King & Spalding
Client Alert

FEBRUARY 11, 2019

For more information, contact:

Robert Hudock
Tel: +1 202 626 5521
rhudock@kslaw.com

Adam Solander
Tel: +1 202 626 5542
asolander@kslaw.com

Kelley Chittenden
Tel: +1 202 626 5440
kchittenden@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

Why Complete an Enterprise Risk Assessment

Your Organization's best defense in an environment of aggressive regulators and litigious plaintiffs' counsel is the completion of an enterprise risk assessment. Regulators and attorneys general are fining–sometimes hundreds of millions of dollars–and plaintiffs' counsel are seeking damages from organizations for data breaches caused in part by failing to complete a risk assessment. Regulations and security frameworks such as the HIPAA[1] Privacy and Security Rules, ISO 27001,[2] and the NIST Cybersecurity Framework require that an organization conduct a risk assessment to validate risk management decisions regarding threats to the organization and to define the level of security safeguards and any mitigations necessary and appropriate to protect an organization's assets.[3] Although conducting a risk assessment will not immunize an organization from inevitable data breaches, it *can* help an organization avoid becoming an easy target for interested parties seeking to take advantage of the organization's misfortune when a data breach occurs.

If an organization conducts a risk assessment, interested parties will be hard-pressed to challenge the organization's risk management decisions, even in the wake of a data breach. To illustrate, when an organization in question has conducted a risk assessment, assessing the reasonableness of the organization's security requires a fact-intensive inquiry specific to the organization's systems and market–expertise that most interested parties do not have. When an organization chooses not to conduct a risk assessment (even if the organization has made substantial investments in cybersecurity), the organization allows interested parties to label its security unreasonable.

In one sense, interested parties are exploiting organizations' confusion about how to conduct a risk assessment. As recent settlements show, even sophisticated organizations with adequate resources are missing the boat on conducting risk assessments, resulting in significant financial implications. This confusion, coupled with the public's moral outrage that organizations cannot prevent data breaches, is fertile ground for action by interested parties.

The confusion comes from vendors, security practitioners, and even lawyers that continue to produce a document *called* a risk assessment that is instead a gap analysis.[4] This confusion is justified in part because regulators and attorneys general have confused the risk assessment and gap analysis concepts in the past. For instance, the U.S. Department of Health & Human Services Office for Civil Rights (OCR) itself created a risk assessment tool that produced a HIPAA "risk assessment" that would be legally insufficient for most organizations in an OCR audit.

There are many ways for organizations to conduct a legally sufficient risk assessment. For instance, an organization may opt for a qualitative, quantitative, or hybrid method. However, any process adopted must begin with engaging organizational stakeholders to identify and understand threats to the organization, including examination of the incentives of potential adversaries to compromise the organization and how to limit risk of these threats to the organization's risk tolerance. Only after such engagement and analysis can an organization implement new tools, initiatives, and safeguards. There are no shortcuts here, but the exercise of analyzing risk should already be familiar to executive stakeholders that engage in a similar process every time the organization launches a new program, product, or service.

During a risk assessment, stakeholders must step beyond the technical minutiae of how a breach occurs to understand why the breach might occur, including the capabilities of the organization's most likely adversaries and any vulnerabilities the organization may have. Although threats are often malicious, they need not be intentionally malicious, targeting the organization, or even conscious beings. Potential threat actors include:

- Nation states (e.g., China, Israel, North Korea, Russia);
- Terrorist groups;
- Competitors;
- Organized crime (e.g., ransomware);
- Hacktivists;
- Business partners or vendors (e.g., poor security practices);
- Employees (e.g., intentional or negligent);
- Script kiddies seeking the target of least resistance; or
- Natural disaster, hurricanes, floods, and fires.

For most organizations, employees are likely to be the root cause of most data breaches.[5] But, if an organization is global, a defense contractor, or has costly-to-develop methods or technology, the organization may additionally attract more sophisticated adversaries (e.g., nation states that have the time and capability to compromise and conceal malicious activity for years).

Human threat actors will be motivated perhaps by politics, religion, curiosity, revenge, laziness, or for other personal gain. Personal gain is often financial, such as when hackers infiltrate company databases of credit card or insurance information, but it may also come in other forms like the desire for knowledge or peer recognition. Possible questions to consider when analyzing likely motives of potential adversaries may include, depending on the organization:

- What asset are they targeting?
- Will they be seeking a quick profit from identity theft using personal financial data on the organization's systems, or are they after trade secrets to setup a competing business?

- Has an executive or manager become irate that someone passed him or her over for a promotion, and he or she wants to hurt the organization by leaking customer information on the Dark Web?
- Is a low-level HR employee targeting older employees' 401(k)s for an easy pay day?
- Is an IT Administrator using company servers to mine crypto currencies?

The target (or asset) sought by an organization's adversary is key to understanding each threat scenario considered when conducting a risk assessment. For example, when an adversary seeks personal financial gain, they look for the easiest target. Such cybercriminals may be analogized to business people that typically will not invest time where the reward is not worth the effort. Alternatively, when an adversary seeks revenge for a perceived or real injustice, they may pursue a specific target even if their actions are damaging or against their own best interest.

All things considered, organizations should consider kicking off 2019 by conducting a risk assessment as additional protection not only from those data breaches that are preventable but also from exploitation by interested parties. Remember, the industry and market position of an organization affects the threats the organization will face. When conducting a risk assessment, organizations should focus on scenarios based on incidents and breaches affecting peer organizations and check out the CERT Insider Threat Center at Carnegie Mellon's Software Engineering Institute (SEI) website for insider threat scenarios. To assist organizations with conducting risk assessments, King & Spalding LLP has developed a threat catalog of over 500 scenarios, most of which are based on real security incidents.

[1] Health Insurance Portability and Accountability Act of 1996 (HIPAA).
[2] ISO/IEC 27001 is part of the ISO/IEC 27000 family of information security standards. The most recent version was published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee in 2013, with minor updates since.
[3] An asset is any data, device, or other component of an organization's environment, including applications, systems, data, people, physical locations, etc. that support the organization and its mission and can be illicitly accessed, used, disclosed, altered, destroyed, and/or stolen, resulting in a loss of some type.
[4] "A gap analysis is typically a narrowed examination of a covered entity or business associate's enterprise to assess whether certain controls or safeguards required by the Security Rule have been implemented. A gap analysis provides a high-level overview of how an entity's safeguards are implemented and shows what is incomplete or missing (i.e., spotting "gaps"), but it rarely provides a comprehensive, enterprise-wide view of the security processes of covered entities and business associates." See https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final for guidance on conducting a risk assessment.
[5] PONEMON INSTITUTE, 2018 COST OF INSIDER THREATS: GLOBAL (Apr. 2018), https://153j3ttjub71nfe89mc7r5gb-wpengine.netdna-ssl.com/wp-content/uploads/2018/04/ObserveIT-Insider-Threat-Global-Report-FINAL.pdf.