ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

My Take: A Corporate Counsel’s Role in Protecting an Organization’s Cyberspace

Community

Technology, Privacy, and eCommerce

October is not just a time to enjoy cooler weather and seasonal festivities — it's also Cybersecurity Awareness Month. The goal of Cybersecurity Awareness Month is to bring attention to the importance of online security to our nation. This year's theme, selected by the National Cybersecurity Alliance (NCSA), is "Do Your Part. #BeCyberSmart."

According to the NCSA, the intention behind this year's theme is to empower individuals to take ownership of their role and impact on cybersecurity in their own space. "If everyone does their part — implementing stronger security practices, raising community awareness, educating vulnerable audiences or training employees — our interconnected world will be safer and more resilient for everyone," states the NCSA.

Interfacing over the internet has become critical to today's interconnected world. Anything that is connected to the internet is inevitably at risk. Hackers are becoming increasingly more sophisticated and, with that, our strategies to combat them must also evolve.

> Anything that is connected to the internet is inevitably at risk.

This, however, is no surprise given how technology advances. Ray Kurzweil's Law of Accelerating Returns aptly highlights the development trend of information technology — a trend that accelerates exponentially. With this, developments in the technology behind the different types of attacks will also be subject to such exponential acceleration.

So, how can you contribute to your cyberspace? Well, that depends on your role and responsibilities, but what is certain is that everyone plays a part no matter how small. Something as simple as clicking on a malicious link in an email can have complex repercussions. Educating yourself and following the recommended security practices can effectively reduce risk.

As corporate counsel, a key part of the job is to advise on risks that may affect your organization. It is safe to say that at some point in time, everyone will be the target of a cyberattack. Simply, this is not a matter of *if*, but *when* one will occur. Here are just a few things to consider in your cybersecurity strategy.

Buy-in

Make sure cybersecurity is a topic that routinely gets onto the agenda for meetings with key stakeholders, such as your board and executive level management.

Ensuring management appreciates the significance of cybersecurity is the bedrock of any cybersecurity program. This includes helping management to appreciate the potential damages — both financial and reputational — of these threats so they can appropriately allocate resources.

But it's not just upper-level management that needs to be involved. Ensuring every department of your organization is cognizant of the importance of good security hygiene is crucial. Your organization needs to embrace security as a culture, not just a checklist.

Communication

Ensure every sector of the organization knows when to come to the security and legal teams for assistance. Remind them that you are accessible and not in an ivory tower. Even if they do not have a full understanding of the laws, rules, and regulations, simply knowing when they need to notify you — and that you are there to help — can avoid unwanted surprises.

For example, when there is a change in the types of data your organization processes or a change in how your organization processes that data, discovering such major changes earlier on in the process can help to avoid extra work required to backtrack and fix processes that fall short of compliance.

Data mapping

Knowing what kind of data your organization handles will help you to understand what controls you will need to put in place and what laws are implicated. Additionally, knowing where that data lives and how that data is being handled is crucial. This will be important if a system is compromised. You cannot accurately assess the damage without knowing the full extent of what has been lost or otherwise compromised.

Compliance efficacy

Having robust and up-to-date security policies and training is an important part of every compliance program. However, it is also important to not think about security as a simple "check the box" type of initiative. Your program should be simple and make people want to participate. Its effectiveness should be frequently tested and benchmarked. Do not let your security controls, policies, and training become outdated. Security is a moving target.

Third-party risk management

Since you are at the forefront of the contracting process, it is important to ensure you work with your

security teams to create minimum security requirements for your vendors. Frankly, every department should have a thorough vendor vetting and onboarding process. Like everything else in your security program, update these regularly as security standards change.

Additionally, make sure the organization follows through with audits and routinely requests security reports from its vendors. If there are material deficiencies with your third-party providers, have a plan for remediation, up to, and including, termination. Do not let their faulty security practices impair your organization's security.

