Information Governance Insights

David White
DIRECTOR
AlixPartners

Collected Columns
from
METROPOLITAN
CORPORATE
COUNSEL

About the Author

David White, a director with AlixPartners, has for more than 20 years helped large corporate clients, law firms and government agencies manage crises such as data breaches, complex litigation and regulatory investigations. His unique blend of legal experience, consulting expertise and technological acumen make him a widely sought after advisor on a broad range of issues, including information lifecycle governance, data privacy and security, e-discovery and litigation analytics.

A former commercial litigation partner at an Am Law 100 firm, David is registered to practice before the U.S. Patent and Trademark Office. He is a certified Six Sigma Green Belt and he uses Lean Six Sigma project management methodologies to develop cost-effective and efficient security, privacy and e-discovery protocols. He is slso a Certified Information Privacy Professional (CIPP/E/U) by the International Association of Privacy Professionals (IAPP). His column, Information Governance Insights, appears monthly in Metropolitan Corporate Counsel.

David can be reached at dwhite@alixpartners.com.

Contents

These columns appeared in editions of *Metropolitan Corporate Counsel* throughout 2016-2017. Footnotes can be viewed online at www.metrocorpcounsel.com

METROPOLITAN CORPORATE COUNSEL

AlixPartners when it really matters

Information Management Is Asset Management

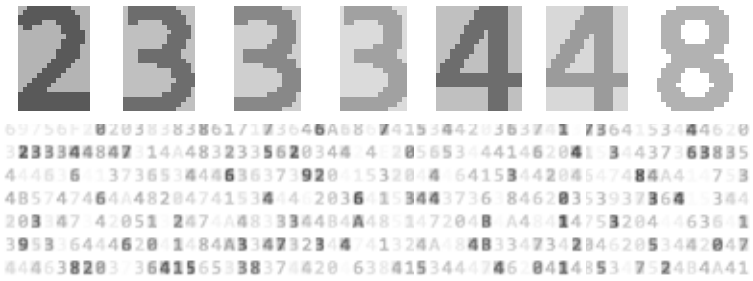
Information management is no longer just an administrative service. It has become an organizational endeavor in asset management and compliance. The columns collected in here explore the impacts of unchecked data growth on corporate compliance and review the steps that can be taken to significantly reduce compliance risk.

Most companies have struggled to dispose of unnecessary data accumulated over the last decade and find themselves retaining excess data, applications, servers and backup tapes that no longer have any utility and significantly add cost and risk to the company. Even though a company may have a long-standing records management program, these programs traditionally rely on a complex classification scheme and voluminous schedules, which can be very difficult for employees to interpret and apply. Such programs also typically fail to extend to electronically stored information, which may be governed by a separate set of policies and procedures. This disconnect results in considerable overgrowth in the volume of data being stored and managed, an elevation of overall IT costs, and a corollary increase in the costs and risks for information security and electronic discovery programs.

Much like IT costs, e-discovery costs are largely a function of data volume. As volume grows, it outpaces the IT and storage budget, overwhelms governance processes, and creates operational complexity that, in turn, increases compliance and financial risk. The more data that must be identified, collected, processed and reviewed, the greater the overall expense. Excess e-discovery costs can also lead to poor settlement dynamics by overshadowing the value of litigation, while lack of insight or visibility to true e-discovery costs can lead to late settlement decisions and excess run rate costs. Excess data also increases production timelines and the risks of inadvertently missing key evidence, both of which can result in sanctions. Historically, keeping more data was perceived as an effective risk mitigation strategy by counsel, but for most organizations, this is no longer true.

Similarly, unchecked data growth appreciably impacts information security programs. Much of the data stolen by hackers was orphaned, left sitting on file servers and nobody knew was it out there. These may include spreadsheets with payroll information or passwords saved by former employees, or copies of personal, health, financial, or proprietary information that has been derived from secure systems but is now unmanaged on an abandoned SharePoint site. The increased volumes also proportionally increase potential litigation damages which are often calculated by record counts. Media headlines commonly use the same counts as a means of reporting magnitude. Retaining old, obsolete and redundant records within a company's data systems increases both the potential legal and PR exposure should one of these systems be compromised.

CHAPTER 1



Data with a Difference

Today's headlines are filled with the news, stories and predictions of the power and value of big data analytics. Most companies are scrambling to develop new ways to monetize their information assets. Yet often, big data seems to be falling off the radar when it comes to legal and risk compliance. As big data becomes operational, it needs the same governance disciplines that we apply to traditional data management. Unless compliance managers fully understand what makes big data different from traditional business analytics, and how these differences impact the way we approach big data governance, they will not be able to successfully govern them. This understanding can also help inform us as to how we can make big data platforms work to our advantage to reduce overall risk.

Contrary to common misunderstanding, big data does not simply refer to bigger database systems nor to business analytics efforts that leverage larger data sets. Big data projects often share these same attributes, but they neither define big data nor distinguish it from traditional relational databases. Beyond the technology itself, the primary distinction that sets big data apart is the way that information is ingested into and stored by the platforms. Traditional databases are highly structured systems based on interrelated tables of predefined fields. To work, data must first be made to conform to this known structure and be shoehorned into it using a process called extract, transform and load (ETL). Having been initially built as a solution for searching the Internet, big data platforms do away with this necessity. Instead, they are able to ingest massive amounts of raw data, much of which has no preexisting need or use, in just about any format it comes in. Structure isn't applied until the analysis phase, which changes the approach to extract, load and transform (ELT).

