the Availability Digest

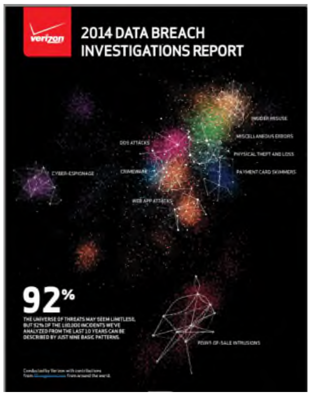
www.availabilitydigest.com
@availabilitydig

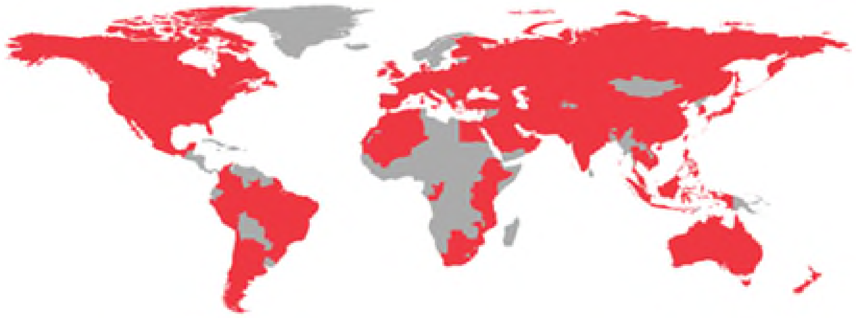
2014 Verizon Data Breach Investigations Report

September 2014

This is the tenth year that Verizon has issued its Verizon Data Breach Investigations Report (DBIR).[1] The DBIR analyzes reported security incidences, data breaches (those in which data was exposed), and confirmed data disclosures (those in which information was actually stolen).

The reports for the 2014 DBIR come from fifty contributing organizations. All in all, this report covers 63,437 security incidences that resulted in 1,367 data breaches. The security incidences originated from 95 different countries around the world.





Countries Included in the 2014 Verizon DBIR Report

Verizon uses the following definitions:

- Security Incident – a security event that compromises the integrity, confidentiality, or availability of an information asset.
- Breach – a security incident that results in the exposure or potential exposure of data.
- Data Disclosure – a breach for which it was confirmed that data was actually disclosed to an unauthorized party.

2014 was the year of large-scale attacks on payment card systems, with the Target hack of 110 million credit cards and debit cards bringing this attention to everyone.[2] However, attacks were made against many industries. The 2014 DBIR records data breaches against the following industries:

Finance	465	Information	31	Real Estate	4

[1] 2014 Verizon Data Breach Investigations Report
http://www.verizonenterprise.com/DBIR/2014/

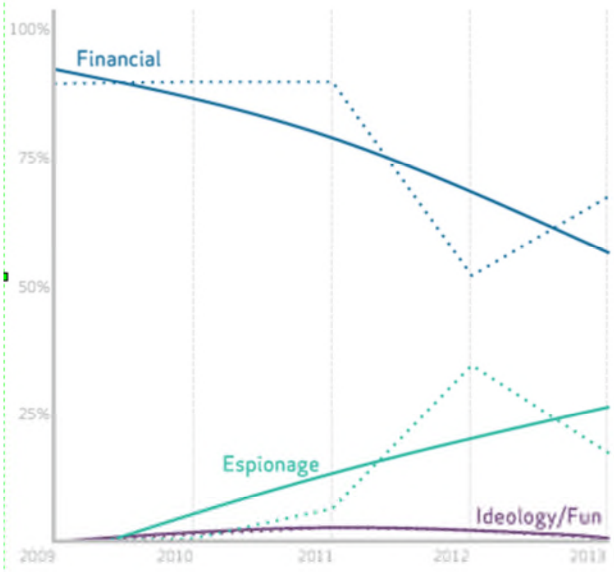
[2] Target Compromises Millions of Payment Cards, *Availability Digest*; January 2014.
http://www.availabilitydigest.com/public_articles/0901/target.pdf

Public	175	Education	15	Trade	3
Retail	148	Mining	10	Construction	2
Accommodation	137	Transportation	10	Management	1
Utilities	80	Administrative	7	Other	8
Professional	75	Healthcare	7	Unknown	126
Manufacturing	59	Entertainment	4		

The reasons for the attacks have changed over time. The two primary attack motives have been financial and espionage. Financial attacks are aimed at obtaining data such as bank account credentials or payment-card information that is easily converted to cash. Espionage attacks attempt to access internal corporate data or trade secrets.

