CGOC
THE COUNCIL

Achieving Rapid Business Value and Good Governance

Table of Contents

1. Understanding Foundational Information Governance Concepts

2. Creating Business Value with Governance

3. Using Governance as an Enabler for Risk and Compliance

Introduction

For over a decade, information governance professionals have wrestled with how to adapt, prioritize and coordinate their activities in the face of a constant deluge of data, the introduction of new technologies, and rapidly evolving regulatory obligations—all while under pressure to support the corporate goal of increasing profits at lower operating costs. Even the ongoing investment in a glut of emerging enterprise solutions to “manage” all this adds to the complexity!

Forward-thinking organizations have responded by creating a C-Level executive position—the Chief Data Officer (CDO)—to build out the competency and processes for aggregating information and using it to make better decisions. Yet Gartner predicts only half of these newly minted executives will be successful, in large part due to formidable roadblocks that include resistance to change, a lack of stakeholder involvement and support, and confusion over information governance.

Often these challenges arise from a perceived conflict between deriving business value from data quickly and prioritizing governance for risk and compliance. However, based on the contributions of many members of the CGOC community, we head into 2020 with the clear understanding that these are two sides of the same coin.

We can’t prioritize one over the other. There is no sustained business value from a new data source if in doing so, privacy is compromised. And it does little good for a business to be compliant if it can’t compete. Further, even if an activity delivers value and is compliant, we still need to ensure it is ethical—if not, we may expose our company to consumer or shareholder activists and the potential for significant brand damage.

The included set of exceptional articles, webinars and blogs—developed in collaboration with our faculty —dive into these challenges, offering recommendations and strategies that can help you on your journey. We hope you will use them in conjunction with our other CGOC resources and tools, such as governance models and worksheets, to help ensure your information governance foundation will support both goals: keeping up with rapidly changing compliance demands while supporting the drive to obtain business value from your data. We hope you will find these new resources of value.

The CGOC is the only organization focused on cross-functional, unified IG, bringing together experts and insight from every discipline. Since 2004, we have developed resources and hosted events to help our members mature their governance programs and overcome other complex information challenges. Our updated Information Governance Process Maturity Model has helped hundreds of organizations understand how to improve their IG programs, and our reference guides, webinars and meetings are vital resources regularly consulted by some of the world’s top organizations. For more information on the CGOC, visit the CGOC website and consider becoming a member.

1. Understanding Foundational Information Governance Concepts

THIS BLOG WAS ORIGINALLY PUBLISHED ON THE CGOG WEBSITE ON MARCH 29, 2019.

What is the Difference Between Information Governance and Data Governance?

As a result of the need to protect data from breaches and comply with complex and evolving global data privacy regulations, we talk about "governance" more than ever, and I'm often asked about the difference between information governance and data governance.

In "Information Governance for Healthcare Professionals: A Practical Approach," which is a terrific resource even if you're not a healthcare professional, Robert F. Smallwood refers to information governance as "a complex amalgamated discipline, made up of multiple sub-disciplines." So true! In fact, data governance is one of these sub-disciplines, as is e-discovery, records and information management (RIM), compliance, risk management, privacy, information security, and data storage and archiving. This means that stakeholders—the leaders who must participate in an information governance program if it is to be successful—must come from Legal, RIM, Compliance, Privacy & Security, IT and the lines of business (including, potentially, representatives from HR, sales and marketing and even site security).

What is data governance?

For Smallwood, data governance is about data quality and security, focusing only on structured data in databases. It encompasses data modeling, de-duplication to eliminate redundant data, and data cleansing to remove corrupted, inaccurate, or extraneous data.

Another definition , is that data governance "is a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods." This definition would apply to both structured and unstructured data.

What is the purpose of information governance (IG)?

From the CGOC perspective, data governance encompasses both these definitions, and Smallwood makes an interesting and equally applicable observation that while information governance "must be driven from the top down by a strong executive sponsor," data governance's focus is "from the ground up at the lowest or root level." I love this distinction because it goes to the heart of what is required for organizations to make information governance and data governance work. In fact, if you look at the sub-disciplines of IG listed above, each, like data governance, requires a "from the ground up" effort to ensure the processes are accurate, complete and meet the specific requirements of the sub-discipline. Meanwhile, information governance is that top-down effort of coordination among stakeholders of all the sub-disciplines to make sure their efforts are coordinated, additive and based on the best possible information from across the organization. Information governance is impossible without data governance and the effort of all the other sub-disciplines. And without information governance, all the effort of data governance and the other sub-disciplines can still leave an organization with governance gaps that make it vulnerable to security breaches, compliance violations, increased costs, increased e-discovery risk and lower productivity.

