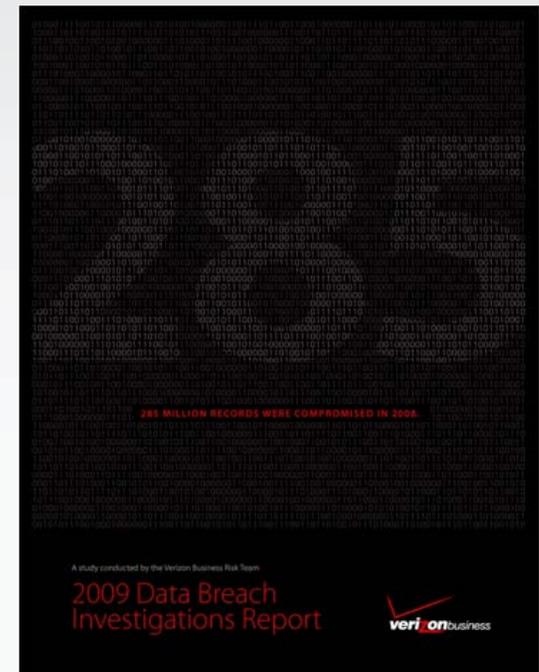




2009 Data Breach Investigations Report

Federal Reserve Bank of Atlanta
November 5, 2009

Christopher Novak
Managing Principal – Investigative Response
T: 914-574-2805
E: chris.novak@verizonbusiness.com





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.

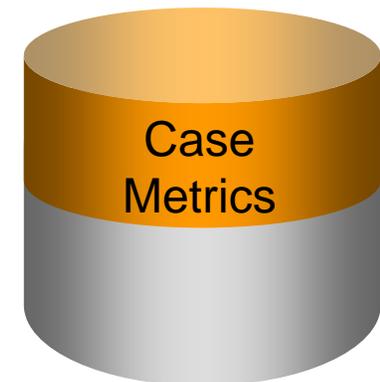
Collection Methodology

Prior to 2007: Some high-level statistics & trends; some diffusion of insight

Mid 2007: Initiative begun to define and parameterize hundreds of case metrics; Systematic collection for historical cases using reports, notes and investigator interviews

Present: Metrics collection process created and adopted as standard operating procedure on all new cases

IR Services
& Data





Study Overview

A few things to keep in mind..

Caseload bias: Data set is dependent upon cases which Verizon Business was engaged to investigate

Failures, not Successes: Report focuses on data breaches and therefore provides information regarding security failures rather than successes

Anonymity: Once the investigator records and submits case metrics, the information is sanitized – the central repository contains no information that would enable one to ascertain a client's identity



Results & Analysis

Breach Sources

External sources

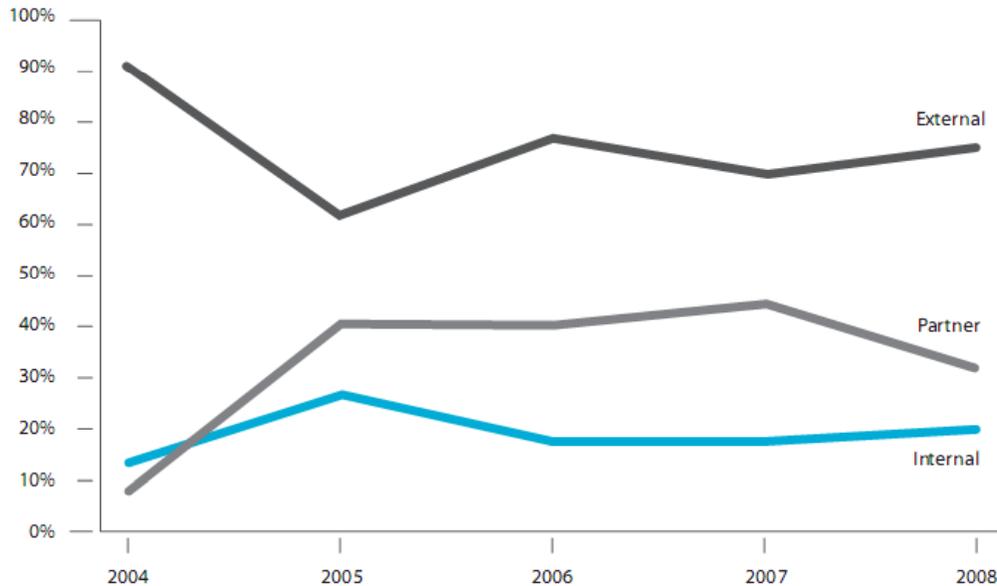
- Most breaches, nearly all records
- 90+% of breached records attributed to organized crime activity

