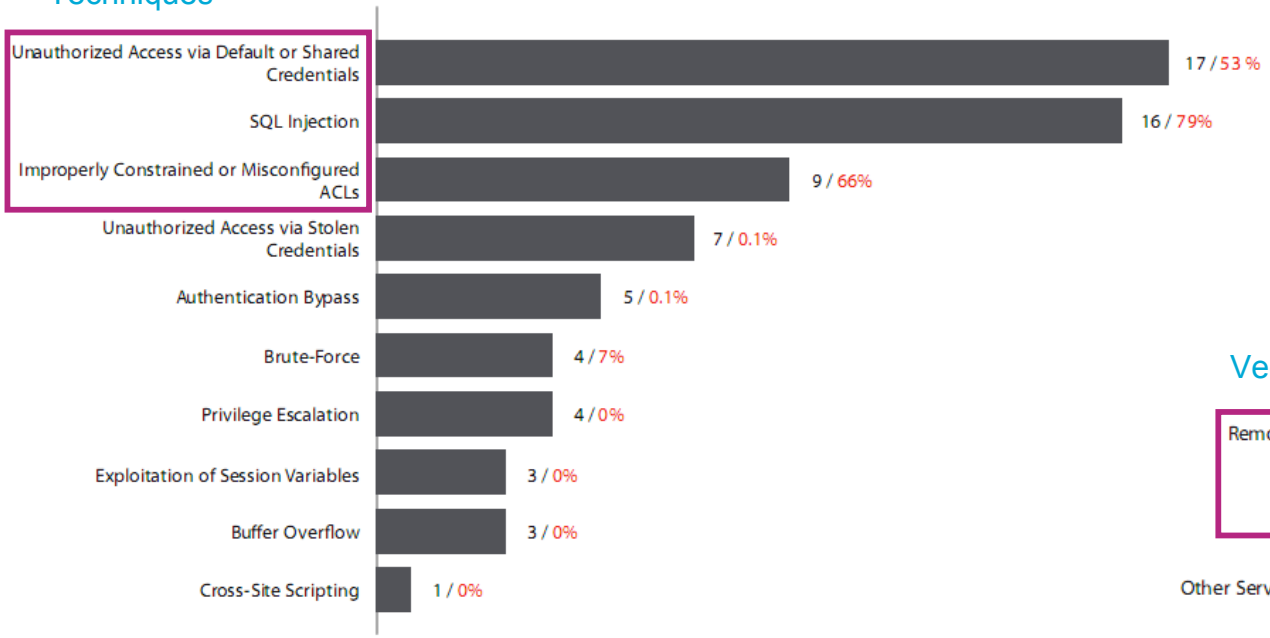
- Similar to previous 4 years for breach percentages
- Most breaches and records linked to Hacking & Malware
- Misuse is fairly common
  - Mostly admin abuse
- Deceit and social attacks
  - Involved a range of methods, vectors, and targets
- Physical attacks
  - Represent minority of caseload
  - Portable media in one case (but not essential to breach)
- Error is extremely common
  - Rarely the direct cause
  - Usually contributing factor (67%)



Breakdown of Hacking
(64% of breaches)

- Default credentials and SQL injection most common
- Few and old vulnerabilities exploited
- Web Apps & Remote Access are main vectors

Techniques

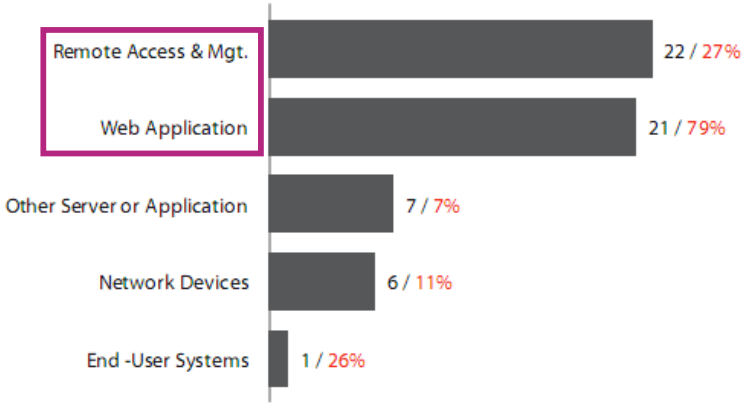


Vulnerability Exploits

Table 2. Patch availability at time of breach

Less than 1 month	0
1 to 3 months	0
3 to 6 months	0
6 to 12 months	1
More than 1 year	5

