Corporate Information Governance with Business Wisdom

David Alexander Cruz Urena

Corporate Information Governance with Business Wisdom

GIAC (GSEC) Gold Certification

Author: David Alexander Cruz Urena, MS, CISSP davidcruzurena@gmail.com
Advisor: Chris Walker, CISSP
Accepted: April 11, 2020

Abstract

Whether a secret ingredient used for a lemonade stand across the street or the business strategies of a Fortune 50 corporation on Wall Street, organizations that collect, process, or transmit any data have the legal and moral responsibility to govern it. Governing information goes beyond technical capabilities. Further, it is unwise to rely on a department to define, organize, present, and protect information. With the explosion of information into every business activity, information governance is a practice that businesses must exercise. This paper provides actionable and comprehensive strategies to develop effective corporate information governance. Three principles are addressed: governance of accountability, clarity of purpose, and clarity of collaboration.

1. Introduction

What is more valuable $40 billion, or Coca Cola's recipe? Choosing the former, realize that Coca Cola's is worth $198 billion. And the entire business was built based on a highly guarded secret formula (n.d.). Google's search algorithm, Kentucky Fried Chicken's ingredients, McDonalds's sauce, WD-40's formulas are regarded as some of the most guarded data in the world. All organizations, whether it is a one-person office or 2.3 million workers giant, rely on the information they produce and collect.

Information is the lifeblood for businesses in today's data-dependent age. Government offices need information to ensure the well-being of its citizens. Financial institutions rely on information for accurate representations of their transactions. Healthcare services need private information to provide proper care. Retail stores know that without the needed information, they cannot deliver goods or collect payments. Manufacturers obtain information to engineer the most relevant and profitable products. Schools require certain data to issue appropriate grades and degrees.

Assumptions, that information governance should be instituted solely by large corporations, should be abolished. Nothing can be further from reality. Adversaries, who are after information, have many motives. For example, there have been cases where crooks compromised third-party vendors to bypass corporation strategies (Perlroth, 2014). A course that is no different from bank robbers breaking to a less guarded business, perhaps next to the bank, to evade the bank's protected measures. Besides, the collateral damages resulting from a coordinated outbreak can impact the weaker posture and be too powerful for small commerce to sustain. With such trends come many risks and issues. No longer is it acceptable for organizations to ignore this fact. Companies must systematize the information regardless of where it is processed, stored, or transmitted.

Clear mandated principles have been enacted to protect information. For example, the European Union has created the General Data Protection Regulation (GDPR). The statues uniformly apply to any organization that processes, transmits, or stores EU citizens' data regardless of their membership's status. It expands the role of information governing in business

today. And the associated ramifications as organizations can be fined up to four percent (4%) of its annual revenue.

When similar legislation would be enacted in the United States at the federal level is difficult to know. Though, in January of 2020, California executed a similar statue, the California Consumer Privacy Act, A.B. 375. New York, Washington, Nevada, and Maine are among other states implementing similar laws in 2020 and beyond. Administrations must note and analyze this and others pending legislation, expressly the expanding definition of "personal information". Information is involved in nearly all aspects of the corporate environment, so implementing information governance now will save time, money, and resources.

Substantial fines can be imposed on those who do not exercise information-care. Make no mistake, compliance with applicable laws and regulations does not equate an effective information governance program. Governing information requires activities beyond those listed on a compliance checklist.

No longer is it safe to trust a single department with business-related data. In effect, all Albert Einstein-typed professionals put together is enough to adequately protect organizations' information assets. Therefore, defenses must aim to reduce the possibility of a major threat and minimize the impact information thieves can have on organizations. As author Tony Saldanha stated in his book, *Why Digital Transformations Fail,* "The fact that no industry is safe from digital disruption is widely understood now. Howbeit the initial digital disruption examples may come from media, finance, entertainment, retail, technology services, and manufacturing, nobody is immune" (Saldanha, 2019, para. 14). Privacy rights clearing house tracks data breaches since 2005.

