How Information Governance Supports Protecting Business Operations in a Time of Increased Cyberattacks

A Whitepaper by

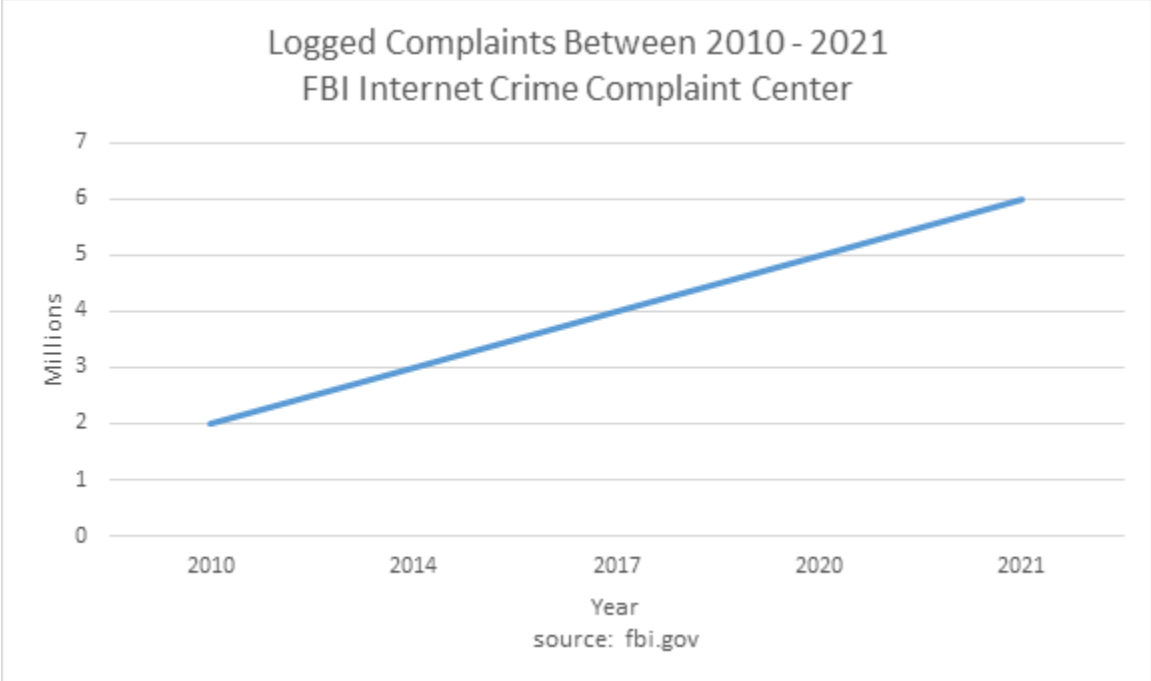
This article is for general information and does not include full legal analysis of the matters presented. It should not be construed or relied upon as legal advice or legal opinion on any specific facts or circumstances. The description of the results of any specific case or transaction contained herein does not mean or suggest that similar results can or could be obtained in any other matter. Each legal matter should be considered to be unique and subject to varying results.

It Happens Anywhere, Everywhere, at any Time

We've all read the headlines – ransomware attacks, data breaches, and other cyber-attacks are getting more sophisticated, impacting more people (directly and indirectly), and are seemingly becoming ubiquitous worldwide. While businesses have been working aggressively to counter cyber threats and data breaches for some time now, the recent wave of high-profile cyberattacks highlight the need for corporate executives to address data security at an enterprise level.

Rising Impact of Cyber-Events

The C–suite is well-advised to be concerned about cyber crime. First, data breaches are occurring at an alarmingly high rate in recent years – and increasing exponentially. According to the FBI's Internet Crime Complaint Center (IC3), on May 15 of this year 6 million crime complaints were logged into the system (see IC3 Logs 6 Million Complaints). To put that in to perspective, in November 2010 there were 2 million complaints, in 2014 3 million complaints, in 2017 there were 4 million complaints, and in March 2020 there were 5 million complaints logged with the IC3. Across the U.S. and in Europe, cyber threats are omnipresent.



(url: https://www.fbi.gov/news/stories/ic3-logs-6-million-complaints-051721)

Second, the sophistication of the cyber threats has also increased; just look to the "SolarWinds" attack on government agencies. Nationally and globally, ransomware has been identified as one of the biggest threats to people and businesses. Only last month, the White House issued an open letter to corporate executives and business leaders with the subject line "What We Urge You to Do To Protect Against The Threat of Ransomware," that stressed how ransomware has

become a threat to core business operations. Indeed, cyber-attacks are costly to a business. IBM produces an annual analysis of the state of data breaches, Cost of a Data Breach Report, which estimated that a breach costs a business 4.24 million dollars, up from 3.86 million last year (see "How much does a data breach cost?").

