

When, Not If...

# Anatomy of a Data Breach

By Matthew J. Jeske  
and James M. Paulino II

The number of data breach incidents will continue to rise with the exponential pace of the data that we generate and the ever-expanding connectivity of our world.

During 2014, the issue of cybersecurity was thrown into the spotlight after numerous high-profile attacks against Sony, Target, J.P. Morgan Chase, Staples, Neiman Marcus, The Home Depot, and even Healthcare.gov, resulting in

the release of data for over 250 million accounts and costing a reported \$500 million in lost profits, theft, security upgrades, additional staffing, debit and credit card replacements, and legal fees. Sharon Tobias, 2014: The Year in Cyberattacks, Newsweek (Dec. 24, 2014), <http://www.newsweek.com/2014-year-cyber-attacks-295876> (last visited Jan. 28, 2015). 2014 also brought the second example of a cyber-attack causing physical damage when a hacker gained control of a German steel mill, which forced an unscheduled shutdown. See Hack Attack Causes “Massive Damage” at Steel Mill, BBC News (Dec. 22, 2014), <http://www.bbc.com/news/technology-30575104> (last visited Jan. 28, 2015). The first happened when the Stuxnet computer virus damaged some uranium enrichment centrifuges in Iran. See Julian Hattam, Snowden: US Started Rash of Cyberattacks, The Hill (Jan. 8, 2015), <http://thehill.com/policy/cybersecurity/228916-snowden-us-started-spate-of-cyberattacks> (last visited Jan. 28, 2015).

started-spate-of-cyberattacks (last visited Jan. 28, 2015); Ahmadinejad Admits Centrifuges Damaged by Virus, Jerusalem Post (Nov. 29, 2010), <http://www.jpost.com/International/Ahmadinejad-admits-centrifuges-damaged-by-virus> (last visited Jan. 28, 2015).

In the first days of 2015, President Obama and Congress already had called for the federal government to take a more proactive role in national reporting standards and military preparedness, with President Obama calling for international efforts with the United Kingdom as part of a joint cybersecurity unit. See White House Office of the Press Secretary, Securing Cyberspace – President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts (Jan. 13, 2015), <http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat> (last visited Jan. 28,



■ Matthew J. Jeske, G.C.F.E., A.C.E., Chief Technology Officer of Crane Data Forensics LLC in Minneapolis, is a certified data forensic examiner who assists clients across the industry with critical data-loss cases and management of human resource incidents and provides digital forensic support for situations involving intellectual property theft, fraud, harassment and other breaches of data security. James M. Paulino II is an associate in the Rochester, New York, office of Goldberg Segalla LLP and a member of the firm’s Cyber Risk Practice Group.

2015); Chris Strohm, Angela Greiling Keane, & Robert Hutton, Obama, Cameron Vow to Bolster Cybersecurity After Sony Hack, Bloomberg (Jan. 15, 2015), <http://www.bloomberg.com/news/2015-01-16/obama-cameron-cybersecurity-agenda-shaped-by-paris-sony-attacks.html> (last visited Jan. 28, 2015). As the stage is set for the first major debate over federal legislation, two basic issues emerge for attorneys and clients alike. First and foremost, what exactly is a data breach? Second, what is the current legal framework through which we litigate in the aftermath of a cyberattack? This article seeks to provide the wary lawyer some fundamental concepts on both the technical and legal sides of this vital issue.

### Data Breach—It Affects Us All

So what is a data breach? Experian, a leader in global information services, provides the following definition:

A data breach occurs when secure data is released to or accessed by unauthorized individuals. The lost data may be sensitive personal data the company has collected on employees or customers or proprietary and confidential data regarding business operations and trade secrets. Data breaches can involve the loss or theft of digital media or physical data and devices, such as computer tapes, hard drives, mobile devices and computers. The incidents pose serious risks for organizations as well as for the individuals whose data has been lost.