It has reported 11, 613, 524, 580 records breached covering several industries. Major disruptions worth mentioning include: Target (Retail), Sony (Entertainment), CapitalOne (financial), The Office of Management (Government), Marriott (Hospitality), Anthem (Healthcare), and The University of Central Florida (Education). The lack of preparation has dire consequences. As this paper is being written, the world has been paralyzed by a biological weapon. COVID 19, as it is co-named, has impacted humanity socially, economically, psychologically and in many other ways. Several trillions of dollars have vanished from the

global market. Consequently, the absence of lives continues to proliferate around the world. While several theories have emerged to justify preparedness for the outbreak, the results are evident. In a sense, the pandemic shall be an educated lesson for organizations to be proactive rather than reactive. A computer virus might not cause deaths, but it will certainly cause financial distress to those that are not prepared. Instituting an information governance program now is a prudent step to avoid chaos and minimize disruptions.

Information governance requires an organizational-wide commitment. From the front to the back office, everyone must have a clear understanding of which information is time-sensitive and which is not. The welfare of information is a good business practice, as the business depends on it. Therefore, it is important that the collection, dissemination, sharing, processing, transmission, and storing corporate data is controlled.

Although this paper will be mostly read by practitioners, the ideas in this research are invaluable to share with decision-makers. The study precisely focuses on three premises: 1) governance of accountability; 2) clarity of purpose; and 3) clarity of collaboration. First, it is essential to explain information governance.

2. Definitions

2.1. Governance

Governance has a wider view as an element that looks at the interest of the firm. Fostering survivability and overall health of the corporation, which would enable it to continue operating with little to no interruptions. It expresses the actions and rules that leadership believes to be necessary for the prosperity and success of the organization while balancing liability and scalability.

2.2. Information Governance

Information Governance is not the same as a policy. However, policies are a component of governance. When information becomes a corporate asset, a need to govern it arises. Hence, organizations begin to draft *information security policies*. However, many industries (Automobile, Healthcare, Insurance, etc.) have used this enigmatic word, "policy," too often to define their company's terms and conditions. An effective policy is not to be written to address every issue in the organization. Rather, a policy deals with problems that management believes are critical to the organization's mission, and that are intended to establish the organization's culture, while reducing liabilities, culpability, and any negative impact to the organization's health.

Information Governance drives an organization's decisions on how information maintains its confidentiality. The result: data is not disclosed to unauthorized entities; available computer systems and information are accessible to authorized personnel only; and no unauthorized modifications are made to the data, regardless of its states. When effective Corporate Information Governance is implemented, executive management demonstrates that information governing is a business necessity, unit management has clear and concise directions to implement strategies, and employees understand its importance.

Information Governance answers the following questions: Where is the time-sensitive data stored? How it is processed? How is it transmitted? Who interacts with this data? Is there a data recovery process in place? Are employees educated to the level that they can identify events before they become a business disruption? Is the business in compliance with the various regulatory and laws associated with the organization?

When information becomes data, it is not observable as physical objects. In his book, *Information Governance, IT Governance, Data Governance: What's the Difference? In Information Governance: Concepts, Strategies, and Best Practices*, Smallwood intensified this point;" Recognize the uniqueness of data as an asset. Unlike other assets, such as people, factories, equipment, and even cash, data is largely unseen, out of sight, and intangible. It changes daily. It spreads throughout business units. It is copied and deleted. Data growth can spiral out of control, obscuring the data that has true business value. So, data has to be treated differently, and its unique qualities must be considered" (Smallwood, 2014, para. 7).

Moreover, there are two principles to remember: 1) it is impossible to protect unknown assets; 2) protection includes every possible point of entry, while an adversary only needs one. Sadly, in many cases, evidence shows that most organizations do not know where their information assets are, who has access, and why.

2.3. Information Assets

An information asset is any medium that produces, collects, stores, and transmits information. It can be as simple as a laptop or as complicated as a competent employee. Two asset types are defined: intangible and tangible. The latter are people, machines, and other physical objects. Information is an intangible asset. Under this category can be customer lists, competitive insights, intellectual properties, just to name a few. Computer-enabled assets, then, can be classified as assets that process, transmits, store, and/or information disposal.

Consider the various business-enabler tools and places where sensitive information can be found: the Internet, computers, tablets, videoconferencing, web-based meetings, fax machines, printers, wall displays, videophones, wireless devices, corporate blogs, helplines, supply chains, package tracking systems, social media platforms, mobile phones, and cloud services, to list some of several. Nonetheless, perhaps the least considered but most important place for storing sensitive information is the human mind. Unlike computers that work on humans' commands, people behave based on feelings and emotions.