Internal sources

- Roughly equal between end-users and admins

Partner sources

- Mostly hijacked third-party accounts/connections



Likelihood

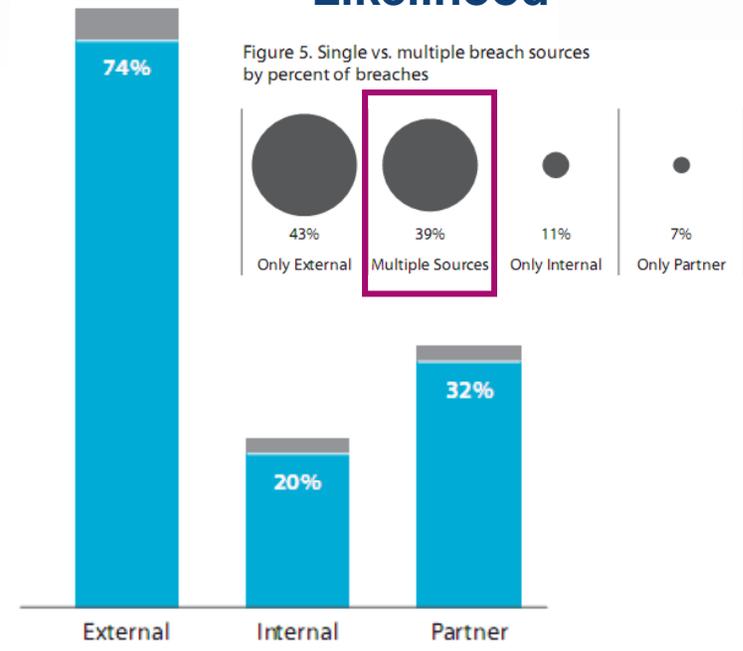
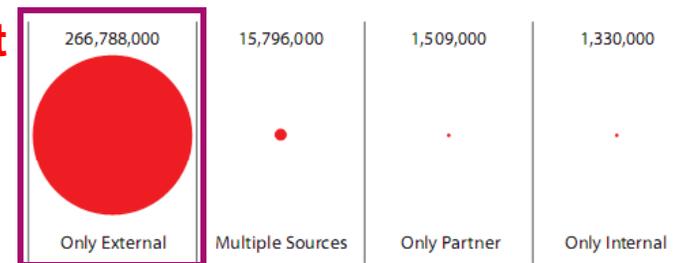


Figure 8. Total records compromised by source

Impact





Information Black Market

```
With Email Access || Paypal Verified With Email Access || (Payment LR)
<MachineX> Cashout Dump+pins EU.US.CA - Also Buys and payment after Cashout,
Only Fresh from Good Suppliers. Also Cashing Bins List 488860 430572 464018
512107 542418 546616
* X-Man-CC ->> selling >>@« Fresh Fullz CCU FR/US/UK/IT/CND... Shopadmins ... Scan
Paage..Maillist...Paypal Verifie>>@«
* +Napushenko selling US/UK/CA/AU/FI/FR/GR/NZ/SP cvv2s,US/UK full info,US/CA dumps without
PIN,socks4/5 any country/state,exchanging LR/WMZ/E-GOLD ??? Msg me for deal ??
* Sells_Fulls_ Selling Fress USA CC Fulls Info, Ebay Users PM ME ?? ++++++
+++++NU CAUT TEPARII+++++
<Skult> ----- Selling 27 POS All TRACKS@ CONTACT ME FOR DEAL@@
* inferno_0000 sell dumps without pin track1&track2 skimmed and fresh staff . If you are
interested contact me dumps_seller99 at yahoo . rippers and biginer fu off bj
<Track4ALL> dumpsmarket crew provides best source of natural dumps track2
skimmed ? READERS AND WRITER DEVICES AVAIVABLE ?
* chaos sets mode: +l 130
* dffff (~ana@c-66-41-126-99.hsd1.mn.comcast.net) Quit (Ping timeout)
* struga_boy_A who can hack php nuke websites msg me to deal who can hack php
nuke websites msg me to deal who can hack php nuke websites msg me to deal
* CashBankLog I am the drop of UK banks: Lloyds, HSBC, Barclays, Natwest, I can cashout
UK bank logins INSTANTLY. Looking for serious partners. Only serious!
<UnWanted`> SELLING US FULLZ 10$ !!!!
<|MandRake|> Selling Wachovia Login Full Info 11k Balance,BOA Full Info Login 30k
Balance,Chase,WellsFargo Login Full Info 140k Balance,Fresh Fulls USA Cvv2
Info + SSM MMN DOR PIN 8$ Per 1,Dell Preferred Accounts,Declined Fulls,Need
Supplier For TimeCards For WOW:Burning Crusade Europe,Msg Me Fast Accept Only
LibertyReserve !!!
* Sells_Fulls_ Selling Fress USA CC Fulls Info, Ebay Users PM ME ?? ++++++
+++++NU CAUT TEPARII+++++
```



Captured IRC

<SB> Hey bro, you here?

