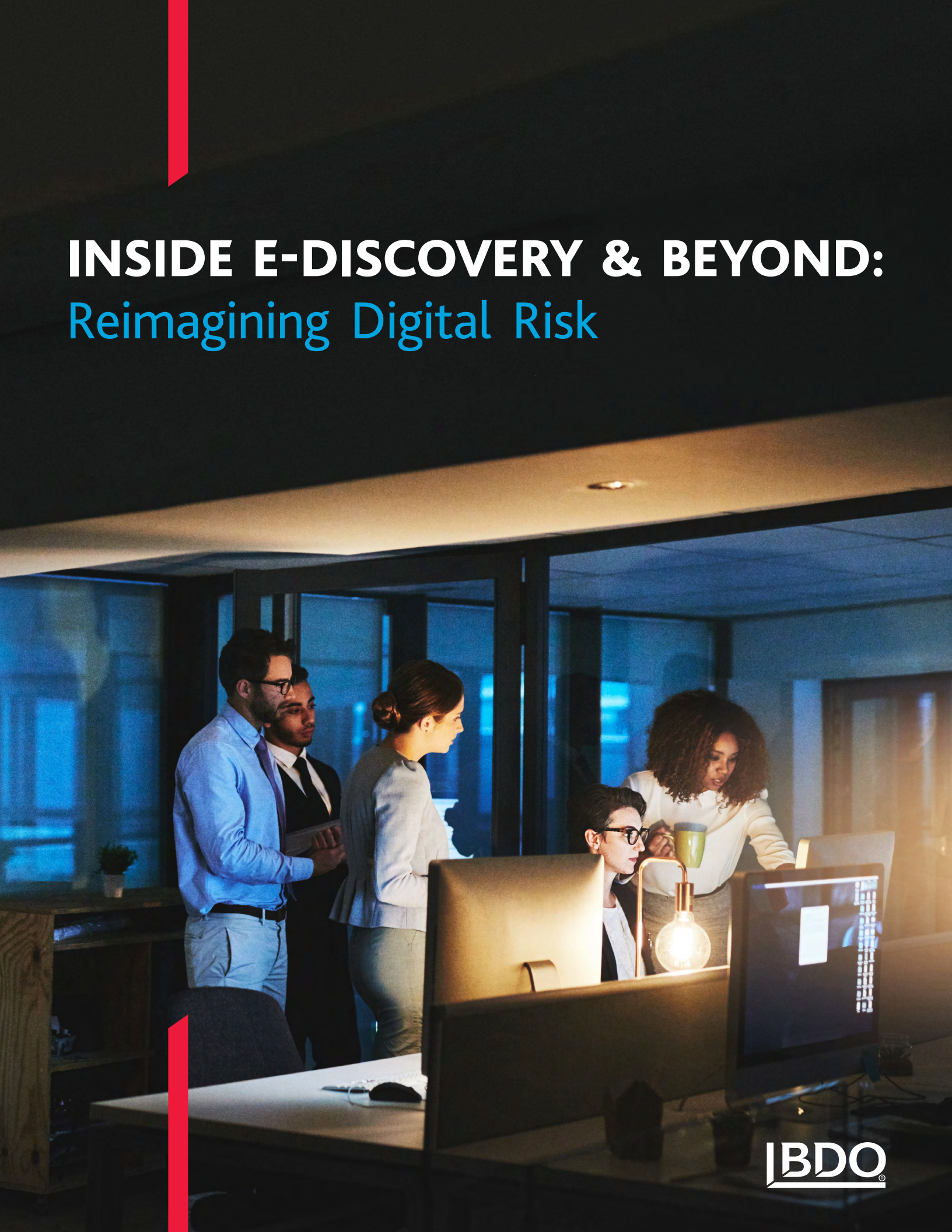
INSIDE E-DISCOVERY & BEYOND:
Reimagining Digital Risk



BDO

CONTENTS

Big Data Gets Bigger

Big Data — the catchall term to describe the explosive growth of digital information — continues to get bigger in every way. In the 12-plus years since the Federal Rules of Civil Procedure (FRCP) were amended to explicitly and emphatically include Electronically Stored Information (ESI) on the list of discoverable materials, the digital universe has expanded beyond our wildest imaginings. Volumes continue to explode; by 2025, research firm IDC estimates the global datasphere will grow to 163 zettabytes — a tenfold increase from the 16.1ZB of data generated in 2016. Variety expands daily; where once we worried primarily about email and office files, now we need to contend with the Internet of Things (IoT), which means myriad forms of data in almost anything that uses electricity. And Velocity and Veracity — two other key measures of Big Data — are increasing apace.

As data transforms every aspect of our lives, from the way we communicate with one another to the way we do business, the role and responsibilities of in-house legal professionals are transforming too. E-discovery is just the tip of the iceberg. Inextricably tied to every aspect of the business, data is now viewed as an organization's most valuable asset. And yet data also can be a company's greatest source of risk. Corporate counsel must contend with multiple—and often competing—demands on data use from different internal and external stakeholders. Think not just Legal and IT but Compliance, HR, InfoGov, InfoSec and business lines internally, and clients and customers, suppliers and regulators externally… and those lists can go on and on. As a result, corporate counsel's responsibilities as legal guardians are expanding to take on new areas of digital risk, and their roles are evolving to more actively participate in strategic business decisions.

In this evolving digital risk landscape, the fourth annual Inside E-Discovery & Beyond survey by BDO examines the opinions and insights of more than 100 senior in-house counsel about changes in their approaches to e-discovery, information governance, compliance and cybersecurity.

"Ultimately, today's corporate counsel must take a holistic view of their organization's digital risk profile — assessing risk based on data flows, cross-functional interdependencies and global operations —and play a proactive, rather than reactive, role in risk-based strategic planning."

