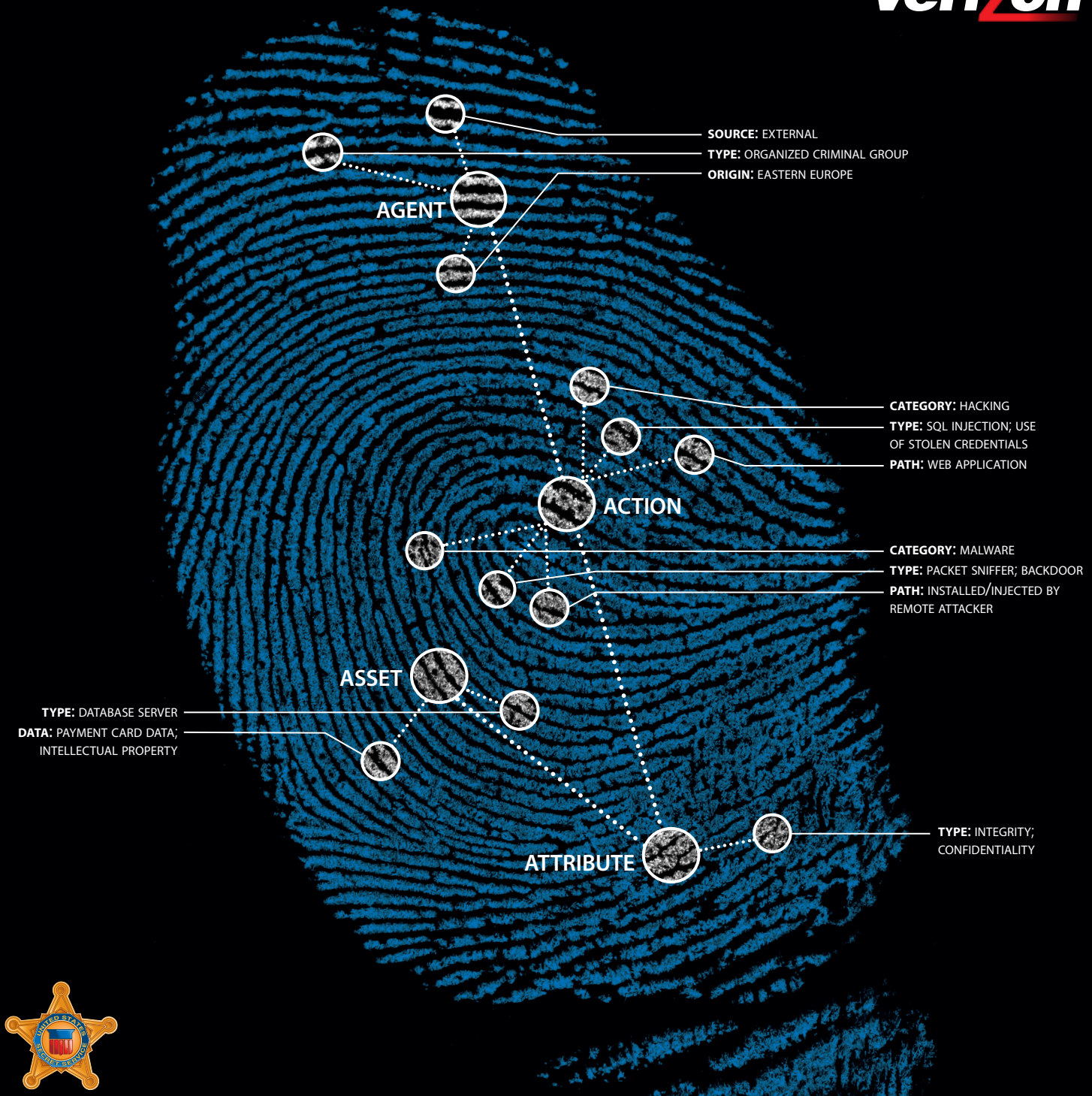


2010 DATA BREACH INVESTIGATIONS REPORT

A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service.

2010 Data Breach Investigations Report

AUTHORS:

Wade Baker
Mark Goudie
Alexander Hutton
C. David Hylender
Jelle Niemantsverdriet
Christopher Novak
David Ostertag
Christopher Porter
Mike Rosen
Bryan Sartin
Peter Tippett, M.D., Ph.D
Men and women of the
United States Secret Service

CONTRIBUTORS:

Thijs Bosschert
Eric Brohm
Calvin Chang
Michael Dahn
Ron Dormido
Ben van Erck
Kylee Evans
Eric Gentry
John Grim
Clarence Hill
Adam Kunsemiller
Kenny Lee
Wayne Lee
Kevin Long
Raphael Perelstein
Enrico Telemaque
Denson Todd
Yuichi Uzawa
J. Andrew Valentine
Nicolas Villatte
Matthijs van der Wel
Paul Wright

SPECIAL THANKS TO:

Tracey Beeferman
Carl Dismukes
Paul Goulding
Carole Neal

TABLE OF CONTENTS

For additional updates and commentary, please visit
http://securityblog.verizonbusiness.com.

For inquiries directed to the United States Secret Service, contact
databreachstudy@usss.dhs.gov.

2010 Data Breach Investigations Report

A study conducted by the Verizon Business RISK team in cooperation with the United States Secret Service.

Executive Summary

In some ways, data breaches have a lot in common with fingerprints. Each is unique and we learn a great deal by analyzing the various patterns, lines, and contours that comprise each one. The main value of fingerprints, however, lies in their ability to identify a particular individual in particular circumstances. In this sense, studying them in bulk offers little additional benefit. On the other hand, the analysis of breaches in aggregate can be of great benefit; the more we study, the more prepared we are to stop them.

Not surprisingly, the United States Secret Service (USSS) is also interested in studying and stopping data breaches. This was a driving force in their decision to join us in this 2010 Data Breach Investigations Report. They've increased the scope of what we're able to study dramatically by including a few hundred of their own cases to the mix. Also included are two appendices from the USSS. One delves into online criminal communities and the other focuses on prosecuting cybercrime. We're grateful for their contributions and believe organizations and individuals around the world will benefit from their efforts.

With the addition of Verizon's 2009 caseload and data contributed from the USSS, the DBIR series now spans six years, 900+ breaches, and over 900 million compromised records. We've learned a great deal from this journey and we're glad to have the opportunity to share these findings with you. As always, our goal is that the data and analysis presented in this report proves helpful to the planning and security efforts of our readers. We begin with a few highlights below.

WHO IS BEHIND DATA BREACHES?	
70% resulted from external agents (-9%)	Including the USSS cases in this year's report shook things up a bit but didn't shake our worldview. Driven largely by organized groups, the majority of breaches and almost all data stolen (98%) in 2009 was still the work of criminals outside the victim organization. Insiders, however, were more common in cases worked by the USSS, which boosted this figure in the joint dataset considerably. This year's study has by far improved our visibility into internal crime over any other year. Breaches linked to business partners continued the decline observed in our last report and reached the lowest level since 2004.
48% were caused by insiders (+26%)	
11% implicated business partners (-23%)	
27% involved multiple parties (-12%)	

	HOW DO BREACHES OCCUR?
Related to the larger proportion of insiders, Misuse sits atop the list of threat actions leading to breaches in 2009. That's not to say that Hacking and Malware have gone the way of the dinosaurs; they ranked #2 and #3 and were responsible for over 95% of all data comprised. Weak or stolen credentials, SQL injection, and data-capturing, customized malware continue to plague organizations trying to protect information assets. Cases involving the use of social tactics more than doubled and physical attacks like theft, tampering, and surveillance ticked up several notches.	**48%** involved privilege misuse (+26%)
	40% resulted from hacking (-24%)
	38% utilized malware (<>)
	28% employed social tactics (+16%)
	15% comprised physical attacks (+6%)

WHAT COMMONALITIES EXIST?

98% of all data breached came from servers (-1%)

85% of attacks were not considered highly difficult (+2%)

61% were discovered by a third party (-8%)

86% of victims had evidence of the breach in their log files

96% of breaches were avoidable through simple or intermediate controls (+9%)

79% of victims subject to PCI DSS had not achieved compliance

As in previous years, nearly all data were breached from servers and applications. This continues to be a defining characteristic between data-at-risk incidents and those involving actual compromise. The proportion of breaches stemming from highly sophisticated attacks remained rather low yet once again accounted for roughly nine out of ten records lost. In keeping with this finding, we assessed that most breaches could have been avoided without difficult or expensive controls. Yes, hindsight is 20/20 but the lesson holds true; the criminals are not hopelessly ahead in this game. The more we know, the better we can prepare. Speaking of being prepared, organizations remain sluggish in detecting and responding to incidents. Most breaches are discovered by external parties and only then after a considerable amount of time.

While we've added some new suggestions to the Conclusions and Recommendations section of this report, what you see to the right is similar to the message we've been preaching from the beginning. That's not because we don't feel like writing another sermon; it's simply that, based on the data before us, all the points in this one still apply.

This study always reminds us that our profession has the necessary tools to get the job done. The challenge for us lies in selecting the right tools for the job at hand and then not letting them get dull and rusty over time. Evidence shows when that happens, our adversaries are quick to take advantage of it.

The amount of breaches that exploit authentication in some manner is a problem. In our last report it was default credentials; this year it's stolen and/or weak credentials. Perhaps this is because attackers know most users are over-privileged. Perhaps it's because they know we don't monitor user activity very well. Perhaps it's just the easiest way in the door. Whatever the reason, we have some work to do here. It doesn't matter how hardened our defenses are if we can't distinguish the good guys from the bad guys.

Malware gets increasingly difficult to detect and prevent (especially once the attacker owns the system). Therefore, protect against the damage malware does after infection, much of which can be mitigated if outbound traffic is restricted.

Finally, the value of monitoring (perhaps we should say "mining") logs cannot be overstated. The signs are there; we just need to get better at recognizing them.

WHERE SHOULD MITIGATION EFFORTS BE FOCUSED?

- ✔ Eliminate unnecessary data; keep tabs on what's left
- ✔ Ensure essential controls are met
- ✔ Check the above again
- ✔ Test and review web applications
- ✔ Audit user accounts and monitor privileged activity
- ✔ Filter outbound traffic
- ✔ Monitor and mine event logs

Methodology

It is often said that the role of science is to explain the "how" of things in the natural world. We find it a fitting description and applaud all who study the intricacies of our field in pursuit of greater understanding. In that vein, the 2010 Data Breach Investigations Report (DBIR) marks the third installment (fifth if you count supplemental reports) in our continuing effort to shed light on the "how" of things in the world of computer crime.

The collection of data through rigorous observation is, of course, one of the cornerstones of any scientific endeavor. While we like to think our methodology has been rigorous, it cannot be said that it has been entirely consistent. The 2008 DBIR was a retrospective covering four years (2004-2007) of Verizon's caseload in one massive data collection effort. The scope was large but the level of analysis was somewhat limited due to the passage of time. The shift from historic to ongoing collection for the 2009 DBIR opened the door to more active observation, greater detail, and new areas of study. This approach certainly would have worked again for this year's report and would have maintained a state of consistency, which is a good trait to have in a methodology. Our ultimate goal, however, is not a state of consistency; our ultimate goal is a state of knowledge. It is to understand and explain the "how."

Not only does this increase the size of the window of visibility we have into the world of data breaches but also grants a new perspective into that world. As will be seen, our caseloads share many similarities, but there are some key differences as well.

For this reason, we are shaking things up again by including a completely foreign and very different (yet still very reliable) dataset in the 2010 DBIR. We're thrilled to welcome the contributions (in data and expertise) of the United States Secret Service (USSS) to this year's report. Not only does this increase the size of the window of visibility we have into the world of data breaches but also grants a new perspective into that world. As will be seen, our caseloads share many similarities, but there are some key differences as well. Both are instructive and we firmly believe this joint effort will lead us closer to the goal described above.

Pulling the two datasets together was quite an undertaking for both parties and the rest of this section will explain how it was accomplished.

Verizon Data Collection Methodology

The underlying methodology used by Verizon remains unchanged from that of previous years. All results are based on firsthand evidence collected during paid forensic investigations conducted by Verizon from 2004 to 2009. The 2009 caseload is the primary analytical focus of the report, but the entire range of data is referenced extensively throughout. Though the Investigative Response (IR) team works a variety of engagements, only those involving a confirmed breach are included in this data set. To help ensure reliable and consistent input, all investigators use the Verizon Enterprise Risk and Incident Sharing (VERIS) framework to record case data and other relevant details. The information collected using VERIS is then submitted to members of the RISK Intelligence team for further validation and analysis. The aggregate repository of case data is sanitized and contains no information that would enable one to ascertain a client's identity.

USSS Data Collection Methodology

With all the talk of "shaking things up" above, one might conclude that consistency was tossed out the window in this year's report. This is not the case. In terms of data collection, the USSS methodology differs little from that of Verizon. For the purposes of this study, the USSS created an internal application based on the VERIS framework. From the thousands of cases worked by the USSS during 2008 and 2009[1], the scope was narrowed to only those involving confirmed organizational data breaches[2] in alignment with the focus of the DBIR. The scope was further narrowed to include only cases for which Verizon did not conduct the forensic investigation[3]. Of these cases, a sample was taken and requests to input data were sent to USSS agents who worked each case. In doing so, these agents utilized investigative notes, reports provided by the victim or other forensic firms, and their own experience gained in handling the case. This yielded 257 qualifying cases for which data were collected within the time frame set for this report. The resulting dataset was purged of any information that might identify organizations or individuals involved in the case and then provided to Verizon's RISK Intelligence team for analysis.

In conclusion, we would like to reiterate that we make no claim that the findings of this report are representative of all data breaches in all organizations at all times. Even though the merged Verizon-USSS dataset (presumably) more closely reflects reality than either in isolation, it is still a sample. Although we believe many of the findings presented in this report to be appropriate for generalization (and our confidence in this grows over time), bias undoubtedly exists. Even so, there is a wealth of information here and no shortage of valid and clear takeaways. As with any study, readers will ultimately decide which findings are applicable within their organization.

A BRIEF PRIMER ON VERIS

VERIS is a framework designed to provide a common language for describing security incidents in a structured and repeatable manner. It takes the narrative of "who did what to what or whom with what result" and translates it into the kind of data you see presented in this report. Because many readers asked about the methodology behind the DBIR and because we hope to facilitate more information sharing on security incidents, we released VERIS earlier this year for free public use. A brief overview of VERIS is available on our website[4] and the complete framework can be obtained from the VERIS community wiki[5]. Both are good companion references to this report for understanding terminology and context.

1 The scope of data collection for the USSS was 2008 and 2009. However, over 70 cases worked in 2008 pertained to breaches that occurred in 2007. Because this is a large enough sample and allows for three-year trend analysis, we show them separate from 2008 breaches.

2 The USSS works many cases related to theft and fraud that are not included in this report. For instance, crimes committed against consumers that do not involve an organization or its assets are not included. Criminal activities that occur after data are stolen (i.e., "white plastic fraud" and identity theft) are also not within the scope of this study.

3 The USSS is often involved in one manner or another with cases worked by Verizon (especially the larger ones). To eliminate redundancy, these cases were removed from the USSS sample. Where both Verizon and the USSS worked a case, Verizon-contributed data were used.

4 http://www.verizonbusiness.com/resources/whitepapers/wp_verizon-incident-sharing-metrics-framework_en_xg.pdf

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

Cybercrime Year in Review, 2009

2009 was, in many ways, a transformational year in the trenches. As attackers and defenders vied for advantage, there were numerous developments on many fronts around the world. It's difficult to measure who's winning with any certainty but there are, at least, some measurements available. One of them, public breach disclosures, fell noticeably in 2009. Organizations that track disclosed breaches like DataLossDB[6] and the Identity Theft Resource Center[7] reported figures that were well off 2008 totals. Private presentations and hallway conversations with many in the know suggested similar findings. Our own caseload reveals this as well. In a report dedicated to the analysis of annual breach trends, it seems wholly appropriate to reflect on why. It also provides a fitting backdrop for discussing some key 2009 milestones.

In our last report, we observed that massive exposures of payment card data in recent years have effectively flooded the market and driven down the prices criminals can get for their stolen wares. 2009, then, may simply be the trough in a natural supply and demand cycle. If supply has outpaced demand, why release more product? Perhaps cybercriminals are directing their resources elsewhere until market conditions improve. It is also possible that breaches are occurring at the same rate but the criminals are sitting on stolen data until demand picks up. Because fraud alerts are the leading method of discovering breaches, it stands to reason that many breaches could occur without anyone being the wiser if the criminal decided it was in his best interest to be patient.

Perhaps cybercriminals are directing their resources elsewhere until market conditions improve. It is also possible that breaches are occurring at the same rate but the criminals are sitting on stolen data until demand picks up.

Another possible reason for this decline is law enforcement's effectiveness in capturing the criminals. The prosecution of Albert Gonzalez was a major event in 2009. He and his accomplices were responsible for some of the largest data breaches ever reported. Taking them off the streets, so to speak, may have caused a temporary (but we can hope for permanent) dip in breaches. It is also possible that their prosecution made other cybercriminals take some time off to reevaluate their priorities in life.

2009 witnessed much discussion and consideration around the world about breach disclosure laws. As seen in the U.S., the creation of these laws can have a huge effect on breach statistics. So can the administration of them. Depending on how the legal environment evolves in this area, it could have a significant impact on the number of known breaches worldwide.

While it's highly unlikely that cloud computing or virtualization had anything to do with breach disclosure rates, they were no doubt hot topics in 2009. We continue to search for a link between data breaches and cloud-based or virtualized infrastructure but continue to find none.

Finally, we would be remiss if we did not touch on the subject of the hour, Advanced Persistent Threats (APTs). Yes, APTs are real but they are not new. Although the hype has grown exponentially, the post-2010 threat of APTs to your organization is more or less the same as pre-2010 levels. While we do appreciate the business, we would like to save you some expense and heartache: APTs are not the source of all malware infections and suspicious traffic on your network. Don't get caught up in the hype. Manage your defenses based on reality, not on publicity. We hope this report helps with that.

6 http://datalossdb.org/
7 http://www.idtheftcenter.org/index.html

Results and Analysis

The Verizon IR team worked over 100 cases in 2009; 57 of them were confirmed breaches. While lower than typical for our caseload, many of these breaches were quite large and complex, often involving numerous parties, interrelated incidents, multiple countries, and many affected assets. The 257 qualified cases in the USSS dataset[8] included 84 cases from 2009, 102 from 2008, and 71 from 2007.

The primary dataset analyzed in this report contains the 141 (57 + 84) confirmed breach cases worked by Verizon and the USSS in 2009. The total number of data records compromised across these cases exceeds 143 million. In several places throughout the text, we show and discuss the entire range of data for both organizations (2004-2009 for Verizon, 2007-2009 for the USSS). No small amount of internal discussion took place regarding how best to present statistics on the combined Verizon-USSS dataset. In the end, we decided that its most compelling feature was not simply the ability to compare and contrast Verizon's cases with those of the USSS but rather the opportunity to study a more representative sample. Therefore, the chosen approach is to present the combined dataset intact and highlight interesting differences (or similarities) within the text where appropriate. There are, however, certain data points that were collected by Verizon but not the USSS; these are identified in the text/figures.

As was the case in our last report, about two-thirds of the breaches covered herein have either not yet been disclosed or never will be. Many were related in some manner (i.e., same perpetrators or source IP). So far, almost 15% of Verizon's 2009 cases led to known arrests while 66% of USSS cases resulted in the arrest of a suspect. Even more impressive is that most of those ended in a conviction.

With the addition of Verizon's 2009 caseload and data contributed from the USSS, the DBIR series now spans six years, 900+ breaches, and over 900 million compromised records.

The figures in this report utilize a consistent format. Values shown in **dark gray** pertain to breaches while values in **red** pertain to data records. The "breach" is the incident under investigation in a case and "records" refer to the amount of data units (files, card numbers, etc.) compromised in the breach. Figures and tables do not always contain all possible options but only those having a value greater than 0. If you are interested in seeing all options for any particular figure, these can be found in the VERIS framework.

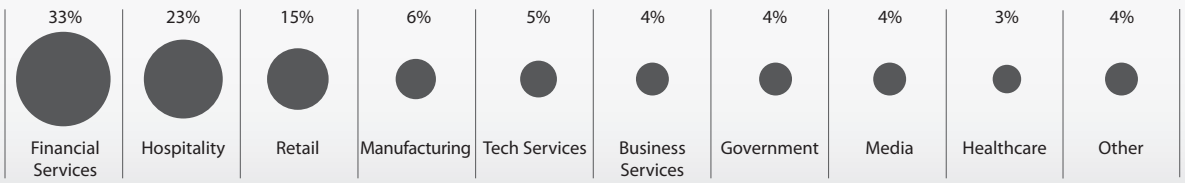
Without further delay, we present the investigative findings and analysis of Verizon and the USSS.

8 Refer to the Methodology section for an explanation of the qualification process.

Demographics

Of all sections in this report, demographics always present the greatest challenge for drawing out deeper meaning behind the numbers. While attack trends, incident response metrics, and other results are certainly dependent upon a given year's caseload, demographic data seem particularly so. Does the fact that we have more/less of a particular industry or region mean it is under increased attack? Is it more vulnerable? Did laws or other environmental factors change? Sheer coincidence? Obviously, it's difficult to know for certain. Demographic information is helpful, though, in establishing the context for other results. Thus, in this section we will relay the statistics, infer what we can, and let you do the rest.