<Skult> ?

<SB> Im interested in buying your dumps

<Skult> Not selling individually, only bulk+ POS terminal

<SB> Really? How much is bulk?

<Skult> \$60K usd for each pos

<SB> whoah, ok. Listen I do make large buys sometimes, but that takes a lot of trust. Plus I cant exactly send you a WU for that much money. If we did a deal I would need to see some proof of what you have. Plus I will ask you somethings to confirm you even know what your talking about. I see a lot of rippers, especially here on IRC

<SB> You said in your ad you have 27 POS, which kind are they then?

<Skult> Just locations, I wont say what kind they are :>

<SB> Fair enough. What kind of traffic are they? High /low?

<Skult> Very high, they are restaurant servers very very good locations

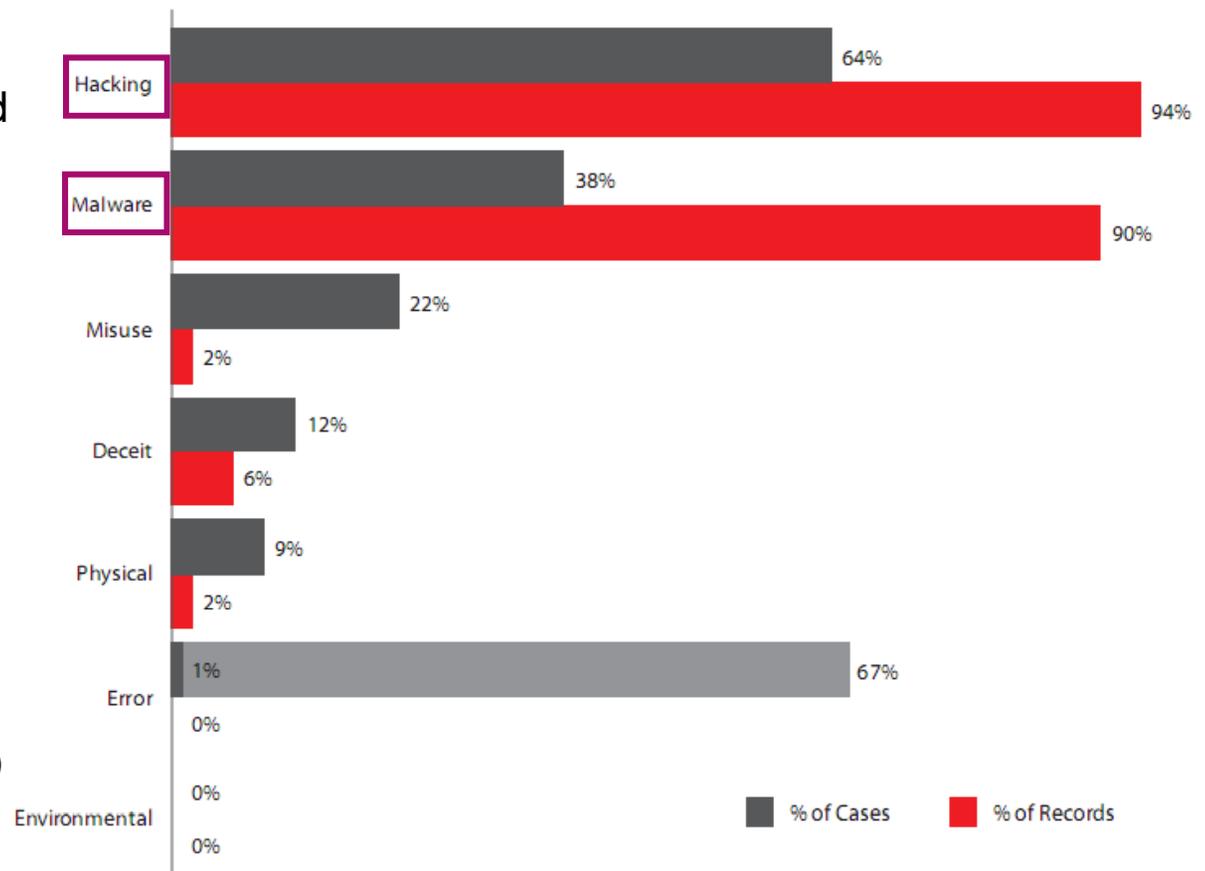
<SB> How many dumps from each POS bro and is there T2/pins?

