ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

# 5 Points to Consider When Upgrading Your Cybersecurity Plan

**Technology, Privacy, and eCommerce**

Wright Studio / *Shutterstock.com*

According to the ACC's Chief Legal Officer Survey released earlier this year, in-house counsel identified cybersecurity, compliance, and data privacy as the areas that could pose the greatest legal challenges to their businesses in the coming years, with more than half of respondents citing industry regulations and data protection rules as their biggest concerns. Staying ahead of the constant changes in these rules, and ensuring that policies are designed to achieve compliance while supporting the new ways of doing business, are imperative.

Particularly for small legal departments, leveraging outside counsel's guidance on legal and regulatory compliance can inform the strategy you develop for your department and company. Here are five points to keep in mind as you consider your cybersecurity needs, and some insights on how your external law firm can help.

## 1. Balance business objectives and security needs.

Optimal decisions for maximizing profitability sometimes collide with the best cybersecurity choices. "There's always that push-pull," says Cara Group, senior legal counsel at Aspirant, a full-service consultancy. "Can you join a Starbucks coffee shop WiFi? Can you use your home cell phone rather than a dedicated work phone and, if so, who owns the data? These are the dialogues we're having. There's always tension between the loss of billable time versus the potential risk to the enterprise

from a bad actor.”

Outside law firms have grappled with these same questions and have clients who have as well. They have seen these issues play out across other companies, especially if they have a data privacy practice, and can offer insight.

One important step general counsel should take, advises Elizabeth Johnson, a member of the Privacy & Data Security Practice Group at Meritas member firm Wyrick Robbins in Raleigh, North Carolina, is to keep their top management in the loop about how they’re tackling cybersecurity. “It’s useful to make sure the highest levels of the organization are aware of and have feedback into the program,” she says. They need to have an understanding of the company’s risk profile, the potential fiduciary ramifications, and other aspects of the cybersecurity landscape at the organization. “That awareness will help leadership set an appropriate risk tolerance that can be communicated to and implemented by others to help bring the necessary balance to security and business needs.”

Effective communication between higher-level management allows the organization to stay aware and cautious of cybersecurity risks.

## 2. Prioritize risk mitigation and legal compliance.

Companies want to mitigate the risk of cybersecurity breaches with the latest technology and best practices. As a one-person law department, Group sits on Aspirant’s privacy-security committee. “We spend the bulk of our time talking about cybersecurity,” she says. “This is top-of-mind for our insurance carriers. It’s kind of the key risk-mitigation strategy.”

At the same time, corporations must comply with a growing and strengthening body of laws and regulations around the world. “Cybersecurity will always be good business practice, first and foremost, but regulation will likely follow,” says Group. “It’s already becoming another compliance thing that all companies have to address.”

In general, the steps required for regulatory compliance are not as stringent as what a strong risk-mitigation strategy would dictate. “If you only focus on the legal compliance, you might not be implementing things that could be very helpful from a risk perspective,” says Johnson. “The laws don’t require a vulnerability assessment, for example, but if you don’t check your vulnerabilities, you won’t be protected from breaches.”


It is imperative to have an equal focal point between risk-mitigation and legal compliance in order to prevent data breaches from happening within the company.

Conversely, focusing too much on cyber risk mitigation, like protecting against hackers, could mean you miss something on the compliance side, like adequate training. “You could have pretty spectacular encryption protection, but then have an employee email a fraudster all of your payroll information,” Johnson says. “You’ll have a data breach because you didn’t train your staff adequately.”

An experienced lawyer from an outside firm who has been dealing with the balance between legal compliance and risk management across clients and industries can offer good insights. “If you’re focused on defensibility at some level, an experienced lawyer can help you figure out what’s ‘good enough,’ and what will give you the most bang for the buck from a regulatory perspective,” says Johnson.

## 3. Realize cyber concerns go beyond your firm.

Your cybersecurity protections need to extend to any company that may have access to or store company, employee, or client/customer data—from technology vendors to law firms, consultants, and other service providers. “Get them into your analysis,” Johnson stresses.

“It’s something we always talk through with any vendor,” says Group. “Everyone is struggling through this, so we ask them lots of questions, and we include a [data security] clause in our NDA. At a bare minimum, they have to agree to hold a reasonable level of data protection. At this point, that’s

a baseline.”