The Nature of Breaches

These days' data breaches are fairly well understood. A cybercriminal penetrates a data source and extracts sensitive information. Data can be illegally obtained by accessing a computer or network, or by bypassing network security remotely. Some of the most common types of cyberattacks are ransomware, malware, phishing, and Denial of Service (DOS). Organizations are most commonly targeted by ransomware. Overall recent data breach trends indicate that there is a shift away from mass attacks seeking consumer information toward attacks that target businesses using stolen logins and passwords. However, this shift does not necessarily mean a drop in the number of individuals impacted. The ransomware attack on Colonial Pipeline impacted people throughout the East Coast of the US. Since ransomware is so prevalent among businesses, experts have identified some specific ransomware trends:

- Exploitation of IT outsourcing services
- Greater attention towards vulnerable industries
- New evolving ransomware attacks (and defenses)
- Spread to mobile
- RaaS is increasing (Ransomware-as-a-Service)

Relationship between Information Governance and Data Security

So, how does data security relate to records management and information governance? At Cadence Group, we would argue that information security must evolve to incorporate records AND information management; organizations need to focus on the state of ALL information (record or otherwise) stored 'behind the walls' of the organization, i.e., all information in the organization's purview.

Data quality and compliance are very much interconnected. Indeed, those unfamiliar with information governance might not realize that cybersecurity (or information security as it is sometimes called) is an aspect of a good Information Governance programs. Organizations process personal information, such as Protected Health Information (PHI) and Personally Identifiable Information (PII), as well as, utilize sensitive customer or corporate information using different processes and systems. As such, organizations need to take a critical look at how they are managing these data assets – and where potential vulnerabilities exist. For example, many organizations are not able to quickly identify where PHI and PII are housed, and many more are unable to identify policies and procedures to manage that data. Every enterprise has a unique footprint and it should balance access, cost, and risk according to its business needs. Consider that keeping more sensitive data than necessary increases the severity of a breach. The enterprise's objective should be leveraging its information assets (for its business needs), while satisfying its compliance requirements and increasingly important, controlling risks of unauthorized access/disclosure of that asset.

Many have heard the phrase that “data is the new oil” and so we cannot blame organizations for collecting data; even mom and pop shops track their clients’ shoe size and preferences. Businesses have genuine purposes for tracking consumers, such as sending emails with links to online sales, and the data brings profits as well. Since organizations are collecting, processing, and utilizing a lot of data they are well – advised to consider the implications and proceed with caution.

To understand the intersection of Information Governance, cybersecurity, risk, and compliance consider an analogy. An organization can be thought of as a small, busy town with various roads, buildings, and parking lots. The cars entering and moving throughout the vicinity are the information assets (or data). A “traffic cop” must manage the “traffic flow” of the cars, so that they move throughout the town safely and guide them in the best direction, as well as store them in the appropriate parking lot. The concepts of information governance (7 key areas: authorities, supports, processes, capabilities, structures, infrastructure, and steering committee) can guide the cars and ensure they maneuver around the town safely and efficiently. The roads are the “infrastructure”, and the “traffic lights” and “road signs” are the structures guiding the cars (data/information assets) on their journeys. As the cars move and navigate throughout the town they should drive cautiously and always have a plan, or from a organization perspective address information risk using readiness and compliance tools. Moreover, the Information Governance professional provides value to the organization by helping to manage the “traffic flow” ensuring that business requirements, implementation plans, and processes and procedures have the appropriate “traffic lights,” “road signs,” “parking lots,” and “navigational systems”.

Shared Goals

So, what is the connection between Information Governance and cybersecurity? Simply put, they have shared goals. As alluded to earlier, we are in an age of data leaks, breaches, and cybersecurity threats and so organizations must take key steps and precautions to protect the information within the enterprise. IBM describes cybersecurity as the “practice of protecting critical systems and sensitive information form digital attacks” (What is cybersecurity?). Data privacy compliance requires identifying, classifying, and documenting internal and external PII. Before proceeding data quality should be addressed. Data quality is a measure of how complete, accurate, and timely the data is residing within an enterprise’s infrastructure. The best approach is to integrate data quality efforts with data governance and data catalog initiatives. Governance can streamline the centralization of data quality efforts, setting controls on different systems to validate data quality for compliance and ensure the accuracy and integrity of data.

An Information Governance program should incorporate the following attributes:

- **Integrity**- Information generated by or managed for the organization has a reasonable and suitable guarantee of authenticity and reliability;
- **Protection**- Ensure a reasonable level of protection to records & info that are private, confidential, privileged, secret, classified, or essential;

- **Access**- Maintain records and information in a manner that ensures timely, efficient, and accurate retrieval of needed information to business continuity or otherwise require protection
-

And the goal of Cybersecurity is to ensure the protection, integrity, and availability of an organization's most important information assets. A robust Information Governance program and the proper management of records and the information lifecycle drive and make cybersecurity possible. Information Governance, together with traditional Records and Information Management, support risk mitigation by determining where information/data resides, its value, and how to manage it through the lifecycle. Cybersecurity measures are implemented to prevent and when necessary attack digital threats. Data breaches are costly financially and when word gets out that an organization has suffered a data breach it might have to manage reputational harm, especially when large amounts and/or sensitive information is exposed.

