



**Cyber risks troubling organisations
Supplementary Reading**

November 2017

Definition of Data Breaches

What is a Data Breach?

A data breach is an incident that involves the unauthorized or illegal viewing, access or retrieval of data by an individual, application or service. It is **a type of security breach specifically designed to steal and/or publish data to an unsecured or illegal location.**

How does a Data Breach occur?

A data breach occurs when **an unauthorized hacker or attacker accesses a secure database or repository.** Data breaches are typically geared toward logical or digital data and often conducted over the Internet or a network connection.

A data breach may result in data loss, including financial, personal and health information. A hacker may also use stolen data to impersonate himself to gain access to a high security area. For example, a hacker's data breach of a network administrator's login credentials can result in access of an entire network.

<https://www.techopedia.com/definition/13601/data-breach>
<http://www.channelnewsasia.com/news/business/ion-orchard-fined-s-15-000-over-customer-data-breach-9010072>

Business

ION Orchard fined S\$15,000 over customer data breach



ION Orchard. (File Photo: Calvin Oh)

SINGAPORE: The company that manages ION Orchard was on Thursday (Jul 6) fined S\$15,000 by the Personal Data Protection Commission (PDPC) over a breach involving the personal data of its customers.

In the incident, which took place on Dec 26, 2015, an unknown perpetrator used valid admin account credentials to log in to a server that held personal customer data.

66
99

"There was no evidence of hacking or that the perpetrator had deployed any brute force attacks," the PDPC said in its grounds of decision.

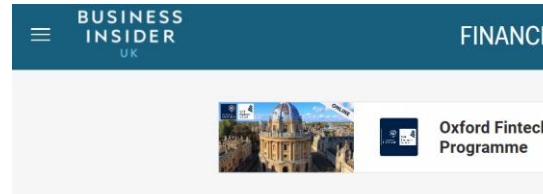
Combating Common Types of Data Breaches

Insider Leaks & Unintended Disclosure

Insider leaks can be a result of negligence or malicious intent. In order to prevent such a situation, it is vital to educate employees and establish policies with periodical compliance audits. This is to lower the risk of confidential information falling into the wrong hands.

Payment Card Fraud

Many cases of stolen credit card information have been reported over the year including the most recent Uber case. Some simple ways to avoid it happening to you include; shredding anything with your credit card number and personal identifiable information on it, avoid giving out your card information, review your billing statements every month and checking ATMs for card skimmers.



KPMG fired 6 people over 'unethical' leaks of confidential information



A fraud factory in a small apartment made 1,000 fake credit cards a day, feds say

November 08, 2017
Sowbug APT uses Felismus backdoor to for cyber-espionage operations

A previously unknown cyber-espionage group called Sowbug has been found using the Felismus backdoor to spy on several South American and Pacific Rim national governments for the last several years.

NOV 21, 2017 @ 10:43 PM 3,500
Hackers Linked To Dangerous Chinese Group Charged With Stealing 400GB Of Data From Siemens

