

The Top 10 Breaches of 2009

FRSecure White Paper

The lessons learned from **The Top 10 Breaches of 2009**

Prepared By:
Evan Francen, CISSP CISM
Managing Partner
FRSecure LLC
evan@frsecure.com

v1.01, 12/8/09

Page 1

The Top 10 Breaches of 2009

Table of Contents

Table of Contents	2
Introduction – The Top 10 Breaches of 2009	3
2009 Breaches	3
2009 Observations	4
#10 – Astomos Energy	5
Stats	5
Breach Description	5
Lessons	5
#9 – Virginia Department of Health Professionals	6
Stats	6
Breach Description	6
Lessons	7
#8 – Network Solutions	7
Stats	7
Breach Description	7
Lessons	8
#7 – Zurich Insurance	8
Stats	8
Breach Description	8
Lessons	9
#6 – Arkansas Department of Information Systems	9
Stats	9
Breach Description	9
Lessons	10
#5 – Oklahoma Department of Human Services	11
Stats	11
Breach Description	11
Lessons	11
#4 – Mitsubishi UFJ Securities	12
Stats	12
Breach Description	12
Lessons	12
#3 – Health Net	13
Stats	13
Breach Description	13
Lessons	14
#2, #4 all-time – National Archives and Records Administration	14
Stats	14
Breach Description	15
Lessons	15
#1, #1 all-time – Heartland Payment Systems	16
Stats	16
Breach Description	16
Lessons	18
Conclusions	19
About FRSecure	19

The Top 10 Breaches of 2009

Introduction – The Top 10 Breaches of 2009

As long as there has been information, there has been this concept of a breach. What is a breach anyway?

At FRSecure we use the definition:

A breach is a loss of information control by a custodian of the information that increases the risk of unauthorized information disclosure, alteration and/or destruction.

Lose a laptop without encryption and you get a breach. Lose a laptop with full-disk encryption, sound key management procedures, and backups, you don't get a breach.

Each and every breach comes with lessons. The lessons can be used to learn more about risks, protection strategies, and information security in general. We don't mention breaches to scare anyone, we mention breaches to point out specific lessons that you can use to make your environment and information more secure. Our ultimate goal is to reduce the risk of unauthorized disclosure, alteration, and destruction of your sensitive information.

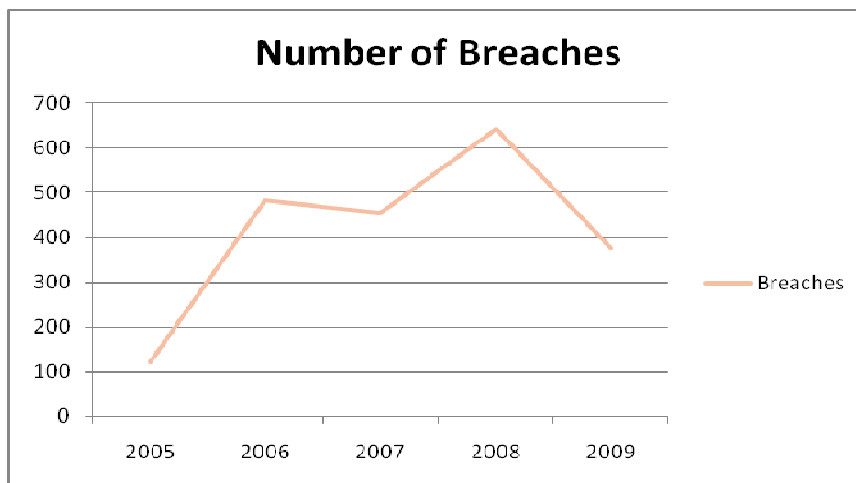
We thank the people at the Open Security Foundation for the creation and maintenance of the DataLoss DB. Their tireless work is paying dividends. Much of the information we reference in this White Paper is taken from their work. Check them out at <http://www.datalossdb.org>.

2009 Breaches

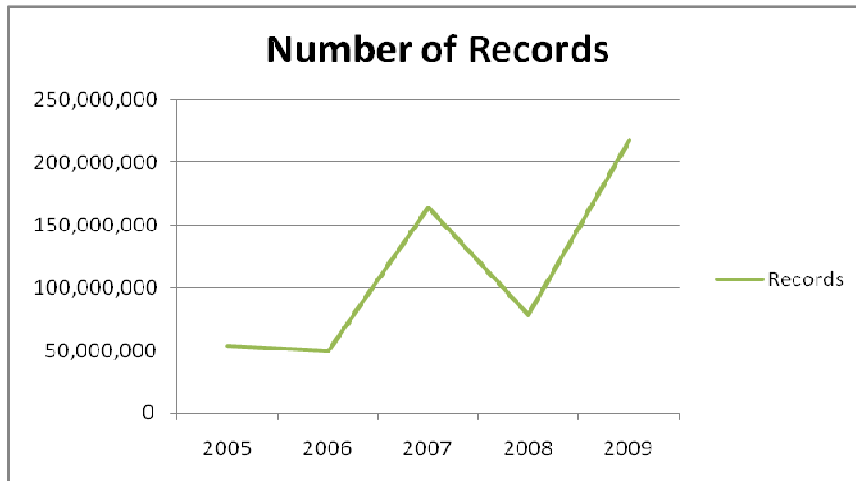
2009 is not over yet, but we have our fingers crossed that we won't have a top 10 breach in December. Let's look at the numbers through November.

The number of breaches tracked in the DataLoss DB through November stands at 375, compared with 645 for the same period in 2008. The average number of breaches reported per month dropped from 58.6 to 34. Does this mean that organizations are experiencing fewer breaches? That would be nice, but there may be other factors. Here are the number of breaches, number of records, and average number of records per breach over the past five years (January – November period).