Continue Reading →

AN ARTICLE FROM information management

13 Questions You Need to Ask to Close The Information Governance Gap

By Heidi Maher, former Executive Director of CGOC

I was stunned recently to see that despite constant security threats and complex, rapidly evolving privacy regulations, the 2018 Information Governance Benchmark Study found a huge gap between the perception and reality of information governance (IG) maturity.

While 81 percent of respondents report progress on IG programs and 72 percent say they have appropriate levels of executive support, 66 percent acknowledge inconsistent collaboration among information stakeholders and a continued reliance on siloed, ad hoc processes – signs that an immature IG program is leaving an organization vulnerable to regulatory compliance failures, data breaches and increasing costs.

The slow progress being made on IG is also reflected in this surprising AHIMA survey. But with IG is now a board priority, what's the obstacle to progress?

The answer is the piecemeal approach that most enterprises still take. Compliance, security, legal, records, IT and lines of business all set out their data requirements and are implementing solutions to meet them, but it's difficult for executives to see the challenges across these functions.

This lack of cross-functional coordination means enterprises remain saddled with siloed data sources, little management of data quality and lineage, few automate end-to-end data management processes, and inconsistent compliance with enterprise-wide requirements, such as the GDPR.

A culture of IG

The only way to accelerate the adoption of IG and close the gap between maturity perception and reality is creating a culture of information governance, in which all information stakeholders work cross-functionally to design, implement, monitor and mature an IG program that meets the needs of everyone.

It may be the compliance team's imperative to meet GDPR requirements, the CISO's need to decrease risk and shorten the response time to a breach, the legal team's desire to respond to an e-discovery request with the minimum required information, the marketing team's need to mine data to power new marketing programs, or the CTO trying to reduce storage and application costs.

A successful IG program enables each stakeholder to execute more efficiently and effectively toward their goals without compromising the needs of the others. A successful program must also provide access to documentation to validate the progress toward IG process maturity.

To create this culture of IG, develop a cross-functional understanding of the people, activities and solutions that constitute your IG program. To do this, be sure you can answer the following 13 questions in the affirmative. If the answer to any of them is "no," work with your peers to change them to "yes." Think of this as your IG cheat sheet. Tape it to your computer or office door to make sure you continue making progress.

The Questions

People

1. Do you understand each stakeholder's expectations regarding data? For example, do you know how fast business users expect relevant data to be delivered? Do you have an actionable plan for eliminating data silos?

2. Is the importance of IG to the organization reinforced through regular training? For example, are there regular communications regarding IG policy effectiveness and user needs? Are business users and non-IT managers educated about storage utilization and costs?

3. Does your organization take a cross-functional approach to IG? Are the right stakeholders in place for each area? Do they understand their responsibilities? Does the CTO talk regularly with legal and the lines of business? Is the CDO involved in the IG program?

Activities

4. Can you clearly state the opportunity and impetus for organizational improvements to align with maturing IG processes? Are there stated KPIs?

5. Can your organization validate that investments in new policies, processes or software tools have achieved the desired results in the context of IG requirements?

6. Can your organization classify data according to its value and monitor the cost vs. the value?

7. Can your organization monitor and document compliance with applicable laws, regulations and standards?

8. Does your organization have controlled practices regarding setting retention policies, backup routines, establishing/ monitoring user access to data – and are these practices applied consistently across the organization?

9. Can your organization identify, act on, and track risks that are not being effectively mitigated?

10. Are all relevant processes sufficiently documented, and is this documentation accessible to other stakeholders?

Solutions

11. Does IT involve other information stakeholders in its purchase decisions? Do other information stakeholders see IT as a facilitator and not an obstacle.

12. Is the technology stack capable of supporting the people and activity goals? Can you measure this? Is the current technology sufficiently agile to adapt to a changing environment?

13. Given the necessity of data lakes, does IT have a clear approach to managing data stewardship, data lineage and data quality? Does IT have the technology to support this approach?

By answering these questions, you can determine just how wide the IG perception and reality gap is at your organization. It is also the only way you can begin taking the cross-functional steps to close it.

Many organizations – 34 percent according to the Benchmark Report – have already succeeded at maturing their IG programs, and a variety of online resources are available to support your efforts. The path may not be a simple or easy one, but the potential benefits extend across regulatory and legal compliance, data security, improved business insight, operational efficiency and cost control.

By spearheading this effort, you can help drive success in all these areas – a result that will certainly be appreciated by your board.

