Praxonomy Blog
EMPOWERING BOARDS

Email for the Board? Think Twice

Written by Carissa Duenas on June 18, 2019

Despite the emergence of new communication platforms on the Internet (e.g. social media, messaging, video calls, etc.), email continues to be the most important electronic business communication tool. It's not only because emails are considered "official" documents, but also because email works. It saves time and offers tremendous convenience, along with ease of use.

Email, however, comes with inherent risks, especially when it comes to data security and privacy. While creating frameworks for the prudent use of email is a responsibility that usually falls on the shoulders of the organisation's IT and compliance functions, Board members and senior executives need to exercise a higher degree of individual caution given the sensitivity and confidentiality of the information they are privy to.

Here are some of the risks associated with sharing highly sensitive information over email and email platforms.

EMAIL SECURITY RISKS FOR THE BOARD

Unintended Recipients

One of the primary risks of the use of email is that it can land in the wrong hands. In many instances, this is due to human error. Incorrectly entering an email address can direct Board-level information to unintended recipients, exposing the organisation to strategic, operational, or security vulnerabilities. There are limited means of "unsending" an email message, but they offer no guarantees that the recalled email hasn't been read or disseminated. As obvious as this problem is, it remains a potentially serious mistake that executives, including Board members, make again and again.

Phishing

Phishing, which is the fraudulent practice of using email (or other messaging platforms) to lure a bulk number of email recipients to perform an action such as giving up passwords or personal financial information (Google's Jigsaw unit created this excellent quiz), has evolved in complexity and sophistication over the last couple of years. Today, email users are confronted with a different security challenge: spear phishing and whale phishing. They substantially require more effort from the hacker, but the success rate from these attacks is notably high.

Spear phishing is a targeted email phishing attack focused on individuals. Whale phishing is a form of spear phishing. The only – yet significant – difference is that whale phishing specifically hones in on the highest-ranking members of organisations. This includes Board members.

A whale phishing attack involves studying the target executive and target company through available social media resources, and then using the obtained data to steal valuable company information. Whale phishers are known to impersonate or pose as Board and c-level executives of the organisation in order to harvest username and passwords, financial records, trade secrets, and confidential information – all primarily via email.

Interception

The journey of an email from sender to receiver has various vulnerability points. For one, the contents of emails, by default, are not encrypted. This means that emails are sent in readable text across the Internet "in transit." There is also no guarantee that emails "at rest" are not susceptible to unauthorised third-party access. Emails can be read and tampered with after they have

been received or sent. By nature, emails are not secure-by-design.

In addition, the widespread use of unsecure network configurations (e.g. such as open, public wifi-connection) gives hackers the ability to read emails as they are transmitted from one's devices to mail servers, placing user and confidential, sensitive information at risk.

Malware infections via email attachments

The prevalence of whale phishing attacks targeting Board and company executives has also made it easier to infect devices with malware, or malicious software, via email. Malware is often delivered through spam and/or the opening of email attachments. Although email users have become more wary of opening email attachments with executable files (.exe), malware can be transmitted through less suspicious file types (such as Microsoft Word documents) or through URLs in email messages and infect devices and users within or outside the company. This can have significant financial and operational impacts on the organisation.

Non-compliance with Regulatory Requirements

The European Union's General Data Protection Regulation (GDPR) has been in effect since May 25, 2018. In a nutshell, the GDPR's objective is to give individuals more control over who can access and use their personal information. It requires "data controllers" (or organisations handling personal data) to protect users' data more rigorously. Non-compliance of the law can result in fines of up to 20 million Euros, or 4% of the organisation's worldwide annual revenue of the prior financial year, whichever is higher. This cannot be overlooked by the Board.

How is the use of email a risk for non-compliance?

The GDPR requires "data protection by design and by default." As mentioned earlier, email is not, by default, secure by design. Technical measures need to be put in place to comply with regulations.

MITIGATING THE RISKS

Email Security Education

The Board, together with the organisation's employees, should be well versed with company email security policies and practices. This requires ongoing training and education, but ultimately serves the interests of the organisation in the long run. A security-oriented culture allows employees to adopt a cautious, informed stance towards the authenticity of emails and the framework for its use within the organisation (e.g. what types of content can be shared, what cannot, and what should or shouldn't be opened via email.)

Email Filtering

Board members should implement – and regularly update – email filtering and monitoring systems that can detect spam, screen for malware, and flag phishing attacks within their email applications. The use of anti-virus and anti-phishing software is also recommended.

End-to-End Email Encryption

To safely satisfy GDPR regulations, emails should be encrypted end-to-end. With end-to-end encryption, information is scrambled in such a way that only the sender and intended recipient can decode and read the email. This reduces the likelihood of data breaches of sensitive, personal, and company-related information, which, in turn, may save the organisation from catastrophic security vulnerabilities.

Moving the Board to a separate, secure email service may be the best option. Alternatively, Board members should consider installing GPG Suite (for Macs) or one of the Windows equivalents such as Gpg4win (for PCs) to encrypt their emails. Even if the Board cannot move to a separate email service, with email content encryption, the body of emails can be protected (but be careful about what goes into the Subject line -- these will still be sent across the Internet in plain text).

In addition and as a best practice, the Board, along with the rest of the organisation, should be discouraged from accessing and sending emails over unsecure, public WiFi networks unless protected by a virtual private network (VPN) service in order to avoid the risk of local interception.

Secure File-Sharing Options

When sending attachments with critical information, Board members should also consider using a tool such as Tresorit. Secure file-sharing/share link options offer end-to-end encryption, as well as offer more control and security for shared files than those sent over as email attachments. With these types of tools, shared files can have a unique password, an expiration date for file availability, tracking features to see who has opened the file, and file-access revocation.

Use of Board Portals

Board portals are an effective alternative to emails for Board communications. Premium board portals, such as Praxonomy, place significant emphasis on data privacy and security. This covers Board-related communications as well.

Board portals typically have built-in messaging systems. Since the use of board portals is limited to authenticated Board members and administrators, this messaging functionality subsequently minimises, if not eliminates, two significant risks:

1. that of sending confidential and sensitive information to unintended recipients
2. that of Board members falling prey to whale phishing attacks and malware infection

Because board-related communication and collaboration can be done within a highly-secure platform, the need for email as a business communication tool amongst Board members diminishes. Furthermore, data and files stored on board portals are protected by strong encryption, and access rights to individual files can be granted or revoked in real time. This offers boards much greater control over sensitive information than email.

To conclude, email is not going to go away anytime soon, and consequential and sophisticated risks will continue to permeate the email landscape.

The best defence against these risks is education and awareness. Board members need to assume a proactive, defensive approach towards email security and set the tone for the rest of the organisation.

ABOUT THE AUTHOR

Carissa Duenas is a marketing consultant and content contributor for Praxonomy. She began her management consulting career at Accenture and has since worked in a consultant capacity for leading organisations in the technology sector and communications space. She is a contributor to The Globe and Mail, Canada's leading national daily.