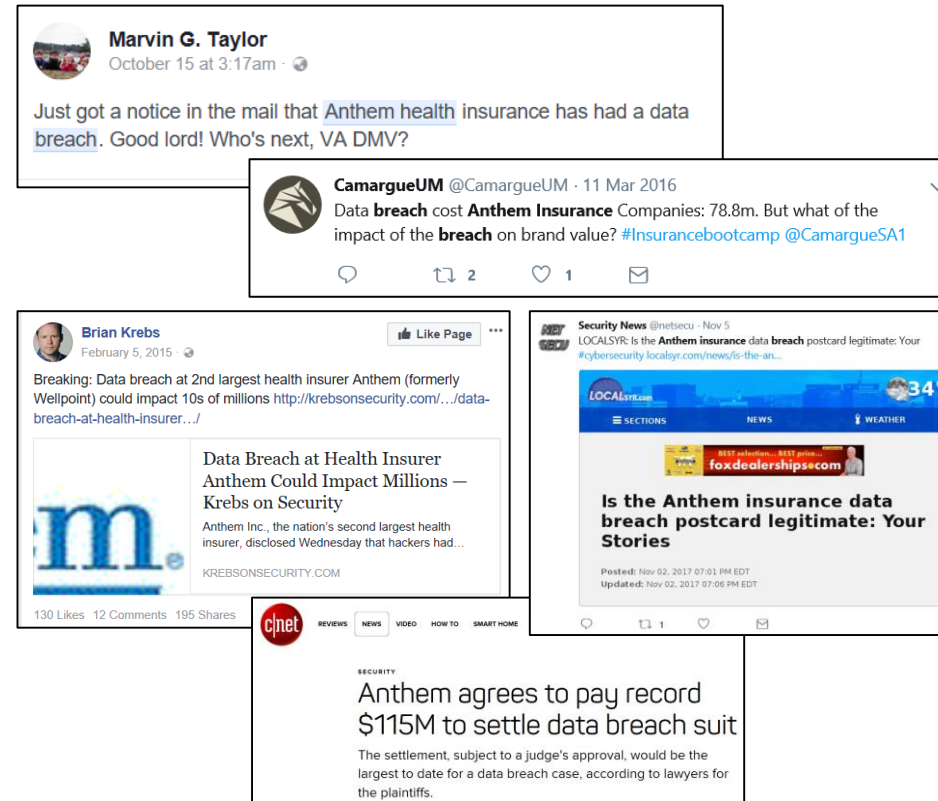
- <http://uk.businessinsider.com/kpmg-fires-6-people-over-unethical-leaks-of-audit-checks-2017-4/?IR=T>
- <https://iapp.org/news/a/2006-10-the-insider-threat-how-to-ensure-information-security-mitigate/>
- <http://www.miamiherald.com/news/local/community/miami-dade/hialeah/article186649473.html>
- <https://www.thebalance.com/ways-avoid-credit-card-fraud-960797>
- <https://www.scmagazineuk.com/sowbug-apt-uses-felismus-backdoor-to-for-cyber-espionage-operations/article/706098/>
- <https://www.forbes.com/sites/thomasbrewster/2017/11/27/chinese-hackers-accused-of-siemens-moodys-trimbles-hacks/#7133293819ef>

Case Study: Anthem pays \$115M to settle data breach

Information about the case:

- Anthem, US largest healthcare insurance company has agreed to settle a class action lawsuit over a 2015 data breach for \$115M
- The 2015 breach resulted in exposure and theft of nearly 80 millions records, including client names, date of birth, physical & email addresses
- Hackers used a stolen password and broke into Anthem's database using a customized malware containing information of former and current customers
- Customized malware is used to infiltrate Anthem's databases

News & information on Anthem which has gone viral online:



The collage includes several social media posts and news snippets:

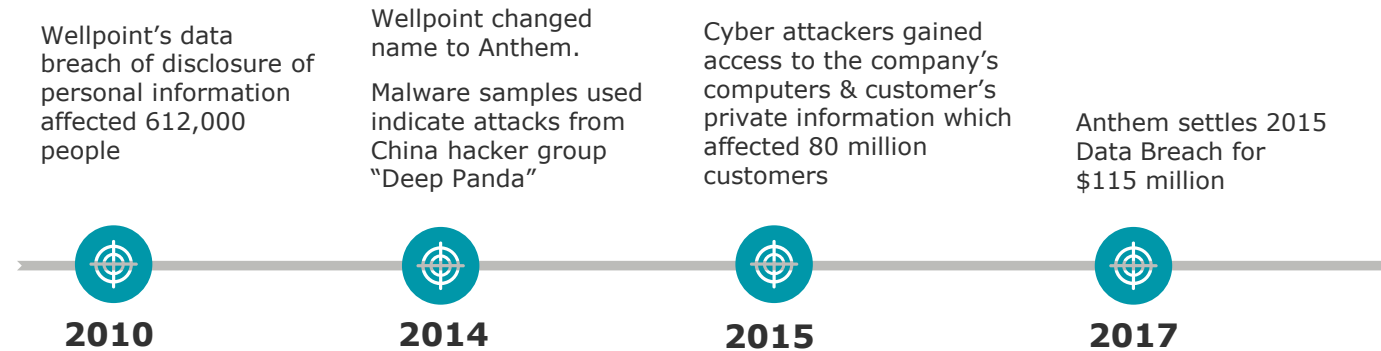
- Marvin G. Taylor** (October 15 at 3:17am): "Just got a notice in the mail that [Anthem health](#) insurance has had a data breach. Good lord! Who's next, VA DMV?"
- CamargueUM** (@CamargueUM · 11 Mar 2016): "Data breach cost **Anthem Insurance** Companies: 78.8m. But what of the impact of the **breach** on brand value? #Insurancebootcamp @CamargueSA1"
- Brian Krebs** (February 5, 2015): "Breaking: Data breach at 2nd largest health insurer Anthem (formerly Wellpoint) could impact 10s of millions http://krebsonsecurity.com/.../data-breach-at-health-insurer..."
- Security News** (@metsecu · Nov 9): "LOCAL51R: Is the **Anthem insurance data breach** postcard legitimate: Your #cybersecurity local51r.com/news/is-the-an-..."
- Security News** (Nov 02, 2017 07:01 PM EDT): "Is the Anthem insurance data breach postcard legitimate: Your Stories"
- cnet** (REVIEW NEWS VIDEO HOW TO SMART HOME): "SECURITY Anthem agrees to pay record \$115M to settle data breach suit. The settlement, subject to a judge's approval, would be the largest to date for a data breach case, according to lawyers for the plaintiffs."

