Five best practices for information security governance

Over 169 million personal records were exposed in 2015, from more than 700 publicised breaches across the financial, business, education, government and healthcare sectors.

INTRODUCTION

Data is everywhere—on mobile devices, in the cloud, in transit. The accumulation of data and the rise of businesses using data to better hone their practices are rapidly evolving as data increasingly comes from various platforms and in different forms. Data growth, new technologies and evolving cyberthreats create challenges for organisations looking to set strategies, frameworks and policies for keeping all of that information secure.

Threats are increasingly common and rapidly evolving as criminals discover new ways to circumvent defences and target valuable data. Over 169 million personal records were exposed in 2015, from more than 700 publicised breaches across the financial, business, education, government and healthcare sectors, according to the ITRC Data Breach Report[1].

The IT Governance Institute[2] defines information security governance as 'a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organisational resources responsibly, and monitors the success or failure of the enterprise security program.'

Overall, information security governance requires an organisational structure, the assigning of roles and responsibilities, and defined measurements and tasks—all strategically developed and defined by the board of directors and executive management.

Diligent

'How does a company most effectively deploy its resources to mitigate cybersecurity risks to an acceptable level?' asks a piece in *Bloomberg Government* magazine[3]. That's a question that only board-level decision-makers can answer.

This paper aims to provide best practices and guidelines to successfully implement strategic information security governance, including answering the following questions:

- How is information security governance defined?
- What are the misconceptions about information security governance?
- Why is information security governance important?
- Who is responsible for information security governance?

WHAT INFORMATION SECURITY GOVERNANCE IS NOT

Information security governance should not be confused with IT management, which is primarily concerned with making tactical decisions to mitigate security risks.

Think of governance as determining who is authorised to make and responsible for making these security-related decisions. It is not the implementation of the policy, but the oversight and creation of the program. It is not the enforcing of the policy (this is IT management's charter), but the enactment of the security policy. In short, information security governance focuses on the strategic, not the tactical.

WHY IS INFORMATION SECURITY GOVERNANCE IMPORTANT?

Information security governance aims to establish strategic measures in order to protect an organisation's information, which can comprise highly sensitive data and information: financial, legal, customer, partner, research and development, proprietary information and more. Organisations are holding more and more data that could be valuable to competitors—or worse, criminals.

In recent years, cybercriminals have made headlines with high-profile hacks and data breaches. From the Sony Pictures Entertainment hack, where criminals stole an estimated 100 terabytes of sensitive data[4], to the Anthem medical data breach[5], all industries are vulnerable to an attack. A data breach can have damaging effects that endure long after the incident: legal liabilities, damage to brand reputation, lack of trust from customers and partners, and associated revenue decreases. According to a 2016 Ponemon study[6], the average cost of a data breach is $4 million (AU$5.1 million approx.).

Strategic information security governance is vital for all organisations in order to assure their customers, partners and employees that they are working with a secure company. As corporate data becomes more accessible to employees via mobile devices and the cloud, it is important for companies to keep up with security practices to ensure that the right employees have access to that data. And, of course, to make sure that criminals don't have access to sensitive data.

WHO IS RESPONSIBLE FOR DEVELOPING INFORMATION SECURITY GOVERNANCE?

While security should be a concern for all teams and employees, leadership is responsible for establishing and maintaining a framework for information security governance. Whether it is the board of directors, executive management or a steering committee—or all of these—information security governance requires strategic planning and decision making.

TOP FIVE BEST PRACTICES FOR INFORMATION SECURITY GOVERNANCE

What follows are strategic solutions to better position an organisation for successful security governance:

1. Take a holistic approach to strategy: Before implementing information security governance, you should take a unified view of how security impacts your organisation. A company-wide survey can help to scope out which data needs to be protected. This can also help get early buy-in from key stakeholders.

Questions to address include the following:

- Which data needs to be protected?
- Where are the risks?
- What strategic policies should be created?

- Which teams should be responsible for carrying out these policies?

Security strategy is also about aligning and connecting with business and IT objectives. You should get input from all stakeholders across the organisation—from the IT, sales, marketing, operations and legal departments—to understand their concerns and challenges, as well as to assess their skills and expertise.

Avoid cookie-cutter solutions and working in silos, which may create more obstacles and fragmented, disparate security solutions. A holistic approach ensures that leadership—the creators of information security governance—gain more control and visibility.

2. Create awareness and provide training throughout the organisation: Establishing information security governance and then walking away can bring negative results, such as a lack of adoption, a misunderstanding of policies, roles and responsibilities, and security vulnerabilities. Ensuring continuous adherence to security governance requires awareness, education and training on the part of all involved.

