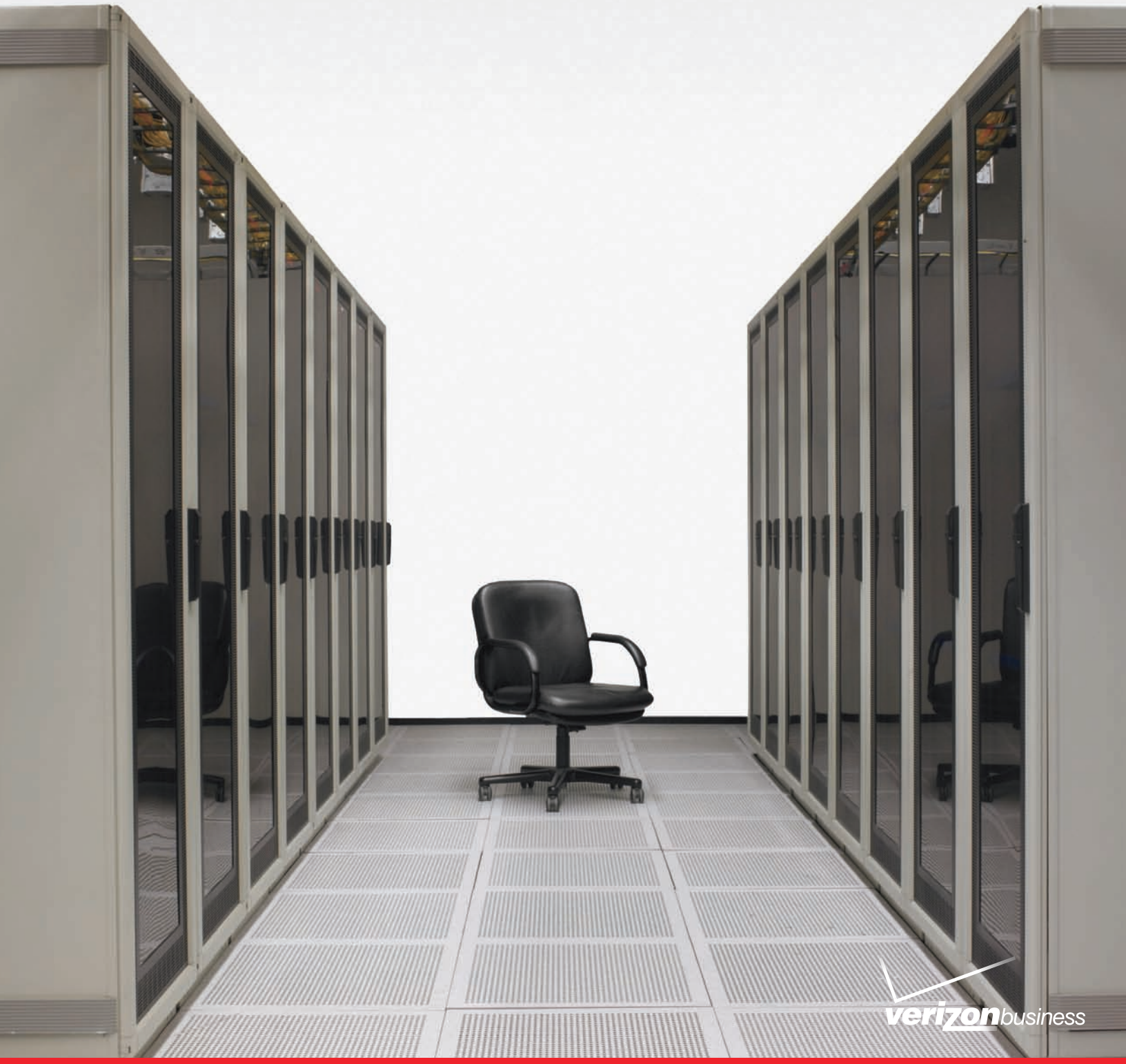
A Study CONDUCTED BY THE VERIZON BUSINESS RISK TEAM

2008 DATA BREACH INVESTIGATIONS SUPPLEMENTAL REPORT

Industry Focus. More Analysis. Greater Insight.

A comparison of risk factors among the finance, food, retail, and tech industries.



verizon business

2008 Data Breach Investigations Supplemental Report

A study conducted by the Verizon Business RISK Team

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

Authors

Wade H. Baker

C. David Hylender

A. Bryan Sartin

Peter Tippett, Ph.D., M.D.

J. Andrew Valentine

Members of the RISK Team

TABLE OF CONTENTS

verizon business

2008 Data Breach Investigations Supplemental Report

A study conducted by the Verizon Business RISK Team

Introduction

Verizon Business published the *2008 Data Breach Investigations Report* (DBIR) in June of this year. Compiling four years of data from over 500 cases worked by the Verizon Business Investigative Response team, it was intended to be a kind of "state-of-the-union" look at recent security breach and data compromise trends. As those who read the report already know, the picture it painted was not altogether rosy.

The DBIR presented statistics in aggregate across all the organizations in our caseload and did not delve into the state of affairs within each of the industries represented (see Figure 1 for distribution). However, since the original publication, we continue to receive many requests for industry-specific data and comparisons. It is the goal of this *2008 Data Breach Investigations Supplemental Report* to meet these requests.

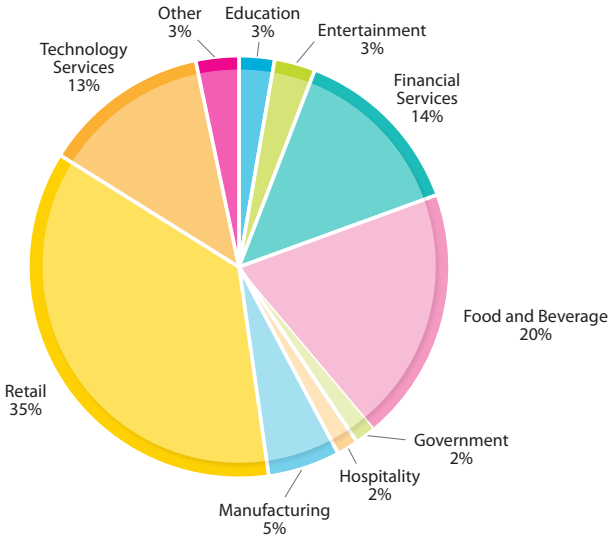


Figure 1. Industries Represented (Original DBIR)

Based on Verizon Business's 2004 through 2007 caseload, we identified industry groups offering a sufficient sample size for independent data analysis. Four industries met this requirement: Financial Services, Food and Beverage, Retail, and Technology Services. It is important to note that no new data was collected for this supplemental report; it leverages the same data set used in the original DBIR. The 2009 DBIR (planned for publication in early 2009) will add new data collected in 2008 along with additional case metrics.

The format of this report is relatively straightforward. It covers the same basic findings as the DBIR except that five sets of statistics (one for "All" organizations plus the four selected industries) are presented and discussed within each section. It is our hope that this industry-specific point of view will bring more clarity to the subject matter and provide additional information helpful to the planning and security efforts of our readers.

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. Furthermore, though we present industry-specific statistics, it is important to remember that the individual organizations within those industries often vary greatly from the aggregate results. What is said of the group cannot always be said of its members. These statistics are based solely upon breaches Verizon Business investigated between 2004 and 2007. Any conclusions or inferences we make are drawn from this sample. Although we believe many of these results to be generally applicable, bias undoubtedly exists. Even so, there is a wealth of information here and no shortage of valid and clear takeaways. As with any study, the reader will ultimately decide which findings are applicable within their organization.

Results and Analysis

Breach Source

As with the original 2008 DBIR, this supplemental report considers three main sources, or origins, of data breaches. They are as follows:

***External*—**Intuitively, external threats originate from sources outside the organization. Examples include hackers, organized crime groups, and government entities but also environmental events such as typhoons and earthquakes. Typically, no trust or privilege is implied for external entities.

***Internal*—**Internal threat sources are those originating from within the organization. This encompasses human assets—company executives, employees, and interns—as well as other assets such as physical facilities and information systems. Most insiders are trusted to a certain degree and some, IT administrators in particular, have high levels of access and privilege.

***Partner*—**Partners include any third party sharing a business relationship with the organization. This value chain of partners, vendors, suppliers, contractors, and customers is known as the extended enterprise. Information is the lifeblood of the extended enterprise and it flows far beyond the boundaries of any single organization. For this reason, some level of trust and privilege is usually implied between business partners.