AN ARTICLE FROM CIO DIVE

4 Keys to Managing an Information Governance Program

By Aaron Bryant, Chief Information Governance Officer at Washington State Department of Health and CGOC Faculty Member

Most organizations understand successful information governance (IG) depends on close coordination among stakeholders, including security, compliance, privacy, legal, records, IT and lines of business.

However, operationalizing this can be challenging, and I have had very different experiences and successes depending on my management role, previously as a mid-level manager and now as a C-level executive.

Over the last 14 years, I have run IG programs and designed, implemented and maintained information management systems to support them.

While I have always focused on aligning IG stakeholder requirements to ensure a mature, organization-wide IG program, all too often, the C-suite introduced an unavoidable obstacle to success, naming an executive program "sponsor" who left program implementation to a mid-level manager.

This is a recipe for failure, leaving organizations saddled with siloed, ad hoc IG processes, poor data quality and increasing vulnerability to data theft, regulatory violations and uncontrolled information management and legal costs.

A lack of hands-on executive leadership also explains this finding in the CGOC Information Governance Benchmark Report 2018: While 72% of organizations believe they have appropriate executive support and leadership for their IG Program, only 33% can defensibly dispose of data and only 7% have tools in place to categorize data and automate retention schedules — critical elements of IG program maturity.

Based on my experiences as a mid-level manager and an executive, I offer the following four management keys to successfully operationalizing and maturing an IG program.

1. A C-level executive, not a manager, must run the IG steering committee

An effective IG program requires close coordination among all information stakeholders.

In every organization I have been associated with, this coordination required a cultural evolution of people, processes and technology spanning multiple departments. Mid-level managers rarely have the authority to effect such changes.

A records manager, even an IG program development expert, is typically excluded from leadership meetings about the technologies, policies, personnel or budgets directly impacting the IG program.

A few years ago, as a law firm records manager, I controlled client data flow and processing, but I could not impose best practices on the firm's administrative data, managed by IT. This disconnect prevented me from making any real progress on moving the firm toward a comprehensive IG program.

2. Build an IG steering committee with stakeholders who fully embrace their responsibilities

The IG steering committee comprises the multi-stakeholder group charged with developing IG program strategy and implementing the necessary processes and controls throughout the organization. As such, an IG program leader must carefully select the group's members.

In my various roles as a mid-level manager, I could not do this and found many steering committee members lacked the knowledge, experience and commitment to implement our IG strategy at the tactical level.

Further, my attempts to impose IG best practices usually fell on deaf ears.

Today, as an executive, I can now bring the right people to the table, and I have the authority and flexibility to attend operational and strategic meetings across the organization, enabling me to identify the best people to accomplish my IG goals.

3. Frame IG as an essential core business function, not a problem-focused project

A few years back, as a hotel chain's records and information governance director, I was a member of the legal team.

Despite my title, a lawyer who understood only the IG issues related to e-discovery assumed responsibility for the entire IG program, ignoring the much broader experience and perspective I could have brought to our IG strategy.

As a result, I had no input at the executive level, and while we had a robust e-discovery program, a true IG program never got off the ground.

When charged from on high with managing an IG program, a mid-level manager (or a lawyer) has little choice but to treat the effort as multiple, narrowly-focused projects, that is, the next best steps for solving a specific IG challenge.

Often, these managers will also limit their projects to their immediate needs, such as the lawyer reducing e-discovery risks or a compliance manager satisfying new privacy regulations. As an executive, I have framed IG as a core business function, as critical to business operations as human resources or finance. Armed with the right authority, knowledge and experience, I can impose IG best practices throughout the information lifecycle across all departments.

4. Align the IG function with other organization-wide strategic initiatives

Without an executive running the IG program, an organization has no top-down coordination among the various IG stakeholders, resulting in fragmented implementations and immature IG processes.

Today, as the CIGO, I regularly meet with the CIO, CISO, CTO and other executives, learning about their roles, responsibilities, requirements and concerns, while coordinating our efforts and aligning them with IG best practices.

Through this effort, for example, I recently discovered the information security team was about to deal with an issue on a particular file share. Since the IG team was also looking at a project related to file shares, we were able to coordinate our activities and develop a project roadmap that delivered strategic, process and cost synergies.

At the executive level, I see far more opportunities to achieve these benefits throughout the agency than a mid-level manager could. As a result, we are making faster and more significant progress toward IG maturity.

We know that information is now an organization's most vital asset, but "having it" is not the same as effectively using it and protecting it in a compliant way.

Only a mature IG program can optimize information access while minimizing compliance and security risks. And the only way to ensure steady progress toward IG program maturity is with a focused, hands-on executive at the helm.