STEPHANIE GIAMMARCO
Partner and BDO Technology & Business Transformation Services Practice Leader

Read more ▶

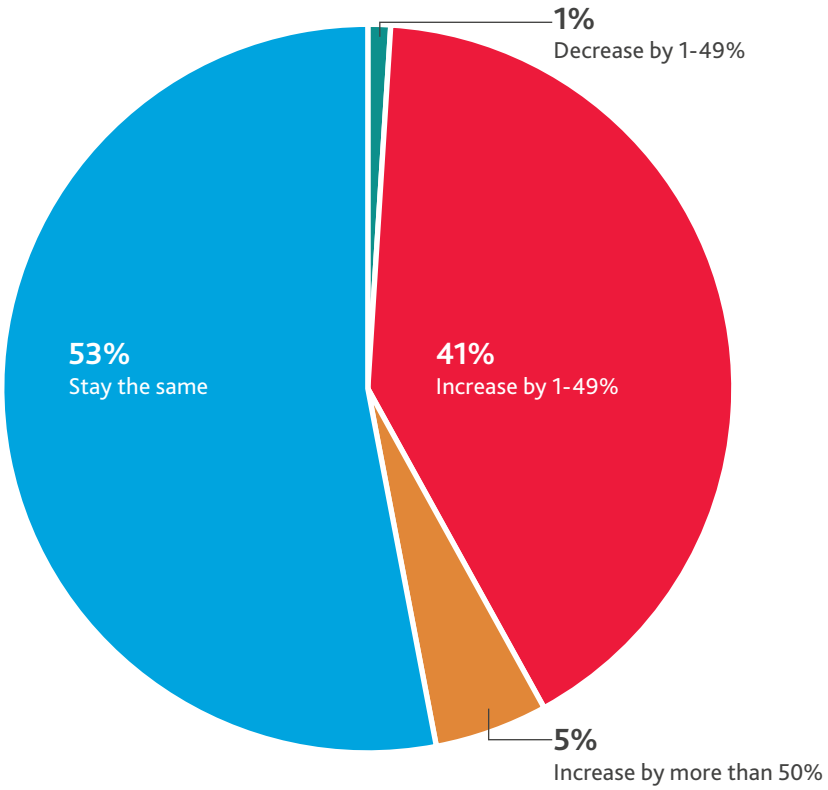
All About Information Governance

Information governance is foundational to e-discovery. Bookending the start and finish of the e-discovery process, it directly impacts the cost, speed, and soundness of decision-making. But e-discovery is just one piece of the puzzle. A proper information governance program encompasses everything from traditional records management, to compliance and risk management, to litigation preparedness, cybersecurity, IT governance, data privacy and overall operational excellence.

According to this year's survey, 46 percent of senior counsel plan to increase their information governance spend in the next 12 months, while 53 percent expect to keep their spending the same. Just one percent intend to decrease their information governance spend.

Most in-house legal teams understand the need to preserve and collect information to respond to a discovery request. But increasingly, corporate counsel are being asked to revisit their organization's information governance policies and procedures with an eye toward increasing efficiencies and value. Of the 90 percent of survey respondents whose organizations have a defined information governance program, 42 percent of those programs are led by Legal, surpassed only by the CIO (47 percent) – indicating corporate counsels' roles are evolving to include a greater focus on digital assets.

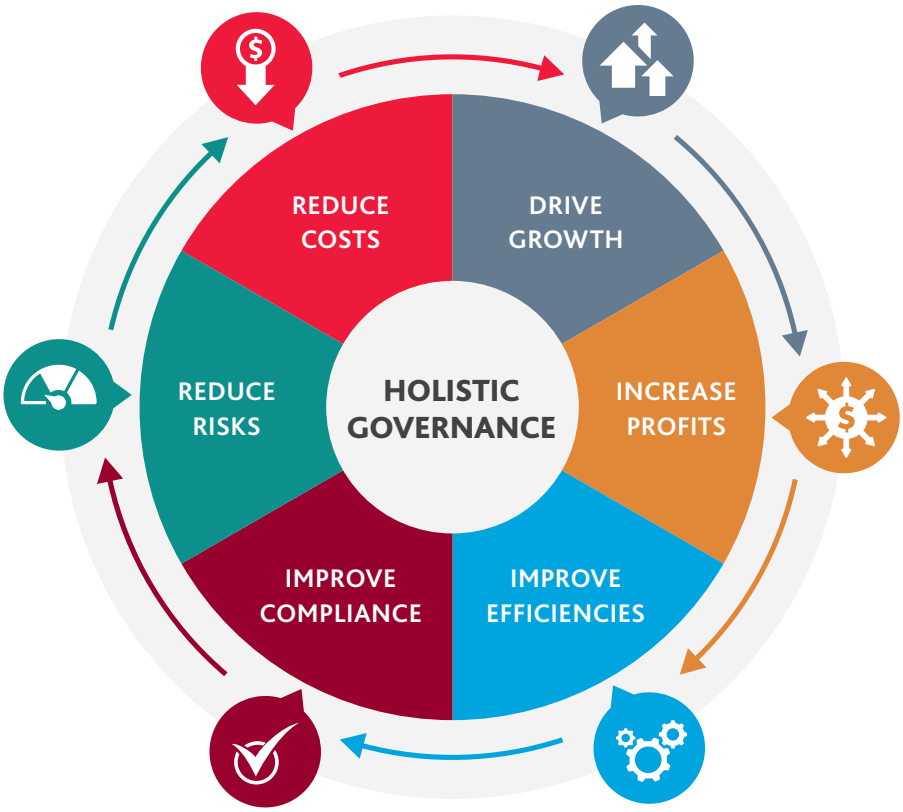
HOW WILL YOUR TOTAL SPENDING ON INFORMATION GOVERNANCE CHANGE IN THE NEXT YEAR?



"An effective approach to information governance enables the organization to leverage information as an enterprise asset and fortify its security. Data, after all, is only as valuable as your ability to know what you have and how to use it."

MARK ANTALIK
Managing Director, BDO Technology & Business Transformation Services

Read more ▶



BDO PREDICTS...

2018 is the year to organize your own IG neighborhood cleanup! It's no longer enough to get your own electronic house in order; now you need to clean up the entire neighborhood, turning your focus beyond your own systems to your entire extended business ecosystem.