Big data requires that we appreciate what differentiates it from traditional data analytics.

This single distinction of loading data before transforming it has massive consequences for information governance and privacy compliance. ETL allows you to work within a predefined environment where the tables and fields holding sensitive or regulated data, such as PII, are known and easily located. This lets you wrap proper controls around them. With massive amounts of raw data being ingested through ELT, often from real-time data feeds and a variety of internal and external sources, the content of the data remains unknown until analysis is conducted, and then only within the scope of that analysis. This results in large data pools with little understanding of what is in them or what compliance obligations attach. The distinction also leads to a wide array of predictions and conclusions that were previously impossible, and that are based on new and often unknown sources of information. This very point is what prompted the Federal Trade Commission to issue guidance last month on what uses of big data could run afoul of consumer protection laws.

Big data does not need to be a big headache. It just requires that we appreciate what differentiates it from traditional data analytics, and how these distinctions impact our compliance programs. It also requires counsel to get involved during the early program design phases and build privacy and compliance in from the start. Successful work with big data begins with having a clear understanding of the data being ingested and ensuring that the analytics layer includes a compliance component for masking, anonymizing and otherwise securing sensitive data as it comes into the company. The saving grace is that big data is inherently suited to do just that. It just needs the right stakeholders involved to ensure that it is done right.

Vendor Security Certifications: Is Your Data Safe?

Data breach headlines are putting more pressure on corporate counsel to ensure that the company's data is properly protected. This includes data managed by third party vendors, which have been spotlighted by the large number of breaches resulting from the exploitation of a vendor's vulnerability. Both the Target[1] and Home Depot[2] hackers gained access to the companies through their service providers. This left the latter with a breach of about 56 million customer payment card accounts and 53 million email addresses. The list continues with upward of a third of all breaches occurring through vendors or affiliates.[3] It is no wonder controlling vendor risk is moving toward the top of board agendas.

Controlling vendor risk is moving toward the top of board agendas.

To address this risk some companies now require vendors to demonstrate that they have appropriate security controls in place. To overcome the burden of monitoring compliance, many also require certification to a particular standard by an independent auditor, typically in alignment with the company's own internal security requirements. Vendor certification may also be required by other governing frameworks. The most common among these include Health Insurance Portability and Accountability Act (HIPAA) assessments, the American Institute of Certified Public Accountants Service Organization Control Reports (SOC 2), the Payment Card Industry Data Security Standard (PCI), and/or ISO 27001 certifications. Similarly, Securities and Exchange Commission Guidance requires that companies not only disclose material cybersecurity events when they occur but also disclose material risks that could occur.[4] For those companies that outsource functions with material risks, the Guidance requires a description of those functions and how companies address the risks.

The biggest challenge for everyone receiving attestations from their vendors, however, is the question of adequacy. Not all certifications are equal, and some appear to be mismarketing them. Companies need to carefully consider certification claims – for example, they may boast of Type II SOC 1, SOC 2, SOC 3 and ISO 27001 certifications for new data centers. Yet, a closer look could reveal that the vendor is simply using a third-party data center that is so certified, as opposed to the vendor's controls being certified. Using a certified data center means those certifications apply only to the level of controls available at the center itself; it does not mean the vendor is applying these standards to all of its own physical, technical and administrative controls deployed across all its processes and workflows. This difference is especially important in an era of rising cyberthreat levels. Just as the best safe in the world is useless if left unlocked, the most secure data center offers little security if the credentials that allow access aren't properly managed. It is also meaningless if your employees' laptops aren't locked down, or they routinely use portable media without proper encryption. It's imperative to dig past these statements and closely examine the actual controls deployed across their entire operation.

This is particularly critical in the age of rising cybersecurity events. Once a public company has outsourced a data processing function to a vendor and that vendor experiences a security incident, it can create a material issue for the company that must be disclosed. The company will then be required to defend itself against a claim that it should have disclosed the (now apparent) material risk associated with the original outsourcing decision. The fact that the company did as much due diligence as possible, including selecting a supplier that was certified to acceptable standards, and subject to ongoing certification audits, could be the best defense in such circumstances.

CHAPTER 3

Data Laws May Limit Globalization

The confluence of globalization and digital transformation presents many new compliance issues for in-house counsel. One such challenge comes from data localization requirements. As companies become more global, they are also beginning to leverage information to create value in a variety of new ways. From collecting more accurate and detailed performance data to profiling customer needs and influencing decision-making in order to develop or improve products and services, data analysis is helping companies facilitate growth and open up new frontiers for increased revenue. But both the globalization and the digital transformation of business operations require that information flow freely around the world.

An increasing number of governments have enacted new regulations restricting the flow of information across their borders.

With this global growth comes an increasing number of governments that have enacted new regulations restricting the flow of information across their borders. Mainly driven by purported concerns over privacy, security, surveillance and law enforcement, many countries have recently imposed data localization requirements. Unlike the prior generation of censorship controls that typically sought to keep information out of a country, such as the Great Firewall of China,[1] these new data localization controls typically seek to keep data in.

