Follow the Data:
Dissecting Data Breaches
and Debunking Myths

Trend Micro Analysis of Privacy Rights Clearinghouse
2005-2015 Data Breach Records

Numaan Huq

Forward-Looking Threat Research (FTR) Team

Contents

"One massive hack after another," this statement would probably best describe what's happened over the past 10 years. Data breaches have become a status quo, an alarming fact, but not surprising, considering how attackers keep finding ways to infiltrate networks and steal information.

These breaches are damaging. You only have to look at the past few months for proof. In February, the Anthem insurance company announced a breach that exposed millions of its confidential records. The hack on the United States (US) Office of Personnel Management (OPM) in June put 21.5 million of the country's government employees and applicants at risk. Most recently, this August, the Ashley Madison hack publicly smeared around 32 million of its clientele. These incidents are no laughing matter, especially since they put reputations and actual lives at stake.

A lot has been said about breaches—their impact on victims, their cost, and whatnot—but not much focus is ever placed on the data stolen, where it goes, what other information can be pulled from it, and how attackers can further use it. This paper aims to cover that. We'll follow the data. Thanks to the Privacy Rights Clearinghouse (PRC)'s Data Breaches database, we got to examine what's been taken, draw out probabilities, and investigate related activities in the cybercriminal underground.

Through the analyses, we observed several interesting facts that dispel common myths on data breaches, which may help organizations identify a course of action that would best secure their information. Here are just a few of our more notable findings:

- Hacking or malware were behind 25% of the data breach incidents from 2005 to April 2015.

- Over the past five years, incidents of payment card data breaches have increased 169%.

- The healthcare sector was most affected by data breaches, followed by the government and retail sectors.

- Personally identifiable information (PII) was the most stolen record type. Financial data came in second.

- Apart from the usual credit card, bank account, and PII dumps—whose prices in the underground have plateaued—there was a prominence of ads selling Uber, PayPal, and poker accounts.

In this paper, we'll also share the critical security controls that enterprises must try to establish and strengthen in order to detect intrusions and unintended disclosures that can lead to data breaches.

Our data source

The Privacy Rights Clearinghouse (PRC) is a nonprofit corporation based in California. PRC's mission is to engage, educate, and empower individuals to protect their privacy[1]. They do this by raising consumers' awareness of how technology affects personal privacy, and they empower consumers to take actions to control their personal information by providing practical tips on privacy protection. PRC responds to privacy-related complaints from consumers and where appropriate intercedes on the consumer's behalf/or refers them to the proper organizations for further assistance. PRC documents consumers' complaints and questions about privacy in reports and makes them available to policy makers, industry representatives, consumer advocates, media, etc. PRC advocates consumers' privacy rights in local, state, and federal public policy proceedings.

PRC publishes the "Chronology of Data Breaches Security Breaches 2005–Present[1]," which is a collection of publicly disclosed data breach incident reports that occurred in the United States. The data is compiled from a variety of sources including: media, Attorney General's Office press releases, company press releases, privacy websites, etc.

What is a data breach?

Reports of data breaches affecting governments, hospitals, universities, financial institutions, retailers, and so on dominate the news with increasing frequency. This is merely the tip of the iceberg, with the vast majority of incidents remaining unreported and undisclosed[2, 3, 4]. To better understand these breaches, it is important to define the term. The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27040 defines a data breach as:

> *"Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed[5]."*

A wide range of sensitive data is compromised across all industries from businesses, both big and small, as well as individuals. These include PII, financial, health, education, payment card data, log-in credentials, intellectual property, and others. In the news, data breaches are almost always attributed to hacking or malware attacks. While these play a big role, they do not account for all incidents. Other breach methods frequently observed include insider attacks, theft or loss, and unintended disclosures.

Perpetrators who compromise sensitive data refer to a diverse group that includes insiders, individual criminals, as well as organized and state-sponsored groups. Stolen data is commonly used to commit crimes such as financial fraud, identity and intellectual property theft, espionage, revenge, blackmail, and extortion.

Because data breaches have become an everyday affair, people may have become desensitized to having their personal, financial, health, education, and other data compromised and sold in criminal marketplaces. This desensitization could be the product of several factors:

• There is an overload of daily news articles on data breaches.

• Stolen sensitive data is not as tangible as, for example, a stolen mobile phone.

• The bad consequences of having sensitive data stolen are not instantly felt.

• There is a lack of understanding of the repercussions of sensitive data theft.

The eventual penalty of having sensitive data stolen is high and some victims (of identity theft and fraud, for instance) are left suffering for years through no fault of their own. Data breach disclosure laws exist in the US. But do these provide the protection required to truly safeguard the everyday individual? Are businesses abiding by them and disclosing data breach incidents when they occur?

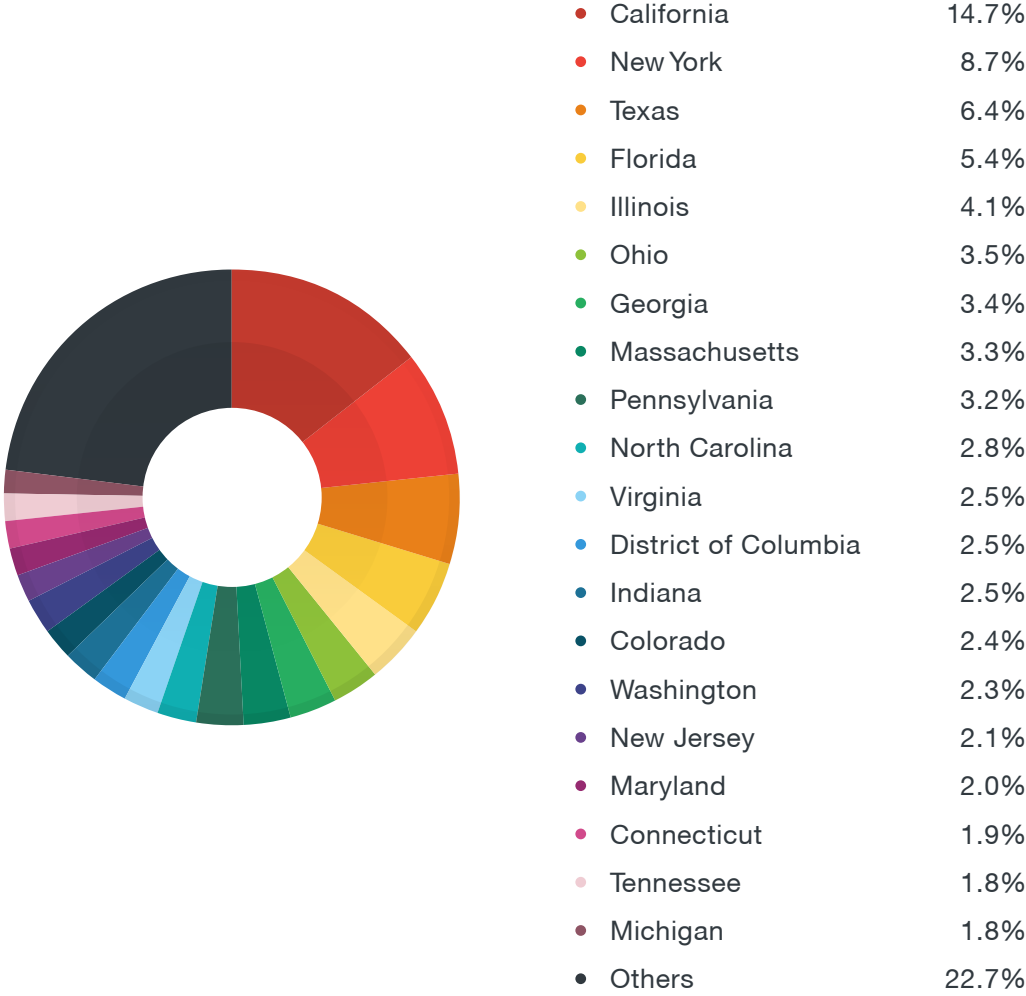|	
California	14.7%
New York	8.7%
Texas	6.4%
Florida	5.4%
Illinois	4.1%
Ohio	3.5%
Georgia	3.4%
Massachusetts	3.3%
Pennsylvania	3.2%
North Carolina	2.8%
Virginia	2.5%
District of Columbia	2.5%
Indiana	2.5%
Colorado	2.4%
Washington	2.3%
New Jersey	2.1%
Maryland	2.0%
Connecticut	1.9%
Tennessee	1.8%
Michigan	1.8%
Others	22.7%

Figure 1: Top 20 US states that reported data breaches

Note: If the impact to the business or organization was multistate, nationwide, or global , the location of the head office was used.

Data breaches are complex events. Any business or organization that processes and/or stores sensitive data is a potential breach target. Even if organizations have an incident response plan to tackle data breaches, figuring out the extent of damage done and managing the response can still be a challenging task. After a breach is discovered, the first questions typically asked are:

- What data or records were stolen?

- How long has the breach been going on?

- How did the attackers bypass defenses?

- How deep did the attackers penetrate the network?

These are difficult questions to answer. Incidents need to be quickly assessed as time is critical when combating active breaches.

It is near impossible to predict if, why, when, where, and how a business or organization will get breached. Breach methods and the data targeted vary across industries and even businesses or organizations within the same industry. Data breaches are typically premeditated, though accidental data breaches also occur. Some data breaches are discovered within a matter of hours or days, while others take months or years. In a majority of the data breach incidents, the stolen data was used for criminal purposes, while in a few cases, the breaches were unintentional.

A decade of breaches

All data breach incident reports in this paper have been collected from the PRC database from January 2005 to April 2015. PRC's original "Organization Types" were expanded to include a wide range of industries in order to provide a fine-grained view of victim profiles. Each entry was analyzed to determine the record types compromised.

- **PII:** Names, addresses, Social Security numbers, dates of birth, phone numbers, etc.

- **Financial data:** Banking, insurance, and billing information, etc.

- **Health data:** Hospital and doctors' office records, medical insurance, etc.

- **Education data:** School, college, university, or related records.

- **Payment cards:** Credit, debit, store-branded credit, and prepaid gift cards.

- **Credentials:** Log-in credentials for eBay, PayPal, Web-based email, online banking, and other accounts.

- **Others:** Intellectual property and intelligence about an organization.

- **Unknown:** In many cases, investigators failed to determine what was stolen.

The data collected was analyzed using tools that include KH Coder[6], MSBNx[7], and Explore Analytics[8].

In reality, only a fraction of all data breach incidents actually get reported. An increase in the number of reported incidents strongly indicates that the total volume of data breaches has also risen and vice versa.
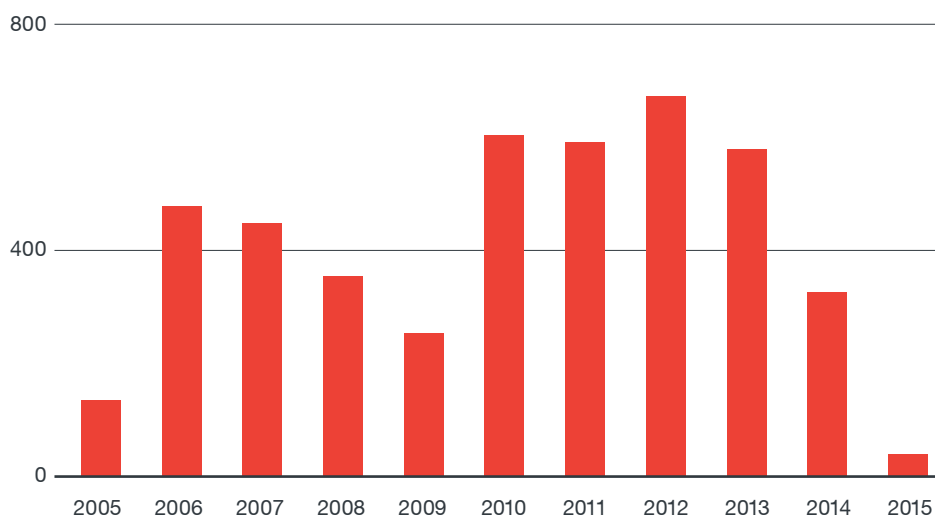
Figure 2: Data breach incident disclosures from 2005 to April 2015

Figure 2 shows that the total number of incidents reported per year has been steadily increasing since 2009, except in 2014 when a marked decline was seen. This increase can have several plausible explanations:

- Data breach notification laws were implemented by different states, compelling businesses and organizations to report incidents.

- As the Internet expands and new applications are introduced, businesses are steadily growing their online presence, leading to increased hacking or malware attacks.

- Criminals are more easily monetizing stolen data and thus committing more data breach crimes.