Figure 2 depicts the percentage of breaches attributed to internal, external, and partner sources for each industry. Since many breaches involve multiple sources, the percentages sum to more than 100 percent. Though this sometimes indicates collusion, more commonly one party is an unsuspecting participant to the crime.

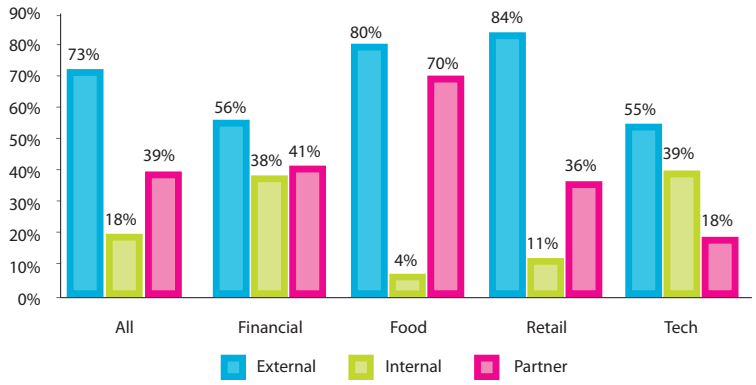


Figure 2. Sources of Data Breaches

The predominant pattern to note here is that each industry exhibits the same pattern or order (external sources being highest, followed by partner sources, then internal ones) except Tech Services, in which insider breaches were more common than those involving partners. Tech Services are often in the role of "the partner" to the other industries, providing management, hosting, and other services. It stands to reason that organizations in this industry likely employ a high percentage of tech-savvy staff and grant them high levels of access to numerous systems. Unfortunately, some find that access to sensitive and valuable resources is a temptation too hard to resist. Facing similar temptations, insiders in the Financial Services industry were behind a large proportion of breaches as well.

The Food and Beverage industry shows a very different yet striking series of statistics. Insider breaches fall well below other industries, while the percentage for partners is extremely high—nearly equaling that of external sources. At first, this may seem counterintuitive as staff within this industry constantly handle money, checks, and credit cards. When incidents happen, however, they are more likely to be handled by law enforcement personnel than by our Investigative Response team, since such thievery doesn't typically involve the compromise of information systems.

The large percentage of partner breaches in the Food and Beverage industry is mostly due to the scenario in which an external attacker compromises a partner and then uses trusted systems and connections as a privileged platform to attack the victim. For Food and Beverage establishments, this is often a vendor supporting the point-of-sale (POS) system using default or shared credentials among many clients. Though not a willing accomplice, the partner's lax security practices—often outside the victim's control—undeniably allow such attacks to take place. This is obviously a much-needed area of focus for security efforts within the Food and Beverage industry.

Breach Size and Source

Readers may remember our "back-of-the-napkin" calculation of risk (likelihood x impact) for external, internal, and partner sources from the original DBIR. These parameters are recorded in Table 1 and the highest source of risk for each industry is highlighted.

Table 1. Simplified Risk Calculation

Industry	Source	Likelihood	Impact (# of Records)	Risk (Pseudo)
All	External	**73%**	30,000	21,830
	Internal	18%	**375,000**	68,617
	Partner	39%	187,500	73,404
Financial	External	**56%**	4,000	2,250
	Internal	38%	175,000	65,625
	Partner	41%	151,250	61,445
Food	External	**80%**	30,000	24,130
	Internal	4%	**200,000**	8,696
	Partner	70%	125,000	86,957
Retail	External	**84%**	45,000	37,778
	Internal	11%	**250,000**	27,778
	Partner	36%	112,500	40,278
Tech	External	**55%**	500,000	272,727
	Internal	39%	1,107,600	436,314
	Partner	18%	**6,000,000**	1,090,909

As a reminder, we are not asserting that the consequences of a breach are limited to the number of records compromised; we use this measure merely as an indicator of the overall financial impact. Though data breaches are more likely to originate outside the organization, insiders tend to cause larger breaches. Tech firms, however, buck this trend and show a drastically higher number of records compromised for incidents involving business partners. Though the median is not as prone to skew as the mean, this statistic for Tech Services is, to some degree, the result of a few very large breaches in our caseload from this industry.

Taken as a whole, business partners represent the greatest risk for data compromise according to our sample of cases. The same is true for all industries in the scope of this study with the exception of Financial Services, where insiders edge out partners as the chief risk. For Financials, the score for external risks is incredibly small and suggests where future mitigation efforts should be focused in that industry. Retail is the only industry for which external nearly becomes the highest source of risk. It also shows the most equal distribution of risk among the three sources.

Breakdown of External Sources

Based on investigative evidence corroborated with other supplemental information, the geographic distribution of external attacks is provided in Figure 3. Though some differences do exist between the four industries, for the most part, they are marginal save for a few notable exceptions. The proportion of attacks attributed to North America for Financial Services is somewhat larger than other industries. This is in line with a trend among our cases of more targeted, focused, multi-faceted attacks aimed at Financials, especially in the United States. Through collaboration with law enforcement agencies, we were able to confirm several instances of U.S.-based attackers with ties to foreign organized-crime groups. Many of these groups reside in Eastern Europe and are largely responsible for the relatively high percentage of direct attacks from that region against Retail companies. We see no significant trend behind the sizeable portion of attacks against the Food and Beverage industry originating from Western and Southern Europe.

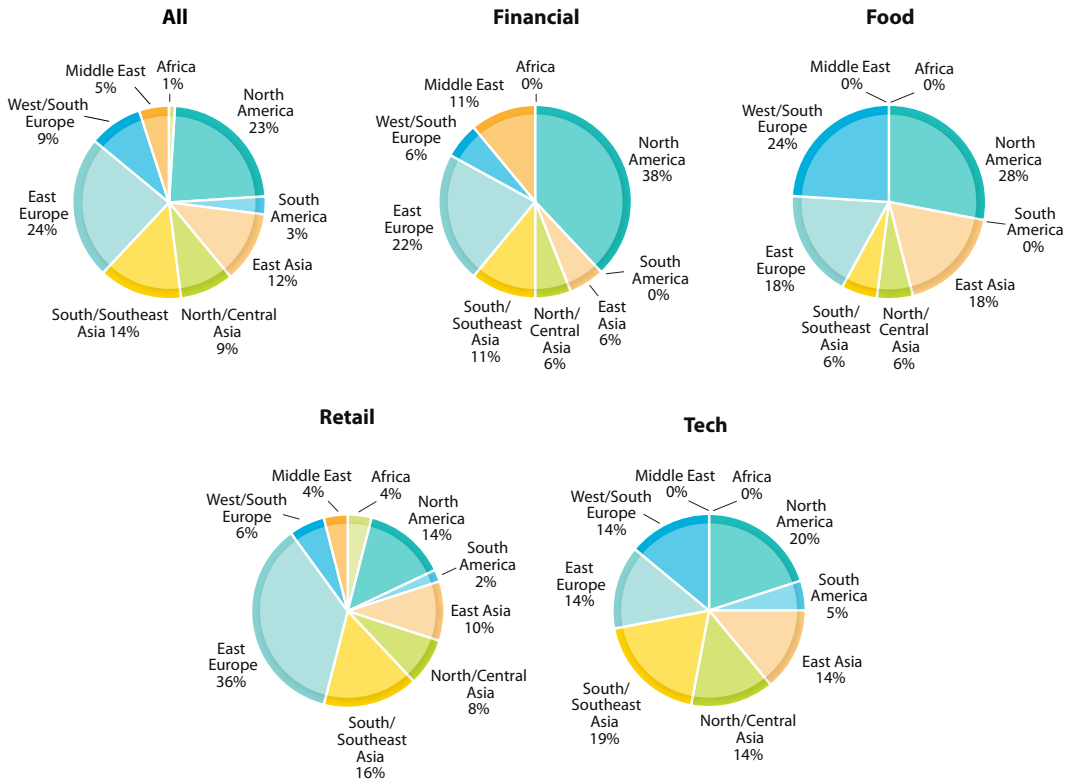


Figure 3. Location of Attacking IPs

Breakdown of Internal Sources

A closer analysis of internal breaches yields some interesting findings. Only in Financial Services are end-users responsible for more breaches than IT administrators. Based on our investigative experience, we associate this with the greater access non-IT employees have to sensitive resources. One doesn't require highly privileged access to systems in order to compromise data. This certainly has ramifications on data-protection strategies in this industry. We also note that Financial Services is the only group with breaches tied to agent/spy activity.

