State of the Union on Data Privacy & Security

Since beginning the annual Advice from Counsel study in 2009, we’ve interviewed hundreds of in-house legal teams on the big trends and best practices impacting e-discovery and information governance.

We’ve presented findings that showcase the people, process and technology that have evolved e-discovery and information governance from an expensive, ad hoc activity to a streamlined and repeatable business process. In an anonymous setting, respondents have at times vented, boasted and cringed about their activities taking place at the tricky intersection of enterprise data and legal and regulatory matters.

As we report the findings from our twelfth study, we’re reminded that today’s challenges are very similar to those in e-discovery’s nascent years – control, quickly finding what’s important, helping to lead organizational change – but the focus has shifted from e-discovery to data security and privacy. To help us better understand how issues of data security and privacy are impacting in-house legal teams, we interviewed 30 in-house counsel for their thoughts and advice on three key and intersecting topics: the General Data Protection Regulation (GDPR), information governance and security, and data remediation.

This paper outlines their top areas of concern as well as practical advice for others that are new to issues of data privacy and security. From these results, corporate legal teams can hopefully avoid common pitfalls and work towards implementing programs that better protect their organization from risk.
In May of 2018, the European Union will begin enforcement of GDPR and many global organizations are waiting to see how rigorous the regulators will be in enforcing the new data privacy rules – which may include fines of up to 4% of annual revenues.

Nearly 80% of Advice from Counsel respondents said that their companies will be impacted by GDPR, and they shared a wide range of concerns in preparing for the new rules, including:

- **How do we keep personal and corporate data separate?**
  
  From the rise of BYOD in the workplace to 'shadow IT' systems accessed without knowledge or permission by the enterprise IT team, respondents worry that the steps necessary to keep personal data secure are incompatible with today’s workstyles. As one respondent stated, “I think companies will be much stricter about the use of personal e-mail systems. It is harder for the company to get to that information if you tell them it is mixed with corporate data. As a result, you will continue to see people walk around with two devices as privacy rules become stricter.”

- **How can we focus on data security when regulations require so much attention?**
  
  For many organizations, the same team focused on data breaches will also own GDPR compliance, forcing the team to juggle resources across two important projects: “You would prefer your information security experts to focus on preventing cyber-security compromises, but instead they have to dedicate so much time and energy to complying with the complex regulatory environment.”

- **How much do we need to invest in order to ensure compliance?**
  
  A number of A&C respondents worried that the level of investment necessary to ensure GDPR compliance would take away from other activities. “There is no way to get around funding a greater investment in that business for privacy compliance. It will crowd out investment in innovation. We will invest less in innovation to meet the new EMEA data privacy requirements.” As another respondent stated, “I think this is a big deal and will be very difficult for American companies to implement. It will be costly and I don’t think it will be an easy thing for people to implement.”

From the rise of BYOD in the workplace to 'shadow IT' systems accessed without knowledge or permission by the enterprise IT team, respondents worry that the steps necessary to keep personal data secure are incompatible with today’s workstyles. As one respondent stated, “I think companies will be much stricter about the use of personal e-mail systems. It is harder for the company to get to that information if you tell them it is mixed with corporate data. As a result, you will continue to see people walk around with two devices as privacy rules become stricter.”
ADVICE:

Respondents were evenly divided among those waiting to see what will happen, and those that were trying to get out in front of any penalties. No matter the approach, legal teams suggested a few activities to prepare for GDPR:

**ADVICE:**

Respondents were evenly divided among those waiting to see what will happen, and those that were trying to get out in front of any penalties. No matter the approach, legal teams suggested a few activities to prepare for GDPR:

**Conduct a GDPR assessment that includes a data map of personal data inventory.**

A third party can cost-effectively assess the enterprise data environment, map where personal data resides, and develop a list of recommendations on areas to prioritize. One respondent recently completed this process and commented that the results were helping the organization on “updating policies and procedures, privacy notices and consents, data breach responses, security controls, supplier management protocols, and accountability within the company to ensure compliance (including the right level of sponsorship).” This exercise can produce additional benefits, such as helping to update a stale records retention program, or reducing storage costs.

**Re-examine and update policies.**

Legal teams suggested getting policies in order and evaluating whether “changing things like consent, converting to opt-in correspondence… and standard contract clauses” can produce some easy and quick wins.

**Think beyond Europe.**

Advice from Counsel respondents also cautioned that GDPR is just one data privacy regulation and that other countries and regions have similar programs in place. “The EU gets all of the attention with data privacy, but it should not be lost that there are many markets like Mexico that have fairly sophisticated data privacy regimes and impose significant fines for running afoul of those laws. People need to think outside of the EU box, which is often very restrictive, but there are many others that are similarly restrictive.”

