Cyberthreat and Securing the Board:
Three Misconceptions That Undermine Boardroom Security

Rates of cyberattack are rising globally. Criminals are becoming increasingly adept at circumventing security systems and high-profile security breaches feature regularly in the world's media. Despite this, many boards still ignore the threat that cybercrime poses, and of those that have acted, many fail to adequately secure the board itself. In response, we have published this article, which is designed to help directors and managers better understand the issue of cybercrime whilst showing them how to reduce board-level security risk.

There are many factors that underpin the growth in cybercrime. The chance of getting caught is low when compared to other types of crime; data can be routed across thousands of computers so that attacks can be both anonymous and untraceable. The financial returns that cybercriminals can expect run into the millions; most cybercrime is committed by organised crime, with analysts estimating that cybercrime costs the global economy US$455B per annum.[1]

A successful attack can inflict huge damage upon an organisation. In addition to financial losses, stolen data and intellectual property can damage trade, competitiveness, innovation and reputations. Organisations can protect themselves, and by rethinking how they work with data and how they secure information, they can limit their exposure to attack.

1 "Net Losses: Estimating the Global Cost of Cybercrime," McAfee, 2014. http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2-summary.pdf

Diligent

ASSESSING YOUR BOARD

As decision-makers for the organisation, boards need to understand the threats that their organisation faces, but this can be difficult. Many directors may not realise just how digital the business has become; directors may not appreciate how the convergence of IT, Enterprise Technology and Operations Technology has shaped the business and led to an increase in opportunities for attackers to gain access.

Hierarchical structures within the organisation are also a consideration. The fact that the board is positioned "above" the organisation means that the employees responsible for the organisation's security my not feel confident enough to report back any misgivings that they have about the firm's security scheme. Research by Deloitte and Systemec suggests that, in some regions, up to 70% of IT decision-makers lack confidence in their company's security policies and concludes that more than two-thirds of organisations lack the ability to protect themselves against attack.[2] Similarly, the security team may not be aware that the board's security falls within their role, assuming that this instead falls under the control of the corporate secretary and should not fall within the remit of the organisation's own security scheme.

Given Boards need to understand the threats that their organization faces but this can be difficult, many directors may not realise just how digital the business has become

Another factor is the actions of the directors themselves contributing to a board's increased potential security risk; in choosing to access, store and distribute board materials in an insecure but convenient manner, directors are potentially exposing this data to third parties and losing control of that data. Email, PDF and cloud-based storage systems, for example, are likely to be much less secure than the methods employed by the organisation.

Directors and personnel need to remain diligent in their approach to communication technology. But the most secure working practices can still be undermined by the misconceptions associated with the technology and workflows in use.

THE THREE SECURITY MISCONCEPTIONS

To avoid directors working in a manner that can undermine your board security, you need to consider the following misconceptions:

1. Email is Secure

Whilst email may be convenient, quick and easy as a means of communicating confidential information, email is simply not fit for that purpose; with email, you cannot restrict the forwarding of content. In addition, rescinding a sent message is difficult, so as soon as an email is sent, you've effectively lost control of the information.

2. Password Protection Equals Security

Whilst it's not unreasonable to assume that adding a password to a PDF renders it inaccessible to unauthorised users, a rudimentary search across any popular search engine yields millions of results showing anyone how to bypass PDF security. Run that search on Google, and you'll find 2,300,000+ results documenting how frighteningly simple it is to breach this apparently secure medium. The truth is that PDF technology is not secure, and you should not rely upon it.

3. In-house Data Storage is More Secure

Perhaps the most important misconception to consider relates to data storage, specifically that data stored in-house is more secure than that stored with a third party. In truth, the opposite often applies; for example, in-house solutions rely on the organisation's own administrators to access and manage data, but with 55% of cyberattacks being carried out by insiders, this access can prove catastrophic.[3] Also, technically and operationally, the organisation's own security program and infrastructure may not be sufficient to protect data from today's threats. Conversely, a SaaS vendor such as Diligent restricts data access to authorised end-client users only; our team has zero access to client data. Furthermore, we have fully audited security policies and procedures, providing data backup and disaster recovery functions as well as security monitoring above and beyond the capabilities of most other organisations.

2 Global Risk Insights, September 2015. "globalriskinsights.com/2015/09/how-strong-are-the-middle-easts-cybersecurity-networks/

3 "IBM 2015 Cyber Security Index" and the "IBM X-Force Threat Intelligence Quarterly Q2 – 2015" https://securityintelligence.com/the-threat-is-coming-from-inside-the-network/

EVALUATING BOARD SECURITY

Leaders who want to assess their board's cybersecurity practices can do so by asking three simple questions:

How is the Board Data Stored?

Any security evaluation should begin with examining who controls the data. Not knowing where information is and having an inability to control where it goes means that 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 on systems that the vendors themselves admit should not be regarded as secure.

