How information governance supports information security

As massive data breaches continue to make headlines, companies of all sizes are focusing their efforts on information security. But before an organization can put security policies and procedures in place, they need a well-crafted information governance framework to properly manage valuable data and minimize risk.

Information security is the protection of systems and assets through controls, policies, procedures, software, and hardware. The type of security measures put in place may depend on a business specialization or the focus of a particular team. Oftentimes, when areas of a business are not integrated in these security procedures, gaps in coverage are revealed which can hurt the company.

Information governance provides a framework that bridges these gaps by horizontally integrating business areas that operate in vertical silos. According to the Sedona Conference, "Information governance is an organization's coordinated, inter-disciplinary approach to satisfying information compliance requirements and managing information risks while optimizing information value."

Before an organization builds an information governance policy, it's important to consider:

- The increased complexity of emerging data privacy regulations
- The exponential expansion in volume of ESI, given the accessibility and growth potential with public cloud storage options
- Newer data forms (especially from social and mobile applications)
- Historically high activity in M&A and divestiture events
- Increased demands on compliance, security, and breach incident response

Contact legalsolutions@epiqglobal.com

Having a strategic vision, as well as understanding all of the options to protect valuable information from a possible breach, is crucial. Companies need to make sure they are implementing policies to help them defend against attacks and respond when they happen, not if they happen. Being proactive rather than reactive on privacy and compliance is key. During a time of crisis, companies should know where their information is stored and how it's organized across the network. But many businesses struggle with managing their data.

The regulatory environment

The Global Data Protection Regulation (GDPR), the EU's data protection regulation with global reach, poses many new challenges for US companies with data subjects in the EU. Organizations should know how regulators currently view the GDPR and how their business could be impacted. There are also state data protection laws, state privacy requirements, and US federal regulations to take into consideration.

As the regulatory environment becomes more and more complex, there are ways to effectively navigate it:

- Understand how your information is being generated and transmitted.
- Educate employees on regulations and simplify processes for them to follow.
- Have a chief privacy officer or chief information officer to focus on governance and regulations.
- Increase engagement with industry groups and consultants for outside expertise.
- Think global—once employees leave a company, they may not stay in the US (and global laws would apply).

Getting corporate buy-in

To get leaders to see the value of information governance, they need to understand your company's exposure. Where you're physically located is just the beginning. Many laws apply to the location of the data, not the location of the company. People often fixate on where the company has a presence, but risk may be elsewhere. Some laws require more of larger companies; often small businesses are exempt. By fully understanding exposure and potential penalties, you can better monitor where the company's data is stored and transmitted, and where your employees and retirees are located, should you need to comply with global rules.

Communicate the risks, such as the private rights of action by current and former employees or by consumers, regulatory actions by state and federal authorities, litigation hold spoliation and discovery risks, reputational risk, and cyber risks due to over-retaining data that is no longer necessary to store.

Choosing the right program for your organization

Not all data protection programs are created equal. Security measures taken should protect your specific information in your specific environment—it's a matter of scale and matter of risk. It is important to assess your company's data, understand the information you need to protect, and comply with the law. Is your data subject to GDPR requirements, HIPPA controlled, confidential or propriety information? Knowing the legal requirements is crucial to making sure that your information governance structure covers both regulatory and contractual requirements.

Large companies seeking rigorous security measures may rationalize a business case to invest in sophisticated platforms and data infrastructure due to:

- Sensitivity of data
- Risk of sabotage
- High cost of manual maintenance
- Brand risk
- Cost of recovery

Managing information governance

Before taking steps to protect data, create a records retention schedule to reduce the costs around storing unnecessary data. This ensures records are protected and reduces litigation and government enforcement discovery risks. It also minimizes exposure and helps companies create a data classification structure in which records can clearly be labeled as low risk or high risk.