Whether information is produced to attract new customers or private information is collected from customers, employees, or proprietary (i.e., trademarks, copyrights, trade secrets),

all must be protected. No longer is it safe to trust an individual with valuable business-related information. An *All hands-on deck* approach must be instituted. It begins from the top, with leadership. From the front office to the back office, everyone must have a clear understanding of which information is time-sensitive and which is not.

Uneducated workers are the most predominant threat to information. Not only do they have less restrictive access to the environment, but they can also disclose insights about defenses and strategies to simplify an adversary's efforts. Examine some of the, regarding data governance, most high-profile cases, there are always uninformed participants involved. Consequently, no education, technology, systems, or procedures outlined in governing information has a greater impact as the active and unequivocal engagement of leadership.

David Alexander Cruz Urena, MS, CISSP, davidcruzurena@gmail.com

3. Principle I:

3.1. Governance of Accountability

The leader holds the power. Governing efforts are misaligned without the present and active participation from leadership. Leaders know the direction for their organizations and are aware of potential risks that can emerge to disrupt their operations and functions. They are the most qualified to produce, develop, and present these principles. Without the active involvement and support of corporate leaders, Information Governance will be unrealistic, unmeasured, unstructured, and unenforceable.

Functional responsibilities should be delegated to a senior manager with the appropriate accreditation, knowledge, and experience to oversee Information Governance. Duties include reporting to the executive team and board of directors. Executive reports must present activities related to how information is treated concerning people, technology and processes. Every department manager has the responsibility to report their current governance strategies to oversee information.

Is information welfare vital enough to have a place on an executive's already crowded desk? President Harry S. Truman had a sign on his desk with the words *The Buck Stops Here*. Meaning the responsibilities, accountability, and liability are not cascaded down from the leader to someone else. It begins and ends at the front office.

A key aspect of an effective program is to hold senior managers accountable for their action or inaction. Thus, an executive's bonus can be directly linked to how well each department unit governs information. If leaders are serious about information governing, they must add a line in their balance sheet that states "information governance" (Hopper, 2005). Management can develop an information governance scorecard for each department leader and review them quarterly or annually.

David Alexander Cruz Urena, MS, CISSP, davidcruzurena@gmail.com

3.2. Strategy

A good strategy to achieve Information Governance is to catalog all information and consider the following questions: Can the organization continue to support customers if this data were to be compromised? What legal liability does the institution face if this information were to be handed to a competitor? Would clients continue to do business after such a compromise? Who has access to it and why? Can one person in an organization answer these questions?

Additionally, when there is a disruption to businesses, is there a business resilience plan in place? For instance, how would a business continue to operate if key employees go on a cruise and their ship disappears in the Bermuda Triangle?

Warren Buffett, a business investor and CEO of Berkshire Hathaway, once said, *it takes 20 years to build a reputation and 5 minutes to ruin it.* The latter part is no longer accurate in today's interconnected world. Where news, which can instantly destroy a brand, travels at an unprecedented speed daily. Nowadays, it can take less than three minutes to destroy a brand.

For instance, reports of organizations disbursing money in large quantities due to "ransomware" attacks splash the news almost daily. Case in point, a government entity approved the payment of $600,000 to recover its data. Some cities were completely shut down, unable to serve its residents for days! (Associated Press, 2019; Miller, 2019). Without having a collective and business supported information governance program, issues such as ransomware can destroy companies.

Case in point in 2018, a company acquired by two private equity firms a year before ceasing its operation and later actioned all its assets due to a ransomware attack (Menapace, B, 2018). There is no life vest under the seat when business' information is exposed. Ransomware works because organizations need their information to conduct business. Attackers are aware that organizations are willing and able to pay a large amount of cash to regain access to their data. In certain cases, as in healthcare, the absence of information can be deadly.

3.3. Risk

All aspects of an organization directly or indirectly interact with business-related information. Even a department as simple as a Housekeeping crew must interact with information. Information, therefore, is the new DNA for all organizations today. As cyber-villains continue to disrupt businesses, organizations must set measures to govern the information they produce, collect, share, and store.