Robust IG Programs Support Effective Cybersecurity Programs

From an Information Governance perspective, cybersecurity must focus on the organization's most critical assets. An organization should identify its risks and eliminate threats from all vantage points. To optimize cybersecurity measures, consider the following:

- data loss prevention
- vulnerability management
- training and awareness
- network security
- application security
- mobile security
- incident and event management

Begin by manifesting an approach to information security; and since some type of cybercrime will likely threaten your organization realize that the goal is to minimize breaches and to respond efficiently. When implementing a robust Information Governance program with cybersecurity, an organization should determine its greatest threats, identify all risks, and data. For example, sometimes breaches result because of an insider threat when an employee impacts security unintentionally or maliciously. This could be a significant threat to your organization. To mitigate that threat, at an enterprise level the organization should educate its employees on cybersecurity best practices.

We recommend a few initial measures:

- Point-of-Contact: Appoint security point-of-contact inside your organization
- Access: Apply sufficient access controls over information
- Communication: Document and disseminate your policies
- Test and Fix: Identify vulnerabilities and optimize efficacy
- Data: Categorize data based on organizational Value and Apply Cyber Hygiene

Once a fundamental infrastructure is in place within the organization there are "before the breach" actions and "after the breach" actions that should be strategized. Any organization, large or small, would be wise to employ the proactive Information Governance measures discussed below, modifying them to suit their needs, and then having mitigation steps in place on how to proceed if/when an incident may occur. Information Governance actions to take (before a breach) include:

- Set conditions to minimize retention of stale data and ROT (Redundant, Obsolete, Trivial);
- Identify and document the value for information assets, balancing risk, efficiency and profit/use;
- Map employee access needs by role and need-to-know;
- Identify collaboration stakeholders who may need to access all or part of the information asset;
- Standardize retention and destruction and enforce implementation of the standard;
- Identify accountability and regulatory requirements that must be incorporated into your management/protection activities

From a privacy perspective, privacy professionals have a few recommendations to stay ahead and be privacy compliant:

- Pay Attention: new state privacy laws (IL Biometric Information Protection Act, CA Consumer Privacy Act, VT)
- Identify your *unique footpri*nt- focus on what matters most for your organization (i.e. data collection, controls, obligations) and operationalize privacy tools (i.e. data mapping and privacy impact assessments
- Right – size the risk profile – apply a technical and legal lens
- Be prepared to respond – backdoor and front door breaches are a reality, some might argue that a cybersecurity program is the last line of defense; governance activities (i.e. documentation of security procedures and practices demonstrate reasonableness of security program and can help mitigate legal consequences for the business
- With the emerging data privacy landscape – data protection risks must be connection to the security agenda

However, even with all of the measures above in place a data breach can and (will) occur. How does this happen? Recall the Clearview AI data breach in Spring 2020. The company notified its clients that it had experienced a breach in early 2020. It is what some call a "front door breach". What was the Clearview AI breach about? Systems were working as designed. Data about customers was accessed, but according to the company neither its systems nor its network were hacked. The liability was due to the authorized sharing of data with an undeclared third party, and without consumer consent. This is just one example of modern data breach, which occurred at the "front door". IAPP hypothesizes that this breach was due to poor data protection and ignoring privacy commitments. So, why should organizations care? Whether a breach occurs

within the U.S. or globally an organization can be struck with a government fine upfront, face legal obligations (orders and fines), and reputational damage. For instance, Facebook was fined 500,000 pounds by the British Information Commissioners Office (ICO) for its role in the Cambridge Analytica scandal when it did not protect its user's information and failed to be transparent about how the data was collected by others.

If a data breach occurs in your organization, it is imperative to take action right away. We offer, a few general suggestions are clear from an Information Governance perspective. Begin by using the records retention schedule and information mapping to determine the scope of the data breach. This will also speed up reporting to affected stakeholders and facilitate the ability to recover from the breach. If the data breach was ransomware, then having documented backups can allow quicker restoration of data.

Conclusion

It has become an accepted axiom to say it is not if, but when a cyber-attack will hit your organization. So, be proactive and address cybersecurity now rather than after an event. A key aspect that can support a sound cybersecurity approach is with a robust Information Governance Program. Cadence Group assists public and private sector organizations in achieving their Information Governance goals, including enacting effective information security measures to assist them in meeting their cybersecurity and Information Governance goals. To learn more, visit www.cadence-group.com, or contact us at info@cadence-group.com.