SULLIVAN & CROMWELL LLP

November 15, 2016

Recent Hacking Incidents and Cyber Threats to Director Communications

Public Companies Should Periodically Review Their Director Communication Practices to Ensure Appropriate Balance of Security and Efficiency in Light of Ongoing Cybersecurity Developments

SUMMARY

The growth in cybersecurity threats combined with the increasing demands placed on outside directors create challenges that often go beyond the risks that public companies face from employee and client communications. If public companies cannot communicate quickly with directors or directors cannot easily share information and discuss options, corporate governance will suffer. On the other hand, outside directors often have professional responsibilities to multiple organizations and, accordingly, are more likely to rely on electronic communications that are outside of any particular company's technology resources.

Recent hacking incidents highlight the need for public companies to review their director communication practices to ensure that they are current and that they appropriately balance security and efficiency. In this regard, public companies may wish to consider exploring or re-exploring alternatives that fit with their information security framework, such as dedicated company email addresses and/or board portals. Each of these options has benefits, as well as some drawbacks in terms of residual security, record-keeping or efficiency. Regardless of the particular approach taken, public companies should periodically review their director communications practices in light of ongoing cybersecurity developments, regularly update directors on information security risks, company practices and response protocols in the event of compromise, and consider providing technology and security support for personal devices and home offices maintained by outside directors.

BACKGROUND

Corporations have various alternatives for electronic communications with directors. Many common means of communication, however, have been subject to highly publicized cyber incidents. Most recently, former Secretary of State Colin Powell and campaign strategist John Podesta became the victims of intrusions into their web-based email accounts through a deceptive email that requested login credentials.[1] These intrusions revealed politically and commercially sensitive information, including acquisition targets and strategies for Salesforce.com, where Secretary Powell was an outside director, and private email addresses of other outside directors. Although online board portals are generally accepted as more secure than web-based email accounts, several years ago a board portal reportedly was infiltrated by malicious code that allowed collection of confidential data stored on the platform. These incidents and the seemingly continuous advancements in computer hacking techniques emphasize that no technology should be considered immune from intrusion and that company practices relating to electronic communication with directors would benefit from periodic review and refreshment.

POTENTIAL ENHANCEMENTS

As companies have continued to evaluate their practices, they have considered different systems for director communications, including the exclusive use of company email accounts by directors, and the adoption, or enhanced use, of online board portals. Each of these systems and policies has benefits and drawbacks and each company will need to strike the right balance for itself and its directors. Additionally, companies have explored general IT policies such as providing regular updates to directors on information security risks, company practices and appropriate protocols in the event information is compromised, and providing technology and security support for personal devices and home offices maintained by outside directors.

Corporate Email Accounts for Directors. Assigning company email addresses to directors has the advantage of placing director communications under the same information security framework that applies to employee emails.

- Company protocols governing the strength and duration of passwords, the length of time that emails and attachments are retained, and filtering for unsafe content, are applied automatically.
- Enhanced security measures such as multi-factor authentication, which requires two or more distinct forms of identification to access secure systems, also can be implemented.
- Policies and technologies can be updated without requiring special action on the part of directors. For instance, in the event a weakness is identified, a security patch or other measure can be implemented quickly without additional action by or further inconvenience to directors.

[1] *See, e.g.*, Lorenzo Franceschi-Bicchierai, *How Hackers Broke Into John Podesta and Colin Powell's Gmail Accounts*, Motherboard/Vice Media (Oct. 20, 2016).

Some of the limitations often encountered with this approach are:

- A director may be less likely to see communications or notifications on a timely basis if they arrive via an account other than the director's primarily email. This concern could be addressed, in part, by non-confidential alerts sent to the director's primary email account when new materials have been sent to the company address. However, for directors that serve on multiple boards, the reduction in efficiency could be compounded if all of the companies required use of an internal email address for all company and board correspondence.
- Directors may have personal devices or computers that differ from those used by the company, which may limit effective and timely access to communications or lead to installation and troubleshooting issues (including with respect to security patches and printing), and could necessitate company access to the director's personal devices.
- A process that is not sufficiently streamlined could result in directors taking steps inconsistent with the policy, particularly in an emergency situation where timely review of materials is critical.

