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

Information Security – Financial & Internal Control Considerations – June 16, 2015

With the importance of the usage and storage of electronic information, security concerns cannot be underestimated. Organizations have realised the importance of protecting competitive information, the privacy of their clients as well as ensure that the regulatory, and legislative requirements. An investment into information security is necessary to assist in maintaining confidentially, and integrity of information within the organisation.

Transmission of Electronic Information

Electronic mail transmission is used widely by people to transmit information. Many people do not do enough to ensure such information is secure. While a basic password security is a minimum, the transmission of secure documents may require the use of digitally encrypted email or the use of a secure site to retrieve and send information.

Consider the inherent nature of email which was not designed with security in mind. Messages can potentially be intercepted without the knowledge of the sender or receiver. As well an unknowing recipient could click on a file that is a Trojan that may allow a third party to gain access to organisational, informational systems which may go undetected. Digital signatures can be used to verify the recipient and encryption protocols to transmit emails securely. The use of secure sites may also need to be considered to transmit information more securely. As well discuss security-related issues from the use of Public Wi-Fi systems which can lead to transmission of information open to others within the network. The use of a VPN (Virtual Private Network) connection can add an extra layer of security when accessing information of a sensitive nature from a public Wi-Fi network.

Quantifying Investments in Information Security

Information security has become increasingly important especially with the use of various devices that allow information to be accessed remotely. Traditional financial ratios that are used to measure projects and investments such as Return on Investment (ROI), Net Present Value (NPV), Payback cannot be used to adequately measure the

importance and the return from investing in information security. Considerations such as the consequences of not investing in security projects need to be quantified using alternative means including risk data and the effects both related to privacy, competitive information, as well as legislative requirements. Data to predict the statistical probability of information risk may not be sufficient given the broad scope of factors that need to be considered that is not limited to internal and external risk.

The cost savings realised by the undertaking such projects cannot be readily determined. We may attribute investment in security infrastructure based on the probability, and potential impact of such events is occurring. The exposure loss cannot be determined as it would depend on the nature of the data breach. Although a potential dollar value impact of an organisation's data exposed can be determined, the loss of goodwill to an organisation as well as legislative requirements will also have an impact.
Organizations should adopt at least the same level of control and care as similar organisations in the industry that it operates. Measurements such as the degree of information security personal compared to organisations in related industries, size, and their effectiveness can be measured. Such measurements can be used to determine if organisations are addressing this important issue with due care, and due diligence. The ranking of information security based projects based on the standard of care, risk and statutory requirements.
Organizations have faced losses due to cybercrime; we may not always hear about such activity such events we need to consider the financial and legal consequences for organisations. The role of finance has morphed from reporting and analysing financial information, to also include compliance. Such compliance requires partnering with a security specialist to determine risk evaluation as part of the review of the internal controls framework.
Information Security is an integral component of an organisation's core activities.

Internal Control Measures for Information Security
A well-established framework for internal controls has a similar foundation to the concerns of an internal or external auditor. Internal checks and ensuring the protection of information is not limited to financial reporting and physical assets, but also information systems. As part of an Internal Controls framework, the following are important factors:

Risk Assessment - identify the areas with the highest threat of risk only limited to dollar amounts but information and the impact of such information. Internal threats can include employees not following policies, and procedures, as well as possible fraud. The various potential threats documented with a risk assessment.

Information and Communication - roles, responsibilities and a well-documented plan for functions and responsibilities related to internal controls are essential

Control Environment - is established by assessing commitment to the framework which includes due diligence in the design of monitoring systems, the assessing of discrepancies, as well as integrity. The encryption of confidential information is essential to prevent unauthorised access, restricting access to electronic information such as through the segregation of duties as well as dual controls, as well as educating staff on appropriate checks and procedures.

Monitoring and Reviewing - a review control measures should be monitored on a periodic basis to ensure that it was functioning as intended, as well as to determine if such measures should be updated based on changes to the operating environment
Control Activities - these include procedures to prevent or detect breaches to the internal control environment

Big Data Analytics and Compliance of Information Security

Consider how the use of Big Data Analytics to identify information that can be used to ensure the integrity of data, detect the probability of fraudulent transaction, track access and usage to organisational systems. The use of data analytics to assist in the prevention of future information breaches will continue to be a significant concern. Information Security is increasingly moving from being a technical issue to an organisational concern. Compliance includes ensuring an appropriate level of internal controls.

The compliance of information security is not limited to verifying and testing of organisational privacy policies and procedures, ensure compliance with legislative requirements, ensure procedures are in place to identify, monitor, and take corrective action regarding information security. Meeting current regulatory compliance may not be enough. Compliance does not exclusively rest with the Information Privacy Department but as information technology increases, as well as the need to ensure legal compliance this department may take the lead. Consider the financial impact the organisation if the information is not secure, which could include legislative penalties, as well as regarding goodwill.

As noted the benefits of investing in information security may not always be visible, but evaluated regarding what the impact would be if such an investment did not take place and manage concerns face organisations in light of our increased dependence on technology.

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/