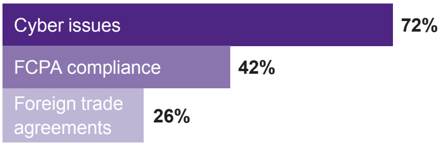
Rising to the risk: Cybersecurity top concern of corporate counsel

Grant Thornton LLP 2017 Corporate General Counsel Survey

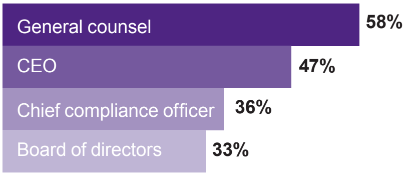
The stakes to proactively manage cyber threats are getting higher as businesses are estimated to lose $3 trillion to cybercrime by 2020, up from $1 trillion in 2016. These days, when organizations are discussing risk, they are most likely addressing cybersecurity and data privacy. In fact, cyber threats top the risk agenda with 72% of legal departments defining it as the top priority risk issue with specific concerns for data security (17%) and data privacy (16%), according to Grant Thornton's 2017 Corporate General Counsel Survey.

Global issues that will expand legal scope



Grant Thornton and Corporate Counsel magazine surveyed corporate general counsel to assess their views on the keys to business growth. More than half (58%) of legal departments are highly involved in responding to organization-wide data security risks, with nearly a quarter (23%) having primary responsibility for the issue, according to the survey findings. General Counsel's involvement in this issue has increased over the last two years when, according to Grant Thornton's 2015 Corporate General Counsel survey, 11% of respondents reported having primary responsibility for responding to data breaches.

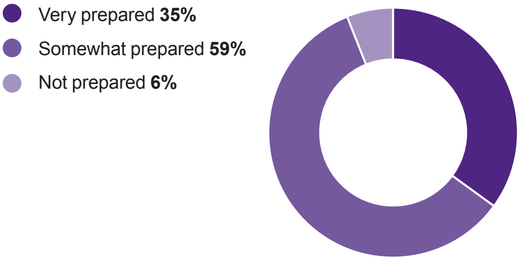
Primary responsibility for responding to data breaches



Concerns associated with customer and client data breaches coupled with anxiety over the unknown inform the four primary data security challenges identified by general counsel. Customer/client data privacy tops the list of cybersecurity risk concerns (51%), followed by potential for undetected breaches (42%), employee and workplace data privacy (38%) and unknown and unidentified risks (36%). When asked to assess the level of risk various issues presented to the organization, data security rated first and data privacy third as most important.

Yet, while 59% are very concerned about data security issues, only a little more than a third (35%) feel their organizations are prepared for a data breach, an increase from 2015 levels when 20% of organizations reported feeling somewhat or very unprepared. In today's high-risk cybersecurity environment, preparedness is paramount to an organization's ability to respond to and recover from data incidents.

Current level of preparedness for responding to data breaches



To achieve a higher state of cybersecurity preparedness, businesses must accept that data is both an outcome of innovation which drives growth and a liability. As noted in Grant Thornton's *"Cybersecurity 2.0: Think like a cybercriminal to combat threats,"* leaders must be willing to understand the potential motivations and threats cybercriminals pose and develop proactive strategies to protect their organization's interests.

"A holistic approach allows companies to place cyberrisks in their proper strategic and business context aligned with their industry-specific legal and regulatory requirements and show how management's acceptance of specific cyberrisks will assist—or fail to assist—in creating business value for their customers and shareholders," explained Vishal Chawla, national managing principal, Risk Advisory Services for Grant Thornton. "Businesses must enact a strategic approach, one that includes all senior managers in defining and meshing their roles in defining organizations' cybersecurity operational risks, cyberrisk appetite, management plan and associated governance structure."

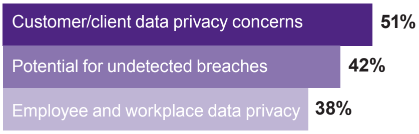
Erik Lioy, national managing partner of Grant Thornton's Forensic Advisory Services, suggested that "Many organizations have a fatalistic attitude when it comes to cyber breaches. If you believe a cyber breach is inevitable, you are not likely to invest heavily in preventative measures."

However, organizations can no longer adopt a fatalistic mentality to cyberrisk preparation. The business and customer costs are too great. Instead, Grant Thornton outlines its three-step holistic approach to cyberrisk management in its report, *"Taking AIM at cyberrisk."* The iterative approach, known as AIM, includes aligning risk management with the business strategy, integrating cyber controls with business processes, and measuring the outcomes, costs and returns of the cyberrisk management program.