2. Creating Business Value with Governance

AN ARTICLE FROM Forbes Technology Council

Four Ways Information Governance Can Protect M&A Value

By Heidi Maher, former Executive Director of CGOC

While the world waits to see the potentially transformative impact of the CVS acquisition of Aetna (assuming it isn't blocked), CVS's CIO is likely thinking about the major data integration hurdles he will need to overcome to attain the value sought by the transaction.

Many other companies will face these same challenges because M&A activity is now big business. Bain & Co. estimates M&A deals totaled $3.4 trillion globally in 2018, with about half those deals involving a company that obtained new capabilities or access to new markets from the acquired business. Based on my discussions with data and information experts from major enterprises, here are the top four ways information governance can help organizations meet the data integration challenges they will almost certainly encounter.

1. Unclog Due Diligence

While due diligence is always a critical topic for M&A deals, in the past, it focused primarily on legal and financial records. Today, due diligence must encompass regulatory impact, human resources, environmental effects, customer outlook, industry reputation, internal compliance and information technology. This broader scope makes due diligence ever more challenging, as does the massive amount of data from multiple sources that must be accessed, authenticated and reviewed, which can clog the due diligence process.

To overcome this, organizations must have in place a solid integration strategy and a mature IG program that ensures cross-functional communication. Due diligence teams must also rely on advances in technology, including machine learning and predictive analytics to help them accelerate and better manage the process while providing additional security.

2. Avoid Cybersecurity Buyer's Remorse

A 2017 West Monroe survey of senior global executives found cybersecurity continues to be a major M&A issue, both before and after the deal closes, with over 50% discovering a cybersecurity issue after closing a deal. And those surveyed cited security as the No. 2 reason why M&A deals fall apart.

To avoid this, an acquiring company must extend its IG smarts to the target company in order to fully examine the target's IT and data security policies, including how the target gathers personal or sensitive information, how this data is used and stored, whether it is encrypted or otherwise protected, and when and how data is destroyed. It is equally important to understand where data is physically stored and on what systems and the types of cyber- or data-related insurance policies the target maintains.

While a primary goal of cyber due diligence is to avoid taking on potential data breach-related liability, including for those in the past, parties should understand that providing another party (such as an acquirer in an M&A transaction, along with financial institutions, consulting companies, law firms, vendors, etc.) with private customer or employee information or other sensitive data can violate privacy regulations and increase the risk of a data breach. This means every third party receiving or storing sensitive data must be carefully vetted for privacy and security policies and procedures.

3. Bridge The Cultural Divide

The CVS-Aetna deal is the perfect example of a culture clash. CVS is a retail company that processes millions of transactions for millions of Individuals. Aetna relies on corporate purchasing from thousands of corporate customers. IG stakeholders are essential to bridging this divide.

For example, to support data integration, the acquiring company must retain target company subject matter experts who know where data is located and the data habits of the employees. This knowledge is essential for successfully combining IT functions without introducing significant business disruption.

4. Clean Up Your Act

The only way to fully and rapidly benefit from analytics performed on data acquired from a target company is to make sure only relevant, high-quality data is added to the existing data lake. Following an acquisition at a bank I worked with a few years ago, executives demanded rapid integration of the new data, and they were so concerned about the possibility of losing some important information that they insisted on importing everything. However, this resulted in mountains of irrelevant and non-sensitive personal information such as vacation photographs being ingested, requiring significant time and money for a post-integration clean-up.

So it is essential not to rush. Instead, the acquiring company's IG program must be extended to the new data to ensure only relevant, high-quality information from trusted sources is integrated.

The Essential Industry Lesson

We will be watching the progress of the CVS-Aetna integration closely because the lessons learned will certainly benefit the entire industry. Meanwhile, M&A shoppers must focus on understanding all the risks associated with a target company's data. If a buyer can't use some of a target company's assets because of privacy, health care, financial or other regulations, or if the acquiring company cannot ensure only relevant, high-quality data is integrated, the future value of the deal could be completely undermined.

These data integration challenges may feel overwhelming, but companies focused on maturing their own IG programs will be in a far better position to identify the potential risks in the target company's data, enabling smarter decisions before, during and after an M&A transaction.

AN ARTICLE FROM Bloomberg Law

Ten Ways Machine Learning Will Transform the Practice of Law

By Caroline Sweeney, *Director of Knowledge Management at Dorsey & Whitney LLP and CGOC Faculty Member*

Law firms are increasingly using machine learning and artificial intelligence, which have become standard in document review. Dorsey & Whitney's Caroline Sweeney says any firm that wants to stay competitive should get on board now and gives examples for use and best practices.

