Chapter 8

Balancing Information Governance and Your Company's Mission

To this point, we have spent quite a bit of time exploring the various aspects of information governance and the clear benefits a solid plan can bring to an organization. However, the question remains whether an information governance plan will be compatible with your organization's current structure. How difficult will it be? How much will it positively or adversely impact the bottom-line?

While these questions might seem to imply that information governance is being forced upon a business, the fact remains that some business models were established without ever taking information governance into account and are therefore not designed in a manner that would easily permit the introduction of internal checks and balances, policies, and procedures regarding your IT systems and data.

None of this is to suggest that you should re-create your business model from the ground up to incorporate information governance, although doing so can pay dividends in corporate security. The phrasing of the question seems to suggest that information governance and a profitable business are in some ways mutually exclusive. That is to say, any gain to one comes at the expense of the other. To move toward adopting information governance would be to move away from profitability.

It is understandable that it may be difficult to move away from this line of thinking while you are metaphorically trying to fit the square information governance peg into

Information Governance and Security. http://dx.doi.org/10.1016/B978-0-12-800247-6.00008-X

a round business model hole. After all, the corporate environment is in the business of being profitable. The very ecosystem of a successful corporation seems to ensure that any procedures, checks and balances, or behaviors acting in contradiction to that goal are identified and neutralized. If information governance is one of those things that are inhibiting profitability, then surely it will be discounted.

The question of how a business should draw the line between having information governance policies protect their important data while not inhibiting the ability to conduct business is difficult to answer. Information governance can be a matter of two extremes: either being protected or not protected. Will giving too many resources to the former inhibit the ability for a company as a whole to function? After all, how much protection is too much? It is definitely not an easy question to answer, and the issues of increased efficiency, improved productivity, and fewer losses need to be evaluated.

Policies

All businesses should have some form of plan or system in which information is handled or gathered. Systems such as the Generally Accepted Privacy Principles are the mainstay in most businesses today.[1] Having a system to follow will limit the possibility of mishandled information while streamlining in-business dealings to be faster and more efficient. In addition, the cost to manage the system should not cut into the business's profit too much. Exactly how much should be decided by the business itself as a part of an overall strategic plan.

Businesses can remain fairly secure by having plans that confine their data to business quarters and a limited number of employees, consistently managing employee regulations, and adhering to a pre-determined system of information handling. Following these basic practices will streamline business affairs without compromising the security of private data. If at any point privacy policies begin to impede too much on efficiency, then the business should re-work its plans. An ideal plan actually improves efficiency. The information governance committee should have improving business processes as a task. Policies should be measured and systematically evaluated.

To avoid issues, a business should carefully create company policies and utilize current technologies to find that fine line between security and profitability. Developing such plans is not a one-time event. Rather, it should remain an ongoing process. Part of the company plan should be to make full use of employee resources, making sure employees who handle sensitive information are properly educated on the requirements of their jobs and that they have read and understand the company policies. A slight lapse by one employee can cause an error that is catastrophic to the company.

In addition to education, companies need to dedicate a percentage of their financial resources to keeping technology up to date in order to maintain the protection of company information (and to constantly improve efficiency). Companies with strong protections are less likely to become victims. Of course, there will always be risks and threats, but the goal of information governance is to conduct business while mitigating risks. Companies need to work constantly to maintain the balance between profitability and security. Deciding just how much risk an organization is willing to assume must be covered in the company's information governance plan.

Strengths and Weaknesses

In assessing the introduction of information governance policies versus maintaining the current operations of an organization, sometimes the only thing that stands in the way of progress is how the organization chooses to look at the proposed changes. Are they strengths or weaknesses? In doing this, we depart from a paradigm of seeking forcibly to insert information governance policies upon a company, choosing instead to begin by accounting for both the risks and benefits of all things information governance. By doing so, we can highlight newly available solutions to old issues.

Possible points of contention seen when forcing information governance into an existing corporate structure can be categorized into positive and negative gains. Negatives that arise due to an incompatibility of the old corporate structure and the inclusion of information governance can be viewed as an opportunity for improvement. Assume for example that an organization learns in advance that the government or law enforcement could subpoena private customer information. If a company were to offer private communication services. a conflict of interests would exist, as the power of subpoena jeopardizes this privacy. If the company were aware of such possibilities in the beginning stages of corporate development, alternatives could be considered that might not be feasible in cases where information governance is later added to an established environment.

