Executive Summary

361 million >> 144 million >> 4 million. Thus goes the tally of total records compromised across the combined caseload of Verizon and the United States Secret Service (USSS) over the last three years. After four years of increasing losses culminating in 2008’s record-setting 361 million, we speculated whether 2009’s drop to 144 million was a fluke or a sign of things to come. 2010’s total of less than four million compromised records seems to suggest it was a sign. But of what? And is it a permanent change in direction or a temporary detour?

To help us answer that, we are very glad to have the United States Secret Service (USSS) back with us for the 2011 DBIR. Additionally, we have the pleasure of welcoming the Dutch National High Tech Crime Unit (NHTCU) to the team. Through this cooperative effort, we had the privilege—and challenge—of examining about 800 new data compromise incidents since our last report (with 761 of those for 2010). To put that in perspective, the entire Verizon-USSS dataset from 2004 to 2009 numbered just over 900 breaches. We very nearly doubled the size of our dataset in 2010 alone!

It is fascinating from a research standpoint that the all-time lowest amount of data loss occurred in the same year as the all-time highest amount of incidents investigated. In addition to being the largest caseload ever, it was also extremely diverse in the threat agents, threat actions, affected assets, and security attributes involved. We witnessed highly automated and prolific external attacks, low and slow attacks, intricate internal fraud rings, country-wide device tampering schemes, cunning social engineering plots, and much more. Some of the raw statistics may seem to contradict this claim of diversity (e.g., the percent of breaches attributed to external agents is more lopsided than ever), but one must consider the change in scale. Whereas “10%” used to mean approximately 10-15 breaches across an annual caseload averaging 100-150, it now means 75 breaches in the context of the 2010 caseload. Consider that fact as you digest and ponder results from this year’s report.
With the addition of Verizon’s 2010 caseload and data contributed from the USSS and NHTCU, the DBIR series now spans 7 years, 1700+ breaches, and over 900 million compromised records. We continue to learn a great deal from this ongoing study and we’re glad to have the opportunity once again to share these findings with you. As always, our goal is that the data and analysis presented in this report prove helpful to the planning and security efforts of our readers. As usual, we begin with a few highlights below.

**Who is behind data breaches?**

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>92%</td>
<td>stemmed from external agents (+22%)</td>
</tr>
<tr>
<td>17%</td>
<td>implicated insiders (-31%)</td>
</tr>
<tr>
<td>&lt;1%</td>
<td>resulted from business partners (-10%)</td>
</tr>
<tr>
<td>9%</td>
<td>involved multiple parties (-18%)</td>
</tr>
</tbody>
</table>

If you’ve followed these numbers over the years, you may be thinking we change our position more than a professional contortionist. We’ll admit to a fair share of head scratching among the RISK team as we tried to interpret what they were telling us. In 2009, breaches involving insiders shot up due to incorporating the USSS data, but returned again to pre-USSS levels in 2010 (even though they’re still with us). Read the report for the full scoop on this, but it basically boils down to a HUGE increase in smaller external attacks rather than a decrease in insider activity. Oh, and partner-caused breaches continued their steady decline.

**How do breaches occur?**

Due to the lower proportion of internal threat agents, Misuse lost its pole position among the list of threat action categories. Hacking and Malware have retaken the lead and are playing dirtier than ever. Absent, weak, and stolen credentials are careening out of control. Gaining quickly, however, is a newcomer to the top three—Physical. After doubling as a percentage of all breaches in 2009, it managed to double again in 2010. Maybe cybercrime is getting less “cyber”? Misuse and Social, though lower in percentage, were still high in number and provided some amazing examples of misbehavior, deception, and plotting for the highlight reel.

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>50%</td>
<td>utilized some form of hacking (+10%)</td>
</tr>
<tr>
<td>49%</td>
<td>incorporated malware (+11%)</td>
</tr>
<tr>
<td>29%</td>
<td>involved physical attacks (+14%)</td>
</tr>
<tr>
<td>17%</td>
<td>resulted from privilege misuse (-31%)</td>
</tr>
<tr>
<td>11%</td>
<td>employed social tactics (-17%)</td>
</tr>
</tbody>
</table>

**What commonalities exist?**

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>83%</td>
<td>of victims were targets of opportunity (&lt;&gt;</td>
</tr>
<tr>
<td>92%</td>
<td>of attacks were not highly difficult (+7%)</td>
</tr>
<tr>
<td>76%</td>
<td>of all data was compromised from servers (-22%)</td>
</tr>
<tr>
<td>86%</td>
<td>were discovered by a third party (+25%)</td>
</tr>
</tbody>
</table>
| 96%        | of breaches were avoidable through simple or intermediate controls (<>)
| 89%        | of victims subject to PCI-DSS had not achieved compliance (+10%) |

Unfortunately, breaching organizations still doesn't typically require highly sophisticated attacks, most victims are a target of opportunity rather than choice, the majority of data is stolen from servers, victims usually don't know about their breach until a third party notifies them, and almost all breaches are avoidable (at least in hindsight) without difficult or expensive corrective action. We would really, really like to report some major change here (negative numbers), but our results won’t let us.

