A New Responsibility for Utility Boards of Directors: Cybersecurity

Given the central importance of electricity in the modern American economy, corporate boards need to consider how to discharge their responsibility for cybersecurity. There is no one-size-fits-all answer.

By Paul Feldman and Dan Hill

Electricity is the engine of the modern American economy. If a cybersecurity breach were to bring down a major portion of our power grid, we could not pump water or fuel, could not access our financial records, and our communications networks would be silent. Electric utilities and their boards of directors need to be proactive in dealing with this threat. The purpose of this paper is to share some thoughts related to utility boards of directors' governance and the responsibility for addressing cybersecurity.

What is a board's responsibility for dealing with cybersecurity? The question does not have a simple answer. It's essential that boards comply with best practice[1] protocols, but agreed-upon best practices for cybersecurity are scarce, especially in the board context. Any response requires a thoughtful understanding of the situation, careful consideration of the implications, and a decision-making system for

***Paul Feldman** is a director and past chairman of the Midcontinent ISO, where he chairs the Markets Committee and serves on the Information Technology and Governance Committees. Previously, Mr. Feldman served on the board of the Western Systems Coordination Council. **Dan Hill** is a board member of the New York ISO, where he chairs the Audit and Compliance Committee and serves on the Commerce and Compensation committee. Mr. Hill is retired from Exelon where he was Senior Vice President and Chief Information Officer. The views expressed here are Mr. Feldman's and Mr. Hill's and should not be attributed to any organization in which they serve. The authors extend their thanks to Robert Marritz for his helpful editing.*

[1] See http://en.wikipedia.org/wiki/Best_practice for a general discussion of Best Practices.

proceeding in unique circumstances. There is no one size fits all – for either board governance or cybersecurity – so it should be no surprise that combining the two is tricky.

Cybersecurity is an increasingly more frequent and important topic in corporate boardrooms. In a speech titled "Cyber Risks in the Board Room", Luis Aguilar, a commissioner of the Securities and Exchange Commission (SEC), highlighted the board's role in cybersecurity oversight:

> "Clearly, boards must take seriously their responsibility to ensure that management has implemented effective risk management protocols. Boards of directors are already responsible for overseeing the management of all types of risk, including credit risk, liquidity risk, and operational risk — and there can be little doubt that cyber-risk also must be considered as part of board's overall risk oversight. The recent announcement that a prominent proxy advisory firm is urging the ouster of most of the Target Corporation directors because of the perceived "failure…to ensure appropriate management of [the] risks" flowing from Target's December 2013 cyber-attack is another driver that should put directors on notice to proactively address the risks associated with cyber-attacks."[2]

Standard practices for how a board exercises cybersecurity oversight are still emerging. Ironically, while there is a common belief that many companies' management of cybersecurity needs improvement, management's operation of cybersecurity processes and protocols tend to be more mature than their board's execution of its cybersecurity oversight role.

The paper includes the following sections:

1. Board Expertise and Structure
2. Boards, Management, and Cybersecurity
3. Key Elements of a Cybersecurity Program
4. Risk Management and Cybersecurity
5. Questions a Director Should Ask
6. Traps To Avoid
7. Technology and Other Things to Think About
8. Conclusion

This paper attempts to address the most important considerations related to electric utility boards and cybersecurity. Each board will have to find its own way, but this paper may be useful in teeing-up the discussion, decision process, and possible directions.

The paper contains many references in the form of footnotes to assist with clarity and/or to suggest further research. In addition, we are developing a much longer document that is a collection of terms, articles, reports and other references that a director might want to access to deepen understanding of the subjects discussed here. It can be downloaded[3] from the Internet, and is a work in process. In addition, the National Institute of Standards and Technology

[2] See http://www.sec.gov/News/Speech/Detail/Speech/1370542057946 emphasis added

[3] Download at http://www.EnergyCollection.us/457.pdf

maintains a useful glossary[4] of cybersecurity terms for reference purposes.

