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.

---

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

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.

---

https://www.techopedia.com/definition/13601/data-breach
Combating Common Types of Data Breaches

Insider Leaks & Unintended Disclosure

Insider leaks can result from 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.

https://www.thebalance.com/ways-avoid-credit-card-fraud-960797
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:

http://securityaffairs.co/wordpress/60464/data-breach/anthem-115m-settlement.html
Case study: Anthem attack timeline

2010
Wellpoint's data breach of disclosure of personal information affected 612,000 people

2014
Wellpoint changed name to Anthem. Malware samples used indicate attacks from China hacker group "Deep Panda"

2015
Cyber attackers gained access to the company's computers & customer's private information which affected 80 million customers

2017
Anthem settles 2015 Data Breach for $115 million

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.forbes.com/sites/brucejapsen/2014/12/03/wellpoint-name-change-to-anthem-official-reflects-brand/#7fd3424dcd54
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.classaction.com/data-breach/lawsuit/
http://focus.forsythe.com/articles/211/8-Steps-to-an-Effective-Vulnerability-Assessment

“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
- Identity 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
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.

https://www.netwrix.com/the_three_best_ways_to_prevent_a_data_breach.html
http://www.tns.com/it_security_framework.asp
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.

© 2017. For information, contact Deloitte Touche Tohmatsu Limited