Here are three ways to get your arms around this bigger, messier world of data:

1. IDENTIFY THE GAPS

What you don't know will come back to haunt you, so gather information now, find out where your data goes, look beyond the first hop, and search for vulnerabilities, remembering to go up and down the value chain.

2. PROVIDE THE RIGHT SUPPORT

Devote the right people and tools to make sure your data gets handled properly. Make sure you and your partners are committed to the effort and stay abreast of data and privacy rules and regulations in the U.S. and around the world.

3. IMPROVE QUALITY

Develop, implement, and follow effective wide-ranging information governance policies and practices—ones extending beyond the limits of your organization—to reduce duplicative, outdated, and unnecessary data inside and outside company walls.

Read more

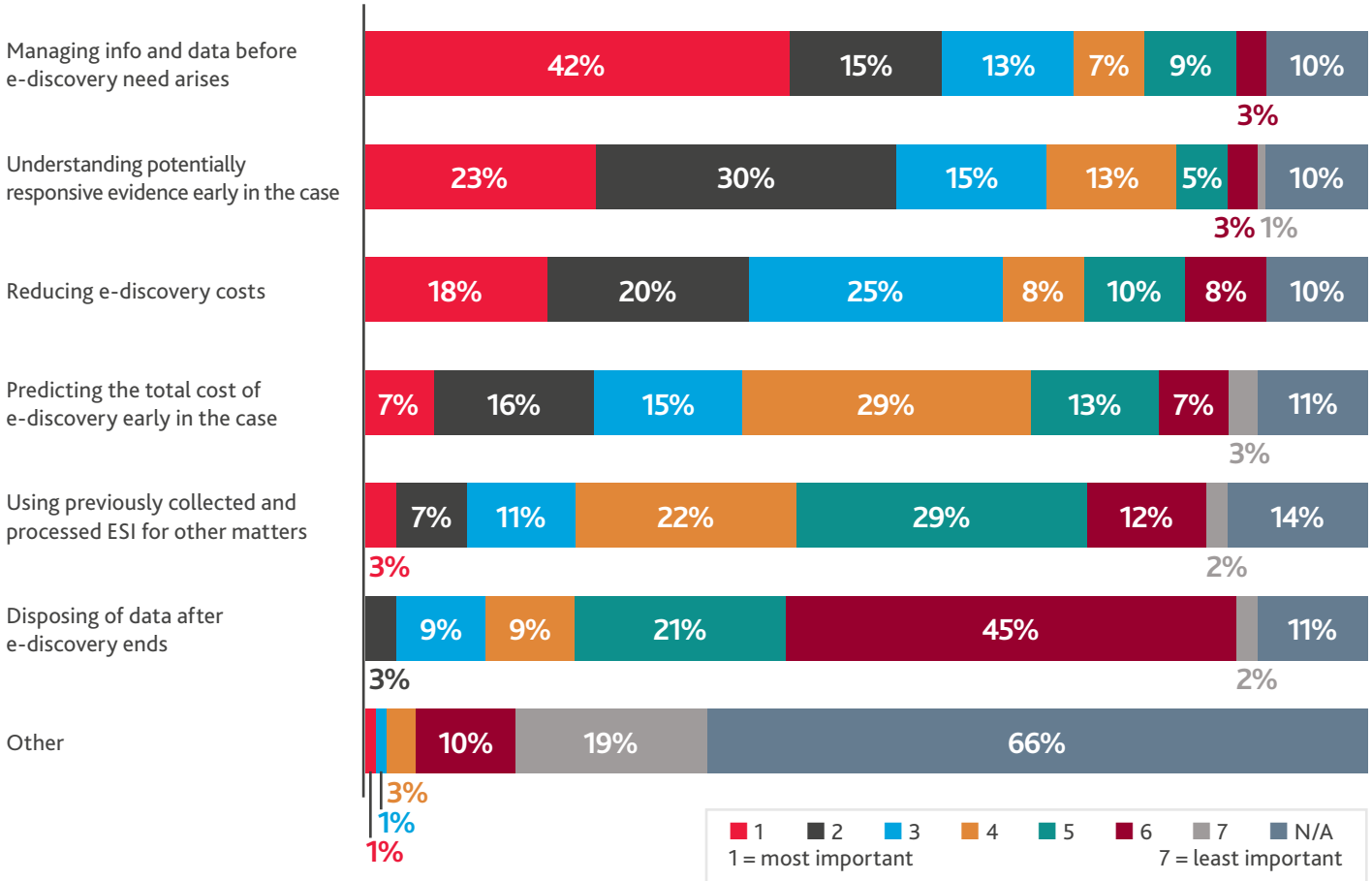
Managing E-Discovery: The Early Bird Gets the Worm

For the second year in a row, survey respondents ranked managing information and data before a need arises as the most important factor in managing e-discovery litigation (42 percent), followed by understanding potentially responsive data early in the case (23 percent) and reducing e-discovery costs (18 percent).

"Implementing a data retention and disposition strategy as part of the ordinary course of business, prior to when the preservation duty kicks in, is a great way to control the amount of data subject to discovery. This simultaneously enhances the ability to quickly develop an early understanding of what information is available and to begin to contain the likely scope and ultimate cost of the entire e-discovery process."

GEORGE SOCHA
EDRM Co-Founder and Technology & Business Transformation Services Managing Director

PLEASE RANK IN ORDER HOW IMPORTANT EACH OF THE FOLLOWING FACTORS IS IN HOW YOU MANAGE E-DISCOVERY IN LITIGATION.