One example is a set of recent amendments to Russia Federal Law No. 242-FZ that went into effect in September 2015. With limited exceptions, this law now generally requires any company that collects personal information pertaining to Russian citizens to "record, systematize, accumulate, store, amend, update and retrieve" such data using systems physically located in Russia.[2]

Similarly, the government of Vietnam recently promulgated several draft laws that included data localization requirements as well as other restrictions on cross-border data transfers. The localization components were eventually shelved. However, as written, they could have potentially required every digital service or website offering services in Vietnam to locate at least one server within that country.[3] The Chinese government also has been considering more regulations with increased localization efforts. The vague State Secrets laws have prevented the removal of certain protected information for several decades.[4] But recently, multiple regulations have been enacted in China that appear to prevent the removal of certain banking,[5] financial,[6] and personal health information[7] from within its borders. Restrictions in other industry sectors in China also appear to be under consideration. Most recently, a draft counterterrorism law was circulated in 2014 that, if enacted in its original form, could have potentially required business operators in the Internet and telecommunications sectors to store data on servers in China and provide encryption keys to public security authorities.[8] While this law was passed without these localization requirements, the possibility of laws with similar restrictions being passed in the future still remains. The list of countries that have data localization laws under consideration,[9] or that have recently enacted or considered them, continues to grow around the globe.[10]

Inevitably, the collection and usage of customer personal data brings about challenging questions regarding data protection and usage. As companies expand their markets and move to digitally transform their operations, they must fully consider both the sources and subject matter of the data they are collecting and the various laws and regulations that apply to them. Privacy laws are typically triggered by the residence and nationality of the data subjects, not simply the location of the data or its collection activities. The questions can be complex, but to avoid compliance gaps, company counsel should begin making the effort to map their data supply chains, fully understand their contents, and align them with the privacy laws of each jurisdiction they may implicate.

CHAPTER 4

How to Rob a Bank in 10 Easy Clicks

Bank robbery used to be a very simple affair. All you needed were a few fast horses, a handful of men or women who were quick on the draw, and some black hats and bandanas to hide behind. Since these attacks were purely physical, banks had simple defenses. Strong vaults and locks kept the money relatively safe. In today's world of digital wire transfers, real-time trading, global financial markets and online payment systems, the rules have changed significantly. Building physical or virtual walls around valuable assets no longer guarantees that criminals are kept out.

Cybersecurity is no longer an IT problem. It should be viewed and treated as a business problem.

This is made clear by the recent hack of the central bank of Bangladesh, which nearly resulted in over $1 billion being siphoned out of the country's accounts. This attack had likely been going on for several years and was only discovered when a spelling error by the cybercriminals in one of the transactions triggered suspicion. While the Federal Reserve Bank of New York, where Bangladesh Bank has a current account for international settlements, blocked most of the transfers, about $81 million ended up in the Philippines, where it will likely go unrecovered after transfers to casinos and offshore gambling sites around the world.[1] It still remains unclear how the culprits got into the country's central bank, or how they were able to manipulate wire transfers using the central bank's Society for Worldwide Interbank Financial Telecommunication (SWIFT) accounts with banks in the U.S. What's clear is that the attack was both highly sophisticated and complex. After all, the SWIFT system is considered to be one of the most secure systems in the world, with end-to-end encryption and dedicated communication channels.[2] And it looks like this is likely not the end, as several similar hacks involving SWIFT are just now surfacing.

It's not the first time this type of advanced persistent threat (APT) has hit the banking industry. In 2014, the Carbanak hack infiltrated upwards of 100 institutions across 30 countries and resulted in nearly $1 billion in losses. Like the Bangladeshi attack, the Carbanak attackers were slow, methodical, and patient. It's estimated that they spent an average of six months inside each victimized bank. They used malware and email phishing attacks on targeted employees to gain access to their workstations. Once inside, they methodically escalated user credentials, infecting hundreds of machines, ultimately working their way to the payment administrators. They also exploited computer video cameras and microphones to watch clerks' screens and work habits so they could be mimicked to reduce suspicion. Once in, they inflated account balances and siphoned off the surpluses, infiltrated ATM systems and forced them to dispense cash to mules, and leveraged online banking and e-payment systems to transfer funds.[3] The Bangladeshi hackers seem to have used similar techniques, but they went even further and erased the transfers they initiated in order to hide their tracks.[4]

The level of sophistication of these hacks make it clear that fortifying banks and other critical infrastructures with hardened firewalls and malware scanners can no longer be the first and only line of defense. Financial institutions should take a more holistic view of data security requirements. Those can be managed by a comprehensive information lifecycle governance framework that includes clear roles and responsibilities, geographic compliance requirements, asset inventory and reporting, data classification and handling, and next-generation technical solutions, such as network analytics and risk fusion centers.

One key element of a solid information life-cycle governance framework is the identification of data flows inside and outside the organization, then mapping them to the organizational control environment. A risk assessment should then be conducted to identify control gaps, and an implementation road map should be developed to mitigate risks outside the organization's risk appetite.

Cybersecurity is no longer an IT problem, solved with IT tools alone. It should be viewed and treated as a business problem addressed with business tools by the board, with a unified plan across the enterprise. Otherwise the bank robbers will continue riding off, uncaught, into the sunset with no trace left behind.

CHAPTER 5

Caring About Cloud Migration

Information technology departments across all industries face enormous pressure to control costs and reduce their budgets. At the same time, they're coping with the massive growth of data to store on IT systems and data servers. This had led to a mass migration of data to cloud-based storage systems run by third-party service providers. These systems differ from traditional hosted storage, where data is simply moved onto discrete servers owned and maintained by a service provider. Cloud-based systems fragment data across large collections of servers that are often spread out across different locations, sometimes on a global scale. These cloud-based systems add to the complexity of privacy, risk and security compliance concerns that are raised by any movement of data from company control to that of a service provider.