When I proposed using concept clustering technology several years ago to facilitate document review in a large e-discovery matter, the idea did not go over well. Today, this is standard for document review, and we are seeing increasing consideration of many other solutions powered by machine learning (ML) and process automation.

What seemed far-fetched 10 years ago is today transforming the practice of law and delivering a return on investment for law offices and legal teams. Firms that aren't adopting or at least exploring the use of these solutions will soon find themselves at a significant competitive disadvantage.

10 Areas of Use

At our firm, we are using ML or exploring its use in the following 10 areas, and we are seeing real or potential cost savings and process improvements for each one.

1. Litigation. ML is now widely accepted in litigation, as illustrated by the acceptance of predictive coding by Courts in the U.S. and abroad. At our firm, continuous active learning (CAL) has become a standard for document review. We continue to explore how we can extend ML beyond document review to other phases of litigation like evaluating deposition testimony or conducting decision tree analysis for settlement decisions.

2. M&A. Firms are increasingly adopting ML to support M&A due diligence analysis. Instead of associates spending hours manually reviewing contract clauses, ML tools that offer automated clause extraction can do this analysis faster and far more efficiently.

3. Investigations. We use CAL to quickly and cost effectively identify key documents and generate timelines of events (e.g., financial trades). We use other analytic tools to identify communication patterns key to an investigation.

4. Information Governance. ML offers great opportunity in this area by helping to mine information residing in various repositories. This can be helpful in managing content, but also in managing risk within an organization. I expect to see this area continue to adopt ML as a necessary data management tool.

5. Privacy. Some vendors now specialize in using ML to help organizations identify personally identifiable information (PII) and protected health information (PHI) to support regulatory compliance and prevent accidental production of this information in litigation.

6. Trademark/brand compliance. We have started adapting our ML tools to help us efficiently review trademark watch notices to identify potential infringement. Although this is new, we are already seeing promising results.

7. Expert systems. Tools that capture attorney expertise related to topics, such as privacy regulations, allow us to provide clients with a gap assessment of their compliance needs.

8. Client service. Firms are using ML-powered systems to automate some client services. For example, a firm may offer a portal where clients can answer a series of questions and, using document automation, be provided with a completed document. By adding robotic automation, the document generated by the client can be routed to an attorney for review, then back to the client. Various practices, including corporate and immigration, can benefit from this sort of automation. We also use process automation for operational processes, such as a new matter intake workflow.

9. Client Collaboration. We are exploring the potential use of ML to aid a client in the legal review of marketing materials for their business. At the recent CLOC conference, one of the keynote speakers mentioned they are also exploring ML for this purpose. Dashboards that leverage analytics to present clients with information on their legal spend are also valuable collaboration tools.

10. Business Analytics. Write-offs are a fact of life for most firms. We are using ML to analyze our write-offs and understand their causes. We can then use this information to improve business processes and reduce the number and amount of the write-offs.

Best Practices

To support successfully moving forward with any of the above use cases, I recommend the following best practices.

1. Obtain executive support. Identify appropriate senior sponsors and other champions. Build the business case by laying out how ML-powered tools and services will increase the bottom line. Learn from clients and assess how you can empower your Firm to improve client processes. Get attorneys onboard by involving them in assessing tools and participating in pilots. Take small steps at a time, validate and communicate the benefits.

2. Understand the market. Identify internal opportunities to increase efficiency, automate commoditized services, and provide better access to attorney expertise. Maintain awareness of new technology but leverage existing tools wherever possible.

3. Prepare for success. Invest in personnel to focus on the process and project analysis required to develop the ML use cases. If needed, pull in third parties for expertise and services. Educate the organization and dispel the myth that ML is about eliminating jobs. It's about new business opportunities, collaboration with clients, and replacing rote work with more substantive and strategic tasks.

ML and AI are the future, and any firm that wants to stay competitive should get on board now.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Enable Governance and Value in the Information Economy

Thorough Data Cataloging, Categorizing and Mapping

Speakers:

- Amir Jaibaji, Program Director, Information Lifecycle Governance - IBM
- Candace McCabe, CIP, Expert Information Systems Architect, Information Governance - JB Hunt

Moderated by Katie Klokner – Compliance Week

ON-DEMAND WEBINAR:

Enable Governance & Value Through Data Cataloging, Categorizing & Mapping

Data is an organization's most valuable asset. Information Governance is the path to capitalizing on your investment in data. At the heart of governance is cataloging, categorization and mapping. Not knowing what data you have, where it is, how to protect it, and how it complies with laws makes it difficult or impossible to monetize this asset.