Figure 1. Industry groups represented by percent of breaches



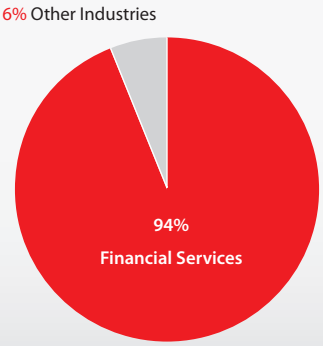
Data breaches continue to occur (in our caseload and elsewhere) within all types of organizations. These are categorized as they have been in previous reports according to the industry groups represented in Figure 1[9]. Financial Services, Hospitality, and Retail still comprise the "Big Three" of industries affected (33%, 23%, and 15% respectively) in the merged Verizon-USSS dataset, though Tech Services edged out Retail in Verizon's caseload. That this is consistently true of both the Verizon and USSS caseloads does seem to carry some significance.

The targeting of financial organizations is hardly shocking; stealing digital money from information systems rather than vaults is basically just a less primitive form of bank robbery. It represents the nearest approximation to actual cash for the criminal. Also, and perhaps more importantly, financial firms hold large volumes of sensitive consumer data for long periods of time. For this reason (and others), they fall under more stringent regulation and reporting requirements. This, in turn, increases the likelihood that breaches will require criminal and/or forensic investigation. In short, where other industries might be able to "sweep it under the rug," financial institutions are finding it increasingly difficult to do so. Regardless of the root cause(s), a growing percentage of cases and an astounding 94% of all compromised records in 2009 were attributed to Financial Services.

9 There are some changes in the way we categorize industries in this report. Most notably, "Food and Beverage" has been folded into the "Hospitality" group as this seems to be standard convention. A complete list of industries can be found in the VERIS framework.

The Hospitality and Retail industries exhibit similar trends when it comes to data breaches, which has a lot to do with their acceptance of payment cards and use of Point of Sale (POS) systems. This tends to draw a certain breed of criminal who favors certain ways and means of attack. There were quite a few public breach disclosures within the Hospitality industry in the last year or so and this spilled over into investigations conducted by Verizon and the USSS. Not surprisingly, restaurants and hotels comprise the bulk of cases in this industry group. Retail, which ranked first in total breaches in our last two reports, has fallen to third place and now accounts for less than half of its former glory (31% in '08 down to 14% in '09). This is not simply a by-product of incorporating USSS data (our own percentage for Retail was an even lower 9%) but we find it hard to attribute much more to these numbers than their face value.

Figure 2. Compromised records by industry group



For regional trends, it's worth making a distinction between the USSS and Verizon datasets. The USSS caseload, as one might suspect, is comprised of nearly all breaches that occurred in the United States (though investigating and prosecuting these crimes takes them all around the world). On the other hand, over half of the breaches investigated by Verizon in 2009 occurred outside the U.S. (the "North America" region includes cases from Canada and the Dominican Republic). Countries in which Verizon investigated confirmed and suspected breaches are highlighted in Figure 3. Over the past two years our caseload has consistently grown in Asia-Pacific and Western European countries. It is unclear as to whether our expanded international IR team or changes in global incident trends are most responsible for this but other sources suggest growth in these regions as well.

The targeting of financial organizations is hardly shocking; stealing digital money from information systems rather than vaults is basically just a less primitive form of bank robbery. It represents the nearest approximation to actual cash for the criminal.

The apparent disparity between the number of known data breaches in the United States and other parts of the globe has led some to conclude that other parts of the world are safer environments for electronic business. We do not believe this to be the case. The same basic information and communication technologies are present in homes, businesses, and governments all around the world. Admittedly, there are some differences that have an impact on cybercrime (the Chip and PIN payment infrastructure is a good example) but these differences are not enough to explain the disparity. The primary reason we hear more about data breaches in the U.S. (and in the report) stems from mandatory disclosure laws. Outside the U.S., breach disclosure differs significantly. Some countries are silent on the matter, others encourage it but don't require, and some even discourage disclosure.

Figure 3. Countries represented

Countries in which a breach was confirmed

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

Countries in which a breach was investigated but not confirmed

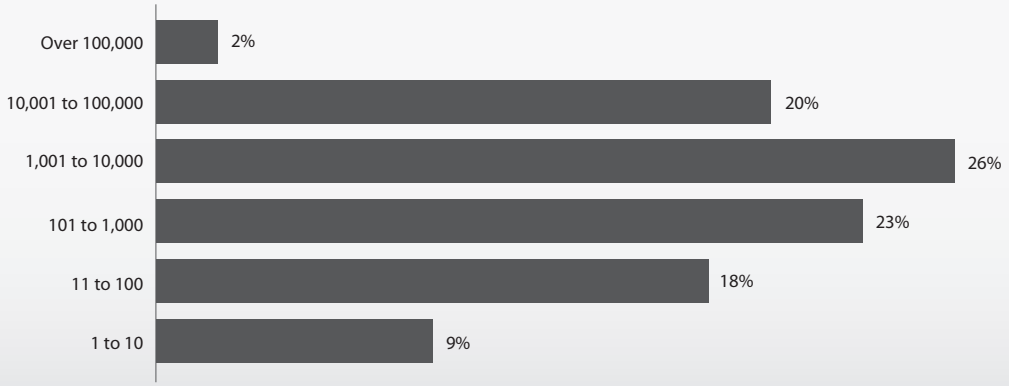
Bulgaria	Singapore
Egypt	Sweden
Italy	

The bottom line is that where disclosures occur, they often require investigations, which sometimes require external investigators, which, in turn, means breaches are more likely to show up in this study. As in previous years, the majority of cases investigated by Verizon in 2009 have not yet been disclosed and may never be. Only a handful of breaches outside the U.S. were publicly reported. Of those, two did so because they were regional facilities of U.S.-based organizations.

Figure 4 shows that, once again, a breakdown of organizational size follows a rather normal-looking distribution. It's quite possible (and perhaps logical) that an organization's size matters little in terms of its chances of suffering a data breach. One might speculate that smaller budgets mean less security spending but it probably also means fewer assets to protect and a lower profile. Thieves are more likely to select targets based on the perceived value of the data and cost of attack than victim characteristics such as size.

Over half of the breaches investigated by Verizon in 2009 occurred outside the U.S.

Figure 4. Organizational size by percent of breaches (number of employees)



Many of our customers express concern about the security ramifications of mergers, acquisitions, and other major organizational changes (perhaps even more so than normal given economic conditions in recent years). This is understandable as these changes bring together not only the people and products of separate organizations but their technology environments as well. Seamless integration of technology, process, and mind-set certainly has its fair share of challenges. Last year, we reported that 13% of our caseload involved organizations that had recently been involved in a merger or acquisition. In 2009 that figure was 9% and another 9% had restructured in some significant way. While nothing can be claimed or inferred directly from these findings, we believe it is well worth watching this metric over time.

Threat Agents

Threat agents refer to entities that cause or contribute to an incident. There can be more than one agent involved in any incident and their involvement can be malicious or non-malicious, intentional or accidental, direct or indirect. Identifying those responsible for a breach is critical to any forensic investigation, not only for purposes of response and containment, but also for creating current and future defensive strategies. Verizon recognizes three primary categories of threat agents—External, Internal, and Partner.

External: External threats originate from sources outside the organization and its network of partners. Examples include hackers, organized crime groups, and government entities, as well as environmental events such as weather and earthquakes. Typically, no trust or privilege is implied for external entities.

Internal: Internal threats are those originating from within the organization. This encompasses company executives, employees, independent contractors (i.e., 1099 staff), and interns, etc., as well as internal infrastructure. Insiders are trusted and privileged (some more than others).

Partners: Partners include any third party sharing a business relationship with the organization. This includes suppliers, vendors, hosting providers, outsourced IT support, etc. Some level of trust and privilege is usually implied between business partners.

VERIS Classification Note: If the agent's role in the breach is limited to a contributory error (see note in the Threat Actions section under Error), they 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.

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

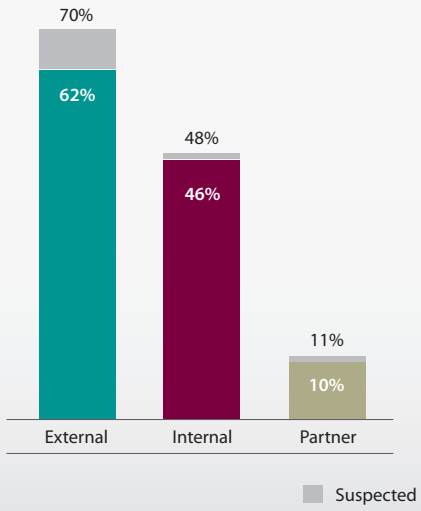


Figure 5 records the distribution of threat agents among breach cases worked by Verizon and the USSS in 2009. Immediately noticeable is a substantial change in the composition of threat agents from previous DBIRs. While these results don't go so far as to justify the "80% Myth[10]" they certainly don't fall in line with the 80/20 external vs. internal ratio that has been a staple of Verizon's caseload. The percentage of breaches attributed to external agents slid 9% (though 70% is not an historical outlier), insiders more than doubled, and partners represent a mere third of their 2008 level. That's a lot of change to digest but this section is dedicated to sorting it all out.

Essentially, there are three possible explanations for these results:

1. They reflect changes in Verizon's caseload
2. They reflect the addition of USSS caseload
3. They are a product of both 1 & 2

We will start with option 1. Figure 6 shows the distribution of threat agents for breaches worked by Verizon over the last five years. From this, it is clear that the lower proportion of external agents is not due to Verizon's caseload, as this statistic hit its highest mark ever in 2009. Neither can it explain the rise for insiders in the merged dataset. The percent of breaches involving partners, however, did drop substantially and for the second year in a row. It is unclear whether this is due to increased awareness of third-party security threats, regulatory guidance focusing on vendor management, a shift in criminal strategy, a change in Verizon's IR clients, all of the above, or none of the above. Whatever the reason(s), we view it as a positive outcome and hope this problem is being reigned in.

The changes evident for threat agents in 2009 stem partially from a drop in partners within Verizon's caseload but mostly from the addition of a materially different USSS dataset.

10 http://taosecurity.blogspot.com/2009/05/insider-threat-myth-documentation.html

Figure 6. Threat agents over time by percent of breaches

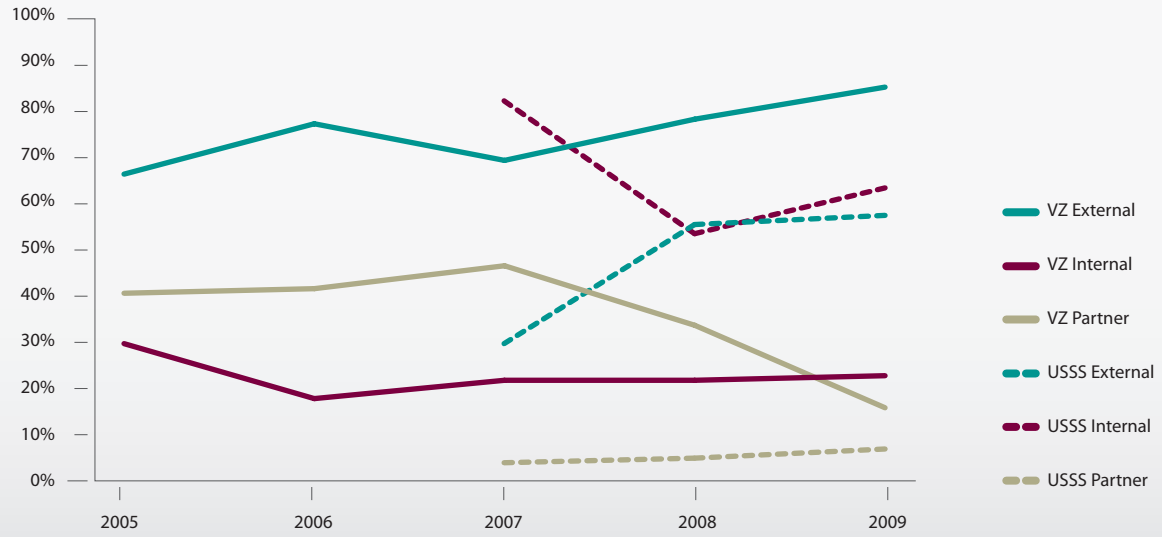
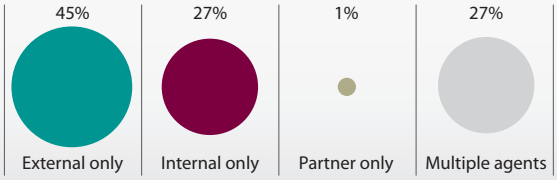


Figure 6 also shows the same information discussed in the preceding paragraph for USSS cases (see dashed lines). Undoubtedly, the changes in Figure 5 are largely due to the inclusion of the USSS caseload, as their results show a strong representation of internal threat agents, comparatively fewer outsiders, and a very low percentage of partner-related breaches. As a law enforcement agency, it would follow that the USSS would have a different perspective on the broader security incident population. For example, an organization suffering a data breach due to the actions of an insider (especially if that insider is part of an easily-identified list of suspects or used simple methods to perpetrate the crime) is more likely to call law enforcement directly. If true, this would reinforce the assertions and findings of some, especially law enforcement agencies, that insiders are a more frequent source of incidents than stats released by external parties like Verizon often show. In addition, it's also important to consider the impact of disclosure laws on the proportions represented in the various datasets.

So, if #1 has some truth to it and #2 is wholly true, then #3 must be the best option. The changes evident for threat agents in 2009 stem partially from a drop in partners within Verizon's caseload but mostly from the addition of a materially different USSS dataset. As stated in the beginning of this report, our motivation in studying a larger sample is to better understand the biases of our own and to gain a more complete and accurate representation of the entire population of breaches. These results are clearly the product of that larger perspective.

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



Following this discussion, there are a few observations to note regarding Figure 7 which contrasts single and multi-agent breaches. The 27% of cases involving more than one agent is well below the 2008 level of 39%. Though not apparent from the figure itself, most multi-agent breaches worked by Verizon exhibit an external-partner combination. In most of these, partner assets are compromised by an external agent and used to attack the victim. On the other hand, external-internal is far more common in USSS cases. As will be discussed later in this report, this scenario often involves an outsider soliciting or bribing an employee to embezzle or skim data and/or funds. Partner-internal pairings are rare within both caseloads.

Breach Size by Threat Agents

Though we do not assert that the full impact of a breach is limited to the number of records compromised, it is a measurable indicator of it. Analysis around financial losses incurred by breach victims is probably the most requested addition to the DBIR. For various reasons[11], forensic investigators do not have nearly as much visibility into this as they have into the immediate details surrounding a breach. We do, however, include metrics for collecting impact data within VERIS and refer interested readers there for more information.

Figure 8. Compromised records by threat agent, 2009

Figure 9. Compromised records by threat agent, 2004-2009

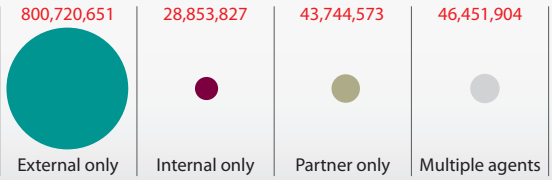


Figure 8 records the distribution of the 143+ million records compromised across the merged 2009 dataset among threat agents. It looks a great deal like it did in our last DBIR. There is not a linear relationship between frequency and impact; harm done by external agents far outweighs that done by insiders and partners. This is true for Verizon and for the USSS and true for this year and in years past. To illustrate this point, we present Figure 9 showing the distribution of the over 900 million compromised records in the merged dataset between 2004 and 2009.

We could provide commentary to Figure 9, but what could it possibly add? If a chart in this report speaks with more clarity and finality we aren't sure what it is.

We could provide commentary to Figure 9, but what could it possibly add? If a chart in this report speaks with more clarity and finality we aren't sure what it is.

11 http://securityblog.verizonbusiness.com/2009/04/16/to-dbir-show-me-the-money/

External Agents (70% of breaches, 98% of records)

Table 1 presents a comparison of the various types of external threat agents identified during 2009 by Verizon and the USSS. The merged results continue to show that external breaches are largely the work of organized criminals. Banding together allows them to pool resources, specialize skills, and distribute the work effort, among other advantages. Figure 10 demonstrates the effectiveness of this approach. Crime has been a business for a very long time. This is just the same old story played out on a different (digital) stage. We refer readers to Appendix A for more information on organized criminal communities.

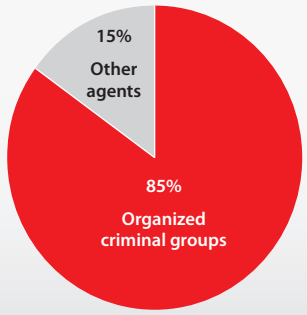
The large proportion of "unknown" in Table 1 is the result of several factors. Sometimes the particular type of agent cannot be determined. Sometimes the victim does not wish to spend time or money toward making this determination. The USSS contains far fewer "unknown" agents due to their role in identifying and prosecuting suspects.

In terms of the role external agents played in 2009 breaches, 84% participated directly in the attack. The rest solicited another agent to perpetrate the attack or supported it in some other manner. Scenarios of this are discussed elsewhere in this report.

Table 1. Types of external agents by percent of breaches within External

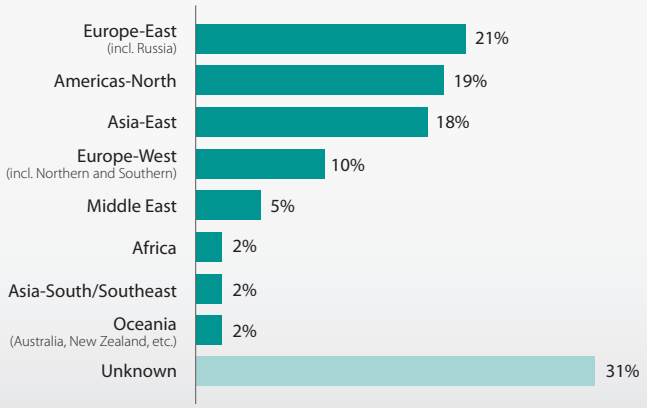
Organized criminal group	24%
Unaffiliated person(s)	21%
External system(s) or site	3%
Activist group	2%
Former employee (no longer had access)	2%
Another organization (not partner or competitor)	1%
Competitor	1%
Customer (B2C)	1%
Unknown	45%

Figure 10. Percent of compromised records attributed to organized crime



Banding together allows criminal groups to pool resources, specialize skills, and distribute the work effort, among other advantages. Crime has been a business for a very long time. This is just the same old story played out on a different (digital) stage.

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



Pinpointing the geographic origin of these attacks can be problematic, especially when it hinges mainly on source IP addresses. Fortunately, forensic investigators—and especially law enforcement agencies—often have much more to go on than that. Even if we accept that the IP address that shows up in log files does not belong to the actual machine of the actual threat agent (i.e., it is a bot controlled by the agent), it is still informative and potentially useful for defensive purposes. Figure 11 shows the regional origin of relevant external attacks.

Once again, more breaches originate from East Europe than any other region (although North America and East Asia remain a close #2 and #3). Comparing "type" and "origin" reveals some interesting findings. For instance, most organized criminal groups hail from East Europe, while unidentified and unaffiliated persons often come from East Asia. Finally, it is worthy of mention that within Verizon's caseload, East Asia rose to the top spot for the first time in 2009.

THERE MUST BE SOME MISTAKE—WHERE'S APT?

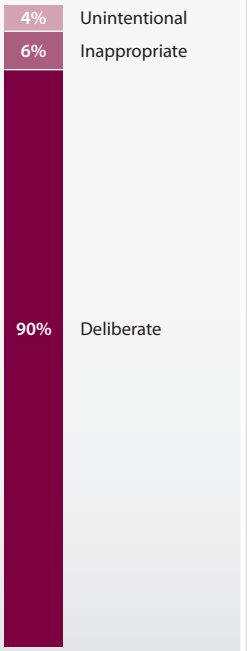
Despite the huge amount of buzz around Advanced Persistent Threats (APT) this year, neither the term nor the concept is new. Due to this attention, we imagine more than one pair of eyes scanned the list of external agent types in search of "APT." One of the difficulties with APT is that, though it may have an official definition, its use in everyday practice varies widely. By it, some refer strictly to nation-states, some to any highly skilled attacker, some to particularly difficult methods of attacks or their unrelenting nature. We're not interested in arguing about the definition. We simply want to explain why it is not listed in any figure or table in this report. Rather than identifying an "APT attack," VERIS classifies threat agents and their actions in a descriptive manner. If interested, you can see glimpses of "APT-ish elements" throughout this report. Look at the types and origins of external agents (note the absence of the "government" category that is an available option in VERIS), examine the types and vectors of threat actions, read our assessments of attack difficulty, notice the length of time that passes from compromise to discovery, and check out the anti-forensics section. These areas might not be stamped with the acronym "APT" but we do believe them to "apt-ly" describe breaches investigated by Verizon and the USSS in 2009.

Internal Agents (48% of breaches, 3% of records)

Of cases involving internal threat agents in 2009, investigators determined 90% were the result of deliberate and malicious activity. This finding does not mean that insiders never unintentionally contribute to breaches; they very often do. As discussed earlier, our method of classification does not consider insiders to be an active part of the event chain if their role is limited to contributory error. Inappropriate actions include policy violations and other questionable behavior that, while not overtly malicious, can still result in harm to information assets. Not only can inappropriate behavior contribute directly to a breach, but it may also be an ill omen of what's to come. Over time investigators have noticed that employees who commit data theft were often cited in the past for other "minor" forms of misuse (or evidence of it was found and brought to light during the investigation).

Recently, many have hypothesized that insider crime would rise due to financial strain imposed by global economic conditions. Hard times breed hard crimes as they say. It is entirely possible that this is occurring, but neither the Verizon nor USSS caseload show evidence of it. As seen back in Figure 6, Verizon shows a flat trend for insiders and the USSS shows a downward trend over the last three years. Nevertheless, it is a logical hypothesis and worthy of further study.

