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 also 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 2017. Footnotes can be viewed online at www.metrocorpcounsel.com

METROPOLITAN CORPORATE COUNSEL

AlixPartners when it really matters

How Counsel Can Improve Cyber-Risk Programs

The role of corporate counsel has been rapidly evolving in the past few years. The scope of responsibilities has expanded beyond legal administrative tasks to include companywide risk management, cost control, regulatory compliance and other areas that affect the company's reputation and bottom line. Data privacy and security, which used to sit squarely in the domain of the information technology department, now has the full attention of customers, shareholders and government regulators. As a result, senior management and the board are relying more and more on corporate counsel to be both the steward and the shepherd of cyber-risk governance programs.

This doesn't mean that counsel have simply inherited IT's responsibilities for managing cyber compliance. Quite the contrary. IT must still ensure that the computer systems they manage are properly secured. Counsel's role is to look beyond this hardening of IT systems to develop a more comprehensive cyber-risk governance program. Ideally, this program should consider cybersecurity from a broad perspective, and ensure that the company's statutory, contractual, regulatory and reputational liabilities are properly managed and minimized. Here are some best practices to consider to improve cyber-risk programs:

1 Take a top-down approach.

Most security professionals and practitioners would agree that total prevention is not possible. However, a top-down approach that embeds cybersecurity management throughout a company's infrastructure is the most effective way to mitigate risk. This means developing a governance model that starts at the board level, and then moves down through the C-suite and line managers to ensure accountability at all levels.

Many directors may not have the technical background to make decisions on their own, so the company should line up mechanisms to ensure that everyone has the assistance they need. These include the company deploying special cyber review or technology committees, and ensuring that other directors or advisory committee members have some technical or cyber experience as well. The committee can then perform periodic (typically quarterly) reviews and report to the board biannually. If it's not possible to create a dedicated technology committee, you should integrate the cybersecurity team into the audit or risk committee agendas for board reporting and decision-making. Determining which structure is most appropriate really hinges on the regulatory requirements, and the overall size and global footprint, of your company.

2 Make sure that the management team fully understands the risks.

You should conduct a full cyber-risk assessment that considers both the likelihood of various potential scenarios and the overall impact that each would have, using in-house resources and supplementing these with external assistance, where needed. To this end, it is important that you require senior management to know who the company's primary threat actors and stakeholders are. These can differ greatly across industries and geographies, and even across internal departments. It is therefore important that management provides a road map of the actual and potential actors or perpetrators they face.

The road map should also include the data privacy and security expectations of their key stakeholders and constituents. In addition, counsel should also require management to provide a clear and comprehensive map of company information assets that are susceptible to cyberattack. It's imperative to know what key assets are, where they are stored and what their internal and external values are in order to understand the controls needed to properly protect them. You should then ask some key questions, such as "How is the company positioned to handle any one of the identified adverse scenarios?" And "Is our current approach the optimal approach?"

3 Involve other departments.

Information assets and the risks they pose can differ greatly across the company. It is important to develop both a cross-disciplinary approach to cyber-risk management and a cross-segmental or divisional approach to cyber-risk management, including effective executive and board reporting. The information that each functional unit reports must be not only meaningful to more senior stakeholders, but also actionable.

The historic response to this challenge has been to use checklists, which are typically developed as a way for counsel to translate requirements into layman terms. Canned reports that IT professionals use to translate technological language into something others can understand and quickly review are equally common. But checklists and canned reports are unlikely on their own to give a clear picture of actual risk. This is especially true when they are just recycled metrics developed for other needs, such as the often-used common vulnerability scoring system (CVSS) reports, which were originally deployed for vulnerability response. Knowing how many vulnerabilities were reported and remediated in each quarter has very little value to a board that cannot discern if they were the right vulnerabilities or if their remediation had any impact on actual risk. (Sure, IT security closed 10,000 application vulnerabilities last period, but did that really help?)

More holistic risk reporting through a comprehensive portal that contains meaningful key performance indicators (KPIs) is essential to building an effective risk governance program. KPIs should be simple and easy to read. They should include, as a baseline, a road map that shows what your current risk profile is, where you want it to go in the future and what steps you are taking to get there.

4 Build cyber-risk partnerships.

Beyond leveraging internal resources, it is equally important that counsel build appropriate cyber-risk partnerships. These include actively engaging with your vendors and business partners, participating in both private-sector industry cybersecurity benchmarking and information-sharing programs. You should also monitor appropriate industry and government initiatives, and routinely engage outside advisors to take a fresh look at your cyber-risk governance program. In my sailboat racing days, we used to call this getting your head outside the boat. You can't hyper-focus on the tasks in front of you. To be successful, you have to also keep abreast of what is happening outside your company and what others around you are doing in response. It's important to look outside the organization and get constant feedback from experts with broader industry experience. Otherwise you will only focus on what you see in the boat, and probably completely miss that giant oil tanker headed straight at you.

Before leaving office, President Barack Obama called cyber-risk "one of most serious economic and national security challenges" facing America. As more and more critical company assets – including intellectual property, corporate strategies and consumer information – are stored electronically, developing robust cyber-risk governance programs could not be more important. As a result, general counsel and their legal teams must be proactive about taking a leadership role on cyber-risk governance. By staying properly informed about the company's cyber-risk profile and liabilities, they can provide the necessary guidance to the board of directors, senior management and other stakeholders. Counsel who assert their dual role as the steward and shepherd of these programs can ensure that their company's most important business assets remain secure and that its risks – legal and otherwise – are kept to a minimum.