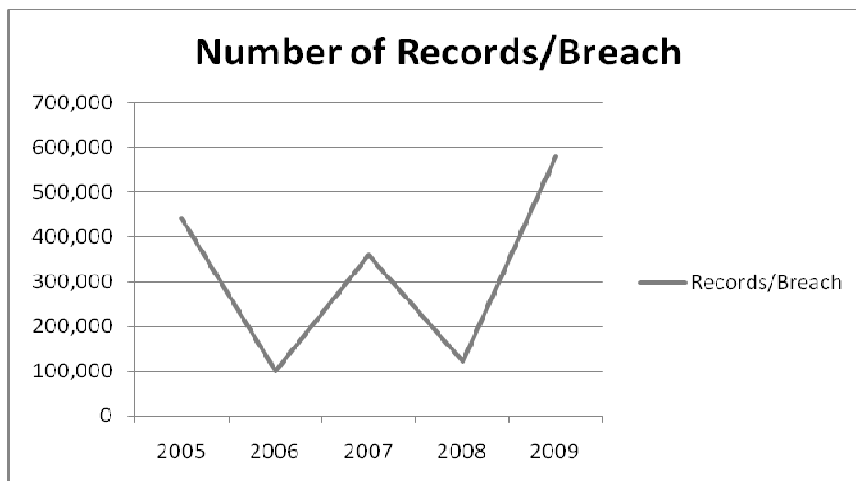
2005	– 121 breaches,	53,664,722 records,	443,510 records per breach
2006	– 484 breaches,	49,158,984 records,	101,568 records per breach
2007	– 455 breaches,	163,803,079 records,	360,007 records per breach
2008	– 642 breaches,	78,734,173 records,	122,639 records per breach
2009	– 375 breaches,	217,723,648 records,	580,596 records per breach



The Top 10 Breaches of 2009



The number of records increased by 176% in 2009.



The number of records per breach increased by 373% in 2009.

We can conclude that the number of breaches discovered by the Open Security Foundation declined by 41.6% in 2009, while the number of records increased by 176% and the number of records per breach increased by 373%. The primary factor in the rise in the number of records and number of records per breach are two largest breaches of 2009; totaling 206,000,000 records combined. These two breaches are highlighted in our Top 10 Breaches of 2009 and are among the top five of all-time

The fact that the number of breaches declined in 2009 could lead us to believe that we have either gotten better at preventing breaches, gotten worse at detecting breaches, or a combination of these and/or other factors.

2009 Observations

Can we really conclude that we have gotten better at preventing breaches? Maybe, but it's premature to make such an assertion. There are other factors:

- **Unknown Breaches** – We know for a fact that for every breach that is publicly announced there are perhaps thousands that go unannounced and/or undetected. According to Shawn Henry, assistant director for the Federal Bureau of Investigation's Cyber Division "Of the thousands of cases that we've investigated, the public knows about a handful," "There are million-dollar cases that nobody knows about."
- **Types of Records** – The breaches reported by the Open Security Foundation primarily concern those that affect one or more of three types of information; personally identifiable information, credit card information, and personal health information. There are many other types of information that

The Top 10 Breaches of 2009

are largely unaccounted for in the Open Security Foundation database, including: financial information, sales figures, new product plans, advertising programs, supplier lists, customer lists, wage and salary data, capital investment plans, projected earnings, changes in management, changes in policy, source code, testing data, designs, artwork, concepts, meeting minutes, and trade secrets. More than an estimate \$200,000,000,000/year is lost in IP theft.

- **The Number of Years** – The limited number of years included in the data we examined are not enough to create a meaningful trend. Information security has only recently gained mainstream media attention.

We can be sure of one thing; the likelihood of a breach still exists. There is a significant amount of risk to your sensitive information and there is plenty of motivation for bad guys to use information for fraudulent gain. Again, our motivation for pointing out breaches is not to disparage the companies experiencing a breach or to scare people. We firmly believe that every breach presents lessons to be learned. As we look at the Top 10 Breaches of 2009, think about what could (or should) have prevented the breach, how the company could have handled the response better, and how these things could apply to you.

Without further adieu, let's examine the 10 largest breaches of 2009 and look at the lessons learned.

#10 – Astomos Energy

Stats

Address:

Tokyo, Japan

Announcement Date:

July 27th, 2009

Number of Records:

435,990

Victims:

Customers

Data Types:

Names, addresses, phone numbers, credit card details and other financial information

Reference:

[DataLoss DB](#)

[Nikkei Business Publications](#) (in Japanese, translated)



Breach Description

On July 27th, Astomos Energy Corporation announced the loss of a backup tape containing personal information belonging to 435,990 customers. The tape was allegedly lost by Astomos' data processing contractor CTC (ITOCHU Techno-Solutions Corporation) sometime between April 17th and July 15th. It is not known if the backup tape was encrypted, but it is assumed that it was not. According to Astomos, the risk of misuse is low because the magnetic tapes require "specialized equipment" to be read.

Lessons

1. Media and data-at-rest encryption.

We are assuming that the information on the lost backup tape was not encrypted. If it were, then it is likely that it would have been mentioned. This breach highlights a case for encrypting the information on backup media, and all sensitive data at rest on mobile media.

Sensitive data at rest should be encrypted, but how? It starts with policy; an encryption policy. The encryption policy states where encryption must be used, when it must be used and how it must be used (i.e. acceptable algorithms and key lengths). The policy grants enforceability and increases the likelihood of consistent application. We support our policy with implementation, processes, procedures, and regular auditing.

We could choose to encrypt all information at rest (i.e. on disk, on flash drives, on tape), but that could get expensive. Instead, we chose to encrypt *sensitive* data. In order to identify sensitive

The Top 10 Breaches of 2009

data we need to classify our data. Data classification is our answer, and again this starts with policy.

Don't think that a breach like this will happen in your company? It's only a matter of time.