In plain English, it's when someone steals data from computers, including computers with expensive and high-tech security systems.

The range of data breaches is as vast as the imagination, from a total wipe of 30,000 computers at a Saudi Arabian state oil company to a small town's failure to erase hard drives containing staff social security numbers and addresses before selling them for second hand use. See Ellen Nakashima, Pentagon to Boost Cybersecurity Force, Wash. Post (Jan. 27, 2013), ([http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/27/d87d9dc2-5fec-11e2-b05a-605528f6b712\\_story.html](http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/27/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html)) (last visited Jan. 28, 2015). As we become more reliant on digital systems, there are an increasing number of points to access sensitive data.

Breaches can be caused by human error, such as when a coding issue in a pharmacy chain's new mobile phone application allows open access to medical files and prescription records, or by human initiative, such as when a high-school student changes grades and attendance records through the school system computers. Most large-scale breaches, however, are the result of calculated espionage against and advanced persistent threats (APT) to large retailers and financial institutions as well as government agencies and our nation's power grid and other critical infrastructure.

These examples make clear that no organization is immune to cyber threats, big or small.

The primary targets of cyberattacks are those that we as consumers use the most often, which hold the majority of our personal records. These targets include retail point-of-sale systems, financial institutions, healthcare, social networks, government agencies, and more. Regardless of how hard we try to protect ourselves, we are forced to trust others with our data. The popularity of cloud computing and storage, services such as Dropbox and Gmail, has introduced petabytes of sensitive data that travel around the world in the blink of an eye. We are putting a great deal of trust in service providers to take the necessary measures to protect our data. New channels to communicate and to access data with social networks, online banking, and cloud storage are introduced at a lightning pace. Keeping up with the security to protect who we are and what we access and share has become extremely difficult. Cyber attackers are just as quick to identify and to exploit vulnerabilities in under tested systems.

Convenience over security is the desire of the majority of consumers today. Ever forget your wallet, purse, or credit cards at home by mistake and find yourself reaching into your glove box to resurrect your checkbook? Try to fill your gas tank or buy lunch at a local restaurant and you will find yourself likely going hungry or running on fumes on your drive home. It is near impossible to find a retailer that will permit the use of a personal check any longer. As a result, we use credit and debit cards everywhere we go. Despite the framework

of the Payment Card Industry Data Security Standards (PCI DSS), you cannot trust that all card handlers follow them. The use of card skimmers and poorly handled client records can easily place client card information in the wrong hands. There is a great deal of ground to be made on keeping up with data security for the small businesses of the world.

As we become more  
reliant on digital systems,  
there are an increasing  
number of points to  
access sensitive data.

Cyber attackers today make victims of nearly every major industry and geographic region on earth. Though many businesses use improved technologies and enforce security policies to protect themselves from attack, it will become mandatory that businesses have cyber insurance policies to protect their assets even further. It's not a matter of "if," but "when" organizations will find themselves in the position of defending themselves from the aftermath of an attack. Furthermore, attackers are often located outside of our national borders, and the lack of international cooperation allows this trend to continue. It was reported by Experian, "The biggest challenge for companies will be awareness of each country's regulations and complying with all of them. Privacy attorneys who work in foreign jurisdictions are best suited to help companies understand the global notification responsibilities after a breach."

### Key Elements and Classifications of Data Breaches

In our best attempts to break down the core anatomy of a data breach, we can identify some key concepts, terms, elements, and classifications. The number of available resources is endless, but we find two worth noting. The National Initiative for Cybersecurity Careers and Studies

has released a comprehensive dictionary, “A Glossary of Common Cybersecurity Terminology” (<http://niccs.us-cert.gov/glossary>) (last visited Jan. 28, 2015), and Larissa Crum of Immersion Ltd. has come up with her list of “top 10 things organizations need to know.” See Tom Hagy, *When a Data Breach Happens: Be Ready, Be Calm, and Preserve Evi-*

Keeping up with the security to protect who we are and what we access and share has become extremely difficult.

dence, <http://www.lexisnexis.com/communities/corporatecounselnewsletter/b/newsletter/archive/2013/05/05/when-a-data-breach-happens-be-ready-be-calm-and-preserve-evidence.aspx> (last visited Jan. 28, 2015).