In the simplest formulation, a *risk* is the uncertainty level (in probability and consequences) organizations face when seeking opportunities. A risk can be caused by a malicious hacker exploring the weakness for certain elements such as, people, data, processes, or the facilities in which they take place. This event can be as simple as accidental deletion of a non-sensitive file or as critical as a malicious hacker deleting all the business' data.

A survey by Ponemon Institute and IBM Security found that "The loss of customer trust has serious financial consequences, and lost business is the largest of four major cost categories contributing to the total cost of a data breach. The average cost of lost business for organizations in this 2019 study was $1.42 million, which represents 36 percent of the total average cost of $3.92 million." (IBM Security Cost of Data Breach Report 2019, p. 5)

The same study found a "significant variation in total data breach costs by organizational size. The total cost for the largest organizations (more than 25,000 employees) averaged $5.11 million, which is $204 per employee. Smaller organizations with between 500 and 1,000 employees had an average cost of $2.65 million, or $3,533 per employee. Thus, smaller organizations have higher costs relative to their size than larger organizations, which can hamper their ability to recover financially from the incident." (IBM Security Cost of Data Breach Report, 2019, p. 7) The vast majority of organizations that are compromised do not report the matter. They justify this approach with the notion that making the invasion public will result in reputational damages. In reviewing previous cases, the conclusion affirmed their position. However, not reporting these will have financial and legal ramification in the future. What is more, failing to report the compromised preclude them from receiving appropriate expertise and support. The vast majority of organizations that are compromised do not report the matter. They justify this approach with the notion that making the invasion public will result in reputational

damages. In reviewing previous cases, the conclusion affirmed their position. However, not reporting these will have financial and legal ramifications in the future. What is more, failing to report the compromised preclude them from receiving appropriate expertise and support.

3.4. Assurance

Businesses, regardless of their market value, must not only govern their information within their walls, but also information that travels in systems and networks outside those walls. By certifying: 1) Outsiders have appropriate accreditations; 2) Outsiders agree to internal assessments, and 3) Outsiders' management supports the data governance program. The process initiates with the information owner wanting to onboard an outsider. She submits the completed questionnaire to the committee for review and approval. After the committed reviewed and provide a recommendation, it goes to decision-makers. An executive has the liberty to dismiss the committee's recommendation. However, it must be in writing and the owner does so at their peril. Ensuring that there is a formal process for onboarding all vendors (not excluding attorney-client privileges and work-product protection) and that Information Governance is included in this vital process. The initiative should delineate specific Information Governance requirements that service providers must have in place before being on-boarded.

In general, information governance is a wise decision on many fronts. For instance, many businesses collect irrelevant or store unneeded information. This practice leads to several issues, including infective business habits. Such as, wasting time trying to find relevant information, discarding important details about customers or business deals. Other issues can be listed here, but points have been made. Inaccurate data and understanding lead to ill-informed decision making. Information stewardship is far greater than a simple nod. Requiring dedication and constant analysis to ensure sensitive information is not use outside its intended purpose.

Leaders must realize that an unseen force is out to disable businesses with no sign of stopping. Super-users with malicious intent, unlimited resources, and no time limitation are after the organization's precious assets. Without regard to laws or ethical means, these villains have a master plan to explorers and take advantage of them.

4. Principle II:

4.1. Clarity of Purpose

One cannot achieve a goal without having a clear purpose. For instance, losing weight is a typical goal for most people. Nevertheless, simply saying, *I want to lose weight* is not the same as saying *I want to lose 20 pounds in 3 months, because I want to feel good and have more energy every day*. In the same manner, saying, *I want to be secured* has no meaning without clearly defining a purpose to be secured. Thus, leaders must take a step back and photograph their vision in a crystal-clear manner.

Considering the analogy above, when it comes to businesses, leaders may utter something like *we want to minimize exposure by 30% within the next 6-12 months because our current state is outside our risk tolerance*. With such a goal, they would have a cleared purpose for achieving it. The tactic is not to prevent a compromise, but rather, it is to develop strategies to minimize the impact. To this end, one must be clear on the following: 1) the core business functions, 2) risk tolerance, and 3) what information assets are in the organization.

The information collected must be relevant to the business by increasing its value and protecting the brand. No information should be retained unless it has a business purpose and should only be stored for the period needed. Legal authorities should be consulted and involved to determine the period certain information must be kept.