Vectors



Breakdown of Malware
(38% of breaches)

- Most malware installed by remote attacker
- Malware captures data or provides access/control
- Increasingly customized

Figure 17. Malware infection vector by number of breaches

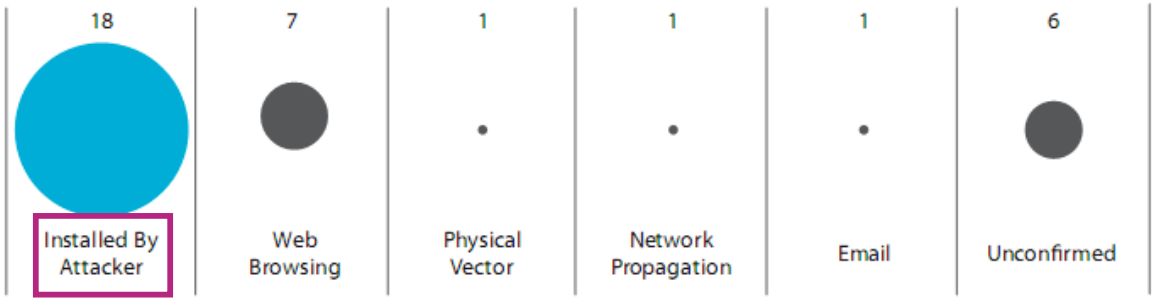
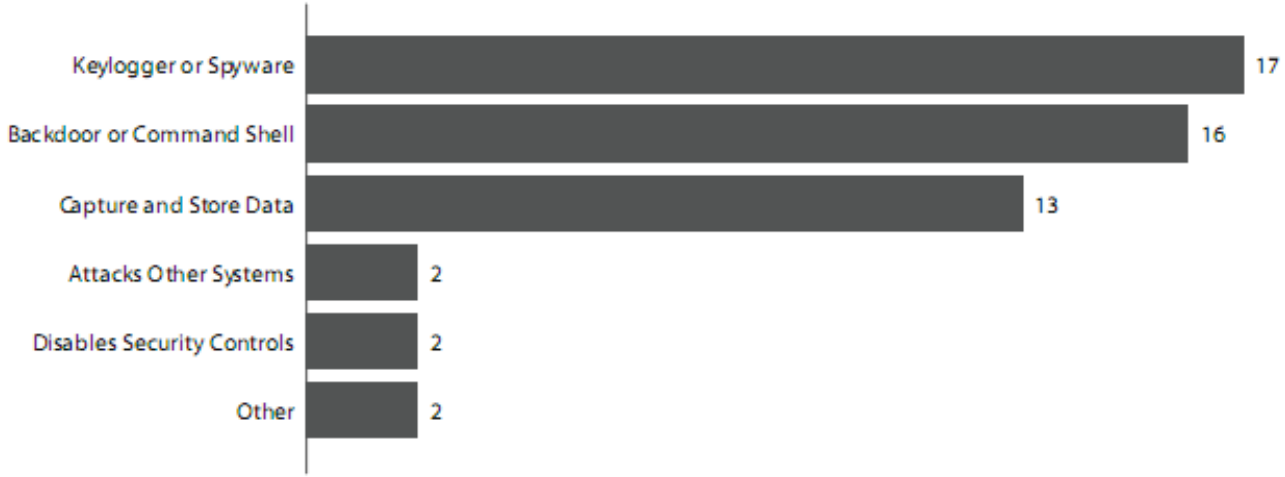
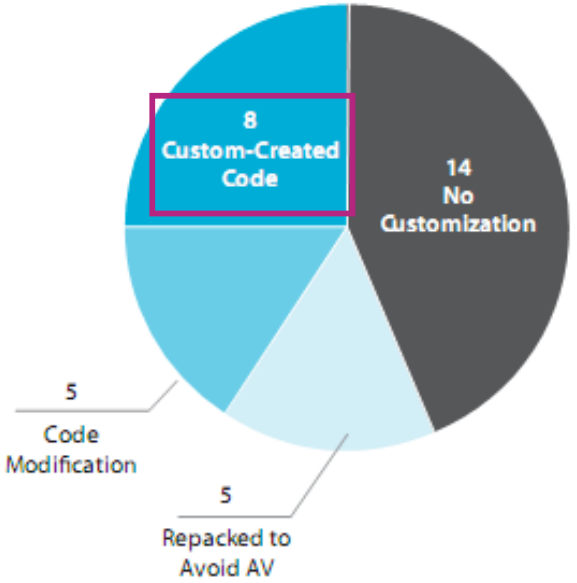


