goulston&storrs

IDENTIFYING NEW EXPOSURES IN A RAPIDLY INNOVATING WORLD

The business world is rapidly changing. We're more connected than ever before, and the Internet of Things is creating unprecedented volumes of data. Artificial intelligence and sophisticated analytics are extracting fresh insights from Big Data. And more and more organizations are adopting an omnichannel approach to customer interaction.

In order to survive, a company must innovate – or risk becoming obsolete. In fact, 93 percent of executives say that organic growth through innovation will drive the greatest proportion of their revenue growth, according to a PwC survey.[i]

Today's innovations, however, involve new integrated technologies – and data security and regulatory compliance may slip through the cracks. As such, many corporations – and their general counsel – face potential exposures, some for the first time.

Costly data breaches, ransomware attacks and insider sabotage are common. Companies can no longer afford to bury their proverbial heads in the sand. Cybersecurity, environmental and corporate governance regulations are in a state of flux, making it hard to keep up. Noncompliance can be costly, but pleading ignorance is no defense.

In the Goulston & Storrs 2017 General Counsel Survey, 61 percent of respondents said that keeping up with regulatory change was their biggest concern. And the cost of not keeping pace can create some serious liabilities, particularly with customer data.[ii]

Noncompliant companies and their GC are open to litigation, but the line between company and GC exposure is sometimes unclear. Fifteen percent of general counsel say they have the most difficulty identifying exposures, and this emerging risk is reshaping the role of GC – GC who may not fully know how protected or indemnified they are.

In this white paper, we'll explain the professional and personal exposures GC face. Then, we'll discuss how to identify and mitigate those risks.

PROFESSIONAL EXPOSURE

Cyber risk

The business world operates increasingly online. Proportionally, the risk of data loss and theft is growing. The monetary cost alone of identifying cyberattacks and data exfiltration, plugging the gaps in defenses and addressing legal liability and reputational damage can be enormous: an average of $3.62 million in 2017, according to the Ponemon Institute.[iii]

Cyber security has come under the radar of the SEC, which is likely to take enforcement action relative to cyber disclosure,

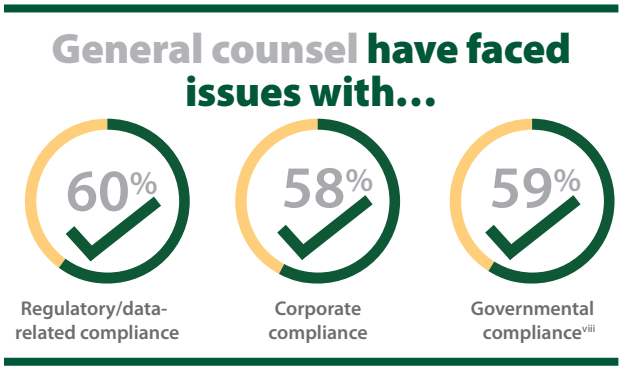
according to the Wells Fargo State of the Market 2017 report.[iv] It's little wonder, then, that cyber risk featured among the top three corporate risks for the first time in 2016.

It's not that companies aren't concerned about the implications of a sophisticated cyberattack on corporate resources. Rather, they tend to underestimate the effects of IT failures, human error and employee malfeasance, according to Allianz D&O Insurance Insights 2016.[v] In just one example, a cyber breach that triggers a share price drop could result in action for breach of fiduciary duty.

Cyber risk law is still developing. While high-profile suits against Target[vi] and Talk Talk[vii] are instructive, many cases are still pending, and the potential impact is hard to quantify. It's important to watch the horizon for other developments in order to build effective protection against litigation.

Regulations and compliance

As global companies face an increasingly difficult regulatory environment, it becomes even more critical for GC to play a role in responding appropriately to alleged misconduct.



Allianz shows that 34 percent of D&O losses were the result of noncompliance – and these losses amounted to 61 percent of total claims by value.[ix] In the G&S survey, 64 percent of respondents cited regulatory risk as their main concern, followed by data (48 percent) and IT (34 percent).[x]

Two major Department of Justice (DOJ) policy initiatives may be provoking change.

1. Yates Memo

The DOJ Policy on Individual Accountability for Corporate Wrongdoing (Yates Memo) issued September 2015 states that corporations will not be eligible for "cooperation credit" – massively reduced fines -- unless they provide "all relevant facts" relating to the individuals responsible for misconduct.

In one example, The Department entered into a Non-Prosecution Agreement with IAP World Services in 2015 because it felt IAP cooperated well and conducted a thorough internal investigation.[xi] Alstom SA, on the other hand, recorded damages of $772 million due to failure to cooperate.[xii]

2. Fraud Division compliance counsel

The DOJ has also appointed a "compliance counsel" to its Fraud Division to help determine whether those corporations subject to DOJ investigation have maintained a compliance program in good faith.

Because of these policy initiatives, GCs play a more central part in determining criminal or civil liability. Counsel, then, must balance their obligation to communicate openly with company officers with their duty to gather evidence of individual misconduct for the government.