While most organizations understand it may not be a question of "if" you will get hacked, but "when", they are not yet effectively addressing how to respond when their data is compromised. "The commoditization of attacks on organizations is profound and won't likely change for years," explained Johnny Lee, principal and forensic technology practice leader for Grant Thornton's Forensic Advisory Services. "The bad guys will always have the upper hand in the short term. The trick is to do all you can to keep data compromises contained and take additional steps to protect particularly sensitive data. The challenge is that most organizations are overwhelmed with so much data that they haven't effectively focused on being strategic when it comes to protecting those data."

Inefficient resources and a gap in specialized skillsets may also serve as contributing factors to an organization's lack of preparedness for cyber threats. More than a quarter (28%) of respondents cited overburdened IT/information security teams as a factor while 17% indicated a lack of crisis management and incident response skills played a role in an inability to manage cyber threats.

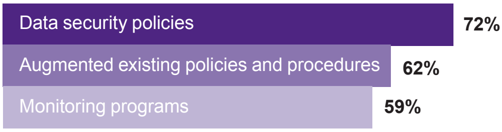
Top data security challenges



"Keeping up with the latest cyber threats is a real challenge," Lioy acknowledged. "Today's threat intelligence and best practices in cyber security are often obsolete in less than a year." While the skill shortage is real, organizations have a number of options available to fill the gap including partnering with specialists, advisors and consultants.

Recognizing the high stakes that cybersecurity risk poses, an increasing number of organizations are becoming more proactive in stepping up their efforts to address it.

Actions taken to mitigate cyber-related risk

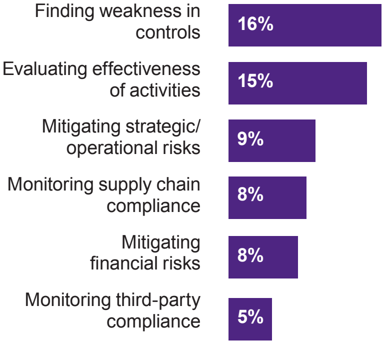


The vast majority of organizations are adding data security policies (72%) or augmenting existing ones (62%), while 59% are implementing monitoring programs and more than half are conducting end user training (55%) and developing incident response plans (53%). Additionally, 47% of responding organizations are employing outside advisors while 40% are adding cyber or data breach insurance.

Increasingly, organizations may find themselves stepping up security measures as they are pressured by state and government agency regulators. For example, regulations promulgated by the New York State Department of Financial Services requires that covered businesses "provide regular cybersecurity awareness training for all personnel."

Nearly seven in ten organizations have increased spending in hopes to mitigate cybersecurity and data privacy risk. Global spending on information-security products and services is expected to reach $86.4B in 2017, up 7% from 2016, according to data from research firm Gartner Inc. In 2018, that number is likely to climb to $93B.

Major impact of data analytics



One area in which organizations may be increasing spending to address cyber-related concerns is in the use of data analytics for compliance and risk assessment. Indeed, 67% of respondents revealed they are employing data analytics to better respond to regulatory and compliance requirements while 65% are using it for e-discovery. Of those using data analytics, 15% indicated they have experienced major improvements when using it to evaluate the effectiveness of governance, risk and compliance activities while 16% found data analytics had the greatest impact when identifying weakness in compliance controls.

"Data analytics allows risk managers to reduce the noise inherent in sifting through vast volumes of data," explained Ward Melhuish, principal and Grant Thornton's Advisory Data Analytics practice leader. "It allows organizations to pull together multiple data types across silos of data to better analyze risk, allowing for improvements in risk coverage, risk monitoring and predictive risk modeling."

He added, "Data analytics allows for better hindsight, insight, and foresight but to gain maximum value from them, organizations need to go beyond just the data and models and fine-tune their strategies, culture and processes."

As organizations better understand how to use data analytics to meet their objectives, including risk assessment monitoring and e-discovery, they will likely increase their investments. Lee added that "Data analytics can be a powerful tool only when applied to solving specific business problems." However, because cyberrisk evolves rapidly, technology solutions alone can't keep pace with cyber threats.

Outside of the US, general counsel are most concerned with regulatory and legislative mandates and data security. However, they are not yet as proactive in establishing data security policies as their North American counterparts, in part because their investments related to monitoring have not kept pace with rising risk.