2. Third-party security management

In this breach, we read about the involvement of a third-party data processing firm. Was the third-party liable too, and if so to what extent? Did Astomos assume that certain protections were in place that weren't?

If we share information with third-parties, we extend the domain of risk, liability and protection. We need to be assured that the third-parties we do business with protect our information in a manner that is consistent with our expectations and requirements. Poor third-party security management is a significant risk that we come across on a regular basis.

The solution to this risk is a formal third-party information security policy that outlines third-party security management. The policy outlines the requirements, and the procedures ensure compliance through due diligence, contractual language, and auditing.

3. Why mention "specialized equipment"?

Astomos stated that the risk of the misuse was low because the tapes require "specialized equipment" to be read. Really? This statement only increases our skepticism, and we would not recommend mentioning it. Only if the information was encrypted AND the encryption keys were not disclosed, do we consider the risk of disclosure to be low. What constitutes "specialized equipment" anyway? A tape drive, server, and off the shelf backup software? Probably.

#9 – Virginia Department of Health Professionals

Stats

Address:

Henrico, Virginia USA

Announcement Date:

June 2nd, 2009

Number of Records:

531,400

Victims:

Certain customers of Virginia pharmacies who use Social Security numbers as customer identifiers

Data Types:

Personally identifiable information including Social Security numbers

Reference:

[DataLoss DB](#)

[Virginia Department of Health Professionals breach notification letter](#)

[The Virginian-Pilot](#)



Virginia Department of
Health Professions

Breach Description

On June 3rd, the Virginia Department of Health Professionals released a breach notification:

"On April 30, 2009, DHP became aware that the Prescription Monitoring Program (PMP) computer system had been accessed by an unauthorized user. A criminal investigation is being pursued aggressively by federal and state law enforcement. Mandated by Virginia law, the PMP collects prescription information from pharmacies across the state for certain types of medications. This information is placed in a central database for use only by authorized users to assist in ensuring the appropriate use of prescription drugs. The PMP does not collect or maintain medical histories of patients.

You are receiving this letter because your social security number may have been contained in the PMP data furnished by the pharmacy where you filled your prescriptions. A small number of pharmacies have used social security numbers for customer identification and included the numbers in the pharmacy's report."

The Top 10 Breaches of 2009

A hacker gained access to the PMP database and demanded a \$10 million ransom. The records contained in the database include patient name, address and date of birth, the name and quantity of the drug prescribed, and identifying numbers for the doctor and pharmacist. There are more than 35 million prescription records contained in the database; however it was determined that only 531,400 are at risk of identity theft (i.e. has Social Security Numbers and identifiers).

Lessons

1. Time between incident and notification is long.

DHP became aware of the breach on April 30th, but did not notify until June 2nd. People expect a more expedited response, and organizations should be prepared to deliver. There could have been legitimate reasons for the delay such as a police investigation hold or an internal investigation hold, but the cause for delay should be made known to the victims. Otherwise we leave them thinking, and what they're thinking is probably not accurate.

2. Did DHP detect the attack or did they only become aware after the ransom demand?

The answer to this question is important because it highlights the level of detective control in this critical information processing environment. Could the attacker have gone undetected if he/she did not demand a ransom? If the organization did not detect this breach, it calls intrusion detection/prevention, logging processes (log levels, locations, and review), and file integrity into question.

3. Social Security numbers as customer identification numbers

Social Security numbers should never be used as customer identifiers, if at all possible. Social Security numbers are global in scale, meaning that a disclosure affects the victim in many ways and places. We need to assign a unique, organization-specific identifier whenever possible. The disclosure of a unique, organization-specific identification number affects only the victim/organization relationship.

#8 – Network Solutions

Stats

Address:

Herndon, Virginia USA

Announcement Date:

July 25th, 2009

Number of Records:

573,928

Victims:

Customers of Network Solutions merchants

Data Types:

Credit card account numbers, names and addresses

Reference:

[DataLoss DB](#)

[Network Solutions Data Security Alert](#)

[The Register](#)



Breach Description

On July 25th, Network Solutions announced the discovery of unauthorized software planted on some of their servers that are used to deliver e-commerce services to their merchants. The unauthorized software diverted transactions from 4,343 merchant websites to a rogue server outside of the control of Network Solutions. The software was on the server for almost three months before being discovered in “the ordinary course of business” by Network Solutions. In total it is believed that 573,928 accounts were affected.

From the Network Solutions Data Security Alert:

“In the ordinary course of business, Network Solutions identified unauthorized code on servers supporting some of our E-Commerce merchants’ websites. We promptly removed this code, and all of our E-Commerce servers are functioning properly. No servers supporting networksolutions.com were affected.

The Top 10 Breaches of 2009

After conducting an analysis with the assistance of outside experts, we determined that the unauthorized code may have been used to transfer data on certain transactions for approximately 4,343 of our more than 10,000 merchant websites to servers outside the company. On July 13, 2009, we were informed by our outside forensic experts that the data being transferred may have included credit card information. The code may have captured transaction data from approximately 573,928 cardholders for certain periods this spring. Exposure varied by merchant, but in all cases took place sometime between March 12, 2009 and June 8, 2009. Transactions after June 8, 2009 were not exposed to the unauthorized code. We have notified law enforcement and are working closely with them on the investigation. “

Network Solutions sent a letter to all of the affected merchants, most of whom are small businesses, but it is unknown if individual customers were ever notified.

Lessons

1. March 12th – June 8th is almost 3 months.

The fact that this unauthorized software was present on the system(s) from March 12th through June 8th is troubling. This breach should have been detected much earlier. Elevated privileges are required to place the software on the servers, and we can only speculate how someone or something gained this level of access. Why didn't network-based intrusion detection/prevention, host-based intrusion detection/prevention, file integrity, and/or logging systems detect this access early-on? We can only speculate.