Cloud-based systems add to the complexity of privacy, risk and security compliance concerns.

One particularly problematic but often overlooked area involves migrating data into the system in a manner that complies with the company's legal obligations to preserve electronic information that is subject to litigation hold due to legal disputes or regulatory matters. It also impacts information that is subject to other preservation obligations, such as records retention regulations or contractual obligations. For example, many companies are migrating their email systems from existing on-premises servers to cloud-hosted email services, such as Google's Gmail or Microsoft Office 365. Before legacy email is moved to the new cloud system as part of the migration plan, it's important to understand the impact that the migration and conversion processes being deployed may have on that email data.

Validation tests typically used by IT departments for these processes are generally neither rigorous nor extensive enough to uncover small but significant changes to the data. These may impact the integrity of the metadata, embedded objects, and message bodies or attachments to the point that the original data may be considered spoliated by a court. Basic forensic testing of random samples will often uncover these changes before the original data is lost forever, but only if the legal team and their e-discovery advisors are involved early enough. This applies equally to other legacy data being imported into the system – it's not limited to email.

It's important to understand any format limitations and conversion impacts on data being exported from the system to meet discovery obligations. Since many cloud-based systems operate on proprietary platforms and fragment data among large numbers of servers, taking data out of the cloud environment can often render all or some of it unreadable or unusable. The export formats available may not be compatible with existing e-discovery processing and hosting software. The search and retrieval capabilities available in the cloud-based system may also have limitations, which will then require exports of larger data sets than otherwise needed, for search and filtering outside the system, using more powerful and accurate tools. However, exporting these large data sets using internet-based interfaces can be slow and cumbersome, and may require extensive quality control measures to ensure the exports are valid and complete if, as found in most systems, the interface lacks such functionality.

These issues typically don't torpedo cloud migration projects. Most companies often don't fully understand them until after the new systems are deployed and problems surface. Often this is at a time of crisis, which puts significant time constraints on resolving issues that may have arisen. However, early involvement in the planning and testing stages of the migration process can help counsel avoid these painful fire drills down the road. A little time invested up front can help the company fully understand the impact of data migration and identify any steps needed to remediate issues before they cause permanent data losses.

CHAPTER 6

The Needle in the Anti-Corruption Haystack

Regulators around the globe have been stepping up anti-corruption compliance efforts. The past few years have seen a marked uptick in both formal inquiries and legal actions related to money laundering and bribery, with regulators demanding increased access to company records. Given their global scope, the costs of responding can be enormous. For example, the global retailer Walmart predicts that its anti-bribery compliance-related costs for this year alone will be upward of $180 million.[1]

This is not atypical for companies with a large global footprint. Earlier this year, Olympus resolved a $22.8 million Foreign Corrupt Practices Act (FCPA) enforcement action concerning alleged misconduct in Brazil, Bolivia, Colombia, Argentina, Mexico and Costa Rica. Managers at an Olympus factory in China were also tied to related company investigations.[2] Separately, Olympus Corporation of the Americas agreed to pay $612 million plus interest to resolve parallel criminal and civil investigations into alleged violations of the Anti-Kickback Statute and the False Claims Act.[3]

The sea of information generated by illicit activities may also be the point of vulnerability when combined with newer analytics tools.

The primary costs are typically pre-enforcement action professional fees and expenses, with the bulk of these expended on information collection and analysis. This information typically comes from a myriad of sources and locations and in an equally diverse number of formats. It often includes company records, such as emails and text messages, invoices, contracts, memos, wire transfer and other financial records, accounting ledgers, spreadsheets, purchase and sales records, and other transactional information, as well as external information from outside sources, such as bank records, trade and customs data. Continually, the ever increasing sophistication of bad actors compounds the problem. Investigators, are constantly struggling to find smaller needles in larger haystacks, often with the needle hidden inside a piece of straw or disguised as an umbrella.

So how can data analytics help organizations find illicit transactions in a multitrillion dollar haystack? Unlike their traditional counterparts, newer analytics systems based on big data technologies, predictive analytics and artificial intelligence are not bound by upfront data transformation and normalization requirements, nor are they bogged down by the large data volumes that can choke a relational database. These more powerful and intelligent systems can also do a lot more of the routine heavy lifting with spreadsheets and other documents, freeing up human resources to focus on the more dynamic aspects of investigations. For example, in using predictive text analytics and concept-based search technologies, legal teams can greatly reduce the amount of time and costs associated with the review of documents and communications. Instead, machine learning may be leveraged to help bring the most critical and relevant communications to the top of the review pile, even where actors are using coded terms to hide illicit activities.

Similarly, new data analytics platforms allow for considerably more flexibility and agility with regard to the types of data they handle and the speed at which they do so. Newer tools often offer single visual workflow interfaces that enable the integration of a variety of data sources on the fly and adjustments to business logic applied to them. Users can twist and turn data easily, blending it from different sources to create custom analytics that yield highly accurate results, all without the need for extensive upfront modeling or a preconceived overarching data model. Here again, the tools take the manual hunting burden off the forensic accounting teams, allowing for quicker identification of the most critical transactions and their comparison across other data sources for validation and highlighting, without the need to pour over books and records line by line and document by document. In the end, the sea of information generated by illicit commercial activities – the invoices, bills of lading, insurance certificates, inspection documents, bank transactions, emails, and more – that makes it difficult to see what's truly happening may also be the point of vulnerability when combined with newer analytics tools, which not only have the ability to identify patterns and anomalies but can also greatly reduce compliance costs.