Internal misconduct isn't the only area GC should worry about: Third-party misconduct can drive an average share price drop of 2.6 percent for a company employing them, says Deloitte.[xiii]

PERSONAL EXPOSURE

GC are also open to personal exposures. The Yates Memo made individuals, not corporations, the focus of investigations from the outset. The DOJ will no longer release individuals from liability when settling a matter with their employer, nor will it close an employer investigation without a plan to resolve related individual cases. Some examples of this liability transference include:

- The Uber legal team faced allegations of failing to properly investigate sexual harassment claims.[xv]
- The SEC took action against RPM International Inc. and its GC for overcharging on government contracts.[xvi]
- Volkswagen's in-house counsel gained criticism for destroying documents related to emissions during the diesel crisis.[xvii]

Alarmingly, in-house lawyers may not fully understand their liability coverage – assuming, for instance, that their company's D&O policy covers alleged malpractice, while it excludes legal malpractice claims from approval. They may not even know if they are covered, in fact.

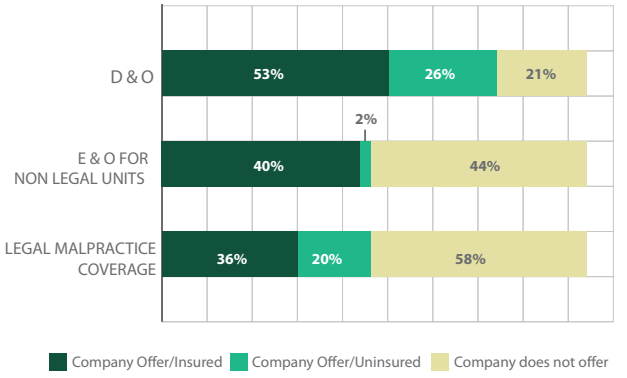
D&O may cover a GC, as an officer of the company, for business advice given, but not for in-firm legal advice. Providing legal advice outside the scope of employment and advice given to other entities may also be excluded. Other liabilities include pro bono work intended to enhance the company profile or personal legal work for company officers.

Legal Malpractice Coverage (LMC) may be added to D&O, but GC must consider its liability limits, which are generally lower than in a standalone policy. If there is an aggregate limit, a large D&O loss may leave nothing for legal malpractice. This is an even greater issue as many companies have begun carrying

an umbrella Executive Liability Policy -- D&O, cyber, fiduciary, employment, crime and other risks, all subject to one aggregate.

Coverage is a mixed bag for GC

- Seventy-nine percent of companies offer D&O; more than one-quarter of respondents are not covered by it (26 percent).
- Forty-nine percent of companies offer E&O for nonlegal units; nearly half the respondents lack coverage.
- Just over half (56 percent) of companies offer legal malpractice coverage; 80 percent of respondents don't have it.[xviii]



What's more, one in five respondents (21 percent) confirmed that they were not indemnified by their company – and 15 percent did not know whether they were.[xix]

Identifying and mitigating risks and liabilities

The risk is growing, but proactive preparation and prompt action goes a long way toward reducing the liability of a company, its officers and its in-house counsel.

For one, GC can spot potential problems early on by keeping in touch with the rest of the executive suite, along with risk directors and those responsible for policy and crisis management. GC can help promote a culture of transparency and accountability and commit to a prompt response to potential misconduct. Remember: A company can substantially reduce fines and reputational damage by reporting misconduct itself.

A well-developed response and communication plan can also inform independent internal investigations by outside counsel – but remember, the results (including the otherwise protected work product) must be disclosed. Are the company's internal privileged communications sufficiently protected from unintentional waiver? Does its

How to Add Protection to Your Next Deal: Representations and Warranties Insurance

What does R&W Insurance cover? Unknown breaches of representations and warranties within a purchase agreement, such as:

- Misstated financial statements
- IP owned by a third party
- Necessary permits not in place
- Litigation pending against the Seller

Key Advantages

Issues covered: Cover losses from breaches not "Actually Known" as of closing.
Term: Typically three years for general and six years for fundamental and tax reps.
Seller post-closing exposure: Limit seller exposure to 1 percent or less of total purchase price.

Market Trends

- Greatly improved pricing
- Streamlined underwriting process
- Used by many U.S. private equity firms

Types of R&W Policies

- Policy can be structured to provide enhanced coverage (e.g., limits, survival periods, etc.)
- Buyers recourse for covered losses is directly against insurer(s) and not Seller
- Coverage for Seller fraud is provided to the Insured or Buyer (insurer retains subrogation rights)
- Often used to backstop escrow and/or indemnification of insured, up to the full purchase price
- Insured/Seller is made whole for covered losses from insurer(s) after Buyer has made a claim under the indemnity structure pursuant to the purchase agreement
- Excludes Seller fraud through knowledge provisions

Contact us for an executive briefing at your next management meeting, or a complimentary analysis of the suitability of R&W Insurance for your next deal.