2. Segmentation

When a single attack affects 4,323 web sites, we immediately question segmentation. Segmentation should be used to limit the effect and impact of an information security incident. Segmentation should be introduced based on the results of a thorough risk assessment and could be physical and/or logical (technical) in nature. There was a single point of failure or common vulnerability that led to this breach. We apply a concept called defense-in-depth to limit and/or avoid single points of failure.

#7 – Zurich Insurance

Stats

Address:

Zurich, Switzerland

Announcement Date:

October 22nd, 2009

Number of Records:

641,000

Victims:

Customers and former customers; “holders of Zurich Private Clients, Zurich Special Risks and Zurich Business Insurance Direct policies”

Data Types:

Insurance policy details

Reference:

[DataLoss DB](#)

[BBC News](#)

[The Register](#)

[Zurich Insurance plc](#)



Breach Description

In August 2008, a Zurich Insurance backup tape was lost in transit to a storage facility in South Africa. The tape contained sensitive policyholder information including insurance policy details.

From the Zurich breach announcement:

“The back-up tape was lost during a routine transfer within South Africa to a data storage centre in August 2008. The back-up tape also held details of customers and other parties in South Africa and Botswana.

The Top 10 Breaches of 2009

Zurich UK's investigation into the loss of the back-up tape has revealed deficiencies in the management of data tape security procedures in South Africa."

"Only holders of Zurich Private Clients, Zurich Special Risks and Zurich Business Insurance Direct policies are affected. We have written directly to all customers and former customers who are affected by this incident. These individuals should receive a letter and supporting documentation over the course of the next few days."

"Zurich UK has appointed KPMG to conduct a thorough investigation of this matter. KPMG will also be supporting Zurich UK to strengthen its data security procedures. At the same time, Zurich UK has taken steps to improve the security around the transportation of its data tapes."

Lessons

1. Media and data-at-rest encryption (see Astomos Energy breach, #10 above)

This is the 2nd breach concerning an unencrypted backup tape in our top 10.

2. The tape was lost in August 2008, but not reported until October 2009

August 2008 to October 2009 is 14 months! How does the organization account for this significant delay in notification? If the information has/had fallen into the wrong hands, how much fraud do you think could be done in 14 months? A lot! If we lose control of information, we certainly want to know about it much sooner, both from an organizational management perspective and a customer/victim perspective.

The company publicly admitted to deficiencies in their backup tape management processes. In our opinion, honesty and candor in a breach notification restores a certain level of confidence and trust.

3. Give more specifics about improvement

How does Zurich intend to "strengthen its data security procedures"? Would you want to know more specifics? We would.

#6 – Arkansas Department of Information Systems

Stats

Address:

Little Rock, Arkansas USA

Announcement Date:

February 20th, 2009

Number of Records:

807,000

Victims:

Current and former Arkansas citizens who had a background check conducted in the state.

Data Types:

Criminal background check information including names, addresses, dates of birth and Social Security numbers

Reference:

[DataLoss DB](#)

[Log Cabin Democrat](#)

[KATV Channel 7 News](#)



Breach Description

On February 20th, the Arkansas Department of Information Systems announced the loss of five backup tapes. The backup tapes were being stored at a third-party storage vendor, Information Vaulting Services (IVS). "Recently when we asked for a specific series of tapes, they were not able to recover one," said State Information Systems Director Claire Bailey. After conducting an inventory, the extent of the breach was discovered. The tapes contained background check information dating back to 1997, and an estimated 807,000 people may be affected.

The Top 10 Breaches of 2009

From news sources:

"Information Vaulting Services, discovered that five computer tapes were unaccounted for after a routine inventory last month."

"Recently when we asked for a specific series of tapes, they were not able to recover one," said State Information Systems Director Claire Bailey.'

'Records for 807,000 Arkansans over the past 12 years has been missing since the end of January. "Private information is on there like your social security number, your name, your date of birth, address information," Bailey explained.'

"DIS and IVS aren't sure what went wrong"

"The department discovered the tape was missing during a review and upgrade of their backup files at the Information Vaulting Services facility in Little Rock, according to Danny Palo, the chief operating officer of the data-storage company."

"I really, honestly, don't know what happened," Palo said. "Clearly there were some missteps between (Information Vaulting Services) and (the Department of Information Systems)."

"This is a very specialized backup tape, if you will. It's not something you and I can pop into our computer and read," said Danny Palo, chief operating officer of IVS.'

Lessons

1. Media and data-at-rest encryption

This is the 3rd breach concerning a lost or stolen unencrypted backup tape.

2. Do you need to keep 12 years of background check information?

This is a good question. People and organizations have a tendency to keep much more information than they need to. The more information we keep, the more information we need to secure. Over the years, organizations were more concerned about storage costs (disk, tape, etc.) than they were about the security of archived information. We do not know what the data retention requirements are for background check information for the State of Arkansas, but we do know that they should be defined and documented in a data retention policy.

Are you keeping more information than you need to? Do you know the ramifications of keeping information you don't need? Are you aware of e-Discovery rules? If you aren't sure about any one of these questions, it behooves you to seek legal guidance and work with the with the business units in your organization to get the answers you need. Once you have the answers, document them and incorporate them into a data retention policy.

3. Should you say you don't know what went wrong?

Danny Palo, the chief operating officer of the data-storage company involved in this breach stated "I really, honestly, don't know what happened." Is it a good idea to be this candid?

The primary purpose of a breach notification and other public disclosures is to give enough information to the affected entities so that they can make informed decisions about how to react. Another purpose is to restore confidence and trust. Restoring confidence and trust comes from ensuring that everything is under control and that steps will be taken to improve so that a similar breach will not be likely in the future. Part of restoring confidence and trust is being open and candid, but stating that we don't know what happened doesn't help.

4. How specialized is a "very specialized backup tape"?

Recall from the Astomos breach that "specialized" equipment is not an adequate control to ensure that data is safe from unauthorized disclosure. A very specialized tape literally just means that the tape was used for a singular purpose (or small number of purposes). Big deal.