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



Analyzing the types of insiders behind breaches yields a great deal of practical information. Each of the types listed in Table 2 represent a certain inherent mix of skills, duties, privileges, etc., all of which speak to the capabilities and resources of that agent and the safeguards most relevant to them. Traditionally, we have seen a large and fairly even proportion of system/network administrators to regular users with a few other types mixed in occasionally. 2009 results are substantially different and, no surprise, this is largely due to USSS data. Specifically, it is related to the types of internal crime investigated by the USSS (see the Misuse section under Threat Actions for a more detailed discussion). As a result, regular employees were responsible for a much larger share (51%) of breaches. These cases typically involved bank tellers, retail cashiers, and other similar personnel taking advantage of their everyday job duties to skim, embezzle, or otherwise steal data from their employers.

Recently, many have hypothesized that insider crime would rise due to financial strain imposed by global economic conditions. Hard times breed hard crimes as they say. It is entirely possible that this is occurring, but neither the Verizon nor USSS caseload show evidence of it.

Finance and accounting staff are similar to regular employees in terms of IT privileges but we differentiate them due to the higher privileges of another sort. Their oversight and management of accounts, records, and finances affords them great propensity for harm. Executives are in a similar position. Though outside the scope of this study, devious acts committed by such employees have caused far more damage to businesses than IT-related incidents.

While it is clear that pulling off an inside job doesn't require elevated privileges, evidence consistently supports that they do facilitate the bigger ones. Overall, insiders were not responsible for a large share of compromised records but system and network administrators nabbed most of those that were. This finding is not surprising since higher privileges offer greater opportunity for abuse. In general, we find that employees are granted more privileges than they need to perform their job duties and the activities of those that do require higher privileges are usually not monitored in any real way.

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%

It is worth noting that while executives and upper management were not responsible for many breaches, IP and other sensitive corporate information was usually the intended target when they were. These acts were often committed after their resignation or termination.

Speaking of that, across all types of internal agents and crimes, we found that 24% was perpetrated by employees who recently underwent some kind of job change. Half of those had been fired, some had resigned, some were newly hired, and a few changed roles within the organization. With respect to breaches caused by recently terminated employees, we observed the same scenarios we have in the past: 1) the employee's accounts were not disabled in a timely manner, and 2) the employee was allowed to "finish the day" as usual after being notified of termination. This obviously speaks to the need for termination plans that are timely and encompass all areas of access (decommissioning accounts, disabling privileges, escorting terminated employees, forensic analysis of systems, etc.).

THE SLIPPERY SLOPE OF INSIDER MISCONDUCT

Verizon investigated a case in which a recently terminated system administrator stole sensitive data from his former employer as well as personal information belonging to its customers. He then attempted to blackmail the organization and threatened to go public with the information if they did not meet his demands. Obviously, not a good situation but what makes it worse is that it might have been avoided with a few changes in policy and practice. On several occasions in the past, this employee had been cited for IT policy violations and inappropriate behavior. There were harassment complaints against him filed by other employees. Finally, when he stole a co-worker's password for a popular social networking site and modified it with slanderous content, he was let go. Unfortunately, his generic administrative account was given to his successor with a minor password change (i.e., "Password2" instead of "Password1") and we've already covered what happened after that.

Partner Agents (11% of breaches, 1% of records)

As discussed already, partner-related breaches are down in comparison to previous years. When partners are a factor, the Verizon and USSS cases have differing perspectives as to their role. Verizon's findings continue to show that the majority of breaches involving partners are the result of third-party information assets and accounts being "hijacked" by another agent and then used to attack victims. This frequently involves a remote access connection into the victim's systems. If compromised, the malicious agent's actions would appear to come from a trusted source and therefore be even more difficult to detect and prevent. Poor partner security practices usually allow or worsen these attacks.

Organizations that outsource their IT management and support also outsource a great deal of trust to these partners. In the end, what we said last year remains true; poor governance, lax security, and too much trust is often the rule of the day. Outsourcing should not mean "Out of sight, out of mind."

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

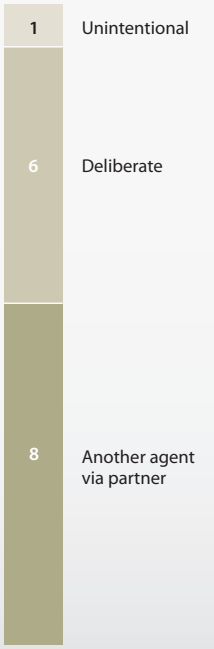


Table 3. Types of partner agents by percent of breaches within Partner

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

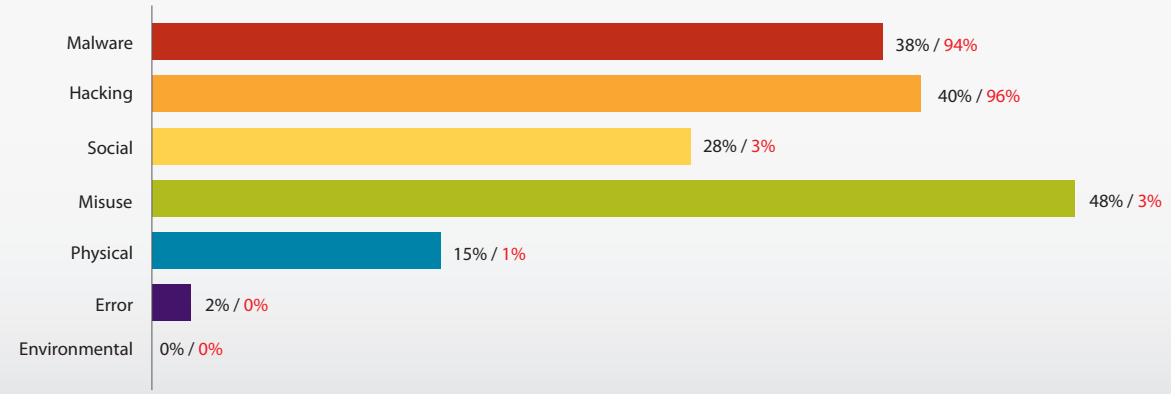
The USSS caseload, on the other hand, shows most partner breaches stem from the deliberate and malicious actions of that partner. An example of this might be a third-party system administrator who maliciously misuses her access to steal data from the victim. We believe that the merged data set balances these two extremes to arrive at the ratio shown here.

The types of partners in each dataset parallel the differences described above. Partners that manage systems are by far the most common offenders, whether their role is accidental or deliberate. Assets often involved in these breaches are point-of-sale systems within the hospitality and retail industries. Organizations that outsource their IT management and support also outsource a great deal of trust to these partners. In the end, what we said last year remains true; poor governance, lax security, and too much trust is often the rule of the day. Outsourcing should not mean "Out of sight, out of mind."

Threat Actions

Threat actions describe what the threat agent did to cause or contribute to the breach. There are usually multiple actions across multiple categories during a breach scenario. Verizon uses seven primary categories of threat actions, which are depicted in Figure 14 along with the percent of breaches and compromised records associated with each.

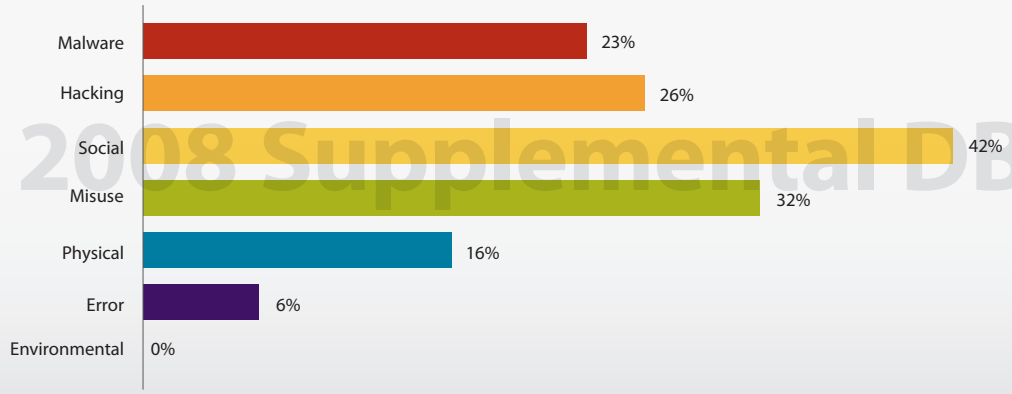
Figure 14. Threat action categories by percent of breaches and records



As with the findings for threat agents, we imagine Figure 14 raises some eyebrows among those familiar with previous versions of this report. Before going any further, we'd like to direct attention to Figure 15 to see if we can turn some of those raised eyebrows into head nods and an "ah-ha" or two. In the 2008 Supplemental DBIR, we presented all the same basic statistics as in the original report except sliced up by industry. Figure 15 shows the prevalence of threat actions in Financial Services from that report. Though by no means a mirror image of Figure 14, it does demonstrate that a dataset containing a large proportion of financial organizations will exhibit a more "balanced" mix of threat actions and higher values in the Misuse and Social categories. On the other hand, the Retail and Hospitality industries are very lopsided toward Hacking and Malware. Therefore, Figure 14 is not a new trend or sudden change in the threat environment. It aligns perfectly well with what we would expect of a merged Verizon-USSS dataset that contains a higher-than-normal proportion of financial organizations.

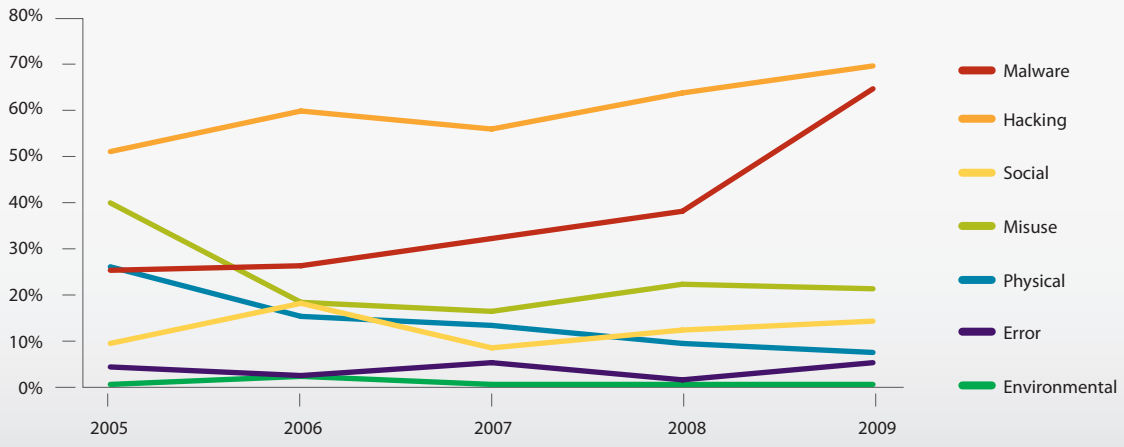
This is quite a sobering statistic but one that adds yet another chapter to a story we already know: In the big breaches, the attacker hacks into the victim's network (usually by exploiting some mistake or weakness) and installs malware on systems to collect (lots of) data. That the USSS cases tell the same story certainly makes it more compelling though.

Figure 15. Flashback: Threat action categories by percent of breaches in Financial Services as shown in the 2008 Supplemental DBIR



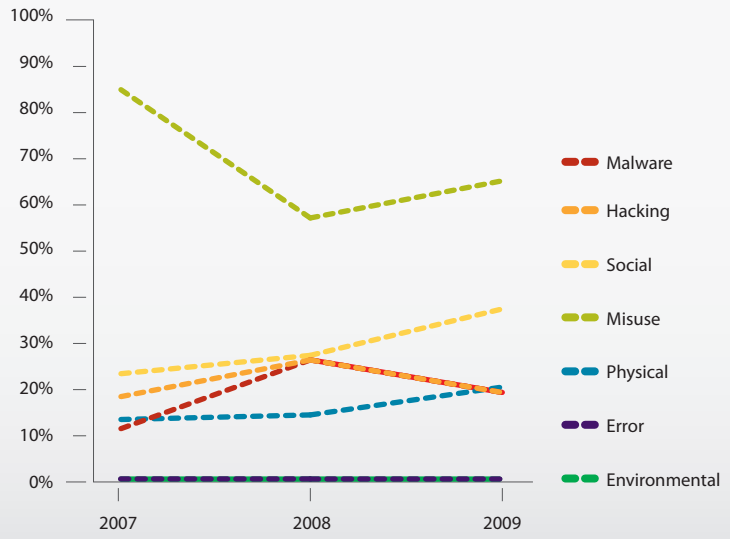
Though less prevalent than in previous reports, Hacking and Malware are even more dominant than normal with respect to compromised records. This is quite a sobering statistic but one that adds yet another chapter to a story we already know: In the big breaches, the attacker hacks into the victim's network (usually by exploiting some mistake or weakness) and installs malware on systems to collect (lots of) data. That the USSS cases tell the same story certainly makes it more compelling though.

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



Those wishing to compare 2009 results to previous years for Verizon's caseload can do so in Figure 16. Another version of the same chart is provided for the three years for which we have data from the USSS *(Figure 17)*. The most noticeable change in 2009 among breaches worked by Verizon was a substantial upswing in malware. For the most part, USSS trends held steady, with Social and Misuse showing some growth while Hacking and Malware declined slightly. The following sections provide a more in-depth analysis of each threat action category.

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



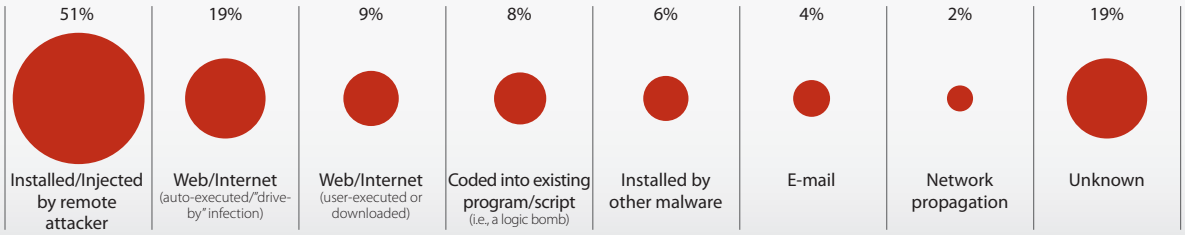
Malware (38% of breaches, 94% of records)

Malware is any software or code developed for the purpose of compromising or harming information assets without the owner's informed consent. It factored into 38% of 2009 cases and 94% of all data lost. When malware is discovered during an investigation, the IR team often works with ICSA Labs, an independent division of Verizon, to conduct the analysis. Through this collaboration, investigators are able to better help the customer with containment, removal, and recovery. Malware can be classified in many ways but we utilize a two-dimensional approach that identifies how it was distributed (infection vector) and what the malware did (functionality). These characteristics have a direct bearing on preventive measures.

Infection Vectors

Per Figure 18, the most frequent malware infection vector is once again installation or injection by a remote attacker. This is often accomplished through SQL injection or after the attacker has root access to a system. Both have the troublesome ability to evade antivirus (AV) software and other traditional detection methods, which has a lot to do with their consistent place at the top of this list.

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



The web continues to be a common path of infection. Among web-based malware, we distinguish auto-executed "drive-by downloads" from those involving user interaction. Many of the latter incorporate a social engineering aspect ("click to clean your system"). The web installation vector is more opportunistic in nature than the "installed by attacker" variety that usually targets a pre-selected victim. Once the system is infected, the malware alerts an external agent who will then initiate further attacks. The web is a popular vector for the simple reason of that's where the users are. Overly-trusting browsers and users operating with administrative privileges only add to this popularity.

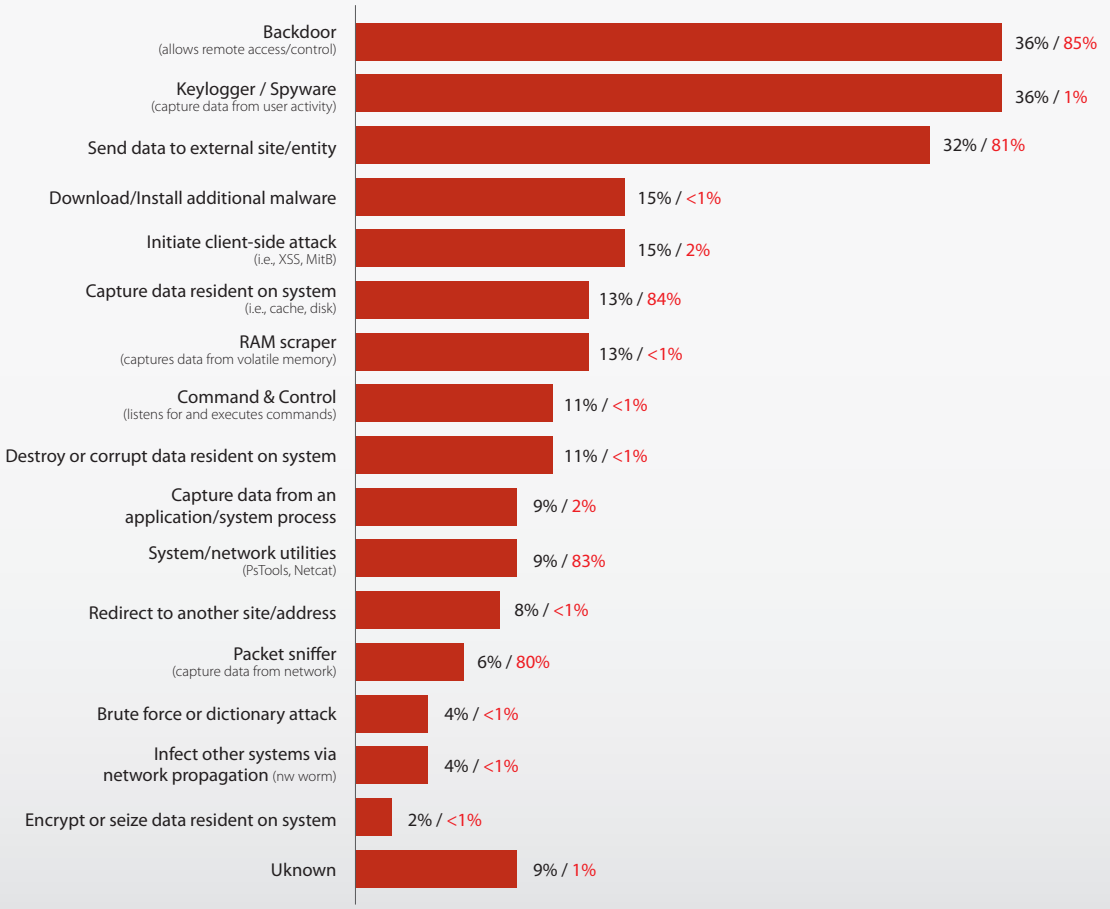
While not extremely common, we did observe several cases in which malware was coded directly into an existing program or script. This, of course, requires access to the system but also knowledge of how the code works. Not surprisingly, these often involve malicious insiders who developed the code or administer the system on which it runs. However, a few very interesting cases of this type were committed by outsiders. One of these involved an external agent that had access to the system for over six months. During this time, he studied the input/output process and developed a custom script to siphon data when new accounts were created.

The rather high percentage of "unknown" in Figure 18 is attributable to many factors. Many times there were no logs, corrupted evidence, and/or users were unavailable for interview. Occasionally, we see some of the "old school" infections vectors like e-mail and network propagation. Outside the world of data breaches, these are still alive and well but when stealth is critical and persistence is the goal, these vectors have less merit.

Malware Functionality

To better capture the intricacies of modern malware, we have defined a more detailed set of functions in the VERIS framework than in previous years. At a broad level though, malware still serves three basic purposes in data breach scenarios: enable or prolong access, capture data, or further the attack in some manner.

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



In terms of enabling access, backdoors were logically atop the list again in 2009 (tied with keyloggers). Backdoors allow attackers to come and go as they please, install additional malware, wreak havoc on the system, retrieve captured data, and much more. Their effectiveness is evidenced by the large percentage of data loss involving backdoors.

Criminals are also getting more proficient and prolific in developing methods to capture data. This can be seen in Figure 19, where many of the functions listed focus on this. Keyloggers and spyware that record user activity were frequent but not involved in some of the larger cases in 2009. This is quite a change from 2008 where they were associated with over 80% of data compromised. "Associated" is the operative word here as keyloggers don't usually steal the bulk of data themselves but instead are used to gain access to install other types of malware for that purpose (i.e., packet sniffers). When malware captures

data on the system (13% of cases), it often does so from forms that cache credentials and other sensitive info. Though only used in some of the smaller cases in 2009, the use of "RAM scrapers" to capture data from a system's volatile memory, continues to increase (13%). We refer the reader to our 2009 Supplemental DBIR for more information on this type of malware. Packet sniffers, while not as common as other varieties of malware, continue to compromise large numbers of records and are usually a factor in the bigger breaches. Malware that "Captures data from an application/system process" (9%) is often associated with the "Coded into existing program/script" infection vector discussed above.

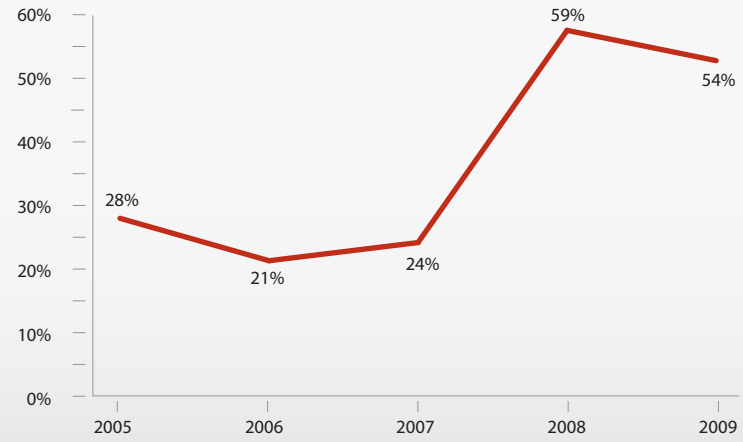
The last major grouping of malware encompasses functions that facilitate the attack in some manner. As is evident, malware often sends data to an external entity (32%). This is sometimes stolen data (like credentials) but is also used to let an attacker know that a system is compromised. We also observed several cases in which malware was used to perform client-side attacks such as man-in-the-browser and cross-site scripting. When malware downloads additional code (15%), it is often in the form of updates or capability extensions. Attackers seem to have an affinity for system and network utilities like PsTools and Netcat. Though these tools are not inherently malicious, criminals are deploying and using them in that way. To clarify, if utilities were added to the system by an attacker, they are listed here under malware. If they were already on the system and were abused as a part of the attack, this would show up under Hacking (i.e., via OS Commanding). It is very interesting to note that there were no confirmed cases in which malware exploited a system or software vulnerability in 2009 (though it was suspected based on partial samples that three may have done so).