Gregory O. Kaden
617-574-3818 | gkaden@goulstonstorrs.com
Goulston & Storrs

internal investigations protocol meet the DOJ's stringent requirements?

There should also be a clear process for conducting interviews pursuant to an internal investigation, as well as ensuring that interviewees are given adequate Upjohn warnings regarding information disclosed in interviews.

GC may act in a variety of roles, offering business advice alongside legal advice. To protect their privilege, communications on legal matters should directly state their purpose. Efforts should also be made to separate a GC's non-legal from his or her legal functions.

Once a potential professional liability has been uncovered:

- Respond quickly – GC will rarely be criticized for investigating too thoroughly, and their actions will be judged in hindsight. The success of the SEC whistleblower program[xx] means a company's risk may only grow. Independent investigations early on can also have significant reputational, business and legal benefits.
- If independent counsel is instructed to investigate, be clear from the outset who they do and do not represent. If a GC instructs an independent investigator who is not a lawyer (e.g., a forensic accountant), that work is not privileged.
- Assume any civil matters pursued by DOJ have a parallel criminal component – and prepare accordingly.

There are also several steps GC can take to mitigate personal liability:

- Document all advice given.
- Triple check the legal basis of their own advice and be aware of the license requirements of the states where they operate. Do not accept external legal advice without question.
- Remember the GC represents the company and shareholders, not its officers – and shouldn't be afraid to question management orders. When dealing with external parties or company employees, it should be clear the GC serves the company.
- Ensure investigations are above board, avoiding questionable tactics like pretexting, and ensure that others are avoiding them, as well – GC could be held responsible for not providing oversight.
- Be aware of "up the ladder reporting" requirements, as detailed in the Sarbanes-Oxley Act of 2002[xxi] – but if director misconduct is suspected, GC may delay with an "information preservation" hold on any investigation notifications.
- Be mindful of the GC's duty to handle witnesses and documentation for both civil and criminal cases; narrow the subpoena scope to avoid obstruction allegations.
- Determine the full extent of D&O and E&O coverage and ask whether GC are covered. Consider additional personal LMC.

CONCLUSION

The creative leap that business innovation has taken of late has also opened companies and their GC up to new legal exposures. The rising specter of cyber risk, the ongoing challenge of keeping up with regulatory changes and the difficulty in establishing the line between company and GC liability – all must be addressed.

There's opportunity for forward-thinking companies and GCs that can take the right actions to prevent these exposures from developing into full-blown disasters with irreparable damage. These complex issues require review, analysis, and positive action – but armed with the right plan and partners, GC can help ensure that the road to innovation is clear.

[i] "Global Innovation Survey: Innovation, growth and business strategy." PwC. 2014.
[ii] Goulston & Storrs 2017 General Counsel Survey. July 2017.
[iii] "2017 Ponemon Cost of Data Breach Study." IBM. June 2017.
[iv] "2017 Insurance Market Outlook." Wells Fargo Insurance. 2016.
[v] "D&O Insurance Insights." Allianz Global Corporate & Specialty. November 2016.
[vi] Masunaga, Samantha. "Target will pay $18.5 million in settlement with states over 2013 data breach." LA Times. May 23, 2017.
[vii] Rodionova, Zlata. "TalkTalk given record fine for data breach that led to data theft of nearly 157,000 customers." Independent. Oct. 15, 2016.
[viii] Goulston & Storrs Survey.
[ix] "D&O Insight Insights."
[x] Goulston & Storrs Survey.
[xi] "IAP Worldwide Services Inc. Resolves Foreign Corrupt Practices Act Investigation." Department of Justice. June 16, 2015.
[xii] "Alstom Pleads Guilty and Agrees to Pay $772 Million Criminal Penalty to Resolve Foreign Bribery Charges." Department of Justice. Dec. 22, 2014.
[xiii] Binham, Caroline. "Companies face lasting damage after third-party misconduct." Aug. 2, 2015.
[xiv] Cox, Christopher. "Speech by SEC Chairman: Address to the 2007 Corporate Counsel Institute." U.S. Securities and Exchange Commission. March 8, 2007.
[xv] Lien, Tracey. "Uber fires 20 workers after harassment investigation." LA Times. June 6, 2017.
[xvi] "SEC Charges RPM International Inc. and its General Counsel for Disclosure and Accounting Failures." U.S. Securities and Exchange Commission. Sept. 9, 2016.
[xvii] Ramey, Jay. "DOJ Claims VW destroyed records as diesel crisis unfolded." Autoweek. Jan. 12, 2017.
[xviii] Goulston & Storrs Survey.
[xix] Ibid.
[xx] Barber, C. Ryan. "The SEC Whistleblower Program's Biggest Year – By the Numbers." The National Law Journal. Dec. 21, 2016.
[xxi] "Final Rule: Implementation of Standards of Professional Conduct for Attorneys." U.S. Securities and Exchange Commission. Sept. 26, 2003.