In regards to the problem of private information being obtained via subpoena, policies could be modified to decide how user information could alternatively be stored. Restrictions could be implemented that prohibits the organization from accessing a client's private information without the client's password. In this way, both corporate and user interests are shielded in a manner that ensures compliance with regulations and cooperation with law enforcement. In addition, the company's marketing can use this feature an additional enhancement in attracting more clients. Often, it is all a matter of how companies choose to look at the possibilities and act upon them.

Balance

Balance is a common theme within information governance, as it is in many facets of running a business. Think of balancing the expense of retooling a factory with the

cost savings it would allow. Having secure procedures and policies that balance with an organization's processes that require meticulous planning and implementation is much the same. The need for balance between these two is important, because having too much or too little of one can spell misfortune for businesses.

Having very limited information governance policies could leave a business unprotected and data vulnerable, whereas implementing too many such policies could affect the way a business functions, thereby curtailing profits. However, because each business has different procedures, goals, culture, management hierarchy, etc., it would be impractical to create a one size fits all for every company to follow.

For example, a small business such as a bookstore will have vastly different needs than a million-dollar corporation in terms of employees, systems, and information. Therefore, an effective start to creating a balance for security and business needs is to identify and analyze the most critical areas of the organization. A good place to begin would be anything that holds valuable information such as databases, servers, and workstations. The next step would be to determine the risks that could affect those services, such as natural disasters, malicious software, physical theft, and other threats. Once the important areas and risks associated with them are identified, businesses must adopt measures to detect, deter, and mitigate these risks.

This may sound like a relatively simple and straightforward process, but as stated above the difficulty lies in creating a balance between information governance and business operations. The solution at times can be to implement very few policies—or sometimes not to implement any policies at all, depending on the risk. If, for example, one of the biggest risks to an organization is an employee stealing office supplies, the best solution would be to install a security camera or have employee training that show the effects and consequences of stealing office supplies. A needless and overly burdensome solution would be to implement an abundance of costly information governance policies, such as hiring security guards to watch the employees. The balance addresses the basic problems and leaves out controls that are not actually needed the majority of the time.

Varying Approaches

While there is no reason to deny the point that the goal of all companies is to make a profit, these goals can be quite different from one company to another based upon the business they are in. Because of these differences, every decision made for the various business aspects is going to vary from one company to the next. Their approaches to information governance are no exception.

The type of business determines where the line is drawn regarding the level at which information needs to be protected. For a financial institution, the line may be drawn where customer information ends and their personal banking information begins. The same may be said of medical institutions where personal information is deemed to be

sensitive. The point, of course, is that once sensitive information—personal, financial, medical, or anything of the sort—is involved, the line must be drawn in the interest of protection through the implementation of information governance.

Another way of examining the issue of when information governance is needed is to focus not on how a business makes money but instead look at how a business attracts and retains its customers. For instance, financial institutions have always attracted customers by assuring them that their money was safe. As we have moved beyond the days of cash and are now more focused on accounts and credits, the collateral of a financial institution now includes their clients' personal information and bank account numbers as well as the balances in their respective accounts. The same rules now apply for medical institutions and private businesses. While the approaches may vary, all businesses need to establish certain levels of security procedures to ensure the information they collect remains secured. A security breach or a leak would be disastrous for any business regardless of their power or status. As was the case for the 2013 data breach at Target, although the breach did not destroy the company it did adversely impact its reputation and financial performance.

Weighing the Benefits

By working together with your company's IT department or equivalent experts on your current set-up for data management, a better understanding can be gained of where the company stands regarding information governance and, more importantly, how much your company needs to further achieve. All of this is considered against the background of the company's earning capacity.

A good rule of thumb when considering the implementation of information governance policies is that the more value your company places on something, the more likely it is that someone else wants to have it and is willing to break the law to get it. Just like money, information has to be stored and secured somewhere. And the more information you have the more of a valuable target your company will become. Hence the need to invest some of the organization's profits into dependable security measures.

Generally, those in charge of the organization will already understand this and be willing to listen to viable solutions. What is often not understood is that expensive security measures might actually be more than needed or not worth the cost for the results they produce. Employing such extreme measures ends up negatively affecting the company by having security that is too restrictive. The business might become frustrated under the weight of security, especially if the policies forbid new technologies, applications, or devices that the company wants to adopt. Rules and policies can expand and become more restrictive until they are too rigid to allow the company to compete and innovate.[2] The reward of safer and smoother information governance should always be balanced against the risk of upsetting your workers and limiting your company's growth and efficiency.

