ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Cybersecurity Basics for In-house Counsel

Technology, Privacy, and eCommerce

Cheat Sheet

- Cybersecurity is a top issue for chief legal officers.
- In-house counsel need to understand cybersecurity concepts to serve their client.
- Information technology (IT) and cybersecurity functions have distinct purposes and drivers.
- Companies should segment their network for better cyber protection.

Cyberattacks have unfortunately become part of the environment for businesses and other organizations. **Cybersecurity is one of the top three issues** for chief legal officers, according to the 2022 ACC Chief Legal Officers Survey conducted by the Association of Corporate Counsel in partnership with Exterro.

View the key findings of the 2022 ACC Chief Legal Officers Survey.

In-house counsel need to understand basic technology aspects of cybersecurity to fulfill their duties

and provide effective counsel. This article addresses such concepts. It was prepared based on the webcast CyberTech in Plain English: Walking Through a Cyber Risk Assessment (May 10, 2022), which was presented by ACC member Robert Kang (Adjunct Professor at Loyola Law School, Los Angeles) in collaboration with several ACC Networks and the ACC Foundation. Professor Kang also kindly provided comments for this article. The basic insights shared in this article were intended to fill gaps found in a fictional cybersecurity assessment performed on a fictional company seeking to proactively mitigate problems.

Learn more about the ACC Foundation's work and its programs.

Monitor the increasing regulatory focus on cybersecurity

Upcoming regulations highlight the importance of cybersecurity. On March 9, 2022, the US Securities and Exchange Commission (SEC) issued proposed rules that would set new requirements regarding cybersecurity at publicly traded companies.

> ... The proposed rules would require companies to make certain disclosures regarding their board of directors' and executive leadership's expertise in cybersecurity.

Among other items, the proposed rules would require companies to make certain disclosures regarding their board of directors' and executive leadership's expertise in cybersecurity. While these rules may end up not being adopted, Kang believes the SEC's growing focus on cybersecurity will continue. He recommends monitoring this proceeding for potential impacts to your companies.

Understand the difference between IT vs. cybersecurity

Contrary to what lawyers sometimes think, IT and cybersecurity are not the same function. IT's focus is on keeping the business running in a quick, seamless, and efficient manner. By contrast, cybersecurity's focus in on security. As a result, the cybersecurity function may act as a brake slowing down the business to ensure it runs in a safe manner.

Ideally, cybersecurity and IT would be separate teams. However, this may not be an option for many small companies, where the cybersecurity function often reports to the IT head. In such configurations, the IT and business teams should be aware of the difference between the two functions, and management should support providing adequate training to the IT team.

> ... The IT and business teams should be aware of the difference between the two functions, and management should support providing adequate training to the IT team.

If your organization doesn't have the luxury of engaging two different teams, an option may be to train people on your IT team to serve as cybersecurity managers. Don't assume they have the skills to perform that function effectively.

"Getting Microsoft Windows up and running requires a different skillset than responding to anomalous behavior found in firewall logs," shares Kang. "If you're going to combine the cyber and IT functions into one person or group, make sure they are trained in both and given clear instructions on which to prioritize when in conflict." Kang adds: "Conflicts happen more often than you think."

Look into your vendors

While your business may have erected tall cyber walls, your vendors who access your systems may have much lower walls, which creates a supply chain risk.

For example, in a breach suffered by a large retail company, an HVAC vendor (heating, ventilation and air conditioning) has been viewed as a point of entry for a large breach. Kang believes that supply chain risk management represents the next frontier for legal professionals working in cybersecurity.

Where to start for a cyber risk assessment?

If you don't have a protocol in place, consider using existing models, such as Lockheed Martin's Cyber Kill Chain®, a framework for delineating the stages of a cyberattack, spotting vulnerabilities, and stopping the attack at the various stages of the chain. That's the framework used by the US Senate Committee on Commerce, Science, and Transportation in its 2014 analysis of a breach suffered by Target**.** Various audit standards have also been developed that could be used to form a cyber risk assessment.

Maintain privilege over cybersecurity assessments as needed

In theory, for privilege purposes, it shouldn't matter whether it is internal versus outside counsel that leads the assessment. However, engaging outside counsel to do so may be better from a perception standpoint.

A 2020 US court case concerned a forensic report developed by an external company engaged by Capital One following a cyber incident. The court ordered the company to disclose the report to the plaintiffs, even though the forensic company's work was performed at the direction of outside counsel.

If you involve a third party to conduct a cybersecurity assessment and want privilege to apply, consider these steps:

- Decide whether to have the assessment performed under privilege. Not all assessments qualify. For privilege to apply, there should be some element of identifying and mitigating legal risk.
- Have the assessment conducted under your instructions (issued in your capacity as legal counsel), with a privileged memo.
- Ensure that you as legal counsel are involved in strategic meetings with the forensic company.
- Ensure that the forensic company reaches out to you as the attorney when they need strategic guidance, as opposed to just liaising with your company's IT team.

Read "Five Questions Corporate Counsel Should Ask About Cyber Risk Assessments"

For more information about performing such assessments, look to the *ACC Docket* and other resources in the ACC Resource Library.