CHAPTER 7

Data Analytics: The Key to Compliance

New anti-graft laws that were promulgated by President Park Geun-hye on March 26, 2015 will take effect in South Korea this month.[1] Consistent with other efforts around the globe to combat corruption, the new legislation prohibits the transfer of value to any public servants, employees of public offices and state agencies, teachers, or journalists in excess of predefined amounts. For example, lunch or dinner shall be limited to a maximum of about $30, and gifts to $45. These can be doubled when they are given at family events such as weddings, funerals or the birth of a child. But if the value of the gift given exceeds these amounts, the offender shall be fined up to five times its value, and if it is more than about $850, criminal penalties shall be imposed.

Modern technology can greatly assist in assessing what anti-corruption controls are most appropriate.

Anti-bribery laws are not new in South Korea. In fact, South Korea was one of the first signatories at the OECD Anti-Bribery Convention in 1997, and in the following year it enacted legislation – the Act on Preventing Bribery of Foreign Public Officials in International Business Transactions (Korean FBPA) – to implement the convention domestically.[2] Criminal and civil penalties for domestic acts of bribery have also been on the books for many years, seeking to discourage both private and public transfers of value in return for favors. However, there are several key differences in the new anti-graft law that may require companies doing business in Korea to reevaluate their compliance programs.

Prior to the anti-graft law, penalties for domestic bribery were only levied after confirming a connection between the received gifts or favors and the activities of civil servants. Under the new law, it is no longer necessary to prove any purpose behind the gift. The gift itself is enough to establish culpability. More importantly, the preexisting anti-bribery laws did not typically impose liability on corporations for bribes made by its employees. Under the new anti-graft law, corporate criminal liability may be imposed for violations by employees, unless the corporation can show it exerted due care and supervision to prevent such a transfer. This latter change will likely entice companies doing business in Korea to ramp up their supervision and compliance controls. But what level of supervision and controls do these companies really need?

Experience from other jurisdictions dictates that the optimal type, placement and quantity of controls is largely driven by the context in which a company operates, the level of the government officials with which a company interacts, and the types of relationships or interactions a company has with those government officials. To assess the risk inherent in a given activity, a company should work to identify and quantify potential transfers of value to regulated recipients. Gifts, travel, meals, jobs for relatives and even contributions to charities may be considered value that could influence the decision-making of the government official, teacher or journalist. All of these factors determine where and by whom the review or approval should be conducted. It is also important to review these activities and provide a mechanism that allows consistent application of this prereview process throughout the organization, with appropriate record keeping and oversight. Companies can't simply ask people to self-report their expenses and then raise flags when value transfers exceed the statutory limits. Doing so would simply convert overt graft giving to covert money laundering schemes where transfers become hidden.[3]

Fortunately, modern technology can greatly assist in these efforts. One of the most efficient ways that companies can assess what anti-corruption controls are most appropriate is by gathering historic expense and communications data and analyzing specific activities. Predictive analytics tools can then be leveraged to map existing relationships with public officials based on past behavior, and machine-learning algorithms can be used to identify potential future risks related to gift giving. Companies can leverage such tools to properly match the intensity of their controls with the identified risks for each particular activity. Basing assessments on actual data ensures that organizations are deploying their resources both in the right areas and in ways that maintain the defensibility and credibility of the compliance process. Compliance programs will not be supported if they are viewed as an impediment to conducting efficient business and appear unnecessary given perceived risk. This in turn makes it much more difficult to maintain the exact mechanisms that mitigate critical risk, which are expected by government regulators. Since the essence of a compliance program is the prevention, detection and remediation of wrongdoing, a company's resources should be allocated to activities that pose the highest risk – and with proper data analytics these risks can easily and efficiently be identified and addressed.

CHAPTER 8

Data Mapping For Global Privacy Compliance

It has been a year since the Safe Harbor framework was invalidated by the European Court of Justice. That framework allowed U.S. companies that registered with the Federal Trade Commission to legitimately transfer data from EU member countries to the U.S. At the time the Safe Harbor was invalidated, about 4,000 U.S. companies were registered under the program. Each of these found themselves scrambling to find alternative ways to legitimatize the transfers that have become a routine part of daily operations at global corporations. The Safe Harbor framework was eventually replaced by the Privacy Shield framework, approved by a vote of the EU's Article 31 Committee on July 8, 2016. Since this time many of the companies that had relied on the Safe Harbor framework have begun to re-register under the new program. Others have sought to utilize one of the several other mechanisms approved by EU lawmakers to legitimately transfer data to the U.S., such as Standard Contractual Clauses and Binding Corporate Rules.