The decline in the number of incidents reported in 2014 could have either marked the start of a new trend wherein organizations quickly clamped down on security breaches and prevented the leakage of sensitive data or businesses and organizations just did not report breaches. This paper collected incident reports up to April 2015 only. As such, it is too early to draw conclusions about any new trend. According to Verizon's "2015 Data Breach Investigations Report[9]," the time to identify and respond to a breach incident is expected to widen, highlighting the growing "detection deficit" companies are faced with. Yet interestingly enough the defender-detection deficit graph (Figure 5 on page 6 of the Verizon report) shows that the deficit gap between the time to compromise and the time to discover has shrunk from 77% in 2013 to 45% in 2014. That was a significant decline and hopefully a new trend moving forward. It could be a sign of quick containment that reduces the number of data breach incidents. Also, businesses are implementing plans, protocols, procedures, and checks to prevent the leakage of sensitive data, which also aids in reducing breaches.
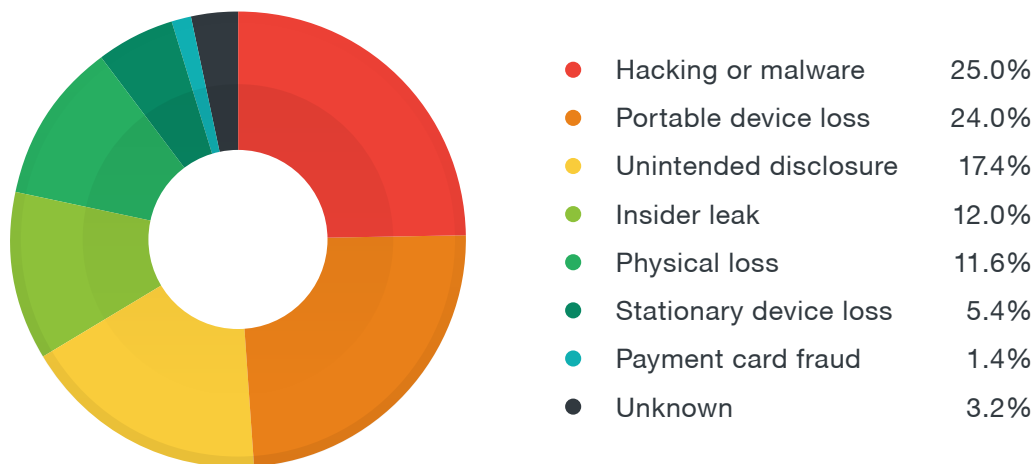
●	Hacking or malware	25.0%
●	Portable device loss	24.0%
●	Unintended disclosure	17.4%
●	Insider leak	12.0%
●	Physical loss	11.6%
●	Stationary device loss	5.4%
●	Payment card fraud	1.4%
●	Unknown	3.2%

Figure 3: Breach methods observed across industries

In the news, data breaches are almost always attributed to hacking or malware attacks. While these attacks play a big role, they only account for a quarter of all of the reported incidents. Other frequently observed breach methods include:

• **Insider leak:** A trusted individual or person of authority with access privileges steals data.

• **Payment card fraud:** Payment card data is stolen using physical skimming devices.

• **Loss or theft:** Portable drives, laptops, office computers, files, and other physical properties are lost or stolen.

• **Unintended disclosure:** Through mistakes or negligence, sensitive data is exposed.

• **Unknown:** In a small of number of cases, the actual breach method is unknown or undisclosed.

We will go into greater detail on record types and record-type combinations stolen based on our analysis of the PRC data in our supplemental material, "Follow the Data: Analyzing Breaches by Industry." The healthcare, education, government, retail, and financial industries were the most frequent data breach victims. We studied five data sets for each industry and looked at trending patterns. The following sections take a look at two frequently observed data breach crimes—payment card data breaches as well as identity theft and fraud.

Payment card data breaches exponentially increased from 2010

Stealing payment card data has become an everyday crime that yields quick monetary gains. The goal is to steal the data stored in the magnetic stripe of payment cards, optionally clone cards, and run charges on accounts associated with cards. Criminals have been physically skimming payment cards (debit and credit cards) for a while now. Common techniques for skimming payment cards include:

- Making a rub of cards
- Rigging ATMs or gas pumps with fake panels that steal data
- Modifying in-store point-of-sale (PoS) terminals
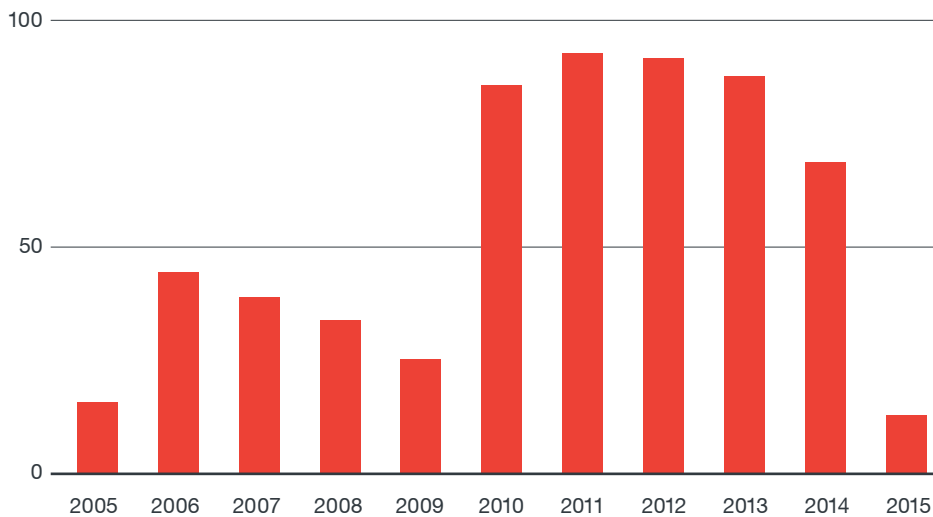- Using off-the-shelf hardware keyloggers on cash registers[10]

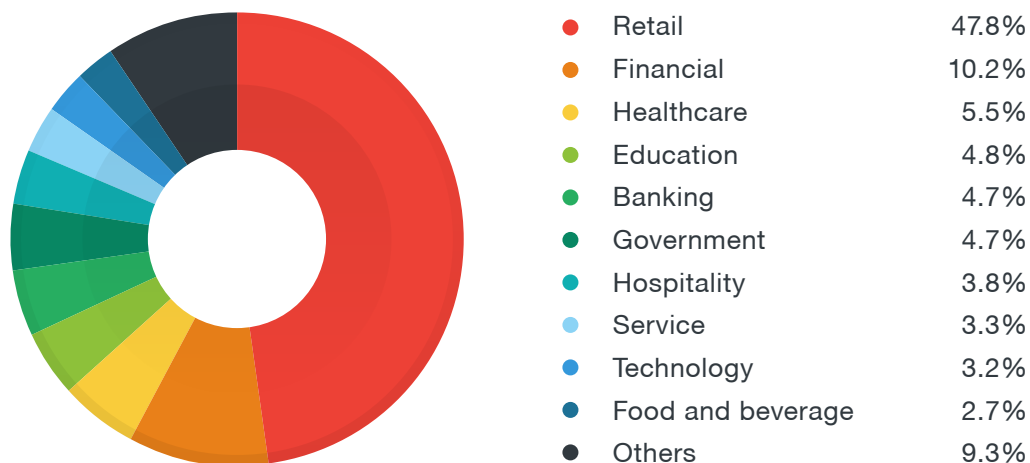*Figure 4: Payment card data breach incidents from 2005 to April 2015*

Retail	47.8%
Financial	10.2%
Healthcare	5.5%
Education	4.8%
Banking	4.7%
Government	4.7%
Hospitality	3.8%
Service	3.3%
Technology	3.2%
Food and beverage	2.7%
Others	9.3%

Figure 5: Industries affected by payment card data breaches

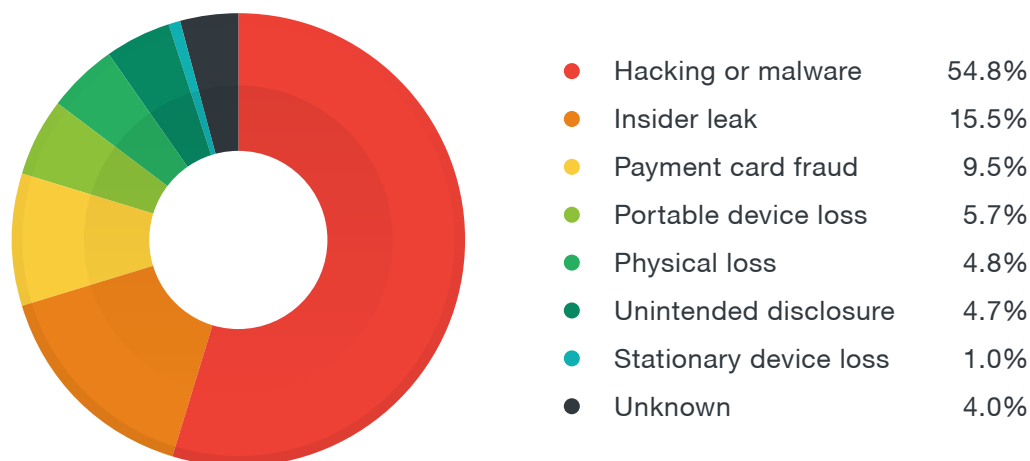| Hacking or malware | 54.8% |
Insider leak	15.5%
Payment card fraud	9.5%
Portable device loss	5.7%
Physical loss	4.8%
Unintended disclosure	4.7%
Stationary device loss	1.0%
Unknown	4.0%

Figure 6: Payment card data breach methods used

These techniques all require physical access to cards or the devices used to process them. This introduces a big risk of getting apprehended. Also, skimmers can't be readily mass-deployed for maximum effectiveness. Therefore, criminals have resorted to using malicious software like PoS RAM scrapers to steal payment card data, primarily credit card information. A variety of infiltration techniques are used to gain initial entry into and laterally move across the victim's network in order to compromise PoS servers.

Looking at the payment card data breach numbers, we see a marked increase from 2010 onward. This can be directly attributed to PoS RAM scrapers, which were developed sometime between 2007 and 2008 and gained popularity as a data theft tool at around 2010. Payment card data theft incidents before

2010 mostly involved criminals using skimming devices. Skimmers have not altogether disappeared but payment card data theft incidents nowadays are predominantly done using PoS RAM scrapers. This is reflected by the fact that hacking or malware attacks accounted for more than half of the payment card data breaches seen.

The retail industry was the biggest victim of payment card data breaches, as most credit and debit card transactions take place in stores. Other industries were also affected. In a nutshell, any business or organization that processes or stores payment card data is a potential victim.

Identity theft was most rampant in the healthcare industry

Identity theft is the preparatory stage of acquiring and collecting someone else's personal information (name, address, date of birth, Social Security number, etc.) for criminal purposes. Identity fraud is the actual deceptive use of the stolen personal information to commit fraud[11]. A criminal pretends to be someone else (living or dead) by falsely assuming and using that person's identity to gain access to resources or services, apply for credit cards or loans, register fake accounts, file fraudulent tax returns to collect rebates, and other activities without the victim's knowledge or consent. The PRC database recorded incidents when stolen data was used to commit identity theft and fraud.

●	Healthcare	29.8%
●	Retail	15.9%
●	Government	13.6%
●	Financial	11.2%
●	Education	10.9%
●	Others	4.3%
●	Banking	3.9%
●	Service	2.7%
●	Insurance	1.9%
●	Hospitality	1.6%
●	Technology	1.6%
●	Manufacturing	0.6%
●	Consumer goods	0.4%
●	Food and beverage	0.4%
●	Materials	0.4%
●	Telecommunications	0.4%
●	Transportation	0.4%

Figure 7: Identity theft and fraud victims by industry

●	Insider leak	44.2%
●	Hacking or malware	15.5%
●	Portable device loss	12.8%
●	Physical loss	9.3%
●	Unintended disclosure	6.2%
●	Payment card fraud	4.7%
●	Stationary device loss	2.3%
●	Unknown	5.0%
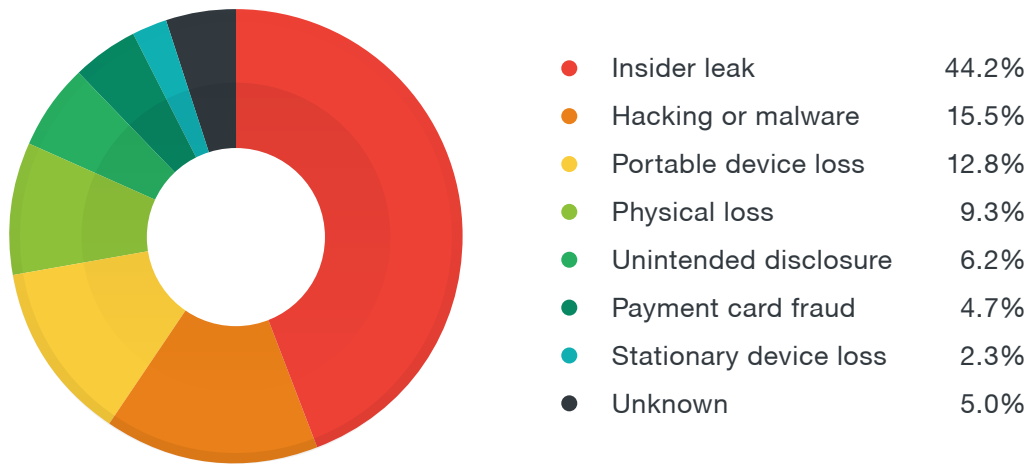
Figure 8: Data breach methods used for identity theft and fraud