Figure 18. Malware functionality by number of breaches





Attack Difficulty and Targeting

- Targeted attacks doubled
- Highly difficult attacks did not increase but are responsible for nearly all breached records
- Message: Some attacks are difficult to pull off but the payout appears worth it

Figure 24. Targeted vs. opportunistic attacks by percent of breaches

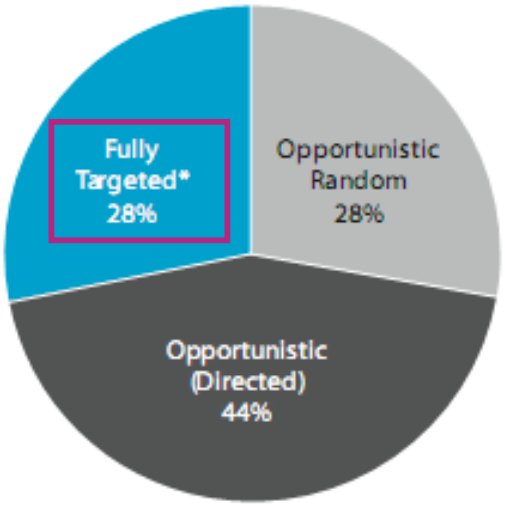


Figure 22. Attack difficulty by percent of breaches

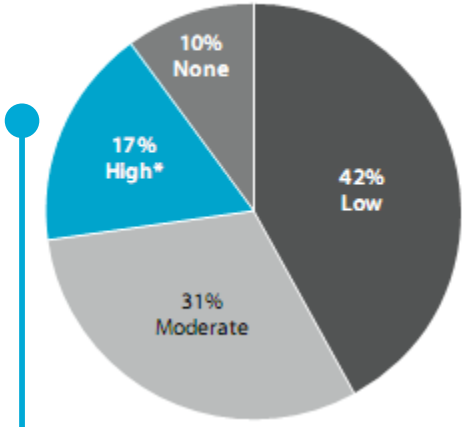
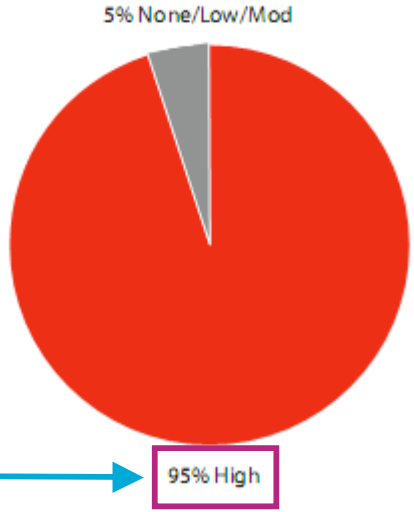


Figure 23. Attack difficulty by percent of records



Compromised Assets and Data

- Most data breached from online systems
  - Different than public disclosures
- Criminals seek payment card data
  - Easily convertible to cash
- Other types common as well
  - Auth credentials allow deeper access
  - Intellectual property at 5-year high