Team Effort

Corporate structures consist of compartmentalized sections focused on groups of goals with similar responsibilities. Although a part of the same organizational, these compartments are a mix of forces involving rivalry and competition over allocated resources such as budgetary funds and symbiotic dependencies. Software programmers could not work on nonexistent blueprints that were not produced by the engineers who were not made aware of the needs and expectations of the project until direction was provided by management.

All of this is understood to be a risk to workflow productivity in a corporate environment, and these functions of communication and information transfer are taken into account as the corporation is established and continues to grow. Such risks are known and accommodated by allowing amendments to policy as new situations arise. Unfortunately, this can also lead to contradicting statements in policies from differing sections of the corporation, as sections are updated without having a full understanding of the greater vision or favoritism is displayed toward some departments over others. In time, this may serve to undermine the founding ideals of the company.

It is also possible that old policies where created in a manner that addressed issues as they existed in an earlier time. Those policies may have once been satisfactory but perhaps did not take into account advances in technology, the increase in the amount of data, or the speed with which it can be transmitted. However, efforts to update antiquated policies could be met with contention by some, based on fears of disrupting those policies that are already in place. For some the older policies assure the inner-operability of the corporation.

A key characteristic of any successful information governance initiative is the establishment of an enterprise-wide approach that clearly sets out roles and responsibilities, emphasizing that everyone has a part to play in enabling successful IT outcomes.[3] Implementation of effective information governance depends on everyone having adequate and appropriate skills to fulfil their specific role. In most organizations, investors and controllers will have a good understanding of governance principles but usually have a poor understanding of how to apply these principles in the world of IT. Likewise, although IT specialists understand IT, they may have a poor appreciation of governance and control principles.[4]

Decision Makers

Whoever is in the appropriate decision-making role in the company may not be fully equipped to make the best decisions when it comes to working out an approach to information governance. By its nature, information governance involves the ever-evolving technology employed by a company to keep its data stored, organized, and safe. Depending upon the type of corporation, those in leadership positions are not

always the foremost experts in their own technology. After all, this is why companies employee IT personnel. Often, those in charge will consult tech-savvy individuals from their IT department to develop solid plans for the company's information governance systems. Alternatively, there are many traps into which higher-ups can fall into by making uninformed decisions, the consequences of which could include losing large amounts of the company's information and money.

Likewise, decision makers need to ensure that the IT is managed appropriately, because in a technological world the key to disrupting business is to disrupt IT. Organizations should strive to have trusted managers to oversee sensitive data, regulate the sharing and safety of data, and ensure efficient operation for everyone's benefit. Doing so allows employees to access the information they need to conduct their work quickly and efficiently.

An effective information governance program is best developed and driven by a committee with a senior leader at the helm who is not in charge of IT. Having someone leading the way with a qualified team but without pre-conceived notions and alliances is your best bet to developing the balance you need.

Factors to Consider

Guidelines

In establishing information governance polices for an organization, it is important to have established guidelines for all departments or sectors of a business. A business needs to implement proper policies that appropriately address how the information in a business is both stored and used by those within the organization.

The first step in establishing guidelines would be to identify what type of information each department needs. Businesses can achieve efficient information governance by outlining specific demands for the information the company holds. In creating proper policies, an understanding of and compliance with applicable laws is crucial. Once the law is understood, a company can tailor a policy that is within the standards of the law but is most effective for their type of business. Efficiency with information governance will help mitigate risks with cost. A company should not store data that it does not need to conduct its business. Excess data can cause unneeded problems and increase cost for data storage.

The next step in the guidelines process is to determine what departments and outside organizations require in order to communicate efficiently. Passwords, encryption, and access to documents would then be established for that department or function. In addition, only the information necessary to perform the function would be accessible. For example, a transaction at a retail store does not require a social security number, but a human resources department does.

Social Media

In today's society, online information is one area where businesses can potentially be very vulnerable. Social media websites like Facebook and Twitter can be great ways to spread promotions and new products your company has to offer. However, these same websites can also spread very sensitive data via posts by current or former employees.

It's important for businesses to give their employees guidelines on how to represent themselves and their company online, especially as it pertains to their personal social media pages. These rules should be made part of the company's information governance polices, with specific language addressing what current or former employees may say regarding the company and its services, as well as the potential civil ramifications for breaching the policy.