I. Board Expertise and Structure

At a minimum, Boards should have the following responsibilities related to cybersecurity:

1. **Discuss and Decide**. Foster periodic discussion of the subject. Recognize it as a risk –a special pervasive and permanent risk. In those discussions, shape the board's specific policies and procedures for addressing the subject.
2. **Assign Board Responsibility.** Within the board structure, decide which committee is responsible.
3. **Get Regular Reports.** Normally, a committee assigned the task of overseeing the company's activities in the cyber area will receive regular reports (updates) from management. This may be an integral part of the company's risk management process.
4. **Stay Informed.** Cybersecurity has not been part of the dossier of most board members but it is now a critical area of business. If board members do not have sufficient experience to assist in their "duty of care" obligation they may need to enhance their knowledge level in this area. Since cybersecurity risks are continuously changing, the board should obtain periodic updates on the cybersecurity landscape.

Boards are typically made up of a diverse skill set that is aligned with the purpose and successful execution of the corporation's mission. Specific expertise required is sometimes legal in nature. SEC regulated companies are required to have director representation with finance expertise. Many boards include directors with expertise in diverse areas such as business operations, marketing, related industries, supply chain, or technology. Today, given the importance of cybersecurity, the question must be asked: "How much cyber knowledge do we need on the board?"

Boards should consider including a director (or directors) having cybersecurity expertise. While it would be a full-time job to be absolutely current with cyber risk and related technologies, it is important that someone on the board has a broad enough understanding of cybersecurity to know what questions to ask of both management and outside experts, and to form an independent opinion as to the adequacy of the company's cybersecurity program.

Duty of care[5] requires directors to exercise reasonable care in fulfilling their duties. They may rely on the business judgment rule[6] for some protection. Reliance on experts is often the route for exercising duty of care – using the opinions of "trusted others" as a substitute for personal expertise, but it is rarely a total substitute.

An operable description of reliance on experts is:

> "Unless an officer or director has knowledge that makes reliance unwarranted, an officer or

[4] See http://www.EnergyCollection.us/Energy-Security/Glossary-Key-Information.pdf

[5] See http://en.wikipedia.org/wiki/Duty_of_care

[6] See http://en.wikipedia.org/wiki/Business_Judgement_Rule

> director, in performing her duties to the organization, may rely on written or oral information, opinions, reports, or statements prepared or presented by: (i) officers or employees of the association whom the officer or director believes in good faith to be reliable and competent in the matters presented; (ii) legal counsel, public accountants, or other persons as to matters which the officer or director believes in good faith to be within the person's professional or expert competence; or (iii) in the case of reliance by directors, a committee of the board on which the director does not serve if the director believes in good faith that the committee merits confidence."[7]

Reliance on experts should be a key strategy when no cybersecurity expertise resides in the board itself, or to supplement cybersecurity expertise on the board. Given the evolving nature of cyber threats and related technologies, reliance on experts is inescapable.

Generally, reliance on experts is exercised by evaluation of the efficacy of the experts, and then execution of a Q&A phase when the experts make conclusions available to the board. At a very minimum, boards should have enough cyber knowledge to reasonably rely on experts, otherwise it is a matter of blind faith and unwarranted.

However, there is no need for all directors to be cyber-literate; a board committee designated for the purpose may be an appropriate solution to consider.

Where should board expertise, whatever its extent, be lodged? Here are four options.

The Audit Committee[8] This could be a possible home, but concerns with defocusing from the primary committee role may arise. Committee talent issues also may arise. Audit Committee advisors may include cybersecurity in their product/service offering, but a board should not assume this option without careful thought.

The Risk Management Committee. Another possible home. In any case, cybersecurity risk should be considered as an element of an Enterprise Risk Management (ERM) program.

The IT or Technology Committee. If the board has such a committee, it may be the logical place for executing the board's responsibilities with respect to cyber risk and to keep the full board informed and advised.[9] The committee would need to be sensitive to, and deal with, funding trade-off decisions between proposed business technology/IT projects and appropriate cyber expenditures.