Read more ▶

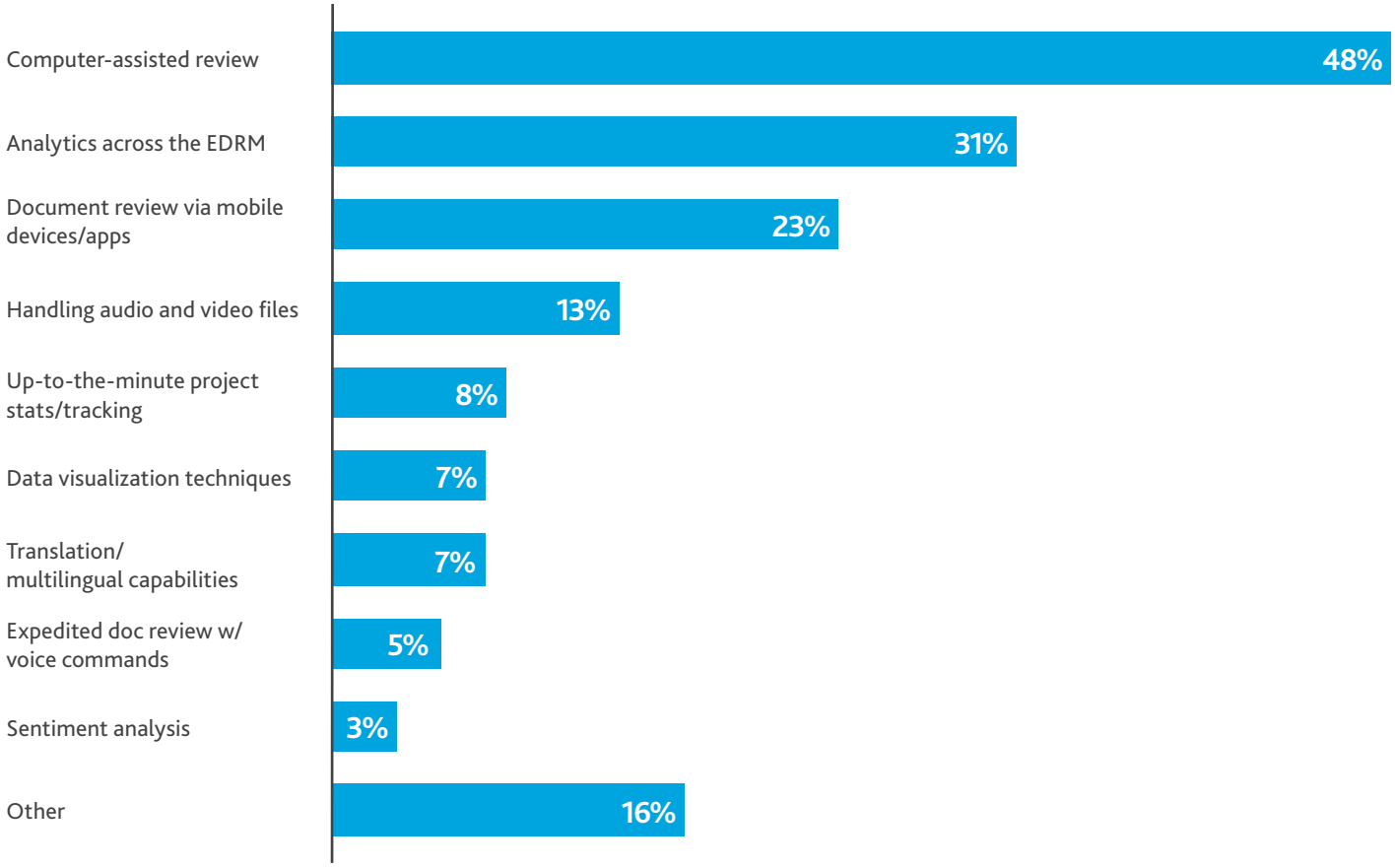
But as Big Data gets bigger, effective management of the ever-expanding data universe is easier said than done. Non-standard and unstructured data sets — audio files, images, text messages, interconnected databases and, increasingly, data from internet-connected sensors — add new layers of complexity to every stage of the e-discovery lifecycle. In recent years, the exponential growth of structured and unstructured data has made a human-only approach to e-discovery review, if not impossible, exorbitantly expensive and time consuming. The adoption of technology-assisted review (TAR) and its subsequent legitimization in case law has resulted in significant time and cost savings for corporate counsel.

If only out of necessity, corporate counsel are finally embracing e-discovery technology advances. Almost half (48 percent) of survey respondents are currently using TAR — an increase of 8 percentage points over last year.

In addition, 31 percent report using analytics across the EDRM, and 23 percent leverage mobile document review.