Table 2. Breakdown of Internal Sources

	All	Financial	Food	Retail	Tech
Anonymous	5%	8%	Insufficient number of cases for statistical analysis	11%	0%
End-User	41%	53%		33%	23%
IT Admin	50%	31%		45%	77%
Executive	2%	0%		11%	0%
Agent/Spy	2%	8%		0%	0%

On the other hand, IT administrators are behind the vast majority of breaches in the Tech Services industry. This is clearly a function of the services provided by these firms, which often involve a significant IT support, management, or hosting element. The ratio of admins to end-users is more evenly distributed among retail companies. Interestingly, a fair number of investigations pointed to a retail executive as the responsible party.

Breakdown of Partner Sources

Table 3 further illustrates the pervasiveness of the "hijacking" scenario described earlier, especially with respect to the Food and Beverage and Retail industries. As stated previously, this frequently involves a remote access connection utilized by a vendor to support a client's systems and applications. In many cases, we find the vendor neglected to change default settings and credentials, making the attacker's job all too easy. The common tendency to utilize shared credentials among clients enlarges the scope of the problem.

Table 3. Breakdown of Partner Sources

	All	Financial	Food	Retail	Tech
Anonymous	21%	31%	13%	17%	Insufficient number of cases for statistical analysis
Remote End-User	3%	15%	0%	0%	
Remote IT Admin	16%	15%	13%	17%	
On-Site Partner	3%	8%	0%	0%	
Partner Asset or Connection	57%	31%	74%	66%	

Though less than half the percentage seen in Food and Beverage and Retail, the Financial Services industry is far from immune to problems surrounding partner assets and connections. As a reminder that not all breaches within the extended enterprise are unintentional, malicious action on the part of IT administrators is a fairly consistent and real threat to each industry. For Financial Services organizations, end-users proved to be equally guilty of illicit activity.

Case Study: Retail

In mid 2007, credit card fraud patterns pointed to a large retail chain as a possible data breach victim. The retailer had no idea that anything had occurred or what systems might be affected. When law enforcement personnel found no conclusive evidence of employee fraud, they contacted Verizon Business in order to help prove or disprove the compromise, and, if necessary, acquire evidence to make a criminal case.

Within a short time, the Investigative Response team was able to obtain hard evidence that a security breach did occur. After making this determination they were able to track the source to a virtual private network (VPN) concentrator used by a third-party vendor to access and manage the retailer's entire POS network. Apparently, an external attacker had gained administrative access to the network via one of the vendor's VPN accounts. Unfortunately, the perpetrator had covered his tracks by erasing his IP address from the VPN logs and left no way to pinpoint the source and close the breach.

From the standpoint of making a criminal case, this was a definite setback. Because the retailer happened to be a Verizon Business Internet customer, another means of identifying the geographic location of the hacker was available. Working with the retailer, Verizon Business produced a 12-hour window of Internet activity showing all IP addresses entering and exiting the retailer's VPN concentrator. Only one IP address had entered during the time of the breach and it pointed to Eastern Europe. The breach was closed and the findings were quickly communicated to the appropriate law enforcement agency.

Threats and Attacks

In their continuing efforts to breach systems and compromise data, criminals employ a myriad of techniques. Examining the frequencies and trends surrounding these threats is essential to safeguarding information assets. It is logical to assume that the threat landscape varies for each organization and especially so among different industries. Figure 4, which depicts the prevalence of each category as a contributing factor to breaches in our caseload, appears to support this assumption.

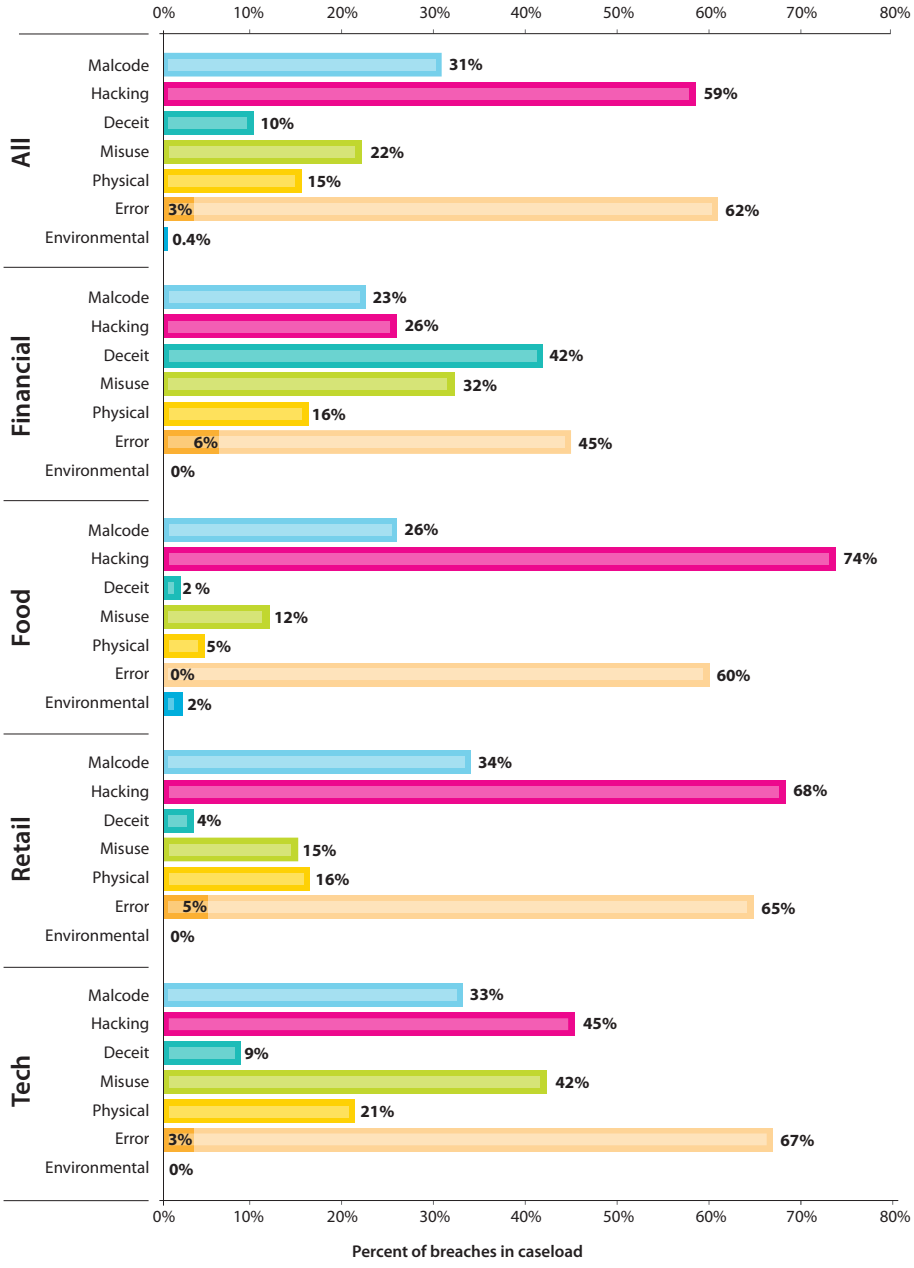


Figure 4. Threat Categories

As a reminder, the 2008 DBIR distinguished between errors that directly caused the incident (the solid region of the "Error" bar) and those that significantly contributed to it (the shaded region). We do the same here, and it is apparent that errors lead to many breaches regardless of industry. Hacking is also widespread and is the leading category of threat (aside from indirect errors) for Food and Beverage, Retail, and Tech Services. Many hacks are relatively "cheap" for the attacker to conduct (often quick, automated, and anonymous) and this overwhelming majority—especially in Food and Retail—speaks to an abundance of soft targets in these industries. In Financial Services, however, hacking falls behind deceit and misuse. In general, we find a much more "balanced" set of tactics in use against Financial and Tech Services firms, likely due to a more hardened security posture that makes them less vulnerable to automated attack tools.

An interesting observation from Figure 4 is that misuse, which refers to using granted resources and/or privileges for any unauthorized purpose, is much higher in Financial and Tech Services. This is related to the larger percentage of insider breaches within those industries (to misuse something one must be authorized to use it). Such behavior is inherently difficult to control but we often find that a lack of accountability over employee activities exacerbates the issue. Trust is needed, but it need not be blind.