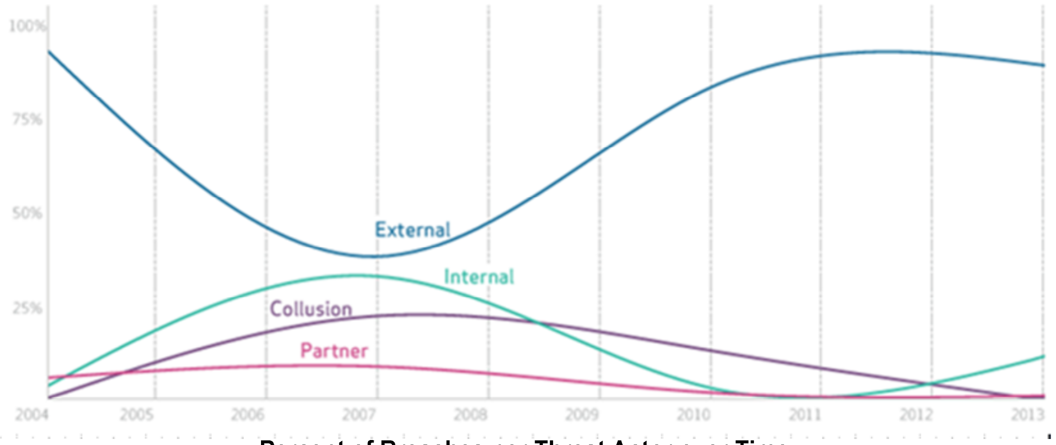
Four years ago, financial motives accounted for almost 90% of all attacks. In 2013, that percentage dropped significantly due to the increase in espionage attacks, which accounted for about 25% of all attacks in 2013. A few attacks have been motivated by ideology, especially the DDoS attacks against major U.S. banks in late 2012 and early 2013 by an Islamic group attempting to get the offensive video "Innocence of Muslims" removed from YouTube.[3]

Almost all breaches have been initiated by one of four "threat actors." These include external and internal attackers, partners, and collusions (attacks initiated by external, internal, or partner actors working together).



Percent of Breaches per Motive over Time

Most attacks over the years have been launched by external actors. In 2013, external attacks accounted for about 80% of all attacks. Internal attacks have consistently been a remote number 2, accounting for about 10% of attacks in 2013.



Percent of Breaches per Threat Actor over Time

Verizon was able to categorize most of the security incidents into nine categories. These categories describe 94% of all data breaches over the last four years:

[3] DDoS Attacks on U.S. Banks Continue, *Availability Digest*; January 2013.
http://www.availabilitydigest.com/public_articles/0801/more_bank_attacks.pdf

- POS Intrusions
- Web App Attacks
- Insider and Privilege Misuse
- Physical Theft and Loss
- Miscellaneous Errors
- Crimeware
- Payment Card Skimmers
- Cyber-Espionage
- Denial of Service Attacks

POS Intrusions

A POS Intrusion is an attack in which POS devices are compromised. Typically, malware is installed in the POS terminals of a retail establishment (retailers, hotels, grocery stores) to collect magnetic-stripe data from the memory of the terminals. Most of these attacks are attributed to criminal groups operating in Russia and Eastern Europe.

In 99% of the cases, the victim learned of the attack through a third party, often a payment-card company that has tracked down the usage of multiple cards involved in fraudulent transactions. These attacks are reported to law enforcement agencies, which can then discover related breaches.

In almost all cases, it took only minutes to launch an attack, but discovery was not until weeks or months later. This delay depended in large part upon the length of time the attacker took to cash in. The longer he waited, the longer was the discovery time and the greater was his financial return.

The predominant industries victimized by POS intrusion attacks include retail, accommodations, and food service.