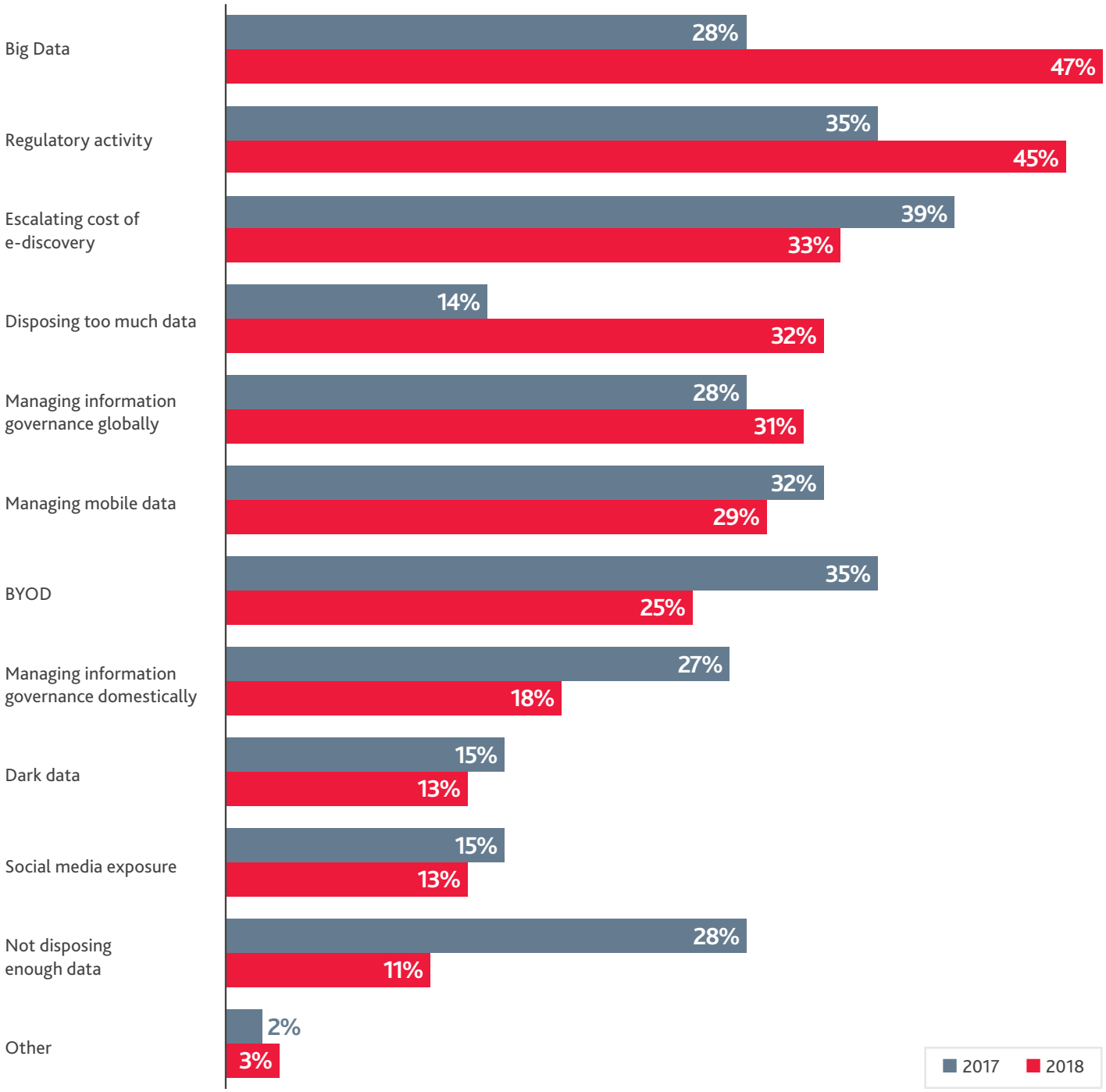
Despite a helping hand from technology, corporate counsel clearly still grapple with the increases in the volume, velocity, variety and veracity of data in the context of e-discovery and the challenges associated with those increases. When asked to choose the three biggest e-discovery-related issues that would have an impact on their business in the future, survey respondents cite Big Data (47 percent), regulatory activity (45 percent), and escalating costs (33 percent). In last year's survey, just 28 percent of respondents ranked Big Data in their top three, with the highest percentage (39 percent) selecting escalating costs.

WHICH OF THE FOLLOWING INNOVATIONS/TECHNOLOGICAL ADVANCES ARE YOU CURRENTLY EMPLOYING WITH RESPECT TO E-DISCOVERY?



Read more ▶

LOOKING FORWARD, WHAT E-DISCOVERY ISSUES WILL HAVE THE GREATEST BUSINESS IMPACT ON YOUR ORGANIZATION? RESPONDENTS WERE ASKED TO CHOOSE THEIR TOP 3 ISSUES.



Read more ▶

BDO PREDICTS...

For years, attorneys and judges alike have said IoT—at least when it comes to e-discovery—is hype. We don't agree. As IoT devices become more pervasive—at home, at work, on your body, and around town—the vast amounts of data and information they store are becoming invaluable evidence.

Our 2018 prediction: Alexa, FitBit and their friends are going to be asked to testify a lot more. At a time when practitioners still struggle with mobile data discovery, expanding the scope of e-discovery to include IoT data introduces a host of new challenges, forcing organizations to reevaluate their approach to data preservation and better understand the data insights that can be extracted. The amended FRCP proportionality rules may help rein in overzealous discovery requests and overcollection, but what constitutes proportionality in the age of IoT is an open question.

VIEWS FROM THE BENCH

The 4th Annual Federal Judges Survey: Judicial Perspectives on the State of E-Discovery Law and Practice collected survey responses from 30 current or recently retired Federal Judges about their views on the state of e-discovery law and practice, including the legal community's e-discovery proficiency and areas for improvement.

Key insights include:

Attorneys' skills still lacking: While e-discovery specialists and large law firms tend to have a high level of expertise, generally attorneys have been slower to develop their e-discovery competence.

More e-discovery education needed: Almost half the judges feel e-discovery education should be mandatory, either in law school or through continuing legal education courses.

Actively manage outside counsel: Legal teams and departments must make sure that outside counsel represent their wishes accurately, most importantly actively advising them to manage costs and steering cases toward resolution, not increasing conflict.

Know the Rules: The surveyed judges believe the 2015 amendments to the Federal Rules of Civil Procedure have helped courts and parties move closer to the "just, speedy, and inexpensive" resolution of legal matters, but the Rules' efficacy is predicated on both the bar's and the bench's awareness and use of them.

Proportionality catches on: Specificity matters. Proactive, data-supported, solution-oriented arguments will carry the day, while boilerplate objections and overly broad requests will not.

Reduce gamesmanship: Preservation practices have largely stayed the same, but the Rules, and the judges, have less and less tolerance for "gotcha" tactics.

Download the full analysis from the 2018 Judges Survey here.

Read more ▶

Digital Compliance Challenges

As lawmakers play catchup with the data deluge and its legal implications, corporate counsel are in an uncomfortable position. They're accustomed to making decisions based on precedent and clearly established policy, but the legal lines are actively being drawn. The rules and regulations governing the digital economy are either outdated or still awaiting that first legal test—and no one wants to be the guinea pig. At the same time, in-house counsel must also consider how these emerging legal and compliance data risks intersect with other areas of enterprise risk—all without stifling opportunities for digital innovation.

Nowhere is this challenge more evident than in the uncertainty surrounding the General Data Protection Regulation (GDPR). Replacing the EU's Data Protection Directive, the GDPR, effective May 25, 2018, will require companies controlling or processing EU citizens' personal data to follow key requirements. More than half of U.S. companies say the law—far stricter than U.S. data privacy protections—would increase levels of complexity and red tape within their business, Censuswide found in a November 2017 survey. And about 35 percent doubt they'll be fully prepared for the regulation in time for the deadline.