66
99

"The Anthem breach and investigation afterward demonstrate how important it is for organizations to clean up and tighten the access control measures and the value of two factor authentication," says Mac Mcmillan, CEO of Security Consulting Firm - CynergisTek

<https://www.cnet.com/news/anthem-would-pay-record-115m-to-settle-data-breach-suit/>
<http://securityaffairs.co/wordpress/60464/data-breach/anthem-115m-settlement.html>
<https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627>

Case study: Anthem attack timeline



Conclusion:

Referring to the timeline, Anthem was breached more than once. There could be a probability that these cyber attacks are linked to one another.

Resolving a cyber attack requires a long time, even years of research and investigation. This is highly dependent on how malicious and severe the attack is.

The amount of time taken for Anthem to settle their legal costs, investigations and to salvage the loss of reputation due to the data breach took 7 years and they are still trying to settle the cost of the breach now.

<https://www.usatoday.com/story/tech/2015/02/05/anthem-health-care-computer-security-breach-fine-17-million/22931345/>
<https://www.bloomberg.com/news/articles/2017-06-23/anthem-reaches-115-mln-settlement-in-massive-data-breach-case>
<https://www.forbes.com/sites/brucejapsen/2014/12/03/wellpoint-name-change-to-anthem-official-reflects-brand/#7fd3424dcd54>

66
99

"The personally identifiable information that HIPAA-covered health plans maintain on enrollees and members — including names and Social Security Numbers — is protected under HIPAA, even if no specific diagnostic or treatment information is disclosed," said Rachel Seeger, a senior HHS adviser.