For example, if a former employee posts information on one of the social media websites that details confidential corporate information, such as formulas or how products are made, the release of this information can be devastating to the company. If the information governance polices does not contain specific language specifying limitations, the offending party can defend themselves against liability by pointing out that nothing in the company's regulations prohibited such actions.

Even in cases where it is not necessarily intentional, employees who post information on corporate developments can be equally harmful to the company. By posting information boasting about the company's future success, employees may be tipping off the competition or giving the competitors ideas they might not have even considered. Therefore, information governance policies need to cover employee behaviors both on and off duty; behaviors which can potentially impact the organization.

It is important to note that information governance policies that address employee conduct have to be carefully considered before being implemented. As an employer, you want your employees to be happy and have some sense of freedom. Forcing employees to delete their entire social media accounts before being hired or while working for a company will generally create a sense of dissatisfaction, especially today when many people see social media websites as a significant part of their social life.

To the contrary, information governance policies can actually encourage employees to share their love for their work and their employer via social media websites. Rather than language that discourages social media use, policies can be drafted encouraging persons to engage in the behavior they want but cautioning against certain dangers. Likewise, these same policies can provide examples of permissible postings on social media, so that employees have a clearer understanding of what to do and what not to do. By not discouraging the use of social media yet limiting the potential exposure to threats, companies may very well reap the benefit of further publicity through the efforts of their employees. The best way to implement information governance policies regarding social media is to have a balance between

freedom and restrictions. It is important to protect your company's valued information, just as it is also important to share with the world the positive things that your company is achieving. At the end of the day, revenue can be generated by companies, without revealing vital information, by advertising themselves in the proper professional manner through the social media posts of employees.

Companies should also have established policies covering what is the permissible use of social media during office hours. The personal use of social media during work hours can result in a significant loss of productivity. It is estimated that 50% of all corporate bandwidth is being used by employees to view social media, check e-mail, and surf the web. While companies can encourage some downtime for employees to recoup and recharge, the Internet can equally prove to be a distraction from the mission. Good information governance policies will not only outline what can be posted but also permissible times to use social media during work hours, such as on approved breaks and during lunch.

Costs

Some aspects of information governance can be expensive. Security measures, system monitoring, and training are all time consuming and come with a cost. It may be easy to look at the expenditure of both time and profits and decide it is not worth the efforts or expense. However, while there are expenses associated with information governance, it is potentially more expensive to defend against lawsuit for not sufficiently protecting the integrity of sensitive information or to provide mitigation to those who have been victimized by a breach. In many ways, information governance is like insurance. You hope never to use it, but you are certainly glad to have it when needed.

This does not mean, however, that every dollar made should be invested toward the protection of that dollar. There is a point where protecting your assets may hamper your company's abilities to acquire those assets in the first place. This is where the line must be drawn. If a company is spending more on protecting information than the information is worth, then this line has been crossed. It may be difficult to determine exactly how much employee or customer information is worth in monetary value, but once the risk for leaking any of it is small enough, pouring more time and resources into this effort becomes a diminishing return. While there is something to be said for the phrase "better safe than sorry," the expression "a penny saved is a penny earned" also has merit.

Profits

In most businesses, money is what decides success. It is the lifeblood of business operations and structure. When we think of information governance as protecting sensitive information, indirectly it is also about protecting the company's profits.

Like the earlier referenced business balance, the same issues have to be considered for information governance when it comes to the profits. Information that leaks into the wrong hands will likely result in major financial consequences—in other words, a loss of profits. However, an overabundance of safeguarding could be detrimental to an organization's flow of business, leading in turn to further loss of profits. Likewise, information that is restrained too securely in business operations can hinder operational functionality, thereby losing money in the process.

All this needs to be kept in mind while generating a profit. Each time a decision to implement a greater measure of security in the name of information governance is considered, the company decision makers need to take into account the type of information they are protecting and whether the possible loss outweighs the cost of protection. Can an informational asset be compromised without major consequence? Complicated steps and passwords can be a hindrance on a simple transaction. In the interest of maintaining a healthy profit margin, a balance is needed between the protection of information and productivity within a business environment.[5]

Communications

When developing an information governance strategy, a business needs to determine how it conducts both its internal and external communications. These communication lines will inevitably be affected by any additions of information governance policies.