For the most part, malcode and physical attacks are consistent across the four industry groups. Threats falling within the category of deceit, however, proved to be substantially higher for Financial Services organizations than any other. In the face of hardened networks and systems, criminals often set their sights on softer human targets.

Threat Category Breakdowns

In the remainder of this section, we highlight more detailed findings within the main threat categories discussed above. In many instances, there are not enough cases to support statistical analysis at this level.[1] We therefore restrict further breakdowns to error, hacking, and malcode, the top three categories across the industries represented (Financial Services being the exception). Even among these, sample sizes are sometimes not sufficient and this is noted within figures and tables. Where appropriate, references are also made to findings within the remaining categories. We begin with error.

It could rightly be said that some form of error occurs somewhere in the chain of events surrounding nearly all data breaches. While this is true, our investigators focus on errors that directly cause or significantly contribute to the incident. Table 4 depicts several broad types of errors encountered by our team within each industry.

Table 4. Breakdown of Error

	All	Financial	Food	Retail	Tech
Omission	80%	70%	79%	76%	88%
Misconfiguration	15%	20%	21%	16%	8%
Inadvertent Disclosure	3%	5%	0%	3%	4%
User Error	2%	5%	0%	3%	0%
Technical Failure	1%	0%	0%	2%	0%

1 For instance, of the 500-plus cases, 14 percent were Financial Service organizations and 16 percent of those exhibited threats in the physical category. This yields approximately 11 cases (500 x 0.14 x 0.16) involving physical attacks. A statistical breakdown of those 11 cases would not provide meaningful information.

The message is loud and clear; omissions plague everyone. Omissions often entail standard security measures that were believed to have been implemented, but in actuality were not. It hardly seems worth mentioning that Financial Services posted the lowest proportion of omissions, since 70 percent doesn't exactly mean they're better off than the rest of the field. "Check, recheck, and check again" seems to be a universally applicable recommendation. What is worthy of mention is that Tech Services suffers a higher percentage of errors of omission than any other industry. This seems counterintuitive as one would like to think that providers of technical services are less susceptible to such blunders.

Case Study: Tech Services

When the hosting clients of one Tech Services firm began to complain about modification and removal of information on their web portals, Verizon Business was called in to determine if a security breach was behind these occurrences. The firm offered its clients, consisting of several hundred small businesses, a web-based content management system (CMS) to manage and update their web portals. Once the Investigative Response team confirmed that an unauthorized intrusion had indeed taken place (and that files containing personally identifiable information, or PII, had been accessed), the focus shifted to containment and mitigation.

The root cause of the breach was soon apparent: a lack of proper authentication credentials. After acquiring clients, it was discovered that the hosting provider rolled out both production and testing web pages to the Internet, but neglected to secure them with any form of log-in requirement. To access a client's CMS (and thereby gain administrative control of the web portal), the intruder needed only to bring up www.companyname.com/admin in a web browser and walk in through the open door.

Deeper examination of the hacking category in Figure 4 reveals that attacks targeting applications, software, and services were the most common technique across all industries with sufficient sample size. In the limited number of cases for Financial Services, the scales tipped slightly in the other direction toward OS/platform attacks. At the application level, SQL injection and authentication bypass scripts were widespread, especially in the Food and Beverage and Retail industries. Compromise of remote access/desktop software and services also occurred quite frequently. Each industry showed similar proportions of OS/platform hacks while Tech Services suffered considerably more attacks exploiting backdoors and control channels.

Table 5. Breakdown of Hacking

	All	Financial	Food	Retail	Tech
OS/Platform Configuration or Functionality	24%	Insufficient number of cases for statistical analysis	31%	25%	0%
OS/Platform Vulnerability	13%		0%	1%	29%
Application/Service Configuration or Functionality	49%		58%	49%	14%
Application/Service Vulnerability	15%		0%	4%	24%
Backdoor/Control Channel	24%		12%	19%	33%

Comparing the ratio of attacks which exploit vulnerabilities to those that exploit configuration weaknesses or functionality yields some interesting findings (yes, we understand that "weaknesses" can be considered "vulnerabilities" but please bear with us on what we feel is a useful distinction to make here). Virtually none of the attacks against Food and Beverage and Retail companies exploited vulnerabilities, whereas we see the opposite result for Tech Services. Investigations involving Financial Services organizations also suggested a greater emphasis on vulnerabilities. Though this may seem perplexing, the simple explanation is that attackers do not rely on vulnerabilities to access systems in the Food and Beverage and Retail industries—poor security configurations provide a much wider door. Tech firms seem to do a better job on basic system and application configurations, forcing attackers to rely on vulnerabilities. Of course, this still does not place the hallowed security crown upon the brow of the Tech Services industry. The logical conclusion is that while the first wave of attacks might be repelled, vulnerability management practices are not adequate to prevent data breaches.

In the malcode category, the industry groups follow a pattern similar to the general (All) statistics with a few notable exceptions. Far more common than any other delivery method was malcode installed on a compromised system by a remote attacker. Cases worked in the Financial Services industry, though smaller in number, revealed the same trend. Less and less dependent on a shotgun approach, malcode is increasingly customized for a specific purpose and even a specific target.

Table 6. Breakdown of Malcode

	All	Financial	Food	Retail	Tech
E-Mail	14%	Insufficient number of cases for statistical analysis	15%	16%	7%
Network Propagation	13%		31%	6%	7%
Downloaded via Web	13%		8%	13%	7%
Physical Installation	2%		0%	0%	14%
Planted by Attacker	59%		46%	65%	64%

More than any other industry, Food and Beverage suffered from malcode with network propagation capabilities. In our experience, this is not always random functionality. We observed a number of cases in which criminals tailored malcode to replicate across servers in multiple locations, effectively spreading through a chain of Food and Beverage establishments. POS systems are often the vector for this diffusion.

Malware infection via e-mail and web browsing tends to be higher for Food and Beverage and Retail than Tech Services. In these establishments, we often find that critical payment and inventory servers are used for personal e-mail and web activities. Needless to say, this practice is not advisable and adds unnecessary risk. The higher percentage of physically installed malcode in Tech Services firms typically involves a sniffer or similar tool loaded by the local administrator. This is one of the reasons why the median size of breaches within this industry is so much larger than the others.

Given the small number of applicable cases in each industry, it is difficult to draw valid conclusions from within the remaining threat categories. We can, however, offer a few observations. Of attacks falling within the category of deceit, phishing scams and other types of fraud were especially prevalent among Financials. Elaborate forms of social engineering were also much more common to this industry. In all industries, misuse almost always involved deliberate malicious action rather than the many non-malicious forms of misuse. In the physical category, observation (i.e., shoulder surfing) was only seen in Financial Services. Retail was prone to wiretapping and sniffing. Unauthorized physical access of systems and tampering appeared to be more prevalent to Tech Services and Food and Beverage.

Attack Pathways

Beyond threat categories, an analysis of the pathways utilized by attacks on information systems is a useful exercise. Across all industries, attackers frequently gained access to the victim via one of the many types of remote access and management software. From Figure 5, it is apparent that this does not hold true for each industry. Retail and Food and Beverage are particularly susceptible to this attack vector. Within these industries, this involves third-party connections provisioned for the management of payment-related networks and systems. The security issues related to such interactions have been discussed previously.

Conversely, we found significantly fewer breaches in Financial Services that involved remote access and management connections. As already shown, Financial Services organizations suffered from a high percentage of insider misuse and these insiders preferred physical vectors over remote networks. As an aside, this also explains the higher proportion of physical-vector attacks within Tech Services. Secondly, we see fewer instances in which vendors utilize shared connections and credentials among Financial Services institutions. This is likely due to more stringent control and third-party contracts in that industry.