The Top 10 Breaches of 2009

#5 – Oklahoma Department of Human Services

Stats**Address:**

Oklahoma City, Oklahoma USA

Announcement Date:

April 23rd, 2009

Number of Records:

1,000,000+

Victims:

Oklahoma's Human Services' clients

Data Types:

Personal information including names, Social Security numbers, birth dates, and home addresses

Reference:

[DataLoss DB](#)

[The Oklahoman](#)

[SC Magazine](#)

**Breach Description**

The Oklahoma Department of Human Services started to notify more than 1,000,000 state residents on April 23rd that their personal information was stored on a laptop that was stolen from an employee of the agency on April 3rd. The laptop was stolen from the employee's car when she made a stop on her way home from work. The laptop was not encrypted.

From news reports:

"The computer, which was stolen when a thief broke into the car April 3 after the employee stopped on her way home from work, was password protected, and officials do not believe the burglar realized what he or she was stealing. Therefore, the risk of the data being accessed is minimal, according to the agency."

"We feel this was not a situation where someone was targeting the agency or that information," DHS spokeswoman Mary Leaver told SCMagazineUS.com on Friday. "We feel it was random."

"The risk of the data being accessed is low because the computer uses a password-protected system," said Director Howard H. Hendrick. "Nevertheless, we have contacted our clients to inform them there is a possibility their personal information may be viewed."

Lessons**1. Laptop encryption**

Sensitive mobile data must be encrypted, period. Mobile devices are more susceptible to loss and theft. It seems like common sense then, that data stored on these devices is then more susceptible to loss or theft.

Mobile device and/or encryption policies should dictate encryption requirements for data stored on laptops. Laptop encryption has been around for years, and companies are using it to protection millions of laptops. The technology is main stream and so is its use.

2. Data permitted on mobile devices

Use a combination of administrative (policy, procedures, training, etc.) and technical controls to restrict the types and amounts of sensitive data permitted to be stored on mobile devices.

3. Password protection is not adequate

"The risk of the data being accessed is low because the computer uses a password-protected system"? Seriously?! So what! Password protection on a Windows system is bypassed in seconds.

The Top 10 Breaches of 2009

#4 – Mitsubishi UFJ Securities

Stats

Address:

Tokyo, Japan

Announcement Date:

April 8th, 2009

Number of Records:

1,486,651

Victims:

Customers

Data Types:

Names, addresses, places of work, phone numbers, annual incomes and other information on those opening new accounts

Reference:

[DataLoss DB](#)

[Mitsubishi UFJ Financial Group press release](#) (Japanese)

[Nikkei Business Publications](#) (Japanese)

[Okinawa HDR](#)



Mitsubishi UFJ Securities

Breach Description

A former middle manager at Mitsubishi UFJ Securities allegedly downloaded the company's entire customer database and copied it to a compact disc (CD) in February of this year. Furthermore, the 44-year-old is alleged to have sold 49,159 customer records to 13 other companies for 328,000 yen (~\$3,750 US). The list that was sold contained "names, addresses, places of work, phone numbers, annual incomes and other information on those opening new accounts or wrap accounts between Oct. 3, 2008, and Jan. 23, 2009." 11 of the 13 companies have agreed to not use the information.

From news reports:

The officials also said that the employee had been fired, and will be subject to a criminal complaint.

The data theft came to light after the company received a spate of reports of telemarketing calls from customers. An investigation of the eight people with access to the customer database led back to the man, who is heavily in debt with a consumer loan company.

The company now plans to add new security measures, including issuing one-time passwords and ensuring no-one uses the system alone."

Lessons

1. Insiders can be dangerous

People are the most significant risk to information security. This is mostly because human behavior is variable and difficult to predict in a number of situations. When inside employees have malicious intentions, the likelihood of compromise is almost certain. Prevention is difficult, so we turn to detective (logging and monitoring) and corrective (incident response) controls.

Every organization with responsibilities for securing sensitive information must have an incident response program. An incident response program consists of a policy, dedicated personnel, procedures, and testing.

Employee background checks at the time of hire and periodically thereafter can help, but the checks are historic and may not be a good indication of future behavior.

Could this breach have been prevented? Lesson #2 may help.

2. Segregation of duties

The lack of adequate segregation of duties may be the single most significant contributing factor to employee criminal activity (other than motive of course).

The Top 10 Breaches of 2009

Let's look at a couple of scenarios:

A small company has a single person who is responsible for purchasing (with the ability to create and approve requisitions) and accounts payable (with the ability to approve invoices, pay invoices, print checks, and sign checks). Is there a problem here?

How about a company that employs systems administrators who have the ability to create accounts, modify system settings, and modify (change and/delete) logs?

Companies may not have the means to employ a separate person for each function requiring segregation of duties. Cross-training can help. Get creative and insert check and balances into sensitive processes.

3. Removable media management

Should a person who has access to sensitive information be able to store the sensitive information on removable media? Removable media includes devices such as external hard drives (see our next breach in the top 10), compact discs, DVDs, and flash drives. We recommend a comprehensive risk assessment, which can be used to determine if the business case for using these devices outweighs the information security risks involved. If there is not a legitimate business case, disable their use. If there is a legitimate business case, look for mitigating administrative, physical and/or technical controls.

The use of removable media should be a topic covered in detail in policy and supporting procedures.

#3 – Health Net

Stats

Address:

Woodland Hills, California USA

Announcement Date:

November 19th, 2009

Number of Records:

1,500,000

Victims:

Customers

Data Types:

Names, Social Security numbers, and private medical information

Reference:

[DataLoss DB](#)

[Hartford Courant](#)

[Hartford Business Journal](#)



Health Net[®]
A Better Decision

Breach Description

An external hard drive belonging to Health Net was lost in May. The hard drive contained seven years worth of personal and medical information belonging to an estimated 1.5 million Health Net customers.