A non-disclosure agreement (NDA) is one way companies can ensure that data is protected and confidential.

The tension between compliance and risk management applies here as well. “There are laws that tell you to have certain provisions in your contract [related to cybersecurity and data use],” says Johnson. “If you’re focusing on risk management alone, like requiring vendors to fix security vulnerabilities once detected, you might miss that required content. If there’s a cyber incident, you need to have that language in the contract to show the regulator you met basic contracting requirements.”

## 4. Remember security concerns impact everything you do.

Aside from cybersecurity, another technology priority for both legal departments and independent law firms is finding solutions for organizing contracts, managing matters, storing and managing documents, automating tasks, and fostering internal and external collaboration. This has been top-of-mind for some time, but the fact that many law departments and law firms remain hybrid or mostly remote — and likely will into the foreseeable future — adds to the urgency.

“How to find a better system to manage documents is a daily question on the ACC’s Small Law Department Forum,” says Group. “In a remote environment, having things on paper doesn’t do any good.”

While law firms are not experts from a technology point of view, they know what their clients are

doing and can offer some input. In some cases, they can also foster connections among different clients to allow them to share information with each other or do business together to the benefit of both.

## 5. Stay apprised of the ever-changing landscape.

New laws governing data privacy and cybersecurity are being implemented and updated all the time, all around the globe. Governments and industry groups are continually tweaking their regulations related to cybersecurity. New bad actors come on the scene continuously, with ever more sophisticated technology at their fingertips. World events, such as the war in Ukraine, bring greater threat of cyberwarfare.

All of this contributes to the urgency of having a strong cybersecurity program. “It seems like an amalgamation of several factors are feeding and building on each other,” says Johnson. “First, there are new and changing laws that require companies to report if they’ve had a cyber event. That creates news, which makes regulators and customers and shareholders more aware, and they start to ask tough questions about whether current security and legal requirements are adequate, and then the cycle repeats itself.”

Law departments must keep up with all of this. “What was the gold standard for cybersecurity three years ago is laughable now,” says Group. “It’s exceptionally difficult to stay on top of each new law and to understand what it says, what the practical implications are, and how to comply.”

This is one area where law firms can provide real value to legal departments. “We can spend at least an hour a day reading about changes in the law and about new security incidents just to maintain our status as specialists,” Johnson says. “We get a lot of calls from clients and prospective clients who say they’re overwhelmed and don’t know what to do or where to start. We can help them cut through the complexity.”

Meritas, a global network of law firms that has implemented a cybersecurity program as part of its long-held rigorous quality assurance process, offers several resources to clients and prospective clients on this topic. Its independent mid-sized firms are well-versed in the laws and regulations of their home jurisdictions. They share information with Meritas colleagues through the Meritas data privacy practice groups and online communities, which benefits their clients throughout the world. They offer insights to general counsel through the Meritas Courtesy Advice service, and publish articles and collaborative business guides that are available on the News & Insights section of Meritas’ public website.

“Providing critical information on the global cybersecurity and data privacy landscape is a place where outside law firms, and especially a network like Meritas, can really be of value to corporate counsel,” says Sona Pancholy, president of Meritas. “Turning to us can save law departments, especially small ones, a lot of time and effort and give them the confidence that their cybersecurity policies and technology decisions meet compliance, risk-management, and business objectives. Meritas has members across the globe that are staying abreast of legal and regulatory changes in their markets and we know that our members are regularly advising their clients on these issues.”

*Check out ACC?s Resource Library.*

Disclaimer: The information in any resource in this website should not be construed as legal advice or as a legal opinion on specific facts, and should not be considered representing the views of its authors, its sponsors, and/or ACC. These resources are not intended as a definitive statement on the subject addressed. Rather, they are intended to serve as a tool providing practical guidance and references for the busy in-house practitioner and other readers.

Kim Heinrich

Vice President, Global Marketing & Engagement

Meritas

Kim Heinrich is vice president, global marketing and engagement, at Meritas, where she has worked closely with member law firms around the world to develop strategies focused on leveraging the global network to enhance client service and business development for more than 25 years. She is a reputation builder and innovator in the legal services industry, identifying critical trends that impact law firm businesses, and is responsible for the Meritas brand.