●	PII	28.7%
●	Health + PII	9.7%
●	Financial + PII	9.3%
●	Payment card	8.9%
●	Financial + health + PII	6.6%
●	Financial	5.4%
●	Health	4.3%
●	Financial + payment card	3.5%
●	Financial + PII + payment card	3.1%
●	Education + PII	2.3%
●	PII + payment card	2.3%
●	Credentials + financial + PII	1.6%
●	Education + financial + PII	1.6%
●	Financial + health + PII + payment card	1.6%
●	Credentials + financial + PII + payment card	1.2%
●	Others	9.9%
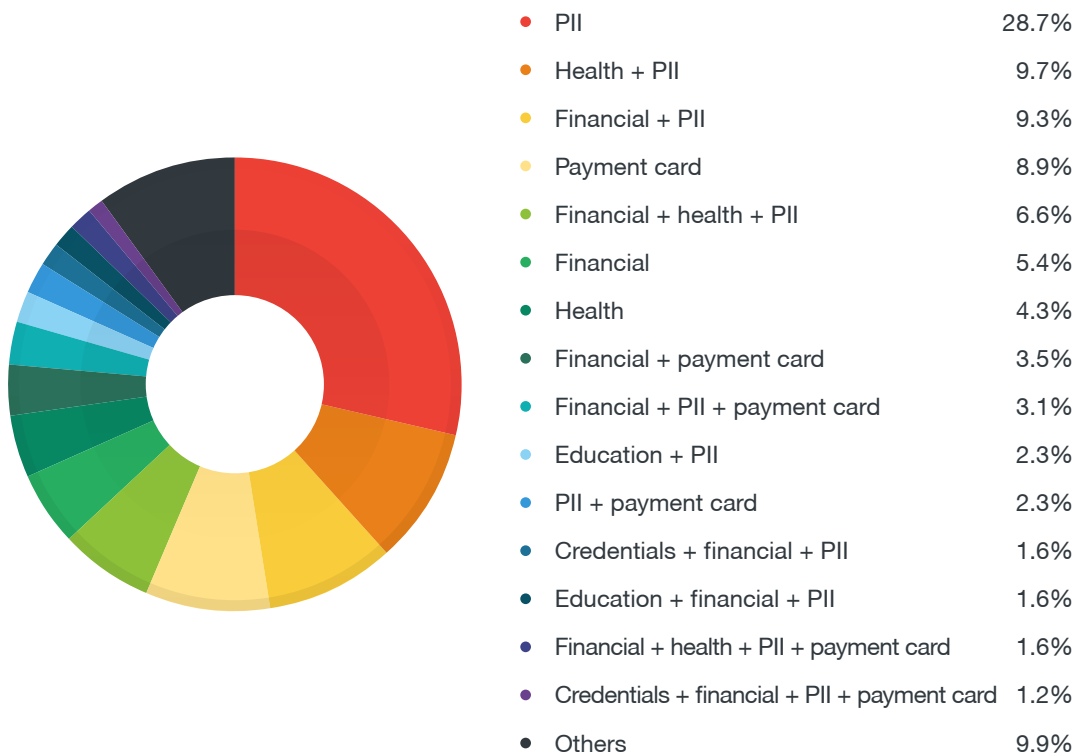
Figure 9: Record-type combinations compromised
in known identity theft and fraud cases

A majority of the known identity theft and fraud crimes affected the healthcare, retail, government, financial, and education industries. This could be because these industries process and store a wealth of PII that can be used to commit identity fraud. Insiders were the biggest perpetrators in known identity theft and fraud cases. Other big threats to PII include hacking or malware attacks and loss or theft.

Following stolen data

News outlets are quick to report on data breaches but rarely follow up on what happened to the stolen data. Tracing the movement of stolen data can be difficult because:

- It may surface after weeks or months or not at all in Deep Web marketplaces.

- When it's sold, it's not explicitly advertised as belonging to a particular breach, business, or organization. This helps criminals avoid drawing unwanted attention and scrutiny.

- Breach victims won't release information that would make the stolen data easy to identify.

- Millions of records are available for purchase in Deep Web marketplaces and stolen data may be hiding in plain sight.

- Access to the stolen data requires purchasing it and that is expensive and a potential criminal offense.

Based on our analysis of the PRC data, we modeled the relationships between different events observed in breach incidents. We created a Bayesian network* to model commonly observed data breach scenarios. To simplify, we chose not to focus on individual industries but instead created general models.

Device loss or theft is the likeliest breach method

Figure 10 shows the probability of different data breach methods being used. (Note that breach methods are mutually exclusive.) The top way by which sensitive data was compromised was through loss or theft. This included the loss or theft of portable devices (USB keys, backup drives, laptops, etc.), physical records (files, receipts, bills, etc.), and stationary devices (office computers, specialized equipment, etc.). Hacking or malware attacks comprised the next major threat, followed by unintended disclosure and insider threats. Payment card data compromised via skimming, keylogging, or similar methods posed less than a 2% risk. In slightly more than 3% of the cases, the actual breach method remained unknown.

A Bayesian, Bayes, or belief network is a probabilistic graphical model (a type of statistical model) that represents a set of random variables and their conditional dependencies.
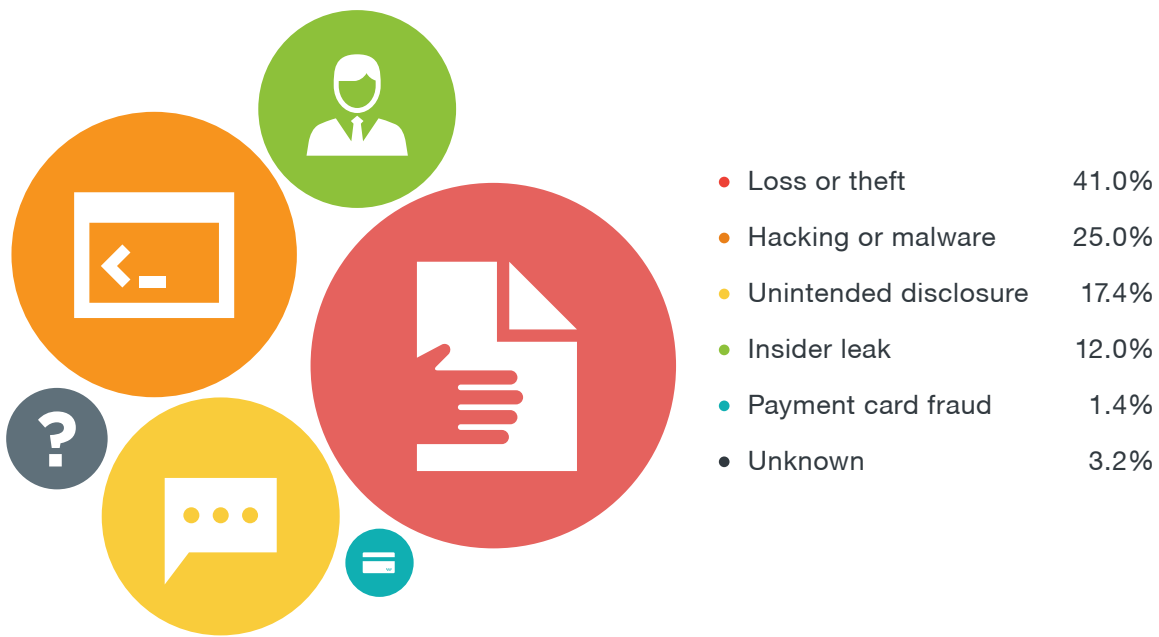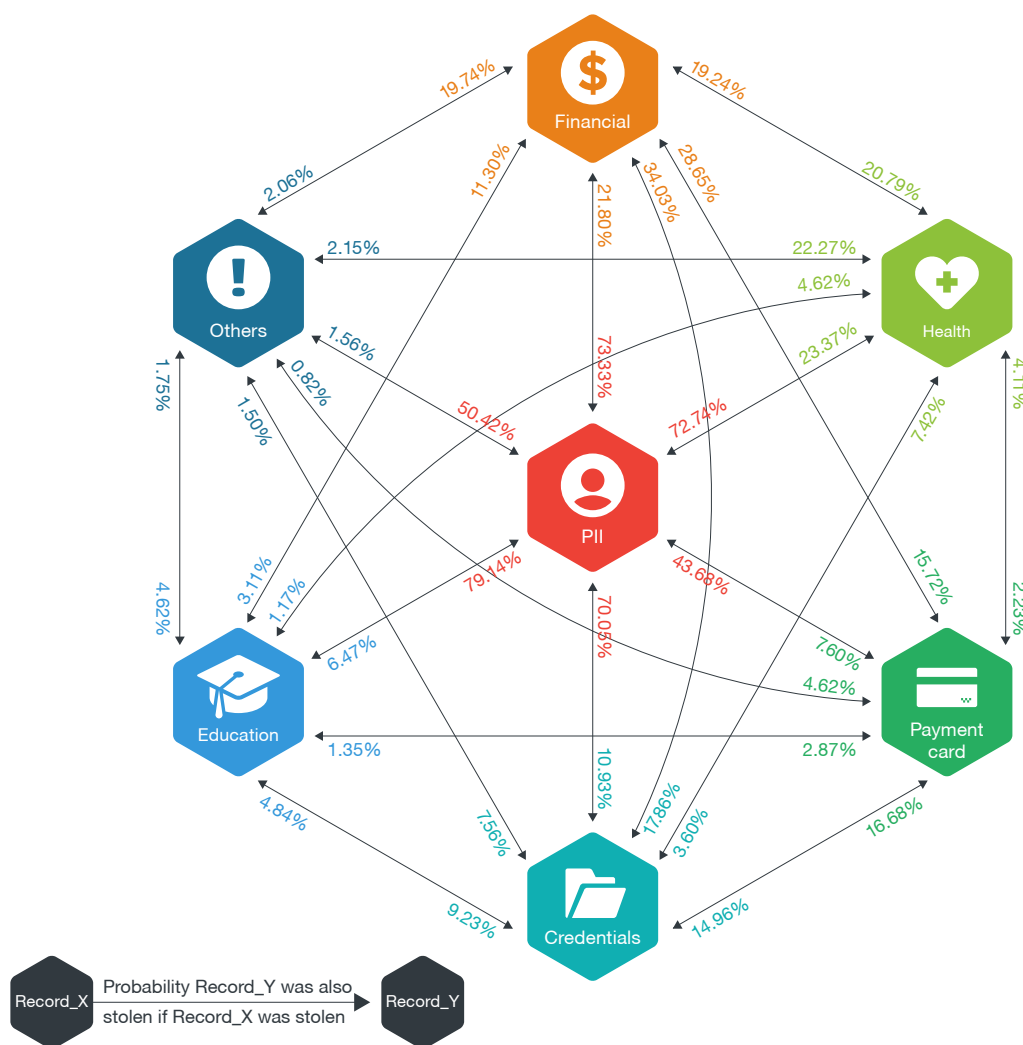
● Loss or theft	41.0%
● Hacking or malware	25.0%
● Unintended disclosure	17.4%
● Insider leak	12.0%
● Payment card fraud	1.4%
● Unknown	3.2%

Figure 10: Probability of using different breach methods

PII is the likeliest data stolen; financial data, second

Figure 11 shows the conditional probability mapping of Record_Type_Y also getting stolen if Record_Type_X is. (Note that the record types stolen are dependent events.) When investigating a data breach, if Record_Type_X is stolen, it is critical to figure out what other record types may also have been stolen. Depending on the industry the victim belongs to, the data type targeted will vary.

- PII was the most popular record type stolen. There is a 70.05% probability that PII was also stolen if credentials were stolen. There is a 73.33% probability that PII was also stolen if financial data was stolen and so on. Almost all record types contain some PII. In the event of a breach, PII will most likely be stolen.

- Financial data was the next most popular record type stolen. There is a 21.8% probability that financial data was also stolen if PII was stolen. There is a 19.24% probability that financial data was also stolen if health information was stolen and so on. Financial data is a popular target because it can be easily monetized. It also contains PII that can be monetized, indicating a double win for criminals.

- Stealing health data became popular from 2010 onward. It contains PII and may also include financial data, making it a lucrative target for criminals. There is a 72.74% chance that PII was also stolen if health data was stolen. There is a 20.79% chance that financial data was also stolen if health information was stolen.

- Education data is stolen for similar reasons as that for health information. Education data theft has, however, declined over the years. There is a 79.14% probability that PII was also stolen if education data was stolen.

- Stealing payment card data became very popular after the creation of PoS RAM scrapers. Payment card data is commonly stolen straight from the RAM of the PoS servers. This is why other record types are rarely stolen alongside payment card data. In incidents where other record types were also stolen, the payment card data was stored with them.

- Credential harvesting is typically done solo, which is why other record types are rarely stolen alongside credentials. eBay, PayPal, Webmail, online banking, and other account credentials are usually stolen.

- Criminals steal all kinds of available data. This was observed in the Sony Pictures breach in November 2014[12]. Internal emails, unreleased movies, health records, passwords, salary data, and others were all compromised and released to the public, hugely damaging Sony Pictures's reputation. More recently, the Hacking Team, the makers of surveillance software, was hacked and 415GB of stolen data was made public. This included emails, customer information, software, zero-day vulnerabilities, and so on[13]. Stealing other information besides PII, credentials, and financial, health, education, and payment card data is not as rare as the probability numbers indicate. Data breach incident disclosures focus on the riskiest data stolen versus all of the information taken. The definition of "risky data" will expand as more breach incidents where other information is stolen are disclosed.

