Cybersecurity and the Evolving Role of Boards:
From Providing Oversight to Setting an Example

Jeffry Powell
Executive Vice President, The Americas

Charlie Horrell
Managing Director, Europe, Middle East and Africa

Al Percival
Managing Director, Australia and New Zealand

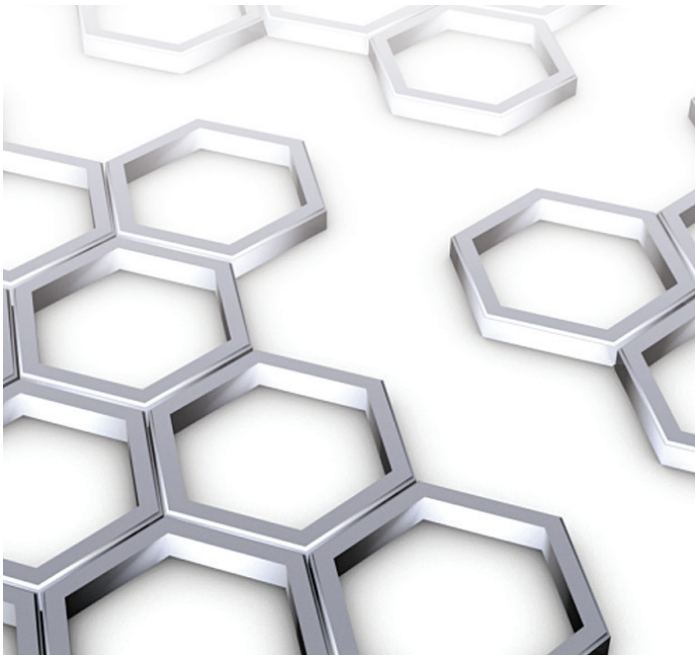
Brian Locke
Director of Security

At a time when the theft of customer information often leads to executive-level shake-ups, boards are taking a greater role in evaluating the adequacy of their organizations' cybersecurity. But many boards have yet to apply the same level of scrutiny to their own security. This article provides an evaluation framework for directors and senior management. Focus is on three main factors: where data is stored, the strength of "locks" that provide access, and the control of "keys" for entry.

Leadership's engagement with cybersecurity is not only internally driven. Regulators have also begun to raise expectations. For example, in the United States, the Securities and Exchange Commission has affirmed the importance of including cybersecurity processes and events in a public company's disclosure of risk factors and material events.[1] And while these regulations may not apply to privately held companies and non-profits, they are nonetheless held to strict standards by their owners, business partners and donors.

Despite the board's responsibility for overseeing cybersecurity, they often overlook one critical link in the cybersecurity chain: the board's own role as custodian of company information. After all, a board routinely handles, stores and internally shares sensitive financial and sales data along with confidential strategic plans, senior executive compensation policies and other privileged information. Unauthorized access to any of this information could have severe consequences.

Diligent



The problem is that a board's position "above" the organization means it is often excluded from the organization's own processes. As a result, when the chief information officer reviews the enterprise's cybersecurity needs, he or she may understandably believe that board security is a matter for the corporate secretary or general counsel. The assumption may be that board-level cybersecurity is outside the CIO's domain.

There is also the undeniable fact that all cybersecurity options entail a trade-off between convenience and effectiveness. Because of the senior status of board members and leadership, there is a natural tendency to minimize any inconvenience on their part. As a result, board members often opt to access, store and share information in ways that may be convenient but that are considerably less secure than what is done by the organization as a whole. These include the sending of hard-copy packs of board materials or the emailing of PDFs.

Another trade-off is where passwords are required. Instead of mandating secure passwords that contain no recognizable words and that consist of a combination of different character types, simple passwords such as a child's name may be permitted. While these practices often arise from ad hoc decisions rather than deliberate policy, they are nevertheless resistant to change due to inertia.

Given the heightened level of threats in these times, boards and senior management must do more than provide oversight of an organization's cybersecurity. They must set an example of security best practices from the top.

A FRAMEWORK FOR EVALUATING BOARD SECURITY

Leaders who want a firm, intuitive grasp of how to judge their board's cybersecurity practices can easily end up in a tangle of jargon. Fortunately, however, it can be easily straightened out by asking three basic questions:

1. **How is the board data stored?**
2. **How strong are the locks?**
3. **Who controls the keys?**

Posing these questions can help with the evaluation of the board's current solutions for information sharing, communication and collaboration – as well as any it may be considering.

How is the board data stored?