Though not applicable to all organizations in our sample, post-breach assessments of those subject to the PCI-DSS revealed compliance levels that were quite low.
Where should mitigation efforts be focused?

- Eliminate unnecessary data; keep tabs on what’s left
- Ensure essential controls are met
- Check the above again
- Assess remote access services
- Test and review web applications
- Audit user accounts and monitor privileged activity
- Monitor and mine event logs
- Examine ATMs and other payment card input devices for tampering

Year in Review, 2010

Cloud, Aurora, Mobility, Zeus, APT, Wikileaks, Stuxnet, Anonymous. If a word cloud were created using infosec headlines from 2010, these would certainly be rendered big and bold. It’s an interesting juxtaposition of themes. While the Cloud and mobile devices increasingly allow us to do anything from anywhere with anyone at any time, Aurora, Zeus, Advanced Persistent Threats (APTs), Wikileaks, and Stuxnet remind us of the difficulty of protecting our information assets in a usability-driven world. Because our caseload (and that of the USSS and NHTCU) is a window into that world, one would expect to glimpse aspects of it in this annual report on breach trends. And this year’s DBIR meets that expectation.

Apart from the word “Security,” “Cloud” was the next most-common word among presentation titles at the 2011 RSA Conference. It’s definitely in our collective hearts and minds. As such, we are often asked whether “the Cloud” factors into many of the breaches we investigate. The question is both easy and difficult to answer. The easy answer is “No—not really.” We have yet to see a breach involving a successful exploit of a hypervisor allowing an attacker to jump across virtual machines (VMs), for instance. On the other hand, we constantly see breaches involving hosted systems, outsourced management, rogue vendors, and even VMs (though the attack vectors have nothing to do with it being a VM or not). In other words, it’s more about giving up control of our assets and data (and not controlling the associated risk) than any technology specific to the Cloud.

We are often asked whether “the Cloud” factors into many of the breaches we investigate. The easy answer is “No—not really.” It’s more about giving up control of our assets and data (and not controlling the associated risk) than any technology specific to the Cloud.

While we’re on the topic of giving up control of our assets and data, we might as well touch on mobile devices. This is another oft-asked topic during our breach-related presentations and discussions. The fact of the matter is that mobile computing devices (tablets, smartphones, mobile phones, etc.) are rarely the source of data loss across our caseload. That has a lot to do with the kind of cases we investigate (which tend to involve deliberate breach and compromise situations rather than accidental loss of devices). Plus, this report includes only confirmed incidents of data compromise.
The threats to mobile devices are real and we fully expect them to increase and diversify along with the use, uses, and users of such devices. Just consider the effect of the iPad since its debut one year ago; many CxOs who were once technology-indifferent now demand to use their iPads at work. The convenience and functionality of these and other similar devices will drive widespread corporate adoption and security will once again find itself rushing to catch up.

Zeus sprouted up within our 2009 caseload, but came to full bloom in 2010. Between the USSS and ourselves, Zeus and its evil business partners, account takeover and transfer fraud, were rampant among consumers and businesses alike. All of these receive further treatment in this report, so we will simply mention it here and move on.

If Zeus shows us that criminals have their minds on our money, Aurora, APTs, Stuxnet, and Anonymous remind us that some threat agents have more than money on their minds. These gave information risk a more sinister, targeted, and personal feel for us all in 2010 (some might add hopeless). Whether these feelings are justified by a significant increase in risk is difficult to discern. Perhaps these feelings are, in fact, justified. Perhaps they are justified only for a subset of us. Maybe risk did not change at all, but our awareness of it changed dramatically. Maybe it’s a nugget of truth surrounded by multiple layers of fear, uncertainty, and doubt. What we do know with certainty is that our 2010 caseload revealed certain characteristics that one might associate with these events. For instance, numbers of public sector victims hit an all-time high. We studied more incidents involving theft of classified information, intellectual property, and other sensitive organizational data than ever before. Simply an artifact of a much larger and more diverse sample caseload rather than a real change? Maybe...or maybe not.