CHAPTER 2

Data Breaches Can Paint A Bullseye on Their Backs

Corporations that fall victim to data breaches are often faced with a deluge of lawsuits, especially when private or sensitive information is disclosed. It is not uncommon for the plaintiffs to pile up after a major breach, each with their own alleged claims for damages. Complaints typically come from the individuals to whom the data pertains, either individually, as a class or as multiple sets of classes. Plaintiffs may also include financial institutions and payment card issuers, third parties such as partners, vendors and clients, and company shareholders or investors. State, federal and foreign regulators are often front and center with their own inquiries and enforcement actions.

Beyond company liability, however, there has also been a steady rise in actions that individually target directors and officers brought by both regulators and shareholders.

One of the first examples was a shareholder derivative suit that named more than a dozen TJX directors shortly after the massive breach that the company suffered in 2005. More recently, similar actions have been brought against Target, Heartland Payment Systems, Wyndham Worldwide, Home Depot, Wendy's and Yahoo – to name just a few of the larger ones.

The primary basis of each are allegations that the directors and officers breached various fiduciary duties, such as those of care and loyalty. In Target, for example, the plaintiffs alleged that the directors breached their duties by "failing to take reasonable steps to maintain [the] customers' personal and financial information" and by failing to implement a system of internal controls to protect such customer information from a data breach.

Duty of Care

The duty of care generally obligates directors to act on an informed basis, in good faith and in the honest belief that the action was in the best interests of the company. The duty of loyalty, on the other hand, obligates them to develop and monitor controls and reporting systems in order to ensure that they are adequately informed of any risks which require their attention. In the data breach context, these fact-specific inquiries typically turn on what the directors knew regarding their cyber risks, and how they acted to prevent them.

None of the early cases survived past summary judgement. After demanding that the boards bring action against the company, the plaintiffs simply could not overcome the high bar of the business judgment rule when applied to the director's decision not to do so. However, as this rapidly developing and volatile area of law matures, so too has the plaintiff's bar adapted.

Plaintiffs have now begun taking an entirely different approach. In the Home Depot and Yahoo cases, for example, they skipped demand on the boards altogether and instead alleged that doing so would be futile because the directors face personal liability and therefore cannot exercise independent business judgment when responding. They have also begun to add additional claims such as deficiencies in disclosure of material information. In the case of Yahoo, which individually named both the company's CEO and CFO, the claims focus on alleged materially false and misleading statements made by the executives and company in their security filings. The court fully denied the plaintiffs claims in the Home Depot case in April. The Yahoo matter is still pending, and the plaintiffs' new actions don't seem to be slowing down.

In addition to the threat of lawsuits, officers and directors also face a threat to their tenure at the affected company in the event that the organization experiences a data breach. For instance, in 2014 Target's CEO and chief information officer resigned after its breach, and in 2015 the CEO of the parent company of AshleyMadison.com resigned after news of a data breach at his company broke. In 2016 Yahoo's general counsel resigned without separation payments after reporting a 350 million dollar purchase price adjustment by Verizon, and over 11 million dollars in legal expense resulting from the company's several breaches. So, although plaintiffs have yet to prevail in any securities class actions, the costs and risks to directors and officers are still quite substantial.

Lessons Learned

In addition to taking enterprise-wide actions to protect their company from liability, directors and officers must ensure that they take steps to minimize exposure to personal liability as a result of a data breach. A review of the claims and allegations along with the final rulings in the several major cases mentioned above shows a clear line of best practices that can help to mitigate these risks.

Implement and monitor security controls before an event happens to demonstrate diligence as to the duty of care.
These controls should not be limited to technical, physical and administrative controls for IT systems and devices. They should extend to the full spectrum of information-related business operations and processes and their resulting risks to data security. This includes such areas as employee background checks and off-boarding, vendor contracts, cross boarder data flows and use of technology policies, among others.

Ensure that the board is informed and equipped to respond.
It's not enough simply to rely on periodic reports from the IT security teams. The directors and officers need to have meaningful and digestible information that they can act upon. This means reporting the correct key performance indicators (KPIs) that go beyond metrics about the number of patches deployed and the number of events averted. Instead, KPIs should measure such areas as time to detect, contain and mitigate those events, improvements in employee readiness and awareness and overall operational maturity. This allows the executives and directors to have meaningful discussions on data security and to ensure that security efforts are in alignment with overall business strategy. Boards should also have technical advisory committees and experts they can rely on to help them distill and understand the information presented to them.

Have a playbook and test it regularly.
The technical teams will typically have their own playbooks that describe their response plans for various security events for each system and data type. While these are invaluable, they should be extended to include the full scope of response activities across the company: from the escalation of events up to executive management and to the board, to company investigations, responses and disclosures. Once defined, these various plays should be tested and validated on a routine basis, so everybody knows what to do before a crisis hits.