From news reports:

"A portable, external hard drive with Social Security numbers and medical records "disappeared" and is still missing from the insurer's Northeast headquarters in Shelton"

The hard drive contains Social Security numbers, medical records and health information dating to 2002 for 1.5 million customers — past and present — in Arizona, Connecticut, New Jersey and New York

"The data were compressed, but not encrypted. The information is formatted as images and requires a special computer program to be read, state and company officials said."

"Health Net's incomprehensible foot-dragging demonstrates shocking disregard for patients' financial security, as well as loss of their highly sensitive and confidential personal health information," Blumenthal (Connecticut State Attorney General Harlan Blumenthal) said in a prepared statement."

The Top 10 Breaches of 2009

Lessons**1. Removable media management**

Again? We will continue to preach proper removable media management. Does storing 1.5 million sensitive customer records on an unencrypted, portable, external hard drive seem a little risky? If not, we have a lot of work to do. If so, good, we probably have less work to do!

The risks in using removable media must be accounted for in an information security program.

2. Six month response

Six months is too long for a notification. People, the media, and obviously the Connecticut Attorney General expect better. Health Net claimed that it took six months for them to determine the type and amount of data that was on the external hard drive, but still, six months is entirely too long to conduct an investigation. The time between incident and notification may correlate directly to consumer confidence and trust.

We strongly suggest, build, and manage comprehensive incident management programs for our clients. When an organization is made aware of an incident, potential incident, or weakness, the organization must initiate a response immediately.

3. Compression and image format, huh?

"The data were compressed, but not encrypted. The information is formatted as images and requires a special computer program to be read, state and company officials said."

It's time for a sanity check. Does this statement offer you assurance and put your mind at ease, or does it make you feel a bit uneasy? Does this statement lead you to wonder if the company 1) is attempting to minimize the situation by leading people to believe that compression and formatting are sufficient controls, or 2) the company officials making the public statement don't know what they are talking about.

Data compression and format do little to protect the confidentiality of the information. OK, we are going to speculate a little and read between the lines.

Read the statement again, if you will. Formatted as images and compression? JPEG is compression used in a number of image formats. How about GIF or PNG? A vast majority of your image formats are compressed! The "special computer program" is what; an image rendering program like Microsoft Paint, Picture Manager or any number of thousands of programs?

#2, #4 all-time – National Archives and Records Administration

Stats**Address:**

College Park, Maryland USA

Announcement Date:

October 5th, 2009

Number of Records:

76,000,000

Victims:

Current and former U.S. military veterans

Data Types:

Private information including Social Security numbers

Reference:

[DataLoss DB](#)

[Wired.com](#)

[Dark Reading](#)



The Top 10 Breaches of 2009

Breach Description

Personnel at the National Archives and Records Administration sent a defective hard drive containing sensitive information belonging to 76,000,000 veterans to a contractor for repair without sanitization, increasing the risk of unauthorized disclosure. When the drive was deemed to be damaged beyond repair, the contractor GMRI sent the drive to another contractor for recycling.

From news reports:

"According to a report in Wired.com, the inspector general of the National Archives and Records Administration is investigating a potential data breach of a hard drive that helped power eVetRecs, the system veterans use to request copies of their health records and discharge papers."

"When the drive failed last November, the agency returned the drive to the contractor, GMRI, which sold it to them, for repair. GMRI determined it couldn't be fixed, and ultimately passed it to another firm to be recycled. But Hank Bellomy, a NARA IT manager who reported the incident to the inspector general, told Wired.com that the drive was not properly erased."

"This is the single largest release of personally identifiable information by the government ever," Bellomy told Wired.com. "When the USDA did the same thing, they provided credit monitoring for all their employees. We leaked 70 million records, and no one has heard a word of it."

"NARA says the lost drive is not a problem because its contractors signed privacy promises in their contracts. A spokesperson told Wired.com that the agency "does not believe that a breach of PII occurred," according to the report."

"The drive was part of a RAID array of six drives containing an Oracle database that held detailed records on 76 million veterans, including millions of Social Security numbers dating to 1972, the report says."

"Bellomy told Wired.com that when the unencrypted drive failed, he tried to subvert the longstanding recycling policy by hiding the drive in his safe. But it was taken out of his control when he was put on long-term leave, he said. He also said that more drives failed after the November incident, and that he performed a forensic scan on them to prove they were full of sensitive data."

"The Pentagon requires that old drives be degaussed (de-magnified) or physically destroyed. In a 2006 report still in effect, the National Institute of Standards and Technology recommended [purging and destruction methods](#) (.pdf), while OMB [rules](#) (.pdf) dating to the same year require that agencies follow those NIST standards and encrypt sensitive data being sent or stored remotely."

"NARA says that while it no longer will send back drives, no rules were broken, and that warning veterans would cause unnecessary fear."

"NARA does not believe that a breach of PII (personally identifiable information) occurred, and therefore does not believe that notification is necessary or appropriate at this time," NARA told Wired.com in an e-mailed [background paper](#) (pdf). "

"US-CERT, the nation's clearinghouse for data breaches and hacks, was notified in February by a NARA employee named Thomas Bennett, according to a [document](#) (.pdf) Bellomy provided to Wired.com."

Lessons

1. Media sanitization, reuse and destruction standards

Sending this drive to a third-party vendor without proper sanitization increases the risk of unauthorized information disclosure and fraudulent use. Anytime we send media anywhere outside of the organization or re-use media for another purpose, we must properly sanitize it.

What is proper sanitization? Sanitization can be achieved in a number of ways and must render the data stored on the media unusable. Sanitization can be achieved through physical destruction, degaussing, or overwriting. Proper sanitization is achieved when the work factor involved in re-constructing the data exceed the value of the data.