<Skult> too many to count : > Pins if I have them I do not sell

<SB> Ok cool.

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%)

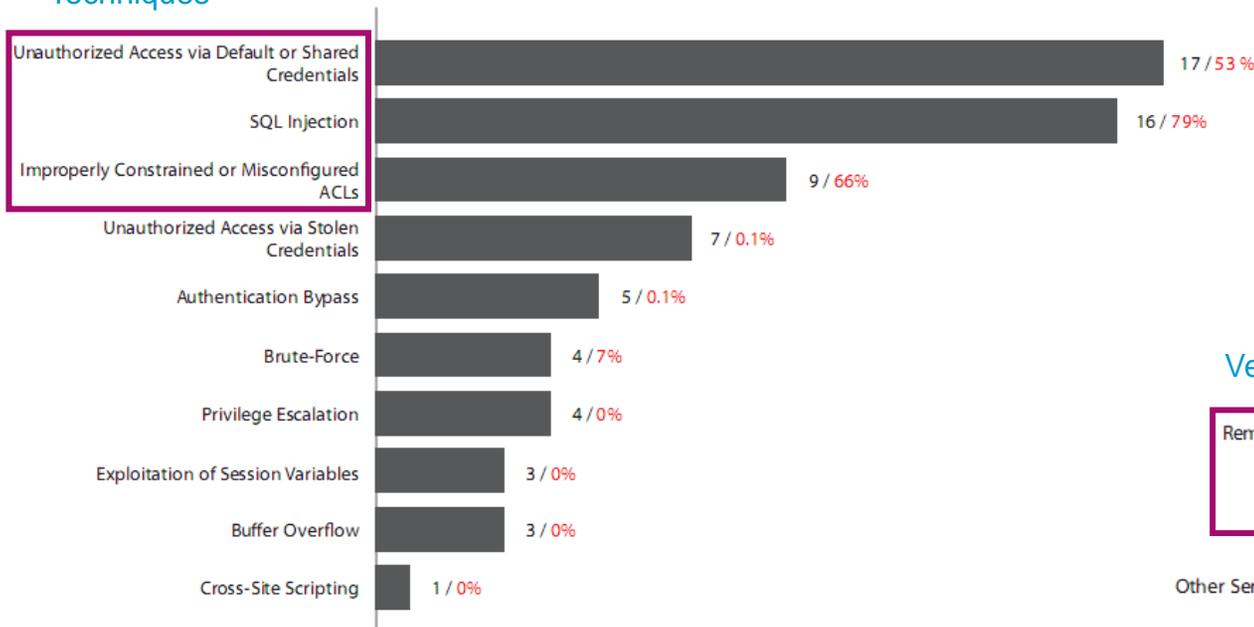




Breakdown of Hacking (64% of breaches)