Board Portals for Director Communications. Many companies have adopted, or are exploring the use of, online board portals to facilitate director communications, either exclusively or in combination with other communication methods. Board portals are specialized web applications that disseminate board materials and communications through a web interface that may have several advantages.

- The organizational features of board portals can help to compensate for the inconvenience of requiring directors to manage a second set of login credentials. Rather than having board materials and communications contained in multiple emails, board portals present these resources in one place, in an organized format.
- The administrators of the board portal can exercise some control over how board materials and communications can be downloaded, viewed/or and printed depending on, for example, the level of sensitivity of a particular document.
- Board portals can support customized document retention policies. Combined with their ability to organize related documents, this feature can promote efficient recordkeeping if used properly.

Some of the limitations often encountered with this approach are:

- Some board portals provide the option to capture metadata, including the extent and duration of directors' review of board materials. This information, while perhaps helpful in assessing the effectiveness of communications, has the potentially significant drawback that it could be attractive to plaintiffs in the event of litigation.
- Concerns have been expressed, including by some jurists, that electronic-only delivery of materials (as compared to delivery of paper copies) may hinder the ability of directors to adequately review, absorb and provide feedback on the content of complex documents. To provide an adequate opportunity for thorough review, it may be advisable to permit directors to download and print, at least the most complex or important information from these files, or to provide for secure delivery of these materials in paper form.
- Board portals, in and of themselves, may not guarantee secure communications because they may present a high profile target for cyber intrusion and because they may be coupled with policies or devices that are less secure.

TRAINING AND SUPPORT

Cybersecurity threats have become a persistent concern for companies and, as the body responsible for oversight and as users of technology themselves, board members may benefit from periodic IT training and briefings regarding the company's communication systems, and from ongoing IT support in the use of those tools.

- If a company has an IT incident response plan, directors may benefit from a briefing on the plan, including how the directors' own technology usage fits into this plan. For example, directors can learn the signs of an attempted or successful intrusion and how to react to them.
- Directors could receive regular IT training for safe practices in the use of a company's communication systems. Such a program could be adapted from materials used for employees and management to highlight emerging cybersecurity threats and techniques, as well as protective strategies and considerations.
- As a supplement to their IT training, directors will likely benefit from ongoing IT support for their accounts and devices. Ideally, this would extend to their use of such technology outside of a formal corporate setting, such as providing support for a director's home office.

OBSERVATIONS AND IMPLICATIONS

The information security landscape is evolving rapidly, and, while it seems clear that virtually all electronic communications systems are subject to intrusions, commercial, legal and regulatory considerations dictate that companies should periodically review their director communications policies and procedures with an eye toward an appropriate balance among user convenience, administrative flexibility and data security. This review should include the board, senior management and IT personnel so that the applicable communication system and polices provide reasonable security while respecting the practical needs of directors. Directors and company employees would also benefit from periodic updates regarding the company's IT policies and recommended practices for information handling as well as developments in cybersecurity and cyber risk management.[2]

* * *

[2] A summary of our firm's Cybersecurity Group and related resources is available at https://sullcrom.com/cybersecurity. On December 1, 2016, Sullivan & Cromwell LLP will host the 2016 Sullivan & Cromwell LLP / RANE Risk Management Summit to discuss pragmatic and proactive ways management and boards can mitigate enterprise cybersecurity risks. Details are available at https://ranenetwork.com/2016-sullivan-cromwell.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, three offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future related publications from Michael B. Soleta (+1-212-558-3974; soletam@sullcrom.com) in our New York office.