The Top 10 Breaches of 2009

The Nation Institute of Standards and Technology (NIST) has developed "[Guidelines for Media Sanitization](#)" for use by all federal agencies, and NARA is a federal agency. Why does NARA seem to think that they are exempt?

2. Signed contracts with "privacy promises"?

Does a signed contract with "privacy promises" alone ensure security of sensitive information? Not likely. Ensuring security in third-party arrangements is much more involved. At a minimum we need a policy to communicate security requirements, a documented risk assessment, and the right to audit. "I promise to keep your information private" is not enough.

3. Where's the news?

The amount of news coverage for this potential breach affecting 76,000,000 military veterans is surprisingly little. Perhaps it's because the NARA claims that there is no breach. Maybe they think a single drive from a RAID 5 array cannot be compromised. Do we need to have fraud and definitive proof of disclosure before we call an incident a breach?

#1, #1 all-time – Heartland Payment Systems

Stats

Address:

Princeton, New Jersey USA

Announcement Date:

January 20th, 2009

Number of Records:

130,000,000

Victim Profile:

Merchants and merchant customers

Data Types:

Credit and debit card numbers and corresponding card data

Reference:

[DataLoss DB](#)

[Heartland Payment Systems Press Releases](#)

[Storefront Backtalk](#)

[BankInfoSecurity](#)

[ComputerWeekly](#)

[Wired.com](#)

[Albert Gonzalez Indictment](#)

Breach Description

Starting as early as December 26th, 2007, Heartland Payment Systems suffered a series of successful SQL injection attacks by which an attacker placed malware onto the company's payment processing system. By the time the attack was stopped, it is believed that as many as 130,000,000 credit and debit card numbers were compromised.

In August 2009 Albert Gonzalez was indicted in Newark, New Jersey of hacking into the Heartland Payment Systems, Citibank-branded 7-Eleven ATM machines, and the Hannaford Brothers computer systems.

To date, this is the largest breach of credit card information in corporate history.

From news reports:

January 20, 2009 — Payments processor Heartland Payment Systems has learned it was the victim of a security breach within its processing system in 2008. Heartland believes the intrusion is contained.

"We found evidence of an intrusion last week and immediately notified federal law enforcement officials as well as the card brands," said Robert H.B. Baldwin, Jr., Heartland's president and chief financial officer. "We understand that this incident may be the result of a widespread global cyber fraud operation, and we are cooperating closely with the United States Secret Service and Department of Justice."

The Top 10 Breaches of 2009

After being alerted by Visa® and MasterCard® of suspicious activity surrounding processed card transactions, Heartland enlisted the help of several forensic auditors to conduct a thorough investigation into the matter. Last week, the investigation uncovered malicious software that compromised data that crossed Heartland's network.

Heartland immediately took a number of steps to further secure its systems. In addition, Heartland will implement a next-generation program designed to flag network anomalies in real-time and enable law enforcement to expeditiously apprehend cyber criminals.

Heartland has created a website — www.2008breach.com — to provide information about this incident and advises cardholders to examine their monthly statements closely and report any suspicious activity to their card issuers. Cardholders are not responsible for unauthorized fraudulent charges made by third parties.

January 28, 2009 - The sniffer malware that surreptitiously siphoned tons of payment card data from card processor Heartland Payment Systems hid in an unallocated portion of a server's disk. The malware, which was ultimately detected courtesy of a trail of temp files, was hidden so well that it eluded two different teams of forensic investigators brought in to find it after fraud alerts went off at both Visa and MasterCard, according to Heartland CFO Robert Baldwin.

Payment security experts pretty much agreed that hiding files in unallocated disk space is a fairly well-known tactic. But it requires such a high level of access—as well as the skill to manipulate the operating system—that is also indicates a very sophisticated attack. One of those security experts—who works for a very large U.S. retail chain and asked to have her name withheld—speculated that the complex nature of the hiding place, coupled with the relatively careless leaving of temp files, could suggest a less-skilled cyberthief who simply obtained some very powerful tools.

Baldwin also added more details to the sketchy timeframes that have been revealed thus far about the attacks, specifying that Heartland was contacted by Visa and MasterCard “in very late October,” possibly October 28. The card brands had been unable to find a common point of purchase with a series of bogus cards, so they started to look for a common point of processor, which took them to Heartland.

Heartland on Tuesday (Jan. 27) announced that it will be creating a new department that will be “dedicated exclusively to the development of end-to-end encryption.”

February 16, 2009 - Two Philadelphia law firms have filed class action suits on behalf of all cardholders in the U.S. who had their credit or debit card data stolen in the Heartland Payment System (HPY) data breach. This brings to three the total number of class action lawsuits filed against the Princeton, NJ-based payments processor.

The law firm of Berger & Montague filed a class action suit in the U.S. District Court for the District of New Jersey, alleging Heartland's failure to safeguard cardholder data when the company's computer systems were hacked and cardholder data was stolen. Heartland says last year it processed 100 million card transactions per month, but an unknown number of cards were impacted by the breach. The law firm says fraudulent activity has occurred on some of those cards.

The law firm alleges that Heartland's security measures and intrusion detection systems were inadequate. “Because of Heartland's inadequate data security, cardholders have had their card information compromised, have been exposed to the risk of fraud, have spent and will spend time to monitor their accounts and dispute fraudulent charges, and have suffered other economic damages,” the law firm says in its statement regarding the suit.

To date, there are more than 330 financial institutions that have come forward to say their customers' cards were compromised because of the breach.

August 17, 2009 - Albert “Segvec” Gonzalez has been indicted by a federal grand jury in New Jersey — along with two unnamed Russian conspirators — on charges of hacking into Heartland Payment Systems, the New Jersey-based card processing company, as well as Hannaford Brothers, 7-Eleven and two unnamed national retailers, according to the indictment unsealed Monday.

