ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

# 5 Questions Corporate Counsel Should Ask About Cyber Risk Assessments

**Technology, Privacy, and eCommerce**

Who is responsible for managing a company’s cyber risks? Many companies still leave this task to the IT department, figuring that it’s only a technical issue. Savvier companies know better: Tackling cyber risk requires a team approach, and in-house counsel must be part of that team.

Risk management is at the heart of the in-house counsel's work, and cyber risks are akin to many other dangers a business confronts. Helping businesses perform cyber risk assessments is one area where in-house counsel can — and should — play a pivotal role.

The benefits of performing these assessments are clear: Combining technical forensics, management consulting, and legal compliance, these assessments can provide companies with a better picture of an organization's overall cybersecurity risk. They can also help the company develop actionable recommendations for improving the company's risk posture, including its legal risks.

When done well, these assessments can significantly improve the company's overall cybersecurity status, and its ability to achieve its business objectives (e.g., entering into contracts with customers who demand cybersecurity representations in contracts). When done poorly, assessments can provide a comprehensive record of the company's failure to maintain reasonable cybersecurity and, even worse, its failure to act on identified weaknesses.

Here are five questions that you should ask (and be able to answer) to help prepare your company against a potential breach and protect its interests.

## 1. Why are we doing a cyber risk assessment?

Your first role will be to develop a risk assessment designed to meet the company's actual needs. To do that, you must have a clear understanding of what those needs are. In some industries — such as financial services, health, and government contracting — security assessments may be required by law.

For many companies, the assessment may be part of a remediation plan following a data breach or other security incident. In other cases, a company may decide to assess the maturity of its cybersecurity program in anticipation of increasing cyber threat, in connection with an assessment of a new acquisition, or in connection with demands by a key customer or business partner.

The scope of the assessment, including issues of privilege and implementation, will be driven by the company's reasons for undertaking the assessment. Counsel should be brought into the planning process as early as possible. No matter when you enter the planning process, you should take time to understand the security, compliance, and legal concerns underlying the assessment push.

## 2. What cybersecurity framework should we use?

Performing an assessment blindly may hinder efficiency. Instead of reinventing the wheel, many security assessors, such as third-party consultants and forensics firm, compare their findings against several well-known cyber frameworks, including:

- The Payment Card Industry Data Security Standard (PCI DSS);
- Center for Internet Security (CIS); Critical Security Controls;
- International Organization for Standardization (ISO) 27001;
- National Institute of Standards and Technology (NIST) frameworks; and
- The Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool.

For those new to the cyber world, these are but a sampling of different frameworks. But they all strive to achieve the same goal: to help companies develop order out of chaos.

For many companies, legal obligations will determine whether a particular framework should be used, and counsel will need to understand the underlying legal obligations and implications. In other companies, counsel will need to work with internal IT and (if applicable) third-party assessors to find the right match. Common drivers here may include the company's contractual obligations, the presence of recent expansion or acquisitions, or industry standards.

In some instances, choosing a framework may be the first step. It's important to calibrate your future assessment by weighing many factors. For example, a smaller company with minimal customer data faces different cyber risks than a large company collecting significant amounts of customer personal information.

A manufacturing company with a physical plant faces risks of physical intrusion that a purely online business won't. Developing an assessment that is either too lax or stringent, relative to your company's status and risk posture, will do little good. Informed legal counsel should work with assessors (both internal and external) to calibrate the risk assessment, even if it diverges from the frameworks listed above.

## 3. Is the company prepared to participate fully in an assessment and act on the results?

Every in-house counsel knows this truth: For a project to succeed, it must be supported by all relevant stakeholders in all parts of the company. The same applies to creating and implementing a strong assessment. Counsel should carefully evaluate how every business units will need to be involved in the assessment in order to properly capture technical, legal, and compliance cyber risks.

You should work with executives and internal communications teams to educate all stakeholders on the need for the assessment and the importance of participation. Hostile or apathetic business units or interviewees can stymie the flow of information in an assessment and lead to an incomplete or misleading report.

Stakeholder commitment is also paramount to ensure that risks identified in the assessment will be addressed. Your assessment may find major issues. While the company will need to prioritize remediation steps, a company without buy-in runs the risk of commissioning a report detailing its flaws without the ability to address them. You should have a good handle on the company's level of commitment to both the assessment and resulting remediation before signing off on the assessment.

## 4. Can we protect the assessment from disclosure?

Cyber assessments rarely paint a rosy picture of a company's risk posture. The report delivered at the end of an assessment will often contain a laundry list of high- and medium-risk areas, as well as gap analyses, timelines, and roadmaps for remediation. In the wrong hands, this information could be highly damaging to the company.

Plaintiffs, plaintiffs' lawyers, or regulators could use the report to support allegations of inadequate security. The same information could be used to establish that a company knew of risks — and did not take action.

Involving legal counsel in the assessment process may help shield that work from third parties. By becoming involved early, you can take steps to protect the assessment under attorney-client or work-product privileges.

Where applicable, corporate counsel should work with outside cybersecurity counsel, who can engage the third-party technical assessor on the client's behalf. The assessment should be structured to allow counsel, both in-house and outside, to provide legal advice to the company regarding its cybersecurity posture.

There are a number of steps companies can take to strengthen a claim of attorney-client and work-product privilege. But they boil down to counsel taking an active role in the assessment process. This may include participating in, and leading, meetings, performing interviews and reviewing/editing drafts of the final report and other work products to be delivered to the company's leadership.

Finally, you and outside counsel will provide much needed analysis of legal and compliance risks to assist leadership in creating a remediation plan as part of the assessment.

## 5. What should be disclosed?

Not all of the work product coming out of a security assessment can be closely guarded. In some instances — especially where an assessment is legally required, such as the risk analysis required under the Health Insurance Portability and Accountability Act (HIPAA) — companies may want to plan for the eventual release of the information in the event of a regulatory investigation.

In these circumstances, it is important to divide and segregate the results, such that releasing some information does not waive other parts of that assessment. To this end, you should consider, as part of the scoping and initial engagement, all required and types of deliverables that will be most useful to the company.

During final review, you should ensure that the work product properly reflects these separate deliverables, including restriction of legal advice to the privileged deliverables.

Finally, be ready to "let go." Most of the in-house counsel's work lies in performing the assessment. It is tempting to remain a part of every aspect of the project. However, performing remediation work belongs to others in the company.

You may be asked for advice from time to time, but most of your work at this point will be done. Talk with your company's executives and stakeholders to find the right time to step back and let others proceed.

## Conclusion

Performing cyber assessments may sound complicated, but the benefits can be tremendous. Finding risks means that your company can develop initiatives, policies, and procedures to mitigate them and provide customers with better products and services.

Armed with these questions and answers, you can help tailor your company's cyber assessment to protect it from disclosure and bad press, and chart a course towards addressing any risks successfully. Good luck, and get to work.

## Robert Kang

Professorial Lecturer

George Washington University Law School

Robert Kang is a Professorial Lecturer at the George Washington University Law School, and a consultant. He is also a former in-house legal executive focusing on technology, cybersecurity and national security. Robert serves as a member of the ACC Foundation’s Cybersecurity Advisory Board.

## Mike Morgan

Partner

McDermott Will & Emery in Los Angeles and Menlo Park

Morgan is co-chair of the firm’s Global Privacy & Cybersecurity practice.

## Jessi Sawyer

Associate

McDermott Will & Emery’s Global Privacy & Cybersecurity practice

Sawyer counsels clients on compliance with US and international cybersecurity and privacy regulations.

## Austin Mooney

Associate

McDermott Will & Emery’s Global Privacy & Cybersecurity practice