This webinar discusses:

- Reasons for mapping, cataloging and categorizing your information
- Insights on its various forms and locations
- Concerns regarding security, compliance, quality, eDiscovery and more.

WATCH NOW

3. Using Governance as an Enabler for Risk and Compliance

THIS BLOG WAS ORIGINALLY PUBLISHED ON THE CGOG WEBSITE ON OCTOBER 8, 2019.

How to Prepare for the CCPA – Here Are the Resources You Need

As many enterprises continue working toward General Data Protection Regulation (GDPR) compliance, they now face the California Consumer Privacy Act (CCPA), scheduled to go into effect in January 2020. The importance of the CCPA to U.S. businesses can't be overstated. One in eight U.S. residents lives in California, and the state has the *world's* fifth largest economy – ahead of the UK. So what happens in California doesn't stay in California. The 1970 Clean Air Act, for example, recognized California's lead in addressing air pollution, and 13 other states, about a third of the U.S. auto market, have since followed California's stricter rules. So given the potential for gridlock at the federal level, California's privacy law may well become the *de facto* standard that other states will follow in developing their own regulations.

U.S. businesses thinking about their CCPA strategy may also want to consider an important cultural shift. Consumers are far more knowledgeable about and sensitive to privacy issues today, so failing to comply with the CCPA could cause serious brand damage. This is changing the way many businesses approach privacy. Recently, premiere technology journalist Kara Swisher spoke with Microsoft President Brad Smith, who has been testifying before Congress about privacy since 1986. In this conversation, Smith emphasized shifting attitudes toward protection of privacy and the importance of the California law. Apple's Tim Cook has also said that privacy is a "crisis" and is a vocal advocate for consumer privacy. In fact, many companies are reporting that there are business benefits to approaching privacy from the strategic level.

What's the difference between CCPA and GDPR? For example, is personal information defined differently in each?

While the general purpose of the two regulations is quite similar, there are key differences, including the scope and territorial reach of each, definitions related to protected information, levels of specificity, and an opt-out right for sales of personal information. Legal and business experts have published excellent resources on the differences between CCPA and GDPR, including:

- Future of Privacy Forum: Comparing privacy laws
- Baker & Hostetler, in Practical Law: CCPA and GDPR Comparison Chart
- IAPP Resource Center: Comparing privacy laws
- DLA Piper: CCPA vs. GDPR, the same only different

How can we satisfy data deletion requests?

Under the CCPA, consumers have the right to demand that a business delete the personal information it has collected, subject to certain exceptions. The business must also instruct its service providers to delete the data. Complying with this provision remains tricky. Some of the confusion stems from the need to balance different obligations, such as a consumer's desire to have their data deleted vs. a legal obligation to preserve.

Continue Reading →

THIS BLOG WAS ORIGINALLY PUBLISHED ON THE CGOG WEBSITE ON AUGUST 2, 2019.

The Ethics of Data: Balancing Risk and Reward

CGOC recently had the pleasure of chatting with the Bloor Group's Eric Kavanaugh for an Inside Analysis Podcast on the ethics of data. Along with Collibra's Stan Christiaen and data governance consultant John Ladley, we discussed the importance of an ethical approach to data and the ethics challenges companies need to consider when they launch their data initiatives.

The following is a condensed version of the more interesting exchanges we had during the conversation. Listen to the full Ethics of Data podcast

---

ERIC KAVANAUGH: We're going to talk today about the ethics of data management. Big regulations are changing things in the world. GDPR, of course, and we've already seen the ripple effects coming out across the U.S., like the California Consumer Privacy Act, the CCPA. The bottom line is that companies have to be more responsible about how they use your data, and you have to be alerted to the fact that companies are capturing your data. Companies like Facebook are poster children for bad ethics: Even though we give them permission in many cases, it's still hard to manage. What does this mean for you, and what you can do to stay on top of your game? To start us off, Stan, tell us your thoughts about responsibility with data and data ethics.

STAN CHRISTIAEN: Cambridge Analytica brought data ethics to the headlines, especially in the context of social media platforms. Now the stories are everywhere, like about the big tech company who trained one of their chat bots on Internet conversations and it turned racist pretty quickly. Ethics brings you to morals pretty quickly, and then it gets kind of difficult. Look at the classic MIT experiment where you have to choose between a train killing one person or three people. Research has shown that you actually make a different choice depending on your culture, so there are no right or wrong answers here. Given that it's such a hot topic in this "algorithm economy," I want to talk about five things I believe you should think about to avoid these nasty situations..