Our survey found that nearly half (48 percent) of senior in-house counsel are aware their organization is required to comply with the GDPR. Sixteen percent also say they must comply with Circular A-130, which provides general policy for the planning, budgeting, governance, acquisition, and management of Federal information resources—and was also recently revised for the first time in 15 years.

Forty-eight percent of survey respondents claim the GDPR is not applicable to their organization. Chances are high that many of these companies are wrong. Any U.S. or foreign company that deals with EU citizens' personal data—and definitions are not entirely clear—will be subject to the GDPR's stringent requirements—even if doesn't operate in any of the 28 EU member states.

"It behooves every organization—whether they touch EU personal data or not—to regularly review how information is used and managed to maximize its value and minimize risk. GDPR is just the catalyst for a higher standard of data privacy and protection to which every company should aspire."

KAREN SCHULER
BDO National Data & Information Governance Practice Leader

BDO PREDICTS...

We're calling it now: Sometime in 2018, the European Court of Justice (ECJ) will come down hard on a U.S. company for GDPR non-compliance.

They won't be alone; we anticipate a significant number of companies to which GDPR applies will fail to be in compliance by the May 25 deadline. And though we don't know for sure, we're betting at least one of them will get hit with the heaviest of financial penalties possible for non-compliance: €20 million or 4 percent of annual worldwide turnover.

Read more ▶

Legal Officers' Cyber Responsibilities Expand

It's impossible to ignore the elephant in the room: cybersecurity. The future of crime, financial and otherwise, is digital, and the corporate rulebook will change along with it.

Last year, our survey found that 74 percent of corporate counsel ranked a data breach as their organization's top data-related legal risk. In fact, the numerous attacks in recent years have been serious and costly enough to prompt action at the state and federal levels. The Federal Trade Commission has been particularly active in its data privacy enforcement actions, issuing charges against a number of high-profile organizations.

In addition, organizations that experience a data breach run the risk of facing a class-action lawsuit. The issue of standing—a threshold plaintiffs have mostly failed to reach in data breach litigation—is actively being decided by the courts. The Eighth Circuit's recent ruling on Article III standing for data breach litigation may encourage more plaintiffs to initiate suits. For a particularly poignant example of the potential damages, just look at Yahoo's 2013 email data breach, which resulted in more than 40 lawsuits and the resignation of the company's chief legal officer.

"Most organizations recognize no system is impenetrable, and attacks will get through. As data breach litigation increases, corporate counsel will need to build a case to disprove cyber negligence."

GREGORY A. GARRETT
Head of U.S. and International Cybersecurity, BDO LLP

Reflecting a heightened level of priority, 73 percent of respondents believe their boards are more involved in cybersecurity than they were 12 months ago. Of respondents who are aware of board meeting proceedings, 43 percent say their boards are briefed on cyber on a quarterly basis, and another 17 percent say their boards are briefed more frequently than that. Just 7 percent of respondents claim their boards are not briefed at all on cybersecurity matters.

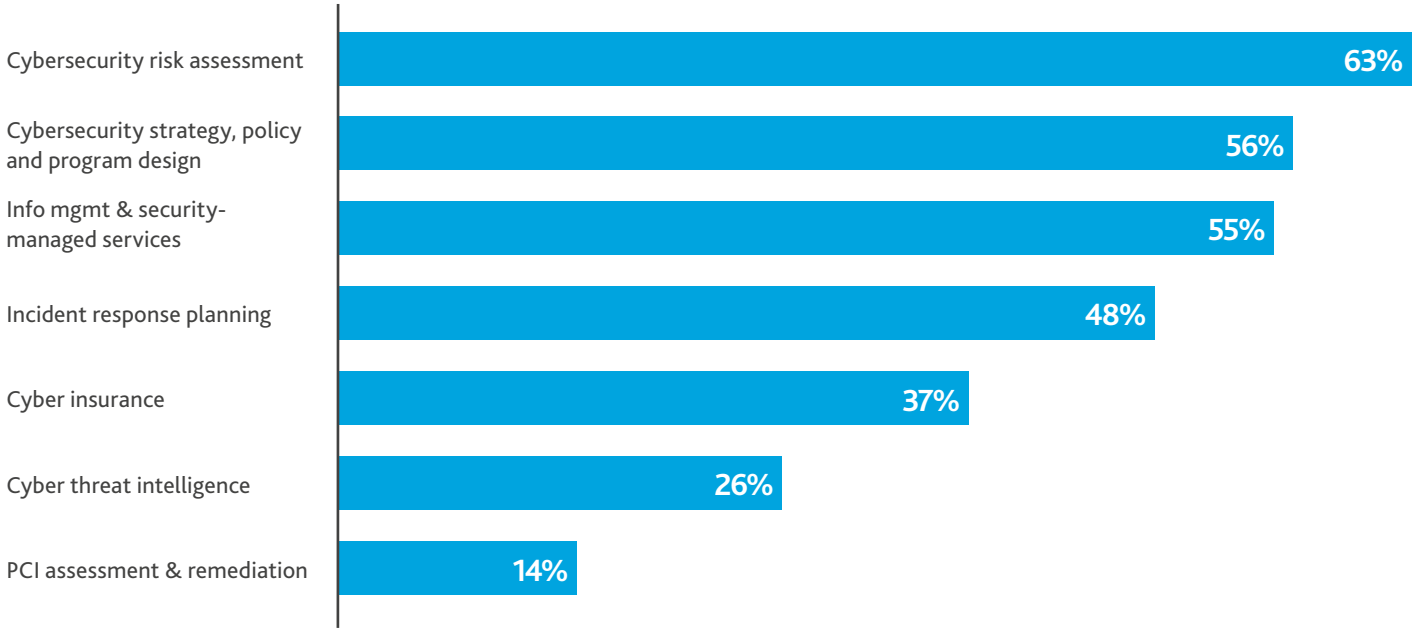
Also pointing toward a heightened focus on data privacy and security, 34 percent of the counsel surveyed say their organizations will increase cyber investment by 10 percent or more in the next 12 months. Interestingly, the smaller the company, the greater the increase in its cybersecurity investment.