In terms of malware furthering the attack, our investigations continue to highlight the importance of detecting and responding to malware quickly. In some incidents, the affected company missed an opportunity to lessen the aftermath of infection by ignoring or not adequately investigating initial antivirus alerts. Regrettably, those alerts sound less often these days.

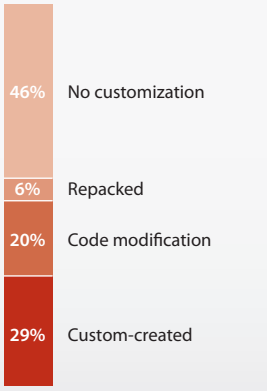
HOW DO THEY GET MY DATA OUT?

When malware captures sensitive information, it must then be exfiltrated from (or taken out of) the victim's environment. There are two basic ways this happens: either the malware sends it out of the organization or the attacker re-enters the network to retrieve it. The general rule of thumb is that smaller packets are sent out (i.e., credentials captured by keyloggers) while larger hauls of data are retrieved (i.e., data collected by a packet sniffer). While any amount of data leaving the owner's possession is never a good thing, the act does (or at least can) provide evidence of foul play. It's a matter of looking for the right indicators in the right places. We advocate paying attention to what goes out of your network and what changes take place within your systems. Don't have any customers or partners in Eastern Europe yet periodic bursts of traffic are sent there from your networks? What about those ZIP or RAR files that showed up last week and have been growing steadily ever since? Maybe there's a perfectly good explanation for these things…but you'll never know unless you take steps to identify and verify them.

Figure 20. Malware customization over time by percent of breaches within Malware*



Level of malware customization by percent of breaches within Malware*



* Verizon caseload only

Malware Customization

We are not so happy to say that the increase in customized malware we reported last year appears not to be a fluke limited to 2008. 2009 revealed a similar proportion of breaches (54% of those involving malware) and an incredible 97% of the 140+ million records were compromised through customized malware across the Verizon-USSS caseload.

The level of customization apparent in malware varies substantially. Some are simply repackaged versions of existing malware in order to avoid AV detection. From Figure 20, it is evident that many attackers do not stop there. More often than not in 2009, they altered the code of existing malware or created something entirely new. As an example of modified code, we observed several instances of RAM scrapers that were "last year's models" with a few tweaks like the added ability to hide and/or encrypt the output file of captured data. Over the last two years, custom-created code was more prevalent and far more damaging than lesser forms of customization.

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

As a defender, it's hard not to get a little discouraged when examining data about malware. The attackers seem to be improving in all areas: getting it on the system, making it do what they want, remaining undetected, continually adapting and evolving, and scoring big for all the above. We are not, however, totally devoid of hope. A major improvement would be to keep attackers from ever gaining access to the system before they are able to install malware. This, of course, is not without its own challenges as will be discussed next.

Hacking (40% of breaches, 94% of records)

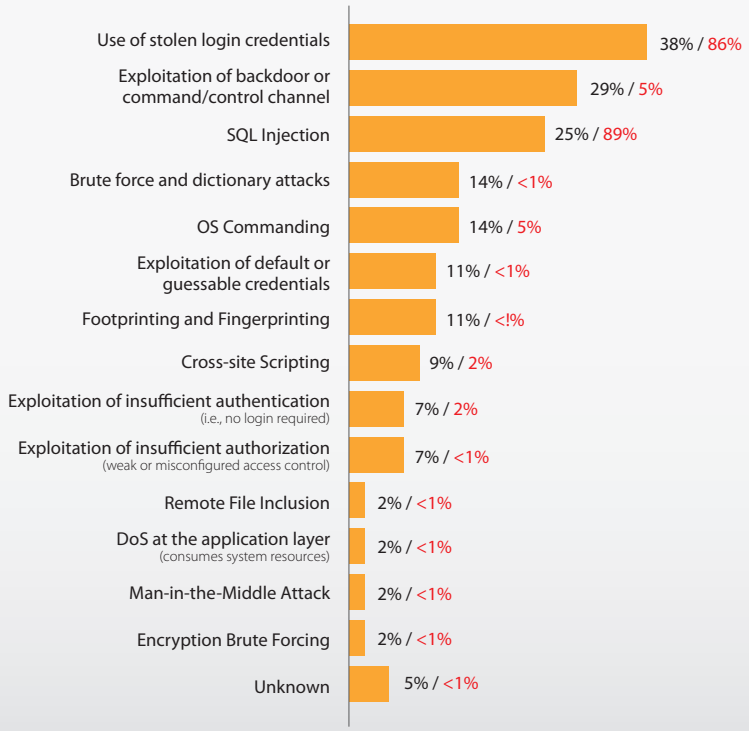
VERIS Classification Note: There is an action category for Hacking and for Misuse. Both can utilize similar vectors and achieve similar results; in Misuse, the agent was granted access (and used it inappropriately) whereas with Hacking access was obtained illegitimately.

Actions in the Hacking category encompass all attempts to intentionally access or harm information assets without (or in excess of) authorization by thwarting logical security mechanisms. Hacking affords the criminal many advantages over some of the other categories; it can be accomplished remotely and anonymously, it doesn't require direct interaction or physical proximity, and there are many tools available to automate and accelerate attacks. The latter lowers the learning curve and allows even less-skilled threat agents to cause a lot of trouble. In this section, we examine the types of hacking observed by Verizon and the USSS in 2009, the paths through which these attacks were conducted, and other details about this important category.

Types of Hacking

The attacks listed in Figure 21 will look a bit different to those familiar with previous DBIRs. The changes are due to our effort to standardize on a classification system for hacking methods in connection with the public release of VERIS. Internally, we had more freedom to simply describe what we observed in our caseload but in order for the USSS (and hopefully others) to use VERIS a more formal approach was necessary. The resulting list (which is not shown here in its entirety) is not exhaustive, as detailed as it could be, or perfect. It is, however, useful for most attacks and provides enough specificity for the intended purpose. It is derived from our own work and from open attack taxonomies from the Web Application Security Consortium (WASC), the Open Web Application Security Project (OWASP), and the Common Attack Pattern Enumeration and Classification (CAPEC) from Mitre. Cross-referencing these is not a quick, easy, or conflict-free process. The list of hacking types in VERIS uses the WASC Threat Classification v2.0 as a baseline[12] and pulls from the others to round out areas not addressed in WASC (i.e., non-application attacks). We refer users to the links above for definitions and examples.

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



12 Thanks to Jeremiah Grossman and Robert Auger from WASC for volunteering their time to serve as a sounding board on attack classification matters.

Evident from Figure 21, there are two standout types of hacking responsible for the majority of breaches and stolen records in 2009—SQL injection and the use of stolen credentials. Both were among the top offenders in our previous report but this year sees them at a whole new level.

The use of stolen credentials was the number one hacking type in both the Verizon and USSS datasets, which is pretty amazing when you think about it. There are over 50 types recognized in the VERIS framework—how can two completely different caseloads show the same result? We have our theories. One of the main reasons behind this is the proliferation of password-gathering malware like Zeus. In fact, though phishing, SQL injection, and other attacks can and do steal credentials, malware nabbed more than all others combined by a ratio of 2:1. There is much more discussion of this in the malware section. Stolen credentials offer an attacker many advantages, not the least of which is the ability to disguise himself as a legitimate user. Authenticated activity is much less likely to trigger IDS alerts or be noticed by other detection mechanisms. It also makes it easier to cover his tracks as he makes off with the victim's data.

Though phishing, SQL injection, and other attacks can and do steal credentials, malware nabbed more than all others combined by a ratio of 2:1.

SQL injection is a technique for controlling the responses from the database server through the web application. At a very high level, the attacker inserts another SQL statement into the application through the web server and gets the answer to their query or the execution of other SQL statements. SQL injection is almost always an input validation failure. If the application trusts user input and does not validate it at the server, it is likely to be vulnerable to SQL injection, cross-site scripting, or one of the other input-validation vulnerabilities. In data breach scenarios, SQL Injection has three main uses: 1) query data from the database, 2) modify data within the database, and 3) deliver malware to the system. The versatility and effectiveness of SQL Injection make it a multi-tool of choice among cybercriminals.

HAPPY 10TH BIRTHDAY SQL INJECTION!

Though first discussed publicly on Christmas Day in 1998, the first advisory on SQL injection was released in 1999. So, perhaps we should say "Happy (belated) 10th birthday" to one of the most widespread and harmful attack methods we've investigated over the years. However, we'd like to alter the customary birthday jingle tagline and instead hope that "not many more" will follow.

The secret to SQL injection's longevity and success is due to a combination of many factors. It's not a terribly difficult technique, making it available to a large pool of miscreants. It exploits the inherently necessary functions of websites and databases to accept and provide data. It can't be fixed by simply applying a patch, tweaking a setting, or changing a single page. SQL injection vulnerabilities are endemic, and to fix them you have to overhaul all your code. Needless to say, this is difficult and sometimes nigh impossible if it is inherited code. There are some tools to help, but it still comes down to coding and developer knowledge. Unfortunately, training gets cut when budgets get tight and application testing is forfeited or compressed to make up time in overdue development projects. All in all, not an easy concoction to swallow but just passing the cup isn't working either. The data in this report testify to the fact that there are many people on the Internet willing to do application testing for you if you don't. Let's pay the good guys instead and make sure SQL injection doesn't live through many more birthdays.

Exploitation of backdoors is another common method of network and system intrusion. In most cases a backdoor is created as a function of malware that was installed at an earlier stage of the attack. The agent then has control of or can access the system at will. It accomplishes the goals of concealment and persistence that cybercriminals crave. As in years past, we most often see backdoors utilized to exfiltrate data from compromised systems.

OS Commanding involves running programs or commands via a web application or through the command prompt after gaining root on a system. Obviously not a capability one wants to grant to an adversary. It can also be used to manipulate systems utilities such as PsTools and Netcat that are legitimately on a system or that have been placed there by the attacker.

What may be striking to many of our readers is the drop in "exploitation of default or guessable credentials" since our last report. This was the most common type in the Hacking category last year and responsible for over half of records breached. It was still fairly common in 2009 but associated with only a fraction of overall data loss (<1%). The drop seems to correspond with fewer cases in the Retail and Hospitality industries stemming from third party mismanagement of remote desktop connections to POS systems.

Vulnerability Exploits

In the past we have discussed a decreasing number of attacks that exploit software or system vulnerabilities versus those that exploit configuration weaknesses or functionality. That downward trend continued this year; so much so, in fact, that there wasn't a single confirmed intrusion that exploited a patchable[13] vulnerability. On the surface this is quite surprising—even shocking—but it begins to make sense when reviewing the types of hacking discussed above. SQL injection, stolen credentials, backdoors, and the like exploit problems that can't readily be "patched."

There wasn't a single confirmed intrusion that exploited a patchable[15] vulnerability.

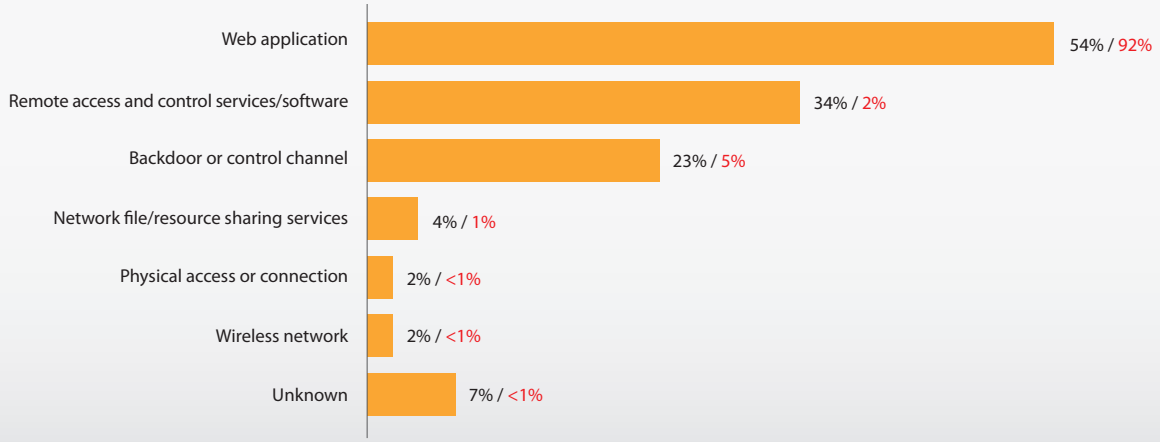
Organizations exert a great deal of effort around the testing and deployment of patches—and well they should. Vulnerability management is a critical aspect of any security program. However, based on evidence collected over the last six years, we have to wonder if we're going about it in the most efficient and effective manner. Many organizations treat patching as if it were all they had to do to be secure. We've observed companies that were hell-bent on getting patch x deployed by week's end but hadn't even glanced at their log files in months. This kind of imbalance isn't healthy. Therefore, we continue to maintain that patching strategies should focus on coverage and consistency rather than raw speed. The resources saved from doing that could then be put toward something more useful like code review and configuration management.

13 The word "patchable" here is chosen carefully since we find that "vulnerability" does not have the same meaning for everyone within the security community. While programming errors and misconfigurations are vulnerabilities in the broader sense, lousy code can't always be fixed through patching and the careless administration patch has yet to be released. Furthermore, many custom-developed or proprietary applications simply do not have routine patch creation or deployment schedules.

Attack Pathways

After being edged out in 2008 as the most-used path of intrusion, web applications now reign supreme in both the number of breaches and the amount of data compromised through this vector. Both Verizon and USSS cases show the same trend. This falls perfectly in step with the findings pertaining to types of attacks discussed above. Web applications have the rather unfortunate calling to be public-facing, dynamic, user-friendly, and secure all at the same time. Needless to say, it's a tough job.

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



Remote access and control solutions also present challenges. On one side stands the organization's internal assets and on the other side a perfectly benign and trusted entity. Well, as evidenced by these results, that last part is not always true and therein lies the rub. Because these solutions are so often picked on and because there are many different types of them, we gathered a bit more detail during 2009. This is what we found:

- Third party remote desktop software (i.e., LogMeIn) – 13%
- Native remote desktop services (i.e., VNC) – 9%
- Remote access services (i.e., VPN) – 13%

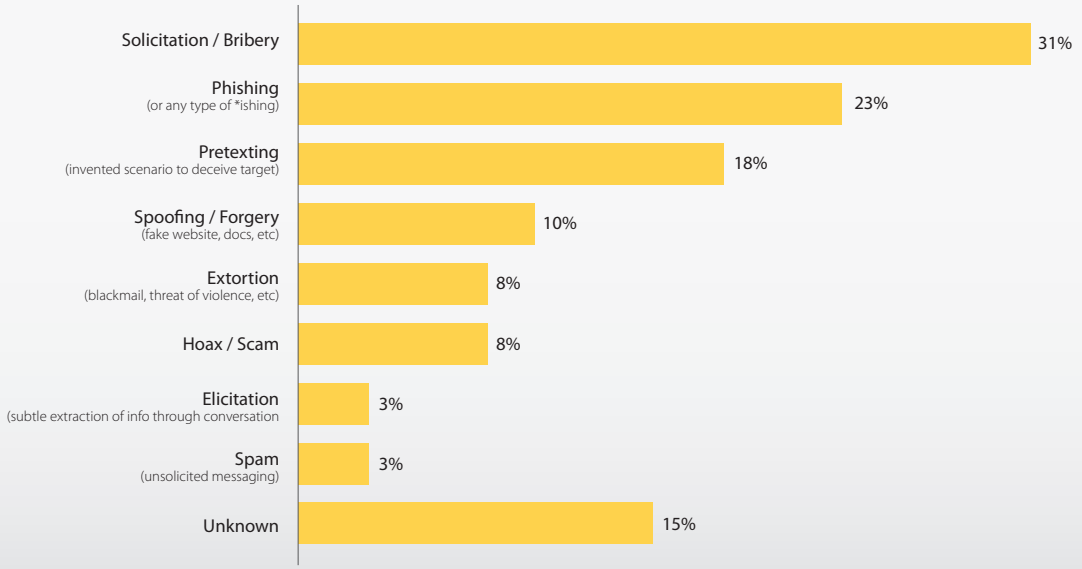
Backdoors were discussed briefly above and more fully in the Malware section. Since their entire existence is to allow malicious agents to traverse the perimeter unnoticed, it's hardly surprising they are a common vector of intrusion. This marks the third year in a row that only a single incident occurred in which wireless networks were used to infiltrate organizational systems. It was completely open. The physical access or connection vector may seem odd in combination with hacking but there are instances in which this comes into play. For instance, one case involved connecting two systems and running a cracking utility against the SAM database on the target system.

Social (28% of breaches, 3% of records)

Social tactics employ deception, manipulation, intimidation, etc. to exploit the human element, or users, of information assets. These actions are often used in conjunction with other categories of threat (i.e., malware designed to look like antivirus software) and can be conducted through technical and non-technical means. Within the past year, social tactics played a role in a much larger percentage (28% vs. 12% in 2008) of breaches, due mainly to the addition of the USSS cases.

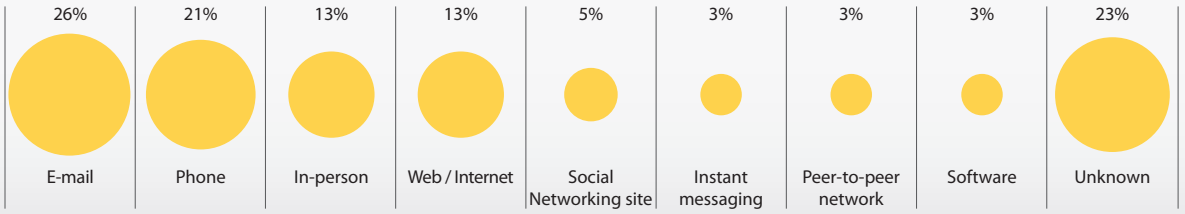
VERIS Classification Note: Those familiar with the 2008 and 2009 DBIRs may recognize this as a new category. This category was previously referred to as Deceit; we believe the change better reflects the broad nature of human-targeted threats.

Figure 23. Types of social tactics by percent of breaches within Social



As seen in Figure 23, solicitation and bribery occurred more often than any of the other types of social tactics recognized by the VERIS framework. This may seem odd, but the explanation is quite simple; these were scenarios in which someone outside the organization conspired with an insider to engage in illegal behavior (usually embezzlement as seen in the next section). According to the USSS, these are usually organized criminal groups conducting similar acts against numerous organizations. They recruit, or even place, insiders in a position to embezzle or skim monetary assets and data, usually in return for some cut of the score. The smaller end of these schemes often target cashiers at retail and hospitality establishments while the upper end are more prone to involve bank employees and the like. Other common social tactics observed in 2009 were phishing and pretexting. These are classic attacks that have been discussed extensively in our previous reports.

Figure 24. Paths of social tactics by percent of breaches within Social



Similar to last year's report, e-mail is still the vector of choice for conducting social attacks. The criminals also apparently like to maintain that personal touch by using the phone or even in-person contact with the victims to get the information they need. Security concerns around social networking sites have been discussed quite frequently of late, but this vector did not factor prominently into breach cases worked by Verizon or the USSS. However, the seemingly non-stop growth of these sites, their extensive use from corporate assets, and the model they employ of inherently trusting everything your "friends" do may be too attractive for criminals to ignore for long. We are interested to see if this vector plays a larger role in data breaches over the next few years.

The targets of social tactics are overwhelmingly regular employees and customers. As in years past, we continue to stress how important it is to train all employees about the various types of social attacks. A security awareness campaign should, at the very least, train them to recognize and avoid falling for the opportunistic varieties like phishing and other scams. Employees in sensitive, trusted, or public-facing positions should also be prepped for more targeted tactics and reminded of corporate policies that (hopefully) deter misconduct. Including social tactics in mock incident or penetration tests can be a good measure of the effectiveness of awareness programs and overall readiness of the organization to thwart these attacks.

Table 4. Targets of social tactics by percent of breaches within Social

Regular employee/end-user	26%
Customer (B2C)	15%
Executive/upper management	5%
System/network administrator	5%
Finance/accounting staff	3%
Helpdesk staff	3%
Unknown	3%

According to the USSS, solicitation usually involves organized criminal groups conducting similar acts against numerous organizations. They recruit, or even place, insiders in a position to embezzle or skim monetary assets and data, usually in return for some cut of the score.