Figure 25. Asset classes by percent of breaches (black) and records (red)

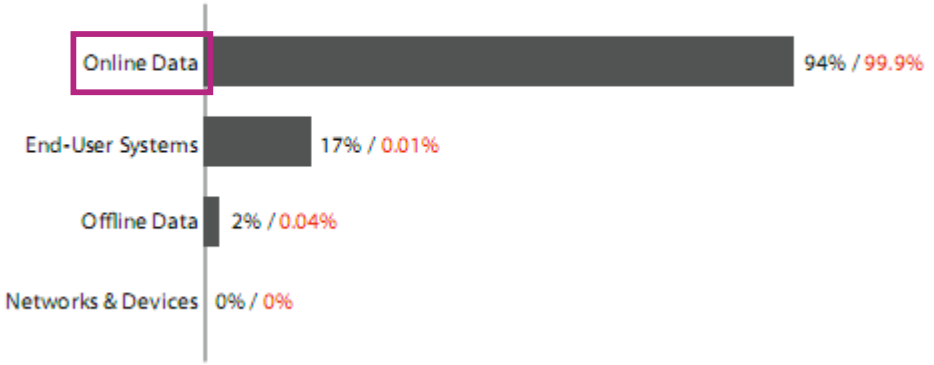


Figure 29. Compromised data types by percent of breaches (black) and records (red)*

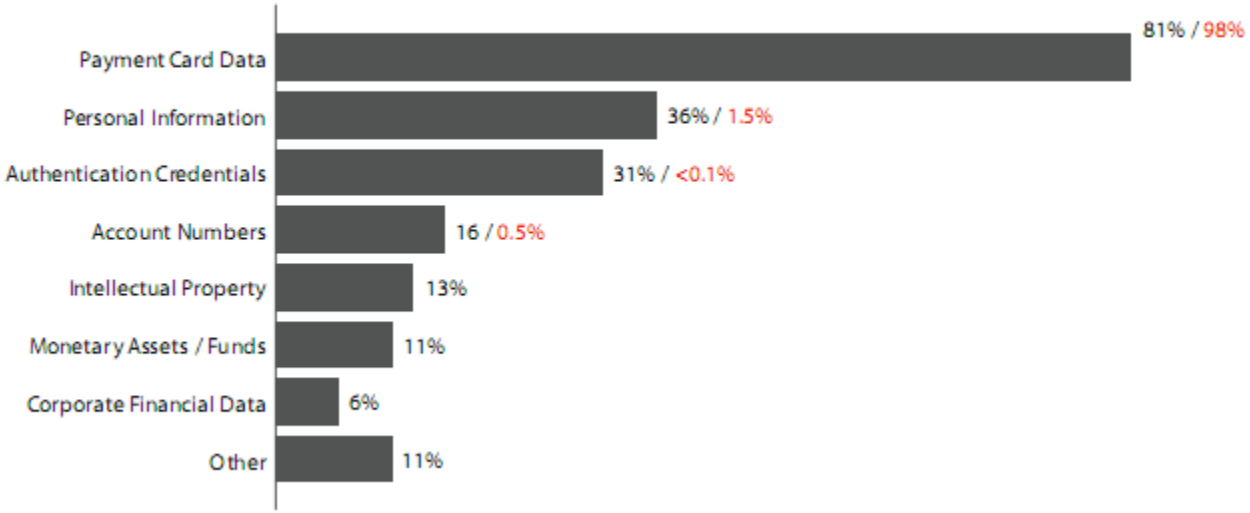
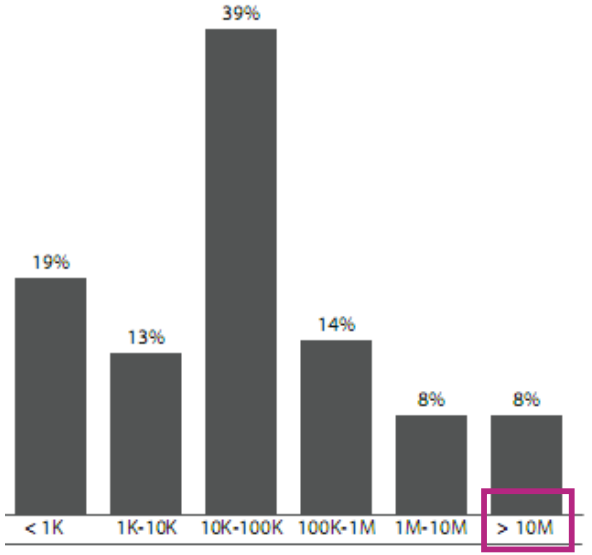