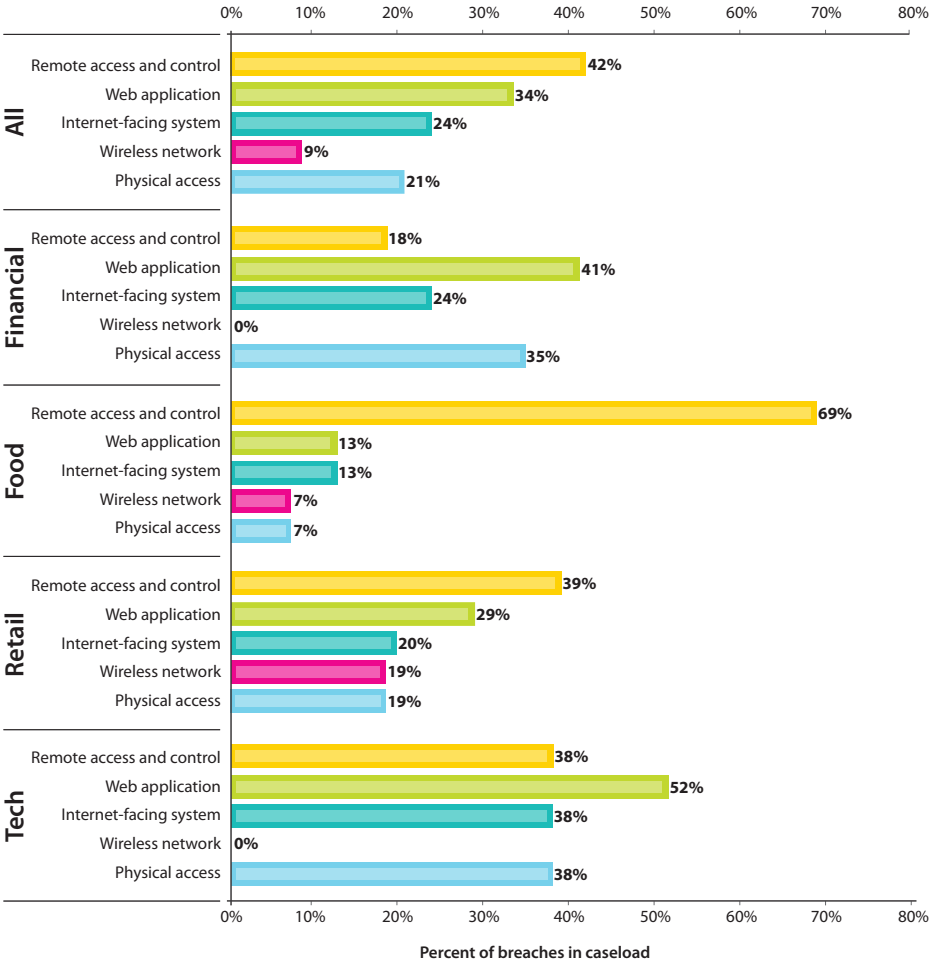


Figure 5. Attack Pathways

For Financial and Tech Services, the majority of attacks exploited web applications. This makes sense, as their web presence is essential to serving customers and conducting daily business activities. After examining the results of the "Threats and Attacks" section of this report, one may wonder why hacking is relatively low for Financial Services organizations if web applications are so prominent a vector. This is due to our inclusion of attacks like phishing and

content spoofing (which exploit this vector) in the deceit category. Within the Food and Beverage industry, web applications as a pathway of attack are relatively low. Many of these establishments do not have an online presence. Those that do, for the most part, do not engage in financial transactions through their web portals.

A final observation from Figure 5 is that no breaches in the Financial or Tech Services industries involved wireless infrastructure. Throughout the entire caseload, we did not encounter a successful attack against an adequately secured wireless network. Such instances in the Food and Beverage and Retail industries stemmed from poor configuration and weak encryption.

Attack Difficulty

The relative difficulty of attacks that successfully compromise enterprise systems is not only an excellent indicator of the current threat environment, but also the state of modern security programs. You may remember that investigators classified attack difficulty according to the following descriptions:

None—No special skills or resources were used. The average user could have done it.

Low—Low-level skills and/or resources were used. Automated tools and script kiddies.

Moderate—The attack employed skilled techniques, minor customization, and/or significant resources.

High—Advanced skills, significant customization, and/or extensive resources were used.

One of the telltale findings from the 2008 DBIR was that more than half of breaches were caused by rather unsophisticated attacks. On the whole, organizations are not making the criminals work very hard to compromise information, but does this hold true from an industry-by-industry perspective? Figure 6 gives the answer.

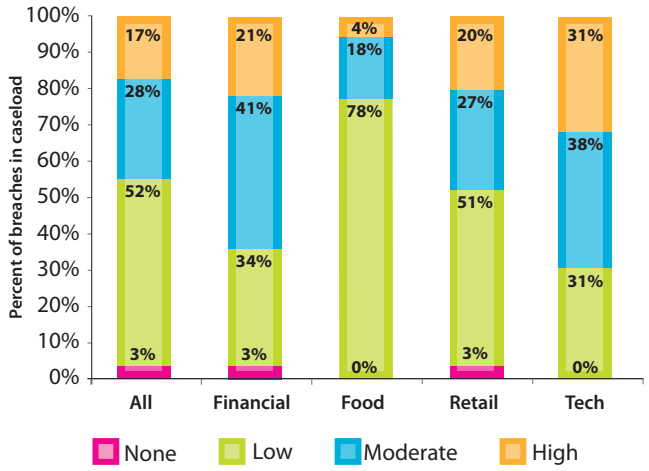


Figure 6. Attack Difficulty

Regrettably, low-difficulty attacks are succeeding across all industries and are rampant in Food and Beverage. This has much to do with inadequate security practices as well as a high degree of homogeneity among systems within the industry. Food and Beverage (and to a certain extent, Retail) establishments often use the same POS systems supported by a single vendor. If the criminal finds a weakness inherent to these systems, it opens the door for copycat hits across a wide range of victims. This type of "skeleton key" attack is a prime example of the "directed opportunistic" category described in the next section. Furthermore, compromising the vendor directly allows easy access to numerous clients when shared or default credentials are in use (which is, unfortunately, not uncommon). The Food

and Beverage and Retail industries would benefit greatly from efforts to reduce the occurrence of these low-effort, high-yield attacks.

The situation is somewhat different for Financial Services and Tech Services. Compromising these organizations seems to require more difficult, multi-faceted attacks. Investigators noted that, in some cases within these industries, preventing breaches would have required the implementation of more advanced or costly controls. As presented in the 2008 DBIR, this is certainly not the case for the vast majority of incidents where less advanced controls would have sufficed. Tech firms tend to be a bit more security conscious and have knowledgeable personnel and better resources at their disposal. Likewise, many Financial Services firms take security very seriously and boast rather large budgets and mature programs for managing information risk.

Given all this, the 20 percent of attacks rated highly difficult in the Retail industry may seem inconsistent to readers. While many retailer breaches involved simple attacks, we did observe some sophisticated (and rather impressive) tactics leveraged against them on occasion.

Targeted vs. Opportunistic Attacks

Standard convention in the security industry classifies types of 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:

Opportunistic (Random)—Attacker(s) identified the victim while searching randomly or widely for weaknesses (i.e., scanning large address spaces), then exploited the weakness.

Opportunistic (Directed)—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 7 contains the distribution of these attacks for each industry and, for the most part, shows exactly what one would expect—Financial Services and Tech Services are more likely to be targeted while Food and Beverage and Retail are less so. Indicative of the scenarios described in the previous section, directed opportunistic attacks represent the majority in both Retail and Food and Beverage. These industries are rarely fully targeted; criminals are looking for an easy score of payment card data and do not care where they get it. If much effort is required, they will quickly move on to the next opportunity.

Attackers often have a more specific target in mind when leveling their sights at Financial and Tech Services firms and tend to be more determined to obtain it.

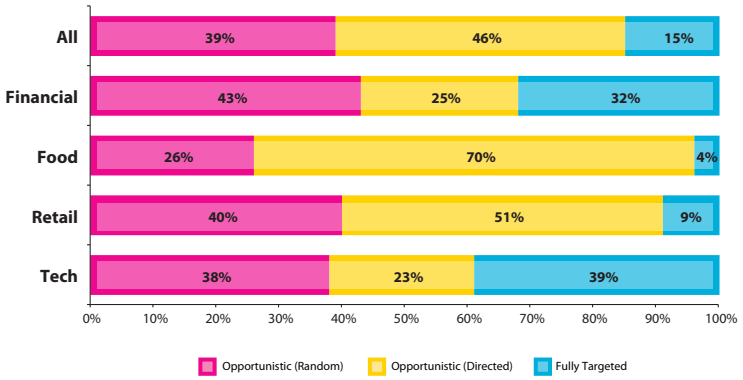


Figure 7. Targeted vs. Opportunistic

Asset Types

In terms of the types of assets compromised, case data reveals a similar pattern across each industry; breaches involving online data (servers, databases, applications, etc.) occur far more frequently than any other asset. As stated in the original 2008 DBIR, this is an area where our caseload differs rather strongly from publicly disclosed breach statistics, which typically reveal a higher percentage of offline data and end-user devices.