Cybersecurity Committee. This is an obvious placement of responsibility, but

[7] See http://www.asaecenter.org/Resources/whitepaperdetail.cfm?ItemNumber=12217

[8] KPMG's 2014 Global Audit Committee Survey indicates that almost 45% of audit committees in the U.S. have primary oversight responsibility for cybersecurity risk, but only 25% say the quality of information they receive is good.

[9] MISO (www.misoenergy.org) has such a Committee and has assigned cyber responsibility to that Committee.

committee proliferation and drains on director’s time must be considered as well, before initiating another board committee.

Any Committee assignment should recognize that cybersecurity is a pervasive risk and cuts across all operations of the company and therefore all board committees.

Given the omnipresent nature of the cyber risk, it may make sense for appropriate board committees at least to have written into their charters consideration for the cyber risk that specifically applies to their own governance area (committee). To fulfill that obligation they may need assistance from the board committee having cyber responsibility assigned.

Another policy boards may want to consider is a periodic meeting of the entire board to hear cybersecurity reports from management and from the board committee on how it is executing its role. This meeting might also include outside experts.

II. Boards, Management, and Cybersecurity

Like all other issues, there needs to be an understanding of the board’s and management’s role in cybersecurity. Perhaps a useful analogy is the Sarbanes-Oxley implementation of recent history. SOX not only requires that the board attest to the validity of financials, but to have controls[10,11] in place to inform that attestation. Cybersecurity can be handled similarly. Someone must tell the board that all is well, but board members need to have insight into why that is so.

Each board deals with this subject in different ways, but it would be a best practice to have a discussion of the subject and a resulting understanding of the “rules” that will govern the interaction between management and the board with respect to cybersecurity.

Here is an example set; others may have adopted different policies depending on their own circumstances:

1. The board takes its responsibilities for cybersecurity seriously in combination with the CEO – “tone at the top” – to

[10] See the Council on Cybersecurity, whose technology practice area is built upon the Critical Security Controls, a recommended set of actions for cyber defense that provide specific and actionable ways to thwart the most pervasive attacks. The Controls have been developed and maintained by an international, grass-roots consortium which includes a broad range of companies, government agencies, institutions, and individuals from every part of the ecosystem (threat responders and analysts, security technologists, vulnerability-finders, tool builders, solution providers, front-line defenders, users, consultants, policy-makers, executives, academia, auditors, etc.) who have banded together to create, adopt, and support the Controls. http://www.counciloncybersecurity.org/critical-controls/

[11] See also NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations." It provides a catalog of security controls for all U.S. federal information systems except those related to national security. It is published by the National Institute of Standards and Technology, which is a non-regulatory agency of the U.S. Department of Commerce. NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act of 2002 (FISMA) and to help with managing cost effective programs to protect their information and information systems. http://en.wikipedia.org/wiki/NIST_Special_Publication_800-53

support appropriate cybersecurity protections.