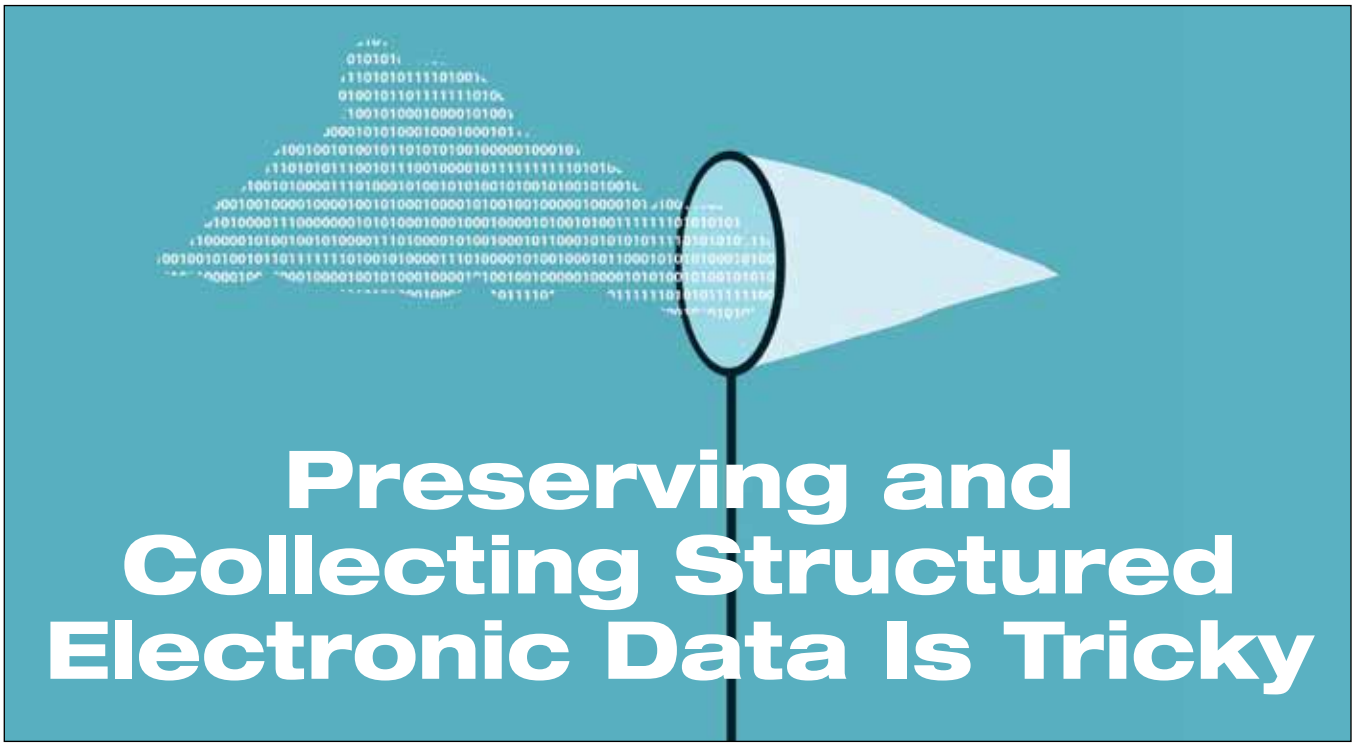
Designate a quarterback to run the plays.
Not so long ago, the responsibility for managing data breach responses fell squarely on the CIO or CISO. However, the dismissal of Yahoo's general counsel demonstrates a shift in expectations as to who should manage the response within the company. Every aspect of a data security incident response is rife with delicate and complex legal issues. The current expectation is that counsel will have clear visibility into, and will participate in, all aspects of cybersecurity planning, monitoring, reporting and, of course, response (in addition to the post-event legal issues). It is fair to say that counsel is now on notice – if there was any lingering doubt – that cyber risks fall squarely within their functional mandate.

Review your disclosures.
These include security filings, privacy and security policies and marketing materials. Given the new focus on disclosures, both from the plaintiff's security bar and regulators, directors and officers must ensure that the company is in fact doing what it says it is doing, and reporting material events in a timely manner.

Check your insurance policies.
Director and officer policies don't often cover losses from cyber events. Take the time to review your coverage and to understand overlaps and gaps between your D&O and cyberinsurance policies and the limits to coverages for both, and ensure that they properly align with your real-world risk scenarios based on the types of data the company is responsible for.

Enlist the help of experts.
The board should learn from the best practices of other similar organizations. One way to do so is to hire an outside firm to investigate internal practices and provide a maturity assessment that benchmarks the company against its peers. Again, this shouldn't be limited to technical IT assessments of your networks and servers, but should extend to all areas of information management and related business risks, including privacy and security.

CHAPTER 3



Preserving and Collecting Structured Electronic Data Is Tricky

Today's litigators are keenly aware of the need to effectively preserve electronically stored information (ESI) when new legal matters arise. And dealing with various types of unstructured data such as user-created documents and email messages has become quite routine. But preserving and collecting structured ESI from enterprise-wide database systems present unique challenges when it comes to e-discovery, and they get far less attention.

A typical medium-sized enterprise has hundreds or even thousands of structured business applications that store financial, product, customer, employee and other material information. These systems are often the lifeblood of the company and the system of record for all business-related activities. Given their importance, e-discovery compliance programs must also incorporate processes for the preservation and collection of ESI from these systems – not just focus on email and file servers.

While documents and email are generally self-contained and static, the information in structured data systems is dynamic and constantly changing. Data in one system or table is also often highly dependent on data in others. The databases themselves also often have longer lifecycles and are continually evolving. This makes discovery on structured data magnitudes more difficult. Without a robust e-discovery program that directly addresses these issues, IT organizations are forced to overpreserve and retain large amounts of information, which can adversely impact system performance and budgets.