**KEY TAKEAWAY**

No matter the company’s risk profile or footprint in Europe, data privacy is a growing global concern. Legal teams should consider evaluating their current processes and/or hire internal resources or bring in a third party to help determine program gaps and steps to ensure that employee and customer data remains secure.

The connection between information governance and data protection has long been a focus within highly regulated industries such as healthcare and financial services. As high-profile data breaches continue to dominate the business news, companies of all stripes are beginning to implement information governance programs that can help better protect data. As one respondent said, “Take it seriously. It is an area that can land you on the front page of the Wall Street Journal if it is not handled properly.”

We asked our participants to share concerns that may fall below the radar for many teams as they work to protect data against breaches:

**Effective information governance and data security programs require executive level sponsorship and funding.**

The c-suite may not yet understand the role information governance plays in protecting data. As one respondent noted, “We do not have uniform buy-in from management that information governance is important. Short of banging your head against the wall, you need to keep revising the issue. We are trying to look at issues or problems, and catalog them, and use them as a use-case for management as way of encouraging them to address it.”

**IT and Information Security are not interchangeable.**

The AfC community was clear that the two have different skillsets. “Not understanding the difference is a critical issue. IT’s job is to get the system up and running. Information security is looking at the investigation for securing the data. They are going to approach it slightly different-ly…..There is a difference between IT and information security so you need to go to the right person at the right time.”

In today’s business climate, all organizations are challenged to better protect enterprise data. It’s not an easy task and requires executive buy-in, deep technical expertise, a holistic approach to mapping the internal and external data environment, as well as consistent training and practice. Third party providers can conduct data protection assessments to find weaknesses, identify priorities and help legal, IT and information security teams execute a plan designed for the company’s risk profile.

Reputedly, respondents made clear that this is an area that is evolving quickly and teams need to work with technical experts to handle effectively. “This is a space where there is real expertise. You need to find the correct individuals to assist.” Another stated, “You should have an expert in-house because it is not the same thing as e-discovery. It is not something you can just wing. You need to have an expert and you need to have a plan in place.” A third suggested, “Leverage really good technical experts – it can be internal or external. The legal team understands broad principles, but cannot solve the problem. They typically don’t know about encryption or an air-gap network. Certain laws require encryption, but lawyers are not sure how to build it into an IT solution.”

Prioritize the crown jewels. “Start with focusing on what information is truly important to protect because you cannot protect everything. Look at the NIST framework for cyber-security as it’s probably the best and most comprehensive framework available. Start with classifying your important information and then create a DLP program. Focus on the data and then endpoint/firewall security. There is a lot you can do that is not too complicated to keep the malware out. Keep it simple stupid and enforce order in your organization.”

Don’t forget back-up tapes. Back-ups can contain sensitive IP and are often overlooked when it’s time to remediate data. As one respondent recommended, “Pay special attention to testing environments and back-up tapes. That is a real security issue and a big one that sneaks up on people. It presents a challenge to back-up tapes if you are keeping them. The test environments should require that people eliminate data when they are finished testing. There is not a lot of rigor put around test environments and that is an issue. Back-ups are a huge problem for everyone! Nobody that I know of has a great solution to the back-up problem.”

Address the human element. Technology can only go so far, according to the AfC community. "Corporate America has spent billions on cyber security and we may not be much safer than we were 5-6 years ago because of the increasing sophistication of the criminals and because human error causes more data leakage than the hackers. The two types of dangerous humans are the malicious insider or the inadvertent one. Focus on awareness training and anti-phishing campaigns. Focus on the human is my recommendation.” Another respondent commented that a good first step for any program is to “create a culture of awareness of the importance and risk of data.”

Audit security practices of your law firms and legal service providers. Many legal teams worry about their internal processes and security, and overlook testing that of their law firms and service providers, even if they handle the same data. “Start paying more attention to the security and privacy practices of your law firms and vendors. It is an underrated security risk.”

Practice. Want to know how your systems and team will respond when a real breach happens? Do practice drills. “Have your IT department send out phony phishing e-mails and conduct practice drills. If an e-mail comes from outside the company, it has a designation and all e-mails contain a report phishing icon.” In addition to helping you identify weaknesses, practice drills can help reinforce the importance of data security. As one respondent said, “I am more careful and more thoughtful about the e-mails that I open” as a result of practice drills.

Seek out experts and benchmark against peers. Repeatedly, respondents made clear that this is an area that is evolving quickly and teams need to work with technical experts to handle effectively. “This is a space where there is real expertise. You need to find the correct individuals to assist.” Another stated, “You should have an expert in-house because it is not the same thing as e-discovery. It is not something you can just wing. You need to have an expert and you need to have a plan in place.” A third suggested, “Leverage really good technical experts – it can be internal or external. The legal team understands broad principles, but cannot solve the problem. They typically don’t know about encryption or an air-gap network. Certain laws require encryption, but lawyers are not sure how to build it into an IT solution.”

