Diligent

10 QUESTIONS

to Ask When Evaluating Board Portal Security

When organisations engage a board portal provider, they are entrusting them to safeguard sensitive documents and provide a system for managing access to those documents. This trust goes beyond technical specifications. That's why it's essential for boards, corporate secretaries, general counsels and CIOs to be comfortable with and confident in their board portal provider's security.

To that end, here are 10 questions that organisations should be asking of any potential board portal providers:

1 Does the provider make a substantial investment in cybersecurity research and development?

Cybersecurity threats are continually evolving – not only due to advances in technology, but also because of changes in the cyber underworld. Lone hackers have given way to sophisticated organisations that can cause disruption on a global scale. A board portal provider should be able to demonstrate research and development capabilities that enable it to stay ahead of emerging threats.

2 Is the provider transparent about its security processes?

The provider should be clearly able to explain its physical security safeguards (protection of the servers, routers and other equipment), screening processes for new hires, internal controls, system monitoring (if they were hacked, how would they know?), and any history of security breaches and their resolution.

3 Does the provider meet the highest industry standards?

As third-party handlers of confidential information, board portals should meet security standards comparable to those of the most demanding IT departments across a number of industries. Key accreditations include: a history of clean annual SOC/SSAE 16 audits (covering how providers report on their internal controls) and ISO 27001 certification for security (compliance of the actual software provider's information security management systems with international standards, as opposed to merely their data hosting centers' compliance).

4 Does the provider allow outside penetration testing?

Most board portal providers conduct penetration testing as part of their quality control. Portals with high security standards will conduct testing on an almost continuous basis instead of annually in order to keep up with evolving threats. They should also allow clients and potential clients to conduct their own security and penetration testing (or engage third parties of their own) to run independent tests. Doing so is a powerful demonstration of confidence – as well as an acknowledgement that security is ultimately a team effort.

5 Does the provider rely on third-party platforms or software?

Many board portals are built on top of commercially available platforms, or they use ready-made plug-in components for certain elements of their software. Those third-party elements, however, come with their own security vulnerabilities, which are attractive to hackers precisely because those platforms are so widespread and not built for the demands of a board portal. Instead, board portals should be built from the ground up with security features designed into the applications at every point.

6 What level of physical security does the provider employ?

While digital information is often thought of as intangible, in fact it is stored on all-too-real servers. Those data hosting facilities need to be protected with onsite guards, closed-circuit television and multiple layers of perimeter security. The servers themselves should be housed in secured cages with each hosted organisation's data physically segregated. And their cryptographic keys should be protected by hardened, tamper-resistant devices.

7 What degree of data redundancy is provided?

Is data backed up and do primary data centres fail over to disaster recovery data centres? Board portal providers must offer remote, geographically dispersed locations to ensure that any event impacting one location will not affect the secondary location. In addition, data redundancy must be supported by real-time, 24/7 intelligence on data performance.

8 Can user access to the portal be restricted to a specific device?

With board members spread around the world and traveling frequently, the need for securing their mobile devices is paramount. Can a user's access to the portal be restricted to a specific device that is enrolled with the board portal? Is there also an option to disable browser access? Device authorisation solutions allow organisations to prevent access from unknown, untrusted devices. The result is stronger control of access rights and locations.

9 Does the provider allow you to "right size" the portal's level of security?

Every security solution involves a trade-off between convenience and security. As a result, one size definitely does not fit all organisations. Instead, a board portal should be able to tailor functions to fit an organisation's specific security needs, such as allowing for different password strengths, lockout policies, and options for exporting and printing board documents from the portal.

10 Are the portal's security features backed up with customer support?

No matter how strong a portal's security may be, human monitoring is needed to ensure that any issues are dealt with promptly. For example, a director who repeatedly mistypes a password and is locked out of the system should receive a customer support phone call immediately, both to provide assistance and to verify the cause of the unsuccessful attempts.

For more information or to request a demo, contact us today:

Email: info@diligent.com
Call: +44 (0) 800 234 6580
Visit: www.diligent.com