### What Type of Evidence Exists After a Data Breach?

The types of evidence left behind in the event of a breach can vary greatly, but there are some constants in all cases. Begin now—have your systems audited to ensure that the systems have the proper means to log data, back up data, and generate documentation. In many cases, third-party monitoring can be very helpful in identifying an attacker and tracking the moves that one makes. Without having regularly generated logs of your systems and appropriate historical data that you have kept on file or archived for later access, you may never be able to determine fully the origin of an attack or how long it went on. It is also important to note that a sloppy response to a breach can wipe out information that can be used to help you mitigate your exposure. After a breach, time is of the essence. Hire a data breach response vendor that will begin identifying the source of an attack and sever continued access. Once the network perimeter defenses have been established, a data breach response vendor will review event logs and perform scans for

malware and viruses. There are many types of vulnerabilities, ways to exploit them, and malicious software used to perform these attacks, so having the right tools to do the job of locating them requires special skills that an IT department nearly always will not have.

### How Can You Be Ready to Respond Quickly?

It is crucial to have a core response team waiting in the wings. Have team members assembled from all of the key areas of your organization. Sometimes this means involving outside counsel or vetted vendors so that you have all of the necessary expertise on hand to respond accordingly. At the same time, it might make sense to limit the people involved to maintain control of the situation in the event of an incident. The next step is to document the processes and to perform routine fire drills to avoid finding your company unprepared. Make sure to review and to update procedures on a regular basis as things change. Technology, staff, and the threat of hackers change with regularity and in turn so does the need to revisit your processes. In the event that an actual data breach has occurred, it is of the utmost importance that you document everything that has been done when making the decisions that you made. It is not classified as a breach until legal or forensic experts have deemed it so.

Verizon’s latest 2014 Data Breach Investigations Report (DBIR) does a great job detailing the definitions and trends in connection with primary bad actors, target industries and data types, infrastructure, and attack methods.

### Primary Bad Actors and Threats

These attackers are the individuals, groups, or governments that have malicious intent to compromise technical systems. Below is a graph of results over 10 years of data history from page 8 of the Verizon 2014 DBIR to demonstrate the *Number of breaches per threat actor category over time*. The source threats that the graph charts are internal, external, and from partners. See Table 1.

### Primary Data Targets

Below is a list of the leading data types that attackers intend to compromise in a breach.

- Credit card numbers—used for fraudulent transactions—have a mature underground market for the sale of compromised records.
- Protected health information (PHI), as defined by U.S. Department of Health and Human Services HIPAA Privacy Rule, “this is individually identifiable health information, that is transmitted or maintained in any form or medium by a covered entity or its business associates, excluding educational and employment records.”
- Social Security numbers, which are useful to building an individual’s profile for identity theft.
- Financial and insurance records, which includes access to online credentials and bank account information.
- Personally identifiable information (PII), often acquired from social networks and other public profiles.
- Trade secrets and credentials, which would include proprietary manufacturing process, product designs, and product formulas.

See Table 2.

### Primary Industry Targets

As reported in the July 2013 *IBM Security Services Cyber Security Intelligence Index*, IBM has identified five primary industries targeted by cyberattacks. Two industries consume nearly 50 percent of attacks annually as reported at that time: manufacturing, experiencing 26.5 percent and financial/insurance, experiencing 20.9 percent. These are the result of the greatest potential payoff for uncovering proprietary manufacturing methods and trade secrets and the obvious target of achieving access to online banking accounts with direct access to the cash in the financial market. The remaining are information and communication (18.7 percent), health and social services (7.3 percent), and retail and wholesale (6.6 percent).