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

Techniques

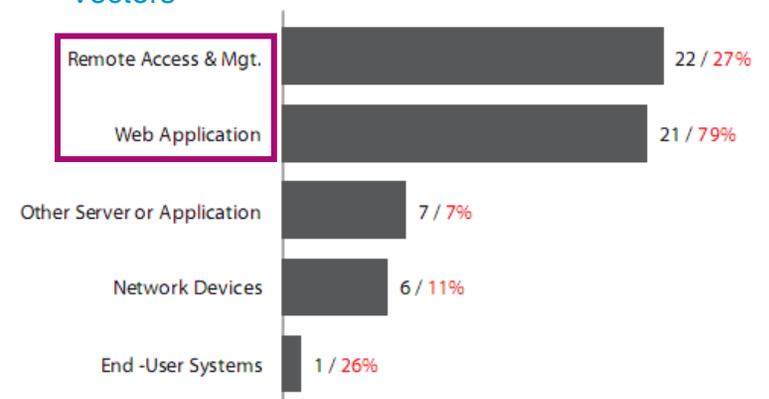


Vulnerability Exploits

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

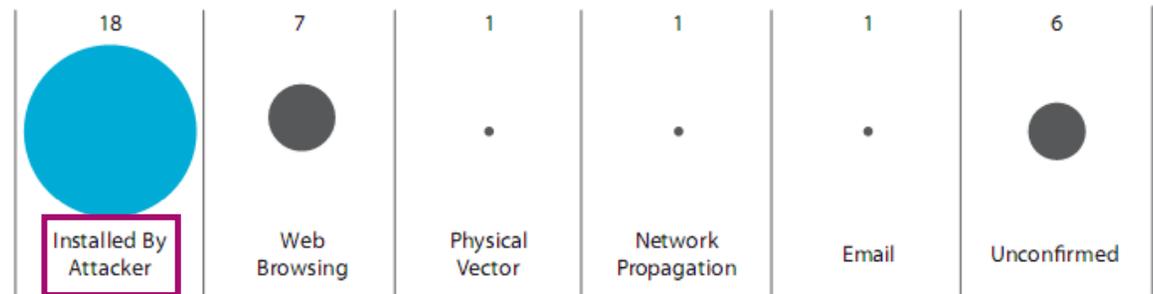
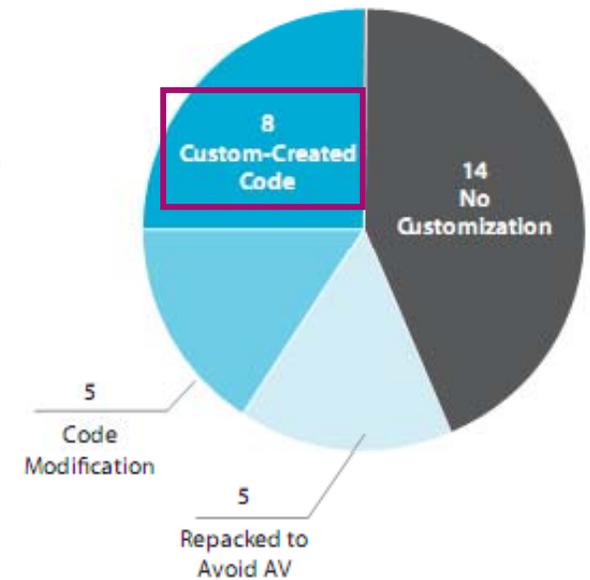
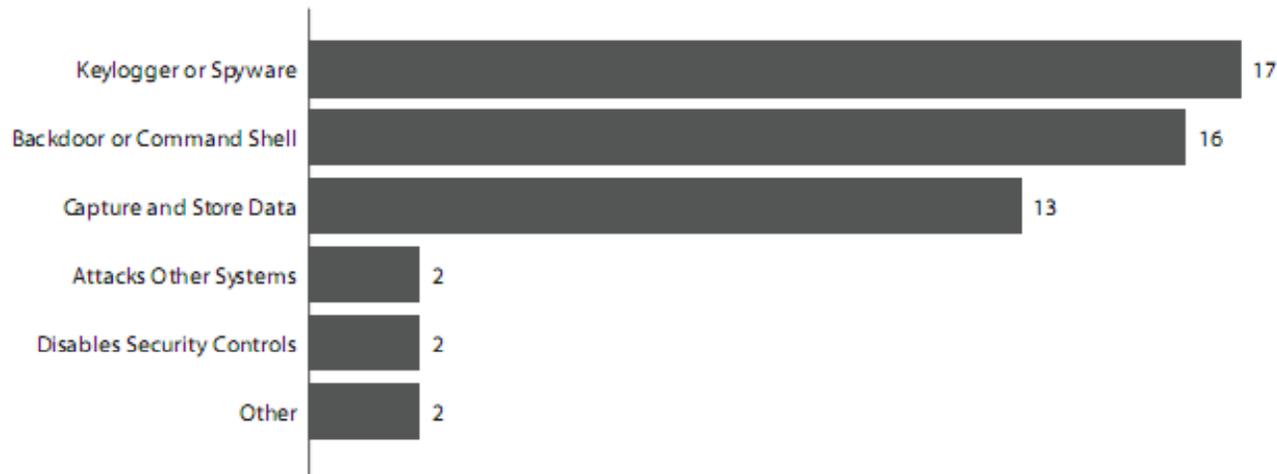