	Annual revenue			
Increase in cybersecurity investment	Over $5b	Between $1b and $5b	Between $500m and $1b	Between $100m and $500m
Less than 10%	11%	7%	18%	23%
Up to 20%	32%	26%	47%	53%
Up to 30%	46%	31%	53%	60%
Up to 50%	46%	33%	59%	63%

Read more ▶

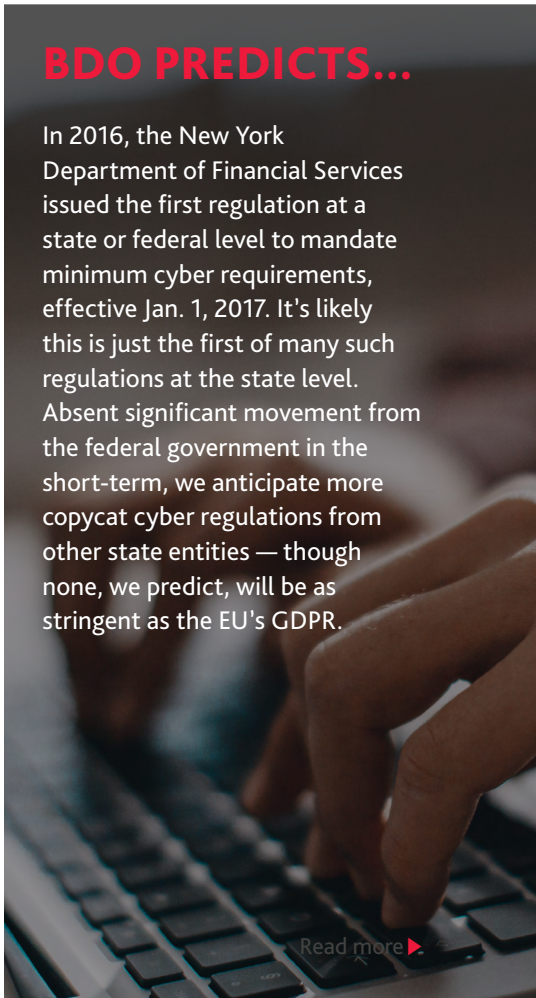
Here's a look at how those dollars will be spent:

WHICH OF THE FOLLOWING CYBERSECURITY SERVICES IS YOUR ORGANIZATION LIKELY TO INVEST IN DURING THE NEXT 12 MONTHS?



Companies whose boards have become more involved in cybersecurity have increased their investments in cybersecurity in the past 12 months much more than companies whose boards have not become more involved. Companies whose boards have not become more involved in cybersecurity in the past 12 months also have done little to increase their investments in cybersecurity in the past year.

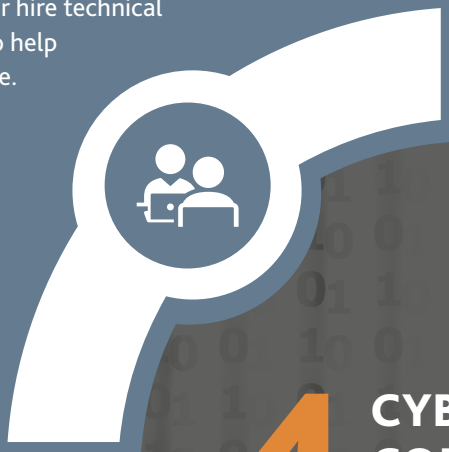
Which of the following cybersecurity services is your organization likely to invest in during the next 12 months?	Is your board MORE involved with cybersecurity than it was 12 months ago? YES	NO
Cybersecurity risk assessment	67%	45%
Information management & security-managed services (i.e. security operations center, cybersecurity education & awareness)	58%	45%
Cybersecurity strategy, policy & program design	57%	50%
Incident response planning	53%	35%
Cyber insurance	40%	35%
Cyber threat intelligence (i.e. dark web recon and analysis)	32%	10%
Payment Card Industry (PCI) assessment & remediation	15%	10%



4 CYBER TIPS FOR CORPORATE COUNSEL

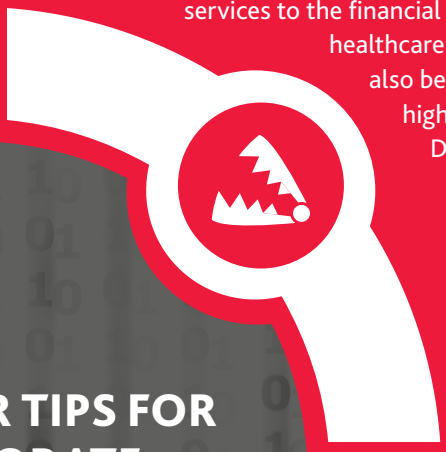
1. GET TECH-Y WITH IT.

What was once the sole domain of the IT department is now a firm-wide issue and a top business priority for the legal team. The challenge is cyber literacy: How do you communicate the effectiveness of your cybersecurity risk management efforts when you don't speak IT? Either learn the lingo—or hire technical personnel to help you translate.



2. AVOID HIDDEN REGULATORY TRAPS

So far, cyber regulation has targeted the financial services and healthcare industries, which already are highly regulated. But because these regulations introduce requirements for third parties, any organization in any industry that provides services to the financial services and healthcare industries is also being held to a higher standard. Don't assume you're off the hook.

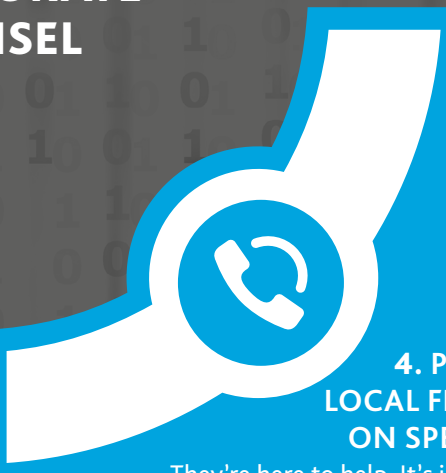


3. MAKE CONNECTIONS.

Existing fraud prevention and anti-money laundering efforts are increasingly intertwined with data security. What often starts out as a cybercrime investigation focused on the technical aspects of a breach and how to defend against it then turns into a financial crimes investigation. It's crucial to have effective and consistent communication between information security and compliance functions within an organization.