Keep in mind, migrating your company's information to the cloud as part of this process means you are shifting the custodial residence of your data to a 3rd party provider. Depending on service provider you choose to work with in housing this data, you can be exposed to more or less risk. Therefore, it is imperative to know where your data is, what is housed externally, and how it's being transferred back and forth so you can quickly recover it from a breach or potential data loss.

A compliance plan should take into account information governance regulations and requirements, manage training of employees; establish measurable actions for every year; and annually assess risks and performance. Having a compliance plan in place allows you to view a problem across the company and disciplines. Consider:

- How can employees use information or a lack of information governance to be an insider threat?
- Why would they use this information?
- What pressures could they be under to use it?

Companies can protect themselves from an internal threat by determining who has access to certain information and why. Compliance plans can further establish controls by using Cyber Protection tools, Document Retention Tools (requirements and action items to manage information that is cloud and software based), and destroying unneeded records per the records retention plan. Additionally, educating the workforce helps organizations identify "at risk" employees to ensure training is targeted.

Technology to shape your information governance program

Technology isn't the "silver bullet" or simply a box to be checked. While it is needed to facilitate the information governance process, it's not the overall solution. Before kicking off a new program or enhancing your current program, outline your objective for the technology solution. There are many tools to manage an IG program, but implementation is only successful once you understand your data and outline your goals. Start with the basics:

- What data do you have?
- Where is it?
- How long do you keep it and how do you get rid of it?
- Is it documented?

There are many technological solutions, including:

- Document/content management
- Records management
- Data classification (this aids in other solutions like content management and records retention)
- Data governance/data privacy
- Data migration
- Imaging (digitize hard copy docs – can outsource this)
- Archiving

When bad things happen

Even companies with the most rigorous data governance programs and response protocols can still find themselves in a dire situation. When faced with a breach, quick diagnosis of the problem is critical to controlling the situation.

- It is the controller duty to report within 72 hours under certain conditions.
- Describe the nature of the personal data breach, including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned. If you have a full breach or an investigation for sabotage, you need to know what data was compromised, which goes back to having data classification in place up front and knowing where your data lives.
- Identify a data protection officer within the company for the authorities to contact for updates and communications. Provide the name and contact details of the data protection officer or other contact point where more information can be obtained.
- Describe/understand the likely consequences of the personal data breach (Were social security numbers taken?)
- Have a protocol in place (a checklist within legal or IT departments) to mitigate personal effects of a data breach. For worst-case scenario planning, think about how data could be used if it got into the hands of a competitor and what it means for the company. By thinking ahead, your legal department can be proactive on protecting the company. Understanding what the different breaches might look like and mapping out the protocol will help when the situation occurs and keep everyone aligned.
- After determining what data is in play, decide who to contact—a regulatory authority, law enforcement agency, the public? Determine if your corporate communications team needs to make an announcement about the response.
- Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including measures to mitigate its possible adverse effects. Damage mitigation is only effective if the data classification and records retention has been done.
- Throughout the process, be sure to document every action thoroughly to demonstrate what you did to legal and regulatory authorities, as well as learn what could have been handled better, or what you did well.

People. Technology. Performance.

Future trends

- We are likely to going to see the GPDR continue to grow and evolve, with more companies having penalties imposed. This will force some of the smaller companies to have data protection officers to ensure they aren't part of headlines, too.
- The California Consumer Protection Act (CCPA) is paving the way for more privacy laws and regulatory legislation globally.
- Businesses will increasingly use artificial intelligence to add value to their data by building from information they already have.
- Due to rapid digitalization, data is growing exponentially year after year. Data loss prevention technologies will increase.

Protecting data and getting information governance right is a coordinated team effort. To mitigate risk, tackle the issues collaboratively. It should be a cross-functional team effort that includes legal, compliance, IT, HR, pricing, contracts, procurement, finance, and executives. While it requires a certain skillset to understand the rules and technology, getting the internal politics right is a huge part of the process. Everyone in an organization can play a role in exercising their information governance muscles, ultimately strengthening how a company responds, recovers, and improves their strategy.