KPMG

cutting through complexity

DATA LOSS PREVENTION

PROTECTING YOUR DATA FROM ENEMY LINES

kpmg.com/cn

UNDERSTANDING THE ATTACK

DATA LOSS AT A GLANCE

This past year was a stark reminder that data breaches are still an ever-prevalent concern for consumers and businesses. Globally, there were over 2,000 incidents exposing 822 million records,[1] and this trend does not seem to be slowing down.[2] Over the past few months, there have been a number of high-profile data breach incidents involving large organisations (e.g. Korea Credit Bureau, Adobe and eBay). Despite the number of data breaches making the headlines, what we are seeing may only be the tip of the iceberg as most incidents involving data loss are not publicly disclosed.

Concerns over data loss are also evident in Hong Kong organisations. According to our recent Audit Committee Institute Survey,[3] many companies' management do not have visibility of their organisations' data.

50% **do not devote sufficient agenda time to data privacy and protection**

41% **are not satisfied with the information they receive on the risk and potential impact of data loss**

OVERVIEW OF DATA LOSS

WHAT data is commonly susceptible to theft?

- Personally Identifiable Information
- Transaction Data
- Intellectual Property

WHO are the common perpetrators of data loss?

WHERE are the common sources/channels of data loss?

- Email
- Webmail
- USB
- Mobile
- Cloud

WHY should you be concerned about data loss?

- Reputational Damage
- Regulatory Damage
- Financial Damage

HOW can you defend yourself against data loss?

- Staff Awareness
- Information Governance
- Mobile Device Management
- DLP Tools

DO NOT BECOME A VICTIM

Incident #1 – Data theft by an insider

Company
Korea Credit Bureau

Data lost
Personal data of 20 million bank and credit card users

Perpetrator
Employee – for financial gain

Aftermath
Financial loss, reputational damage and regulatory investigation

Incident #2 – Data theft by a hacker

Company
Large Hong Kong bank

Data lost
Confidential customer data residing with a business partner

Perpetrator
Hacker – for financial gain

Aftermath
Financial loss, reputational damage, regulatory action and impact to share price

Incident #3 – Accidental data loss by employee

Company
Stanford Federal Credit Union

Data lost
Personal data of over 18,000 people

Perpetrator
Employee accidentally emailed data to incorrect recipient

Aftermath
Reputational damage

[1] https://www.riskbasedsecurity.com/reports/2013-DataBreachQuickView.pdf
[2] https://www.riskbasedsecurity.com/2014/05/first-quarter-2014-exposes-176-million-records-troubling-trend-of-larger-more-severe-data-breaches-continues/
[3] https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/global-audit-committee-survey-2014.pdf

FORMULATING YOUR DEFENCE

ADDRESSING THE SERIOUS THREAT OF DATA LOSS

Companies cannot afford to take a reactive stance against data loss. Key considerations should be made to identify your level of risk exposure to data loss and what needs to be done to mitigate such risks. Based on our experience, we believe companies should take a holistic view and consider the three lines of defence – People, Process and Technology.

People – People are often the weakest link and the primary cause of data loss incidents. An employee unaware of the threats and measures against data loss can put your company at risk. Such an employee is more prone to accidental data loss (e.g. misplacing an unencrypted USB containing confidential data), and is more likely to become a victim of data theft (e.g. through social engineering and phishing attacks).

Have you considered the following?

- Do you know whether your employees are capable of identifying social engineering attacks[4]?
- Do your employees leave confidential data in public workspaces?

Process – Policies and procedures should be in place to address the handling of confidential data, from collection to destruction. From our experience, many companies underestimate the importance of inventorying their data. The best data loss prevention tools will not work if you do not understand your data.

Have you considered the following?

- Is there a clear classification of data based on audience type and level of confidentiality?
- Is there a mechanism in place to track data sources and owners?
- Does your organisation retain, disclose or maintain data in accordance with laws and regulations?

Technology – With the steep rise in the sophistication of attacks, technology – if implemented well – can offer peace of mind. Increasingly common trends such as Bring Your Own Device ("BYOD"), cloud computing and big data make it nearly impossible to track your data without automation. An effective Data Loss Prevention ("DLP") tool should help you monitor data at rest, data in motion and data stored in endpoint devices.

Have you considered the following?

- Do you have visibility on data egress (e.g. USBs, webmail, cloud sites)?
- Can your company detect and restrict confidential data from being emailed outside the company?

COMMON MISCONCEPTIONS ABOUT DATA LOSS

1. **Misconception:** The risk of data loss is minimal for my business, since we do not rely on external transmissions or outsourcing of confidential data.

   Reality: Data loss is relevant to organisations of any size, industry or market. Even without the external transmission of data, data can be compromised. In fact, most data breach incidents result from hackers targeting data stored on servers. All companies should assess their risk exposure to data loss and consider the appropriate mechanisms to protect their information assets accordingly.

2. **Misconception:** I have a data loss prevention tool that is sufficient to safeguard me against the risk of a data breach.

   Reality: Data loss cannot be solved by a set of tools. It requires an ongoing effort involving people, process and technology. In many cases, people are the primary cause of data loss, and while there may be tools in place to reduce the risk of accidental or deliberate data loss/theft, they are not foolproof and cannot make up for staff awareness.

3. **Misconception:** We are compliant with regulatory requirements and is therefore protected against data loss.

   Reality: While being compliant is essential, regulatory guidelines usually represent the minimum baseline for data security. This is evident as many victims of data breaches have been in some of the more highly regulated industries such as banking and healthcare. Furthermore, attacks are becoming more targeted and sophisticated to the point that compliance is not sufficient. A risk-based approach can help you identify areas of focus and raise your level of defence against data loss.

[4] The act of deceiving and / or manipulating people in order to obtain unauthorised access to confidential information.

WE CAN HELP

KPMG has an established approach to help our clients protect their data. We can start with a review of your environment to understand the current gaps and what can be done to strengthen your defence against data loss. A common difficulty among clients is conflicting viewpoints on data classification due to the wide spectrum of people providing input – business users, IT staff, compliance teams, etc. We can help you mediate between parties so that stakeholders have a clear and consistent understanding of the classification of their data.

Depending on your needs, we can help you reduce the risk of data loss through various changes in your People, Process and Technology. We can work with you to define a strategy for data loss prevention, from information classification and process alignment, to embedding a new workflow. We can deliver training and roll out staff awareness programmes to equip your staff with up-to-date knowledge of data security in the workplace. We also have extensive experience performing privacy impact assessments to ascertain whether personal and sensitive data is processed appropriately. Companies that are seeking technical solutions like DLP or BYOD solutions can make use of our solution strategy, vendor selection and implementation support services.

We have the knowledge and experience to help your organisation formulate and improve its defence against data loss.

For more details about information protection, data loss or KPMG's cyber security services, please visit us at www.kpmg.com/cn/information-protection or contact our Information Protection and Business Resilience team:

Henry Shek
Partner, Advisory
Information Protection and Business Resilience
T: +852 2143 8799
E: henry.shek@kpmg.com

Philip Ng
Partner, Advisory
Information Protection and Business Resilience
T: +86 (10) 8508 7093
E: philip.ng@kpmg.com

Reynold Liu
Partner, Advisory
Information Protection and Business Resilience
T: +86 (21) 2212 3626
E: reynold.jg.liu@kpmg.com

Kelvin Leung
Partner, Advisory
Information Protection and Business Resilience
T: +86 (755) 2547 3338
E: kelvin.oc.leung@kpmg.com

kpmg.com/cn