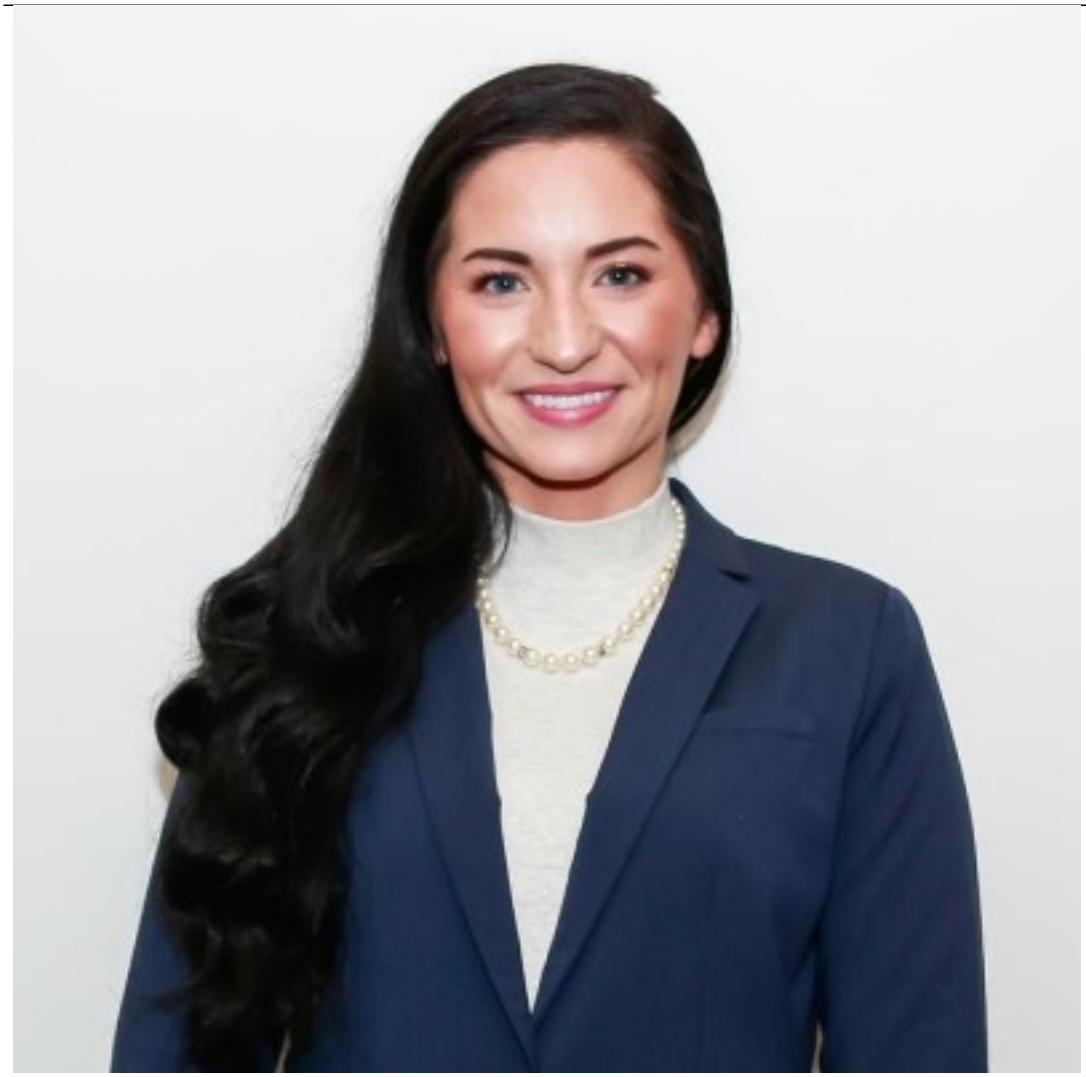
Have a plan

Prepare for the worst-case scenario. It is important to ensure you have a robust disaster recovery plan and that everyone knows their role in it. When something goes wrong, the legal department will be tasked with damage control. Think in terms of having the most defensible position possible. If your organization were to be subpoenaed after a security incident, for instance, what information might be revealed? What loopholes would be found during discovery?

Of course, this is a non-exhaustive list. There are many ways you can help reduce your organization's cybersecurity related risks. Even if you feel that your organization already has a decent program in place, make sure you are benchmarking it against others in your industry. Run drills if you are able.

Cybersecurity is, and will continue to be, a moving target. Make sure the processes your organization implements are not only effective for what it does today but are also forward-looking and can scale with the organization's roadmap. Lastly, research is monumental. Staying apprised of the latest developments in cybersecurity can help you to proactively anticipate threats that may impact your organization.

Alicia Dietzen



General Counsel

KnowBe4

Alicia Dietzen is general counsel of KnowBe4, Inc., a publicly traded security awareness training and simulated phishing company listed on the Nasdaq stock exchange. In addition to building out the company’s legal team as its first in-house counsel, Dietzen has assisted the company with its international expansion efforts, multiple investment rounds and their recent IPO. She is the recipient of the 2021 Florida Business Observer’s 40 Under 40 recognition, 2021 Association of Corporate Counsel Top 10 30-Somethings recognition, 2021 finalist of the CSWY Cybersecurity/Privacy Woman Law Professional of the Year recognition, and received the 2019 Tampa Bay Business Journal Top Corporate Counsel Honoree and 2018 finalist recognitions. Dietzen currently serves on the Women’s Committee of the Association of Corporate Counsel’s West Central Florida Chapter and has her IAPP CIPP/E certification.