Figure 18. Malware functionality by number of breaches



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

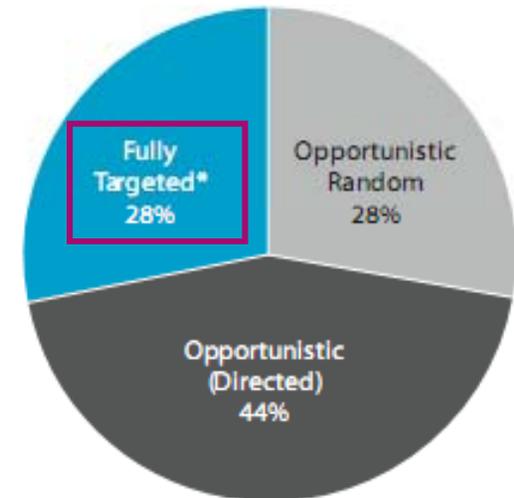


Figure 23. Attack difficulty by percent of records

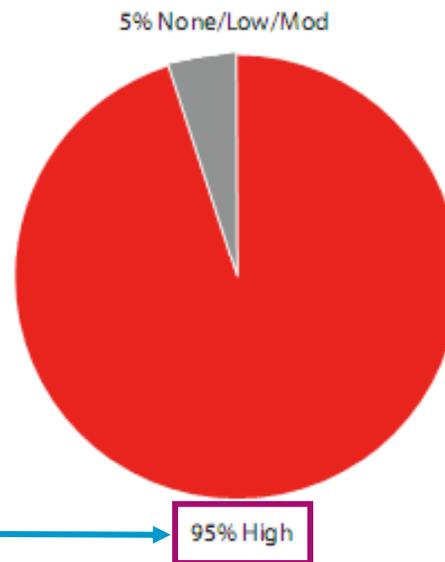
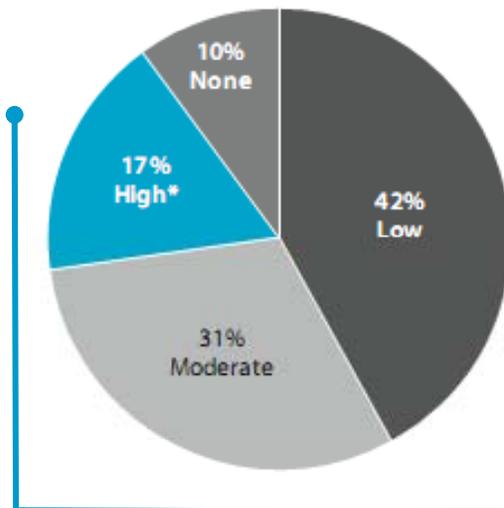


Figure 22. Attack difficulty by percent of breaches



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)

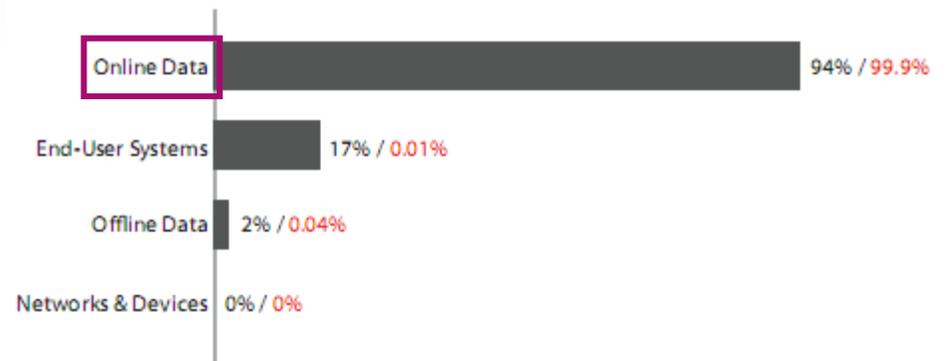


Figure 29. Compromised data types by percent of breaches (black) and records (red)*