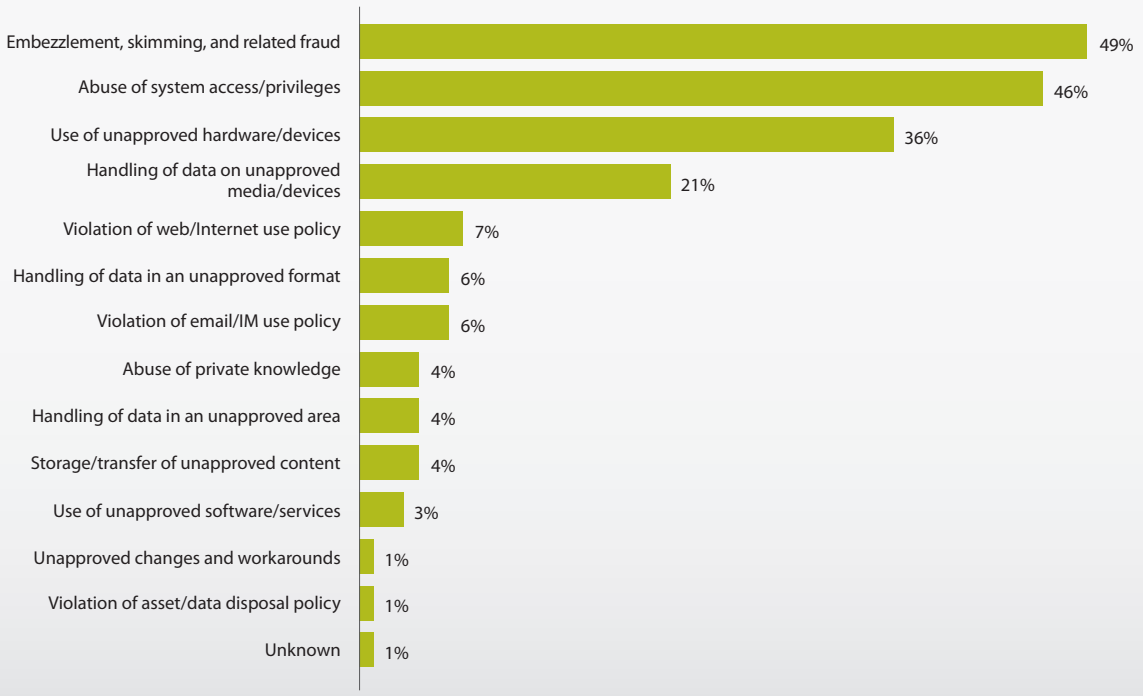
Misuse (48% of breaches, 3% of records)

We define misuse as using organizational resources or privileges for any purpose or in a manner contrary to that which was intended. These actions can be malicious or non-malicious in nature. The category is exclusive to parties that enjoy a degree of trust from the organization like insiders and partners. For the first time since we began this study, Misuse was the most common of all threat actions (48%) in our dataset. It was not, however, responsible for a large proportion of records breached (3%). It may seem strange that such a frequently occurring problem accounts for so small a number of records, but when one considers the circumstances that surround misuse it begins to make sense.

VERIS Classification Note: There is an action category for Hacking and for Misuse. Both can utilize similar vectors and achieve similar results; in Misuse, the agent was granted access (and used it inappropriately) whereas with Hacking, access was obtained illegitimately. Additionally, the line between Misuse and Error can be a bit blurry. In general, the categories divide along the line of intent. Errors are wholly unintentional, whereas Misuse involves willful actions typically done in ignorance of policy or for the sake of convenience, personal gain, or malice.

Embezzlement, skimming, and related fraud were seen more often than other forms of misuse and were exclusive to cases worked by the USSS. These actions were typically perpetrated by employees entrusted with the oversight or handling of financial transactions, accounts, record keeping, etc. Not surprisingly, this often occurred in financial institutions, retail stores, and restaurants. In many cases the use of handheld skimmers and other devices were utilized to facilitate the theft. This accounts for much of the "use of unapproved hardware/devices" depicted in Figure 25. While such activity may not fit some people's notions of cybercrime, cases included in this study did constitute a legitimate data breach. Payment cards, personal information, bank account data, and other sensitive information were compromised and often sold to external parties or used by the insider to commit fraud. It may not be the type of thing readers have come to associate with the DBIR but that is precisely why the addition of the USSS data is so valuable; it lets us study cases we would otherwise never see.

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



The prevalence of embezzlement and skimming is one of the major reasons why the total amount of data compromised through misuse is so comparatively low. An employee engaging in this type of fraud has a completely different M.O. than an uberhacker systematically draining data from a large payment card processor. The employee has a vested interest in keeping their job, remaining undetected, and avoiding prosecution. Siphoning small amounts of data or monetary assets over a longer period of time is more suited to this than a "grab as much as you can and run" approach. Embezzlers also have the luxury of targeting exactly what they want in the amount they want when they want it.

Abuse of system access and privileges follows a close second behind embezzlement. As the name implies, it involves the malicious use of information assets to which one is granted access. System access can be used for any manner of maliciousness but in this report, naturally, its result was data compromise. While common among the USSS' cases (42% of all those involving misuse), it was even more so among Verizon's (67%). Though not apparent from Figure 25, which covers 2009 cases, the abuse of system access tends to compromise much more data than embezzlement and other types of misuse. It often involves system and network administrators (especially the larger breaches) but also other types of employees.

Handling of data on unapproved media and devices was a common type of misuse in both caseloads. It is typically used in conjunction with other forms like "abuse of access" as a convenient way to transport data. Sometimes the devices themselves are contraband but more often the data in question were not approved for storage on an otherwise sanctioned device. We continue to find that the success of a breach does not hinge on the perpetrator being able to use a certain portable device. Unfortunately, insiders have a plethora of choices when it comes to media and devices fit for secreting data out of their employer. For this reason, we have always held that it is easier to control the datasource than the media.

Figure 25 lists several other forms of misuse uncovered during 2009 investigations. Policy violations, storing unapproved content, and other dubious activities can directly breach data (i.e., via personal e-mail accounts) and often pave the way for other badness like the installation of malware. Also, experience shows that employees who willfully engage in "minor" misconduct are often the very same employees engaging in major crimes down the road. Better to establish policies and procedures that nip it in the bud early.

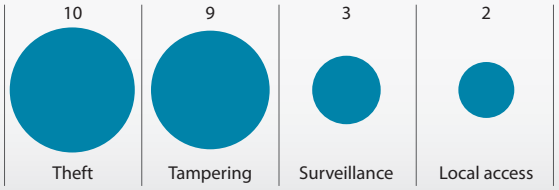
Embezzlement, skimming, and related fraud were seen more often than other forms of misuse and were exclusive to cases worked by the USSS. These actions were typically perpetrated by employees entrusted with the oversight or handling of financial transactions, accounts, recordkeeping, etc.

Physical (15% of breaches, 1% of records)

This category includes human-driven threats that employ physical actions and/or require physical proximity. As in years past, physical attacks continue to rank near the bottom of our list of threat actions. We recognize that this is not in line with what our readers commonly hear and, as we have stated in the past, it is largely due to our caseload. The nature of a great many physical attacks precludes the need for any investigation, and furthermore, they often do not lead to actual data compromise. When regulated information is stored on a stolen laptop, it is considered "data-at-risk" and disclosure is often required. This is true whether or not the criminal actually accessed the information or used it for fraudulent purposes. Our dataset, on the other hand, is comprised of incidents in which compromise was confirmed (or at least strongly suspected based on forensic evidence). The same is true of the USSS' cases, yet the combined dataset still exhibits the highest percentage of physical attacks we've ever reported.

VERIS Classification Note: Natural hazards and power failures are often classified under Physical threats. We include such events in the Environmental category and restrict the Physical category to intentional actions perpetrated by a human agent. This is done for several reasons, including the assessment of threat frequency and the alignment of controls.

Figure 26. Types of physical actions by number of breaches



In almost half of the cases involving physical actions, theft was the type. It would appear that theft is not any more or less prevalent to any particular agent, as we observed external, internal, and partner entities partaking in this crime[14]. Typically, the assets that were stolen were documents, but also frequently included desktop or laptop computers. In our caseload, theft typically occurred in non-public areas within the victim's facility like offices and storage rooms, although there were a few exceptions to this rule.

KNOW YOUR ATTRIBUTES: CONFIDENTIALITY AND POSSESSION

The lost or stolen laptop scenario is one of the reasons we really like the distinction made between Confidentiality and Possession in the "Parkerian Hexad" rather than the more well-known "CIA Triad." In the VERIS framework, we borrow Donn Parker's six security attributes of Confidentiality, Possession, Integrity, Authenticity, Availability, and Utility. The first two perfectly reflect the difference between data-at-risk and data compromise that we so often discuss in these reports. From VERIS:

Confidentiality refers to limited observation and disclosure of an asset (or data). A loss of confidentiality implies that data were actually observed or disclosed to an unauthorized agent rather than endangered, at-risk, or potentially exposed (the latter fall under the attribute of Possession and Control).

Possession refers to the owner retaining possession and control of an asset (or data). A loss of possession or control means that the organization no longer has exclusive (or intended) custody and control over the asset or is unable to adequately prove it. The concept of endangerment (exposure to potential compromise or harm) is associated with this attribute whereas actual observation or disclosure of data falls under confidentiality.

14 A VERIS classification distinction should be made here: If an insider stole assets, funds, or data they were granted physical access to as part of their job duties, we would consider this to be in the "Misuse" rather than "Physical" action category.

Nearly equal in number to theft, all instances of tampering were related to ATM and gas pump skimmers and were unique to the USSS caseload. These are electronic devices that fit over credit card reader slots and often (though not always) work in concert with hidden cameras to capture your account number and PIN. Although some of these devices are rudimentary and crude, others are ingeniously constructed and are incredibly difficult to spot[15]. The cases that involved video surveillance were, as one might expect, all ATMs rather than gas pumps. The majority of these occurred in outdoor areas at the victim location such as an ATM located outside of a bank. This type of crime, while not organized crime as we typically speak of in connection with large-scale hacking cases, does indeed have organization and defined methods. It is most commonly the work of small gangs of criminals who specialize in this type of theft. It should be noted that while physical actions of this type constituted a rather small number of cases, they encompassed a large number of individual crimes. For instance, several cases of this type worked by the USSS in 2009 involved skimmers that were set up at over 50 separate ATMs (in each case) covering a large geographic region.

Table 5. Location of physical actions by number of breaches

Victim location—Indoor non-public area (i.e., offices)	7
Victim location—Outdoor area (grounds, parking lot)	7
External location—Public area or building	3
Victim location—Indoor public/ customer area	3
External location—Public vehicle (plane, train, taxi, etc)	2
Victim location—Disposal area (i.e., trash bin)	1

Error (2% of breaches, <1% of records)

Error refers to anything done (or left undone) incorrectly or inadvertently. Given this broad definition, some form of error could be considered a factor in nearly all breaches. Poor decisions, omissions, misconfigurations, process breakdowns, and the like inevitably occur somewhere in the chain of events leading to the incident. For this reason, we distinguish between error as a primary cause of the incident vs. contributing factor. If error is a primary cause it independently and directly progresses the event chain leading to an incident. On the other hand, if error is a contributing factor, it creates a condition that—if/when acted upon by another threat agent—allows the primary chain of events to progress. For example, a misconfiguration that makes an application vulnerable to attack is a "contributing factor" whereas one that immediately crashes the server is the "primary cause."

We include all that gobbledygook because, quite honestly, how to best classify the role of error in a breach confuses us at times (and we created the classification system). In past DBIRs, we merged all errors together in a single chart if they "significantly" contributed to the breach. Over time, determining whether an error was "significant enough to be significant" and thus counted as a statistic in the report, caused no few heated discussions (yes, we're geeks and take this stuff seriously). Therefore, we've decided to bypass all that and handle things slightly differently than we have in the past. In Table 6, we present only errors fitting the "primary cause" description given above. We can directly observe these and they had a direct and measurable role in the breach. To us, it seems the most straightforward and honest approach and we hope it satisfies you as well.

15 http://krebsonsecurity.com/2010/01/would-you-have-spotted-the-fraud/

Table 6. Types of causal errors by number of breaches

Misconfiguration	2
Loss or misplacement	1
Publishing error (i.e., posting private info on public site)	1
Technical / System malfunction	1

It will undoubtedly be noticed that the overall numbers are much lower than they have been in the past. Mainly, this is a result of the causal vs. contributory distinction. It is also true that incidents directly resulting from an error are less likely to require outside investigation as it's often painfully obvious what happened. Please don't let these low numbers mislead you; though not shown among the causal variety in Table 6, contributory error is ALMOST ALWAYS involved in a breach. It would be a mistake to use our classification minutia as an excuse not to unyieldingly strive to minimize errors and their impact to data security in your organization.

Environmental (0% of breaches, 0% of records)

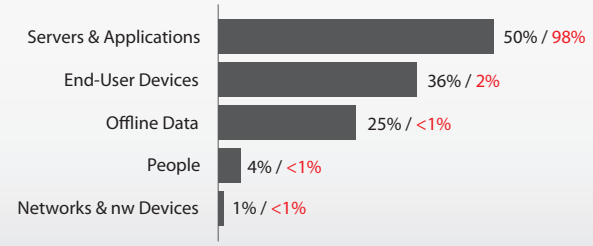
This category not only includes natural events like earthquakes and floods but also hazards associated with the immediate environment (or infrastructure) in which assets are located. The latter encompasses power failures, electrical interference, pipe leaks, and atmospheric conditions. Nothing in this category contributed to data breaches in either the Verizon or USSS caseloads in 2009. Although environmental hazards most often affect the attribute of availability, they do occasionally factor into scenarios resulting in the loss of confidentiality as well. We have, for instance, investigated incidents in the past in which a power outage led to a device rebooting without any of the previously-configured security settings in place. An intruder took advantage of this window of opportunity, infiltrated the network, and compromised sensitive data. Such events are not common but are worth some consideration.

Compromised Assets

We discussed the agents, their actions, and now we turn to the assets they compromised in 2009. This section specifically refers to the assets from which data were stolen rather than assets involved in other aspects of the attack (i.e., an external agent often breaches the internal network in order to compromise data from a database but only the latter would be referenced here). Those familiar with this section from previous DBIRs may notice a few changes. First, what was previously called "Online Data" is now "Servers and Applications" simply because it's more descriptive and sets a clearer boundary between it and the other categories. We also made "People" its own category because information can be directly stolen from them (think phishing and torture) and they (we?) should receive separate consideration and protection. Figure 27 shows results for the five asset categories. Those interested in a more specific list of the most compromised asset types can refer to Table 7.

What has not changed is that servers and apps account for 98.5% of total records compromised.

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



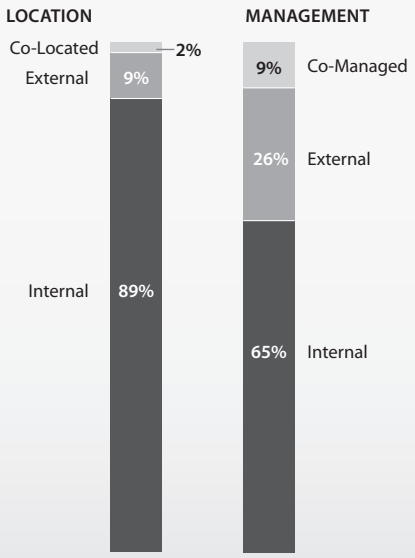
Once again, servers and applications were compromised more than any other asset (that makes six straight years). However, 2009 shows quite a drop from 2008 levels (94% to 50%) primarily due to cases contributed by the USSS. Verizon-only cases also showed less of a super majority at 74% than in previous years. What has not changed is that servers and apps account for 98% of total records compromised (see Figure 27). The top types of assets within this category are basically the same as they have always been: databases, web servers, and point-of-sale (POS) servers.

Breaches involving end-user devices nearly doubled from last year. This was quite consistent between both the Verizon and USSS datasets (37% and 36% respectively). Much of this growth can be attributed to credential-capturing malware discussed earlier in this report.

Offline data is the yin to the servers and apps yang. Where the latter dropped, the former grew. Whereas our cases have been almost devoid of offline data theft (remember—this is different from, for instance, the use of portable media to facilitate data theft, which we see fairly regularly), it occurs often among those investigated by the USSS. Most of these involved insiders stealing IP, engaging in embezzlement and skimming, and actions of that nature. This is another one of those areas where the merged dataset serves to create a more complete view of the world. That view, however, doesn't change our perspective on where most loss occurs; offline assets once again comprised less than 1% of all compromised records. The same was true of the people and networks categories.

Cloud computing is an important topic and the relationship of hosted, virtualized, and externally-managed systems to data breaches is an important area of study. Figure 28 shows the location and management of these assets discussed in this section. The question of whether outsourcing contributes to the susceptibility of assets to compromise cannot be answered from these results. That would require more information. For instance, is the 89% shown for internally-sited assets higher or lower than that of the general population? If such a statistic exists, it would make for an interesting comparison. For now, we will simply relay our findings and continue to collect what information we can.

Figure 28. Location and management of compromised assets by percent of breaches*



* Only assets involved in 2% or more of breaches shown

Table 7. Types of compromised assets by percent of breaches and percent of records*

Type	Category	% of Breaches	% of Records
Database server	Servers & Applications	25%	92%
Desktop computer	End-User Devices	21%	1%
Web app/server	Servers & Applications	19%	13%
Payment card	Offline Data	18%	<1%
POS server (store controller)	Servers & Applications	11%	<1%
Laptop computer	End-User Devices	7%	<1%
Documents	Offline Data	7%	<1%
POS terminal	End-User Devices	6%	<1%
File server	Servers & Applications	4%	81%
Automated Teller Machine (ATM)	End-User Devices	4%	<1%
FTP server	Servers & Applications	2%	3%
Mail server	Servers & Applications	2%	4%
Customer (B2C)	People	2%	<1%
Regular employee/end-user	People	2%	<1%

* Only assets involved in 2% or more of breaches shown

Compromised Data

In terms of data theft, we are glad to say that 2009 was no 2008. Just among breach cases worked by Verizon and the USSS, over 360 million records were compromised in 2008 (overlap removed). While nowhere near the 2008 figure, 2009 investigations uncovered evidence of 143 million stolen records, making it the third-highest year in the scope of this study (see Figure 29). Not exactly a successful year for the defenders but we'd be happy if the 50% drop continued over the next few.

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

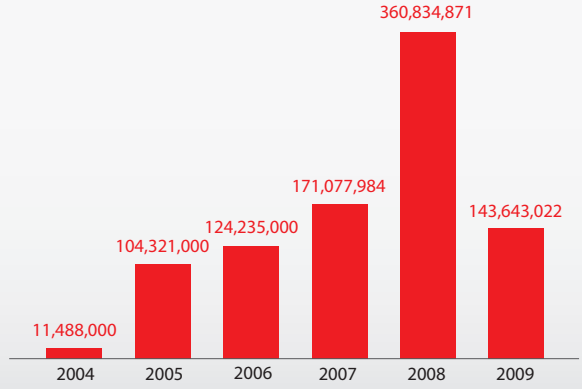
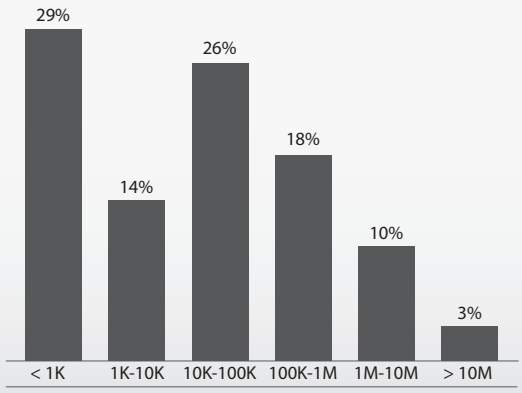


Figure 30. Distribution of records compromised by percent of breaches, 2004-2009



What's not apparent in Figure 29 is that this total is the low-end estimate for 2009. In about 25% of cases, investigators confirmed compromise but were unable to quantify losses, and so, these cases did not contribute to the 143 million figure. The true number is somewhere north of that. The difficulty in quantifying exact losses is also part of the reason Figure 29 shows different values than in previous years (the major reason being that 2007 onward reflects additional USSS cases). Occasionally, we learn of exact losses after the close of an investigation (i.e., when the case goes to trial) and we update our figures accordingly.

As was the case in the previous year, most of the losses in 2009 came from only a few breaches. The average number of records lost per breach was 1,381,183, the median a scant 1,082, and the standard deviation a whopping 11,283,151. While those figures are interesting to understand a bit more about the variance among 2009 cases, loss distributions are far more interesting when they describe larger samples. Therefore, we'd like to break from discussing 2009 for a moment and present what we hope will be useful data for those of you who get into this kind of thing. Figure 30 and Table 8 present descriptive statistics on all breaches and all 900+ million records investigated by Verizon and the USSS since 2004 (at least those that have been studied and classified using VERIS for the purposes of this study).

With that short excursion out of the way, let's return to examining 2009 results, specifically, which types of data were stolen during breaches worked last year. The first observation is that Figure 31 is not as one-dimensional as in years past. Although still the most commonly breached type, payment card

data dropped from 81% of cases to 54% in 2009. Both Verizon and the USSS showed the same result within a few percentage points. It does still account for 78% of total records breached but that is also down (from 98%). Payment cards are prized by criminals because they are an easy form of data to convert to cash (which is what most of them really want). Most payment card cases worked by Verizon and the USSS involve fraudulent use of the stolen data. Losses associated with post-breach fraud are not counted as part of this study but total in the tens of millions of dollars just for the subset of breaches for which we know an amount.

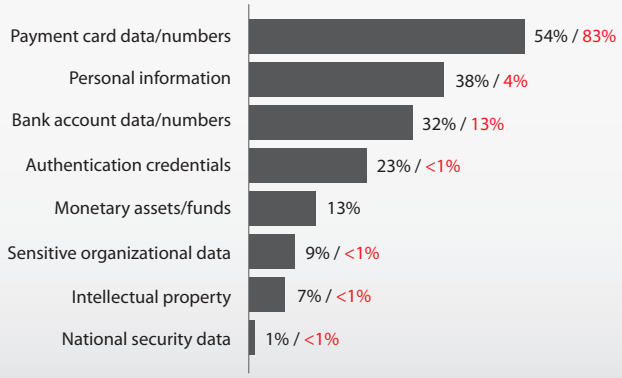
Personal information and bank account data were the second and third-most compromised data types. Like payment cards, both are useful to the criminal for committing fraud. Bank account data rose substantially due to the many cases of insider misuse at financial institutions worked by the USSS. Often related to this, monetary assets or funds stolen directly from these and other compromised accounts were fairly common.