"Organizations are increasingly acknowledging that regulation is a primary consideration in their business strategies that can and should be perceived as a competitive advantage rather than a burden," said Mark Hoekstra, global leader, Forensic and Investigation Services for Grant Thornton Netherlands. "It's critical to embrace a cross-functional, holistic approach to risk management that will allow organizations to turn emerging risks into opportunities for growth."

Increasingly, organizations are pursuing a quintessential approach to data analytics that transitions from descriptive analytics to predictive and prescriptive analytics. Grant Thornton helps businesses leverage the power of predictive analytics using a combined approach that includes digital forensics, e-discovery and data analytics that addresses both structured and unstructured data analysis. This kind of multi-pronged approach can help businesses not only prepare for and respond to cybersecurity issues and data breaches, but also ramp up risk decision making in a proactive manner.

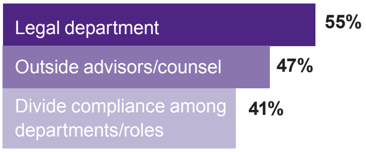
Overall, general counsel respondents reveal a more optimistic view of the regulatory environment with the shift in the political landscape compared to just two years ago when 69% of organizations indicated the regulatory environment made it more difficult to do business and 29% and 21% respectively acknowledged it decreased profits and impeded growth. However, in 2017, more than a third (37%) of organizations do not envision changing the way they manage regulatory compliance.

Since taking office, President Trump has sought to roll back regulations, declaring it the key to achieving his campaign promise of generating at least 3 percent annual economic growth. He signed a "two-for-one" executive order requiring federal agencies to identify two regulations to eliminate for each new rule they want to impose. Additionally, with the help of a Republican-led Congress, the president has killed or delayed more than 860 federal rules and regulations. The business community is in support of Trump's deregulation campaign, a perspective that may be reflected in the 8% jump in growth by the Dow and S&P 500 in 2017 to date.

Proponents of regulatory reform have suggested rollbacks will result in organizations increasing profits, reallocating resources to core competencies and improving their competitive position. However, the road to deregulation must first pass through a challenging risk landscape that includes increasing cyber threats, conduct risk and reputation risk.

The responsibility for managing an increasingly complicated risk landscape sits squarely with the legal department. According to the Grant Thornton survey, more than half (55%) of organizations indicate managing regulatory risk remains the responsibility of the legal department, often with help from outside advisors. However, for more than 40% of respondents, regulatory risk responsibility is divided among various departments.

Regulatory risk management responsibility

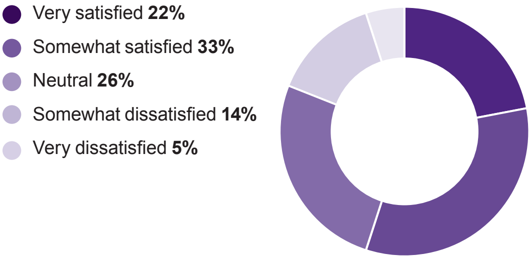


There is no one-size-fits-all solution when it comes to assigning responsibility for managing regulatory risk. “While best practice may dictate having a full-time Chief Risk Officer, it is not always economically feasible to do so,” suggested Lioy. “Ultimately, every organization must tailor a unique solution based on its assessment of risk, budget and risk appetite.”

The risk landscape has become so complex that it requires a veritable village of specialists to manage it effectively. “The pace of change is relentless,” explained Lee. “General Counsel can’t possibly handle all types of risks. That’s why it’s necessary for organizations to develop a true unifying approach to address all risks that includes choosing the best trusted advisors and specialists.”

Faced with constant change and expanding risks, many organizations are unsure that their efforts to control risk and comply with regulations are working or driving positive return on investment. Nearly half (45%) of organizations indicated they were ambivalent or uncomfortable with their risk management effectiveness while a fifth of organizations are very or somewhat dissatisfied. This perception is also reflected in the frequency and formality of risk assessments being performed. While 68% of large ($1B+) organizations conduct quarterly or monthly evaluations, many smaller organizations have yet to formalize their risk assessment process. In fact, more than a quarter (29%) of midsize ($100-$999M) organizations and more than a third (36%) of small (under $100M) organizations rarely or never conduct formal risk assessments.