Figure 11: Conditional probability of Record_Type_Y also getting stolen if Record_Type_X is

	Hacking or malware	Payment card fraud	Unintended disclosure	Insider leak	Loss or theft	Unknown
PII	68.89%	15.62%	86.92%	65.68%	84.18%	59.15%
Financial	22.64%	32.81%	22.05%	29.13%	20.22%	34.51%
Health	6.95%	-	20.00%	34.88%	35.87%	18.31%
Payment card	29.32%	100%	3.59%	17.25%	3.21%	16.9%
Credentials	30.39%	10.94%	9.36%	7.42%	3.21%	12.68%
Education	6.86%	-	13.2%	1.86%	4.73%	3.52%
Others	2.14%	-	2.69%	3.33%	2.28%	1.41%
Unknown	25.85%	-	-	-	1.09%	7.75%

Figure 12: Breach method to record-type probability mapping

Figure 12 shows the probability mapping of data breach methods to record types stolen. (Note that breach methods and record types are independent events.)

- Credentials and payment card and other data are rarely compromised through loss or theft.

- A majority of the data breach methods have a 60+% probability of being used to compromise PII.

- Payment card data is rarely accidentally disclosed. On the other hand, accidental or unintentional disclosure of PII is common.

- Insiders rarely go after education data and credentials. In breach incidents involving insiders, the record types stolen are identified.

- In incidents where investigators failed to discover what breach method was used, there is a high probability that financial data and/or PII were stolen.
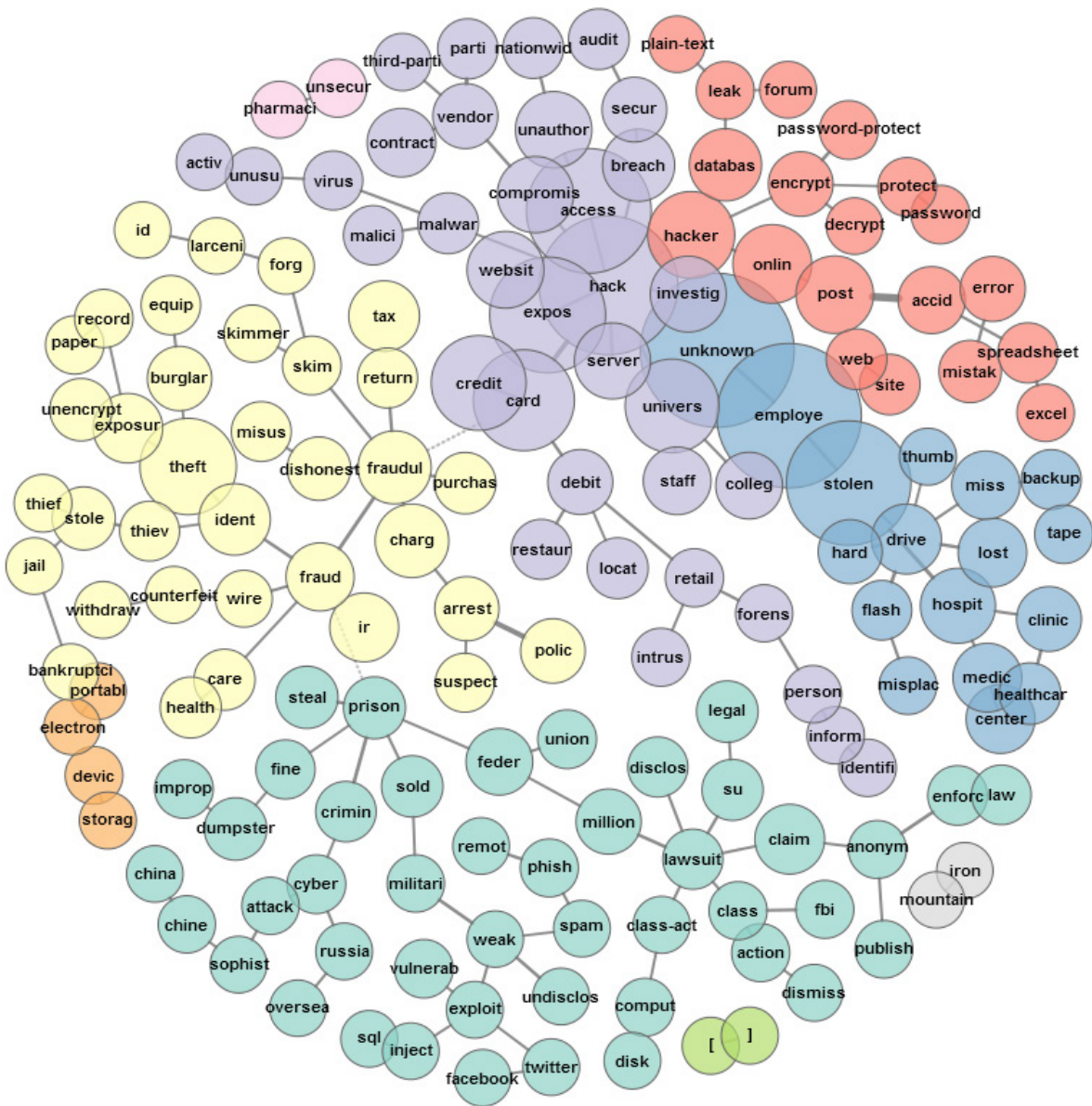
Figure 13: Co-occurrence network for extracted keywords

Each entry in the PRC database was converted into the following format:

```
Record_Index, Company_Name, Industry, Location, Breach_Date, Breach_Method, Total_
Records_Stolen, Record_Type, Information_Source, Extra_Information_Keywords
```

An example has been given below.

```
13, Piedmont Advantage Credit Union, Financial, North Carolina, 02-Mar-15, Portable
Device Loss, Unknown, ["PII"], Media, ["credit union""password protect""unknown"]
```

To create an alternate view of data breach incidents, a co-occurrence network diagram was generated for the top 1,000 extracted keywords using KH Coder⁶. In Figure 13, the sizes of the bubbles represent frequency, the colors indicate keyword-clustered communities, and a minimum spanning tree (MST) connects the nodes (with bold lines representing strong links). The co-occurrence network shows interesting keyword groupings and their connections such as:

- The blue community shows that portable device loss or theft was a frequent problem in the healthcare industry. A lot of events are currently unknown and may involve employees.

- The purple community shows bubbles associated with hacking or malware attacks connecting credit cards, servers, educational institutions, third-party vendors, websites, and so on. Credit cards were frequently linked to breaches involving retail outlets and restaurants.

- The red community connects keywords from two seemingly disparate groups—unintended disclosures and hacking or malware attacks. The connection exists because hacktivists publicly post stolen data to harm businesses or organizations while unintended disclosures are conceptually similar, except in that leaks occur because of mistakes or negligence.

- The yellow community connects the different crimes committed. Some keywords indicate that the criminals were arrested but those incidents had a lower frequency.

- The green community is a mixed bag, connecting everything from dumpster diving to lawsuits to prison sentences for criminals. Not that many meaningful correlations were derived from this clustering aside from the fact that there are incidents that connect a subset of these keywords.

Hacking or malware are the go-to breach methods

Data breaches are complex events with numerous probable scenarios. Based on our analysis of the PRC data, we created a Bayesian network (Figure 14) to model commonly observed data breach scenarios.

- Hacking or malware were used to compromise all record types. Hacking or malware attacks typically include phishing, vulnerability exploitation, gaining unauthorized access, and compromising servers and databases. Credit and debit card data was also compromised via hacking or malware attacks.

- In incidents where the breach method is unknown, PII and financial, payment card, and/or health data were likely compromised.

- Retailers and restaurants were frequent victims of payment card fraud. Skimming devices are used but PoS RAM scrapers are by far the most popular tools for collecting payment card data. Stolen payment card data is often used to make fraudulent purchases.

- Unintended disclosures exposed PII and health and education data. Unintended disclosures happen when data is accidentally posted online, leaked through negligence, or exposed because of mistakes or negligence on the part of third-party vendors and contractors who handle information.

- Insiders targeted PII and financial, payment card, health, and other data. Making fraudulent tax claims, identity theft and fraud, and selling data to outside parties are common crimes committed by insiders.

- PII and financial, health, and education data were frequently compromised through loss or theft. This includes the loss or theft of portable devices (USB keys, backup drives, laptops, etc.), physical records (files, receipts, bills, etc.), and stationary devices (office computers, specialized equipment, etc.).
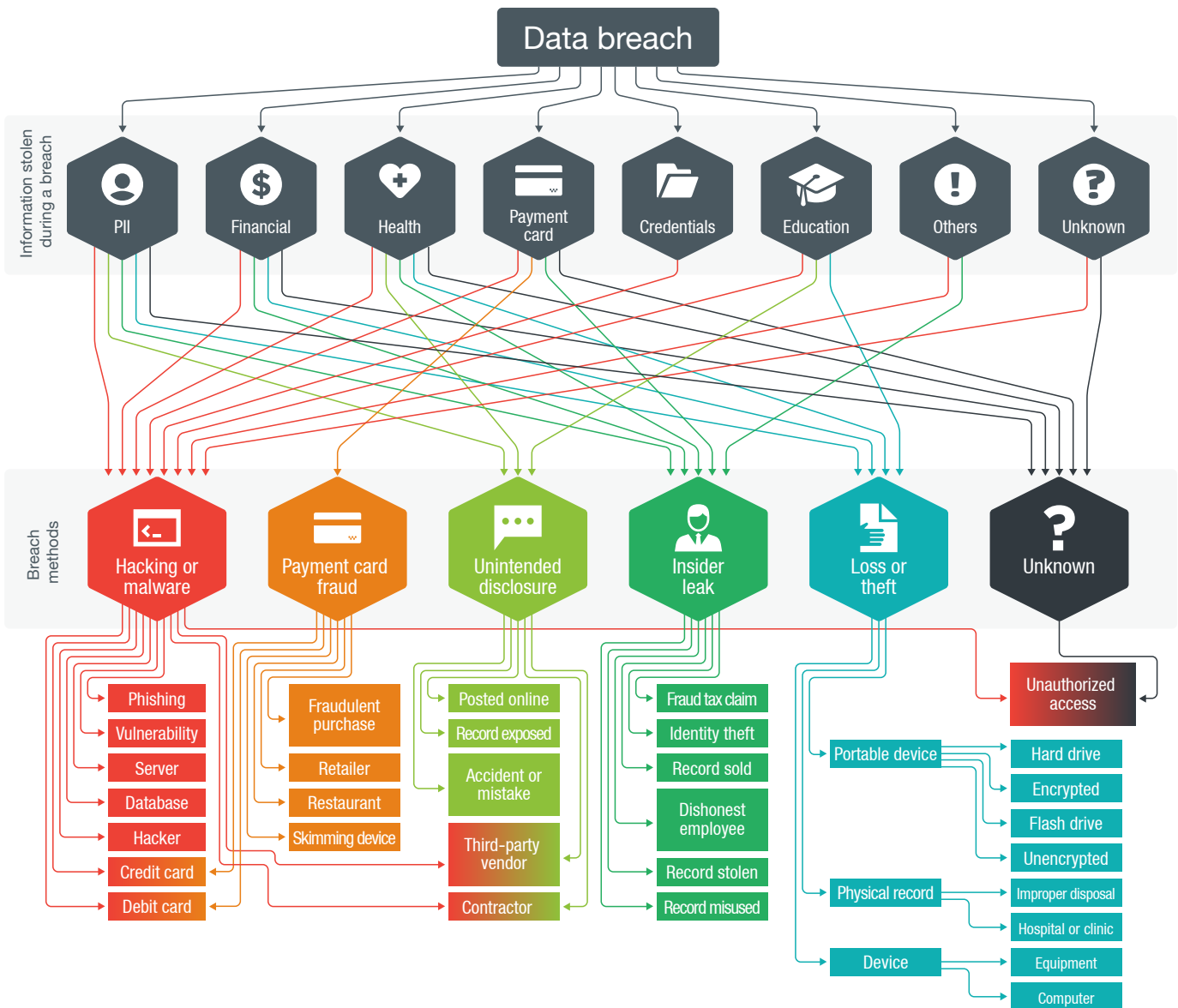

Figure 14: Bayesian network showing commonly observed data breach scenarios

Who is stealing data?

Perpetrators who compromise sensitive data make up a diverse group:

- **Insiders:** It is difficult to understand what motivates insiders. They act against organizations that they are or were part of and indirectly act against their own interests[14]. Insiders could be motivated by money, ideology, coercion, and ego. More than one of these motives are frequently in play.

- **Individual criminals:** These typically refer to one-man to two-men operations that steal and sell sensitive data in the black market. They often launch hacking or malware attacks. They purchase malware from hacking or criminal forums, use these to compromise victims' systems, steal sensitive data, and sell stolen information in Deep Web marketplaces[15, 16, 17, 18]. Hacktivists steal data as an act of vengeance against a business or organization by releasing it to the public.

- **Organized groups:** These are well-funded criminal groups who run organized rackets to steal and monetize sensitive data. Known crime syndicates usually fund and run these groups. Hacktivist groups like Anonymous steal data for ideological reasons and release stolen information to the public in order to cause businesses or organizations embarrassment and harm.