The usefulness of authentication credentials to cybercriminals has been discussed already in this report so we won't do so again here. Sensitive organizational data (like financial reports, e-mails, etc.), intellectual property, and national security data were not nearly as common as some of the more directly cashable types of data but there are reasons for this. Perhaps the primary reason is that disclosure or outside investigation is not usually mandatory as it often is with payment cards and personal information. This means we are less likely to conduct forensics. Furthermore, since most organizations discover a breach only after the criminal's use of stolen data triggers fraud alerts, we infer that breaches of data not useful for fraud are less likely to be discovered. In other words, this kind of information is likely stolen more often than these statistics show. It also tends to harm the organization (or nation) a great deal more in smaller quantities than do payment cards and the like.

Table 8. Descriptive statistics on records compromised, 2004-2009

Total records	912,902,042
Mean[16]	1,963,230
Median[17]	20,000
Standard deviation[18]	13,141,644
Percentiles[19]	
10th	12
25th	360
50th	20,000
75th	200,000
90th	1,200,001
99th	60,720,000

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



16 The average of a set of numbers
17 The middle value in an ascending set of numbers
18 A measure of variability in a set of numbers
19 The value below which a certain percent of a population falls

Attack Difficulty

Given enough time, resources and inclination, criminals can breach virtually any single organization they choose but do not have adequate resources to breach all organizations. Therefore, unless the value of the information to the criminal is inordinately high, it is not optimal for him to expend his limited resources on a hardened target while a softer one is available. While rating the difficulty of attacks involves some subjectivity, it does provide an indicator of the level of effort and expense required to breach corporate assets. This, in turn, tells us a lot about the criminals behind these actions and the defenses we put in place to stop them.

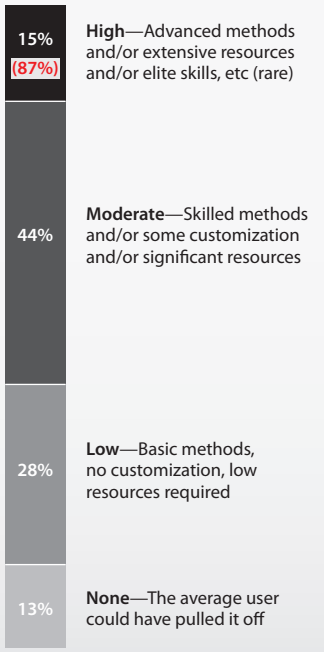
Our investigators assess the various details around the attack and then classify it according to the following difficulty levels:

- **None:** No special skills or resources required. The average user could have done it.
- **Low:** Basic methods, no customization, and/or low resources required. Automated tools and script kiddies.
- **Moderate:** Skilled techniques, some customization, and/or significant resources required.
- **High:** Advanced skills, significant customization, and/or extensive resources required.

Attack difficulty is not a part of the VERIS framework, so it is not a data point collected by the USSS (the same applies to the Attack Targeting and other sections). The primary focus of sharing between the organizations was on objective details about each case. Therefore, results in this section pertain only to Verizon's 2009 caseload.

From 2004–2008, over half of breaches fell in the "None" or "Low" difficulty ratings. The scales tipped in 2009 with 60% now rated as "Moderate" or "High." This finding is in line with the assertions outlined in the beginning of the Results and Analysis section: the breaches worked by our IR team are, in general, getting larger and more complex. This also mirrors our historical data pertaining to the Financial and Tech Services industries.

Figure 32. Attack difficulty by percent of breaches and records*



* Verizon caseload only

Given enough time, resources and inclination, criminals can breach virtually any single organization they choose but do not have adequate resources to breach all organizations.

Looking more closely at the distributions, the percentage of breaches on the low end ("None") and high end ("High") of the difficult rating remains similar to that reported in last year's study. Also, highly difficult attacks once again account for the overwhelming majority of compromised data (87% of all records). The real growth this year is in the moderately difficult category.

Attack scenarios are most effectively and efficiently prevented earlier in their progression rather than later. Said differently, stop adversaries before they own the box because it's awfully hard to stop them once they have.

As discussed in the section detailing hacking activity, and continuing from last year's report, techniques used by criminals to infiltrate corporate systems remain relatively low in skill and resource requirements (though there are certainly exceptions). The sophistication is once again found in the malware that is used in these attacks. These programs are often written from scratch or customized substantially to evade detection and serve a particular purpose in the attack.

Difficult attacks, therefore, are not necessarily difficult to prevent. At the risk of stating the obvious, there is a message here that should be clearly understood: attack scenarios are most effectively and efficiently prevented earlier in their progression rather than later. Said differently, stop adversaries before they own the box because it's awful hard to stop them once they have.

Attack Targeting

Standard convention in the security industry classifies attacks into two broad categories: opportunistic and targeted. Due to significant grey area in this distinction, we find it useful to separate opportunistic attacks into two subgroups. The definitions are provided below:

- **Random Opportunistic:** Attacker(s) identified the victim while searching randomly or widely for weaknesses (i.e., scanning large address spaces) and then exploited the weakness.
- **Directed Opportunistic:** Although the victim was specifically selected, it was because they were known to have a particular weakness that the attacker(s) could exploit.
- **Fully Targeted:** The victim was first chosen as the target and then the attacker(s) determined a way to exploit them.

Figure 33. Attack targeting by percent of breaches and records*

* Verizon caseload only

The percentage of fully targeted attacks in our dataset (27%) is consistent with last year's report (28%), which means the majority of breach victims continue to be targets of opportunity. This is both good news and bad news. Good for those in our profession who's job difficulty levels correlate highly with criminal determination. Bad because it means many of us have made ourselves targets when we otherwise might not have been. Doubly bad because when targeted attacks are successful, they can be quite lucrative for the attacker. In 2009, targeted attacks accounted for 89% of records compromised. Laying this information side by side with data points in the Attack Difficulty section, one begins to get the message many criminals are hearing: find a juicy target (even if well-protected), apply your resources, work hard, and you'll reap the reward. We need to change that message.

We still believe that one of the fundamental self-assessments every organization should undertake is to determine whether they are a Target of Choice or Target of Opportunity.

Though the same overall proportion, random and directed opportunistic attacks have fluctuated somewhat in the last year. As discussed in last year's report, we encounter many breaches that seem neither truly random nor fully targeted—particularly in the Retail and Hospitality industries. In a very common example, the attacker exploits Software X at Brand A Stores and later learns that Brand B Stores also runs Software X. An attack is then directed at Brand B Stores but only because of a known exploitable weakness. We don't believe the dip in directed opportunistic attacks stems from changes in the threat environment. Rather, it is more likely due to the lower percentage of retailers and breaches that involve compromised partner assets within our 2009 caseload.

We still believe that one of the fundamental self-assessments every organization should undertake is to determine whether they are a Target of Choice or Target of Opportunity. The security media hype machine would like us to believe that we're all Targets of Choice and there's nothing we can do to stop the new *[insert whatever you like here]* threat. This simply isn't true and is not a healthy line of reasoning for security management. Consider instead questions like these: Do you have information the criminals want? How badly do they want it? How can they profit from it? How far would they go to obtain it? How difficult would it be for them to get it if they started trying today? What could you do to decrease the chances they will choose you or increase the work required to overcome your defenses? Not answering such questions honestly and properly can result in serious exposure on one hand and serious overspending on the other.

Unknown Unknowns

Past DBIRs have shown a strong correlation between security incidents and a victim's lack of knowledge about their operating environment, particularly with regard to the existence and status of information assets. Though the numbers are down in 2009, the year can hardly be called an exception. In nearly half of Verizon's cases, investigators observed what we not so affectionately call "unknown unknowns." These are classified as meeting at least one of the following conditions:

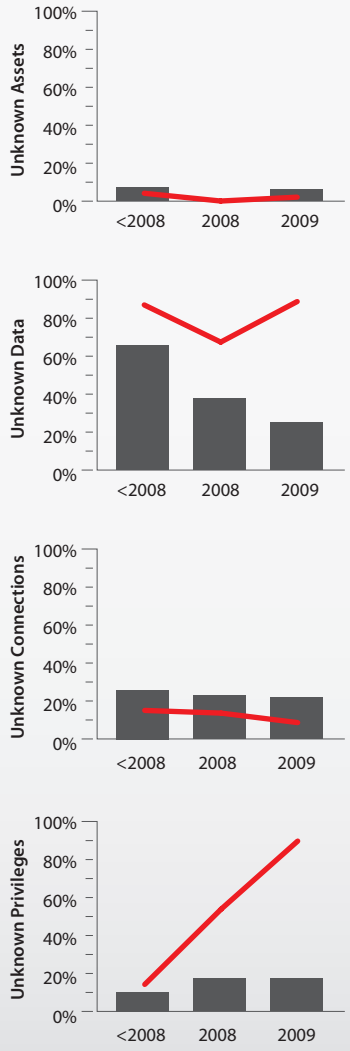
- **Assets** unknown or unclaimed by the organization (or business group affected)
- **Data** the organization did not know existed on a particular asset
- Assets that had unknown network **connections** or accessibility
- Assets that had unknown user accounts or **privileges**

The downward trend in the overall representation of unknowns as a contributor to data breaches is somewhat perplexing (from 90% several years ago to 43% this past year). As seen in Figure 34, this is mainly the result of a steady decline in assets that were storing unknown data. This could be because organizations are getting better at managing their environment; lets hope so. The case could also be made that demographics are a factor. As reported in our 2008 Supplemental DBIR (and supported by data collected since then), Financial Services organizations boast a much better track record when it comes to unknown unknowns. It makes sense that the growing share of our cases worked in this industry would influence these statistics. We also suspect the growth of certain regulations, like those that restrict POS systems from storing data locally, are having a positive effect. It could also be argued that the problem has simply shifted elsewhere; that attackers have changed their tactics. They no longer rely on the accidental storing of data in the clear but are employing RAM scrapers, packet sniffers, and other methods to actively and selectively capture the data they desire.

Setting "unknown data" aside, the other categories are fairly level. Losing track of network connections and accounts seems to be a persistent problem for data breach victims. Data loss linked to cases involving "unknown privileges" rocketed up again to 90%. In the past we've recommended practices like asset discovery, network and data flow analysis, and user account reviews, and we'd be remiss not to restate their value here.

Finally, it is very important to note that though the overall occurrence of "unknowns" is down, it would be wrong to relegate them to a problem of yester year. By examining these results from the perspective of data loss, one realizes that the "impact" of unknown unknowns has never been higher, contributing to nine of ten records breached in 2009. What we don't know continues to hurt us.

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



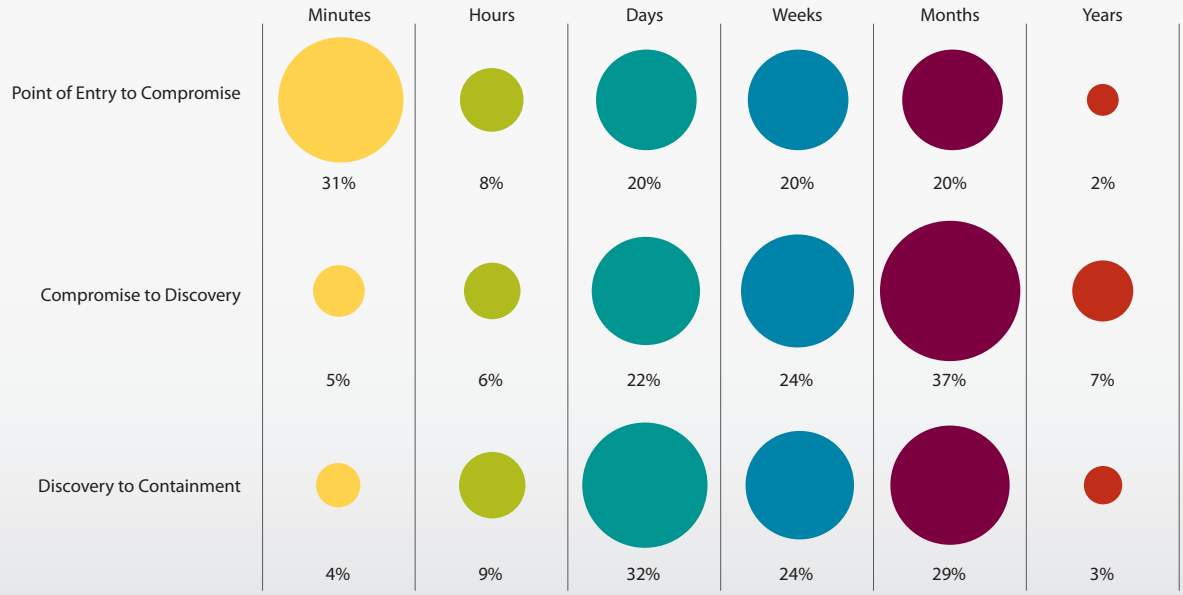
By examining these results from the perspective of data loss, one realizes that the "impact" of unknown unknowns has never been higher, contributing to nine of ten records breached in 2009. What we don't know continues to hurt us.

Timespan of Breach Events

If you've ever seen a Hollywood version of a data breach, it probably went down something like this: the attacker launches some nifty tool with flashy graphics, punches keys for 30 seconds, and then exclaims "We've got the files!" Meanwhile, on the defending side an analyst looks up at a large screen, goes pale, and stammers "Sir—they've breached our firewall." Based on our experience, real-world breaches follow a very different script. Understanding that script tells us a lot about the interplay between attackers and defenders.

In describing the timeline of a breach scenario, one could identify numerous discrete events if so inclined. Separating events into three major phases serves our purposes quite well and closely aligns with the typical incident response process. These phases are depicted in Figure 35 and discussed in the paragraphs that follow.

Figure 35. Timespan of events by percent of breaches



Point of Entry to Compromise

This phase covers the attacker's initial breach of the victim's perimeter (if applicable) to the point where they locate and compromise data. This often involves an intermediate step of gaining a foothold in the internal network. The amount of time required to accomplish this varies considerably depending on the circumstances. If data are stored on the initial point of entry, compromise can occur very quickly. If the attacker must navigate around the network probing for data, it can take considerably longer. The timeline also changes based on the methods and tools employed by the attacker.

In over 60% of breaches investigated in 2009, it took days or longer for the attacker to successfully compromise data. The Verizon and USSS datasets vary little on this statistic. While some may interpret this to be a rather small window of time, it could be worse. If victims truly have days or more before an attack causes serious harm, then this is actually pretty good news. It means defenders can take heart that they will likely get more than one chance at detection. If real-time monitoring fails to sound an alarm, perhaps log analysis or other mechanisms will be able spot it.

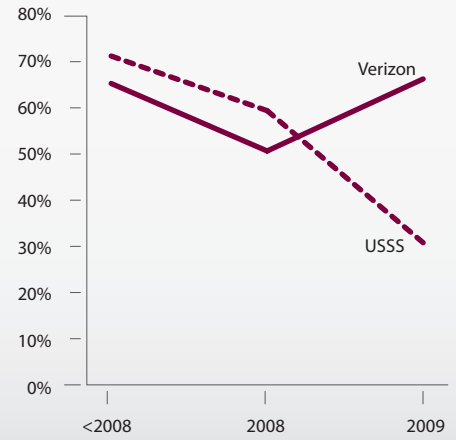
If victims truly have days or more before an attack causes serious harm, then this is actually pretty good news. It means defenders can take heart that they will likely get more than one chance at detection.

Unfortunately, we're speaking hypothetically here. The bad news is that organizations tend not to take advantage of this second window of opportunity. The telltale signs are all too often missed, and the attacker has all the time they need to locate and compromise data.

Compromise to Discovery

Over the last two years, the amount of time between the compromise of data and discovery of the breach has been one of the more talked about aspects of this report. It is not without reason; this is where the real damage is done in most breaches.

Figure 36. Percent of breaches that remain undiscovered for months or more



That a breach occurred is bad enough but when attackers are allowed to capture and exfiltrate data for months without the victim's knowledge, bad gets much worse. In the 2009 DBIR, we closed this section hoping that the slight improvement we observed from the previous year would continue. While Figure 35 would seem to suggest it's time for some modest celebration, we're not sipping champagne just yet.

Yes, it's true that the percentage of breaches extending months or more before discovery is down for the third year in a row (65% to 50% to 44%). While the first two of those figures speak to Verizon's dataset only, the last includes USSS data. Figure 36 gives a clearer picture of what's really going on and explains our hesitation. For Verizon cases, 2009 was actually the worst year yet in terms of the time to discovery metric. For the USSS, it was the best by far. That the merged statistic is down (which best represents "what we know of the world") is a slightly encouraging sign. At least we'll choose to view it as one and continue to hope and work for improvement.

Discovery to Containment

Once an organization discovers a breach, they will obviously want to contain it as quickly as possible. It should be noted that this is a triage effort and not a complete remediation of the root causes of the breach. Containment is achieved when the "bleeding has stopped" and data are no longer flowing out of the victim. This can be as simple as unplugging the network cable from the affected system, but as Figure 35 shows, it's usually not that easy.

The Verizon, USSS, and merged datasets offer nearly identical testimony on this; over half of all breaches go uncontained for weeks or more after they have been discovered. That's either one extremely hard-to-find network cable or something else is afoot. The truth of the matter is that some breaches are harder to contain than others and some victims are more prepared to handle them than others. Organizations represented on the far left of Figure 35 either had very simple containment or a good plan that enabled them to execute quickly. Those on the far right had tougher duty, weren't prepared, or both.

While there are scores of reasons for this, many containment problems can be traced back to failing to remember the five P's: Proper Planning Prevents Poor Performance.

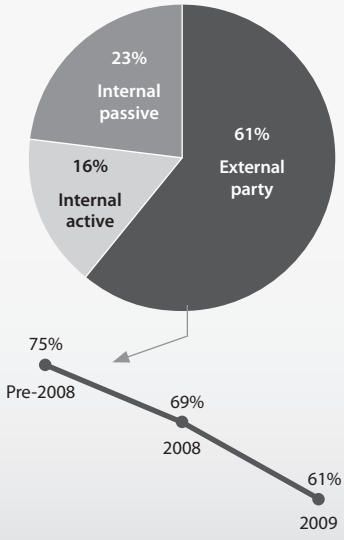
While there are scores of reasons for this, many containment problems can be traced back to failing to remember the five P's: Proper Planning Prevents Poor Performance. We often find organizations have a plan (check P #2) but they downloaded a template from the web and never tailored, distributed, or rehearsed it (uncheck P #1). Others, in their frantic attempts to stop the breach, actually make matters worse and damage valuable evidence at the same time. A lack of adequate and current information like network diagrams is also a common time sink to the response process. Finally, contractual problems can slow the containment of a breach (i.e., What happens when assets involved in an incident are hosted by a third party? What does it take to get the cable pulled?). Again, proper planning prevents poor performance.

Breach Discovery Methods

We discussed how long it takes for victims to discover a breach but it is equally important to examine how they make that discovery or, rather, how others make it for them. The time to discovery is inextricably bound to the method of discovery, as some methods take longer than others. Both metrics are indicators of the maturity of the security program since they reflect on the ability of the organization to detect and respond to threat actions. Unfortunately, Verizon's past research consistently finds that breaches are not found by the victim organization, but by an outside party. We would like to be able to proclaim that this was the result of caseload bias and that things really aren't all that bad outside our sample, but alas, we cannot. Data obtained from the USSS show a very similar finding.

We can offer some good news from 2009, though—perhaps even a glimmer of hope. As seen in Figure 37, breaches discovered by external parties are down for the third year running (75% to 69% to 60%). The difference was made up by internal active measures (those actually designed and deployed to detect incidents) while internal passive discoveries (someone just happened to notice something awry) remained static. Through the rest of this section, we dive into each in more detail[20].

Figure 37. Simplified breach discovery methods by percent of breaches



20 Comparing the discovery methods listed here (and the complete list in VERIS) to prior reports will show significant differences. In most cases, we simply split out existing categories into more discrete items.

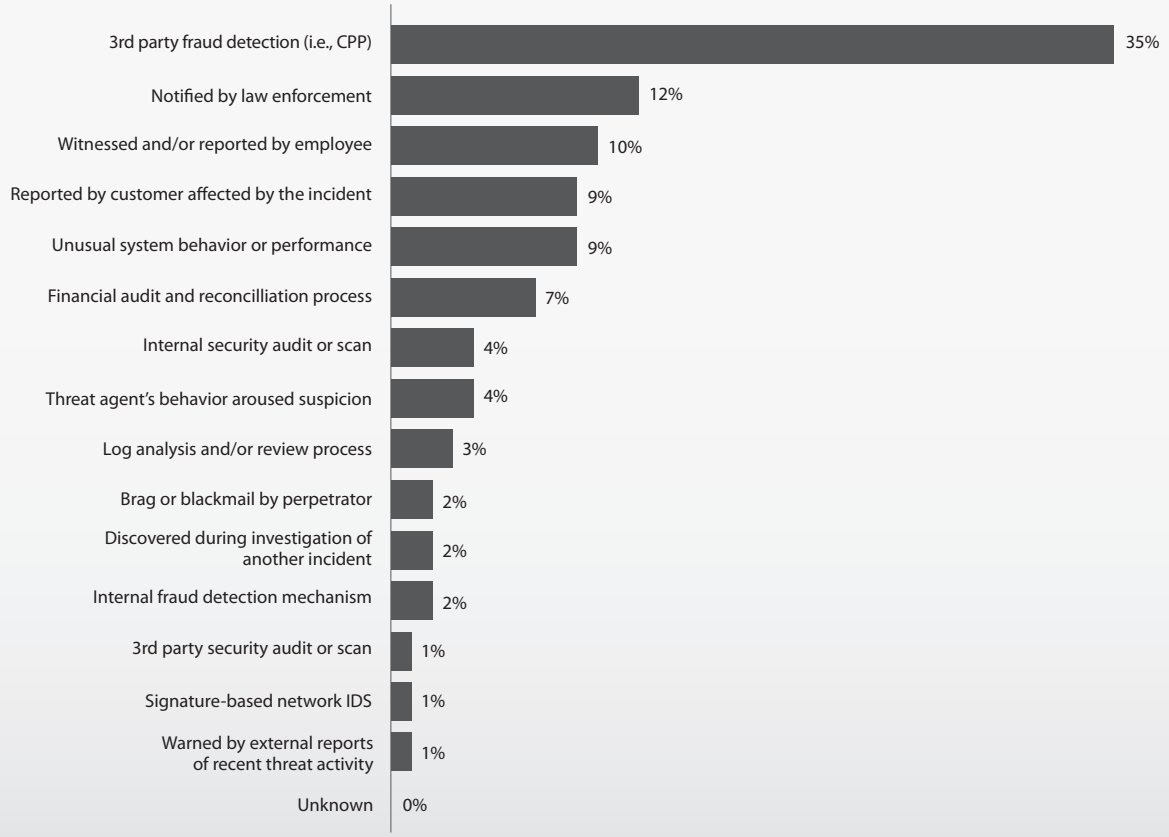
Discovery by external parties

Though substantially lower than ever before, third party fraud detection is still the most common way breach victims come to know of their predicament. When this happens, the organization was usually identified because fraud pattern analysis pointed to them as the common point of purchase (CPP) for payment cards involved in the compromise. We find it more than a little ironic that the most effective way of detecting data breaches is for the perpetrator to fraudulently use what was stolen.