2. Management is responsible for cybersecurity and will be fully responsible for achieving an appropriate cyber-secure state at all times.
3. No matter how management chooses to execute its responsibilities, the CEO is ultimately responsible. The board's main task is to hold the CEO accountable.
4. The XYZ committee of the board has lead responsibility for management oversight and duty of care execution related to cybersecurity, including advising the full board on such matters. The committee only acts in an advisory capacity to the full board and committees of the board.
5. The board should carefully consider the nexus of physical and cybersecurity threats, given that an attack from either of two significant threat actors, nation states and terrorists, would likely be a coordinated assault featuring both cyber and physical elements. Boards should consider whether these two responsibilities should be housed together in terms of responsibility. There are arguments on both sides. The two take somewhat different skill sets, but it is equally certain that the skills needed on the physical side are increasingly reliant on IT components and the cybersecurity of those components.
6. The board may elect to put certain "guiding principles" in place to guide management actions on cybersecurity. An example set might be:
   6.1. Management must assign total cyber responsibility to a single high-level manager with direct access to the CEO. This may be a CIO or CISO,[12] or another individual that would have CISO responsibilities in addition to other responsibilities. The board committee will have full access to this CISO for Q&A.
   6.2. Compliance must be accomplished within the context of being cyber-secure.
   6.3. Management will adopt a cybersecurity framework on which to base and align its cybersecurity program.
   6.4. Management will maintain a set of best practices with respect to cybersecurity and measure and report against these best practices. These best practices must additionally result in full compliance with legal requirements. Contradictions between compliance/legal obligations and best practices will be vetted as information to the responsible board committee.
   6.5. Where an employee observes non-compliance with a best practice, policy should require that it be reported to the CIO/CISO.
   6.6. Management will secure and periodically rotate an outside entity to perform a cyber-assessment of the company's cybersecurity condition, including penetration testing.[13] The assessment will be made available to the responsible

[12] CISO = Chief Information Security Officer

[13] See https://en.wikipedia.org/wiki/Penetration_test

board committee, and the assessor will be available for director Q&A.

6.7. All successful cyber intrusions will be timely reported to the responsible committee chair.

6.8. After adopting any best practice, all deviations from this best practice will be reported to the responsible board committee.

6.9. The board committee should consider budgetary responsibility. While typically the audit and finance committee of the board oversees and advises the board on the budget, it may make sense for the cyber-responsible committee to have a strong hand in approving the cybersecurity budget. In any case, the budget request of the CISO should be scrutinized by the responsible committee and not altered arbitrarily without discussion with the responsible committee and a firm understanding of the implications.

Of course, there are always temptations[14] to step over the line. Things like ordering "glue- shut all USB ports on finance organization machines" might be a good idea, but that should be management's call and not for the board to decide. Excessive board intervention into cyber-security shifts the burden of responsibility and lessens the probability of actually being cyber-secure.

That said, there are also legitimate reasons, related to duty of care, to step over an otherwise clear demarcation of management/board. Such a case might be repeated failure to maintain metrics, repeated breaches, repeated shortfalls in implementing best practices, unreasonable schedule slips, etc. Where the required results are not forthcoming, the board has a deeper responsibility to understand why, and to continue until it understands why and is satisfied with the resulting recovery plan.

Finally, the CEO has to play a role in cybersecurity even though it is customary to delegate this to a CIO or CISO. Because cybersecurity is everyone's business in a company, the CEO needs to:

1. Choose a CIO and CISO wisely and closely monitor performance.
2. Personally approve and support the company cybersecurity plan/policies and display visible support for the cybersecurity effort.
3. Increase her skills and knowledge about this cyber risk and mitigation.
4. Be an active part of the bridge between the board and management.
5. Ensure proper budget and expenditure prioritization.

Board members having cyber responsibility should also be familiar with current and pending legislation in the area of cybersecurity, including activities at the federal, state, and local level.[15]

[14] Subject matter passion, subject matter expertise, misunderstanding of roles, or showmanship.

[15] E.g. Executive Order 13636 issued by the President 2013-02-12 and the Presidential Policy Directive 21. See http://tinyurl.com/aglp8qh.

III. Key Elements of a Cybersecurity Program

There are a number of dimensions to consider as board members evaluate the adequacy of a company's cybersecurity program. Below are several key elements of a good cybersecurity program for which a board should see evidence:

Multi-layered, defense-in-depth approach. It's almost become cliché, but it is more important than ever for cyber defenses to be built upon multiple layers. This creates a barrier in which successful penetration requires the perpetrator to defeat defensive measures at successive layers.

Aligned with an industry framework. The National Institute of Standards and Technology (NIST) provides a framework[16] for improving cyber defenses that many companies find useful. Management may select an alternative framework or combine elements of various frameworks to guide efforts and measure progress, but there should be a defined framework.