Effectiveness of risk assessment processes



Lee suggests that too often risk assessments are defunded because they are considered distractions from the core priority of revenue generation. Yet, strategically-minded leaders understand that to better manage risk, organizations need to refocus the purpose of the entire risk assessment exercise. “Frequency isn’t the right measure of efficacy; usefulness is,” he explained. “When executed well, a risk assessment should provide a roadmap and call to action to help your organization focus on business problems and grow strategically for the long term. Moving from a plan to action is hard. It requires putting in place the right mix of bandwidth, expertise and partners to move forward.”

Ambivalence can also lead to complacency when it comes to conducting thorough risk evaluations. “The world is changing so fast,” Lioy noted. “There might have been a time 20 years ago when your regulatory risks were relatively static year to year. But in today's constantly evolving business landscape, you need to conduct assessments at least once a year."

Lioy also suggested that successful organizations understand that risk management is not just a compliance exercise but an opportunity to gain a competitive advantage. "The initial knee-jerk reaction for many organizations is that all risk is bad," he explained. "The reality is all organizations face risk so they need to mitigate it and define their risk tolerance threshold. Businesses make profits because they're willing to take risks. The more proactive you are in discussing risk on a frequent basis, the more likely you are to turn risk into a competitive advantage."

As legal departments continue to play a critical role managing risk and monitoring its effectiveness, especially in the area of cybersecurity, organizations will increasingly move from thinking about risk only in terms of management and compliance to that of risk agility. The agile enterprise will be better equipped at all levels of the organization to turn risk into a true competitive advantage.

That means organizations need to embrace risk management in general, and privacy and data security specifically, as core values. Cybersecurity must be developed and implemented in the context of a well-funded, well-coordinated, enterprise-wide cyberrisk management program. The conversation that will sustain that program has to begin at the top of the agenda and be supported through continuing senior executive engagement.

About Grant Thornton Advisory Services

Grant Thornton's Advisory professionals are progressive thinkers who create, protect, and transform value today, so our clients have the opportunity to thrive tomorrow. While business goals and strategies evolve, our services can support you wherever you are – whether you're looking at a transaction to propel you forward, focusing on developing and implementing the right controls to mitigate risk, or transforming your company's finance and technology infrastructure to match your aspirations.

Learn more about how we help our clients at www.grantthornton.com

About Grant Thornton LLP

Founded in Chicago in 1924, Grant Thornton LLP (Grant Thornton) is the U.S. member firm of Grant Thornton International Ltd., one of the world's leading organizations of independent audit, tax and advisory firms. Grant Thornton (GTIL), which has revenues in excess of $1.7 billion and operates 60 offices, works with a broad range of dynamic public and privately held companies, government agencies, financial institutions, and civic and religious organizations.

GTIL and the member firms are not a worldwide partnership. Services are delivered by the member firms. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions. Please see grantthornton.com for further details.

Demographics

The Grant Thornton LLP Corporate General Counsel Survey was conducted online May 4 through August 23, 2017, by ALM Marketing Services. There were 198 respondents, 35% of whom were general counsel and chief legal officers. Respondents' organizations represented a broad range of sizes, with the mean annual revenue of the respondent's firm being $2.3 billion. Organizations also were distributed widely across industry sectors. This survey also received responses from not only North America (79%) but internationally as well (21%).

For more information, contact one of Grant Thornton's Advisory Services leaders:

Brad Preber
National Managing Partner, Business Risk Services
T +1 602 474 3440 **E** brad.preber@us.gt.com

Erik C. Lioy
National Managing Partner, Forensic Advisory Services
T +1 704 632 6915 **E** erik.lioy@us.gt.com

Vishal Chawla
National Managing Principal, Risk Advisory Services
T +1 703 847 7580 **E** vishal.chawla@us.gt.com

Johnny Lee
Principal & National Practice Leader,
Forensic Technology Services
T +1 404 704 0144 **E** j.lee@us.gt.com

Ward Melhuish
Principal & National Practice Leader,
Advisory Data Analytics
T +1 703 837 4537 **E** ward.melhuish@us.gt.com

Grant Thornton

GT.COM

Content in this publication is not intended to answer specific questions or suggest suitability of action in a particular case. For additional information on the issues discussed, consult a Grant Thornton LLP client service partner or another qualified professional.

"Grant Thornton" refers to Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd (GTIL). GTIL and its member firms are not a worldwide partnership. All member firms are individual legal entities separate from GTIL. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions. Please visit grantthornton.com for details.