Figure 28. Distribution of breach size by number of records



Breach Timeline

- Amount of pre-attack research varies
- Data compromised within hours/days after breaching perimeter
- Breaches go undiscovered for months
- It typically takes days to weeks to contain a breach

Figure 31. Time span of breach events by percent of breaches

Breach Discovery

- Most breaches discovered by a third party
- Event monitoring caught few breaches

Figure 32. Breach discovery methods by percent of breaches

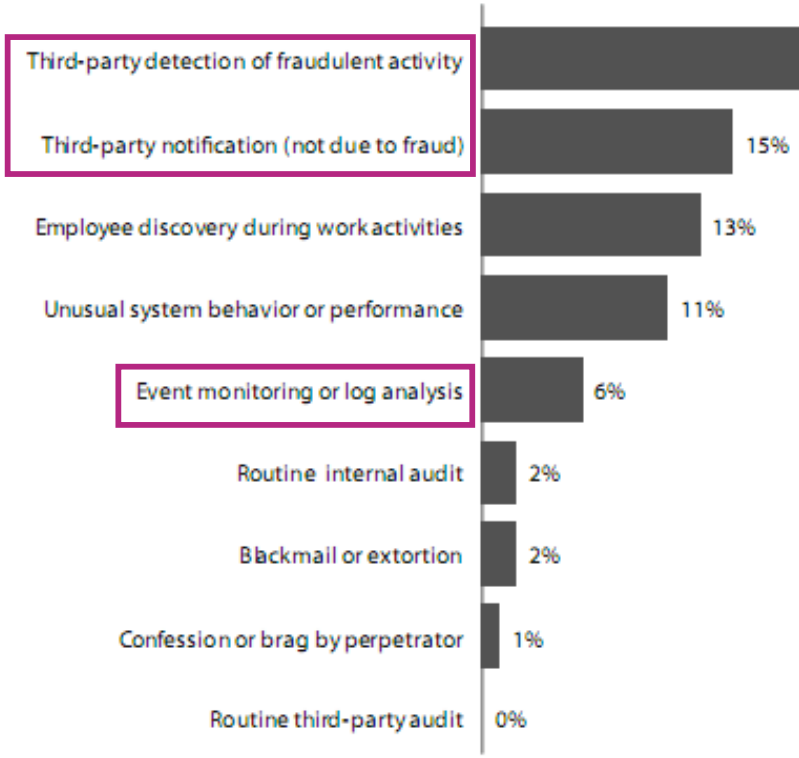
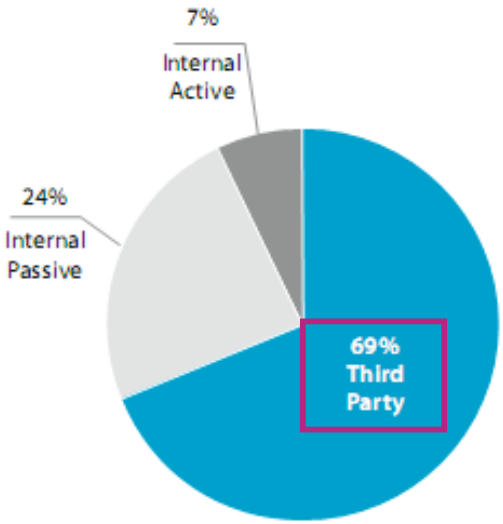