The primary challenges to be addressed when building a successful e-discovery and compliance program for structured data fall into four primary areas:

1 Identification

The proper identification of the specific information or data objects within the system that are subject to retention obligations is central to ensuring that the company is neither overpreserving nor underpreserving information. In addition to the records they contain, databases comprise a variety of other elements, including reports, printouts, queries, application layer source code, pick lists and more. The relevance of these elements to an e-discovery request depends on the system, the business, the industry and the type of legal action. Yet, instructions from the legal departments often simply say "preserve all payroll records." This offers little actionable guidance to system administrators. Counsel must make an effort to identify the specific elements needed so that they can provide actionable and auditable instructions.

2 Preservation and collection

Once identified, the specified data must be preserved and collected. High-volume transactional information often has very short retention periods. Other data is often overwritten and updated. This means that counsel should make decisions about what to preserve quickly. Another challenge is deciding how to preserve this data. It must be captured in a way that preserves the integrity of the relationships within the system – or else it may be rendered meaningless. Because these systems evolve organically over time, they often lack descriptive documentation, and it can be difficult to find employees with sufficient knowledge of all their intricacies. Therefore, an iterative investigation is often necessary along with a bit of trial and error during the extraction process.

Another common collection challenge arises when defining queries. Requests that seem simple and clearly defined to the legal team can be unclear to a database administrator. For example, you may request a report containing "all employees in the state of New York." But how do you define a New York employee? Is it by the address where their paycheck is sent or the zip code of the facility they are assigned to? What about an employee who is assigned to a facility in New York but lives in New Jersey and is always on the road covering sales territory in Pennsylvania?

3 Validation and authentication

Once the required information has been collected, it still must be validated and authenticated. Validation is the technical process of determining whether the extraction was accurate and complete. For example, did the queries used actually return the right employees, and were any records inadvertently omitted? This process typically relies on a combination of techniques, which may include comparisons of record counts, fielded values, and summarized or consolidated reports from both the source system and the exports.

Authentication is a legal construct concerned with tracing the chain of custody from the physical copy of the information you are producing to opposing parties all the way back to the system of record. This important process ensures that the information is what it purports to be, hasn't been changed or tampered with along the way, and is still accurate and complete. Frequently, the internal IT team executes the data extracts with help from external resources. Service providers may perform some filtering and sorting of this data, and outside counsel may mask or redact certain elements, such as social security numbers. When the exports are finally disclosed, it is important to have a fully documented chain of custody describing who pulled the data, who else touched the data along the way, and exactly what was done to it at each step. In addition to the signed chain of custody forms, documentation typically includes retaining a copy of the original queries or specifications used for extractions, recording record counts and calculating MD5 hash values.

4 Custody and control

Believe it or not, e-discovery does have some limits. One of these is that parties are only obligated to disclose information within their custody and control. The issue of custody and control is generally a relatively easy one to address when dealing with unstructured data such as email and user files. It can be a much trickier issue to address with structured databases. This is because all data elements within large enterprise databases are not necessarily owned or controlled by the same entity, and portions of data processing or aggregation may be outsourced to third parties. When building an e-discovery program, it is very important to determine exactly who owns and controls what elements at any given point in time and what portions of the systems may therefore be subject to each entity's preservation and production obligations.

This issue is further complicated by the use of cloud services. It is common for an organization to own and control the transactional data in the system but have no control over the source code, architecture and algorithms, nor even over certain aggregated or processed outputs of the database. For example, SalesForce.com considers its database structure to be a proprietary trade secret, and disclosing the tables, fields and relationships within the database during e-discovery would likely be a breach of its end-user license agreement. The same holds true for many solutions offered by Google Apps.

Corporate governance and structure can also complicate custody and control issues. For example, a parent or subsidiary company may own or control the database and database software yet lease its use to junior entities or to other subsidiaries. In these cases, it may not be clear who controls what at any given time, creating complex legal questions to work through before responding to discovery from the system.

Given these complexities, and others such as data privacy issues, it is no wonder that counsel often gets tripped up when attempting to meet their discovery obligations for structured data systems. To this end, a little advance planning and investigation before litigation strikes can go a long way toward greasing the wheels for when a timely disclosure becomes necessary. It can also help to enlist the assistance of a trusted advisor who has both the technical and legal acumen and experience regarding e-discovery and structured systems to help wade through these complex issues.

CHAPTER 4

The Data Breach Response: Who Will You Tell?

Responding to data breaches can be a tricky business. If not managed correctly, corporate liability can easily be exponentially compounded. The key to successfully managing any complex crisis lies in the planning. It's important to develop a carefully laid-out process long before the fire alarms start ringing. Once they do, there's usually not much space for thinking of creative solutions. That's why we map out our escape routes and post them on the wall for all to see.

Data breach planning is no different. Once counsel gets that call saying there's been a security event, many moving pieces must be carefully and strategically orchestrated. These include notifying insurance carriers, engaging outside counsel and forensic experts, managing the internal IT response team, notifying board members and executives and overseeing public relations damage control with the media, just to name a few. For breaches involving customer or employee personally identifiable information (PII), counsel must also determine the company's obligation to notify government regulators and the individuals whose data was stolen, often referred to as the "data subjects." This task may seem fairly simple on its face, but it's often the most complex part of post-incident breach response – especially for companies with global footprints.