- **State-sponsored groups:** Data is frequently stolen for intelligence gathering and espionage or to gain competitive advantage. The media tends to blame nation-states for these type of attacks. The blame game is often played when governmental organizations and defense companies are hit by data breaches but in reality, attribution is very difficult to ascertain. State-sponsored attacks follow one of two operational models—a state controls the hacking team and its resources or a state outsources hacking activities to third parties, which attack the same or different targets.

What crimes are committed using stolen data?

Data breaches affect individuals and businesses (big and small) on a daily basis. A majority of data breaches aim to steal PII, financial data, and credentials. It is important to identify crimes that are committed using each kind of stolen data.

- **PII:** This can be used for committing identity fraud, filing fraudulent tax returns, applying for loans or credit cards, registering fake accounts, selling to marketing firms, and launching spam and phishing attacks.

- **Financial data:** This can be used for creating counterfeit credit cards, paying bills, making fraudulent online transactions, and transferring money out of victims' bank accounts.

- **Credentials:** These can be used for stealing intellectual property, committing espionage, and launching spam and phishing attacks.

- **Others:** There are cases where the stolen data is used in vengeance attacks and/or hacktivism. In these, victims are blackmailed or the stolen data is held for ransom.

How much is stolen data sold for?

Stolen data can be readily found for sale in Deep Web marketplaces. Transactions are completed using bitcoins, WebMoney, or escrow accounts. These payment methods offer convenience and anonymity to both buyers and sellers. In this section, we looked at the different types of sensitive data sold in marketplaces, along with their selling prices.

Mobile phone, Uber, PayPal, and poker accounts for sale

Different accounts are available for sale in Deep Web marketplaces.

- Accounts for various mobile phone operators in the US are available for up to US$14 per account.

- Compromised PayPal and eBay accounts are commonly available for purchase. Facebook, FedEx, Google Voice™, Netflix, Amazon, Uber, and other accounts are also sold.

- Compromised Uber accounts have recently become very popular in Deep Web marketplaces, as these can be fraudulently charged with phantom rides[19].

- Stolen accounts from victims in Canada, Australia, the United Kingdom (UK), and other European countries are readily available for purchase. Criminals probably prefer to distribute their fraud operations worldwide in order to improve the probability of success and reduce operational risks.

- There are no price differences between verified and unverified PayPal accounts. The available balance on each account is listed to help potential buyers make informed purchases. The seller can sell the same compromised account to multiple parties. The buyer accepts the risk that the accounts could have been flagged and locked.

- PayPal and eBay accounts, which are mature (has months or years of transaction history), are sold for up to US$300 each. Mature accounts are less likely to be flagged for suspicious transactions.

Figure 15: Mobile phone accounts for sale

Figure 16: Miscellaneous accounts for sale

Figure 17: PayPal accounts for sale

II. Sell moneymakerz stuff.

- bank logins (for sale and for cashout), other accts like poker accts, paypal, ebay, neteller, moneybookers etc etc (any stuff from uk logs)
- cvvs:
Usa - 3-6 usd per 1
CA - 8-9 usd per 1
EU, Asia - 15 usd per 1
AU, GB- 10-15 usd per 1
CC + VBV (MCSC) code UK - 100-120 usd per 1
US fullz
- SSN+DOB 6$
- sell botnets (the unique offer in the market now!)

Its not my general business, but possible:

- Full info for person(full background - Autos,Real property,Relatives etc.) - $25 - Driver Licence - 15$ - Business Report - 35$ - Credit report - $30 - Employer Info - 15$ - Motor Vehicle - 15$ - Real Property - 15$

- Dumps:
USA - 25-40 usd per 1 Canada - 40-55 usd per 1 EU and World: (101) - 100-120 usd per 1 EU and World: (201) - 70-90 usd per 1

Figure 18: Bank and poker accounts for sale

Figure 19: Credentials for sale

Figure 20: Uber accounts for sale

Figure 21: PayPal and eBay accounts for sale

UK and US bank log-in credentials for sale

Log-in credentials for banks around the world are sold at steep prices of between US$200 and US$500 per account in Deep Web marketplaces. The larger the available balance of an account, the higher its selling price. Banking malware have been and continue to be a massive problem in Brazil[20]. As such, it is not surprising to find so many compromised Brazilian bank log-in credentials available for purchase.


```
⊘ Selling cvv , fullz , track1&2, dumps , logins .......!!!!!!

SELLING CVV , FULLZ , TRACK1&2, DUMPS , LOGINS .......!!!!!!
PRICE LIST:
1 US cc= 6$
1 CA cc= 6$
1 UK cc= 12$
1 AU cc= 12$
1 EU cc= 16$

tracks1 and tracks2 (jp,it,usa,au,uk) with good balances.
dumps:100$- 10pcs
gold:120$ -12pcs
platinum:150$ -20pcs
business:200$ when buy more me reduce
Avaliable uk bank logins
Alliance & Leicester
Lloyds TSB Bank
Abbey Bank
Northern Bank
Jodrell Bank
Avaiable usa bank logins
BOA,
CHASE BANK,
WAMU
WELSFARGO
WACHOVIA
HSBC

1 US CVV full info = 30$
1 CA CVV fullz=$30$
(FR IT GER ESP BEL AU UK EU)= 50$

nation wide bank login $500 (£68,000.00GBP)
halifax bank login $500 (£30,000.00GBP)
lyods bank login $500 (£122,070.000GBP)

ACCEPT:::BTC/PM &WU/MG :::
Please contact me if you are a Serious player.
Minimun orders for :::BTC/PM::: is $60
No tests
Ripper's are not advised to Pm me PLS be informed .
I Sell good fresh CVV"s and dumps to all my clients.
I make sure the payment is received and confirmed before I deliver, and items are delivered on time
```
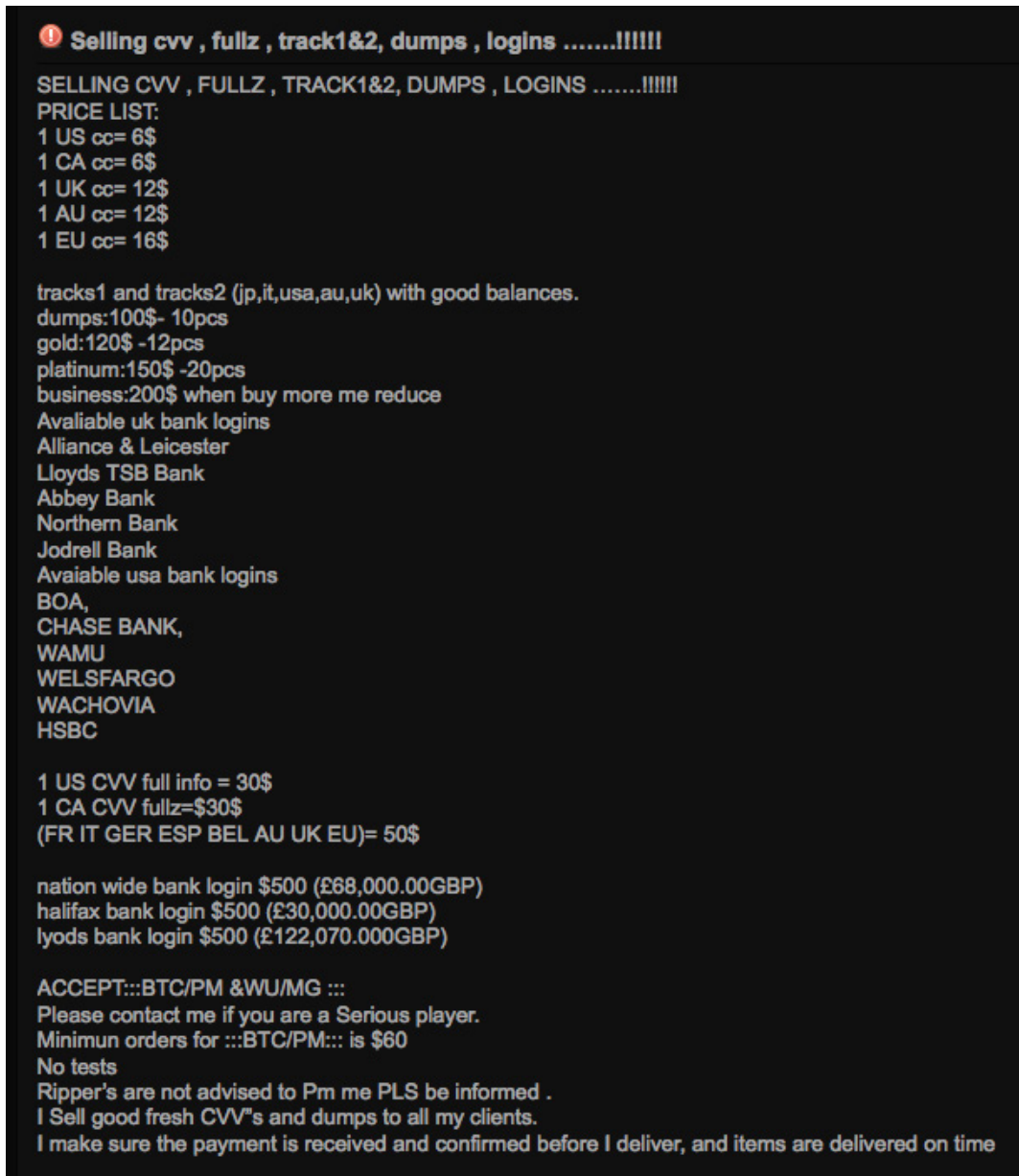
Figure 22: UK and US bank log-in credentials for sale

Buy Random BankLogin For Cheap

What Your Get : Full Owner Info DOB/SSN/Secret Answer , Email With Password and Bank Login

Country	Bank	Balance	Email	Password	Price	Cart
Australia	POLICE ASSOCIATION CREDIT CO-OPERATIVE, LTD.	4875USD	@gmail.com	Yes	200$	Buy
Brazil	BANCO SANTOS, S.A.	375USD	@gmail.com	Yes	200$	Buy
Brazil	BANCO DO ESTADO DO RIO GRANDE DO SUL S/A	3161USD	@gmail.com	No	200$	Buy
Brazil		3228USD	@gmail.com	Yes	200$	Buy
Brazil	BANCO BRADESCO CARTOES, S.A.	1105USD	@hotmail.com	Yes	200$	Buy
Canada	CANADIAN IMPERIAL BANK OF COMMERCE	4617USD	@aol.com	No	200$	Buy
Canada	TORONTO-DOMINION BANK	3456USD	@msn.com	No	200$	Buy
Canada		2730USD	@gmail.com	No	200$	Buy
Denmark	PBS INTERNATIONAL A/S	1376USD	@gmail.com	No	200$	Buy
Ecuador	Banco del Austro SA	2409USD	@aol.com	No	200$	Buy
France	CREDIT AGRICOLE, S.A.	307USD	@gmail.com	No	200$	Buy
France	CAISSE NATIONALE DE CREDIT AGRICOLE	4642USD	@gmail.com	No	200$	Buy
France	SOCIETE GENERALE, S.A.	3671USD	@hotmail.com	Yes	200$	Buy

Figure 23: Bank log-in credentials with balance information for sale

Ads list the available balance for accounts. Illegal money transfers are done to offshore accounts in order to cash out on compromised bank accounts. Ryanair in Ireland fell prey to such a fraudulent money transfer in April 2015 when €4.2 million was removed from one of its bank accounts via electronic fund transfer (EFT) through a Chinese bank[21]. This is an example of a massive-scale EFT fraud, which was quickly traced and funds related to which were frozen by the relevant authorities. The criminals buying compromised bank log-in credentials normally won't attempt something this big; instead they will remove smaller amounts over a longer period of time that they will bounce across multiple accounts in different countries to make transaction tracing difficult.

Credit card sales are now brand agnostic

Carding forums and Deep Web marketplaces sell payment card data to anyone willing to pay. Card data sells for different prices in various forums. The prices depend on supply and demand, whether cards are validated or not, and how much money the criminals can potentially steal from them before they are deactivated.

- Buying credit card data in bulk reduces unit prices. In some cases, sellers only sell card data in bulk, which could indicate they have been freshly acquired.

- Unlike a year ago, there no longer appears to be differences in prices with regard to card brand[22]. This is probably because of an oversupply of credit cards from numerous data breaches.

- Credit cards from every continent—Europe, Asia, Africa, North and South America, and Australia—are available in carding forums.

- Non-US credit cards fetch higher per-unit prices compared with US ones.

- Carding forums have search functions that allow buyers to select credit cards from different states and/or issuing banks. Using stolen cards to make purchases near the geographical locations where they were stolen is less likely to be flagged as "suspicious."