Regular Vulnerability Assessment and Penetration Testing. Every organization should conduct vulnerability assessments and penetration testing on an ongoing basis. Management should determine the frequency of the testing in its cybersecurity program design. Assessment and testing results should be shared with the board.

Capability Maturity Model cybersecurity program assessment. Various critical infrastructure sectors[17] should adopt mechanisms[18] to help evaluate, prioritize and improve cybersecurity programs. The DOE model is used to evaluate the maturity and sophistication of the organization's cybersecurity risk management approach at a strategic and holistic level.

Participation in cyber information sharing groups. All sectors in the economy have realized that sharing of real-time information is a vital part of the protection regime. Various groups are emerging to help fill that need.

Recovery Plan. Most experts now agree that planning to repel or recover from a successful attack is of extreme importance. The recovery plan should envision the worst possible successful attack and spell out how the company would recover to normal operations.

IV. Risk Management and Cybersecurity

Risk Management is an old idea but one that maintains its profound relevance in decision-making. Much has been written on the subject and there are many well defined frameworks and materials to assist in applying this important principle.

The unofficial Internet Security Glossary defines risk management as: "The process of identifying, measuring, and controlling (i.e., mitigating) risks in information systems so as to reduce the risks to a level commensurate with the value of the assets protected."

[16] See http://www.nist.gov/cyberframework/

[17] See http://www.dhs.gov/critical-infrastructure-sectors

[18] The DOE Cybersecurity Capability Maturity Model can be found at http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program

Many are familiar with some form of the Risk Equation. Most board members have been on the receiving end of an explanation of how a nice graph of a company's risk analysis chart was developed. Most have also seen the famous Risk Management Equation:

Risk = [Threat] x [Probability of Threat] x [Impact if Successful]

Some will claim they actually use the equation; others believe that is notional and meant to guide further work. The goal of the equation, of course, is to try to quantify and understand risk exposure, and to inform decisions related to mitigating the risk. Expenditures on mitigation that are less than the risk exposure might at least make the prudent possibilities list.

In the cybersecurity world however, while not deterring its widespread use, the equation is of limited value beyond thinking about its ramifications. "Threat" is an occurrence of an attack that few if any have experienced and can come in many forms; some would fit under the heading of persistent, pervasive, military grade. The probability of such a threat is most likely very low, but unknowable. The "Impact if Successful" threat is so large as to be almost unthinkable. What remains is a very, very low probability times a very, very high negative impact; the multiplication of one by the other, coupled with confidence limits, would cover a very large dollar span indeed—so large as to be quite useless when comparing this to various cost levels of mitigation.

While the calculation of cyber risk using traditional methods is not very useful, as highlighted above, it is nonetheless critical that cybersecurity risk be tracked through the company's Enterprise Risk Management process. Cybersecurity should appear on every organization's ERM "heat map."

Traditional approaches to Risk Management fall short in the cybersecurity example but nonetheless expose a real issue: How do we know when we have done all that we should when there is not a quantitative approach that can adequately inform our decisions? One way to develop additional insight is for a board to understand the kinds of attacks and resulting damage that the company is exposed to, no matter how small the probability. A risk register might rank the probability of various attacks; management could then show how the company would be protected from each, and the level of resources needed. That would at least allow the company to understand tradeoffs being made, and risks not covered.

V. Questions a Director Should Ask

A board's responsibilities include "duty of care,"[19] which often is displayed, informed, and executed in the form of Q&A to management and subject matter experts. Below is a list of questions that a board or board committee might ask in the area of cybersecurity to help carry out its duty of care in the cyber area:

1. **Do we have the skills on the Board to properly execute our duty of care in the area of cybersecurity?**
2. **What is the entire set of Compliance obligations and laws we have to**

[19] See http://en.wikipedia.org/wiki/Duty_of_care

follow in the IT and Cybersecurity areas? Make sure state laws are considered as well as federal. Discuss legal liabilities.