Any security evaluation should begin with the examination of who controls the data. Not knowing where information is and having an inability to control where it goes mean the solution is highly unsecure.

This is why emailing board documents as PDF files is not a secure solution. Files can be accidentally forwarded by directors to others outside the board, or housed in personal email accounts with minimal consumer-level security.

The same holds true for public file-sharing systems where files are stored "in the cloud." What it really means is that your files could be on any server in the file-sharing network; you as a customer have no way of knowing exactly where they are. This nebulousness is why it's called a "cloud" in the first place. One reason for the popularity of cloud-based storage systems among consumers has been the assumption that such systems are relatively secure. But high-profile cases of hacking, such as revelations of passwords and celebrity photos from cloud providers,[2] demonstrate just how flawed that assumption is.

Although hosted board portals do seem cloud-like – and are often mistakenly referred to as "cloud-based storage" – there are important differences. For one thing, they carefully control where your data is stored on the hosted system. What's more, they keep the information of each hosted organization segregated from each other. Knowing where data is located as well as its protective security measures provides greater control and assurance over who has access to the information.

How strong are the locks?

Keeping close tabs on data's whereabouts is certainly crucial, but so is ensuring that only authorized users can access it. This is accomplished through encryption, i.e., the enciphering of data into a string of meaningless 0s and 1s. Only those with the correct digital key can decipher it.

Of course, paper board packs have no digital key at all; the information can easily be read by everyone who gets their hands on it. And while it may be true that PDFs that are emailed or stored on file-sharing systems can be encrypted and protected by passwords, it puts the onus on whoever is distributing and receiving the material to manage password protocols. Further, documents "protected" in this way still remain vulnerable to "brute force" attacks via readily available software.

Higher-quality hosted board portals typically use 256-bit encryption – a key of 256 0s and 1s. Since there are more possible combinations than stars in the universe, it's safe to say that it would take almost an eternity for even the most determined hackers using the most advanced technology to crack the code.

Who controls the keys?

No matter how strong an encryption system may be, anyone with the right key can still access the information. For example, anyone who has the password to a password-protected PDF virtually owns the document. Stolen passwords mean stolen documents.

However, with a hosted board portal, a password only goes so far. Yes, it allows access to the portal. But because control of the encryption keys protecting the board documents resides within the system, the person logging in will only see what he or she is allowed to see. A strong portal never loses control of the documents. The security implications are significant. If a password is stolen, the administrator can simply deny access for that password.

And after sensitive documents are no longer needed, the administrator can conduct a "virtual purge," closing off the documents to anyone trying to access that user account with the stolen password.

Given the heightened level of threats in these times, boards and leaders must do more than provide oversight of an organization's cybersecurity. They must set an example of security best practices from the top.

Beyond the protection of needing the right password to gain access, a board's administrator can limit access to specific board documents according to criteria such as a committee membership, allowing them to be visible only to members of the audit committee or compensation committee, for instance. The administrator can also control from which specific device a director may access the system.

1 "CF Disclosure Guidance Topic No. 2: Cybersecurity," U.S. Securities and Exchange Commission Division.

2 *Wall Street Journal*, "Apple Denies iCloud Breach: Tech Giant Says Celebrity Accounts Compromised by 'Very Targeted Attack,'" September 2, 2014. http://online.wsj.com/articles/apple-celebrity-accounts-compromised-by-very-targeted-attack-1409683803

THE RIGHT MESSAGE STARTS AT THE TOP

While cybersecurity may have a permanent place on the agendas of boards and senior management in more and more organizations, that's not enough. Security must also be a permanent part of boards' behavior.

Having the right platform to handle board information, communication and collaboration will ensure essential security practices are followed in the boardroom. It also sends the right message, namely: cybersecurity is everyone's business.

Diligent

Unleashing the value of information. Securely.

Diligent is the leader in helping boards and senior executives make better decisions through information sharing and collaboration. Over 3,500 clients and 96,000 directors, executives and administrators in 45 countries rely on Diligent (NZX: DIL) to speed and simplify how board materials are produced, delivered, reviewed and voted on. Serving over one-third of the Fortune 1000, we provide the world's most widely used board portal via iPad, Windows devices and browsers. Diligent has pioneered ease of use, stringent security, and superior training and support since 2001.

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

Email: **info@diligent.com**

Call: **+1 877 434 5443**

Visit: **www.diligent.com**

AICPA SOC

ISO 27001 CERTIFIED BY BRIGHTLINE

Download on the App Store

Download from Windows Store