Figure 24: Credit cards for sale

Figure 25: Site to search for and purchase credit cards

Figure 26: US credit cards for sale

CC Autoshop

Welcome to the CC autoshop! This section allows you to search for credit cards or fulls in the most convenient way possible. Be careful when using checkers, as they can have side effects on the cards.

| Buy Cards | Buy Accounts | My Purchased Cards | My Purchased Accounts |

BIN: [ ] City: [ ] State: [ ] Zip: [ ] Country: [(Any) ▼]
DOB: [(Any) ▼] SSN: [(Any) ▼] Birth Year: [0000] to [9999] Price: [0.01] to [999.99] Sell...
Bank: [(Any) ▼] Type: [(Any) ▼] Credit: [(Any) ▼] Level: [(Any) ▼] [Search]
[Clear All]

Country dropdown options: Austria, Azerbaijan, Bahrain, Bangladesh, Belgium, Belize, Brazil, Brunei, Bulgaria, Cambodia, Canada, Chile, China, Colombia, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Finland

	BIN	Exp.	Seller	Name	City	State	Zip	Country		SSN	Price
☐	535928	7 / 15	BroomBroomVends	(90%Paolo ...	crocetta del montello	NA	31035	Italy		I/A	$8.00
☐	526430	5 / 17	BroomBroomVends	(90%Manuel...	Foligno	NA	06034	Italy		I/A	$8.00
☐	402360	9 / 15	BroomBroomVends	(90%GIUSTI...	Sant'antimo	NA	80029	Italy		I/A	$8.00
☐	402360	8 / 16	BroomBroomVends	(90%anna s...	napoli	NA	80132	Italy		I/A	$8.00
☐	540033	10 / 17	BroomBroomVends	(90%Federi...	Montecatini Terme	NA	51016	Italy		I/A	$8.00
☐	402360	12 / 15	BroomBroomVends	(90%Michel...	L'Aquila	NA	67100	Italy		I/A	$8.00
☐	402360	9 / 15	BroomBroomVends	(90%Ilaria...	Varedo	NA	20814	Italy		I/A	$8.00
☐	534207	4 / 16	BroomBroomVends	(90%andrea...	Sorso	NA	07037	Italy		I/A	$8.00
☐	402360	11 / 19	BroomBroomVends	(90%Simone...	Ospitaletto	NA	25035	Italy		I/A	$8.00
☐	534207	4 / 17	BroomBroomVends	(90%Teodor...	Brindisi	NA	72100	Italy	N/A	N/A	$8.00
☐	402360	12 / 15	BroomBroomVends	(90%Mattea...	Ficarazzi	NA	90010	Italy	N/A	N/A	$8.00
☐	459819	11 / 16	BroomBroomVends	(90%Veroni...	Ostiglia	NA	46035	Italy	N/A	N/A	$8.00
☐	526736	4 / 17	BroomBroomVends	(90%Marghe...	Chieti	NA	66100	Italy	N/A	N/A	$8.00
☐	534207	9 / 17	BroomBroomVends	(90%Federi...	Monza	NA	20900	Italy	N/A	N/A	$8.00
☐	526736	3 / 17	BroomBroomVends	(90%Maria ...	Modena	NA	41126	Italy	N/A	N/A	$8.00
☐	534207	6 / 16	BroomBroomVends	(90%Vaness...	Camponogara	NA	30010	Italy	N/A	N/A	$8.00
☐	533883	9 / 15	BroomBroomVends	(90%France...	Grumo Appula	NA	70025	Italy	N/A	N/A	$8.00
☐	402360	7 / 18	BroomBroomVends	(90%Cristi...	Pagnacco	NA	33010	Italy	N/A	N/A	$8.00
☐	459819	10 / 16	BroomBroomVends	(90%Elisa ...	Certaldo	NA	50052	Italy	N/A	N/A	$8.00
☐	402360	8 / 16	BroomBroomVends	(90%Antone...	Palermo	NA	90146	Italy	N/A	N/A	$8.00
☐	459819	1 / 17	BroomBroomVends	(90%Landi ...	Siena	NA	53100	Italy	N/A	N/A	$8.00
☐	432918	3 / 18	BroomBroomVends	(90%BHUSHA...	GRAZZANISE	NA	81046	Italy	N/A	N/A	$8.00
☐	402360	2 / 19	BroomBroomVends	(90%FRANCE...	TORINO	NA	10153	Italy	N/A	N/A	$8.00
☐	486470	6 / 17	BroomBroomVends	(90%MARINO...	firenze	NA	50058	Italy	N/A	N/A	$8.00
☐	402360	6 / 18	BroomBroomVends	(90%ENZO D...	PORTOFERRAIO	NA	57037	Italy	N/A	N/A	$8.00
☐	402360	3 / 19	BroomBroomVends	(90%giovan...	napoli	NA	80128	Italy	N/A	N/A	$8.00
☐	526724	1 / 17	BroomBroomVends	(90%ANTONI...	marano di napoli	NA	80016	Italy	N/A	N/A	$8.00
☐	402360	11 / 19	BroomBroomVends	(90%robert...	massa	NA	54100	Italy	N/A	N/A	$8.00
☐	539832	12 / 15	BroomBroomVends	(90%Stefan...	Monza	NA	20900	Italy	N/A	N/A	$8.00
☐	526430	10 / 17	BroomBroomVends	(90%Cristi...	Carlentini	NA	96013	Italy	N/A	N/A	$8.00

[Purchase Selected]   ⏮ ◀ 1 2 3 4 5 6 7 ▶ ⏭

Figure 27: International credit cards for sale

Search Dumps

Card Brand	○ ☑ Visa ○ Visa ○ Master ○ Discover ○ AmEx
Bin	[ ]
Country	[All ▼]
	[Search] [Reset Form]
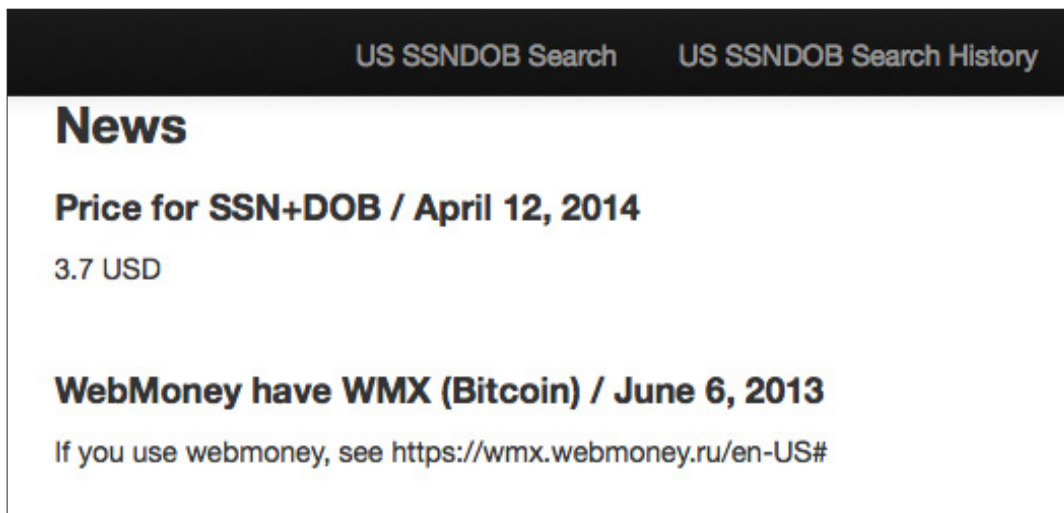
Bin	TYPE	Expires	Country	Issuer	Mark	SCode	Track	Price	Cart
443409	Visa	8/2018	Australia	CUSCAL, LTD.	CLASSIC	101	T1 +T2	65$	[Buy]
448387	Visa	2/2018	Austria	CITICORP	PREPAID	101	T1 +T2	65$	[Buy]
526763	Master Card	10/2020	Canada		STANDARD	101	T1 +T2	65$	[Buy]
373399	AmEx	6/2022	Canada	AMERICAN EXPRESS	BLUE AIRMILES CASH BACK CARD	101	T1 +T2	65$	[Buy]
520152	Master Card	1/2020	Comoros	CHINA GUANGFA BANK CO., LTD.	GOLD	101	T1 +T2	65$	[Buy]
547533	Master Card	6/2022	Czech Republic	KOMERCNI BANKA, A.S.	BUSINESS	101	T1 +T2	65$	[Buy]
402801	Visa	11/2015	Finland	LUOTTOKUNTA	CLASSIC	101	T1 +T2	65$	[Buy]
492069	Visa	5/2022	Finland	BANK OF AALAND LTD. (AALANDSBANKEN AB)	CLASSIC	101	T1 +T2	65$	[Buy]

Figure 28: International credit card dumps for sale

PII prices fall due to oversupply

PII is another hot commodity available for purchase in Deep Web marketplaces at comparatively reasonable prices.

- PII is commonly sold on a per-line basis at US$1 per line. Each line contains a name, a full address, a date of birth, a Social Security number, and other information. Criminals need to purchase only a few lines to commit identity fraud.

- The average price of PII has fallen from around US$4 in 2014 to US$1 this year. This is probably due to an oversupply of PII from numerous data breaches.

- Full credit reports of people with very high FICO[23] scores are available for purchase at US$25 per report.

- Full scans of documents like passports, drivers' licenses, utility bills, and others are available for purchase from US$10 to US$35 per scanned document. These are used to create counterfeits and steal PII.

Figure 29: Social Security numbers and dates of birth for sale

Figure 30: Ad selling PII

Figure 31: US-based PII for sale

ID	Name	State	City	ZIP	Date of Birth	Cost	Action
4553	██████	NC	WILSON	27896	1973	$1	🛒
4556	██████	NC	TARBORO	27886	1982	$1	🛒
4584	██████	MD	SILVER SPRING	20906	1979	$1	🛒
4597	██████	TN	REAGAN	38368	1983	$1	🛒
4612	██████	TX	LUFKIN	75904	1978	$1	🛒
4628	██████	TX	SAN ANTONIO	78266	1977	$1	🛒
4630	██████	FL	JACKSONVILLE	32211	1978	$1	🛒
4638	██████	TX	HIGHLANDS	77562	1974	$1	🛒
4640	██████	IA	MASON CITY	50401	1973	$1	🛒
4651	██████	SC	BAMBERG	29003	1981	$1	🛒
4652	██████	SC	MOUNT PLEASANT	29466	1948	$1	🛒
4659	██████	FL	ORLANDO	32805	1970	$1	🛒
4669	██████	TN	ANTIOCH	37013	1939	$1	🛒
4682	██████	MD	TIMONIUM	21093	1983	$1	🛒
4709	██████	TN	WHITE HOUSE	37188	1977	$1	🛒
4714	██████	GA	LITHIA SPRINGS	30122	1982	$1	🛒

Figure 32: Social Security numbers for sale with owners'
full names, locations, and dates of birth

SSN WITH CREDIT REPORT

SCORE	GENDER	ZIP	STATE	CITY	DESCRIPTION	PRICE	
770	Female	46748	IN	Huntertown		$25	Buy
771	Female	46825	IN	Fort Wayne		$25	Buy
777	Female	46835	IN	Fort Wayne		$25	Buy

Figure 33: Credit reports for sale

Figure 34: Scanned documents for sale

The perceived and actual monetary values

In this day and age when privacy, security, and the lack of both are considered major issues, the question, "How much is your personal data worth?," is becoming more and more relevant. Trend Micro asked a thousand customers from the US, Europe, and Japan this question and found that[2]:

- Passwords comprise the most-valued personal data type at US$75.80.

- Health information and medical records came second, valued at an average of US$59.80. US respondents put the highest value on their health records at US$82.90 while European consumers considered theirs to be worth US$35.

- Social Security numbers came in third at US$55.70.

- Payment details ranked fourth at US$36.60. US citizens priced this information at US$45.10 while the Japanese valued it at US$42.20. Europeans priced it at US$20.70.

- Purchase history ranked fifth, valued at US$20.60. US respondents again valued it most compared with the Japanese and Europeans.

- Physical location information ranked sixth, valued at US$16.10. US citizens priced it at US$38.40 while those from Japan and Europe priced it a paltry US$4.80 and US$5.10, respectively.

- Home address ranked seventh, valued at US$12.90. US consumers once more priced it at US$17.90. Japanese respondents pegged this information at US16.30 while those from Europe priced it at US$5.00.

- Personal photos and videos ranked eighth, valued at US$12.20. US respondents priced them at US$26.20 while those from Japan and Europe only priced them at US$4.70.

- Marital status information was pegged at an average of US$8.30. Japanese consumers priced it at US$12.70 while those from the US and Europe pegged this information at US$6.10 and US$6.00, respectively.

- Name and gender information were least valued at US$2.90.

One conclusion that we can draw from the survey is that US respondents valued nearly all of their personal information more than their counterparts from other countries. Besides cultural differences, this could also be due to how much US consumers value their privacy and how their day-to-day lives revolve around their own personal information amid the social media boom. Another thing that stood out was how everyone considers passwords their most valuable information. This is a strong indicator of how connected people have become in the age of the Internet.

While the perceived value of stolen data differs from its actual selling price, the final dollar value of damage inflicted to a business, an organization, or an individual by the criminal exploitation is significantly higher than both the perceived value and selling price.

Where do "other" stolen data go?

Until now, discussions largely focused on stolen data sold in Deep Web marketplaces and exploited to commit crimes. But what about other stolen data? As previously mentioned, a vast majority of breaches remain unreported and undisclosed[3, 4, 5]. There are many reasons why businesses or organizations do not report data breaches. One of the top reasons is that breached organizations are not legally mandated to disclose what data was compromised if this doesn't belong to customers. An example of this would be intellectual property. This leaves a gaping hole in our understanding of data breaches and we can only speculate about what happened using bits and pieces of available information.