Third party fraud detection is still the most common way breach victims come to know of their predicament.

Notification by law enforcement is second on the list of discovery methods. Underground surveillance, criminal informants, intelligence operations, fraud investigations, etc. are all examples of how law enforcement personnel learn about the breach. Having your customers inform you of a breach is probably the worst of all options. Such notification often comes in the form of a very distressed "what happened to my money?" or some derivative of that not fit for print.

Figure 38. Breach discovery methods by percent of breaches



Internal passive discovery

It turns out that employees aren't bad breach detectors, which is a good thing because most organizations have a decent amount of them. While performing their everyday duties, personnel occasionally witness an incident or stumble upon something that makes them report it. Systems affected by a breach often exhibit unusual behavior or degraded performance. These methods are consistently toward the top of our list and though such discoveries are accidental, it is proof that employees can and should be considered a third line of defense against breaches. Training (good training) can enhance their ability to identify and report incidents and so, seems like a smart direction in which to allocate some budget.

Internal active discovery

Organizations spend far more capital on active measures to detect incidents but results show—at least for breach victims—disappointingly little return. Before discussing what's not working, let's touch on some things that are (sort of).

Internal audit methods—both financial and technical—are the bright spot in all of this. Financial audit and reconciliation processes found several account and ledger discrepancies that were investigated by the organization and discovered to be the result of a breach (remember *The Cuckoo's Egg*?). The increased prominence of this is likely due to the larger ratio of financial institutions in the combined dataset and the nature of breaches worked by the USSS. Technical audits (routine system checks, scans, etc.) also uncovered a respectable number of breaches. Organizations that treat routine security audits in a "just get it done as cheaply and quickly as possible" manner are squandering what could be an effective detection method.

ON LOGS, NEEDLES, AND HAYSTACKS

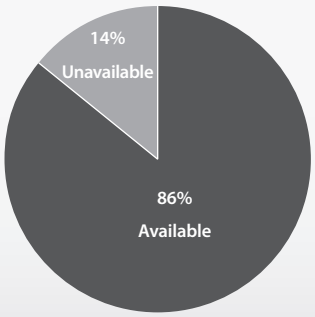
These findings are not easy to digest, especially when you consider that the log data used by our forensic investigators are the very same log data stored on the victim's systems. It cannot be a pleasant experience to learn that the six months of log data you've been collecting contained all the necessary indicators of a breach. It is, however, a common experience. We consistently find that nearly 90% of the time logs are available but discovery via log analysis remains under 5%. That is a very large margin of error. What gives?

Many claim—with good reason—that looking for evidence of malicious activity among the huge number of logs collected in the typical organization is like looking for a needle in a haystack. Maybe they're right (but there are good needle-searching tools out there to help). However, maybe looking for needles isn't what we should be doing; maybe we should be looking for haystacks.

Our investigators spend a great deal of time searching through log files for evidence. It is absolutely true that we have the benefit of hindsight in doing this; we can narrow the search to a certain window of time, certain systems, certain types of events, etc. Nevertheless, we often find what we're looking for because of three major tip-offs: 1) abnormal increase in log data, 2) abnormal length of lines within logs, 3) absence of (or abnormal decrease in) log data. We've seen log entries increase by 500% following a breach. We've seen them completely disappear for months after the attacker turned off logging. We've noticed SQL injection and other attacks leave much longer lines within logs than standard activity. Those are more like haystacks than needles.

No, it's not perfect. It won't catch everything. By all means, if your solution finds needles effectively, do it. We have little doubt, however, that if the organizations we've studied had tuned their systems to alert on abnormalities like this and actually looked into them when alarms went off, that 5% would be a lot higher. We might need to find needles to find perfection (close the gap to 86%), but just finding the haystacks would be a very real improvement.

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



* Verizon caseload only

Overall, however, the data in context of the broader security industry suggest that we must remain pessimistic about the state of active detection mechanisms within organizations. In the 2009 DBIR, we reported that event monitoring and log analysis, which should be the doyen of detection, successfully alerted only 6% of breach victims. This year that figure has dropped—yes dropped—to 4%. Of that 4%, log analysis lead to the discovery of a handful of breaches while intrusion detection systems identified only one. As with each prior year, we will offer our assessment as to why this situation exists. This time, we use a simple Q&A structure.

Q: Are IDS and log analysis tools ineffective?

A: No. Among breach victims they aren't very effective but the controls themselves can be effective.

Q: Were these technologies utilized by organizations in your dataset?

A: Sometimes. The leading failure is definitely that these tools are not deployed. None of these technologies showed more than a 40% adoption rate among our sample. As further evidence of this, see the level of non-compliance with requirement 10 in PCI DSS.

Q: What happened with those that did use them? Why didn't they help?

A: Usually poor configuration and monitoring. Event monitoring and analysis tools are not "set and forget" technologies, yet many treat them that way. We commonly find these devices neutered (intentionally or unintentionally) to the point of ineffectiveness so as to cause minimal noise and disruption (which is understandable). They are also often undermanned and/or completely unwatched.

Q: You said "usually"—not "always." Are you saying some do a decent job of deploying, configuring, and monitoring detective technologies and the attacker still gives them the slip?

A: Yes. The techniques and level of artifice used in many threat actions discussed throughout this report are unlikely to be seen as malicious by these tools. If an attacker authenticates using stolen credentials, this will look like a legitimate action. Devices scanning for certain pre-defined signatures or hashes will not see those that are altered in some manner. There is no such thing as a silver bullet and if there were, the werewolves would wear armor.

Q: Can you offer any hope?

A: Yes. We continue to find that victims usually have evidence of the attack in their log files. This year that figure was 86%, which suggests that, while we might miss the attack as it happens in real-time, we have a good chance of detecting it later. Combine that with the previous section showing that we have a little breathing room before actual data compromise occurs, and one begins to see some brightness ahead through the gloom. We'll never bask in that light, however, if we do nothing to adjust our course.

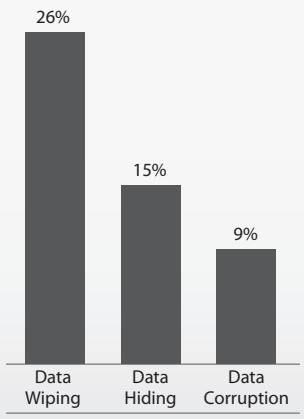
The short answer is that we are not seeing a significant representation of organizations making consistently strong efforts to detect and respond to security events among the victims in these datasets. We truly hope to see that change in the coming years.

Many claim—with good reason—that looking for evidence of malicious activity among the huge number of logs collected in the typical organization is like looking for a needle in a haystack. However, maybe looking for needles isn't what we should be doing; maybe we should be looking for haystacks.

Anti-Forensics

Few criminals want to be behind bars and those who engage in actions to breach information assets are no different. In the wake of the Albert Gonzalez prosecution and other crackdowns, cybercriminals have more reason than ever to hide their tracks and not get caught. Anti-forensics consist of actions taken by the attacker to remove, hide, and corrupt evidence or otherwise foil post-incident investigations. There are varying flavors of anti-forensics, and their use is generally determined by the perpetrator's intended actions. This type of activity is at least partially responsible for the breach discovery and response struggles discussed earlier in this report.

Figure 40. Types of anti-forensics by percent of breaches*



* Verizon caseload only

Investigators found signs of anti-forensics in about one-third of cases in 2009—roughly equivalent to the prior year's DBIR. It should be understood, however, that the very nature of these techniques centers on not leaving signs of their use. Therefore, we believe this figure represents the low-end estimate of the actual prevalence of anti-forensics across our caseload.

While the overall use of anti-forensics remained relatively flat, there was some movement among the techniques themselves. Data wiping, which includes removal and deletion, is still the most common but declined slightly. Data hiding and data corruption remain a distant—but gaining—second and third; the former rose by over 50% and the latter tripled (we're working with fairly small numbers on those though). The use of encryption for the purposes of hiding data contributed most significantly to the increase in that technique while the most common use of data corruptions remains log tampering.

These changes reflect some broader trends observed by investigators over the last year and half with respect to anti-forensics. While the objective to remain hidden is still very real, the ability of criminals to compromise and immediately exfiltrate large quantities of data is diminishing. That's not to say they aren't successfully doing so, but positive action on the part of many organizations has eliminated, for instance, large stores of unencrypted data residing on systems. As a result, perpetrators find it necessary to steal data "on the fly" using malware like network sniffers and RAM scrapers. These tools accumulate a stockpile of data over time and the criminal will want to protect and hide their loot to avoid discovery. Think pirates and buried treasure (which is mostly myth but let's not ruin a good metaphor with technicalities).

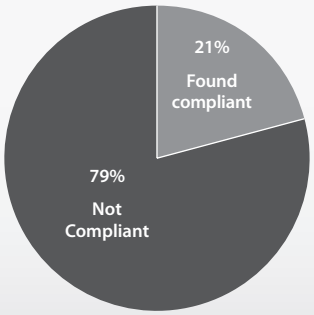
Perpetrators find it necessary to steal data "on the fly" using malware like network sniffers and RAM scrapers. These tools accumulate a stockpile of data over time and the criminal will want to protect and hide their loot to avoid discovery.

Another recent trend is that anti-forensics seem to have trickled down to smaller breaches. In the past, these techniques were much more common in large-scale breaches but the distribution is becoming more uniform. The proliferation of commercial and freeware utilities that can perform these functions makes anti-forensics more accessible and easy to share within criminal communities.

This is clearly a trend of interest to our IR team as the use of anti-forensics can have a profound impact on almost every facet of an investigation. We will certainly continue to monitor and report on the evolution of anti-forensics within cybercrime.

PCI DSS Compliance

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



* Verizon caseload only

Although the concepts of regulatory compliance, security, and risk are overlapping and interrelated, it is their correlation to data breach incidents that proves most reflective of the Payment Card Industry (PCI) and what changes are necessary to reduce account data compromises. Analysis of Verizon's 2009 dataset offers useful insight into the divergent nature of organizational security efforts and the many attack methods outlined in this report. To better understand this, we draw the distinction between the concepts of 'compliance' and 'validation' against the Payment Card Industry Data Security Standard (PCI DSS). Compliance is a continuous maintenance process while validation is a point in time event. The difference between security efforts and breach incidents runs parallel to these concepts.

The PCI DSS is a set of control requirements created by the Payment Card Industry to help protect cardholder information. Based on the demographics and compromised data types presented in this report, it is no surprise that a sizeable proportion of the organizations in Verizon's[21] caseload are subject to PCI DSS. For these cases, investigators conduct a review of which PCI DSS requirements were and were not in place at the time of the breach. The results of this assessment are recorded, usually appended to the case report, and then conveyed to the relevant payment card brands. This exercise is not an official PCI DSS assessment and it does nothing to uphold or overrule the victim's compliance status. It does, however, provide useful insight into the condition of the security program and posture of the organization at the time of the incident.

Since these organizations are breach victims, the burning question is "were they compliant?" Over three-quarters of organizations suffering payment card data breaches within our caseload had not been validated as compliant with PCI DSS.

Since these organizations are breach victims, the burning question is "were they compliant?" Figure 41 gives the answer to this question and, interestingly, it is the same one that was given last year. Over three-quarters of organizations suffering payment card data breaches within our caseload had not been validated as compliant with PCI DSS at their last assessment or had never been assessed.

If we accept that a non-compliant organization is more likely to suffer a data breach, then the more interesting component in Figure 41 is the 21% that had validated as compliant during their last PCI DSS assessment. This is especially so when one considers that all but one of them were Level 1 merchants. The reader should not immediately interpret this as a failure of the PCI DSS to provide excellent guidance, but rather consider the concepts mentioned above of validation vs. compliance. Due to the point-in-time nature of assessments, it is entirely possible (even probable) for an organization to validate their compliance at time A but not be in a compliant state at the time of the breach. This may reflect a desire within organizations to achieve compliance with the standard for the purposes of validation but a lesser commitment to maintaining that state over the long-term. Furthermore, the validation process is not always consistent among Qualified Security Assessors (QSAs). It should also be remembered that compliance with the PCI DSS (or any other standard) is not an absolute guarantee against suffering a data breach.

21 All findings referenced in this section reference only Verizon's caseload.

Regarding the size of the organizations suffering data breaches, although over a third of data breaches originated from the largest merchants (Level 1) the remainder resulted from the small and medium sized merchant population. Although the large data breaches may outstrip all others in volume of card numbers compromised, it is often the smaller merchants that struggle the most in recovering from the fallout of a data breach. This analysis underscores the need for adoption of basic security practices for these merchants such as the use of PA-DSS compliant payment applications, secure remote management tools, and stronger controls when using trusted third party vendors for maintenance.

The aggregate data from the post-investigation PCI Requirements Matrix for 2009 is presented in Table 9, and is compared to our 2008 findings.

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%

There have been a number of changes from 2008 to 2009 and it is important to highlight this delta and its implications and impact on data breaches. Year over year the PCI DSS requirements that saw the greatest increase in compliance were 4, 10, and 12 (22%, 25%, and 26% respectively). Those requirements with the greatest decrease in compliance were 2 and 5 (-19% and -9% respectively). Although Requirement 10 (audit Logging) is still low at 30% compliance, the increase may pay dividends in avoided compromise and shortened response time in the future. Requirement 6 (secure software development) is also quite low but given the problems discussed in this report, any improvement in that area must be viewed as a plus.

When reviewing the percentages for each requirement, several very interesting statistics begin to surface. Requirements 6 and 11—which many organizations complain are the most onerous—are indeed the least compliant across our caseload. These are trailed only slightly by Requirements 2, 3, 7, and 10. Considering the range of controls that this represents, it does not bode well for the security of systems within these organizations.

At the top of the missed list are items in Requirement 6, including secure software development. Attacks relevant to this practice, such as SQL injection, are consistently among the most common and damaging year over year. Considering the fact that vulnerable code can exist not only in custom applications which a company can alter, but also in commercial off the shelf software (COTS) suggests that iterative layers of protection are needed to prevent attacks that exploit these vulnerabilities.

The lack of compliance in Requirement 11 reflects poorly as this section is meant to validate the proper implementation and robust nature of other controls in the standard. Testing, measuring, and reviewing that reality is in line with belief is something we consistently recommend because it is consistently a problem. Knowing (not just recording) what is actually occurring within networks and systems is likewise critical.

The question most pertinent to security management becomes, if companies fail to maintain the ongoing operational maintenance of systems throughout time, does that increase the likelihood of a data breach?

At this point, it's worth considering a common thread that readers may have noticed among the least-met control areas discussed so far—they all require maintenance processes. If this doesn't immediately sink in, take a moment and let it do so. The question most pertinent to security management becomes, if companies fail to maintain the ongoing operational maintenance of systems throughout time, does that increase the likelihood of a data breach?

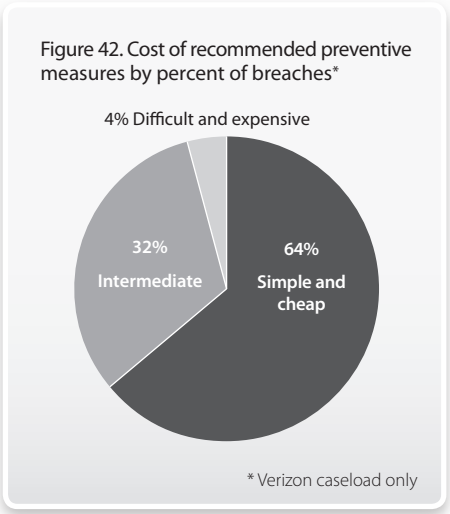
On the other end of the spectrum, a staggering 90% of the organizations breached were found to be encrypting transmission of cardholder data and sensitive information across public networks in compliance with PCI DSS Requirement 4. This is not proof that encryption is useless; it is simply evidence of what we discuss often in this report. Attackers are adept at maneuvering around a strong control (like encryption) to exploit other points of weakness. Perhaps the real strength of encryption should not be measured in key size, but rather in the context of the organization's aggregate security posture.

The use of AV software another requirement toward the top of the compliance list, shares a similar fate to that of encryption. In order to skirt detection, attackers continue to develop and use repacked or customized malware to breach systems.

Clearly PCI DSS is designed not to be a series of compartmentalized controls operated independently to protect information assets. The standard is authored to provide an approach towards security, built to make unauthorized access to systems and data iteratively harder through a series of control gates. When viewed from that perspective, preventing a security breach from turning into a data compromise becomes a much more realistic goal. Hopefully studies like this can be leveraged to complement compliance requirements with risk management efforts to reduce the total cost of security.

Conclusions and Recommendations

Although the overall difficulty of attacks observed in 2009 was a bit higher than previous years, our findings show that the difficulty of preventing them dropped. Only 4% of breaches were assessed to require difficult and expensive preventive measures. This finding is partially explained by Figure 43 in which these recommended preventive measures are divided into several broad categories. Configuration changes and altering existing practices fix the problem(s) much more often than major redeployments and new purchases. The same was true of previous years.



There is an important lesson about security management in all this. Yes, our adversaries are crafty and resourceful but this study always reminds us that our profession has the necessary tools to get the job done. The challenge for us lies in selecting the right tools for the job at hand and then not letting them get dull and rusty over time. Evidence shows when that happens, our adversaries are quick to take advantage of it. Don't let them.

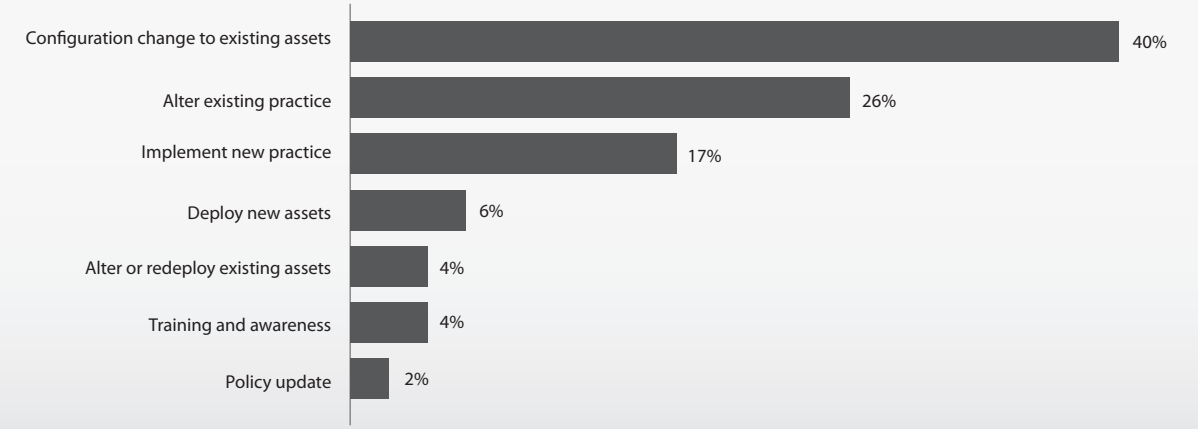
Creating a list of solid recommendations gets progressively more difficult every year we publish this report. Think about it; our findings shift and evolve over time but rarely are they completely new or unexpected. Why would it be any different for recommendations based on those findings? Sure, we could wing it and prattle off a lengthy list of to-dos to meet a quota but we figure you can get that elsewhere. We're more interested in having merit than having many. We did find a few new ones (or extensions of old ones) that we believe to have merit based on our analysis of 2009 and they are listed below. We do, of course, continue to recommend our old ones that can be found in the 2008 and 2009 DBIRs and the 2009 Supplemental report.

Restrict and monitor privileged users: Thanks to data from the USSS, we saw more insider breaches this year than ever before. Insiders, especially highly privileged ones can be difficult to control but there are some proven strategies. Trust but verify. Use pre-employment screening to eliminate the problem before it starts. Don't give users more privileges than they need (this is a biggie) and use separation of duties. Make sure they have direction (they know policies and expectations) and supervision (to make sure they adhere to them). Privileged use should be logged and generate messages to management. Unplanned privileged use should generate alarms and be investigated.