4.2. Risk Governance

Information, whether stored, processed, or transmitted, is ubiquitous. In general, however, it can be found in three places: on paper, in systems, and the human mind. Most information risks emerge from these areas. Information found on paper can be stolen or altered. Humans can be misled to disclose sensitive facts or turn evil and compromise their trust. Interconnected systems carry so much information that it is impossible to control. Risks are everywhere. Eliminating risks is not an option for a competitive business. Therefore, they have the legal and ethical responsibilities to govern risks. To reduce uncertainty and increase predictability.

Identifying information risks requires collaboration and commitment from everyone involved. Business partners, suppliers, and vendors must be considered when analyzing risks to the information entrusted to them. Legal must review all contracts and agreements to ensure clauses are incorporated with these engagements.

One must determine how much risk the business is willing to endure. For instance, it is beneficial for businesses to outsource certain functions. However, it is a high risk for there is no way for an organization to monitor and evaluate all activities performed by the outsourced entity. Thus, the goal is to minimize risks to an achievable level for management.

4.3. Resilience

Leaders should consider their most valuable information and contemplate these questions: If someone offered $10k for this information, would they relinquish it? How about $100k? $500k? $10M? How much are they expending to protect this information proportionate to its attributed value? Does management know their risk appetite and tolerance? How are they addressing these relative to the probability of a risk materialization? How do they identify who is authorized to interact with sensitive information, to categorize this information and become aware of the legal ramification when this data is compromised? How can they implement a personnel-succession plan, to exercise staff preparedness, minimize business disruption, allocate appropriate resources to protect this information, and ensure employees, partners, and third-party entities know how to treat time-sensitive information?

4.4. Classification

A business has a wide variety of information. However, not every piece of information has the same value to the business. There is information that, if loss, alter, disclose can cripple the business. While there is other information that has little to no ramifications. Leaders need to analyze the data entering the organization. The source of entering and how such of information is needed. In other words, why is this information been collected? Does it provide an advantage or an opportunity to the business? Only 31% of information has any legal or business value (Smallwood, 2019, para 14). How much of that 69% of worthless information is protected in vain?

In practice, information can be organized into two principles: public and private. Public information is any fact that the business has a vested interest in sharing and make known to everyone. Private information is sensitive, thus requiring more attention. There are two fundamental reasons to classify information. One is the need to know principles that indicate that an individual only has access to an object when there is a specific reason for this access. In other words, if the subject does not have a legitimate business reason to interact with this information, access should be prohibited. The second reason is that an organization needs to focus on protecting assets based on asset value; namely time sensitivity, reputation, and its core mission.

When information becomes so involved in a society that not a single business can function without it, the phenomena surpasses a mere business' activity. Picture a business without having access to information such as customer lists, procedures, financial information, transaction records, to name a few. Robert Hillard states in his book, *Information-Driven Business: How to Manage Data and Information for Maximum Advantage* "Information doesn't just provide a window on the business, increasingly it is the business. The global economy is moving from products to services which are described almost entirely electronically. Even those businesses that are traditionally associated with making things are less concerned with managing the manufacturing process (which is largely outsourced) than they are with maintaining their intellectual property" (Hillard, 2010, desc). Businesses that do not manage, and control information are buying a ticket to their own grave. Acting of government with legal fines or an adversary that compromises the organization is the effect of this lack of control. The latter is more probable than the former since any business can become a target of an opportunity.

One of the most important aspects of information governance is succinct collaboration. The notion that if everyone is committed to treating time-sensitive information like gold, the organization would be in a better position to suppress the enemy and defend compliance related matters.

David Alexander Cruz Urena, MS, CISSP, davidcruzurena@gmail.com

5. Principle III:

5.1. Clarity of Collaboration

Clarity of collaboration is achieved when everyone understands their roles and responsibilities and is committed to a specific goal. In an organization, for example, all employees and stakeholders understand the missions and objectives. Strategic direction is supported by business leaders, functional management, line employees, and everyone associated with the organization.

Information Governance must be relevant to the business direction, as to prescribe business practices acceptable to the company. Whilst these are great objectives, they can only be achieved with the active and committed support from everyone. The by-product is that information governing aligned with business valued-added services.