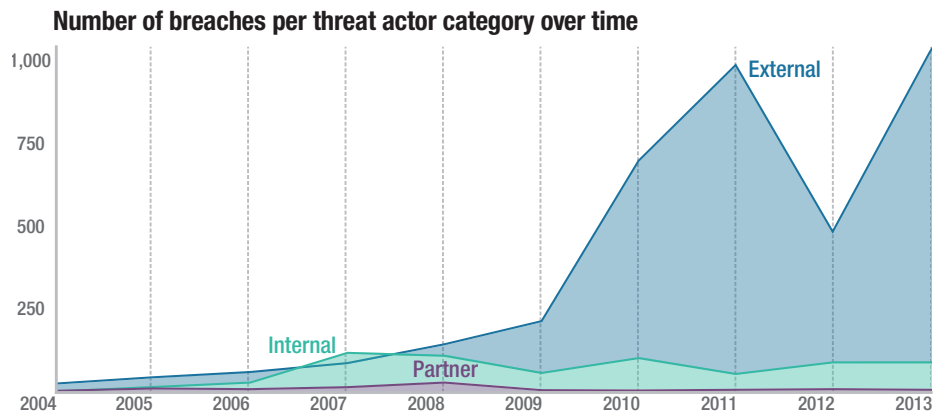
The Verizon 2014 DBIR page 14, further classifies data breaches into nine primary patterns and defines them as follows, listed in order of incident frequency in 2013.

- Web app attacks with 35 percent, defined as an incident in which a web application was the vector of attack. This includes exploits of code-level vulnerabilities in the application as well as

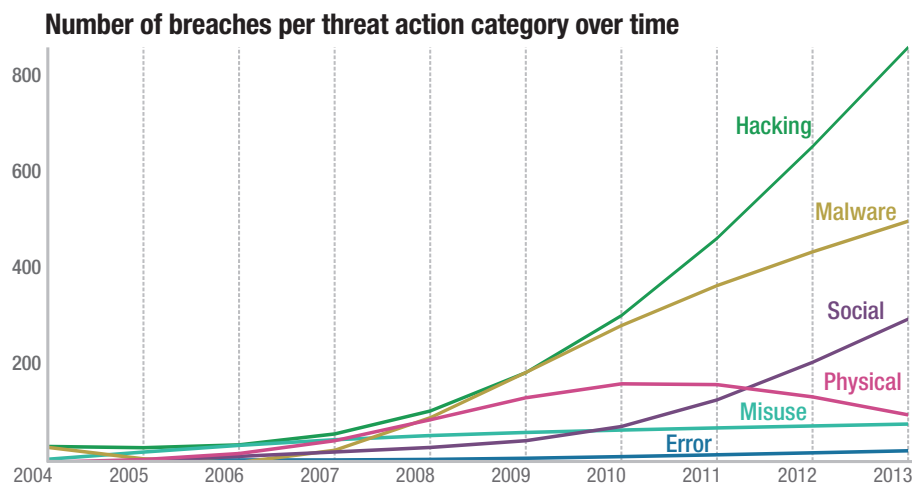
thwarting authentication mechanisms. Top industries suffering these attacks were information, utilities, manufacturing, and retail.