Verizon’s recommended controls for POS intrusion attacks include:

- Restrict remote access to POS terminals.
- Enforce password policies (do not use defaults).
- Don’t use POS terminals to browse the web, get email, use social media, or play games.
- Install and maintain anti-virus software on POS systems.
- Segment POS network environments from the corporate network.
- Monitor network for suspicious activity.
- Use two-factor authentication.

Web App Attacks

A Web App Attack exploits a weakness in a web-based application. A typical weakness is inadequate input data validation, such as the recent wide-spread Heartbleed vulnerability.[4]

Another strategy to gain access to a web application is to use stolen credentials to impersonate a user. Such information is gained by phishing, password guessing, and SQL injection attacks. Many of these attacks result in infecting a server for inclusion in a botnet for DDoS attacks.

The predominant industries victimized by web application attacks include Information, Utilities, and Retail.

Verizon’s recommended controls for web application attacks include:

- Don’t use single passwords.

[4] Heartbleed – The Worst Vulnerability Ever, *Availability Digest*; April 2014.
http://www.availabilitydigest.com/public_articles/0904/heartbleed.pdf

- Be careful using CMS (Content Management Systems) like WordPress, Joomla, and Drupal.
- Validate data input vulnerabilities.
- Enforce lockout policies (multiple failed attempts).
- Monitor outbound connections in order to block suspicious traffic (such as to Eastern Europe).

Insider and Privilege Misuse

Privilege Misuse attacks involve taking advantage of the system access privileges granted by an employer to an employee or partner who uses the access privileges to commit nefarious acts. These acts can range from self-serving (gaining information to aid in promotions) to those aimed at financial gain or espionage.

Often, the attacker makes off with sensitive information by writing it to a USB drive or be emailing it to himself. In some cases, attackers have stolen someone else's credentials to obtain their privileges or have found ways to circumvent access controls.

The predominant industries victimized by privilege misuse include Public, Real Estate, Administrative, Transportation, Manufacturing, and Mining.

Verizon's recommended controls for privilege misuse attacks include:

- Build controls to protect data and detect misuse.
- Review user accounts.
- Watch for data exfiltration.
- Publish anonymized results of audits of actions to alert employees that their actions are being monitored.

Physical Theft and Loss

Physical Theft and Loss involves an information asset that went missing either through misplacement or malice. Information assets involve laptops, disk drives, and documents.

The predominant root cause in Theft and Loss attacks is employee carelessness. Fifteen times more assets go missing because of loss rather than theft. When it comes to theft, 43% of all thefts are from employees' workplaces. Theft from employees' personal vehicles accounts for 23% and 10% from their personal residences.

The predominant industries affected by physical theft and loss include Healthcare, Public, and Mining.

Verizon's recommended controls for physical theft and loss include:

- Encrypt information (and check encryption periodically).
- Keep sensitive devices in sight and in possession at all times.
- Regular and preferably automatic backup of all critical information on a device.
- Lock devices down.
- Use unappealing technology (old laptops, disguised laptops).

Miscellaneous Errors

Miscellaneous Errors include unintentional actions that directly compromise a security attribute of an information asset. Highly repetitive and mundane business processes involving sensitive information are particularly error prone.

Examples of miscellaneous errors include sending paper documents or emails to the wrong recipient (49%), accidentally posting non-public information to a public web site (29%), and disposal errors (20%).

The predominant industries affected by miscellaneous errors include Public, Administrative, and Health Care.

Verizon's recommended controls for miscellaneous errors include:

- Use Data Loss Prevention software to track email recipients.
- Tighten up processes for posting documents to internal and external sites.
- Spot-check samples of large mailings to ensure that the name on the envelope matches the contents.
- Sanitize assets such as computers and disks before disposing of them.

Crimeware

Crimeware attacks attempt to gain control of systems as a platform for illicit purposes, such as stealing credentials, DDoS attacks, spamming, artificially boosting ad revenue, etc. Crimeware attacks consist primarily of opportunistic infections tied to organized criminals with financial, espionage, or other motives.

A Crimeware attack is fairly simple to launch. There are online markets that offer Cybercrime-as-a-Service.

The predominant industries victimized by Crimeware attacks include Public, Information, Utilities, and Manufacturing.