APTs deserve some special treatment here. Some will remember that we voiced concern in the 2010 DBIR and subsequent blog posts over the APT hysteria sweeping the security community. We still believe that a “scope creep” exists in the definition of APT. The term’s originators use it primarily in reference to state-sponsored attacks from the People’s Republic of China. Others use it to describe any threat possessing above average skill and determination. The logical outcome of the former is to seriously assess and seriously address security posture within government agencies and the defense industrial base (which is right and good). The logical outcome of the latter is to conclude that “everyone is a target” of APT (which is an oxymoron and leads to irrational fears about the boogeyman while common thieves clean you out of house and home). It is simply not possible for everyone to be a target. It is undoubtedly true (based on investigative experience) that some are the target of state-sponsored attacks (originating from China and/or elsewhere). It is also undoubtedly true (also based on experience) that some who think they are victims of APTs are really the victims of organized criminals, hacktivists, glorified script kiddies, and their own mistakes. Because “APTs” (any definition) are real, it’s time we get real about defining and defending against them.

Outside the spotlight of these headlines, however, a very different story played out in 2010. The amount of compromised data hit an all-time low across the combined Verizon and USSS caseload. DataLossDB, the Identity Theft Resource Center, and other sources also show a marked decline in total records lost and exposed. What’s going on? The headlines seem more hopeless than ever yet the numbers (some of them at least) seem almost hopeful. Why the contrast? What’s the “real” 2010? We believe threads of truth exist in both stories. As discussed above, there is some truth behind the headlines. Similarly, data loss figures point to a possible and real change in the motives and tactics used by criminals to steal information. We’ve done our best to relay these stories and statistics within these pages and unpack their core messages and meaning. We hope this effort will play some small part in leading us all to a happier ending in 2011 and beyond.

If Zeus shows us that criminals have their minds on our money, Aurora, APTs, Stuxnet, and Anonymous remind us that some threat agents have more than money on their minds. These gave information risk a more sinister, targeted, and personal feel for us all in 2010.
Conclusions and Recommendations

At the conclusion of our last report, we stated:

“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.”

But surely after examining another 800 breaches in the past year, we’d have plenty of new recommendations to solve all your security woes, right? Quite wrong, actually. The latest round of evidence leads us to the same conclusion as before: your security woes are not caused by the lack of something new (Figure 43 looks about like it always does). They almost surely have more to do with not using, under using, or misusing something old.

The argument levied against that notion is that our adversaries are clever rascals and will adapt in order to thwart our “old” defenses. That is true (and we’ve seen and discussed evidence of such adaptation), but let’s be real, shall we? As a whole, do you really think we’re making them scramble to adapt? Year after year our data seems to suggest that we are not, and that is something that needs to change. If they adapt, then they adapt. C’est la vie. But let’s quit allowing them to find success in stagnation.

To that end, we’ve found some old recipes for achieving newfound success. We examined top attacks from 2010 and identified recommendations from our previous reports most applicable to them. They are categorized and listed below and we hope they help you at the planning and budget negotiations table.

Overall

Achieve essential, and then worry about excellent: We find that many organizations achieve very high levels of security in numerous areas but neglect others. Criminals will almost always prefer the easier route. Identifying a set of essential controls and ensuring their implementation across the organization without exception, and then moving on to more advanced controls where needed is a superior strategy against real-world attacks.

The argument levied against that notion is that our adversaries are clever rascals and will adapt in order to thwart our “old” defenses. That is true (and we’ve seen and discussed evidence of such adaptation), but let’s be real, shall we? As a whole, do you really think we’re making them scramble to adapt?

Access Control

Change default credentials: Simple and sweet, when system/network admins stand up a new system, change the password. If you outsource this to a third party, check that they’ve changed the password. Don’t assume that your staff or your partners consistently follows through on all policies and procedures. Along with changing default credentials, organizations should ensure that passwords are unique and not shared among users or used on different systems. This was especially problematic for assets managed by a third party.
Every year that we study threat actions leading to data breaches, the story is the same; most victims aren’t overpowered by unknowable and unstoppable attacks. For the most part, we know them well enough and we also know how to stop them.

User account review: Prior year’s data breach reports and years of experience lead us to believe in the value of reviewing user accounts on a regular basis. The review should consist of a formal process to confirm that active accounts are valid, necessary, properly configured, and given appropriate (preferably least) privileges.