- Cyber espionage, with 22 percent, defined as incidents involving unauthorized network or system access linked to state-affiliated actors or exhibiting the motive of espionage. The top industries affected were professional, transportation, manufacturing, mining, and the public sector.
- Point-of-sale intrusions, with 14 percent, defined as remote attacks against the environments where retail transactions were conducted, specifically where card-present purchases were made. The top affected industries were accommodation and food services and retail.
- Payment card skimmers, with 9 percent, defined as incidents in which a skimming device was physically implanted on an asset (tampering) that read magnetic stripe data from a payment card (e.g., ATMs, gas pumps, POS terminals). Top affected industries were finance and retail.
- Insider and privilege misuse, with 8 percent, defined as incidents tagged with the action category of misuse—any unapproved or malicious use of organizational resources. This is mainly misuse, but outsiders, due to collusion, and partners, because they are granted privileges, show up as perpetrators as well. Top affected industries were the public sector, real estate, administrative, transportation, manufacturing, and mining.
- Crimeware, with 4 percent, defined as a malware incident that did not fit the other patterns such as espionage or point-of-sale attacks. We labeled this pattern “crimeware” because the moniker accurately describes a common theme among such incidents. In reality, the pattern covers a broad swath of incidents involving malware of varied types and purposes. The top affected industries were the public sector, information, utilities, and manufacturing.
- Miscellaneous errors, with 2 percent, defined as where unintentional actions directly compromised a security attribute of an information asset. This does not include lost devices, which is grouped with theft instead. Top industries

**Table 1**



**Table 2**



- tries affected included the public sector, administrative, and health-care.
- Physical theft or loss, with less than 1 percent, and is pretty much what it sounds like: an incident in which an information asset went missing, whether through misplacement or malice. Top affected industries were health-care, public sector, and mining. The next thing to note is the ratio of loss to theft, by a 15-to-one difference.
- Dos attacks, which the data pool did not identify, represented by 0 percent, but defined as an attack intended to compromise the availability of networks and systems and includes both network and application layer attacks. The top industries that we would expect to experience these types of attacks are finance, retail,

- professional, information, and the public sector.
- A category of miscellaneous attack types experienced 6 percent.

### Current Patchwork of Federal and State Laws

While the issue of cybersecurity is relatively new to the general public, it is nothing new in the eyes of the law. The current legal framework, however, differs from state to state, and there has been limited involvement by the federal government, which likely will change in 2015.

After the attack on Target, which released personal information for 110 million customers, litigation promptly commenced, with consumer claims consolidated by the Judicial Panel on Multidis-



strict Litigation into a single action before U.S. District Court Judge Paul A. Magnuson. *In re Target Corp. Cust. Data Sec. Breach Litig.*, D. Minn. MDL No. 14-2522 (PAM/JJK) (Dec. 18, 2014). In the First Amended Consolidated Class Action Complaint, the plaintiffs allege violations of distinct and conflicting state laws, including 49 consumer protection laws, all states

It's not a matter of "if," but "when" organizations will find themselves in the position of defending themselves from the aftermath of an attack.

except Alaska, and 38 data-breach laws requiring prompt notification of breaches to allow consumers to change passwords, obtain new debit or credit cards, and otherwise monitor personal accounts. Target, of course, moved to dismiss, and on December 18, 2014, Judge Magnuson decided the motion, and in doing so wrote an extremely detailed and helpful explanation of the nation's patchwork of laws.

As for the 49 separate consumer protection laws, Target argued that 26 states required allegations of economic injury, such as "pecuniary loss" in Wisconsin, Wis. Stat. §100.20; 18 states required allegations regarding a "duty to disclose," including California, Delaware, Kansas, Maryland, Minnesota, and Texas; eight states expressly prohibited class action treatment; three states, Delaware, Oklahoma, and Wisconsin, allow no private right of action; and two states, Ohio and Utah, allowed claims only when a court or the state attorney general has already declared the act deceptive.

As for the 38 specific data-breach statutes, eight allow enforcement through consumer protection laws (Alaska, Illinois, Maryland, Montana, New Jersey, North Carolina, North Dakota and Oregon); eight allow enforcement only by the government

(Arkansas, Connecticut, Idaho, Massachusetts, Minnesota, Nebraska, Nevada, and Texas); six have ambiguous enforcement provisions, which may allow private actions (Colorado, Delaware, Iowa, Kansas, Michigan and Wyoming); three states are silent but deemed to create a private cause of action (Georgia, Kentucky, and Wisconsin); one state, Rhode Island, is silent but deemed to create no private right; and three states, Florida, Oklahoma, and Utah, provide no private right of action at all.