Beware of publicly available sensitive information

Malicious actors who do reconnaissance ("recon") about your company, you, or vendors: Assess public information about your company's systems. What information could malicious actors easily find online about your company's computing and vendor management systems?

Some companies post a link on their websites for vendors to connect to the organization's vendor management system. While this is efficient from a business standpoint, it may be risky from a cybersecurity standpoint.

Tips to consider regarding social media:

- Consider what information is available on your staff's LinkedIn public profiles and might describe which systems, firewall, and other computer and cyber tools your company has implemented.
- Consider implementing a social media policy that prohibits employees from posting sensitive information such as the systems and tools your company uses. If you engage in any type of monitoring of employee social media profiles, stick to the publicly available profile.

Tips to consider regarding access to your vendor management system:

- Consider using the zero trust model in which users can't access a system unless they have a legitimate reason to do so.
- Consider requiring registration and validation before granting access credentials.

- Consider making the link to your vendor-management system password-protected, and requiring each vendor to use a unique password that you give them.

  None of these considerations are mandatory. Instead, they are elements to consider while developing your company's overall cybersecurity risk management program.

Read more tips for responding to cyberattacks and insider threats.

Flat or segmented? Consider your company's architecture

Get an understanding of your organization's cyber architecture from cloud to modem to firewall to router to endpoint. Consider what defenses are in place and whether your network is flat or segmented.

Often, companies set up systems with a goal of making them easily accessible by company employees. The downside is, a flat network architecture makes it easy for intruders to navigate your systems once they are past the firewall.

> Get an understanding of your organization's cyber architecture from cloud to modem to firewall to router to endpoint. Consider what defenses are in place and whether your network is flat or segmented.

Firewalls are a primary tool your company can use to prevent malicious actors from accessing your systems. However, once someone passes the firewall, often, the company's systems are flat, i.e., it is easy to navigate from one part of the company's systems to another.

The solution is a segmented network, one that has access controls between the company's various systems. As a small company grows, it should consider upgrading the sophistication of its systems and implement a segmented network.

Kang uses an analogy to compare the two: "Think of a flat network like a company's 'open office.' If a burglar picks the lock to the front door, she or he can steal things from every cubicle or desk in the open office. In contrast, a segmented network is like a hotel. Even if a burglar entered the lobby of the hotel, s/he would need to pick the lock of every hotel room in order to steal things from each room."

Implement multi-factor authentication (MFA)

Don't rely on simple password access. Systems that don't require multi-factor authentication (MFA) open your company to the risk of "password spray" attacks, in which a malicious actor targets your systems with a high volume of password guesses based on a password pattern that the bad actor has figured out. For example, for temporary password resets, many companies unfortunately use a pattern that is too easy to guess. In 2018, the United States Attorney's Office unsealed an indictment against foreign actors who used this technique to gain entry into numerous government and private sector systems. Such attacks continue to this day, notes Kang.

To reduce this risk:

- Put in place multi-factor authentication, i.e., a two-level authentication where the users must input their password then receive a text or email with a separate code that they must input to access your systems.
- Require strong passwords. Although using a combination of characters is important, the length of the password is key.
- Check if your company uses easy to figure out patterns for temporary reset password. If so, ask your IT staff to use a random password generator instead.

Inventory your company's endpoints

Endpoints are the devices in your organization's network (cellphones, laptops, printers, etc.). Many companies don't have a precise understanding of the endpoints they have, which makes it difficult to manage cybersecurity. Conduct an audit and inventory of which devices are part of or connected to your network.

> Many companies don't have a precise understanding of the endpoints they have, which makes it difficult to
> manage cybersecurity.

Patch, patch, and patch

Make sure your systems regularly receive the latest patches from the manufacturer. Ensure you have a defensible patching schedule. That said, there may be sound business reasons for postponing installation of a patch.

Keep in mind that your company's IT team may want to test patches before implementing them, which may delay the introduction of the patch. Companies may also want to "batch install" multiple patches at one time, to minimize business disruptions. Kang suggests developing a defensible, repeatable process and to schedule for testing and installing patches.

Calibrate your detection-and-alert system

The security incident management system (SEIM) is akin to a guard shack on a property, per Kang's analogy, with guards checking what an alarm ringing is about. SIEM gets security information from different sources and uses pre-determined settings to assess what the incident is about.

A common issue that companies face is they have robust SIEMs but haven't calibrated them properly. This may result in false positives, which might lead the team to stop paying proper attention to the alarms. This goes to Kang's earlier point that an IT manager may be skilled in keeping the company's computer systems running, but may not be trained in modern security techniques. For example, make sure your team knows how to calibrate the SIEM and interpret its results.

Cybersecurity requires ongoing attention. In-house counsel have an important role to play in advancing cyber safety at their organization, and in limiting the risk of tremendous losses that can result from cyber incidents.

Read more ACC cybersecurity articles by Professor Robert Kang.

Interested in a cybersecurity law practices? Read "What is a Cybersecurity Legal Practice?" by Daniel Sutherland.

Join the ACC IT Privacy & eCommerce Network.

Find more resources in the ACC Library.

Association of Corporate Counsel

Staff

ACC