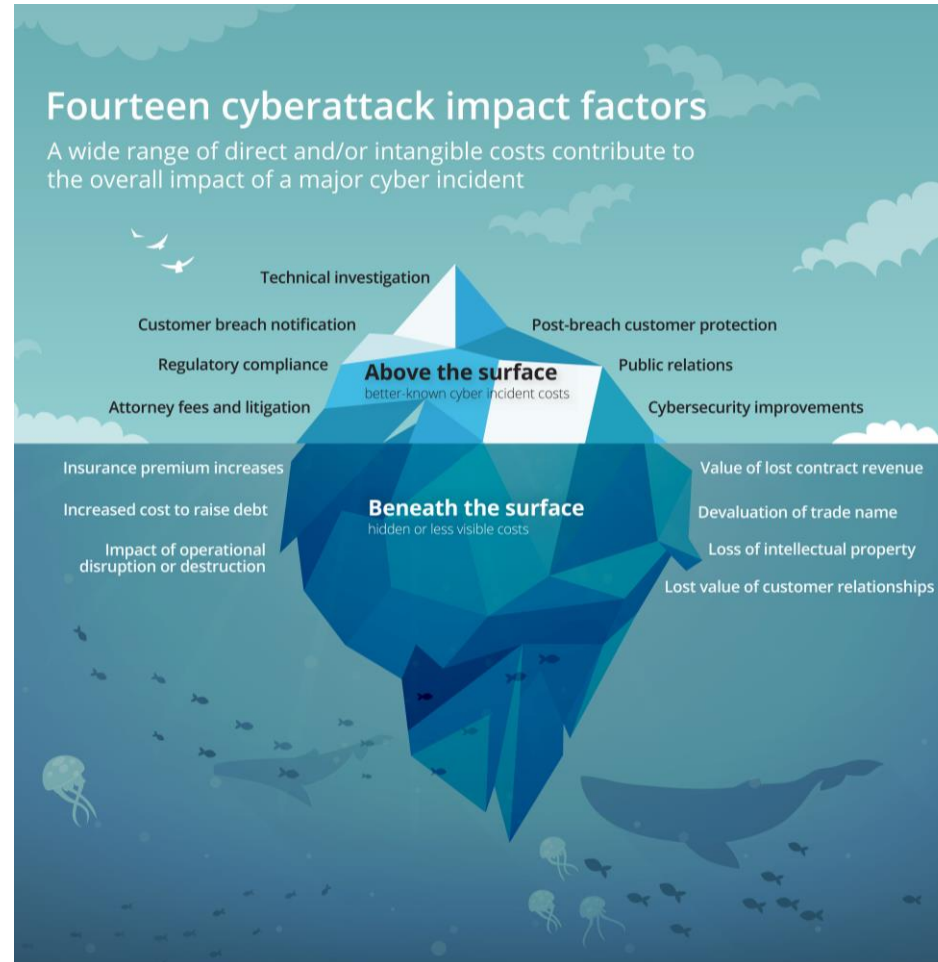
Lessons learnt: The Impact on Anthem

Impact on Anthem:

- Loss of customer relationships
- Loss of intellectual property
- Lost value of customer relationships
- Loss of reputation
- Loss of trust towards employees as the culprit misused company data
- Cost of Attorney Fees & Litigation
- Risk of cyber attackers disguising themselves as customers to make medical claims

Impact on customers:

- Risk of theft identity from cyber attackers, making claims from Anthem using their name
- Loss of trust towards Anthem
- Loss of personal confidential information



What to do after a Data Breach?

1) Determine what was stolen.

You'll need to pin down exactly what kind of information was lost in the data breach. Understand the severity of the breach and determine the kind of attack which has been executed.

2) Change all affected passwords.

If an online account has been compromised, change the password on that account right away. If you used the same password for any other accounts, change those as well, and make up a new, strong password for each and every account.

3) Contact relevant financial institutions.

If a payment-card number has been stolen, contact the bank or organization that issued the card immediately.

4) Check for IT systems failure.

Routinely assess vulnerabilities in your IT environment. Steps should be taken to find hidden sources, work down the layers of infrastructure to identify the servers and understand the network devices which your hardware and applications depend on and apply business and technology context to scanner results.

<https://www.tomsguide.com/us/data-breach-to-dos,news-18007.html>

<https://blog.barkly.com/data-breach-crisis-communication-plan-strategy>.

<https://www.classaction.com/data-breach/lawsuit/>

<http://focus.forsythe.com/articles/211/8-Steps-to-an-Effective-Vulnerability-Assessment>

<http://www.healthcareitnews.com/news/ponemon-business-continuity-management-vital-data-breach-recovery>

Healthcare IT News

Privacy & Security

Ponemon: Business continuity management vital for data breach recovery

Average cost per lost or stolen record is less for organizations employing BCM, group finds.

By [Bernie Monegain](#) | July 05, 2017 | 02:19 PM



An IBM-sponsored global study examining the impact of business continuity management on the cost of a data breach, concludes companies that use business continuity management and disaster recovery services recover more quickly than those who don't.

“Business continuity management continues to play an important role in determining the impact of data breaches that put organizations at risk worldwide,” Larry Ponemon, chairman and founder of the Ponemon Institute, said in a statement.

