HANIF SHAMJI, MBA, CPA, CGA
CHARTERED PROFESSIONAL ACCOUNTANT
FINANCE BUSINESS PARTER -
OPERATIONS AND STRATEGY PROFESSIONAL

Data Analytics & Importance of Information Security – August 2, 2016

Importance of Information Security

From a financial and operational management, perspective the importance of information security cannot be downplayed. Information security should be part of the development of new data systems to ensure that the design of systems takes into consideration information integrity, breaches, and to provide adequate information audit trails are in place. It must be a fundamental part of an organisation procedures.

Information is an important factor in the valuation of a company. Consider information that is stored electronically such as application source code, designs, and plans. Also consider internal financial records of the enterprise, as well as confidential customer information. Examine the consequences to the bottom line of an organisation should a third party have access to some or all of the information.

Organizational Reputation

The reputation of an organisation as a trustworthy custodian of information could be at risk. In the private sector, customers could transfer their business towards competitors. In the public-sector pressure could see pressure placed on governing bodies otherwise see a loss in confidence in public sector organisations safeguard personal information.

Electronic Information as an Asset
Organizational Electronic information is an asset that an organisation use as part of business management, as well as provide new insight for future business operations. Just as an organisation protects its physical asset so to should it protect the electronic asset it processes. The importance of information security should not be downplayed due to the fact it is electronic. At times, we have noted organisations downplay the importance of information security, temporary modify their behaviour after a security breach and return to the ordinary course of business once such breaches are forgotten.

In recent years, we have noted information security breaches that result from various sources including lack of training or proper internal control, or from external sources. Lack of internal control could include ensuring that information is properly encrypted on medium when stored, proper password protection, ensuring users have appropriate access to information systems. Increasing security awareness within the organisation is ever increasingly important.

Information Security Policy and Procedures
Information Security involves developing and maintaining policies and procedures to identify threads, contain risk, and investigate risk, detect and establish procedures to reduce or eliminate threats. A holistic approach involves an evaluation of not only information system architecture, but where and how information is stored, risks related to data storage, as well as user perspective associated with those who access the information both internal and external to the organisation.

Organizations may have policies and procedures that are in place related to information security, but the question is, are these understood and adhered? As well organisations must determine actions if these policies and procedures are breached. Information security threats from external sources also require an evaluation of the effectiveness of technology infrastructure including disaster recovery, and critical core business continuity. Reducing the overall inherent risk resulting from lack of adherence to policies and procedures has an impact on the overall security of an organisation.

Approaches towards Information Security
Three common approaches to information security include: reactive, proactive, and predictive.

- Reactive Approach: This approach based on information breaches that are responding to incidents that already have occurred such as loss of customer, or private client information. Such occurrences can affect the reputation of an organisation in the delivery of their services. If the breach is large enough, it can impact the short term, and perhaps the long-term effects on the bottom line profitability of an organisation. In the case of a not-for-profit organisation, it could affect funding, or see the responsibilities of the organisation transferred.

- Proactive Approach: This approach identifies a risk assessment of organisational policies and procedures. From a user, perspective this can include assessing if proper internal controls are in place, understood, followed by the end user and ensuring passwords not taped on a desk or computer, logging access to sensitive information systems such as healthcare, or financial reporting. It also includes ensuring users only access to information that is required to undertake their tasks. From an Information Technology, perspective this can include ensuring that proper security patches for operating systems, applications are in place, appropriate firewalls, and antivirus applications are in place. Network activity both from internal sources, and external sources should be monitored; any suspicious activity suspended until identified.

- Predictive Approach: Based on predicting future vulnerabilities and threats based on an evaluation of risk analytics, strategy, information, and technology infrastructure. An assessment of the system on an architectural system level to take a proactive

approach to reduce from attacks due to the inherent risk resulting from inadequate system design. The predictive approach will also need to consider reducing threats that may occur from internal sources within the organisation related to access to information.

Considerations include a determination if an information attack can occur in the future both from internal, and external sources and what steps need to be taken in order to ensure strong internal controls are in place. Compensating controls may also be used in conjunction with effective internal information security controls.

Information Security and Big Data Analytics

With the increasing reliance on "Big Data Analytics," the use of information from various people in the organisation will continue to improve. Safeguards including the level of information that is required to undertake some of these strategic analytics that is necessary for a team to maintain its competitive advantage is needed. The use of "data views" to provide such level of information required for analytics without compromising individual or targeted information. An evaluation of the type information that is needed by people should be undertaken to reduce data breaches or compromise security therein.

User authentication accessing of information systems in a variety of ways through traditional user authentication, as well as the use of monitoring information systems for unusual activity. The increased use of real-time analytics across multiple data-points will no doubt improve the quality of information but also increase the threat of compromised information.

Sophisticated Network Topology should not be a reason to ignore Information Security
From an information security, perspective even firms that have implemented an advanced network security topology could still see small information security data-points that leave an organisation vulnerable to:

- Discovery of incomplete data-points – that is information stored on external peripherals that cannot be monitored or maintained by information security team.
- Lack of procedures to deal with information from various data-points, integration, and integration including the linkage of internal organisational data sets to those external to the organisation both ongoing as well as ad-hoc data-points.

Importance of procedural changes to meet Information Security Concerns
Consider the importance of a change management plan both within the Information Security Department as well as other units within the organisation.

- Staff awareness related to the importance of information security.
- Individual responsibility towards fulfilling information security policies and procedures.
- Change routine habits both paper and electronic to promote stronger information security controls.
- Evaluate information risk levels and impact to the organisation, where applicable departmental procedures may need to be modified to reduce information risk to an acceptable inherent risk tolerance level.

- Users are installing software that allows third parties access organisational systems through their account; this can include clicking on a link that appears to be from a friend or co-worker more likely to be opened.

Information Technology Procedures Overview to reduce network-based information security threats.

1. Ensure Operating system, and applications are up-to-date otherwise, organisations could be vulnerable to attacks via breaches in applications.
2. Adequate understanding of network-based attacks, as well as physical loss of data and equipment therein.
3. Lack of IT Network security policies or policies
4. Lack of understanding of the importance of security policies which can include IT Network staff circumventing security procedures as a quick fix to solve user problems and a lack of a consistent policy can cause damage to an organisations information systems.
5. Lack of any information security training or updated training based on best practices within the industry.

Benefits of an Information Security Policy

The benefits from a well-founded information security policy include

- Reduction in financial loss steaming from incident beaches
- Adherence to statutory compliance
- Protection of intellectual property
- Business continuity resulting from natural disasters

Conclusion

With increased reliance on big-data analytics for organisational strategy, as well as some information organisations store electronically that is of a sensitive nature to various stakeholders the importance of an Information Security policy will no doubt increase.

The reliance of electronic information will only increase thus leading to the need to address safe storage of information. The benefits of storing information can be leveraged for an organisation's benefit for better operations management if undertaken in a manner that addresses not only the strategic benefits but any potential risk.

With the increasing reliance on big-data analytics including accessing information from various data-points both internal and external to the organisation the need for a proper information security protocol will only increase. The need for organisations to be proactive rather than reactive will only increase. The safeguarding of information is not only the responsibility of one department but everyone in the organisation.

About the author:

Hanif Shamji, MBA, CPA, CGA is a Finance Business Partner / Sr. Financial Analyst with an information technology background, experienced in several industries.

Contact: info@hanifshamji.ca

http://www.hanifshamji.ca/