Figure 33. Breach discovery methods, simplified



Unknown Unknowns

- Unknown data lower than ’04-’07 rates but still accounts for 2/3 of compromised records
  - Discovery and classification
- Unknown privileges up
  - Account review

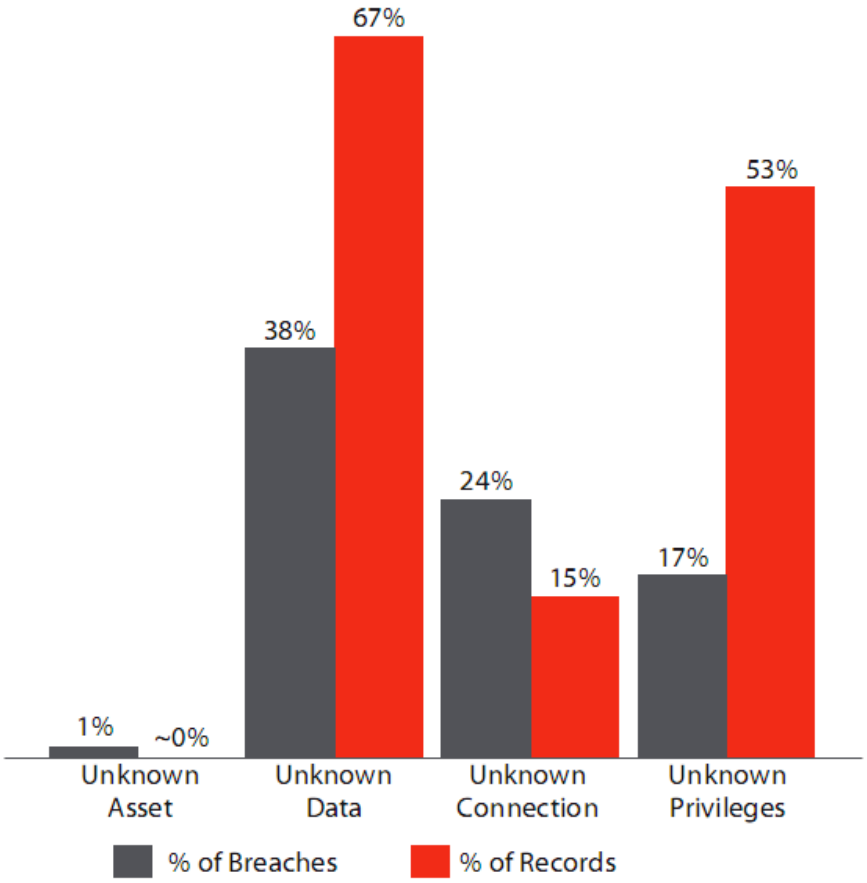
An **asset** unknown to the organization

Data unknowingly stored on an asset

Unknown or forgotten external IT **connections**

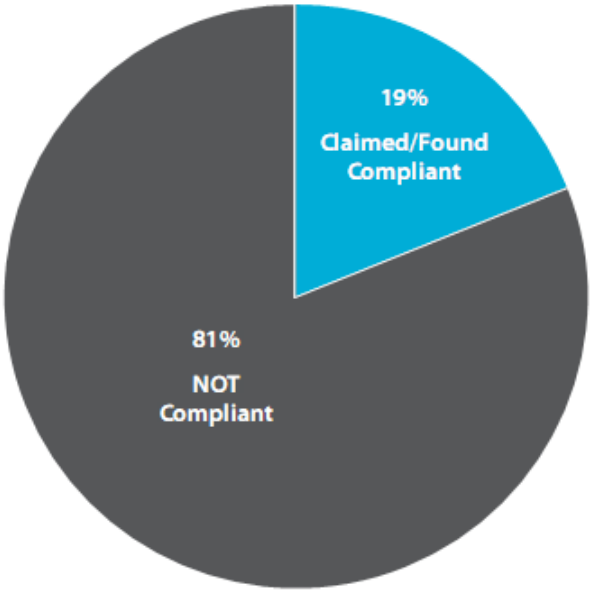
Accounts and **Privileges** not known to exist

Figure 30. Unknown unknowns by percent of breaches



PCI DSS

Figure 37. PCI compliance status based on last assessment by percent of breach victims



Is PCI a Failure? NO!