Table 7. Compromised Assets (Percentage of Records)

	All	Financial	Food	Retail	Tech
Online Data	82%	74	98%	87%	73%
Offline Data	7%	16%	2%	5%	7%
Networks and Devices	7%	5%	0%	5%	11%
End-User Devices	4%	5%	0%	6%	9%

Even though online data represents the majority of breaches in each industry, there are some differences worthy of note. In Food and Beverage, for instance, nearly all incidents involved online data (98 percent), whereas this percentage drops to 74 percent for the Financial and Tech Services industries. Among Financials, offline data accounted for the difference and for Tech Services it was networks and devices. These findings are intuitive. Criminals attacking Food and Beverage and Retail companies overwhelmingly target large online repositories of payment card data, while Financial Services institutions offer a more diverse set of valuable data in various forms. Similarly, Tech Services providers commonly administer or host networks and devices for their clients. These differences are even more pronounced in the following section.

Data Types

A glimpse at Figure 8 solidifies the notion that the modern-day cybercriminal is financially motivated. Payment card data consistently tops the list of compromised data across all industries under analysis. There is a difference, however, in terms of how far the scales are tipped in that direction.

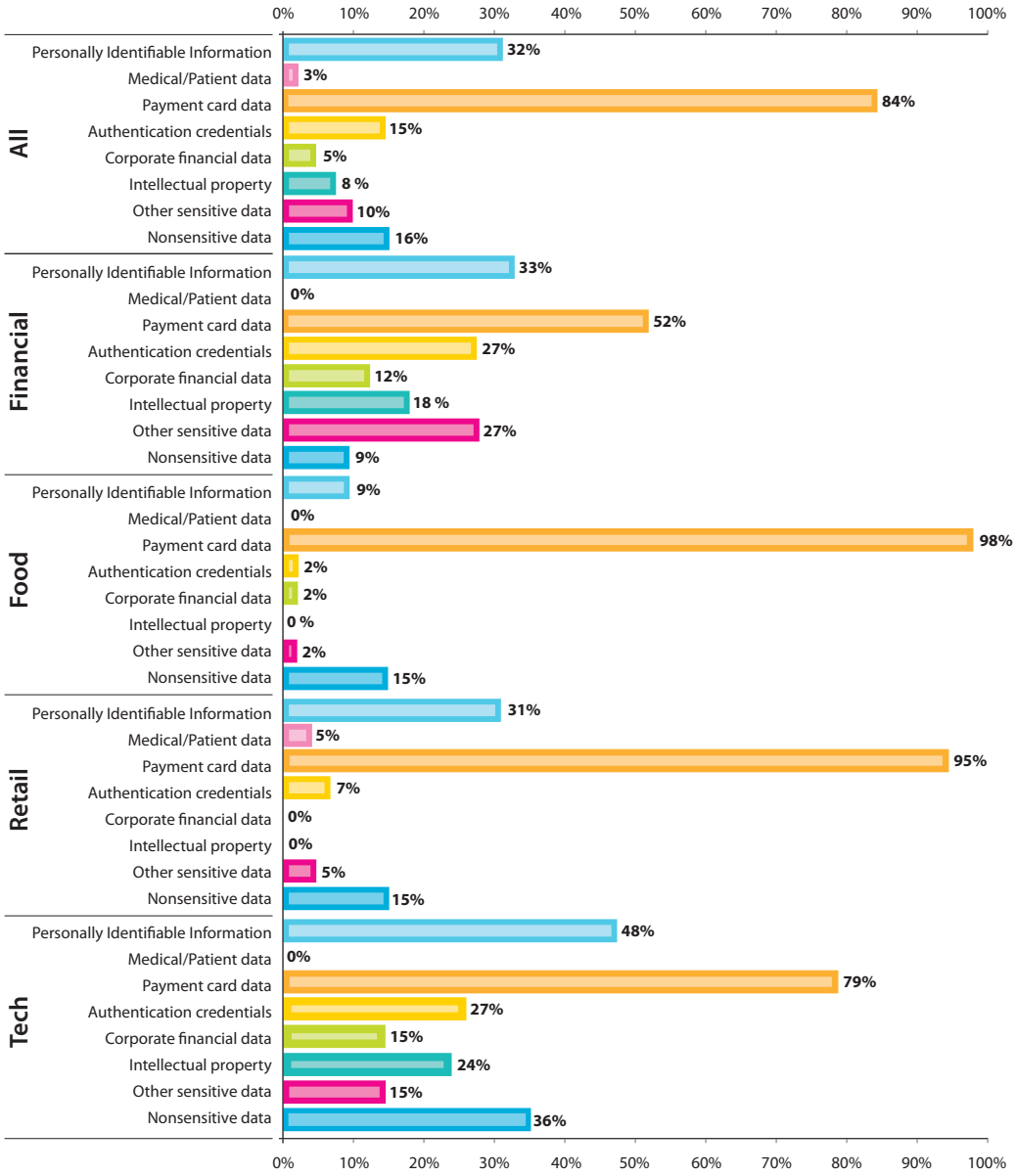


Figure 8. Data Types

Not surprisingly, breaches of payment card data are particularly high within the Food and Beverage and Retail industries. In fact, Food and Beverage compromises are almost exclusively payment card-related while Retail also demonstrates a sizeable portion of personally identifiable information (PII). The latter result is likely tied to the common practice of retailers keeping customer records for use in membership programs, clubs, mailings, etc. Though such a small number, it is worth mentioning (if for no other reason than to stave off confusion) that the 5 percent attributed to medical and patient data within Retail is due to the presence of pharmacies within that industry group.

Though still payment card heavy, Financial and Tech Services are comparatively more balanced among the data types. Each stores a great deal of customer PII (particularly firms specializing in such services as data warehousing) in addition to other data desirable to criminals for various reasons. Authentication credentials, for instance, are sought after because they allow the prospect of increased privileges and access for subsequent illicit activities. As a reminder that criminals aren't only interested in quick cash, compromises to intellectual property account for a substantial portion of breaches in the Financial and Tech Services industries.

Time Span of Data Breach Events

As might be imagined, the time span of events leading up to and following a data breach varies greatly depending on a multitude of factors. Some attacks unfold rapidly, compromising systems within a matter of minutes. Others take months, or even years, of planning and execution. Though any number of events can occur during this time, it is helpful to separate an incident into three major phases: point of entry to compromise, compromise to discovery, and discovery to mitigation. Figure 9 gives a breakdown of time for these three phases in each industry group.