The same is true of "cloud"-based solutions where your files could be on any server in the file-sharing network and where you have no way of knowing exactly where they are. The success of cloud solutions is based upon the assumption that they are secure, whereas in fact, high-profile cases of hacking, such as revelations of passwords and celebrity photos from cloud service providers[4] demonstrates just how flawed that assumption of security is.

Although hosted board portals do seem cloud-like and are often mistakenly referred to as "cloud-based storage," there are important differences; hosted board portals carefully control where your data is stored and keep the information of each hosted organisation segregated. Knowing where data is located and how it is secured provides greater control and assurance over who has access to the information.

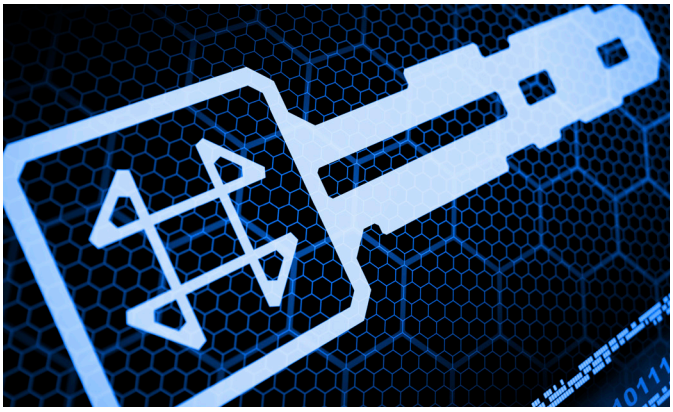
How Strong are the Locks?

Whilst knowing the whereabouts of your data is crucial, so too is ensuring that only authorised users can access it. This can be accomplished by encrypting that data, that is to say, converting the data into a string of meaningless 0s and 1s so that only those in possession of the correct digital key can decipher it.

Paper board packs have no digital key at all; everyone who holds a copy can read the information. Whilst it may be true that PDFs that are emailed or stored on file-sharing systems can be encrypted and password protected, it puts the onus on whoever is distributing and receiving the material to manage password protocols. Even then, PDF documents remain vulnerable to "brute force" attacks using readily available software.

Higher-quality hosted board portals typically use 256-bit encryption, and 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.

4 BBC News, http://www.bbc.co.uk/news/technology-29011850



Who Controls the Keys?

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

However, a strong portal never loses control of the documents; a password only goes so far because control of the encryption keys resides within the system; the person logging in will only see what he or she is allowed to see, and if a password is stolen, the administrator can simply deny access for that password.

In the case of authorised users, administrators can limit access to specific documents as well as assign access and visibility of documents to a user group; for example, a compensation committee may prefer to withhold sharing their information with the board as a whole.

The administrator of a hosted board portal can control device access too, restricting director access from personal, less-secure devices and mandating access through organisation-owned systems. Also, when sensitive documents are no longer needed, the administrator can conduct a "virtual purge," closing off the documents to any users trying to access those files. Similarly, access can be restricted according to user or device, useful if a director leaves the board and materials need to be recovered or a password has been stolen.

SET A SECURE EXAMPLE

Cybersecurity, particularly the security of the board's own information and data, must be of paramount consideration; having a secure, intuitive board portal handling all board information, communication and collaboration facilitates better board security and improved working practices.

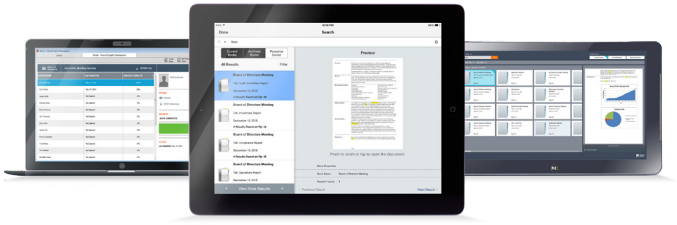
A board's failure to uphold high security standards can undermine the security scheme of the organisation as a whole, whereas a board that leads by example increases the effectiveness of the organisation's security and places it in a robust position in the face of increasing threats.

Diligent

Unleashing the value of information. Securely.

Diligent helps the world's leading organisations unleash the power of information and collaboration – securely – by equipping their boards and management team to make better decisions. Over 4,000 clients in more than 70 countries rely on Diligent for immediate access to their most time-sensitive and confidential information along with the tools to review, discuss and collaborate on it with key decision makers. Diligent Boards expedites and simplifies how board materials are produced and delivered via iPad, Windows devices and browsers. At the same time, it delivers practical advantages like cutting production costs, supporting sustainability goals, and saving administrative and IT time

Join the Leaders. Get Diligent



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

Call: **1800 646 207 (Australia)**
0800 434 5443 (New Zealand)
Email: **info@diligent.com**
Visit: **www.diligent.com**

AICPA SOC

ISO 27001 CERTIFIED BY BRIGHTLINE

Download on the App Store

Get it from Microsoft