The future of each of these transfer mechanisms still remains a bit uncertain, however. Max Schrems, the Austrian law graduate and privacy advocate whose challenge to the Safe Harbor resulted in its invalidation last year, has vowed to also challenge the legality of the Privacy Shield. He has filed a complaint with Ireland's data protection commissioner challenging Facebook's use of Standard Contractual Clauses in moving its data between Ireland and the U.S. A provisional view of the case by the commissioner found Schrems' complaint to be "well founded." Accordingly, the commissioner has asked the High Court in Ireland to issue a determination on the validity of model clauses. The High Court has agreed to consider whether to refer the question to the Court of Justice of the European Union and has set a date of February 7, 2017, for the beginning of hearings on whether it should do so.

Companies that transfer regulated data across EU borders need to fully understand this data and what mechanisms are being relied upon to legitimize the transfers.

Given these uncertainties, companies that transfer regulated data across EU borders need to fully understand this data and what mechanisms are being relied upon to legitimize the transfers. When the Safe Harbor program was invalidated, many companies found themselves in the precarious position of not fully understanding what data was being transferred to various vendors, processors and business partners under that framework and what data was being transferred by other mechanisms. This left them unsure of which transfers were still legitimate and which would potentially violate the law once the short moratorium offered by the EU regulators lapsed.

Conducting an audit of physical data transfers is the first logical step to avert these types of issues. In addition to cataloging any cross-border transfers of personally identifiable information (PII), the audit should also clearly identify and validate the mechanisms relied upon for each transfer. Second, companies should ensure that each mechanism relied upon is in line with other potential contractual or regulatory obligations. As such, the review of these obligations should be part of the audit process too. For example, an audit may show that the scope of the company's Privacy Shield certification is limited to internal PII relating to employees, yet certain contracts with clients or customers may incorporate the certification based on a misunderstanding that it also extends to data being processed on their behalf. This is a compliance gap that should clearly be closed. Correlating the physical data transfers, the transfer mechanisms relied upon, and the company's other contractual and legal obligations relating to the PII it collects, stores, processes, manages and transfers across borders not only helps the company close these compliance gaps, it also positions it to respond in a timely and cost-efficient manner should any one or several of the current transfer mechanisms be invalidated in the near future. After all, the last response that anybody wants to have to provide when asked about a transfer mechanism by a board member or a regulator is "we are not sure."

CHAPTER 9

Diving into the Dark Web

The Dark Web is a term that has been getting a lot of attention in corporate boardrooms and media outlets as of late. The general preconception of the Dark Web is that it's a seedy underground digital hiding place for drug dealers, assassins, cybercriminals and pedophiles, which isn't far from the truth. For this reason, security researchers and law enforcement agencies have been surveying the Dark Web for years and keep close eyes on what goes on there. Quite often it is the first place that people learn of a data breach. This has also made it a place of interest for corporate IT security teams and risk managers. According to the rumor mill in cybersecurity circles, stolen data from the Target and Sony breaches potentially sat on the Dark Web for months before making headlines. However, while Dark Web intelligence may be helpful in defending your organization from cybercriminals, counsel needs to have a basic familiarity with the underground regions of the Internet and some understanding of how malicious actors use it to commit their crimes in order to avoid running afoul of unnecessary risks.

Just like other underground black markets, the Dark Web is full of unscrupulous actors who enjoy taking advantage of the unacquainted.

The Internet is composed of three primary layers: the World Wide Web (or Surface Web), the Deep Web and the Dark Web. The top layer, which is the area that most users are familiar with, represents only a very small fraction of the Internet. It is the roughly 4 percent of the Internet that is easily accessible via any common search engine. Underneath the Surface Web is the Deep Web, a much larger pool of information that is largely untouched by search engines. No one knows the exact size of the Deep Web, because it is hard to quantify without search engines. Typically, the Deep Web consists of corporate and academic environments that can only be accessed through direct queries. In other words, you need to know precisely what information you're looking for and you often need to have some kind of authorization to obtain the information. Legal research databases and subscription services are common examples. The third layer is the Dark Web. It's referred to as "dark" because it can only be accessed with special browsers, routers and encryption tools that render all traffic to its sites anonymous. The sites also use tools to hide their IP addresses, which make tracking their location and ownership especially difficult. These two aspects of anonymity are what make the Dark Web suitable as a digital underground. However, they are also what enables anonymous whistleblowing and protects users from surveillance and censorship in authoritarian regimes.

Given the wealth of intelligence that can be gleaned from the Dark Web, it is understandable that corporate security and risk teams are attracted to it. However, counsel must ensure that these teams proceed with due caution in order to avoid what can be very significant risks.

Most importantly, impromptu Dark Web reconnaissance can inadvertently expose an organization to greater security risks because of unknown malicious files that can infiltrate the corporate network. Just like other underground black markets, the Dark Web is full of unscrupulous actors who enjoy taking advantage of the unacquainted. If IT staff isn't properly trained nor has the right resources and equipment they could easily bring that malware and its controllers back home without even knowing it. In fact, connecting to the Dark Web from any corporate network is always ill-advised. It's important to use air-gapped assets that have no way to transfer malicious data into the corporate environment, as well as to use multiple layers of encryption.