Having information governance plans is one thing, but effectively communicating them to your employees and customers is another. Changes or brand new implementations need to be communicated properly to your employees to ensure the methods are being utilized in the proper manner. Likewise, by communicating these changes or implementations to an organization's customers, the business can effectively gain consumer confidence, which can possibly translate into increased revenue.

Another necessity is to understand how information governance policies could negatively impact the flow and level of communication. New or more complicated procedures can delay request from both employee and outside customers. Response times can also be slowed. It may be that before policies were implemented everyone in that company had access to certain information, but now procedures create checks and balances in releasing information. Companies must communicated to their employees how best to minimize any new delays that might have developed, while also communicating to customers how these potential delays are in their best interest because they ensure information security.

To help in these situations, a business should implement some type of easily accessible, cross-functional team that caters to the company. A cross-functional team would be able to bridge a gap between the various parties responsible for new information governance policies, teams making requests, and those who handle information.[3] Using a team as opposed to a single contact allows multiple eyes to create

checks and balance for good governance. It also keeps the lines of communication open to reduce delays.

Culture

Whenever changes are contemplated, an organization must be aware of the corporate culture that exists and how it may be impacted by any potential changes. The acceptance of change will vary from business to business. Because many people are reluctant to embrace change, organizations need to be aware of any potential impact that the change may have on their employees (which can negatively affect productivity) as well as the impact that change can have on clientele (which can affect customer loyalty).

One of the best ways to help merge information governance into a corporate culture is for the leaders of the change to embrace awareness. Having employees and customers aware of policy changes coming well in advance allows time for both parties to adjust to the new way of working.[6] A staggered approach to implementing policies also gives employees and customers time to figure out how to work optimally within these new policies. This allows minimal disruption to a business's culture and allows it to continue operating at a (mostly) normal level. This is critical to the company's ability to conduct itself in a proper manner.

Significant benefits can be gained for the organization by tailoring the policies wherever possible to match the existing businesses culture. Allow sufficient time for various aspects of the new information governance policies to be put into effect gradually, rather than a wholesale implementation of new rules overnight.[7] Allowing time for adjustment to a few new policies alongside normal operations will lessen the apprehension of those who—regardless of the benefits—do not embrace change. It is ultimately not what policies are implemented but how and when they are implemented that can affect a business. While information governance is important to the functionality of a company, it also needs to make allowanced for a user-friendly environment for the clients. It is important that a company's clientele can still be provided with the necessary products and services to which they are accustomed.

CIA

Information governance includes the concept of CIA: confidentiality, integrity, and availability.[8] The absence of any of these three concepts undermines the proper practice of information governance policies.

Confidentiality is the prevention of information disclosure to unauthorized individuals or systems. If information governance policies did not adequately maintain the confidentiality of research and development files, and these files were to be accessed by a rival company, the loss of confidential information would have a negative affect on the company.

Integrity ensures that the information has not been altered and is recorded and stored accurately. Easily gaining access to information is not of any value if the information in question is not what it should have been. In the interest of saving money on the cost of storage, a company would never consider randomly deleting sections of documents. Ensuring information integrity is crucial to supporting information governance.

Availability is the ability to access information when it is needed. If an organizational leader needs information for a shareholders meeting, but cannot access the files, the availability of this information is too low and will undoubtedly have a negative impact on the perception by the shareholders. If the availability of information is so low that the people who need it cannot access it, the information cannot properly serve its purpose. Information, no matter how valuable, is essentially worthless if it cannot be used to carry out tasks for which it is needed.

All three aspects of CIA must work together to achieve the necessary balance for information governance to function in the sought-after fashion. Too much or too little of any of these attributes will cause information governance to fail. Businesses should therefore apply these concepts on a case-by-case basis. Within the corporate structure, various documents may call for various levels of security. Research and development may be guarded more securely than lesser administrative functions like plans for company fire drills. Elements of CIA will need to be applied to all aspects of information, but it is up to the organization's leaders to decide upon where and how much.

Security

How does a business balance making money with mitigating risk to their data or information? Measures that can be set in place to help a company run smoothly in terms of making money while also accomplishing the mission of information security. Before determining what information governance policies to undertake, we first have to determine exactly what needs to be secured. Like reading a map, once we figure out where we want to go, we can then figure out how best to get there.