At the federal level, although Congress has not passed legislation, in 2009, the U.S. Strategic Command created the United States Cyber Command, a sub-command that "plans, coordinates, integrates, synchronizes and conducts activities to direct the operations and defense of specified Department of Defense information networks and; [sic] prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries." See U.S. Strategic Command, U.S. Cyber Command, [http://www.stratcom.mil/factsheets/2/Cyber\\_Command/](http://www.stratcom.mil/factsheets/2/Cyber_Command/) (last visited Jan. 28, 2015). The U.S. Army created its own Cyber Command in 2010, See U.S. Army Cyber Command, Establishment of the U.S. Army Cyber Command, <http://www.arcyber.army.mil/history.html> (last visited Jan. 28, 2015). And the FBI has had ongoing anti-cyber-terrorism activities for years. See Leo Kelion, FBI 'Could Hire Hackers on Cannabis' to Fight Cybercrime, BBC News (May 22, 2014) <http://www.bbc.com/news/technology-27499595> (last visited Jan. 28, 2015).

On the consumer protection side, the federal government has had no substantive involvement. While the 2015 National Defense Authorization Act (H.R. 3979) did provide new mandatory reporting for national defense purposes, those reporting procedures are determined by the Secretary of Defense and require businesses to inform the military of breaches, and not to inform consumers. See H.R. Amend. to S. 1848, 2015 National Defense Authorization Act (Dec. 2, 2014) (H. Rules Comm. Print 113-58), available at <http://www.gpo.gov/fdsys/pkg/CPRT-113HPRT91496/pdf/CPRT-113HPRT91496.pdf>.

In short, America's current legal framework is piecemeal and state by state and not as comprehensive or up to date as recent developments in hacking and cyberattacks. As such, and as made clear by Judge Magnuson's insightful decision, there is significant room for improvement at the national level.

### 2015 Data Breach Forecast

Looking at what the future has to hold for cybersecurity and data breaches, we find some great predictions from the Experian 2015 Second Annual Data Breach Industry Forecast. The effect of heavily publicized data breaches in 2014 has businesses and consumers changing their attitudes on cybersecurity. Nearly half of organizations are increasing their investments in technologies to prevent a breach—while the adoption rate of cyber insurance policies more than doubled in 2014 over the previous year. Other predictions include the last ditch efforts of hackers to steal consumer credit card records before the required adoption of retailers to use EMV "chip and PIN" technologies to assist in preventing theft in the future. The deadline for the EMV implementation is October 2015 for VISA and MasterCard payments.

Protecting your passwords—the keys to the kingdom—is essential to protecting access to all that we store in the cloud. The use of multi-factor authentication is highly recommended to prevent unauthorized access to your sensitive information, even in the event that you are one of the unfortunate millions whom have their logins stolen in the countless data breaches that we see publicized in the media.

Health care will continue to create a growing threat as electronic medical records become more accessible and the growing popularity of wearable technologies begin gathering data about its users. Many are unsure what hackers have to gain from stealing a patient's PHI; it isn't clear what can be of value. The answer is that many hackers use these records to gain access to medical services, acquiring drugs, and defrauding insurers and government agencies that issue benefits programs.

In 2015, we will continue to see the shift of blame for breaches moving away from IT departments and toward the leadership of the business security practices across the

board. As with Target Corporation, we have seen top-level executives lose jobs or jumping ship as details unfold on the root causes for cyberattacks. Key areas of focus to minimize the likelihood of an incident are to be pointed inward because employees and the human element, as in the past will continue to be the leading cause of a successful breach of a system.

**Coordinating mock runs of breaches and systems evaluations and implementing proper intrusion prevention, monitoring and alerts, and anti-virus and anti-malware solutions are crucial.**

One final area to keep an eye on as we move into 2015 is the “Internet of Things” (IoT). Manufacturers of everything from thermostats, keyless entry, wearables, and more will continue to create a means of access to unforeseen exploits. The world of technology is ever-changing and affects us all more and more every day. Don’t let the exhaustive reports of data breaches and other forms of cyberattack leave you thinking that there is nothing that you can do to protect yourself. Identify theft protection, multifactor authentication, and creating unique passwords are very effective in protecting you from becoming the next victim.