Watch for "minor" policy violations: Sticking with the insider theme, we mentioned several times about a correlation between "minor" policy violations and more serious abuse. Perhaps we should label this as the "Broken Window Theory of Cybercrime." We recommend, then, that organizations be wary of and adequately respond to policy violations. Based on case data, the presence of illegal content, pornography, etc. on user systems (or other inappropriate behavior) is a reasonable indicator of a future breach. Actively searching for such indicators rather than just handling them as they pop up may prove even more effective.

Implement measures to thwart stolen credentials: Stolen credentials were the most common way of gaining unauthorized access into organizations in 2009. Regardless of whether it is a blip or a trend, it's worth doing something to counter it. Keeping credential-capturing malware off systems is priority number one. Consider two-factor authentication where appropriate. If possible, implement time-of-use rules, IP blacklisting (consider blocking large address blocks/regions if they have no legitimate business purpose), and restricting administrative connections (i.e., only from specific internal sources). A "last logon" banner and training users to report/change passwords upon suspicion of theft also have promise.

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



* Verizon caseload only

Monitor and filter egress network traffic: Most organizations at least make a reasonable effort to filter incoming traffic from the Internet. This probably stems from a (correct) view that there's a lot out there that we don't want in here. What many organizations forget is that there is a lot in here that we don't want out there. Thus, egress filtering doesn't receive nearly the attention of its alter ego. Our investigations suggest that perhaps it should. At some point during the sequence of events in many breaches, something (data, communications, connections) goes out that, if prevented, could break the chain and stop the breach. By monitoring, understanding, and controlling outbound traffic, an organization will greatly increase its chances of mitigating malicious activity.

Change your approach to event monitoring and log analysis: A quick review of a few findings from this report will set the stage for this one. 1) In most attacks, the victim has several days or more before data are compromised. 2) Breaches take a long time to discover and 3) when that finally happens, it usually isn't the victim who finds it. 4) Finally, almost all victims have evidence of the breach in their logs. It doesn't take much to figure out that something is amiss and a few changes are in order. First, don't put all your eggs in the "real-time" basket. IDS/IPS should not be your only line of defense. You have some time to rely on more thorough batch processing and analysis of logs. Next, focus on the obvious things (the "haystacks") rather than the minutia (the "needles")[22]. This need not be expensive; a simple script to count log lines/length and send an alert if out of tolerance can be quite effective. Finally, make sure there are enough people, adequate tools, and/or sufficient processes in place to recognize and respond to anomalies. We are confident that this approach will reap benefits and save time, effort, and money.

Share incident information: This final recommendation will also serve as our concluding paragraph. We think this report is a proof that it can be done responsibly, securely, and effectively. We believe that the success of our security programs depends on the practices we implement. Those practices depend upon the decisions we make. Our decisions depend upon what we believe to be true. Those beliefs depend upon what we know and what we know is based upon the information available to us. The availability of information depends upon those willing to collect, analyze, and share it. If that chain of dependencies holds, you could say that the success of our security programs depends upon the information we are willing to share. We believe that this is a call to action and commend all those who take part.

Thank you for taking the time to read this report.

22 See "On Logs, Needles, and Haystacks" in Discovery Methods if it isn't clear what we're talking about.

Appendices from the United States Secret Service

Many readers of the DBIR have questions surrounding what happens after the breach. Where does the information go? How do the perpetrators move it? What goes on behind the scenes in the criminal community? What is being done to stop it? While our investigators have some visibility into these matters, they are squarely in the purview of the United States Secret Service. Thus, the following appendices come directly from the USSS. One delves into the shady world of online criminal communities and the second focuses on prosecuting cybercrime using the example of the USSS' efforts to bring Albert Gonzalez to justice.

Appendix A: Online Criminal Communities

No Monolithic Computer Underground

One of the significant challenges in producing an analysis of the computer underground lies in the diversity of the online criminal community, which manifests itself in a variety of ways. For example, criminals may choose to cluster around a particular set of Internet Relay Chat channels, Internet-based chat rooms or web-based forums. In some instances, a group of online criminals may come from a particular geographic area and may know each other in real life; in other instances, the criminals may be dispersed across the globe and know one another only through their online interaction. Many online underground venues are populated largely by the young and the curious who are not hard-core criminals and whose capabilities and sophistication are as limited as their experience. Other, more exclusive online groups count among their members professional criminals who have a decade or more of experience and extensive contacts in diverse criminal communities.

This diversity also is reflected in the groups' interests and aims. One group may see the researching of vulnerabilities and development of new exploits as a technical challenge fundamentally related to the basics of computer security. Another group may have little or no interest in underlying technological issues, but will happily use exploits developed by others in order to intrude into third-party computer systems and harvest data of commercial value. Still other online criminal communities show even less interest in coding and exploits, but utilize the Internet as an operating base, taking advantage of the anonymity and instantaneous communications the Internet affords them. As such, one needs to keep in mind that blanket statements such as, "Here is what the criminals are doing now..." may reflect only one particular group or type of criminal community and not be universally applicable.

Well-Developed Organizational Structure

Two of the hallmarks that distinguish effective online criminal groups are organizational structure and access to a well-developed criminal infrastructure. Again, these can be manifested in a variety of ways depending on the online community from which the group emerged.

One striking manifestation of these trends in online criminality is found in the web-based online forums that first began to emerge approximately a decade ago. In the early days, these online forums were established by hacking groups or by groups of carders (criminals who traffic in or exploit stolen credit card data). Many of these forums have a strong representation of members from Eastern Europe, although membership often spans the globe and includes members from multiple continents. By utilizing the built-in capabilities of the forum software, the people behind the organization are able to set up a system of forum administrators and moderators who form the core of the organization and who maintain order at the site.

These administrators control the membership of the organization and can simply banish or limit disruptive members, members who cannot back up the claims they make or those who provide poor quality services. At the same time, other members can be elevated within the organization and given enhanced status—such as the rank of Vendor or VIP Member—which will be evident to all other forum members. As the forum continues to grow, existing members can develop good (or bad) reputations for the goods and services they provide; at some forums, these informal authority structures have been augmented by formalized reputation systems similar to those used at online auction sites, so that all forum members will be able to assess another member's reliability at a glance. At many forums, persons who want to become a full-time vendor of goods or services must undergo a formal review process in which senior members of the forum must inspect and rate the product to be vended. By studying the forums, a member who is interested in purchasing, for example, an exploit toolkit will be able to compare the pricing, feature sets and terms of sale of the available toolkits, review the reputations of their respective vendors and conduct interactive discussions with other customers in order to mine their experience with fielding the toolkits under real-world conditions. These abilities enhance the buying experience as well as the quality of goods and services available to the criminal community.

Some of these online forums developed into online bazaars for criminal goods and services. By 2004, such forums as DumpsMarket, CarderPortal, Shadowcrew and CarderPlanet were already well-developed criminal marketplaces overseen by an experienced group of administrators who were often established criminals. While these and similar forums are sometimes called "carding forums," in reality these sites serve as a business platform for a fusion of criminal communities, each of which provides its own contribution to the development of the organization's capabilities by making a greater variety of reliable criminal services available to all members. Some of the major classes of participants in these forums include the following broad categories:

- Carders (Traffic in and exploit stolen financial data)
- Hackers / Security Technologists
  - Perform targeted intrusions for harvesting of data
  - Develop exploits and exploit toolkits
  - Decryption services
  - Anonymity services (proxies, criminal-run VPNs, private messaging systems, etc.)
  - Provide security engineering and consulting services
- Spammers
- Bot Herders (Build and run botnets, which have a variety of criminal uses)
- Money Launderers
- Renegade Hosters and Internet Developers
  - Provide stable platform for criminal business, i.e., criminal sites
  - "Bulletproof Hosts" for phishing, malware drop sites, etc.
- Malware Developers (Creation/dissemination of specialized crimeware)
- Document Forgers (Produce counterfeit drivers' licenses, passports, checks, etc.)
- Information Services (Research services for identity theft)
- Specialized Hardware Providers (ATM skimmers, card production equipment, etc.)
- Calling Services (Provide fraudulent telephone calls to defeat out-of-band authentication)
- Drop Managers (Recruit and manage "drops" or money mules)

Over the past decade, there have been several dedicated carding forums operating at any one time, and many of the more mainstream "hacking forums" (especially in Eastern Europe) have developed sub-forums which include many of the services typically found at a carding forum. Not surprisingly, many of the most serious and/or widespread online attacks attributed to criminal sources over the past decade—both in terms of malware and intrusions—have been linked to established members of these online criminal forums.

As evident from the array of criminal service providers listed in the previous section, the development of diverse online criminal organizations has greatly enhanced the criminal infrastructure available to pursue large-scale criminal activity. At the same time, these criminals' ability to operate anonymously has been augmented by parallel trends on the Internet. One example of such a trend is found—paradoxically enough—in the increasing availability of easy-to-use security technologies; e.g., professional online criminals tend to be avid users of strong encryption, which they use to complicate investigations and conceal evidence of their online activities.

Another online phenomenon often preferred by the criminal community is the appearance of so-called digital currencies. Online digital currencies, such as E-gold, whose operators pleaded guilty to money laundering and illegal money remitting charges in 2008, have allowed online criminals to pay one another for services and goods and to move the proceeds of their criminal schemes internationally with little to no regulation or oversight. The far-reaching availability of a reliable criminal infrastructure in combination with other developments on the Internet presents a global challenge to law enforcement, which has found itself forced to adapt in order to apprehend and prosecute online criminals.

Steady Growth in Attackers' Numbers and Capabilities

By the mid-2000s, online criminal organizations such as those represented by the carding forums had already developed effective and sustainable organizational models which allowed their members to perpetrate some of the most serious security incidents of the time. By this time, even the computer trade and popular press began to notice a pronounced trend which had long been obvious to observers of the carding scene: Today's cybercriminals are not hobbyists seeking knowledge or thrills; they are motivated by the illicit profits possible in online crime.

Since that time, the organizations have continued to evolve; many of the trends seen online have not been favorable to the defenders:

- Online criminal organizations as represented by the Internet forums continue to grow in terms of membership. When it closed in August 2004, the infamous CarderPlanet site was the largest forum of its kind—at its height, the CarderPlanet forum had approximately 7,900 user accounts. By 2010, there are multiple analogous forums whose membership dwarfs that number. At the present time, there are multiple online hacking forums, venues with significant criminal traffic advertising malware, DDoS and hacking services on a daily basis, which have many tens of thousands of registered users.
- As time has gone by, an "old guard" of experienced cybercriminals has developed. It is no longer unusual for a professional criminal to have almost a decade of experience under his belt, during which time he may have been able to develop solid, long-term relationships with a trusted group of similarly experienced associates. Some of these professionals no longer operate with any sort of public presence on Internet venues, but rather deal exclusively with a smaller group of trusted associates. Some of these professionals also are believed to have developed operational relationships with established criminals in the real world as well, which augments their capabilities in ways that the Internet cannot.

- At the same time, the illicit profits associated with top Internet criminals also appear to have grown significantly. A decade ago, someone whose criminal operations brought in tens of thousands of dollars annually was considered fairly successful, depending on the community in which he operated. More recently, experienced cybercriminals have been linked to various attacks and schemes that are known to have garnered them millions of dollars in profits.
- The commercialization of the computer underground continues to develop. One of the more visible manifestations of this phenomenon can be found in the various "affiliate programs" which recruit young hackers into schemes such as "software loads" or "software installs" or the promotion of dubious Internet pharmacies. Some of these affiliate programs have been known to advertise on underground forums, openly recruiting affiliates who will make their botnets available to these schemes in return for a small percentage of the final take.
- Some groups of attackers have been able to develop significant familiarity with and expertise in particular types of target systems, such as those used to process financial data. In some cases, this experience has allowed attackers to manipulate target systems in novel ways that have allowed them to mount attacks that may not have been envisioned before they were successfully executed. In some instances, attackers are known or believed to have had advanced technical or scientific training at prestigious foreign educational institutions, which they have been able to apply in their criminal work through such pursuits as attacking encryption systems.
- The criminal community continues to develop and deploy new back-office services that enhance existing practices. One example of this is found in the multiple antivirus checking services that are run by various criminal groups. These services have purchased subscriptions to dozens of commercially available antivirus and security software packages and allow their customers—for a small fee—to upload malware to see if any current security product will detect it. This type of service allows criminals to know with certainty if the malware they are planning to deploy will be detected by any of the widely deployed antivirus products.
- Criminals are surprisingly adaptive in developing entire new categories of online schemes. One example of this can be found in the fake anti-virus industry that has boomed over the past couple of years; this scam typically involves bogus alerts on the desktops of Internet users designed to trick them into purchasing a useless piece of software which would purportedly protect their system. While there had been scams along this line earlier in the 2000s, in 2008 traffic relating to this "business model" exploded on underground forums, and by 2010 fake security products comprised a significant percentage of all malware, according to industry estimates.

The Criminal Marketplace

One of the perennial questions surrounding the online underground marketplace concerns the cost of various goods and services. Although such figures often appear in the popular press as part of titillating headlines, in reality the pricing of goods tends to be a complex issue, as it depends on a wide variety of factors including the circumstances of the sale, the exclusivity and quality of the goods in question, the volume in which they are acquired, the number of competing vendors, etc. Consider the question, "How much does it cost to buy a car? A comprehensive answer would have to note that one can buy an aging jalopy for a few hundred dollars, while a luxury sports car can cost more than a quarter of a million dollars. The underground exhibits the same variety in terms of pricing. If a criminal needs a piece of spyware, he can download several samples of such software (many of low quality in one regard or another) from several Internet archives, possibly trying to modify it for his needs. Alternately, he can spend several thousand dollars and buy a full-featured, undetectable spyware package from a current vendor who will support it. If he needs an exclusive package, there have been reports of other spyware products that can cost tens of thousands of dollars, if one knows the right people.

Much the same is true in terms of prices of such goods as stolen credit cards. First of all, there is a wide variety of types of cards (classic cards, gold cards, platinum cards, cards issued by U.S. banks, cards issued by foreign banks, etc.), and these distinctions influence the price. Secondly, some vendors have an "all sales final" policy with no guarantee of validity, whereas others will replace invalid card data; the latter group of vendors tends to have higher prices. Thirdly, buyers who deal in volume almost always get a better price than people who purchase small amounts of stolen cards. Fourthly, cards are sold in the underground in different formats, which is one of the main factors in determining the price of the data. So-called "cvv2s" typically include the card number, expiration date, cardholder name and address, and the CVV2 security code from the back of the card. This type of data typically sells for $1 to a few dollars per unit, depending on the type of card and circumstances of the sale. Another type of card is called a "full-info" card—this type of card includes all the data associated with a "cvv2" but is enhanced with other data about the cardholder such as his date of birth, mother's maiden name, Social Security Number, place of birth, and other information that will aid in authenticating fraudulent transactions. Full-info cards will typically cost more than $10 and up per unit in the underground, depending on a variety of factors. Credit card track data (electronic data from the magnetic stripe on the back of a credit card) is called in the underground a "dump." The price for dumps usually starts at around $15 and may be considerably more, depending on the type of card and validity rate of the data being sold.

Appendix B: Prosecuting Cybercrime—The Albert Gonzalez story

In April 2005, the United States Secret Service (USSS) San Diego Field Office initiated an online undercover operation, Carder Kaos, targeting top tier suspects participating in financial crimes committed through the Internet. Operation Carder Kaos focused its investigation on a suspect known online as "Maksik", since identified as Maksym Yastremskiy, a Ukrainian national regarded as the most prolific vendor of compromised credit card numbers in the world. A series of undercover online purchases of credit cards led to face-to-face meetings with Yastremskiy in Thailand, the United Arab Emirates, and Turkey where enough evidence was obtained to secure an indictment. In July 2007 another undercover meeting in Turkey was arranged and Yastremskiy was arrested and prosecuted by Turkish authorities. Maksym Yastremskiy is currently serving a thirty-year sentence in Turkey.

As a result of the Carder Kaos investigation, the USSS, Criminal Intelligence Section (CIS) leveraged considerable intelligence and directly identified two suspects who perpetrated the network intrusions that provided Maksik with his database of illicit credit card numbers. The suspects were known online as "Johnnyhell" and "Segvec". Based on the forensics from the intrusion of the restaurant chain, Dave & Busters, and evidence recovered from Maksik's computer, "Jonnyhell" was identified as Alexander Suvorov. Following a coordinated international effort led by the USSS, Suvorov was arrested in Germany in March 2008, as he prepared to travel to Bali, Indonesia. In July 2009, Alexander Suvorov was extradited to the United States and has pled guilty to his involvement in the network intrusion of Dave & Busters.

Building on this success, CIS and other agents concentrated efforts on identifying the real world identity of "Segvec". Using traditional law enforcement techniques, agents linked "Segvec" and additional high level targets to multiple network intrusions including the TJX Corporation intrusion, acknowledged at the time to be the single largest compromise of customer credit card numbers and accounts in the Unites States. Working in unprecedented cooperation with the private sector, USSS agents associated Albert Gonzalez with the online moniker "Segvec".

In May 2008, USSS agents arrested Albert Gonzalez, and he was later indicted along with eight other co-conspirators for hacking into the wireless computer networks of TJX Corporation, BJ's Wholesale Club, OfficeMax, Barnes & Noble, Forever 21, Discount Shoe Warehouse, Boston Market, and Sports Authority. The defendants from the United States, Estonia, Ukraine, the People's Republic of China, and Belarus demonstrate the worldwide reach of this illicit community.

In January 2009, Heartland Payment Systems detected an intrusion in its processing system and learned of the subsequent theft of credit card data. The comprehensive USSS investigation revealed more than 130 million credit card accounts had been compromised and data was sent to a command and control server managed by an international group related to other ongoing USSS investigations. During the course of the investigation, the USSS revealed that this international group committed other intrusions into multiple corporate networks from which they stole credit card and debit card data. The USSS relied on a variety of investigative methods, including computer forensics, log analysis, malware analysis, search warrants, Mutual Legal Assistance Treaties with our foreign law enforcement partners, and subpoenas to identify three main suspects. Albert Gonzalez was again found to be involved, and in August 2009, Gonzalez and two other suspects were charged for their involvement in the data breaches into Heartland Payment Systems, 7-11, JC Penny, Wet Seal, and Hannaford Brothers.

In March 2010 Albert Gonzalez was sentenced to 20 years in prison for his involvement in these data breaches. This investigation to date is the largest data breach in United States history and also represents the longest sentence for a cyber criminal.

About Verizon Investigative Response

Security breaches and the compromise of sensitive information are a very real concern for organizations worldwide. When such incidents are discovered, response is critical. The damage must be contained quickly, customer data protected, the root causes found, and an accurate record of events produced for authorities. Furthermore, the investigation process must collect this evidence without adversely affecting the integrity of the information assets involved in the crime.

The IR team has a wealth of experience and expertise, handling over 650 security breach and data compromise cases in the last six years. Included among them are many of the largest breaches ever reported. During these investigations, the team regularly interacts with governmental agencies and law enforcement personnel from around the world to transition case evidence and set the stage for prosecution. The expansive data set generated through these activities offers an interesting glimpse into the trends surrounding computer crime and data compromise.

About the United States Secret Service

As the original guardian of the nation's financial payment system, the United States Secret Service has established a long history of protecting American consumers, industries and financial institutions from fraud. Over the last 145 years, our investigative mission and statutory authority have expanded, and today the Secret Service is recognized worldwide for our expertise and innovative approaches to detecting, investigating and preventing financial and cyber fraud.

Today's global economy has streamlined commerce for both corporations and consumers. Financial institutions and systems are readily accessible worldwide. Today's financial fraud and cybercriminals have adapted to this new means of global trade and seek to exploit this dependence on information technology. Cybercriminals consequently have become experts at stealing stored data, data in transit, and encrypted data. They operate based on trust, long standing criminal relationships, high levels of operational security, and reliability. The culture also has evolved over the last decade and is now described as non-state sponsored, transnational and is almost impossible to infiltrate due to its dynamic nature and operational security.

To combat these emerging threats, the Secret Service has adopted a multi-faceted approach to aggressively combat cyber and computer related crimes by establishing a network of 29 Electronic Crimes Task Forces (ECTF), including the first international ECTF located in Rome, Italy, 38 Financial Crimes Task Forces (FCTF) and a Cyber Investigations Branch. This approach enables the Secret Service to detect, prevent, and aggressively investigate electronic crimes including cyber attacks on the nation's critical infrastructures and financial payment systems.

In Fiscal Year 2009, agents assigned to Secret Service offices across the United States arrested more than 5,800 suspects for financial crimes violations.

For more information or to report a data breach, please contact your local Secret Service office: www.secretservice.gov.

Cyber Intelligence Section

The Cyber Intelligence Section (CIS) of the Secret Service was founded in 2005 to combat trends in fraud and identity theft. The CIS serves as a central repository for the collection of data generated through the agency's field investigations, open source Internet content and a variety of information obtained through financial and private industry partnerships as it relates to identity theft, credit card fraud, bank fraud, and telecommunications fraud.

CIS leverages technology and information obtained through private partnerships, to monitor developing technologies and trends in the financial payments industry that may enhance the Secret Service's abilities to detect and mitigate attacks against the financial and telecommunications infrastructures. CIS penetrates, disrupts and dismantles online criminal networks, investigates and coordinates network intrusion investigations, and provides case agents with actionable intelligence to support their investigations.

How does the Secret Service get involved in a data breach investigation?

The Secret Service is the only entity within the Department of Homeland Security that has the authority to investigate violations of Title 18, United States Code, Section 1030 (Computer Fraud). Congress also directed the Secret Service in Public Law 107-56 to establish a nationwide network of Electronic Crimes Task Forces (ECTFs) to "prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems." Members of ECTFs include academic partners, international, federal, state and local law enforcement partners, and more than 3,100 private sector partners.

Furthermore, the methodology employed by CIS has prevented data theft by providing intelligence recovered during criminal investigations to assist victim companies in mitigating further exposure of their network assets.

verizonbusiness.com

verizonbusiness.com/socialmedia verizonbusiness.com/thinkforward