Principles for Data Ethics

First, take a proactive approach to data ethics. Don't wait until somebody steals your data or you build a racist chat bot and then think about it. You can make the right decisions when you start thinking about what problems you can solve next, rather than just reacting to situations that happen.

Second, understand the journey that data makes. Data moves around. It's eaten by the AI bots. People use it in their data warehouses and the data analytics. You can put it on a USB stick. So you have to understand where it comes from and how it moves.

Third, data is not just leftovers from what you do as a business. It's active on its own. And that's why it's important to explain the value of data to the business. How can they actually make money from it? You also have to think about the risks. If you explain to the business why data's important, then also explain to them why ethics is important.

Fourth, involve a wide range of stakeholders. It's not just about the Chief Data Officer or whatever CX role it is. It's about all the stakeholders. The IT team, the analysts, even the CEO. If you're out there bringing a message about ethics and privacy, you really have to make sure that your actions match your words.

Continue Reading →

THIS BLOG WAS ORIGINALLY PUBLISHED ON THE CGOG WEBSITE ON MAY 16, 2019.

GDPR Has Changed the World, but the Full Impact Hasn't Been Felt

In early 2018, many legal and privacy experts hailed the European Union's General Data Protection Regulation (GDPR) as the most important legislation of the past 20 years. Companies worldwide panicked, terrified the slightest infractions could lead to hefty GDPR fines and serious damage to brand reputation. While this hasn't fully materialized, presentations and discussions at our recent annual CGOC Regional Meeting in New York demonstrated that companies of all sizes doing business in Europe cannot afford to be complacent.

GDPR Enforcement – Fines Are Just Getting Started

GDPR is still young and both companies and regulators are still figuring out how it should work. Companies that rushed to comply with GDPR mandates in late 2017 and early 2018 report little evidence of enforcement. For example, a survey by global law firm DLA Piper found that while the number of reported data breaches over the last year increased to over 59,000, only 91 resulted in fines.

In January of 2019, France's data protection authority, National Commission on Informatics and Liberty (CNIL), fined Google €50,000,000 for a lack of transparency and consent in advertising personalization. But in general, GDPR fines across Europe have been small and infrequent. In Germany, data protection authorities issued just 41 fines for violations of the GDPR through mid-January, and the largest single fine was about $91,000. Other notable actions involved a Portuguese hospital network, an Austrian betting site, and a German social media and chat network, but those fines were only a few thousand dollars each.

> Still, smart businesses are holding their breath in anticipation of the inevitable increase in GDPR enforcement and impact.

For example, according to the Irish Data Protection Commission, while its investigations have taken significant time, they include complaints against Twitter, WhatsApp, Instagram, LinkedIn and Apple—with seven separate probes involving Facebook. The commission expects to levy substantial fines this summer. In the U.S., Facebook anticipates a $5 billion privacy-related fine from the Federal Trade Commission.

The Surge of Global Privacy Laws

The broader impact of the GDPR is the rise of privacy regulations around the world, including Australia, Brazil, Canada and Thailand. In the U.S., the GDPR has inspired the California Consumer Privacy Act (CCPA), which takes effect in January 2020, along with a patchwork of 12 other states passing privacy legislation and Congressional movement on a federal privacy bill.

While consumers may be happy about the momentum toward greater privacy, many organizations remain confused about GDPR requirements, and only 27 percent of U.S. companies are GDPR compliant (with only 14 percent CCPA compliant).

Privacy experts I speak with lament that the country-by-country GDPR data protection agency pronouncements mean we cannot count on these authorities to offer clear guidance. Further, the potential for individual executive liability and time-consuming complaints raised by consumers and employees create significant uncertainty.

Continue Reading →

THIS BLOG WAS ORIGINALLY PUBLISHED ON THE CGOG WEBSITE ON SEPTEMBER 17, 2019.

Data Breaches: The impact and how to prevent them

Fines associated with privacy violations and misusing private data are increasing, and more regulations are coming. In January of 2019, Google was fined €50,000,000 for lack of transparency and consent in processing personal data for advertising purposes. In July, Facebook was hit with a $5 billion fine after violating a pledge not to misuse consumer data. Other well-known brands that paid recent penalties include British Airways, Equifax, Marriott International, Uber, Yahoo and State Farm.

And this is just the beginning. More substantial GDPR fines are on the way, as are new regulations.

Comparing evolving data protection regulations

California's CCPA begins on January 2020, and several other countries and U.S. states are developing their own data protection regulations. This resource lets you compare evolving data protection laws around the world, while this one from CIO Dive focuses on the U.S.