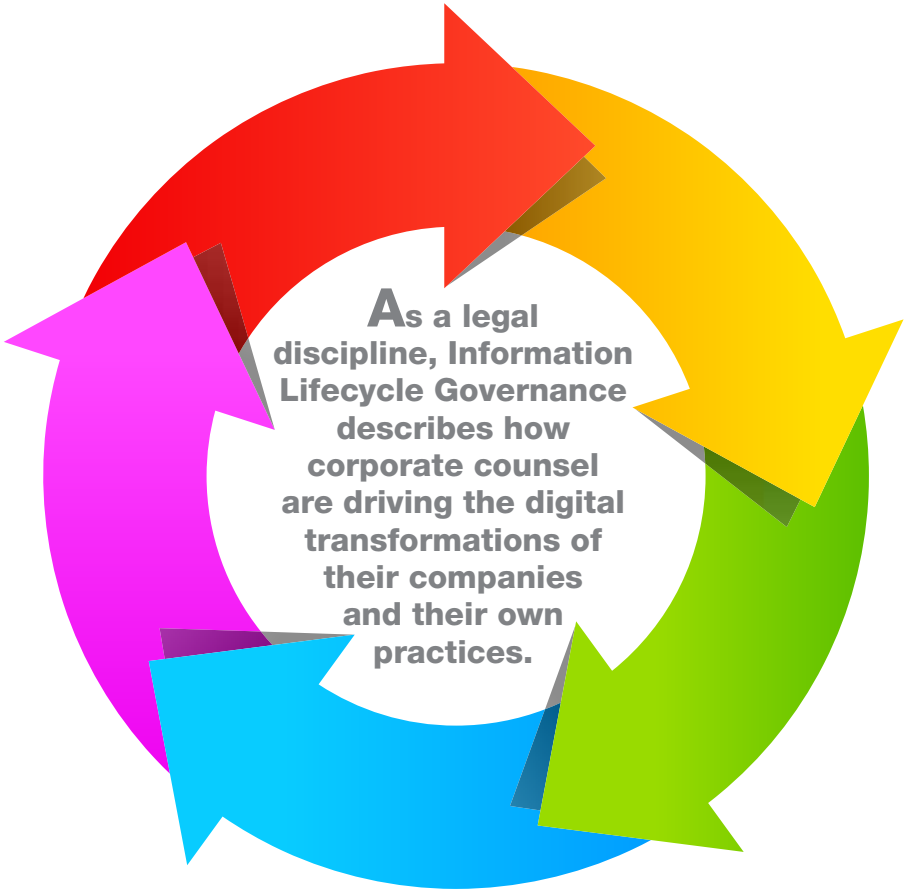
Further, gaining access is not for the faint of heart. Not all content on the Dark Web is immediately accessible. It can take considerable time, expertise and manual effort to glean useful information. It may take a researcher years to establish trust in certain communities and sales forums. Your in-house staff likely don't have the luxury of such time, energy and resources. Additionally, several criminal forums on the Dark Web utilize a "vouching" system, similar to a private members club, which might require an investigator to associate with criminals or stray into significantly gray ethical territory to gain access to the content. The average systems administrator probably doesn't have the operational skills necessary to pass himself off as a hacker on the Dark Web. Without the requisite skills, reconnaissance is likely to prove fruitless and will open the company up to further danger.

Lastly, even if your team was successful in safely gaining access, their activities must be closely monitored to ensure they do not run afoul of any laws. For example, you certainly wouldn't want your employees accidentally viewing child pornography or bringing it onto the corporate network. Also, while it can be tempting to download files pertaining to purported breaches, taking receipt of stolen goods is a felony in the United States (18 U.S.C. § 2315) that can cause legal issues for your team. Beyond that, such activities may disrupt the legitimate work of law enforcement agencies engaged in their own actions. Also, keep in mind that there is no way to confirm who the seller actually is. Purchasing data in such places can subject the company to risks of violating the Patriot Act if it turns out the data is being sold by a terrorist organization and you transfer funds to them.

A better strategy is to engage a reputable security firm to assist with these services. Many firms now offer some level of Dark Web reconnaissance, ranging from manual intelligence gathering to more automated approaches using Web scraping and analytics tools. Further, by integrating and organizing social media, Deep Web public records and peer-to-peer domains, skilled researchers are able to provide a more unified view of their external threats than internal teams can. The use of artificial intelligence and deep learning enables a more valuable exploration and indexing of large unstructured data sources, while enriching the analysis. The result is real-time finished intelligence, safe from the risks of self-gathering.

CONCLUSION

Information Lifecycle Governance Takes Center Stage



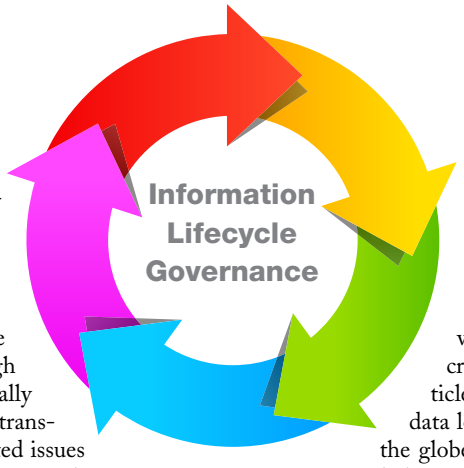
Over the past year I have used this column to explore the various topics relating to Information Lifecycle Governance (ILG). ILG means many different things to different people. Ask 10 people for a definition and you are likely to get at least a dozen different answers. This lack of consensus is not all that surprising since ILG is still relatively immature as a discipline. It has therefore been my intent throughout the year to help raise awareness of this new practice area by drawing out some of the ways in which it impacts the daily life of corporate counsel.

