Five Best Practices for Information Security Governance

Over 169 million personal records were exposed in 2015, from more than 700 publicized 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 comes from various platforms and in different forms. Data growth, new technologies and evolving cyber threats create challenges for organizations looking to set the strategies, framework and policies for keeping all of that information secure.

Threats are increasing and rapidly evolving as criminals discover new ways to circumvent defenses and target valuable data. Over 169 million personal records were exposed in 2015, from more than 700 publicized breaches across the financial, business, education, government and healthcare sectors, according to 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 objectives are achieved, manages risk and uses organizational resources responsibility, and monitors the success or failure of the enterprise security program.”

Overall, Information Security Governance requires organizational 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 decisions-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 authorized 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 (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 set strategic measures to protect an organization's information, which can be comprised of highly sensitive data and information: financial, legal, customer, partner, research and development, proprietary information and more. Organizations are holding more and more data that could be valuable to competitors, or worse, criminals.

In recent years, cyber criminals 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 even 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.

Strategic Information Security Governance is vital for all organizations 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 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 organization for successful security governance:

1. Take a holistic approach to strategy: Before implementing Information Security Governance, take a unified view of how security impacts your organization. A company-wide survey can help scope out what data needs to be protected. This can also help get early buy-in from key stakeholders.

Questions to address include:

- What 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. Get input from all stakeholders across the organization — 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 leadership — the creators of Information Security Governance — gain more levels of control and visibility.

2. Create awareness and training throughout the organization: Setting Information Security Governance and then walking away can bring negative results, such as a lack of adoption, misunderstanding of policies, roles and responsibilities, and security vulnerabilities. Continuous adherence to security governance requires awareness, education and training for 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 toward handling the company's sensitive data?

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

Although developed by the board of directors, executive management and steering committees, Information Security Governance is for all employees in the organization. Governance creates policies and assigns accountabilities, but each member is responsible for following the security standards.

Awareness, training and education for security best practices must be continued. For example, an organization can send selected team members to security training conferences to learn the latest industry techniques. With the new knowledge gained, these individuals can then share their insights with the larger organization.

3. Monitor and measure: Information Security Governance requires constant assessment and measuring.

- What policies are working?
- Which policies are not?
- What teams or individuals are not following the security policies?
- Are the number of security incidents impacting reputation with customers and partners?

Measuring the performance on 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 organization might hold mock data breach scenarios to see how well the teams hold up. The results can showcase what a company needs to work on, and what they have nailed down.

4. Foster open communication between all stakeholders: It's vital that all stakeholders feel 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 organization feel comfortable enough letting leadership know? Or will they attempt to shield any negative news from the top?

Open communication promotes trust while augmenting visibility throughout the organization. To further enhance engagement, consider creating a steering committee comprised of executive management and key team leads to review and assess current security risks. Members might include leaders from the IT, finance, PR, marketing, legal and operations departments. Regular steering committee meetings can make sure that there is ongoing adherence to the security policies. For example, if a new security policy is created, department leads, who are part of the steering committee, can make sure 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, while establishing solid policies and guidelines, must be open to adaptation. An organization should monitor and measure the overall strength of the security policies. Questions to ask include:

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

For example, an employee in the IT security trenches may have the hands-on experience and insights on the effectiveness of a particular security policy. If leadership is receptive to hearing the team member's feedback and suggestions, there should also be agility in 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 its specific needs, securing their data is a common goal for all organizations. Emerging technologies and cyber threats will continue to evolve. Data breaches and security incidents will happen. Rather than scrambling after a security breach, organizations 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 strengthen your organization's security posture while protecting your valuable information.

SOURCES:

1. "Data Breach Reports," ITRC, December 29, 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, April 21, 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, December 16, 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, February 4, 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/