In June 2011, several US defense contractors became security breach victims. Their RSA SecurID tokens were exploited via cloning[24]. No information was ever released about what type of data was compromised in this attack. In November 2014, the National Oceanic and Atmospheric Administration (NOAA)'s weather network suffered a security breach[25]. The satellite data stolen is vital to disaster planning, aviation, shipping, and other crucial uses. Details about exactly what data was compromised, how the breach happened, and the supposed intentions were not disclosed.

This June, a small Canadian gold mine called "Detour Gold" suffered a security breach where over 100GB of data was stolen[26, 27]. Out of the 100GB worth of data stolen, 18GB was publicly released and contained PII; financial and health data; emails; and others. The release intended to embarrass and cause harm to the mining company. But the real harm would have been caused by the theft of other information that was not released. It is speculated that the other stolen data includes geological exploration information of potential gold-mining sites. The company would have spent millions of research and development (R&D) dollars to generate this vital exploration data.

Theft of other data types strongly indicates espionage, intelligence collection, and gaining a huge advantage over a business competitor. These breaches are orchestrated by groups who have a vested interest in procuring data for their advantage. Victimized businesses or organizations rarely disclose the actual damage inflicted, as that entails disclosing details about the breach and what data was stolen but that could easily amount to millions or billions of dollars.

Defending against data breaches

In a nutshell, any business or organization that processes and/or stores sensitive data is a potential breach target. In today's interconnected world, data breach prevention strategies should be considered an integral part of daily business operations. Ultimately, no defense is impregnable against determined adversaries. The key principle of defense is to assume compromise and take countermeasures:

- Quickly identify and respond to ongoing security breaches.

- Contain the breach and stop the loss of sensitive data.

- Preemptively prevent breaches by securing all exploitable avenues.

- Apply lessons learned to further strengthen defenses and prevent repeat incidents.

Data breaches are inevitable. Having effective alert, containment, and mitigation processes is critical. In this section, we will present recommendations to defend against data breaches. Defensive strategies for some of the breach methods discussed in this paper are outside the scope of this research and have thus been omitted.

Employ as many critical security controls as possible for effective cyberdefense

The "Critical Security Controls" is a publication of best practices for computer security. A consortium of private companies worldwide jointly developed these guidelines[28, 29]. It is a "living" document that goes through periodic updates to address new risks posed by an evolving threat landscape. It is maintained by the Center for Internet Security (CIS), an independent global nonprofit entity. Its latest published version is v5.1. An upcoming version, v6, is currently available for public comment[30]. A summary of the security controls is shown in the following table[31, 32].

Critical Security Control	Description
1. Inventory of Authorized and Unauthorized Devices	Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
2. Inventory of Authorized and Unauthorized Software	Actively manage (inventory, track, and correct) all software on the networks so that only authorized software is installed and can executed, and that unauthorized and unmanaged software is found and prevented from installation or execution.
3. Secure Configurations for Hardware and Software	Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
4. Continuous Vulnerability Assessment and Remediation	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and maximize the window of opportunity for attackers.
5. Malware Defenses	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.
6. Application Software Security	Manage the security life cycle of all in-house-developed and -acquired software in order to prevent, detect, and correct security weaknesses.
7. Wireless Access Control	The processes and tools used to track/control/prevent/correct the security use of wireless LANs, access points, and wireless client systems.
8. Data Recovery Capability	The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.
9. Security Skills Assessment and Appropriate Training to Fill Gaps	For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

10.	Secure Configurations for Network Devices	Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
11.	Limitation and Control of Network Ports	Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.
12.	Controlled Use of Administrative Privileges	The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
13.	Boundary Defense	Detect/Prevent/Correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.
14.	Maintenance, Monitoring, and Analysis of Audit Logs	Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.
15.	Controlled Access Based on the Need to Know	The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the format determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.
16.	Account Monitoring and Control	Actively manage the life cycle of system and application accounts—their creation, use, dormancy, and deletion—in order to minimize opportunities for attackers to leverage them.
17.	Data Protection	The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.
18.	Incident Response and Management	Protect the organization's information as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.
19.	Secure Network Engineering	Make security an inherent attribute of the enterprise by specifying, designing, and building in features that allow high-confidence systems operations while denying or minimizing opportunities for attackers.
20.	Penetration Tests and Red Team Exercises	Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

Implementing all 20 security controls can be very expensive and requires dedicated teams for daily operations, monitoring, response, and maintenance. A large business or organization should have the resources to implement all of them but most small businesses can only afford to implement a subset of the controls. The "Critical Security Controls" provides a comprehensive set of guidelines and implementing even a subset of them will go a long way in preventing data breaches.

Security software vendors offer bundled packages to small businesses that include anti-malware, anti-phishing, and Web-filtering solutions. These are easy to set up, require minimal administration, and provide excellent security out of the box. Some vendors also include device control, data loss prevention (DLP), patch management, and application control solutions in their small-business bundles. Windows® comes with a built-in easy-to-configure software firewall. Most wireless routers come with built-in hardware firewalls. All of these technologies work to protect a business from data breaches.

Another key technology all businesses or organizations should consider implementing is disk and device encryption. We have observed that the loss or theft of portable devices (USB keys, backup drives, laptops, etc.) poses a major data compromise risk. Disk and device encryption will make the data on the stolen devices useless to all but the most resourceful criminals.

Detect insider attacks, much like external attacks

Insiders are trusted individuals or persons of authority with access privileges who steal data. They can be motivated by money, ideologies, coercion, and their egos. More than one of these motives are frequently put into play. Dealing with insider threats is a difficult task. Broadly speaking, prevention and mitigation techniques can be grouped into two categories—technical and nontechnical[33].

Technical steps to prevent insider attacks use security best practices. Insider attacks should be accorded the same level of prioritization as external attacks. Like external attacks, insider attacks can't be prevented and so they need to be detected as quickly as possible. Monitoring and logging activities like what data is moving within a network can be used to detect potentially suspicious behaviors. The key principle of defense is to assume compromise. This also includes identifying compromised insiders. Proper access controls should be put in place to ensure that employees can't access information that they do not need for their day-to-day functions. The credentials of employees who leave organizations should be immediately disabled to prevent security leaks.

Nontechnical means of security are equally effective in preventing insider threats. Employee discontent increases the risks that insider attacks pose. Good management practices in handling delicate situations, recognizing and rewarding employees, and looking after employee well-being all help diffuse potential insider threats. In a nutshell, happy employees are less likely to turn against their employers.

Data breach legislation in the US

As the average cost of a data breach increases to a high of US$201 per record[34], it is an economic necessity to have a strong legal framework in place to protect data breach victims and affected individuals. US-based companies are frequent victims of data breaches yet there are no federal standards in place that provide a uniform set of rules governing notification procedures[35]. Instead, 47 US states, the District of Columbia, Guam, Puerto Rico, and the US Virgin Islands each enacted their own legislations, requiring private or government entities to send out notifications of security breaches[36].

California enacted the first data breach notification law in 2002, on which other states modeled their own. This explains why there are so many reported data breach incidents in California. In general, notification laws require companies to let impacted individuals know in a timely manner about the compromise of their sensitive data as soon as a breach is discovered. Some states also require that the State Attorney General or a consumer-reporting agency be notified. Variations in notification laws exist across states. Some states require consumer notification whenever a breach occurs while others require notification only when there is a risk of the misuse of compromised data. Some states allow a notification delay period, pending an investigation, while others require that notifications be sent within a defined period of time. A company that fails to comply with notification laws may be subjected to civil penalties enforced by the Attorney General's Office.

Some state-level data breach notification laws are a decade old and lawmakers are in the process of tightening and expanding them[38]. Most of these are reactive but some also have proactive requirements (requires record encryption, response plans for data breaches, periodic drills to test response plans, etc.). The main problem with each state having its own data breach notification law is that requirements vary from state to state and could at times be conflicting. Companies that operate in multiple states or nationwide have to comply with multiple data breach notification laws, which adds complexity on top of dealing with an incident. Having a federal standard can simplify this process.

It is incorrect to claim that federal data breach notification laws don't exist. Specialized laws exist but a universal data breach notification standard is still missing. Depending on the type of organization and data involved, specialized federal laws may apply[36]:

- The "Health Insurance Portability and Accountability Act (HIPAA)" imposes requirements on the healthcare industry to notify impacted patients if their health records have been compromised.

- The "Gramm-Leach-Bliley Act" requires financial institutions to notify customers about a data breach.

- Securities and Exchange Commission (SEC) regulations and the "Sarbanes-Oxley Act" impose certain obligations on publicly traded companies in the event of a data breach.

The White House recently proposed "The Personal Data Notifications and Protection Act" as part of the Obama Administration's efforts to shore up the US's cybersecurity[37, 38]. This proposed act defines the following as sensitive data:

"(1) An individual's first and last name or first initial and last name in combination with any two of the following data elements:

(A) Home address or telephone number;

(B) Mother's maiden name;

(C) Month, day, and year of birth;

(2) A nontruncated Social Security number, driver's license number, passport number, or alien registration number or other government-issued unique identification number;

(3) Unique biometric data such as a fingerprint, voiceprint, a retina or iris image, or any other unique physical representation;

(4) A unique account identifier, including a financial accounting number or credit or debit card number, electronic identification number, username, or routing code;

(5) A username or electronic mail address, in combination with a password or security question and answer that would permit access to an online account; or

(6) Any combination of the following data elements:

(A) An individual's first and last name or first initial and last name;

(B) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, username, or routing code; or

(C) Any security code, access code, or password, or source code that could be used to generate such codes or passwords.

The proposed act also defines the terms of notification and the penalties businesses or organizations will face if they fail to notify a data breach has occurred."

In the past two years, five different data breach notification bills were introduced to the US Senate but none of them received enough support for passage[39]. A multitude of reasons could be behind these failures, including lobbying groups, complex technology assessment, unclear definitions of sensitive data and data breaches, and privacy concerns.

The proposed "Personal Data Notifications and Protection Act" aims to address the theft of sensitive data that can harm individuals but not theft of intellectual property, which can affect business operations, company valuation, and possibly national security. Should intellectual property theft incidents also require disclosure in the public's interest? Does the proposed act nullify any stronger state-level data breach notification laws? Does it add yet another level of complexity to the process? At the end of the day, businesses do not need legislations to implement effective breach prevention strategies to safeguard against sensitive data leakage. Data breach prevention strategies should be considered an integral part of daily business operations.

Data breaches are here to stay

Data breaches have become part of daily news. As of this writing, several prominent data breach incidents have been publicly disclosed. They attracted a lot of media attention and prompted everyone to ask, "How secure is our data?" The incidents that recently made headlines include:

- Hacktivist group, Anonymous, hacked into US Census Bureau computers and leaked employee data[40].

- Hacking Team—the creators of surveillance software—was hacked and 400+GB worth of data was leaked[15].

- 21.5 million Americans had their Social Security numbers and other sensitive data stolen in the "second" breach of the OPM's background check database[41].

- Hackers stole detailed information on 104,000 taxpayers from the Internal Revenue Service (IRS) website by exploiting an online tool[42].

- Hackers broke into the massive University of California, Los Angeles (UCLA) hospital network to access computers that stored the sensitive records of 4.5 million people[43].

- Ashley Madison—an online dating service that exclusively caters to extramarital affairs—was hacked, resulting in the theft of 37 million site members' records[44].

- Walmart Canada, CVS, Costco, and Sam's Club's online photo service sites were compromised via a third-party vendor[45, 46].

The number of data breach disclosures involving big retailers is increasing, which can only mean that smaller businesses or organizations are also being relentlessly targeted even if they are not making headlines. Nonetheless, the damage done to everyday individuals, irrespective of whether their sensitive data was stolen from a large corporation or a small corner store, is still the same—they face serious risks of identity, financial, and other types of fraud.

In reality, any business or organization that processes and/or stores sensitive data is a potential breach target. As long as sensitive data can be monetized through fraud and other crimes, data breaches are going to happen and with increasing frequency in the future. From a business or an organization's point of view, data breaches are inevitable. No defense is impregnable against determined adversaries. Having effective alert, containment, and mitigation processes is critical. In the US, federal standards need to be put in place to provide a uniform set of rules governing data breach notification procedures.

Mobile computing platforms like phones, tablets, wearables, and other devices as well as the apps that run on them are fast becoming primary computing platforms worldwide. App development is constantly being made simpler. Buying, selling, and marketing apps have been made easier via established online marketplaces. Apps support revenue models that are profitable for developers. The entire ecosystem has been designed to remove market entry barriers and encourage the development of new and innovative apps. All these contribute to the explosion of apps catering to every activity imaginable. Everyday users aren't aware that sensitive data is collected, processed, stored, and transmitted via apps and not necessarily in a secure manner. In the next couple of years, apps and mobile computing devices are bound to become major data breach targets.

It is crucial to build public awareness of the risks and repercussions of sensitive data getting compromised. Heightened awareness will lead to increased caution and the pressure will mount on federal governments and businesses or organizations to come up with effective and permanent solutions.

References

1. Privacy Rights Clearinghouse. (2015). *About the Privacy Rights Clearinghouse.* Last accessed on 3 July 2015, https://www.privacyrights.org/content/about-privacy-rights-clearinghouse.