5.2. Culture

Information risks increase when an organization neglects to take the following steps: 1) identify all information it collects and produces 2) determine the reason for collecting or producing this data, 3) analyze the legal ramifications when that information is lost or stolen, and 4) define roles and responsibilities to protect information assets. Cultural changes commence with those who have the fiduciary duty of care to the company: Board of Directors, the Chairman, and the Chief Executive Officer. Then, cascades down, until it is communicated to everyone in the organization.

Consider issues related to current information governing strategies. Among these may include no clear direction, undefined accountabilities, unqualified roles and responsibilities, communication barriers, reactive practices, and ineffective resource allocation. Wired to think reactively, organizations ten adopt an "*if it is not broken, do not fix it"* mentality. Conversely, companies need to rethink this approach. And build some proactive measures so when something does break, fixing it is not going to cost triple (Bloomberg, n.d.), the amount that it would have cost if they did not wait until it ruined. Being proactive is a far better practice to have a resilient and sustainable business.

Often, decisions are made without clearly seeing the complete picture. Considering so many botched examples -- Target Corp, Equifax, Capital One, Anthem, and others -- in business because ineffective measures, focusing on fundamental business objectives, to bring tangible results, rather than illogical practices that are detrimental to businesses, is essential.

5.3. All-Hands on Deck

Organizations that do not embrace technology are at a competitive disadvantage. Nonetheless, incorporating technology involves certain risks. Information risks encompass the inability of businesses to continue providing services and products after an interruption. Affirming that a business is immune from a cyber-attack is as inconceivable as stating that all diseases have been cured.

All department leaders are responsible and accountable for information welfare within their respective departments. Every information assets, defined as any asset that processes, transmits, and stores information, must have an inventory.

Every business unit must participate in this program. “One of the many reasons information governance functions fail is that they do not integrate into the other organizational functions” (Giordano, 2014, para. 1). Institutions that apply information governance as a means of doing business, are going to have a far greater return on their resources invested. Ideally, governance aims to help the organization achieve its missions. By analyzing how the business operates and building strategies to ensure those business activities integrate safeguards for the information that functions depend on.

Information Governance can only be achieved with the active participation of everyone involved. The governing body must have a clear purpose of how Information Governance will be executed, beginning with a concise mission statement. An example could be, *Information, whether on paper or digital, would be protected proportionate to the value it provides to the business*. A resilient model such as the National Information Standard of Technology (NIST) is a good outline. Also, the Federal Trade Commission (FTC) publishes many articles, booklets, and other helpful resources. They release these free with complimentary shipping for those who prefer hard copies.

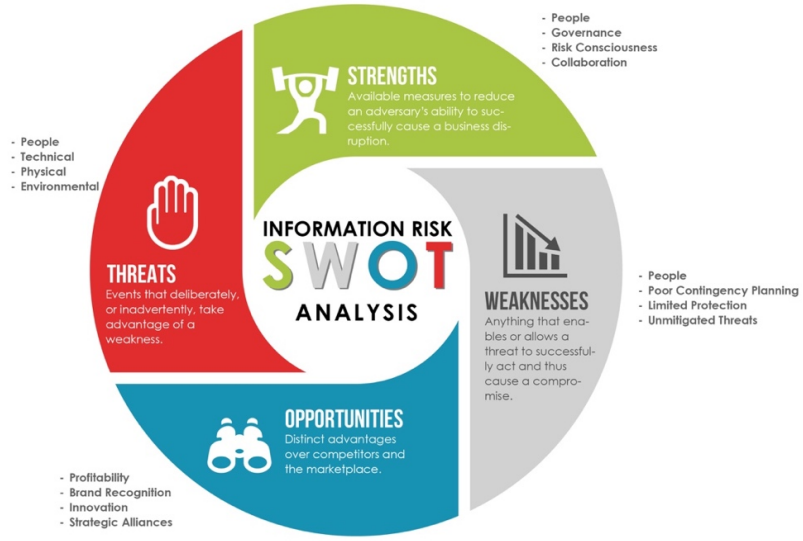
Furthermore, employee education must be received quarterly or as needed. A suitable and cost-effective standard (i.e. CoBiT, NIST, etc.) must be selected to develop documents, standards, procedures, guidelines, and baselines that support the Corporate Information Governance. All information must be classified, as either public, confidential, or internal. Information risks must be identified, assessed, controlled, and monitored. Contingency plans must be in place for each business unit according to the recommendations from industry leaders. Finally, a monthly executive report must be issued and presented to senior management.