Verizon's recommended controls for miscellaneous errors include:

- Keep browsers and plug-ins up to date.
- Disable Java in browsers.
- Use two-factor authentication.
- Deploy system configuration change monitoring.
- Use threads of threat data to accelerate detection.

Payment-Card Skimmers

In a Payment-Card Skimmer attack, a skimming device is physically implanted on an assed that reads magnetic-stripe data from a credit card. 87% of affected devices are ATMs. Gas pumps account for 9%, and POS terminals and other devices make up the rest.

The skimming devices are realistic in appearance and are difficult to spot by the untrained user. They export data via Bluetooth or cellular transmission to protect the attacker from discovery.

Skimming attacks are typically detected by the payment-card companies or the customers based on fraudulent transactions.

The predominant industries victimized by payment-card skimmers include Finance and Retail.

Verizon's recommended controls for miscellaneous errors include:

- Use tamper-resistant terminals.
- Use tamper-evident controls to make it obvious when tampering occurs.
- Regularly check terminals for signs of tampering.
- For consumers:
  - When entering a PIN, block your hand to prevent tiny cameras from recording your PIN.
  - If something looks out of the ordinary, don't use the terminal.
  - If something looks out of place, report it.

Cyber-Espionage

Cyber-Espionage is the unauthorized access to networks or systems for the purpose of espionage. Cyber-espionage attacks have tripled in the last year.

Most cyber-espionage attacks are launched by state-affiliated attackers (87%). 11% are launched by organized crime actors. Most attacks are launched from Eastern Asia (China – 49%) and Eastern Europe (21%). Access to victimized systems is typically through the theft of credentials via phishing (78%).

The predominant industries victimized by cyber-espionage include Professional, Transportation, Manufacturing, and Mining.

Verizon's recommended controls for cyber-espionage attacks include:

- Keep all patches up to date.
- Use an up-to-date antivirus utility.
- Train users to recognize and report potential incidents.
- Segment networks to contain an incident.
- Log system, network, and application activity.
- Implement solutions that defend against phishing.
- Use threat-indicator feeds to monitor and filter outbound traffic for suspicious connections and exfiltration of data to remote hosts.
- Stop lateral movement inside the network.

Distributed Denial of Service Attacks

A distributed denial-of-service (DDoS) attack is intended to compromise the availability of networks and systems to take down a company's web portals. DDoS attacks have become more frequent, larger, and longer. A recent attack against Spamhaus comprised 300 gigabits/second of data launched at it for days.[5]

DDoS attacks are launched from botnets of thousands of infected PCs or servers under the control of a botmaster.

The predominant industries victimized by DDoS attacks include Finance, Retail, Professional, Information, and Public.

Verizon's recommended controls for DDoS attacks include:

- Servers and services should always be patched when in use, turned off when not in use, and available only to the people who need them to keep them from being infected with DDoS attack malware.

[5] History's Largest DDoS Attack?, *Availability Digest*; April 2013.
http://www.availabilitydigest.com/public_articles/0804/spamhaus.pdf

- Segregate key IP/servers from non-essential IP space. Any non-essential IP space should be advertised out of a separate circuit.

- Use your provider’s anti-DDoS service and test it quarterly.
- Have a plan in place in case your primary anti-DDoS defense doesn’t work.
- Most attacks are just over the amount of data that you can manage.
- Understand the traffic capacity of your anti-DDoS provider.

Conclusions

Verizon notes the following characteristics that apply to a great number of the attacks that it studied:

- Aside from DDoS attacks, in most cases it took weeks to months for the victim to discover the breach, though it only took a few minutes to launch the attack. Most attacks were discovered by outsiders.

- Most security incidences did not result in data disclosures except for POS Infiltration and Payment-Card Skimming attacks. !00% of these attacks resulted in data disclosures.

- Phishing and browser infections are the primary threat actions. A phishing campaign of only ten email messages has a 90% chance of getting at least one click-through.

Verizon’s 2014 Data Breach Investigations Report is well-written, informative, and easy to understand. The seven pages in this review are expanded to fifty-eight pages in the report. We recommend that anyone who is concerned about malicious attacks on their systems read the report.