One of the unique aspects of data privacy laws is that they typically get triggered not by the storage location of the data – though that's sometimes part of the equation – but by the residence of the person to whom the data pertains. This is equally true both domestically – among the various U.S. state laws – and internationally. The reason behind it is that data is highly mobile and governing bodies want to protect the privacy rights of their citizens regardless of where the data itself may be stored. Otherwise, data controllers would move data from more restrictive locations to less restrictive ones and thwart all protections. The end result for those responding to data breaches is that even a relatively small set of data can trigger the laws of a large number of jurisdictions.

Unless a privacy assessment has been conducted in advance, counsel may have to wait until a forensic investigation is completed before it can determine which jurisdictions are implicated. Such an investigation includes listing all of the countries and all of the states where the data subjects reside. Then, for each, a legal assessment must be performed to determine which jurisdictions have notification requirements and whether those requirements have in fact been triggered.

For example, there's significant deviation both domestically and internationally as to what kinds of data constitute personally identifiable information. Most jurisdictions include in their definitions people's names combined with at least one of the following: home addresses, national identification numbers or account numbers. Others, but not all, include email addresses, IP addresses and international mobile equipment identity numbers (IMEIs). Therefore, it's important to determine the specific content of the actual data breached in order to assess whether the definitions of any specific jurisdictions apply.

Even when a definition does apply, notice requirements still might not be triggered. Although not the norm, a few jurisdictions in Southeast Asia have territorial limits to their breach notice requirements. In those locations, notices may only be required for breaches that occur within the jurisdictions or for breaches that relate to activities conducted in the jurisdiction or that specifically target that jurisdiction's citizens.

More commonly, jurisdictions worldwide typically have individual threshold limits that must be reached before notice requirements trigger. For example, notices may have to be sent to data subjects only when more than 10,000 records were exposed. Or regulator notification may be required only when a certain record type is involved, such as financial or health records. Some jurisdictions may require that both regulators and data subjects be notified; and in others, only one or the other. The required content and form of notices also vary greatly – from public notice in a newspaper, to emails, to written letters.

Those are just a few of the many issues that need consideration in order to tackle breach-notice requirements. Combine them with all the other issues involved and the benefits of advanced planning should be obvious. This is especially true because time will also be working against you: the initial forensic analysis will likely take several weeks, and the legal analysis will likely take even longer. Yet, at the same time, the clock will be ticking against the timeliness requirement stipulated by most notification regulations.

For example, in April New Mexico became the 48th state to enact a data breach notification law – leaving Alabama and South Dakota as the two states that lack requirements. Under that law, notice must be made to the attorney general, New Mexico residents and consumer reporting agencies within 45 calendar days of discovery of a security breach – if over 1,000 residents are impacted. However, the notice requirement is waived if an investigation determines that the event does not give rise to a significant risk of identity theft or fraud. This essentially leaves companies with less than 45 days to complete their full investigation and impact assessment, unless they have taken steps to plan for such an event in advance.

This is one more reason why those who are prepared will fare the best. Including breach response planning in your routine privacy assessments, and understanding your potential notice requirements before a breach occurs, will save you a lot of headache pills when your breach day comes.

CHAPTER 5

Whose Laws Govern That Slippery Data?

The issue of jurisdiction over data stored in cloud-hosted environments has been a hot topic lately. In early June, Apple, Microsoft, Amazon, Cisco and several other technology giants filed amicus briefs in support of Google's move to overturn a federal court order requiring it to produce information stored on servers outside the United States in response to a search warrant. In their amicus briefs, each company argues that reaching into foreign territory for data isn't allowed under federal law, while the government retorts that data in the control of U.S. companies is subject to its search and seizure powers under the Stored Communications Act (SCA).

The SCA itself is silent as to whether it applies outside of the U.S. In the absence of clear statutory guidance, courts tend to assume that the intent of the lawmakers was not to extend jurisdiction outside the U.S. Yet, given the nature of cloud storage, the courts are having significant trouble shoehorning new technologies into longstanding legal frameworks.

Thus far, only the U.S. Court of Appeals for the Second Circuit has addressed the extraterritorial application of the SCA head on. Last year in *Microsoft Corp. v. United States*, the appeals court held that the statute's focus was on privacy, rejected the government argument that it was a permissible disclosure and ruled that Microsoft did not have to produce data stored on servers located in Ireland. The court reasoned that doing so would be an invasion of the Irish customers' privacy and an improper extraterritorial application of the law.

The Google court has distinguished the present case from *Microsoft* in that the data requested by the subpoena is not "tethered" to any particular user location. Therefore, the court decided, the disclosure of information that is stored abroad but processed and retrieved from the company's U.S. headquarters is a domestic application of the SCA, and is not overreaching.

On its face, this ruling seems to be a split from *Microsoft*, even though the two are actually consistent. Hosting emails in a foreign data center is not akin to sheltering funds in an offshore bank account. Most users have little to no control over where their information is physically stored. This precept is often the main selling point of cloud storage. Powerful algorithms determine the most efficient and optimal storage location, and often fragment the data to achieve this.