5.4. Information Risk Analysis

An information SWOT analysis provides the strategies businesses need to balance risks and opportunities. SWOT stands for Strengths, Weaknesses, Opportunities, and Threats. It helps management prioritize. This analysis ensures the best return on investment (in terms of time). In practice, take each high-value asset and determine its actual value based on the SWOT criteria.

When analyzing information at risk, businesses can use the Information Risk SWOT framework. Strength delineates the current measures in place to organize and protect time-sensitive information. Often, organizations acquire technological solutions without understanding their current capabilities. A practice that is similar to acquiring a dog when there is already a lion presence. Other uneducated leaders buy technology services to later realize no one that knows how to use it. It is like buying a private plane without a pilot's license.

Threats can emerge from anywhere, thus it is important to identify the most probable threats. The analysis coordinates activity to classify threats based on possibility and impact. Just as humans are full of weaknesses so to organizations. Poor planning can lead to organizations focusing on lower vulnerabilities. These four elements must be analyzed holistically and programmatically. Realizing that Threats and weaknesses lower the strengths of an organization leading to fewer opportunities.



©

5.5. Governance Committee

The information governance committee constitutes top executives with diverse backgrounds and responsibilities. Members will vary depending on the industry and company size. Legal, Communication, and Audit are the key players forming this committee. Therefore, a representative from each department ought to be included. This commission established roles and responsibilities, develop policies, and ensure the organization follows the various laws and regulations associated with the institution. The committee also serves as an oversight to ensure information governing protocols are practical and actionable.

For illustration, it has been the norm in most organizations to focus on being compliant rather than being protected. In so doing, they seek to achieve compliance rather than a greater goal, which is to ensure their organizations' information assets are governed. Leading to organizations paying to comply rather than to be protected, what often happens is that an outside entity hired by the organization comes in and asks numerous questions. These questions are boilerplate and usually, have little to no consideration for the organization's mission. This is not realistic, despite the organization's risk posture. When the results are presented to management, they inaccurately depict the current state.

6. Conclusion

6.1. Further Research

Privacy regulations such as the General Data Protection Regulation, and others mentioned, will continue to be enacted. Leading to more organizations incorporating information governance in every business's function. Those neglecting to act upon the issues discussed in this study might face precarious matters soon. The world is changing drastically and unprecedented speed. Businesses that adapt will strive for the foreseeable future. Focus on the capabilities presently available, apply a risk-based approached, and ensure everyone plays a part in the solution.

Attackers will continue to innovate new strategies to circumvent whatever safeguards are placed on their way. Adapting to the reality that cowboys and guns are a thing of the past. Now computers and the Internet are society's best friend and worst enemy. Because of the same power and capacity that is used for many good things are also used for evil. And the never-ending game of good and evil continues.

Take a hard look at how many companies are no longer in business because they fail to embrace the information. Radio Shack, Blockbuster, Kodak, Borders, were among the many organizations in this category. Over the next decades, more will join this list, if they do not embrace the importance of information governance. Organizations now face new challenges, as technological advances frame businesses in general. As a result, business leaders must conclude that formalizing Information Governance is undoubtedly a business matter.

David Alexander Cruz Urena, MS, CISSP, davidcruzurena@gmail.com

7.0 References

Associated Press. (2019). Florida city pays $600,000 ransom to save computer records. Associated Press.

Bloomberg. (n.d.). https://www.bloomberg.com/news/articles/2019-08-07/cybersecurity-pros-name-their-price-as-hacker-attacks-multiply

Giordano, A. D. (2014). Preparing the Information Governance Organization. In Performing Information Governance: A Step-by-Step Guide to Making Information Governance Work [O'Reilly] (Integrating Information Governance Into Project Work).

Hillard, R. (2010). *Information-Driven Business: How to Manage Data and Information for Maximum Advantage*. John Wiley & Sons.