### Proactive Assessment and Management

As hackers become increasingly sophisticated, businesses must take proactive measures to protect against cyberattacks, and they can never let their guard down. Coordinating mock runs of breaches and systems evaluations and implementing proper intrusion prevention, monitoring and alerts, and anti-virus and anti-malware solutions

are crucial. There are many resources available today that can be used to develop effective incident response plans. Experian has published a *Data Breach Response Guide*, which does a fantastic job of describing how to ensure that a business has a data breach preparedness plan (<http://www.experian.com/assets/data-breach/brochures/response-guide.pdf>). The guide covers everything from how to assemble a response team, public relations, and working with law enforcement, to companywide preparedness training, checklists, reporting a breach, plugging the holes, and so much more.

Encryption is a must. As our networks continue to meld with the cloud and hybrid solutions that are no longer located on our premises, we have lost control over whom and what can access our data. With encryption, you’re not only preventing access by outsiders, but from the possibility of malicious insiders, ensuring that your data is only accessible by those needing it to perform their jobs. In addition, encryption should be used not only on portable devices, but also on internal devices to protect all data generated internally, even as it passes between computers and servers on a company’s network. Flat networks can no longer be trusted as safe. With the involvement and access of outside vendors and connectivity between sites, you’re only as strong as your weakest link.

### Case Studies

Let’s now turn to three case studies; they can help us to flesh out how cyberattacks have played out for three companies.

#### Sony PlayStation Network Consolidated Class Action Complaint

A hacktivist group using the name Anonymous claimed responsibility for the theft of 77 million user accounts in 2011. Case 3:11-md-02258-AJB-MDD, Document 190, filed June 13, 2014. The records included account names, birth dates, e-mail addresses, and credit card numbers from the PlayStation Network (PSN) network.

Systems were compromised by hacking into an application server behind a web server and two firewalls. The attacker, still unknown, disguised entry as a purchase transaction in the system that exploited a vulnerability known by Sony. Sony agreed to a preliminary settlement of \$15 million.

#### Heartland Payment Systems

This data breach occurred in late 2008, resulting from SQL injected into website code written for a web form, which allowed access to Heartland’s corporate network. The intruders spent six months hiding their activities using software that monitors and records network traffic to capture payment card data including card numbers, expiration dates, and cardholder names used within Heartland’s processing system.

“Heartland was certified by network-approved quality security assessors (QSAs) as being PCI compliant at the time of the breach and, in fact, had received this certification several times during the period in which the vulnerability had been present,” stated Robert Carr, the Heartland CEO during the time of the breach, in the article *Heartland Payment Systems: Lessons Learned from a Data Breach* in January 2010.

As stated in the same article,

In his concluding remarks on information sharing, Carr noted several additional observations taken from Heartland’s data breach experience that are instructive: (1) do not underestimate the insider threat, (2) ensure the appropriate audit scope, and (3) maintain in-house security expertise at the senior executive level. Carr emphasized that insider threats may not stem from intentional fraud but rather from misplaced employee goodwill.

#### Target Data Breach

The Target data breach was the largest retail attack in history, performed successfully via an outside partner’s system with access to the Target system; it affected up to 70 million individuals. Target reported in its fourth-quarter earnings that it had spent over \$61 million through February 1, 2014, responding to the breach. There are said to be more than 90 lawsuits filed against Target by customers and banks.

As stated in Target’s Data Breach FAQ online regarding what happened, “In mid-December 2013, we learned criminals forced their way into our system, gaining access to guest credit and debit card information. As the investigation continued, it was determined that certain guest information was also taken. The information included names, mailing addresses, email addresses or phone numbers.”