Every company—from the smallest operation to the large corporation—will have a certain amount of PII. Employee dates of birth, social security numbers, and bank account numbers for payroll deposits are all maintained by the company, and the company must be responsible for securing this information.

Next is the concern for the security of customer information. A company might have bank account information for their purchasers and suppliers. Those doing business with the public can accumulate a significant amount of credit card numbers. Those in the business of issuing credit cards will have the personal information of potentially millions of customers.

From a business standpoint, information governance plays a vital role in keeping both information and a company's reputation secure. However, security all comes

down to finding that delicate balance. While protecting the company's reputation, if things become protected to the point that security is too difficult to manage, security can actually work against the information governance plan.

Overly complicated passwords can become a nuisance to input every time if it is too demanding for the employee to remember. When password requirements become too complicated, employees will opt to write them down so that they do not forget. The intent behind a complex password is noble but can undermine the effort by allowing prying eyes to obtain the written password. Companies should require passwords difficult enough to deter hackers but not so complex as to discourage use by their employees.

Also, it is also an excellent idea to require passwords to be changed at regular intervals, usually anywhere from three to six months. Regardless of security measures that are in place, it is inevitable that an employee will in some manner lose, forget, or share their password, which compromises security integrity. By mandating regular password changes and not permitting recently used passwords to be recycled into use again, the threat of hack or other breaches of password security can be greatly diminished.

Clearance level access is a security method used in organizations that have highly classified information that must be kept secret. Various employees will possess various levels of clearance in order to obtain data secured at different levels. Overclassifying information unnecessarily or not compartmentalizing out unclassified information from a classified document will limit the availability of the data for those who might need to work with this information.

Most hackers do not want to spend an enormous amount of time trying to get into a company's system. Most hackers prefer the easy steal. By incorporating a few basics into a company's network security plan, many of the threats of unauthorized intrusion to a network can be eliminated. Sensitive data on a company network should have levels of security to minimize the threat of being hacked, but there are basic and balanced steps a company can take to limit this threat without applying overly complicated methodologies.

The first step would be to limit who has access to the network. Of course, an organization wants its IT people to be able to access the network, but there may be others in the company who have a need as well. Determining who has a need and who does not can limit the accidental or purposeful exposure of the company's network security.

Second, from what locations can the network be accessed? Again, you probably want your IT personnel to be able to access the network any time of the day from anywhere in order to immediately address problems that might occur. But do other personnel have the same needs? Should employees be able to work from home on their personal computer, when the company does not know how secure that computer may be before it accesses the corporate system? Malware on the home computer can be spread to the work computer. Requiring employees to take home a work laptop that is securely maintained solves the problem of working from home without threatening network security.

Likewise, what about the times when the network can be accessed? IT may have a reason to be on the network day and night, but the average employee probably does not. By limiting network access to business hours or when a laptop has been checked out to work from home or while away on business, those monitoring information governance security will be able to see who is accessing the system at odd hours. Those not authorized to do so may be accessing the system for nefarious reasons that can then be prevented.

Training is one of the greatest and most cost-effective ways to ensure an organization's level of information security. If training is conducted at regular intervals and with repetition of subject, employees are likely to grasp the importance of the security standards and better adhere to the policies.

The use of technology to help keep data secure is forever changing. At times it can be difficult for everyone within the organization to comprehend. These difficulties could cause annoyance, which can then translate into a lack of concern on the part of some employees. However, with an investment of a minimal amount of time, employees can receive refresher training to ensure they are comfortable with their roles in securing information.

Likewise, most attacks such as cold calling for social engineering and e-mail scams that contain malware are successful against persons who are least familiar with proper information governance. Knowledgeable employees can stop most basic attacks themselves, as well as inform IT personnel so that the rest of the company can be made aware of the attempted attacks. The minimal downtime from work to provide regular employee training will more than pay for itself in the avoidance of corrupted networks and monetary expenses to repair the damage of compromised information.

Companies walk a fine line in trying to decide how much security is needed for their organization in order to balance the needs of business verses the needs of information safety. Companies need to decide what is important, and each department needs to gauge importance. An all-in-one policy can hinder certain profit areas. Each security measure needs to be company and department specific, and to provide a clear understanding employees about information that is readily accessible and data that needs to be more securely protected.

Need-to-Know

In order to limit sensitive data from seeping outside the boundaries of where it should be confined, businesses should take steps to permit data to be accessed only by those who require access for specified purposes. This aspect of information security can be accomplished in several manners.