Security is not just a concern for IT. It's everybody's responsibility.

- Are your employees bringing their own devices to work?
- Are they using approved apps?
- What are their attitudes towards handling the company's sensitive data?

Frequent company-wide surveys, security seminars and education on security best practices are all possible ways of keeping security top of mind for all employees.

Although it's developed by the board of directors, executive management and steering committees, information security governance is a matter for all employees in the organisation. While governance creates policies and assigns accountabilities, each member is responsible for following the security standards.

Awareness, training and education in relation to security best practices must be continued. For example, organisations could send selected team members to security training conferences to learn about the latest industry techniques. These individuals can then share their new-found knowledge and insights with the wider organisation.

3. Monitor and measure: Information security governance requires constant assessment and measuring.

- Which policies are working?
- Which policies are not?
- Which teams or individuals are not following the security policies?
- Is the number of security incidents impacting the company's reputation with customers and partners?

Measuring the performance of information security governance efforts ensures that objectives are being achieved and resources are appropriately managed.

- How often do you test your security measures?
- How often do data breaches occur?
- What is the response time for incidents?
- Which security policies are working and which ones are not?

For example, an organisation might stage mock data-breach scenarios to see how well its teams hold up. The results can showcase what a company needs to work on, and what it has nailed down.

4. Foster open communication between all stakeholders: It's vital that all stakeholders feel that they can communicate directly with leadership. Working in silos risks obfuscating important communication that relates to security governance.

If a data breach occurs, do employees at any level of the organisation feel comfortable enough to let leadership know? Or will they attempt to shield any negative news from the top?

Open communication promotes trust while augmenting visibility throughout the organisation. To further enhance engagement, consider creating a steering committee comprising executive management and key team leads with the goal of reviewing and assessing current security risks. Members might include team leads from the IT, finance, PR, marketing, legal and operations departments. Regular steering committee meetings can ensure ongoing adherence to the security policies. For example, if a new security policy is created, department leads sitting on the steering committee can make sure that their teams implement the policy.

5. Promote agility and adaptability: The digital landscape is rapidly evolving as new platforms impact the way we do business. Your information security governance plan, while establishing solid policies and guidelines, must be open to adaptation. An organisation should monitor and measure the overall strength of its security policies. Questions to ask include the following:

- What's working?
- What's not working?
- What can we change?

For example, an employee in the IT security trenches may have the necessary hands-on experience and insights to assess the effectiveness of a particular security policy. If leadership is receptive to hearing the team member's feedback and suggestions, it should also be agile in terms of making those changes.

CONCLUSION

Successful information security governance doesn't come overnight; it's a continuous process of learning, revising and adapting. While every company may have specific needs, securing the data they hold is a common goal for all organisations. Emerging technologies and cyberthreats will continue to evolve. Data breaches and security incidents will happen. Rather than scrambling to react after a security breach occurs, organisations must put proactive and strategic information security governance at the forefront. The goal for all companies should be to deliver information security and to reduce adverse impacts and risks to an acceptable level. Threats and incidents will occur, but with a strategic information security governance plan in place, you will strengthen your organisation's security posture while protecting your valuable information.

SOURCES:

1. 'Data Breach Reports', ITRC, 29 December 2015, http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf
2. 'Information Security Governance: Guidance for Boards of Directors and Executive Management', 2nd edition, IT Governance Institute, 2006, http://www.isaca.org/knowledge-center/research/documents/information-security-govenance-for-board-of-directors-and-executive-management_res_eng_0510.pdf
3. 'Why cyber is a boardroom issue,' Tom Skypek, 21 April 2016. Bloomberg Government, http://about.bgov.com/blog/why-cyber-is-a-boardroom-issue/
4. 'The Sony Hackers Still Have A Massive Amount of Data That Hasn't Been Leaked Yet,' Business Insider, James Cook, 16 December 2014, http://www.businessinsider.com/the-sony-hackers-still-have-a-massive-amount-of- data-that-hasnt-been-leaked-yet-2014-12
5. 'Insurance Giant Anthem Hit by Massive Data Breach,' CNN Money, Charles Riley, 4 February 2015, http://money.cnn.com/2015/02/04/technology/anthem- insurance-hack-data-security/
6. '2016 Cost of Data Breach Study,' 2016 Ponemon Study, http://www- 03.ibm.com/security/data-breach/

Information security governance establishes strategic measures to protect an organisation's information.

Call: 1 800 106 454
Email: info@diligent.com
Visit: diligent.com/au