Restrict and monitor privileged users: 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.

Network Management
Secure remote access services: In many instances, remote access services have been enabled and are Internet-facing. We recommend tying these services down where only specific IP addresses or networks can access them. Additionally, it’s important to limit access to sensitive systems within the network. Many organizations will allow any device on the network to connect and remotely access any other device; we highly recommend not managing your devices this way. Tie down remote access services to specific management networks via access control lists.

Monitor and filter egress network traffic: 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.

Secure Development
Application testing and code review: SQL injection attacks, cross-site scripting, authentication bypass, and exploitation of session variables contributed to nearly half of breaches attributed to hacking or network intrusion. It is no secret that attackers are moving up the stack and targeting the application layer. Why don’t our defenses follow suit? As with everything else, put out the fires first: even lightweight web application scanning and testing would have found many of the problems that led to major breaches in the past year. Next, include regular reviews of architecture, privileges, and source code. Incorporating a Security Development Life-Cycle (SDLC) approach for application development is recommended as well. Finally, help your developers learn to appreciate and write more secure code.

Log Management and Analysis
Enable application and network witness logs and monitor them: All too often, evidence of events leading to breaches was available to the victim but this information was neither noticed nor acted upon. Processes that provide sensible, efficient, and effective monitoring and response are critical to protecting data.

However, don’t just focus your logging efforts on network, operating system, IDS, and firewall logs and neglect remote access services, web applications, databases, and other critical applications. These can be a rich data set for detecting, preventing, and investigating breaches.
Define “suspicious” and “anomalous” (then look for whatever “it” is): This is admittedly vague, but—in truth— generalizing what this entails in order to prescribe something for everyone would counteract the point. Discover what is critical, identify what constitutes normal behavior, and then set focused mechanisms in place to look for and alert upon deviations from normality.

Change your approach to event monitoring and log analysis: Based on the data we collect in the Time of Breach events, we believe that organizations would be better served to focus less on the “real-time” methods of detection, and more on the “this-week” methods. If we can shift Compromise to Discovery time frame from Weeks and Months to Days, it will significantly reduce the damage done to your organization. Focus on the obvious things rather than the minutia. 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. We are confident that this approach will reap benefits and save time, effort, and money.

Training and Awareness

Increase awareness of social engineering: Educate employees about different methods of social engineering and the vectors from which these attacks could come. In many of our cases, we see where users click on links they shouldn’t and open attachments received from unidentified persons. Reward users for reporting suspicious e-mail and sites and create the incentives necessary for vigilance.

Train employees and customers to look for signs tampering and fraud: Such awareness campaigns have been around in certain areas for some time, but ATM and Pay-at-the-Pump tampering/fraud seem to be increasing in number and scope. Organizations operating such devices should consider conducting regular examinations of them. Additionally, empower customers to help protect themselves as well as aiding the organization in spotting potential issues.

Incident Management

Create an Incident Response Plan: If and when a breach is suspected to have occurred, the victim organization must be ready to respond. An effective Incident Response Plan helps reduce the scale of a breach and ensures that evidence is collected in the proper manner.

Engage in mock incident testing: I mean listen, we’re sitting here talking about practice; not an incident, not an incident, not an incident—but we’re talking about practice (sports fans among you might get that reference). Yes, we are talking about practice, because practice makes perfect. In order to operate efficiently, organizations should undergo routine IR training that covers response strategies, threat identification, threat classification, process definition, proper evidence handling, and mock scenarios.

A Call to Data Sharing

One of the most critical and persistent challenges plaguing efforts to manage information risk is a lack of data. As community decision-makers and practitioners, we have little data because we do not share and while there are many reasons for this, doubts that it can be done in a practical, private, and mutually beneficial manner are chief among them. We would like to think that this report is an example that sensitive and useful data can be shared responsibly to the benefit of many. In the past two years, several other investigative firms have begun to share their results and we commend those efforts. Every little “bit” shared helps. It would be great if others joined in as well—and if you’d like to report results using VERIS so we can all compare apples to apples, we’ll be glad to help however we can.
We would also like to extend an invitation to other organizations to consider using the VERIS community website to anonymously report security incidents (any kind—not just data breaches). All (aggregated and anonymous) results will be made freely available to the community. By sharing incident information, you will add to the collective knowledge of the community while gaining access to the VERIS dataset for yourself. The overall goal is to lay a foundation from which we can constructively and cooperatively learn from our experiences to better manage risk.

We realize that your time is valuable, so we once again thank you for taking out a chunk of it to read this report.