Much of the legal discourse on this topic seems to focus on the physical storage locations of the data and on the producing party's ability to access and control the data from within the U.S. Yet, these two concepts are actually irrelevant constructs that carry over from our notions of a physical or analog world. What was truly central to the *Microsoft* case was that the data sought was sent and received by a user most likely located in Ireland and who had certain expectations of privacy that were protected by the sovereign power of his state, and that they were not U.S. emails subject to the boundaries of the SCA. A domestic email sender or recipient would not typically have a reasonable expectation that their electronic communications will be free from legitimate U.S. government search simply because a technology service provider moved this data to an offshore server, any more than a foreign actor would expect to lose their rights to privacy simply because data was (often without the actor's knowledge) moved to a U.S. server.

The law, which was written at a time when the storage of digital information was more akin to a single physical object, is having trouble wrapping itself around this digital transformation when dealing with ones and zeros that can manifest themselves in multiple locations all at the same time. It also is in tension with most foreign data protection and privacy laws, which often seek to extend the protection of citizens' privacy interests in data stored abroad.

Rather than focusing on the location of the data, or the ability to access it, the primary focus should be on the bubbles of privacy rights that surround and attach themselves to the data regardless of its physical location. In the Google case, the disputed warrant relates to the further investigation of persons who have already been indicted in the district, and there is no indication that the relevant email accounts were used by persons outside the United States. These are key facts that should not be overlooked.

The court, while not directly acknowledging the attachment of privacy rights, seems at times to allude to them. For example, it stated that "[e]lectronically transferring data from a server in a foreign country to Google's data center in California does not amount to a 'seizure' because there is no meaningful interference with the account holder's possessory interest in the user data." Contrary to the position taken in the amicus briefs filed in support of Google, the court was not holding that the data should be disclosed just because remote access was possible, but rather because remote access did not violate the privacy rights and expectations of the data owners, as it would have in the *Microsoft* matter.

Given the fluid nature of electronic data, and the simple fact that companies now move information around the globe faster than the blink of an eye, it is no wonder that the courts are struggling to resolve these issues. This is particularly true given the need to apply precedent that originates from a world with very different physical boundaries.

How courts will apply established legal precedent to cloud considerations in future cases is anyone's guess. But what is certain is that these issues will be an unavoidable challenge for judges, given the growing prominence of cloud services. Until new legal constructs are fleshed out, we are bound to continue to see these cases coming up over and over again.

CHAPTER 6

Spotting Corruption In the Wild

It's been just over a year since the DOJ launched a pilot program designed primarily to motivate companies to voluntarily self-disclose misconduct related to the Foreign Corrupt Practices Act. The program was set to expire after 12 months, but in April it was extended for a second term.

To encourage voluntary self-disclosure, the program offers significant reductions in penalties for those who cooperate with investigations, and even greater reductions for those that discover on their own activities that may run afoul of the act and self-disclose. A cursory review of DOJ's public announcements regarding declinations of prosecution during the past year shows a deliberate effort to broadcast the benefits of cooperation and the resulting reduced penalties. In each, DOJ repeatedly cites voluntary disclosures and cooperation as primary reasons for leniency.

In order to be in a position to self-disclose, however, companies must have a compliance program that is robust enough to identify potential violations well before they fall under government scrutiny. At the core of any such program is data analytics.

Most modern compliance programs are already leveraging some form of data analytics. Most often the data, metrics and other objective evidence is used in a defensive posture to demonstrate that the compliance program is working effectively. However, to catch the carrot the DOJ is dangling, companies must expand these efforts to identify potential violations very early in their lifecycles.

This is also made clear in the DOJ's guidance regarding risk assessments. The guidance says that companies must proactively collect data and metrics to help proactively detect potential misconduct as part of their routine information-gathering and audit activities. In other words, a company's monitoring, internal-control testing and auditing should collect and analyze data in an effort to identify red flags.

Unfortunately, most global companies that are at risk have mountains of data to sift through. The only way they can root out potential misconduct is to custom-tailor analytical procedures so that they can locate the anomalous signals in all the daily noise. Finally, the fact that enforcement agencies themselves, such as the DOJ, the SEC and FINRA, have all instituted their own data analytics programs evidences the need to stay ahead of the curve.

Looking to recent enforcement actions gives a good indication as to how these programs might be tailored. For example, a recent $3.9 million settlement exposed a scheme in which a global account manager was offering software packages to his resellers at a significant discount. The resellers, in turn, were selling the packages to end purchasers at larger-than-normal mark-ups. This allowed them to create a slush fund of excess revenue that was used to pay bribes in exchange for future government sales contracts.

To monitor for such activity, compliance programs can analyze the baseline of discounts offered to all vendors and use data analysis to flag anomalies that deviate from the established norm. A similar approach might also consider inflated or unearned sales commissions. Fully understanding and evaluating data points around the activities of sales consultants also allows the compliance team to identify potential relationships that may not have a clear business purpose.

Inflated or fictitious sales commissions or bonuses, which are then used to pay bribes, often come up in enforcement efforts. Here again, analysis of payments and compensation data can be used to uncover those above the normal baseline or at odd times of the year. Similar analysis of expenses and gifts can help flag travel to unusual locations and payments to unintended beneficiaries. These are also common schemes.

Although these examples are demonstrative, using data analytics to support proactive compliance programs is not one-size-fits-all. To be effective, the use of analytics in the compliance realm must rely upon both a full understanding of data analysis methods and a deep knowledge of the business and its routine activities.