Target was certified as meeting standards for PCI in September 2013. In addition, the company made a recent \$1.6 million investment in malware detection from computer security firm FireEye, which also serves clients that include the CIA and the Pentagon, only to find the company breached six months later.

## Conclusion

“There are two types of companies: those who have been hacked, and those who don’t yet know they have been hacked,” explained John Chambers, CEO of Cisco at the World Economic Forum.

It’s not a matter of “if,” but rather “when” a data breach will occur. The number of data breach incidents will continue to rise with the exponential pace of the data that we generate and the ever-expanding connectivity of our world. It is crucial to have a plan, protection, and a policy to cover your assets. Know where your data lives and encrypt it.

As we look ahead at 2015, attorneys and clients must pay close attention to developments in technology and law, including the anticipated federal legislation mandating business to disclose details regarding any breach of consumers’ private information and credit card data. Because the proposed Personal Data Notification and Protection Act would require businesses to notify customers within 30 days of discovering a breach, it is our hope that the new federal law will be merely a foundation for states to build laws to protect their customers even more. The push for exposure of “how” a business was breached could be a huge value to other organizations to prevent future hacks, as long as it happens with care to ensure anonymity of details disclosed about the affected individuals.

In addition, we recommend taking a closer look at which types of data should require data encryption so that in the event of a data breach, the risk of sensitive information falling into the wrong hands will not be a cause for concern. It will be important that laws continue to be reviewed and revised with regularity because systems and technologies will not remain frozen for decades. They will continue to evolve in ways that we could never have imagined. 

## Sources

- *Verizon 2014 Data Breach Investigations Report*, available at <http://www.verizonenterprise.com/DBIR/2014/>
- *Experian 2014 Data Breach Industry Forecast*, available at <http://www.experian.com/data-breach/data-breach-industry-forecast.html>
- Experian Data Breach Resolution *Data Breach Response Guide* (August 2013), available at <http://www.experian.com/assets/data-breach/brochures/response-guide.pdf>
- NICCS National Initiative for Cybersecurity Careers and Studies, *Explore Terms: A Glossary of Common Cybersecurity Terminology*, available at <http://niccs.us-cert.gov/glossary>
- Jordan Robertson, *10 Head-Slapping Data Breaches*, Bloomberg (Feb. 11, 2013), <http://www.bloomberg.com/slideshow/2013-02-11/10-head-slapping-data-breaches.html>
- Alina Selyukh, U.S. offers companies broad standard to improve cybersecurity, Reuters (Feb. 12, 2014), available at <http://www.reuters.com/article/2014/02/12/us-usa-cybersecurity-standards-idUSBREA1B0AL20140212>
- Scribd.com, *Sony agrees to \$15M settlement*, available at <http://www.scribd.com/doc/234917930/Sony-agrees-to-15M-settlement#download>
- Julia S. Cheney, *Heartland Payment Systems: Lessons Learned from a Data Breach*, Payment Cards Center, Federal Reserve Bank of Philadelphia (January 2010), available at <http://www.phil.frb.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2010/d-2010-january-heartland-payment-systems.pdf>
- Target’s *Data Breach FAQ*, available at <https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ>
- Michael Riley, Ben Elgin, Dune Lawrence and Carol Matlack, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, Bloomberg Businessweek Technology (March 13, 2014), available at <http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data>
- U.S. Department of Health & Human Services, *New Rule Protects Patient Privacy, Secures Health Information* (January 17, 2013) available at <http://www.hhs.gov/news/press/2013pres/01/20130117b.html>
- IBM Global Technology Services, *IBM Security Services Cyber Security Intelligence Index* (July 2013), available at <http://public.dhe.ibm.com/common/ssi/ecm/en/sew03031usen/SEW03031USEN.PDF>
- Ponemon Institute *2014 Cost of Data Breach Study: Global Analysis* (May 5, 2014), available at <http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/>