2. Marianne Kolbasuk McGee. (5 May 2014). *Healthcare Info Security.* "Why Health Data Breaches Go Unreported." Last accessed on 19 June 2015, http://www.healthcareinfosecurity.com/health-data-breaches-go-unreported-a-6804.

3. Adam Greenberg. (8 November 2013). *SC Magazine.* "More Than Half of Corporate Breaches Go Unreported, According to Study." Last accessed on 19 June 2015, http://www.scmagazine.com/more-than-half-of-corporate-breaches-go-unreported-according-to-study/article/320252/.

4. Thomas Claburn. (31 July 2008). *Dark Reading.* "Most Security Breaches Go Unreported." Last accessed on 19 June 2015, http://www.darkreading.com/attacks-and-breaches/most-security-breaches-go-unreported/d/d-id/1070576.

5. ISO/IEC. (2015). "International Standard ISO/IEC 27040." Last accessed on 28 August 2015, https://infostore.saiglobal.com/store/downloadFile.aspx?path=Previews%%205ciso%%205cupdates2015%%205cwk2%%205cISO-IEC_27040-2015.PDF.

6. KH Coder [Computer Software]. (2015). Retrieved from http://khc.sourceforge.net/en/.

7. Microsoft Bayesian Network Editor [Computer Software]. (2010). Retrieved from http://research.microsoft.com/en-us/um/redmond/groups/adapt/msbnx/.

8. Explore Analytics [Online Software]. (2015). Retrieved from https://www.exploreanalytics.com/.

9. Verizon. (2015). "2015 Data Breach Investigations Report." Last accessed on 4 July 2015, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf.

10. Brian Krebs. (October 10, 2013). *Krebs on Security.* "Nordstrom Finds Cash Register Skimmers." Last accessed on 9 July 2015, http://krebsonsecurity.com/2013/10/nordstrom-finds-cash-register-skimmers/.

11. Royal Canadian Mounted Police. (2013). "Identity Theft and Identity Fraud." Last accessed on 9 July 2015, http://www.rcmp-grc.gc.ca/scams-fraudes/id-theft-vol-eng.htm.

12. Mark Seal. (February 2015). *Vanity Fair.* "An Exclusive Look at Sony's Hacking Saga." Last accessed on 14 July 2015, http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg.

13. Thomas Fox-Brewster. (6 July 2015). *Forbes.* "Hacking Team Breach Exposes Insecurities of a Controversial Surveillance Dealer." Last accessed on 14 July 2015, http://www.forbes.com/sites/thomasbrewster/2015/07/06/hacking-team-hacked/.

14. Jim Gogolinski. (9 December 2015). *TrendLabs Security Intelligence Blog*. "Insider Threats 101: The Threat Within." Last accessed on 20 July 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/insider-threats-101-the-threat-within/.

15. Trend Micro. (30 June 2015). *TrendLabs Security Intelligence Blog*. "Lordfenix: 20-Year-Old Brazilian Makes Profit Off Banking Malware." Last accessed on 20 July 2015. http://blog.trendmicro.com/trendlabs-security-intelligence/lordfenix-20-year-old-brazilian-makes-profit-off-banking-malware/.

16. Trend Micro. (13 April 2015). *TrendLabs Security Intelligence Blog.* "One-Man PoS Malware Operation Captures 22,000 Credit Card Details in Brazil." Last accessed on 20 July 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/fighterpos-fighting-a-new-pos-malware-family/.

17. Ryan Flores, Lord Remorin, Mary Yambao, and Don Ladores. (16 June 2015). *Trend Micro Security News.* "Piercing the HawkEye: How Nigerian Cybercriminals Used a Simple Keylogger to Prey on SMBs." Last accessed on 20 July 2015, http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hawkeye-nigerian-cybercriminals-used-simple-keylogger-to-prey-on-smbs.

18. Trend Micro. (26 May 2015). *TrendLabs Security Intelligence Blog.* "Attack of the Solo Cybercriminals—Frapstar in Canada." Last accessed on 20 July 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/attack-of-the-solo-cybercriminals-frapstar-in-canada/.

19. Tom Heyden. (28 May 2015). *BBC News Magazine*. "How Did My Dad's Uber Account Get Hacked?" Last accessed on 20 July 2015, http://www.bbc.com/news/magazine-32900600.

20. Fernando Mercês. (18 November 2014). *Trend Micro Security Intelligence.* "The Brazilian Underground Market: The Market for Cybercriminal Wannabes?" Last accessed on 20 July 2015, http://www.trendmicro.ca/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-brazilian-underground-market.pdf.

21. Ciarán Hancock. (29 April 2015). *The Irish Times.* "Ryanair Falls Victim for €4.6M Hacking Scan via Chinese Bank." Last accessed on 20 July 2015, http://www.irishtimes.com/news/crime-and-law/ryanair-falls-victim-to-4-6m-hacking-scam-via-chinese-bank-1.2192444.

22. Numaan Huq. (September 2014). *Trend Micro Security Intelligence.* "PoS RAM Scraper Malware: Past, Present, and Future." Last accessed on 6 July 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf.

23. Gerri Detweiler. (19 September 2013). *Credit.com.* "What Does FICO Stand For? What Is a FICO Score?" Last accessed on 21 July 2015, http://www.credit.com/credit-scores/what-does-fico-stand-for-and-what-is-a-fico-credit-score/.

24. Fahmida Y. Rashid. (2 June 2011). *eWeek.* "Northrop Grumman, L-3 Communications Hacked via Cloned RSA SecurID Tokens." Last accessed on 21 July 2015, http://www.eweek.com/c/a/Security/Northrop-Grumman-L3-Communications-Hacked-via-Cloned-RSA-SecurID-Tokens-841662.

25. Mary Pat Flaherty, Jason Samenow, and Lisa Rein. (12 November 2014). *The Washington Post.* "Chinese Hack US Weather Systems, Satellite Network." Last accessed on 21 July 2015, http://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html.

26. Rachelle Younglai. (23 June 2015). *The Globe and Mail.* "Small Canadian Gold Firm Suffers Computer Hack." Last accessed on 21 July 2015, http://www.theglobeandmail.com/report-on-business/industry-news/energy-and-resources/small-canadian-gold-firm-suffers-computer-hack/article25083416/.

27. Lee Johnstone. (24 June 2015). *CTRLBOX.COM.* "Detour Gold Corporation (TSX:DGC) June 2015 Data Leak Analysis." Last accessed on 21 July 2015, https://www.ctrlbox.com/docs/reports/Detour-Gold-Breach.pdf.

28. SANS Institute. (2014). *SANS.* "Critical Security Controls." Last accessed on 22 July 2015, https://www.sans.org/critical-security-controls/.

29. SANS Institute. (2014). *SANS.* "Critical Security Controls: A Brief History." Last accessed on 22 July 2015, https://www.sans.org/critical-security-controls/history.

30. Council on CyberSecurity. (2014). "Critical Security Controls." Last accessed on 22 July 2015, http://www.counciloncybersecurity.org/critical-controls/.

31. SANS Institute. (2014). *SANS.* "Critical Security Controls for Effective Cyberdefense." Last accessed on 22 July 2015, http://www.sans.org/media/critical-security-controls/fall-2014-poster.pdf.

32. Council on CyberSecurity. (2014). "The Critical Security Controls for Effective Cyberdefense." Last accessed on 22 July 2015, https://ccsfiles.blob.core.windows.net/web-site/file/bb820ab03db7430abac40451ba4d3bb7/CSC-MASTER-VER5.1-10.7.2014.pdf.

33. Ponemon Institute and IBM. (May 2014). "2014 Cost of Data Breach Study: Global Analysis." Last accessed on 24 June 2015, http://www-935.ibm.com/services/multimedia/SEL03027USEN_Poneman_2014_Cost_of_Data_Breach_Study.pdf.

34. Christopher J. Cox and David R. Singh. (2015). *Weil.* "Security Breach Notification Laws Data Privacy Survey 2015." Last accessed on 23 June 2015, www.weil.com/~/media/files/pdfs/security_breach_notification_broch_en_digital_2015_v2.pdf.

35. National Conference of State Legislatures. (11 June 2015). "Security Breach Notification Laws." Last accessed on 23 June 2015, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

36. Rodika Tollefson. (22 June 2015). *Fox Business.* "What Are the Data Breach Notification Laws in Your State?" Last accessed on 23 June 2015, http://www.foxbusiness.com/technology/2015/06/22/what-are-data-breach-notification-laws-in-your-state/.

37. The White House. (2015). "The Personal Data Notification and Protection Act." Last accessed on 23 June 2015, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf.

38. Peter Carey and Kenneth Wainstein. (12 February 2015). *Cadwalader.* "The Obama Administration's Personal Data Notification and Protection Act: An Analysis." Last accessed on 23 June 2015, http://www.cadwalader.com/resources/clients-friends-memos/the-obama-administrations-personal-data-notification-and-protection-act-an-analysis.

39. Meena Harris. (25 February 2014). *Inside Privacy.* "Comparison of Five Data-Breach Bills Currently Pending in the Senate." Last accessed on 18 September 2015, http://www.insideprivacy.com/united-states/congress/comparison-of-five-data-breach-bills-currently-pending-in-the-senate/.

40. David Gilbert. (23 July 2015). *International Business Times*. "Anonymous Hacks US Census Bureau over TTIP Agreement, Leaking Employee Details Online." Last accessed on 23 July 2015, http://www.ibtimes.co.uk/anonymous-hacks-us-census-bureau-over-ttip-agreement-leaking-employee-details-online-1512244.

41. Kate Vinton. (9 July 2015). *Forbes*. "21.5 Million Americans Were Compromised in OPM's Second Breach." Last accessed on 23 July 2015, http://www.forbes.com/sites/katevinton/2015/07/09/21-5-million-americans-were-compromised-in-opms-second-breach/.

42. Kenneth R. Harney. (2 June 2015). *The Washington Post*. "IRS Data Breach May Prove Worrisome for Those Seeking a Mortgage." Last accessed on 23 July 2015, http://www.washingtonpost.com/realestate/irs-was-told-in-2011-that-its-security-and-privacy-controls-were-inadequate/2015/06/01/de42884a-0886-11e5-95fd-d580f1c5d44e_story.html.

43. Jose Pagliery. (17 July 2015). *CNN Money*. "UCLA Health Hacked, 4.5 Million Victims." Last accessed on 23 July 2015, http://money.cnn.com/2015/07/17/technology/ucla-health-hack/.

44. Cassandra Fairbanks. (22 July 2015). *The Independent*. "Ashley Madison Hack: 'Out of All the Data Breaches This Is Probably the Funniest.'" Last accessed on 23 July 2015, http://www.independent.co.uk/voices/comment/ashley-madison-hack-out-of-all-the-data-breaches-that-have-happened-this-is-probably-the-funniest-10407666.html.

45. Thomson Reuters. (21 July 2015). *CBC News*. "Costco Joins Walmart in Shutting Online Photo Store After Possible Data Breach." Last accessed on 23 July 2015, http://www.cbc.ca/news/technology/costco-joins-walmart-in-shutting-online-photo-store-after-possible-data-breach-1.3161523.

46. The Canadian Press. (14 July 2015). *News 1130*. "Possible Data Breach on Walmart Photo Site." Last accessed on 30 July 2015, http://www.news1130.com/2015/07/14/possible-data-breach-on-walmart-photo-site/.
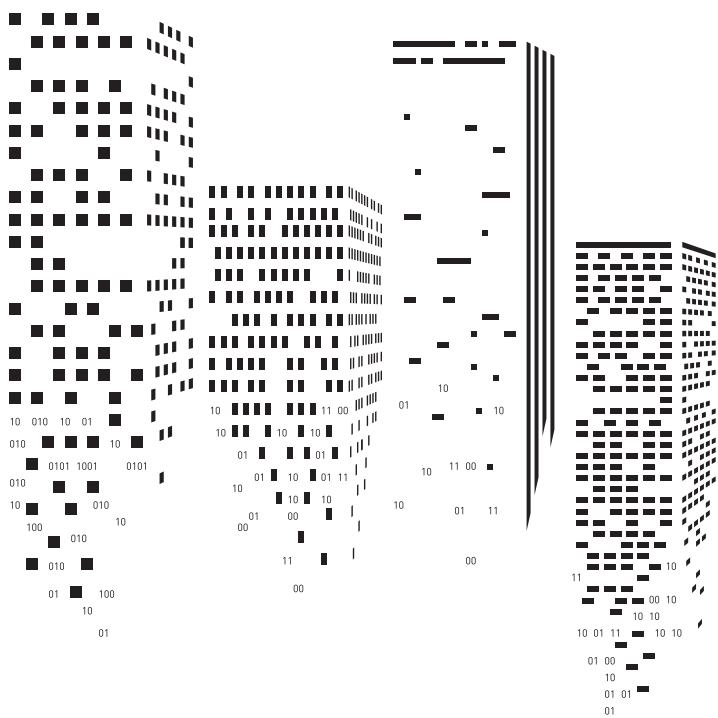
Created by:

Trend**Labs**

The Global Technical Support and R&D Center of **TREND MICRO**

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver topranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

TREND MICRO
M I C R O™

Securing Your Journey
to the Cloud