4. PUT YOUR LOCAL FBI OFFICE ON SPEED DIAL.

They're here to help. It's important to note that proactively contacting the FBI doesn't absolve private sector companies from all regulatory liability or preclude law enforcement from sharing relevant information with regulators. However, companies that proactively contact and cooperate with law enforcement often receive favorable treatment.



Read more ▶

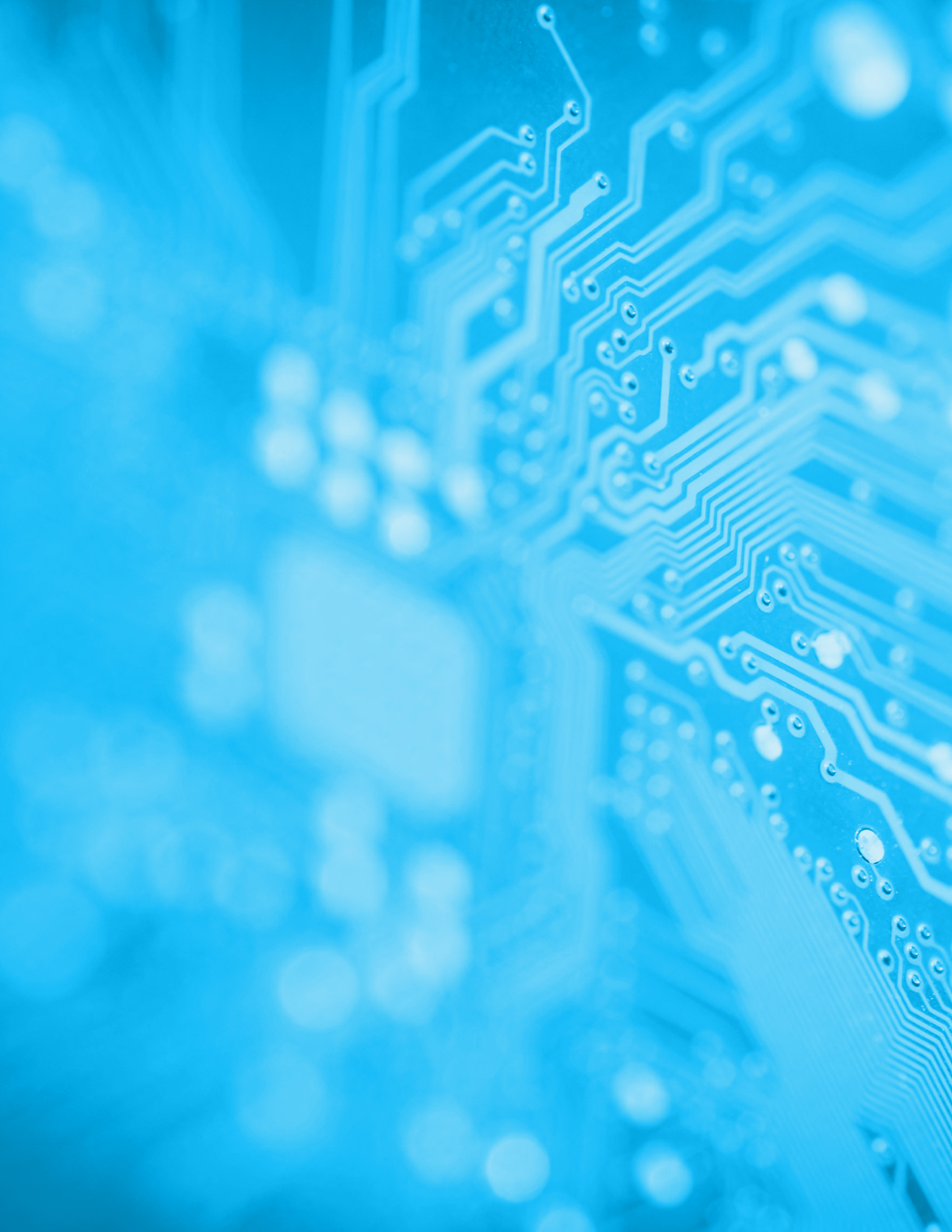
We've said it before and we'll say it again: Resisting technology—even in this most conservative of professions—is futile. But we don't deny that, for all the much-needed lift it provides, technology introduces a whole new world of complications. Technology makes corporate counsel's job doable, but not necessarily easier.

And as their purview expands beyond the legal and compliance realms, corporate counsel must increasingly consider the strategic value of data in addition to its risks. The savviest legal professionals are starting to think about how they can reinvent themselves as practitioners and as business advisors.

SURVEY METHODOLOGY

The Inside E-Discovery & Beyond survey by BDO is a national survey conducted by ALM, a global leader in specialized business news and information serving the legal, real estate, consulting, insurance, and investment advisory industries, and an independent and impartial research firm. ALM surveyed more than 100 senior in-house counsel at leading corporations throughout the United States to collect their insights for BDO's fourth annual study. Respondents come from corporations with revenues ranging from $100 million to over $5 billion from a variety of industries throughout the United States.

Read more ▶



CONTACT US

STEPHANIE GIAMMARCO
Partner and Technology & Business Transformation Services Practice Leader
212-885-7439 / sgiammarco@bdo.com

MARK ANTALIK
Technology & Business Transformation Services Managing Director
617-378-3653 / mantalik@bdo.com

GEORGE SOCHA
EDRM Co-Founder and Managing Director, Forensic Technology Services
952-656-2632 / gsocha@bdo.com

KAREN SCHULER
National Data & Information Governance Practice Leader
703-336-1533 / kschuler@bdo.com

DOUGLAS HERMAN
Principal and E-Discovery National Leader
312-730-1260 / douglas.herman@bdo.com

GREGORY A. GARRETT
Head of U.S. & International Cybersecurity
703-770-1019 / ggarrett@bdo.com

JENNA AIRA-VENTRELLA
Managing Director and Global E-Discovery Practice Leader
310-557-8256 / jaira@bdo.com