One of the more prominent ways to limit corporate information to those who have a need to know is though the use of in-house software. By utilizing programs that are not necessarily off the shelf but rather designed specifically for a particular

company's business needs, it makes it much more difficult for employees to abscond with information if they do not have the software necessary to read the information. This allows a business much greater control over its private data.

The idea of business specific software can be taken even further by having different software programs for different branches of a company's operation. This enables the company to further limit their data and other sensitive information to only those who have access to these particular programs. Lower-level employees will only have limited access, and access will increase as employees have more specific functions or hold higher positions within the organization.

Additionally, by maintaining this software and the accompanying data in in-business databases separated from the open web, businesses do not have to rely on firewalls and other networking security to ensure their information is not compromised through computer intrusion. This allows for clean, efficient data management without hindrance or data flow impediments. In the end, this mean the primary locus for information slippage is the employees themselves.

It is important for only those employees that need to use certain information to be the ones with access to that information. A company should have policies that allow employees to do their jobs and ensures appropriate access to information while also requiring employees to be accountable for their actions. If an employee is dealing with crucial information, they need to know how to handle it appropriately.[9]

Mitigation of Risks

In order to find the balance between information governance and a company's ability to conduct business, there needs to be a balance of protective measures within the company and measures that mitigate potential risks. The company must decide how much risk they can afford in the event of lost or misused data and information without hamstringing operations to the point that clientele is discouraged from doing business and instead seeks out a competitor that operates more freely. Similarly, if a company is not secure enough, the company can be the victim of data loss, espionage by a competitor, and a variety of other events. Nevertheless, there are some basics any organization can undertake to mitigate their risks from some of the more common threats.

Mitigating the risk of employees misplacing data begins before the new employee is even hired. Thorough background checks should be undertaken to ensure that personnel are qualified for the position they are being sought to fill. Are these employees being recruited from a rival company? Do they have designs on starting their own competing business? Do they have a history of criminal offenses or arrests, especially ones involving cybercrimes and the compromise of information? Are these individuals experienced at handling sensitive information and, if so, how successful were they at performing these duties? As part of the pre-employment screening of a company's information governance plan, these questions and others should be asked

before new hires are welcomed on board. In doing this, the likelihood of a purposeful data-leak by a less-than-trustworthy employee is greatly reduced.

Once hired, it is equally important for all new hires to be thoroughly briefed on the company's information governance policies. Just as efforts were expended to limit the potential for an intentional data leak, these efforts will greatly reduce the likelihood of an accidental leak. Furthermore, consideration should be given occasionally to administering employee testing to monitor their knowledge of and consistency in following the company's information governance rules.

Closing Thoughts

The primary goal of any business is making money. However, a business in the pursuit of profit should not do so by being careless with their most valuable data, whether it be employee information, network topologies, access credentials, financial data, or any other critical information. Instead, businesses need to balance the goal of making money with the necessity of solid information governance policies. The trick is to find the proper balance. The fine line that allows a company to protect valuable data and yet remain profitable is up to each company to determine for themselves. In today's world, the two functions can no longer be mutually exclusive.

References

1. "Generally Accepted Privacy Principles," accessed December, 2013. http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/generallyacceptedprivacyprinciples/pages/default.aspx.
2. Andreas M. Antonopoulos, "Can You Have Too Much Security?" May 31, 2011, accessed February 2014. http://www.networkworld.com/article/2177700/security/can-you-have-too-much-security-.html.
3. ISACA, *An Introduction to the Business Model for Information Security* (Rolling Meadows, Ill.: ISACA, 2009), 12. http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf.
4. Ibid.
5. David Cowan, "Comment: Too Much Security May Affect Business Practices," June 27, 2012, accessed December, 2013. http://www.infosecurity-magazine.com/view/26550/comment-too-much-security-may-affect-business-processes/.
6. IT governance, 2005, 25.
7. ISACA, *Introduction*, p. 13.
8. Terry Chia, "Confidentiality, Integrity, and Availability: The Three Components of the CIA Triad," *IT Security Community Blog*, August 20, 2012, accessed December, 2013. http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/.
9. Debra Logan, "What is Information Governance? And Why is It So Hard?" *The Gartner Blog Network*, January 11, 2010, accessed December, 2013. http://blogs.gartner.com/debra_logan/2010/01/11/what-is-information-governance-and-why-is-it-so-hard/.