Be thoughtful about employee training. Data security is a serious issue but employee training can backfire if it’s too heavy-handed. As the Advice from Counsel community advised, “Try to tackle it without trying to fear monger. Most companies address this issue through fear mongering, but then employees lose their focus on it.”

FOR THOSE EVALUATING WHETHER AND HOW TO IMPLEMENT AN INFORMATION GOVERNANCE STRATEGY TO BETTER PROTECT DATA, OUR RESPONDENTS HAD ADVICE:
Data Remediation

Organizations know they are creating and saving too much data, but don’t know where to begin in remediating content. While rules exist that dictate retention of corporate information, especially in highly regulated industries, the amount of over-retention and ROT is so massive, organizations may not know where to begin with a data remediation project. Also, data remediation is contrary to human nature, and storage prices are low. One legal practitioner said “I want to save every e-mail I have ever sent,” but knows that “the liability for it is too great.”

Outside legal holds and human nature, the Advice from Counsel community shared a few other areas of concern:

**Balancing data remediation with Big Data projects**
The growth of cloud storage and machine learning is making it easier for organizations to identify trends and realize monetary benefits from enterprise data. Finding the right balance between Big Data and over-saving can be a challenge. “You want to be aware of the competing issues involved in data remediation. While you want to comply with legal holds and statutory issues involved with preserving that information, as well as costs of culling through it, there are benefits of maintaining that information from a Big Data standpoint. Speak with your technologists before removing it to determine whether there is opportunity in the data.”

**Getting budget and buy-in**
Building a business case for data remediation can be difficult for organizations that are already strapped for resources. It may also seem counterintuitive given declining storage costs. “Records management is about getting rid of information that is not important, but IT is acknowledging how inexpensive storage is so they are keeping data. The business case for records management is changing as storage costs drop.”

**Looking beyond email**
“There is a tendency to focus just on electronic data, but there is also information in paper documents that might be unstructured and known to people from time to time. In the course of data remediation, we have found information in paper documents or unstructured documents online that was not in a system and protected (e.g., old payroll records and W2s). Recognize there is legacy information and either protect it or delete it.”

**KEY TAKEAWAY**
Taking control of enterprise data through a data remediation program can dramatically reduce enterprise risk and costs. Building a business case, ensuring executive buy-in, training staff and executing an effective program to address today and tomorrow’s challenges – these are serious roadblocks that if overcome, can help put your company on better footing as data volumes and formats further expand.

For more information on legal holds, data remediation, data mapping and achieving quick wins, please visit http://www.ftitechnology.com/solutions/information-governance-and-compliance-consulting-services.
THERE IS HOPE, HOWEVER. MORE THAN HALF OF THE ADVICE FROM COUNSEL RESPONDENTS HAD SUCCESSFULLY CONDUCTED DATA REMEDIATION PROJECTS AND PROVIDED THE FOLLOWING ADVICE TO OTHERS:

- **Minimize business disruption.**
  When it comes to internal data remediation, a project has a greater chance of success if it can be customized to how employees work. For example, “end users would rather be touched once with a single tool than 12 times with multiple tools so streamline how much you need to touch the customer to engage in data remediation.” Also, make the decision-making process as easy as possible for employees. “People who are not in IT don’t want to be responsible for stuff they think IT or information governance should do. They don’t want to have to think about whether something should be declared a record or to effectuate disposition. They want the legal and IT teams to work behind the scenes.”

- **Future-proof the program.**
  How can you ensure that fewer data pools are created in the future? “Build controls into any new initiative before it is launched so you have already asked people about the disposition plan. Build it into the requirements in advance because it is very hard to do after you have amassed data.”

- **Look for quick wins.**
  For some, starting a small project can help your team learn about what works and also gain broader momentum. “We acquire a lot of companies so while we want to be proactive, our data practices are often reactive…. Each business unit has its own way of storing data…. Start small and work with a dedicated team. Select a single business unit with which the legal team has a strong relationship and use it as a pilot partner when focused on data management issues. Once successful, you can tell that story on a broader scale.”

- **Make the most of bad events.**
  If your company or a competitor faces a significant event, use that as a catalyst to advocate for a change. According to one assistant general counsel, “Your business case has to come after an adverse event. The company hasn’t implemented a program and hasn’t had the e-discovery issues that other companies have had. I think you need an event to motivate the company to do that. You need a significant e-discovery event to help precipitate change.”