CHAPTER 7

Managing Cyber Risk In the Cloud

More businesses around the globe are moving their data to cloud-hosted environments than ever before. In fact, Gartner predicts the worldwide public cloud services market will grow to $246.8 billion this year, an increase of 18 percent from $209.2 billion in 2016. With this migration comes an increase in concern for information security. After all, shifting company data, processing and systems to an environment controlled by a third party doesn't relieve a data owner from its obligation to protect the data, nor from the fallout of damages that follow data breaches.

In response, cloud service contracts now commonly include extensive provisions addressing data use and ownership, confidentiality, required security controls, liability, and audit and monitoring rights. Due diligence in the vendor selection process also now routinely includes a full review of all third-party attestations regarding security controls and related certifications.

While these measures are helping, they often create a false sense of security, leaving several other key areas overlooked. Beyond ensuring that their vendors' environments are secure, companies must also ensure that they themselves have implemented controls for data movements in and out of the cloud environments and for user access to these environments. With regard to the latter, the inability to detect, protect and respond to unauthorized access to cloud-hosted systems, especially through compromised, spoofed or forged credentials, can increase risk significantly. Companies need to carefully monitor how their employees are interacting with the hosted services to proactively detect improper access by malicious actors and take remedial measures.

Unfortunately, doing so isn't always easy. While many cloud applications offer some level of logging user access and activity, the logs require active review by a system administrator. This is a manual task that is both time-consuming and tedious. Furthermore, the shift to cloud services is often accompanied by a shift in the responsibility for system administration from IT to the business unit managers whose functions align with that service. These managers are not usually trained in IT system security and rarely (if ever) review these logs except, perhaps, in response to an adverse incident. This ad hoc manual review by untrained administrators often leaves anomalies in access patterns or inappropriate data exports completely undetected.

The challenges don't end there. It may be difficult to tell whether employees are accessing cloud apps from unmanaged or unsecure personal or public computers. It may also be difficult to detect access from known suspicious hosts, devices, countries or locations, at unexpected times of day, or with anomalous access patterns. The company may also have little insight into which users are sharing data, what data they are sharing and with whom. The result may be a failure to distinguish between routine and anomalous user activity, and a failure to then deny access when needed to stop data loss. A malicious actor who has acquired valid user credentials through malware or social engineering can go undetected for months. Given that even midsize companies now often deploy several hundred, or even thousands, of cloud systems, this can create a massive security gap.

The problem is exacerbated by the common habit of employees using the same passwords for multiple systems, both personal and business. This means that when less secure systems are compromised, such as an employee's personal social media account, so too are your business systems – if that employee was using the same credentials for both. Further, lost or forgotten credentials are often easily recoverable through authorized email accounts, which means that a malicious user who gains access to an employee's email can easily gain access to cloud systems by requesting a password reset. New passwords are sent to the employee's compromised email account, and the hacker is then free to steal or modify data, lock out users or simply lurk and collect sensitive information over time. If the targeted employee had administrator rights, the damage could be compounded significantly.

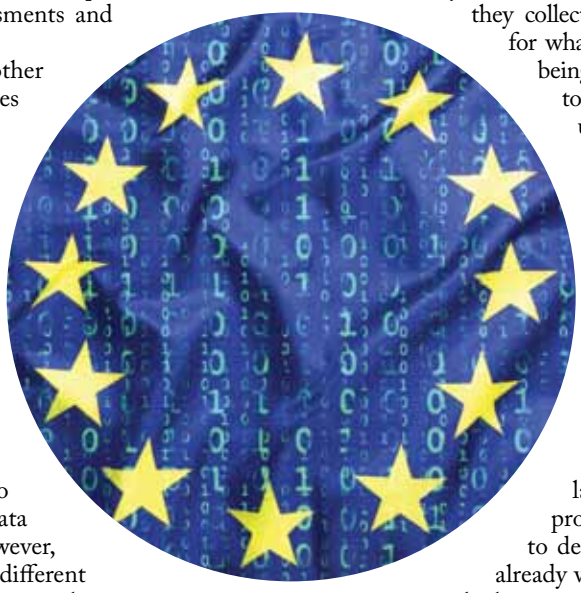
All is not lost, however. As more and more companies adopt cloud-based services in their IT models, a new set of cloud-based security solutions has emerged to address the gaps. These solutions are interchangeably referred to as cloud access security brokers (CASBs) or cloud security gateways (CSGs). By leveraging the data feeds of company cloud platforms, these solutions serve as a single monitoring and control portal for company security managers. They also commonly allow for visual reporting and trending of use, activity and incidents in user-friendly dashboards. Functionality differs across solutions, but common elements often include personal device access control and policy enforcement, user identity management across cloud provider platforms and single sign-on control using company issued and managed credentials. They may also give companies the ability to proactively detect and intercept unusual or fraudulent activities. While such solutions are still quite new, counsel for any company leveraging cloud services should be considering how these tools fit into their cyber risk management strategy.

CHAPTER 8

Data Map Now to Ease GDPR Compliance

The new European Union General Data Protection Regulation (GDPR) formally takes effect in May 2018. The move from the current Data Protection Directive to the GDPR brings with it a whole series of new requirements forcing prudent companies to conduct assessments to identify compliance gaps. Among the key components are the requirements to implement data protection policies, conduct data protection impact assessments and appoint data protection officers.