For decades, companies have generally allowed their end users to manage and govern the information controlled by or held within their domains. They have also relied heavily upon IT managers to make the bulk of decisions regarding information stored on the system they administer. Corporate counsel may have historically given very little thought to company data, other than when they needed information to support or defend their legal matters, or for niche regulatory requirements in certain industries. In the past, counsel simply may have had little reason to care how much information the company was amassing, from where it was coming, how it was being used, whether it was adequately protected, or how long it was being kept. These were traditionally all operational concerns left to business managers and did not involve significant issues regarding corporate risk or compliance.

The scope of corporate counsel duties has changed rather rapidly and drastically in the past decade, however. Companies have quickly begun to digitalize nearly every aspect of their operations. Digital information is generally now the lifeblood and primary as-

Continued on following page

Continued from previous page



set of all companies, in every industry, in every sector. Whether a company makes or sells widgets, transports goods or people, facilitates markets or transactions, or provides services of any sort, it has likely also become an information business in the past few years. The volume of digital information flowing through the company has also likely grown exponentially in this same short period. This rapid digital transformation has brought many information-related issues to the forefront for corporate counsel which can no longer be ignored. Information creates great value to the enterprise, and anything of value also presents proportionate risk. This is where Information Lifecycle Governance can help.

Early in the year I wrote a piece on Big Data[1]. This technology is more than just a buzzword. It is a primary driver of the digital transformation process and it often has profound enterprise risk and compliance impacts. These arise not only because companies are collecting and utilizing more data points in operations and decision making than ever before, but also because the technology itself is fundamentally different from all prior data management and analysis technology we have seen. Because these systems have the ability to ingest massive amounts of raw data, much of which has no predefined utility, the full content of the data often remains unknown until some type of business analysis is conducted. The result tends to be large data pools with little understanding of what is in them or what compliance obligations attach. They are commonly called dark data pools because there is no visibility into what they contain, which may include any manner of regulated information or contraband, and numerous companies have found themselves in hot water in recent years due to a lack of awareness of what data their business units were amassing. For this reason alone, it is imperative for counsel to get involved during the early program design phases and build privacy and compliance in from the start.

Big Data does not only present challenges for counsel, it is also a powerful tool. Several articles this year have drawn out examples of how it can be leveraged to improve compliance programs and reduce company risk. Big Data is particularly useful in anti-corruption investigations and in building internal monitoring programs. (See "Finding the Needle in the Anti-Corruption Haystack"[2].) The exact same attributes that make it a powerful tool for digital transformation of business operations also allow counsel to transform their own practices as well. For example, predictive text analytics and concept-based search technologies allow legal teams to greatly reduce the amount of time and costs associated with the review of documents and communications. Instead, machine learning may be leveraged to help bring the most critical and relevant communications to the top of the review pile, even where actors are using coded terms to hide illicit activities. Analytics tools can also make the hunt for correlating transactions and documentation much easier for both monitoring and investigations. This point was discussed more deeply in "Data Analytics May Hold Key to Compliance with South Korea Anti-Graft Scheme"[3] to show how the tools can be useful in building a successful internal compliance program, especially in areas where relevant evidence may be hidden or obscured.

Not only must counsel understand what data is being collected and stored by the enterprise, and how they can mine that data for their own needs, it is also important that they know where it is being stored, and by whom. Data privacy issues around the globe create a myriad of compliance issues. May's article[4] discussed the complex issue of emerging data localization laws that are popping up around the globe. Data localization requirements are driven mainly by concerns over privacy, security, surveillance and law enforcement, and typically require that data collected or used in a particular jurisdiction remain in that jurisdiction, or at the very least a copy of the data, so law enforcement or government officials can have access to it if needed. These laws present just one issue, prohibitions on cross border data migrations also add significant compliance problems of their own. For suggestions on how to properly address these and related issues, see November's article "Data Mapping for Global Privacy Compliance"[5].

One of the most important aspects of ILG is ensuring the company's assets are properly protected. There is certainly no glut of headlines regarding data breaches in the news these days, and there is no indication of any slowdown in hacker activity any time soon. The digital transformation of our enterprises equally empowers the digital transformation of criminal activity (See "How to Rob a Bank in Ten Easy Clicks" [6].) To this end it is important that counsel remain diligent with regard to both data stored in the corporate environment and that hosted or held by third-party service providers. In April, I also discussed vendor security certifications[7] and the importance of knowing exactly how your vendors are protecting your data. Many over-focus on the security of their data centers without disclosing anything about their internal processes or policies for accessing and moving data in and out of those centers. More recently, I discussed the value of the Dark Web for cyber reconnaissance, and how to avoid unnecessary risk when leveraging these digitally transformed black markets.[8]

Finally, one of the best ways to reduce all of the above risks and also help control budgets is through the clean-up of legacy data.[9] The more data the company must manage, the greater the cost to do so, and the more data counsel must sift through for compliance, e-discovery, or records retention programs, the greater the costs to them to do so. Old data is also often the most vulnerable to hacking, as it typically has the least protections or is being overlooked. Projects aimed at cleaning up this data often serve as a central component for ILG programs, and the data storage and maintenance cost savings alone can often more than offset the total costs of the entire ILG efforts.

Simply put, ILG is the specification of decision rights and an accountability framework to encourage desirable behavior in the valuation, creation, storage, use, protection, archiving and deletion of information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals. As a legal discipline, it describes how leading corporate counsel are embracing their new roles and driving the successful digital transformation of their companies and their own practices through better information risk mitigation and control.