- **Figure out what you have.**
  “It is impossible to do appropriate record destruction unless you know what you have in the first place.” Conducting a data mapping exercise is often the first step in identifying redundant, old or trivial data that is ready for remediation.

- **Target PST files.**
  PST files are low-hanging fruit when it comes to data remediation. “A PST is a huge file so if an employee wants, they can save individual messages to their hard drive/jump drive or copy all of their personal folders to a PST file. That is generally implemented on the local hard drive and so you end up with people having huge PST files and there is no way to really enforce archiving once a file has been moved to a personal folder.”

- **Consider automation.**
  Developing a policy is one thing, but executing it can be a challenge. Respondents reported success in using a wide variety of software tools to set a data remediation schedule and actually implement it. “Automated systems are increasingly used and serve as the only way to get people to pay attention.”

- **Find internal partners to secure buy-in and funding.**
  Projects have greater chances of success when you partner with another team or executive – CIO, data governance officer – to “ensure that the message of support for data remediation is heard throughout the company. Sometimes funding data remediation is a challenge and partnerships can make it easier to obtain financing since others can advocate for you and help explain the need for the investment.”

- **Training is critical.**
  “Train staff on the company’s retention policy. People should be more trained and aware of the need for document retention because there are significant fines and penalties in certain jurisdictions for improper data management. Think about it as you would as it if it were any part of your compliance program. Apply similar types of rigor around it.”
Appendix

Ari Kaplan Advisors personally interviewed 30 in-house lawyers with responsibilities that included some aspects of e-discovery and information governance. Most participants were from Fortune 1000 corporations and all spoke by telephone, under condition of anonymity, during November and December of 2016.

Of this year’s participants, 79% develop and implement e-discovery processes while 89% develop and implement information governance processes.

80% of participating organizations had total annual revenues greater than $5 billion and 67% had over 10,000 employees. In terms of litigation events over the past 12 months, 33% reported managing 100 to 500 litigation events, and 33% reported managing more than 500 litigation events.

By Industry:

- 30% Financial services, including banking and credit institutions, as well as insurance companies
- 33% Manufacturing
- 7% Life sciences
- 10% Technology
- 3% Energy and utilities
- 3% Construction
- 3% For-profit education
- 3% Entertainment
- 3% Hospitality
- 3% Retail

3% Energy and utilities
3% Construction
3% For-profit education
3% Entertainment
3% Hospitality
3% Retail
7% Life sciences
10% Technology

30% Financial services, including banking and credit institutions, as well as insurance companies
33% Manufacturing
Participants’ Annual Revenues Totals for 2015:

Number of Employees at Participants’ Companies:

Number of Litigation Events in the Past 12 Months:
About the Authors

Ari Kaplan
Ari Kaplan Advisors


In addition to serving as the principal researcher for the Advice From Counsel series since its inception, he has been the keynote speaker for events in Australia, Canada, the United Kingdom, and throughout the U.S, including the 2010 ABA Techshow.

Chris Zohlen
FTI Technology

Chris Zohlen is a managing director in the FTI Technology segment’s Information Governance, Security & Privacy practice. He assists legal, records, IT and information security departments identify, develop, evaluate and implement in-house e-discovery and information governance processes, programs and solutions. These solutions are designed to produce the largest return on investment while simultaneously reducing risk. Prior to joining FTI Technology, Chris Zohlen was an executive within IBM’s Information Lifecycle Governance (ILG) business. He graduated Cum Laude from Cal Poly San Luis Obispo with degrees in Business Administration and Computer Science.
About Advice from Counsel

Through in-person events, virtual meetings, webcasts, surveys and reports, Advice from Counsel helps e-discovery leaders share ideas and advice with peers in an open and collaborative forum. Since it’s inception as an annual survey and report on top e-discovery trends, Advice from Counsel has evolved into an interactive community of e-discovery professionals working to strengthen the people, process and technology at the core of e-discovery. Advice from Counsel is sponsored by FTI Technology.
FTI Technology solves data-related business challenges, with expertise in legal and regulatory matters.

As data grows in size and complexity, we help organizations better govern, secure, find, analyze and rapidly make sense of information. Innovative technology, expert services and tenacious problem-solving provide our global clients with defensible and repeatable solutions. Organizations rely on us to root out fraud, maintain regulatory compliance, reduce legal and IT costs, protect sensitive materials, quickly find facts and harness organizational data to create business value.

For More Information:
ftitechsales@fticonsulting.com
www.ftitechnology.com

North America: +1 (866) 454 3905
Europe: +44 (0) 20 3727 1000
Australia: +61 (2) 9235 9300
Hong Kong: +852 3768 4500
Shanghai: +86 21 5108 8002
Tokyo: +81 3 5369 3939