3. **What is our cyber-risk tolerance? Are there parts of the overall system that need to be protected more than others?**
4. **Are the responsibilities for cybersecurity clearly spelled out, communicated, and being enacted across the entire organization?**

Look for centralization of overall responsibility, but company-wide participation.

Make clear the role of the internal auditor.

Carefully consider the reporting relationship of the CISO and CIO. It is often hotly debated whether the CISO should report directly to the CEO or to the CIO or perhaps somewhere else.[20]

5. **How are you thinking about cybersecurity vs. compliance?**

Hopefully, compliance requirements are being accomplished and true cybersecurity is the first line of defense.

No CIO or CISO should believe that compliance will make the company secure.

6. **How do we measure cyber risk and our activities to address it?**

Not an easy question to answer. The state of the art is evolving and initial tries will likely improve over time.

Once best practices for the company are established, number of deviations may be appropriate as one of the metrics.

7. **To which cybersecurity framework have we aligned our cybersecurity program?**

The NIST Cyber Security Framework, directed by Executive Order[21], might be an acceptable answer; many think it is a de facto standard.[22]

8. **What are our best practices, where did we get them, why did we select them, and how are we keeping them up to date?**

Not an easy question; there are many sources for best practices.

9. **What is our present status for implementing best practices and schedule going forward?**

When considering the various systems that we control – have you asked and answered the question: "What is the worst thing a person or group could do to a critical asset if they possessed the intent, access, and knowledge to perform a malicious act?

[20] This is one topic where the authors of this paper disagree with each other. Suffice it to say that there are passionate arguments on both side of the debate. A future paper will provide the advantages and disadvantages.

[21] See Presidents Executive Order directing NIST to develop a voluntary Framework - http://tinyurl.com/b7ag5fr

[22] See Patrick Miller comments at http://www.EnergyCollection.us/Companies/FERC/TC-2014-04-29/Anfield-Group-Patrick-Miller.pdf

This reference[23] is worth reading before engaging management in the cyber discussion.

10. When considering the various systems that we control – have you asked and answered the question: "What is the worst thing a person or group could do to a critical asset if they possessed the intent, access, and knowledge to perform a malicious act?

This reference[24] is worth reading before engaging management in the cyber discussion.

11. What is the most sophisticated adversary[25] we require our cyber defenses to repel with high assurance?

12. Given our present cybersecurity defenses, what attacks are still possible?

No company can protect itself 100%, so the board needs to know the possibilities for cyberattacks when considering allocation and approval of resources.

A difficult area relates to insider attacks (or mistakes) – many consider this the main threat. The board should understand this risk and mitigation measures.

13. Given our present cybersecurity defenses, what attacks are still possible? How are we incorporating the concepts of resilient systems[26] into our operations?

This is a complicated subject in its own right, but generally refers to our ability to "harden" our capabilities to survive, and/or partially function and quickly recover from a cyber-attack.

14. Do we have a Security Operations Center (SC[27])?

Many companies have found this to be a beneficial approach. "A security operations center (SOC) is a centralized unit in an organization that deals with security issues, on an organizational and technical level. A SOC within a building or facility is a central location from where staff supervises the site, using data processing technology. Typically, it is equipped for access monitoring, and controlling of lighting, alarms, and vehicle barriers."[28]

15. Do we have a Security Information and Event Management (SIEM[29]) System?

[23] Quoted from Industrial Control Systems Cyber Threat Research - http://www.EnergyCollection.us/Energy-Security/Industrial-Control-Systems.pdf The Question for Management is taken directly from the reference.

[24] Quoted from Industrial Control Systems Cyber Threat Research - http://www.EnergyCollection.us/Energy-Security/Industrial-Control-Systems.pdf The Question for Management is taken directly from the reference.

[25] See UglyGorilla Hack of US Utility Exposes Cyberwar threat - http://www.EnergyCollection.us/Energy-Security/UglyGorilla-Hack-US.pdf

[26] See Resilient Control Systems - http://en.wikipedia.org/wiki/Resilient_control_systems

[27] SOC is pronounced with a short "O".

