CxO Trust Newsletter - March 2022

CEO Intersection

Jim Reavis, CEO & Founder, CSA

Hi All,

I hope your "cyberyear" is going well so far and you are being vigilant while hoping for the best.

We are excited that former NSA general counsel Glenn Gerstell will be joining us at SECtember this year. We are working with him on his speech topic, but he has done a lot of writing and speaking recently about more effective cyberwar collaboration and response within government and the private sector and I expect this will be a theme. He will also take part in an interactive session at the CxO Trust Summit @ SECtember, which will be great for those of you wanting to have more confidential conversations about the topic.

It has now been three weeks since we announced the Zero Trust Advancement Center and we are heartened by the great response. One of the first initiative deliverables is a survey to be presented at RSA, "CISO Perspectives and Progress in Deploying Zero Trust". Readers of this newsletter have a special job – to provide peer review of the survey questions. We want to make sure that survey questions match what questions you might have about Zero Trust pain points and success stories. You will receive the draft survey shortly and we hope you will help us out in addition to taking the final survey when available.

Finally, I wanted to make you aware that CSA has partnered with the international law firm Orrick Herrington & Sutcliffe LLP on an important call to action. The SEC has proposed new cybersecurity rules and our industry needs to work quickly to send our responses in. While you may want to send a response representing your own company, we find that responses coming from CSA tend to carry a lot of weight, due to our non-profit status and a perception that we can address the issues without any encumbrance. Orrick attorneys Carolyn Frantz and Aravind Swaminathan will act as facilitators for CSA, answering questions you may have and helping us draft a consolidated response. Carolyn was kind enough to draft a message to you with more information and I think she hits the nail on the head in regards to concerns we should have about the rules.

As you know, the SEC has proposed new disclosure rules for public companies regarding cybersecurity incidents and related policies and procedures. The proposed new disclosures fall into two main categories:

1. **Incident reporting**: 8-K disclosure of material cybersecurity incidents involving information systems owned or used by an issuer within four days of an issuer's determination that an incident is material, such determination to be made as soon as "reasonably practicable", and certain updates in periodic reports, including reports on the remediation of previously reported incidents.

2. **Periodic disclosure of cybersecurity risk management, strategy, and governance**: reporting of an issuer's internal approach to cybersecurity, which would require disclosing, among, other things (i) policies and procedures to identify and manage cybersecurity risks, (ii) the role of cybersecurity in company strategy, financial planning, and capital allocation, (iii) board oversight, (iv) management's role and expertise, including its processes for assessing and mitigating risks from third parties, and

(v) the names of any directors with cybersecurity expertise, and such detail as necessary to fully describe the nature of the expertise.

The SEC has invited comments, which will be due on May 9.

While there are many potentially problematic aspects of the SEC's proposed rules, we have tentatively identified some areas of possible focus for CSA membership:

- **Lack of national security/law enforcement exception.** Unlike state cyber incident disclosure statutes, the SEC's proposed rule contains no provision allowing a delay in disclosure where law enforcement or national security officials request it. The SEC has specifically asked for commentary on this aspect of the rule, and it is of obvious concern. The CSA may be uniquely positioned to provide constructive suggestions for how a workable national security/law enforcement exception could be implemented into the rule, based on members' experiences with incidents that implicate these concerns.

- **Third-party reporting.** The rules as proposed define a registrant's "information systems" as "information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations." And then defines a "cybersecurity incident" (which has to be reported if material) as "an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing thereon." This reporting obligation would likely, therefore, include many incidents involving third parties, including IaaS, PaaS, and SaaS providers. In addition, the SEC also wants issues to disclose whether they have "policies and procedures to oversee and identify the cybersecurity risks associated with [your] use of any third-party service provider." Issuers will often have challenges, however, in reporting incidents originating at third parties because they may not have sufficient information about them, particularly for SaaS providers. Given the CSA's expertise in recommending how to divide responsibility for cybersecurity incident response between cloud customers and cloud service providers, we believe we could help provide the SEC guidance on how to make these rules clearer and more effective.

- **Reporting timing.** The rules provide for issuers to report incidents within four days of a determination that an incident is material, which determination should be made as soon as is reasonably practicable. This approach is undefined, and difficult to implement where incidents themselves, as well as the information about them, is evolving. Especially if "incidents" are defined to include vulnerabilities, which is likely under the proposed definitions and the SEC's recent enforcement approach, early disclosure can create additional security risks, for example where the reporting organization has not contained the vulnerability/attack, because they may be subject to follow-up attacks. While the problems with the SEC's proposed timing are obvious, CSA members could help the SEC craft a better system for timing of disclosures, perhaps differentiating between vulnerabilities and other types of incidents, providing a stay for reporting until containment is achieved, and suggesting appropriate principles issuers should follow in determining the appropriate time for disclosure.

Please review the information and submit your comments here.