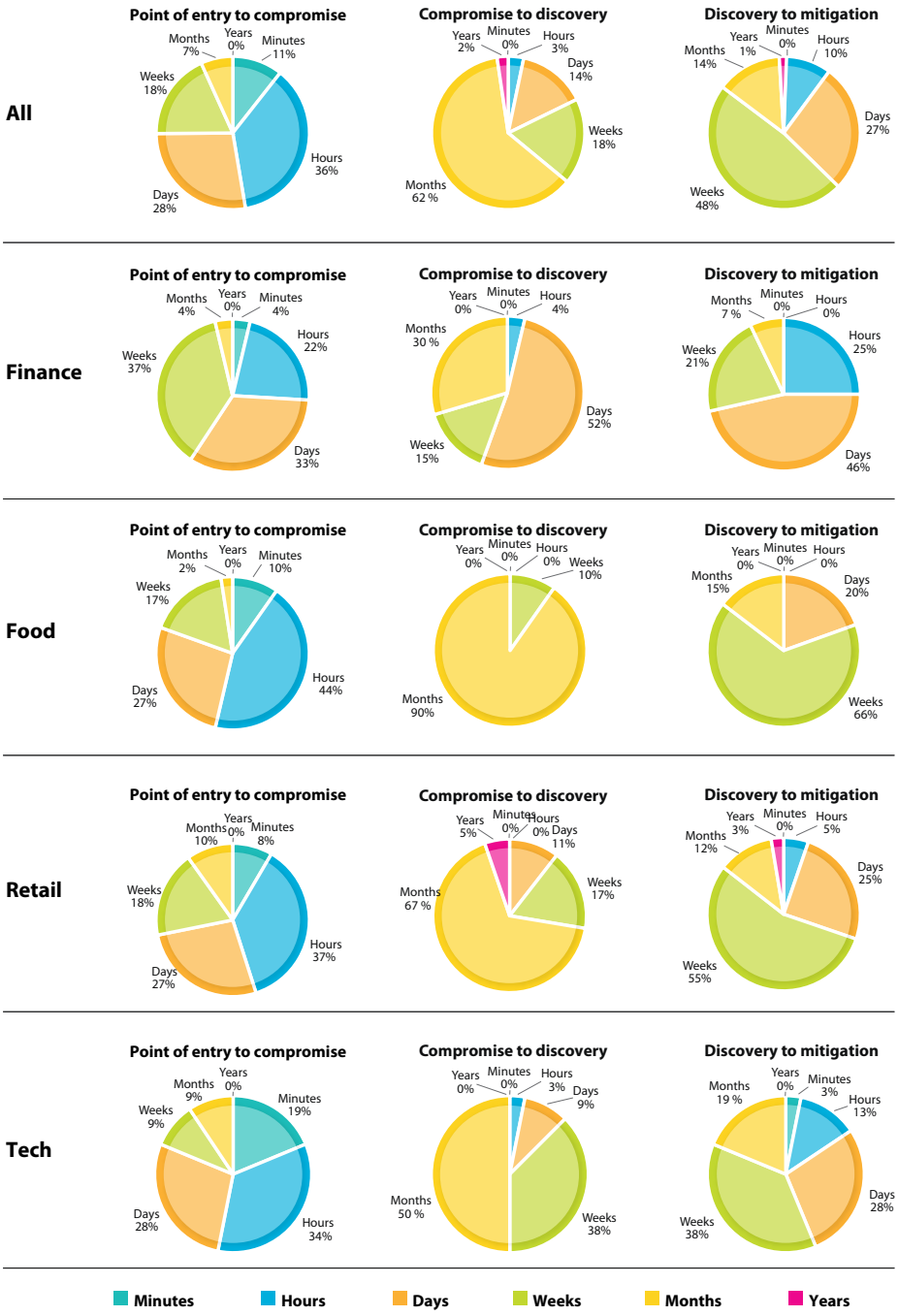


Figure 9. Discovery Time Span

Point of Entry to Compromise

Between entering the corporate perimeter and compromising information, intruders typically explore the network and systems until locating their desired plunder. To an attacker unfamiliar with the territory or when defenses are strong, this can be a time-intensive activity. For Food and Beverage, Retail, and Tech Services, this was accomplished within hours in roughly half of the cases. Much of this can be explained by the extensive use of relatively similar payment systems and applications in the Retail and Food and Beverage industries. After breaching one establishment, intruders know exactly where to find similar information in a subsequent victim's environment and how to quickly access it. For Tech Services firms, homogeneity is less of an issue and this result has more to do with security failures and losing track of assets, data, connections, and privileges (see the "Unknown Unknowns" section).

In contrast, this time frame is noticeably longer in Financial Services. "Weeks" and "days" are the largest segments in Figure 9 and represent over two-thirds of cases. This harkens back to the types of attacks carried out against Financials, which tend to utilize slower, more determined and deceptive methods. When hacking was the method of choice it required more exploration and footprinting.

Case Study: Financial Services

In a rather clever ploy, a Financial Services firm was targeted for infiltration by an international fraud ring. The fraudsters believed they could obtain secret information regarding the manner in which foreign currency-exchange fraud is detected. The heist consisted of several stages, the first of which involved temporary workers whose goal it was to footprint the organization and determine how to access the desired information. The Financial Services firm's human resources (HR) practices were identified as the "low-hanging fruit" and the second phase of the attack was initiated. The ring created a fake background and resume for one of its members, who then applied for an open position as an IT auditor with the organization. He was eventually hired. The sting successfully operated for approximately two weeks until the HR department finally ran a background check and discovered the perpetrator had supplied fraudulent credentials. Verizon Business was engaged to investigate the nature and extent of the breach.

Compromise to Discovery

There is a striking difference between industries in the length of time that passes before an incident is discovered. While we expected longer intervals in Food and Beverage, we were shocked to find that 90 percent of breaches go undiscovered for months. Retail and Tech Services post better times but not by much. Even though Financial Services firms become aware of breaches within days in 50 percent of cases, a sizeable number still go undetected for weeks and months. While this seems like an impressive feat relative to other groups, no industry can claim victory in the contest of timely breach discovery.

Discovery to Mitigation

When examining the time frame between discovery and mitigation, this trend among industries continues. Food and Beverage requires the most amount of time for mitigation, followed by Retail, Tech Services, and, lastly, Financial Services. Those organizations which take longer to respond and remediate breaches often lack formalized and vetted incident-response plans. Though differences exist among industries, there is clearly much improvement needed across the board to effectively deal with post-incident scenarios.

Data Breach Discovery Methods

The length of time that transpires before a victim organization learns it has suffered a data breach begs the question of how this determination is finally made. Moreover, when examining discovery methods within an industry, the distinction between what works and what does not grows even clearer. Figure 10 contrasts breach discovery methods among the four industries represented in this study.

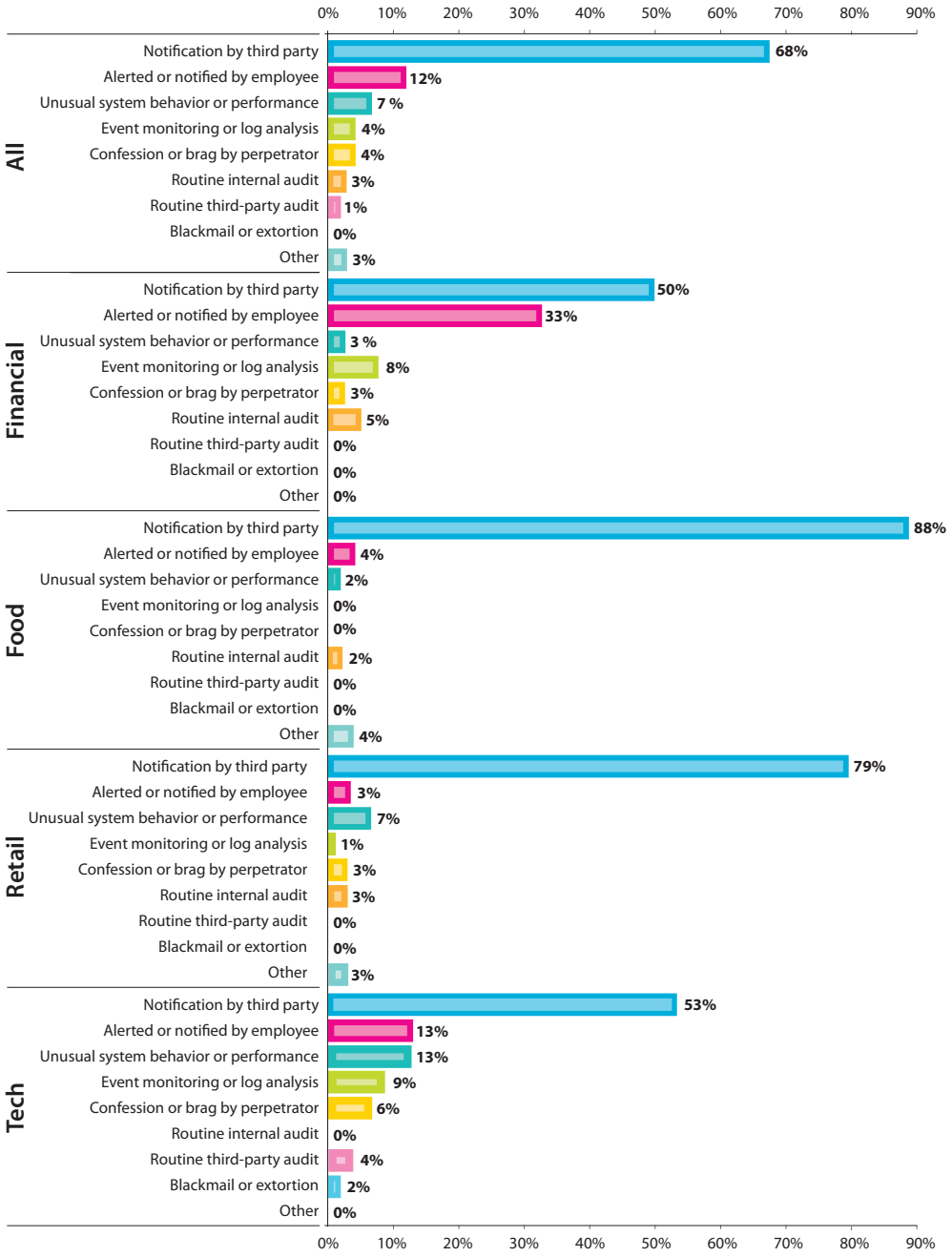


Figure 10. Data Breach Discovery Methods

By far, organizations—regardless of industry—are more likely to learn of breaches after being notified by a third party than any other method. Within the Retail and Food and Beverage industries in particular, the large majority of compromises are discovered only after credit card fraud patterns point to a merchant as the probable source. The very low percentage of breaches discovered by other means in Figure 10 suggests that breach detection is an almost completely reactive process in these establishments. While one does not expect the local small-town diner to have elaborate breach detection mechanisms in place, it would be nice to see a little more proactive approach, especially from the larger chain establishments.