What to do after a Data Breach? Cont'd

5) Manage the crisis communication.

Have a unique strategy planned out for each crisis, the upper management should determine when should they communicate and admit the breach. Effective planning and execution of a data breach may help to salvage the situation. An organisation needs to admit the breach and then prepare for it.

6) Have an incident response plan.

A successful IR plan should involve people who take ownership and maintain the documentation. This will ensure a smooth transition from the planned initiative to business-as-usual. A basic incident response plan is akin to building a muscle memory. It requires the following:

- Internal team to follow and document the breach
- Identify external data security resources
- Create a checklist
- Track key breach-related rights, obligations & deadlines
- Review & update response plan regularly

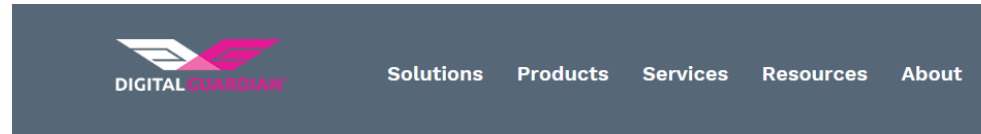
7) Determine whether legal action is necessary.

Only a licensed attorney will determine if an organisation is eligible for a data breach lawsuit. The attorney will also see if any state laws have been violated.

<https://www.classaction.com/data-breach/lawsuit/>

<https://digitalguardian.com/blog/incident-response-plan>

<http://fortune.com/2016/06/15/data-breach-cost-study-ibm/>



DATAINSIDER

Data Protection

Security News

CYBERSECURITY INCIDENT RESPONSE PLANNING: EXPERT TIPS, STEPS, TESTING & MORE

66
99

“Don’t be caught off guard when the next data breach affecting your firm comes to light. Be prepared.”says Caleb Barlow, Vice President at IBM Security

3 Ways to Prevent a Data Breach

1) Ensure that changes are documented

The **main key to visibility across the entire IT infrastructure is to keep a complete audit trail of system activities and changes made.** Remember that the human factor is always a pain point in security and consider thorough documentation of user activity as a solution to reduce the risk of employees' negligence.

2) Have an IT Security Framework.

This is a set of documented policies and procedures that govern the implementation and ongoing management of an organization's security. Think of it as a blueprint or operator's guide for security. Majority of the damage is usually caused by simple mistakes, such as unintended or unauthorized actions of legitimate users and IT engineers who are either untrained in security, and/or who misunderstood the instructions from the management.

3) Audit and evaluate your environment continuously

Auditing procedures are of little value if they are done only occasionally. **Continuous auditing of user activities and changes made to data and system configurations helps to avoid critical mistakes that might potentially damage security and service uptime.** Analytics built upon this knowledge helps to detect security incidents and find the root cause of each violation. In addition, continuous monitoring provides irrefutable proof that your security policies are in place and always have been), which is very handy when needing to pass compliance audits.

Prevent data breaches, don't just report them

Posted May 9, 2017 by [Jeff Kosseff \(@jkosseff\)](#)



Jeff Kosseff
CONTRIBUTOR

Jeff Kosseff is an assistant professor of cybersecurity law at the United States Naval Academy. The views expressed are only his,



Imagine if a state police department website listed every home burglary that occurred in the past decade. The website contains each home's address, the items stolen and a precise description of how the criminals broke in to each home.

https://www.netwrix.com/the_three_best_ways_to_prevent_a_data_breach.html
<https://techcrunch.com/2017/05/09/prevent-data-breaches-dont-just-report-them/>
<http://www.hypeorripe.com/2017/04/07/what-is-a-common-security-framework-csf/>
http://www.tns.com/it_security_framework.asp

66
99

The public data breach lists are a symptom of a deeper problem: U.S. cybersecurity laws place a disproportionate emphasis on notifying the public after a breach has occurred. While notice always will play a role in remediating harm, policymakers should shift their focus to preventative measures, such as more robust and clearer data security standards and incentives for investments in cybersecurity..



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte’s more than 244,000 professionals are committed to becoming the standard of excellence.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.