Hopper, G. (2005, August 21). Quotes from Grace Hopper, Computer Programming Pioneer. https://www.thoughtco.com/grace-hopper-quotes-3530092

Menapace, B. (2018, September 13). Colorado Timberline Abruptly Closes After Ransomware Attack. https://magazine.promomarketing.com/article/colorado-timberline-abruptly-closes-after-ransomware-attack/

Miller, M. (2019, August 22). Texas ransomware attacks deliver wake-up call to cities. https://thehill.com/policy/cybersecurity/458357-texas-ransomware-attacks-deliver-wake-up-call-to-cities

Perlroth, N. (2014). Hackers Lurking in Vents and Soda Machines. https://www.nytimes.com/2014/04/08/technology/the-spy-in-the-soda-machine.html

Saldanha, T. (2019). Sensing Risk. In Why Digital Transformations Fail: The Surprising Disciplines of How to Take Off and Stay Ahead [O'Reilly].

Smallwood, R. F. (2014). Information Governance, IT Governance, Data Governance: What's the Difference? In Information Governance: Concepts, Strategies, and Best Practices (p. para. 7). Hoboken, NJ: John Wiley & Sons.

Smallwood, R. F. (2019). *Information Governance, 2nd Edition* (2nd ed.). Hoboken, NJ: John Wiley & Sons.

2019 Cost of a Data Breach Report IBM Security. (n.d.). https://databreachcalculator

Vault of the Secret Formula. (n.d.). https://www.worldofcoca-cola.com/explore/explore-inside/explore-vault-secret-formula/

7.1 Framework: Information Governance

The following framework addresses information from the moment it enters an organization until it is no longer valuable.

Acquisition

- Business reason for collecting this information
- Legal responsibilities as the controller of this information
- Methods use for collecting information appropriate

Ownership

- Identify the data owner and custodial
- The individuals who are going to require access
- Any third-party entity requiring access

Repository

- Allocate the relevant repository to store this information
- Identify systems redundancy to protect this information
- Controls that need to be placed to organize and protect this information

Education

- Employee awareness should be incorporated
- Executive education must be considered
- Technical staff may need specific training

Responsibilities

- Consider the functional activities
- Analyse compliance mandates regarding this information
- Confer the underline risks associated with this data

Examine

- Conduct a gap analysis to ensure current measures
- Evaluate the current risk structure related to this information
- Suggest if this information is to be included to business impact analysis

Disposal

- The legal and organizational obligations to retain this information
- Parameters to discard this information an orderly and legal manner

7.2 Sponsors

This paper was made possible by the following sponsors.

- ECPI University - www.ecpi.edu
- RB Advisory LLC - www.rbadvisoryllc.com

Last Updated: July 4th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Amsterdam August 2020 Part 1	Amsterdam, NL	Aug 03, 2020 - Aug 08, 2020	Live Event
SANS Reboot - NOVA 2020	Arlington, VAUS	Aug 10, 2020 - Aug 15, 2020	Live Event
SANS FOR508 Canberra August 2020	Canberra, AU	Aug 17, 2020 - Aug 22, 2020	Live Event
SANS Amsterdam August 2020 Part 2	Amsterdam, NL	Aug 17, 2020 - Aug 22, 2020	Live Event
SANS Virginia Beach 2020	Virginia Beach, VAUS	Aug 30, 2020 - Sep 04, 2020	Live Event
SANS Philippines 2020	Manila, PH	Sep 07, 2020 - Sep 19, 2020	Live Event
SANS London September 2020	London, GB	Sep 07, 2020 - Sep 12, 2020	Live Event
SANS Baltimore Fall 2020	Baltimore, MDUS	Sep 08, 2020 - Sep 13, 2020	Live Event
SANS Munich September 2020	Munich, DE	Sep 14, 2020 - Sep 19, 2020	Live Event
SANS Network Security 2020	Las Vegas, NVUS	Sep 20, 2020 - Sep 25, 2020	Live Event
SANS Northern VA - Reston Fall 2020	Reston, VAUS	Sep 28, 2020 - Oct 03, 2020	Live Event
SANS San Antonio Fall 2020	San Antonio, TXUS	Sep 28, 2020 - Oct 03, 2020	Live Event
Oil & Gas Cybersecurity Summit & Training 2020	Houston, TXUS	Oct 02, 2020 - Oct 10, 2020	Live Event
SANS OnDemand	OnlineUS	Anytime	Self Paced
SANS SelfStudy	Books & MP3s OnlyUS	Anytime	Self Paced