beazley

Article

View from the Beazley Cyber Council: How the new SEC rules on cyber are impacting corporate boards and CISOs

Bethany Greenwood

The Beazley Cyber Council meets quarterly. Its membership includes former US and UK security officials with specific expertise in cyber as well as commercial sector experts well-placed to understand the latest developments in the behaviour of criminal cyber groups, the technology which is transforming cyber (both attack and defence), and the regulatory developments which are likely to impact this space. The Cyber Council is a horizon-scanning body whose conclusions are designed to confer expert advantage on Beazley underwriters and their clients.

The new US SEC rules on cybersecurity[1], came into effect in December 2023 for public companies and will apply to smaller US companies from June 2024. Three months in, the Beazley Cyber Council (a diverse group of experts from government, technology research and specialist cyber sector backgrounds including Beazley cyber leadership) has reviewed the real world impact its experts are observing.

Engagement with Chief Information Security Officer (CISO) and C-Suite executives across the US make it clear that they feel a marked increase in overall corporate scrutiny and in the levels of reputational damage to their careers. And it is not just in the US where regulatory oversight is stepping up. The new NIS2 directive[2] which will come into effect across the EU by October 2024 puts direct responsibility on boards to approve cyber risk management measures and oversee their application. Under this new EU regulation, members of the C-Suite can be held personally liable if found negligent in serious cyber incidents.

Beazley Cyber Council members noted that CISO concern spiked in the aftermath of the SEC complaint against Solar Winds and its CISO on 30 October 2023 and has continued to build since. In a February 2023 survey of 200 US and UK CISOs conducted by Globalsurveyz (and commissioned by Cynet), 94% of CISOs described themselves as stressed[3]. In addition to the increased regulatory burden on them, CISOs face an expanding attack surface due to digital transformation programmes within their companies, and they find themselves struggling to understand the changes in the cyber threat with the advent of generative AI.

At a corporate level, the new SEC rules have required an update to operational procedures as public companies are mandated to reveal their management expertise in the assessment and management of cyber risk. The shift increases the pressure on CISOs to ensure accurate disclosures. Board members can potentially challenge a CISO's decision to report a 'material' cyber incident because of the impact on the share price. A CISO is then stuck between appeasing the Board or prosecution for negligence.

Proactive companies are addressing these regulatory changes by establishing robust processes for determining the materiality of cyber incidents promptly after discovery[4]. Some companies are considering the insertion of an independent, trusted (under NDA) arbiter to act as a challenge function in cases where the CISO and other company seniors may disagree.

In response to the 2023 SEC ruling, we have introduced a new endorsement to support our public company cyber clients. In the event of a cyber incident our endorsement covers the cost for a securities attorney to prepare and file the disclosure report on the behalf of a client. The client can either use an attorney from our existing panel of providers or a securities attorney of their choice to file the disclosure. Our Full Spectrum Cyber solution enables us to continually adapt and manage risks as they evolve. To find out more on our new SEC endorsement, click here.

Bethany Greenwood

Group Head of Specialty Risks

[1] www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214

[2] NIS2 Directive | Prepare Your Organization Now

[3] CISO Stress Survey (cynet.com)

[4] https://www.ey.com/en_us/cro-risk

admitted basis in some but not all US jurisdictions, through Beazley Insurance Company, Inc., and is available on a surplus lines basis through either Beazley Excess and Surplus Insurance, Inc. or a licensed surplus lines broker underwritten by Beazley syndicates at Lloyd’s. The exact coverage afforded by the product described herein is subject to and governed by the terms and conditions of each policy issued. The publication and delivery of the information contained herein is not intended as a solicitation for the purchase of insurance on any US risk. Beazley USA Services, Inc. is licensed and regulated by insurance regulatory authorities in the respective states of the US and transacts business in the State of California as Beazley Insurance Services (License#: 0G55497). BZ CBR 114.

beazley