The Top 10 Breaches of 2009

Gonzalez, a former Secret Service informant, is already awaiting trial over his involvement in the TJX hack.

According to the court document, the hackers allegedly stole more than 130 million credit and debit card numbers from Heartland and Hannaford combined. Prosecutors say they believe these breaches constitute the largest data-breach and identity-theft case ever prosecuted in the United States.

According to the New Jersey indictment, Gonzalez, 28, and an uncharged conspirator identified only as "P.T.," allegedly found their targets on a list of Fortune 500 companies and then did reconnaissance to determine the payment-processing systems they used and uncover vulnerabilities. The hackers used computers they leased or controlled in California, Illinois and New Jersey as well as in Latvia, Ukraine and the Netherlands to store malware, launch their attacks against the networks, and receive the stolen numbers.



Using a SQL-injection attack, the hackers allegedly broke into the 7-Eleven network in August 2007, resulting in the theft of an undetermined amount of card data. They allegedly used the same kind of attack to infiltrate Hannaford Brothers in November 2007, which resulted in 4.2 million stolen debit and credit card numbers; and into Heartland on Dec. 26, 2007. Of the two unnamed national retailers mentioned in the affidavit, one was breached on Oct. 23, 2007, and the other sometime around January 2008.

Once on the networks, the hackers installed back doors to provide them with continued access at later dates. According to authorities, the hackers tested their malware against some 20 different antivirus programs to make sure they wouldn't be detected, and also programmed the malware to erase evidence from the hacked networks to avoid forensic detection.

Heartland reported in May that the breach had cost it \$12.6 million so far, which includes legal costs and fines from Visa and MasterCard, who say the company was not compliant with payment-card-industry rules.

Trustwave, a computer security firm, conducted its 2008 audit of Heartland on April 30 and deemed it compliant with Payment Card Industry Data Security Standards (PCI DSS). But shortly thereafter, the intruders began stealing batches of unencrypted card-track data from Heartland's network, and continued doing so for months before being discovered.

Lessons

1. This is one large breach!

A confirmed breach affecting as many as 130,000,000 credit and debit card numbers, and confirmed fraud is huge. This breach affects 38% more records than the next largest breach in history; 94,000,000 credit and debit card numbers stolen from TJX Companies.

Ironically, Albert Gonzalez has responsibility in both,

2. It's one thing to gain unauthorized access; it's another to do so undetected.

Unauthorized access was obtained to Heartland's systems in late 2007 and Heartland had no idea until being notified by Visa and MasterCard of fraudulent credit and/or debit card activity in late October, 2008. This means that the attack went undetected for 10 months, or more!

We don't know much about the alerting and monitoring systems in place at Heartland, but we wonder why this attack wasn't detected. Given the type of business and the sensitivity of the data within the environment, one would think that there would be a good mix of network-based intrusion detection/prevention, host-based intrusion detection/prevention, file integrity monitoring, extensive centralized logging, frequent audits, and dedicated highly-trained monitoring staff.

It is embarrassing to find out about something you are responsible from someone else.

3. PCI Compliance

"Trustwave, a computer security firm, conducted its 2008 audit of Heartland on April 30 and deemed it compliant with Payment Card Industry Data Security Standards (PCI DSS)." We have

The Top 10 Breaches of 2009

preached that good information security equals compliance, not the other way around for years. This means that organizations should manage their information security programs in accordance with risk, not in accordance with compliance (non-compliance is a risk also).

[PCI DSS](#) and compliance in general will NOT ensure that your data is adequately protected. It is a baseline only standard; a start if you will. The PCI DSS was updated in July, 2009 and is currently version 1.2.1. PCI DSS does not mandate encryption on internal networks and does not provide anything more than high-level requirements for monitoring/detection systems (See PCI DSS 11.4 and 12.9.5). Anyone who has designed, implemented, and/or managed an effective alerting and monitoring architecture knows how much it takes to do these things right.

Do not make the mistake of thinking that compliance and information security are synonymous.

Conclusions

It's easy to play Monday morning quarterback when looking at breaches, but the objective of this exercise is not to be critical of the organizations mentioned in this report. The objective of this white paper is to examine the breaches and look for lessons that we can use to reduce risk.

Four of the top 10 breaches were caused by lost or stolen media (backup tapes, hard drives, etc.); accounting for 3,383,990 sensitive records. The lost/stolen media consisted of three sets of lost backup tapes and one lost external hard drive.

Three of the top 10 breaches resulted from a remote compromise (sometimes referred to as a "hack") of organizational systems. These three breaches accounted for a total of 131,105,328 records, 130,000,000 of these records were compromised in a single breach (Heartland Payment Systems). SQL Injection was an attack type used in the Heartland Payment Systems breach, but we are not sure what type of attack was used in the others.

The remaining three breaches in our top ten resulted from a stolen laptop, a malicious insider, and a poorly sanitized hard drive. These three breaches accounted for a total of 78,486,651 records.

Well designed and implemented encryption for data-at-rest would have considerably reduced the likelihood of compromise in six of the top 10 breaches. A well designed and comprehensive alerting and monitoring architecture would have increased the likelihood of early detection in at least four of the top 10 breaches. In turn, early detection would have increased the likelihood that the number of records would have been significantly less.

The ten breaches outlined in The Top 10 Breaches of 2009 constitute a very small percentage of the total number of breaches that occur every year, both reported and unreported.

About FRSecure

FRSecure LLC is a full-service information security consulting company dedicated to information security education, awareness, application, and improvement. FRSecure works with businesses of all sizes, in all industries; enabling clients to achieve optimal results per every information security dollar spent. All of our clients are in business to make money, so we design secure solutions that drive business, protect sensitive information assets, and improve the bottom line.

Regulatory and industry compliance is built into our solutions. Our experience has shown that good information security equals compliance, not the other way around.

To read more about FRSecure, call us at 888.676.8657 or visit us online at <http://www.frsecure.com>.