Case Study: Food and Beverage

In an interesting Food and Beverage case, an external intruder exploited the point-of-sale controller in one location of a larger restaurant chain. Using the initial establishment as a launch pad, the intruder was able gain access to additional locations across the country. After this, he remotely installed sniffers designed to capture magnetic stripe credit card information at each payment terminal.

The restaurant chain did not realize there was a problem until months later. After one of the terminals kicked off a "disk space" error, local IT personnel noticed strange files scattered about the system. Verizon Business was contacted to investigate the situation and quickly determined the cause of the error: The files of payment card data captured by the sniffer had grown so large that it consumed all remaining disk space on the system and prevented further writing. Truly, one of the more "resourceful" breach discovery tactics we've ever witnessed.

Although significantly lower, the fact that half or more of all breaches in the Financial and Tech Services industries are detected by third parties is perhaps more disheartening. Event monitoring and auditing at least make a showing, but are still seldom the means of discovery. Quite a few Tech Services firms get the tip-off from abnormal system behavior and employee notification. Financial Services employees discovered one-third of the breaches within that industry during the course of their normal work activities. While we would like to provide adequate reason for this, we cannot do so strictly from the data we have. We suspect that security awareness programs and response training have something to do with this but investigators did not consistently gather sufficient evidence to test this correlation. Conversely, it is entirely possible that employees recognize a problem only after a breach interferes with their daily activities. Based on these findings, we have updated our case metrics collection process and hope to provide more definitive conclusions on this topic in the 2009 DBIR.

Unknown Unknowns

Throughout hundreds of investigations over the last four years, one theme emerges as perhaps the most consistent and widespread trend of our entire caseload. Nine out of 10 data breaches involved one of the following:

- A **system** unknown to the organization (or business group affected)
- A system storing **data** that the organization did not know existed on that system
- A system that had unknown network **connections** or accessibility
- A system that had unknown accounts or **privileges**

We refer to these recurring situations as "unknown unknowns", and they appear to be the Achilles heel in the data protection efforts of every organization. The percentage of cases in which each of these was present within each industry is shown below in Figure 11.

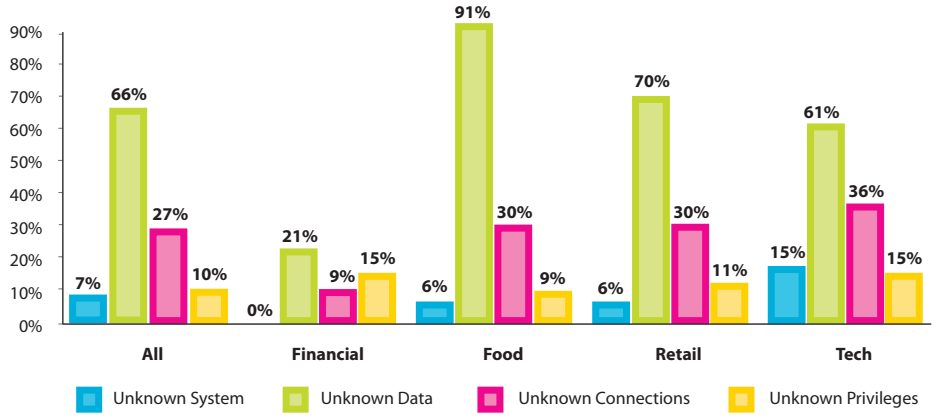


Figure 11. Unknown Unknowns

Evident from the figure, each industry demonstrates the same order of precedence among the unknowns (data, connections, privileges, systems) except Financial Services, in which we observed more instances of unknown privileges than connections. Regardless of industry, many breaches are clearly tied to data the victim did not know was on the system. This is especially true for Food and Beverage, in which over 90 percent of incidents fell within this category. For many restaurants and retailers, this stems from out-of-date POS applications that store transaction data unbeknownst to the merchant. During an investigation, we often discover the merchant did not even know to ask vendors whether the system stores data locally.

Also very noticeable is how much lower the percentages are within Financial Services, where no category is higher than 21 percent. This certainly speaks to the stronger emphasis on asset discovery and classification, tracking, and audits within that industry. It also provides a testimony and incentive to other industries that this problem can be reduced through such practices.

One of the more surprising statistics is that Tech Services records the highest percentage in three of the four categories. One would like to believe that Tech Services firms—which often manage the assets of others—are on top of their game. Placing unquestioning faith in the security practices of any organization—regardless of industry or expertise—does not appear to be a prudent course of action.

Conclusion

If we forget for a moment that this report examines only security failures, we might interpret the statistics presented for the Financial Services industry as a kind of success story. Perhaps in some ways it is. We must remember, however, that all the organizations covered herein suffered a data breach of sufficient impact to warrant outside investigation. Granted, it seems more difficult to compromise Financial Services firms and there is no "one size fits all" type of attack, but the end result is the same. That said, these statistics do suggest that security within this industry is more advanced than others. In this regard, there is something to be learned from their (admittedly flawed) example.

The Food and Beverage industry tells an entirely different story. All the findings either directly or indirectly stem from the root issue of POS systems and the vendors that manage them. Most attacks originate from external sources but leverage a POS vendor's trusted remote access connection as a vector into online repositories of payment card data. These attacks rely on poor security configurations and are quick and highly repeatable. Though they represent 20 percent of our caseload, these "smash and grab" cases involving Food and Beverage establishments were an anomaly during a short time from late 2006 through 2007. We have seen far fewer in 2008. Interestingly, the hospitality industry seems to have replaced Food and Beverage as the de facto target of opportunity and exhibits many similarities.

The Retail industry faces many of these same issues but has its own nuances. Attacks via partner connections are less common than in the Food and Beverage industry but are by no means rare. Increased exploits of web applications seem to have taken up some of the slack as well as attacks on wireless networks, which were significantly higher than in any other industry. Simple attacks were prevalent, but a considerable number of more difficult attacks were employed against retail establishments. Retail is highly reliant on third parties to discover breaches but this seems to happen more quickly than in Food and Beverage. Overall, attacks against this industry are largely opportunistic in nature, seeking quick payloads of data that can easily be used for fraudulent purposes.

The Tech Services industry comprises a diverse collection of organizations from data warehousing operations, software firms, IT services, telecommunications providers, consultancies, etc. Likewise, the findings for this industry are varied—even contradictory—and are sometimes difficult to interpret. For instance, errors (especially omissions) contributed to a higher percentage of breaches than in any other industry, yet the industry also boasted the largest proportion of highly difficult attacks. Hacking and intrusion attacks almost exclusively exploited vulnerabilities rather than configuration weaknesses or normal functionality. Tech Services received more targeted attacks, which may contribute to the larger magnitude of these breaches as well as the diverse nature of the compromised data. Web applications represent the most utilized attack vector but other pathways are also common. Malicious insiders are a very real threat and "unknowns" a definite challenge for organizations in this industry.

We hope this report expands and clarifies the findings presented in the *2008 Data Breach Investigations Report* in ways that are helpful to your organization. Even if your industry is not included among the four discussed throughout this report, perhaps you can identify with certain characteristics of them or experience similar challenges in your business environment. At the very least, this supplemental report should reinforce the notion that an efficient and effective information security program cannot be achieved through a standardized template applied without regard to the unique risks faced by each organization.

WP13242 10/08

WP13242 10/08

www.verizonbusiness.com

verizon business