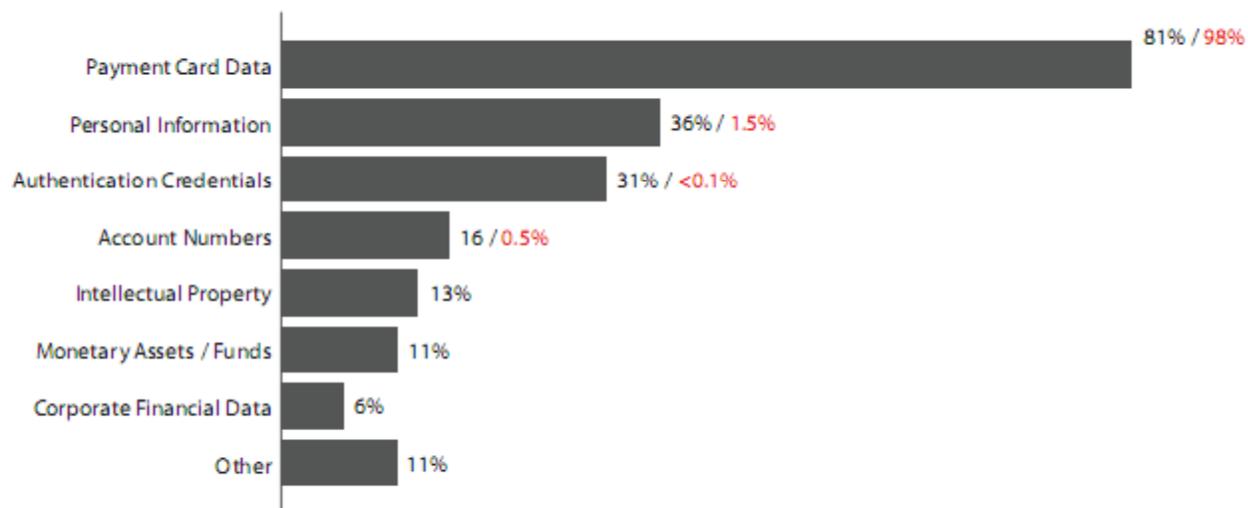
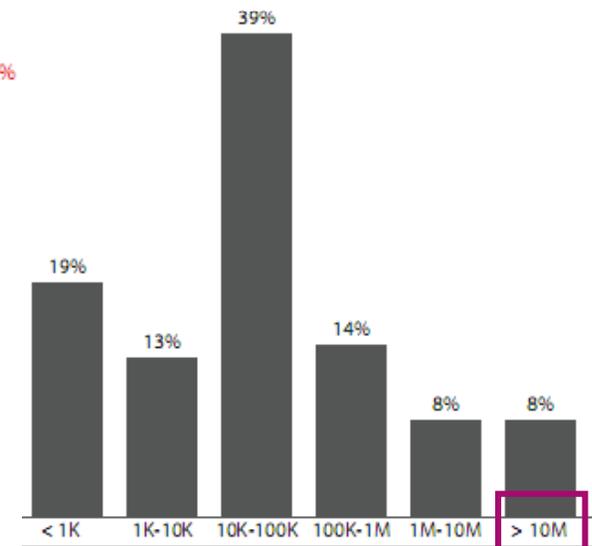


Figure 28. Distribution of breach size by number of records



Breach Timeline

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

- 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



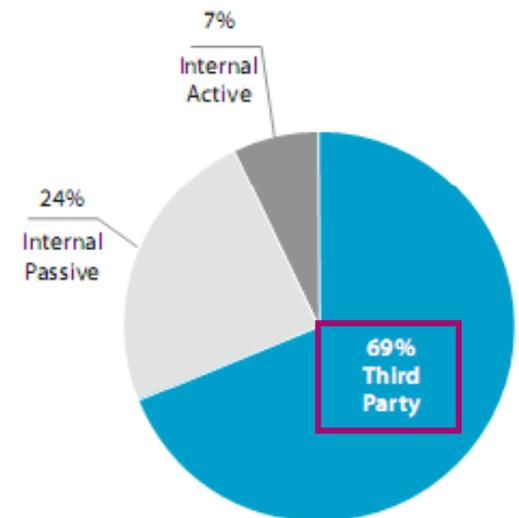
Breach Discovery

- 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





PCI DSS

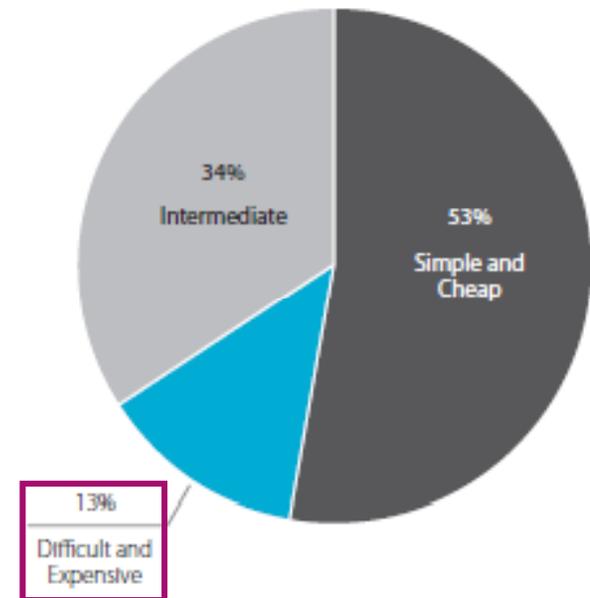
Table 10. Results of post-breach PCI DSS reviews conducted by Verizon Business IR. Values represent the percentage of organizations for which each requirement was found to be in place.