CONTACTS

New York

Francis J. Aquila	1-212-558-4048	aquilaf@sullcrom.com
Robert E. Buckholz	1-212-558-3876	buckholzr@sullcrom.com
Catherine M. Clarkin	1-212-558-4175	clarkinc@sullcrom.com
Jay Clayton	1-212-558-3445	claytonwj@sullcorm.com
Audra D. Cohen	1-212-558-3275	cohena@sullcrom.com
H. Rodgin Cohen	1-212-558-3534	cohenhr@sullcrom.com
Heather L. Coleman	1-212-558-4600	colemanh@sullcom.com
Donald R. Crawshaw	1-212-558-4016	crawshawd@sullcrom.com
Robert W. Downes	1-212-558-4312	downesr@sullcrom.com
Mitchell S. Eitel	1-212-558-4960	eitelm@sullcrom.com
John Evangelakos	1-212-558-4260	evangelakosj@sullcrom.com
William G. Farrar	1-212-558-4940	farrarw@sullcrom.com
Matthew M. Friestedt	1-212-558-3370	friestedtm@sullcrom.com
Joseph B. Frumkin	1-212-558-4101	frumkinj@sullcrom.com
David B. Harms	1-212-558-3882	harmsd@sullcrom.com
Alexandra D. Korry	1-212-558-4370	korrya@sullcrom.com
Stephen M. Kotran	1-212-558-4963	kotrans@sullcrom.com
John P. Mead	1-212-558-3764	meadj@sullcrom.com
Mark J. Menting	1-212-558-4859	mentingm@sullcrom.com
Scott D. Miller	1-212-558-3109	millersc@sullcrom.com
Nader A. Mousavi	1-212-558-1624	mousavin@sullcrom.com

Robert W. Reeder III	1-212-558-3755	reederr@sullcrom.com
Melissa Sawyer	1-212-558-4243	sawyerm@sullcrom.com
Glen T. Schleyer	1-212-558-7284	schleyerg@sullcrom.com
Marc Trevino	1-212-558-4239	trevinom@sullcrom.com
Krishna Veeraraghavan	1-212-558-7931	veeraraghavank@sullcrom.com
Washington, D.C.		
Janet T. Geldzahler	1-202-956-7515	geldzahlerj@sullcrom.com
Brent J. McIntosh	1-202-956-6930	mcintoshb@sullcrom.com
Robert S. Risoleo	1-202-956-7510	risoleor@sullcrom.com
Los Angeles		
Patrick S. Brown	1-310-712-6603	brownp@sullcrom.com
Eric M. Krautheimer	1-310-712-6678	krautheimere@sullcrom.com
Alison S. Ressler	1-310-712-6630	resslera@sullcrom.com
Palo Alto		
Nader A. Mousavi	1-650-461-5600	mousavin@sullcrom.com
Sarah P. Payne	1-650-461-5669	paynesa@sullcrom.com
John L. Savva	1-650-461-5610	savvaj@sullcrom.com
London		
Nikolaos G. Andronikos	44-20-7959-8470	andronikosn@sullcrom.com
Kathryn A. Campbell	44-20-7959-8580	campbellk@sullcrom.com
John O'Connor	44-20-7959-8515	oconnorj@sullcrom.com
David Rockwell	44-20-7959-8575	rockwelld@sullcrom.com
George H. White III	44-20-7959-8570	whiteg@sullcrom.com
Paris		
William D. Torchiana	33-1-7304-5890	torchianaw@sullcrom.com
Frankfurt		
Krystian Czerniecki	49-69-4272-5525	czernieckik@sullcrom.com
Melbourne		
Robert Chu	61-3-9635-1506	chur@sullcrom.com
Sydney		
Waldo D. Jones Jr.	61-2-8227-6702	jonesw@sullcrom.com
Tokyo		
Izumi Akai	81-3-3213-6145	akaii@sullcrom.com
Keiji Hatano	81-3-3213-6171	hatanok@sullcrom.com

Hong Kong

Garth W. Bray	852-2826-8691	brayg@sullcrom.com
Michael G. DeSombre	852-2826-8696	desombrem@sullcrom.com
Chun Wei	852-2826-8666	weic@sullcrom.com