Then why were 19% breached?

- Self-attestation
- Study includes failures only
- Scope / Unknowns
- Assessment Sampling
- Partners (transitive trust)

Table 10. Results of post-breach PCI DSS reviews conducted by Verizon Business IR. Values represent the percentage of organizations for which each requirement was found to be in place.

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

Open DBIR Case Metrics

Data is needed.

Data is needed.

Data ***quality*** is needed.

Data is needed.

Data *quality* is needed.

Data ***similarity*** is needed.

(we need to be able to compare data on a same to samebasis.)

We are considering “opening” our metrics and methodology

Why should the industry care?

- Data breach information helps determine “what doesn’t work”
- Data breach information helps determine “what does work”
  - Both from a protection and attack standpoint
- Timely data breach information can significantly increase the quality of predictive analytics (state of wisdom)

verizon business

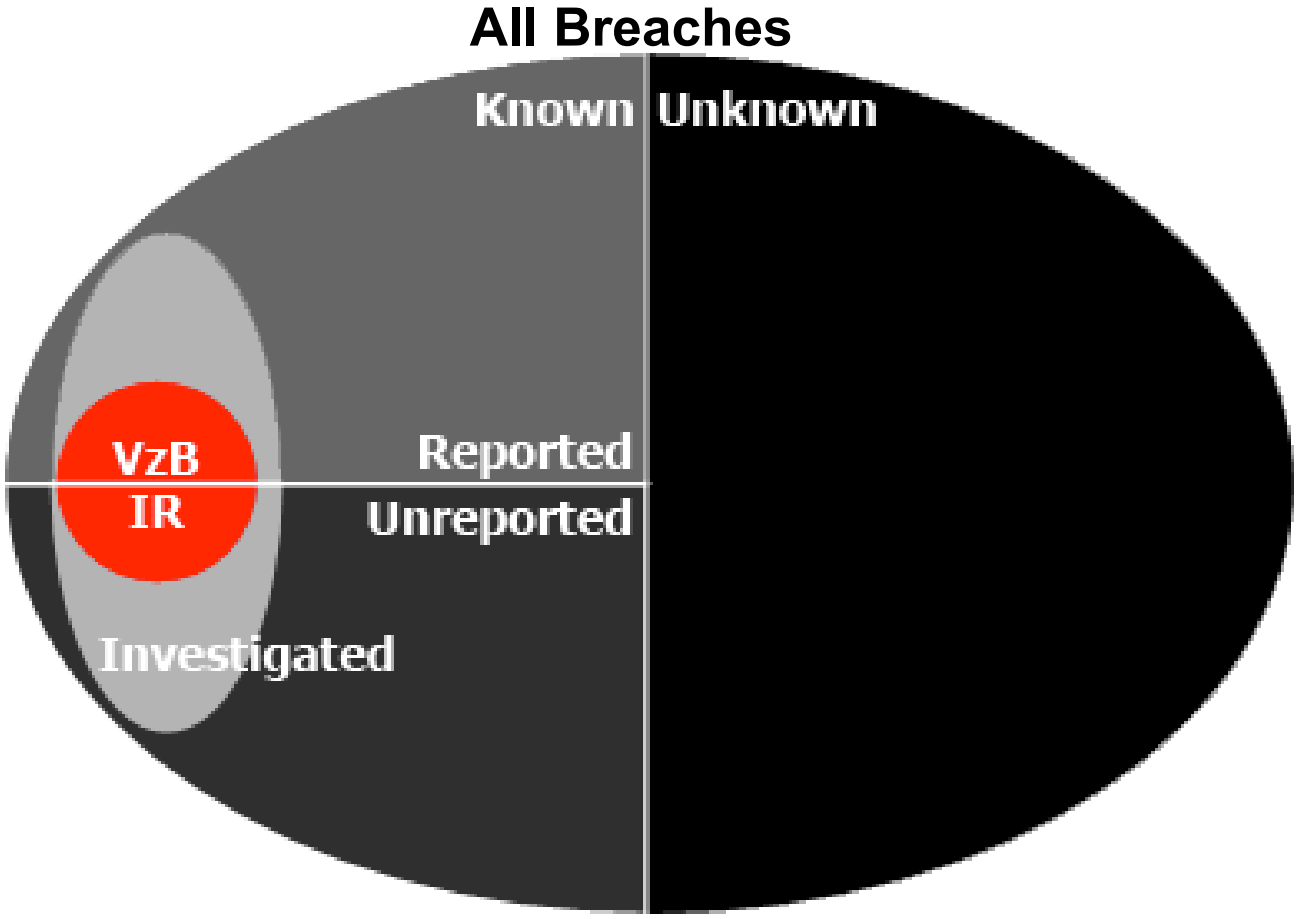
What We're Considering

* We don't have final blessing yet (and may never).

- Release our case metrics for public use
- Provide the methodology we use to collect them.
- Get feedback from the security community
  - be open and willing to change based on *rational* criticism.
- Receive, aggregate, and freely report incident data collected and submitted by any organization using our metrics

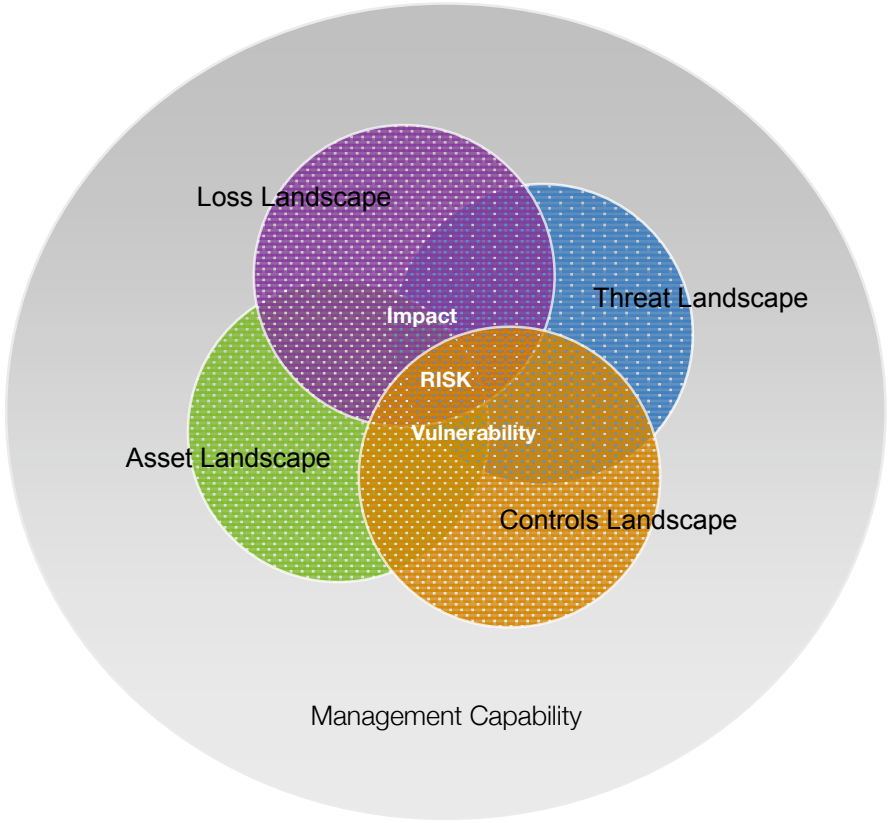
Hopeful Result #1

Significantly expanded sample size



Hopeful Result #2

Information about the dynamic elements of the threat, asset, controls, and security management landscapes



Hopeful Result (Overall)

An aggregate increase in the ability of practitioners to align their capability to manage risk to the risk tolerance of their organization.

(i.e., risk management)