When viewed along with all of the other changes, it is clear that the GDPR creates a fundamental shift away from simple protection and transparency toward a need to actively manage and control data. This increased accountability for data practices means that most companies will need to make a number of operational changes to meet the new requirements.



For example, businesses will need to significantly enhance their record-keeping activities. Under the current directive, companies who control personally identifiable information are often required to notify their local regulators of their data collection and processing activities. However, each EU member state currently has different notification requirements, which makes compliance particularly difficult for multinational companies or for those that hold data from citizens of multiple member states.

Under GDPR, it will no longer be necessary to submit data processing or transfer notifications or registrations to each relevant regulator, nor will it be a requirement to obtain approval for certain transfers. Instead, there is now an internal record-keeping requirement for all data collection, processing and transfers. The data protection authorities have also reserved their right to audit these activities and the corresponding records. The failure to document has strict penalties for noncompliance. To avoid running afoul, companies will have to start tracking and documenting all of their data gathering and processing activities, both new and existing.

The GDPR's mandatory breach notification requirements are another significant area of change. Data controllers must provide notice within 72 hours of having become aware of any breach that is likely to "result in a risk for the rights and freedoms of individuals." Data processors will also be required to notify controllers "without undue delay" after first becoming aware of a data breach. Given that it can often take weeks or even months to determine exactly what data was accessed in a data breach, these timelines are quite short. Unless companies fully understand their data holdings before a breach incident occurs, they are not likely to meet them.

To address both changes, the most important thing companies can do right now is data mapping. They must spend the time to fully understand exactly what personal information they collect, manage and process, from whom, for what purposes, and where and how it is being used and shared. If they are unable to do this, they cannot even begin to understand their level of compliance and what they need to do to close any gaps. This exercise should also look at international data flows and seek to understand what the legal basis is for legitimizing the transfers. It should also map out all of the service providers who are processing data on the company's behalf and ensure that the proper contractual protections are in place.

Companies need to get moving, however, and not wait until it is too late. Changes to internal business processes and workflows take time to design and implement. If you are not already working on them, you may not meet the looming deadline.

Thankfully, there are a number of technology solutions that can help expedite the process. For example, there are several tools that can crawl across repositories of unstructured data looking for personally identifiable information and other controlled data in order to build data maps and remediation plans. They typically deploy a combination of pattern matching and conceptual search algorithms to home in on the many various types of protected information.

Automated contract review tools can also be a considerable help. They deploy artificial intelligence and machine learning to automate the review of variations in customer and vendor contract clauses, such as confidentiality, data protection obligations, intended uses, legitimate bases for transfer or processing and subcontractor obligations. When combined with traditional data-mapping techniques, these technologies can significantly reduce the time needed for companies to fully understand and document their data flows to meet their compliance obligations. It does not have to be a manual process, and you don't have to do it alone.

CHAPTER 9

Measuring the True Costs of E-Discovery

Taming budgets has long been a primary goal of all corporate legal departments. To this end, many companies have begun taking cost-cutting measures such as reducing the number of law firms they work with, developing alternative fee arrangements and putting pressure on firms to reduce their hourly rates for the more commoditized work. However, since discovery often eats up the majority of litigation budgets, it is no surprise that curbing e-discovery costs is often highest on the list of priorities. Yet, even though every legal department manager will tell you they want to cut costs, very few can actually tell you the true costs of e-discovery.

This is because true costs are often confused with price tags or overall spend. Yet, these are two very distinct concepts. The same conflation of ideas is often seen with automobiles. People treat the sticker price of a car with its true cost of ownership. They assume that a car with a higher sticker price costs more to own. But the true cost of ownership for any automobile has little to do with the sticker price. True cost is actually a function of depreciation of value over time, maintenance costs, gas mileage, and insurance, taxes and loan or lease interest. As a result, a car with a much higher sticker price can often turn out to cost a lot less to own for five years than one with a lower price tag. The same holds true for e-discovery costs, especially when they are simply reduced to per unit pricing or some other arbitrary flat fee figure, as is most often the case. Sure, it may be costing the company X dollars per gigabyte to process or host electronic documents for review. But does that number really communicate anything meaningful, and will reducing it actually reduce your overall costs?

True cost reduction is not just a matter of demanding lower rates from your service provider. Unfortunately, the difficulties of bringing collection, processing and hosting in-house, combined with fiscal pressure to control costs, has led to the commoditization of e-discovery services. This, in turn, has led to a race to the bottom on per unit pricing. Yet, even with rock bottom prices, many companies have failed to realize any actual savings in their budgets year over year. Many like to point to increasing data volumes in response, which certainly have had an impact. However, the real issue is that the lower prices have begun to squeeze profit margins to a point where quality of service and thoughtfulness of service is suffering significantly. Without thoughtfulness and planning, over-collection and over-processing can significantly increase costs even where the per-unit price is extraordinarily low. Like automobile sticker prices, per-unit pricing is important, but it is not the primary metric of success. This is why many companies that have negotiated master service agreements with exceptionally low per-unit costs are not as happy as they thought they would be.

Instead, companies should work more to identify partners who can add the most value to their overall process, and who are willing to work with them on constant improvements in efficiency and risk reduction. This is a far more important measure over time than simply cutting the costs on each service offering ever could be. And only then will the company start to see true reductions in per custodian spend, in overall risk exposure, and their overall legal budgets.