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%

Recommendations

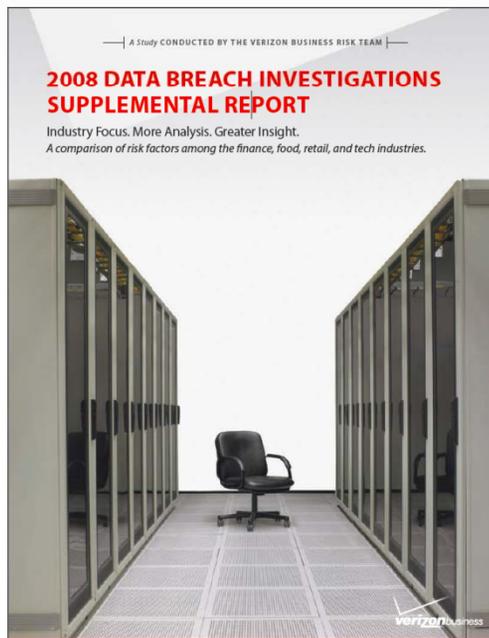
- Secure Business Partner Connections
- Create a Data Retention Plan
- Align process with policy
- Avoid shared credentials
- Application Testing and Code Review
- Smarter Patch Management Strategies
- Monitor your logs / alerts
- Create an Incident Response Plan
 - Increase awareness
 - Engage in mock incident testing

Figure 41. Description of the effort and expense of recommended preventative measures by percent of breaches





Security Intelligence Resources

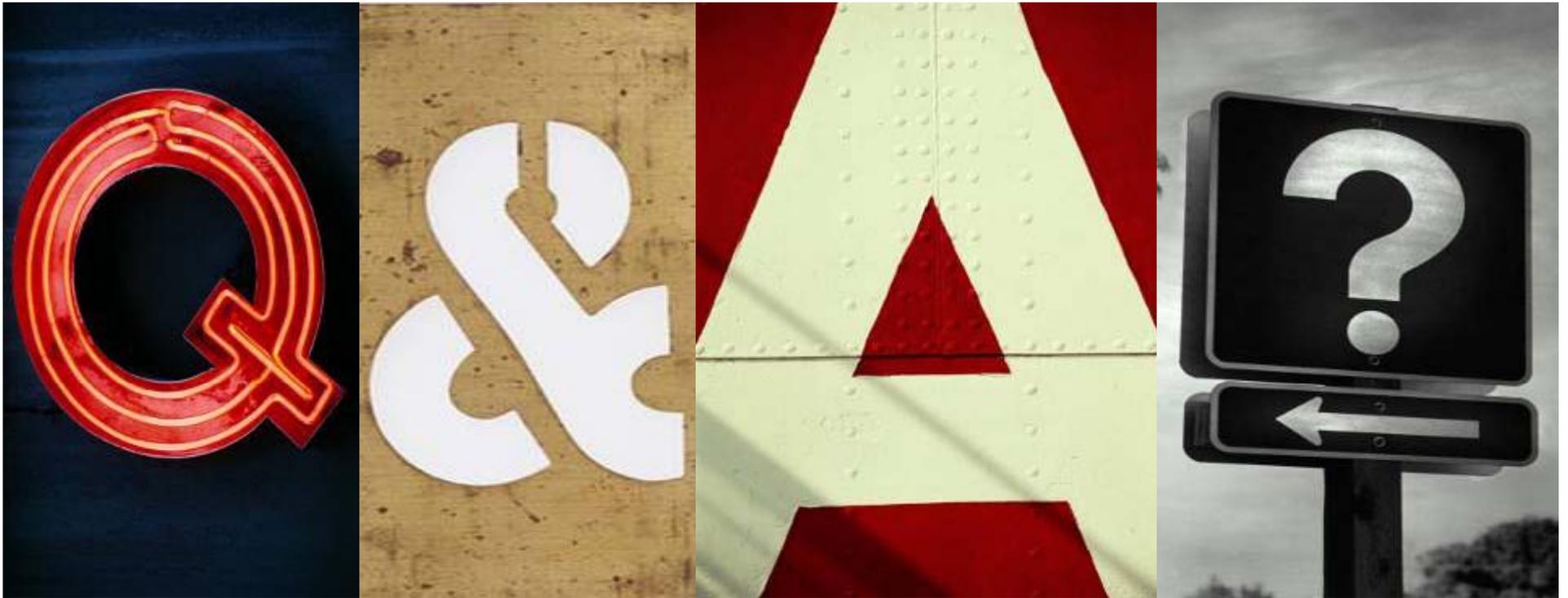


Available Online:

- Data breach reports
- Security research
- Whitepapers & studies
- Videos
- Podcasts
- Webinars
- Demonstrations
- Investigative case studies
- And more...

URL - <http://www.verizonbusiness.com/databreach/>

Blog - <http://securityblog.verizonbusiness.com/>



Christopher Novak
Managing Principal – IR Americas
T: 914-574-2805
E: chris.novak@verizonbusiness.com