Data breaches at the heart of the problem

Despite all this awareness, data breaches are still all too common. The recent Capital One breach is one of the largest ever. Now managed services providers (MSPs) have become a favorite target, exposing their clients to an increasing threat.

Meanwhile, the cost and complexity of dealing with breaches also continue to go up, with the global average cost of a data breach rising to $3.92 million. Delta's lawsuit against its chatbot vendor highlights one of the potential legal consequences of a breach. What's worse, despite growing awareness of privacy challenges among board members, according to a recent survey, 69 percent of companies reported they had yet to create a data-driven organization. Even worse, 52 percent admitted they weren't even treating data as a business asset.

Zeroing in on the data challenge

Why are organizations struggling to protect their data and comply with privacy regulations? Because they are saddle with immature information governance (IG) processes.

Key indicators that your IG processes are immature include:

- Incomplete or inaccurate data inventory
- Little insight into data flows
- Over-retention of redundant and obsolete data
- Siloed governance of disparate types of data
- Inability to implement strong access control policies for employees
- Insufficient or ineffective use of encryption

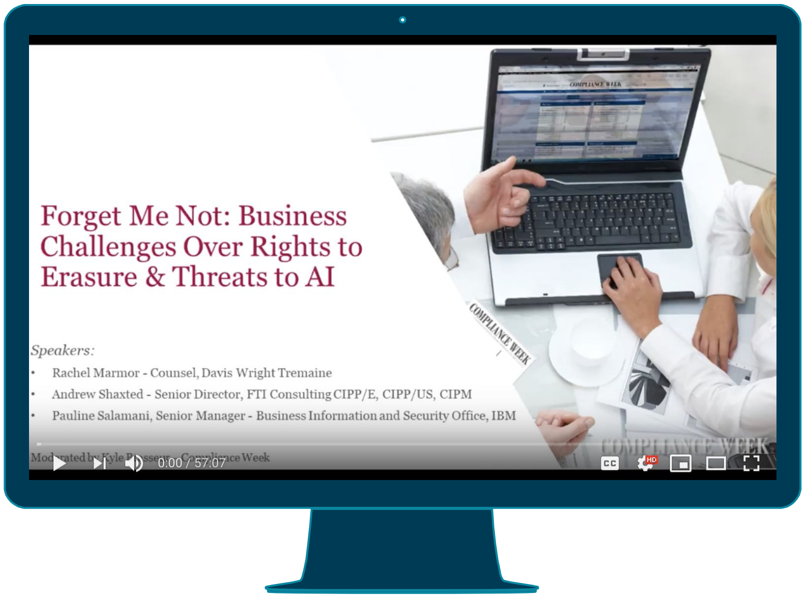
Four tips for maturing your organization's Information Governance processes

1. Recognize you can't do it alone. Collaborate with records managers, lines of business, legal and IT to ensure data is mapped correctly and governed.

2.Collect and retain only the data you need. Less information reduces risk and makes data management and data governance simpler and less expensive.

3. Make the business case to the board. The total cost of fines, damage to the brand, and getting the business back to normal following a breach can dwarf the ...

Continue Reading →



Forget Me Not: Business Challenges Over Rights to Erasure & Threats to AI

Speakers:

- Rachel Marmor - Counsel, Davis Wright Tremaine
- Andrew Shaxted - Senior Director, FTI Consulting CIPP/E, CIPP/US, CIPM
- Pauline Salamani, Senior Manager - Business Information and Security Office, IBM

Moderated by Kyle Brasseur - Compliance Week

ON-DEMAND WEBINAR:

Forget Me Not: Business Challenges Over Rights to Erasure & Threats to AI

Developments in artificial intelligence and machine learning are bringing unprecedented insight and value to the modern enterprise. At the same time, the right to be forgotten is well-established in the current and upcoming privacy regulations such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA).

This webinar discusses:

- The connection between deletion requirements and data privacy limits on data retention
- The law regarding data deletion
- The consequences of non-compliance
- The impact of compliance requirements on artificial intelligence and machine learning initiatives

WATCH NOW

CGOC
THE COUNCIL

Get Connected with Information Management Professionals Worldwide

The CGOC (Compliance, Governance and Oversight Council) provides a forum where information and data stakeholders from across organizations can gain insights into the intersection of information governance, data privacy, compliance, security, eDiscovery and records management.

Our events and resources provide members with an opportunity to benchmark their information governance progress against peers, share best practices, and develop successful strategies for solving their challenges to creating a best-in-class information governance program.

Join the CGOC Community