[28] Quote from Wikipedia

[29] SIEM is pronounced with a long "I" and silent "E" as in SIM.

A SIEM[30] is a widely used and accepted Best Practice; it collects logs and event information into a centralized location, for analysis and event correlation.

16. Are we testing for Advanced Persistent Threats[31]?

APT activity is not detected by traditional security monitoring. Specialized firms (e.g. Mandiant) that have done government or military consulting have the expertise to identify fingerprints left by APT attempts or actual APT infestation.

17. Are we training our software developers to build security into their code?

This is becoming more critical since security was historically an afterthought or add-on for most software development.

18. How do we stand relative to others that have the same challenges as our company?

It is often common for like companies to form formal and/or informal groups to discuss Best Practices and results.

19. Do we have adequate budget, and how are we prioritizing?

20. How do our cybersecurity policies extend into the supply chain, and how are we protected from supply chain vulnerabilities?

Note: There have been cases of shrink wrapped USB memory sticks that were already infected.

We buy and use a lot of third party software – how do we ensure it is free of infection and backdoor[32] vulnerabilities.

Do we have the right procurement language built into our RFPs?[33]

21. What qualifications do our employees have in the cyber area to be able to identify and put in place best practices?

22. Do we have a training program for all employees?

Consider using social engineering[34] testing. Generally, the weakest entry point into our systems is through human resources. Awareness programs coupled with specific testing of social engineering approaches tends to improve the security profile.

CIOs report that it is very difficult to reduce employee's clicking links in test fraudulent emails to a level even below 10%.

23. Do we have a pre-defined, robust business resumption plan in the event of a successful cyber-attack?

[30] Security Information and Event Management - http://en.wikipedia.org/wiki/Siem

[31] Advanced Persistent Threat - http://en.wikipedia.org/wiki/Advanced_persistent_threat

[32] See http://en.wikipedia.org/wiki/Backdoor_(computing)

[33] See Cyber security procurement language for control systems from DOE at http://energy.gov/oe/downloads/cyber-security-procurement-language-control-systems-version-18

[34] See http://en.wikipedia.org/wiki/Social_engineering_(security)

24. Do we have cyber-insurance? Should we? Often the process of procuring cyber-insurance requires a company to undertake actions that have the effect of improving the effectiveness of their cybersecurity program.

25. How is our D&O Insurance connected to the question of being cyber-secure?

26. With what organizations (including government) are we working to lessen our chances of a successful attack?

27. What question haven't we asked that we should have asked?

Some of these questions might trigger additional questions when the cyber-responsible committee meets with the external organization[35] hired to assess the state of the company's cyber security posture. The committee also ought to ask: "Has anyone tried to influence the content of the report and is there any information being withheld?" It is also a good idea to ask the outside expert the open-ended trigger question: "What question haven't we asked that we should have asked?

As an additional reference, the National Association of Corporate Directors (NACD) has a report available[36] – "Cybersecurity: Boardroom Implications" – that provides a perspective based on interviewing board members, management, and cyber-experts. A useful part of the 16-page document is "Ten Questions Directors Can Ask Management Once a Breach Is Found."

VI. Traps to Avoid

It is almost impossible not to have findings or opportunities identified from an industry-specific cybersecurity compliance audit, a general cybersecurity audit, penetration test, or vulnerability assessment. It is important to understand each particular finding in context and to react accordingly. The management team needs to know that the board is focused on cybersecurity within its risk context, and not as an all-out effort to ensure compliance no matter what. The board must evaluate cyber-audits similarly to how it evaluates other audits, i.e., from a risk perspective.

"Gotcha" questions related to a drill-down on some specific cyber technology will rarely contribute to management/board relations or better company cybersecurity. Cybersecurity is a complicated and wide-ranging subject and the board needs to take a holistic top-down approach that can increase in sophistication over time.

Trust is not a substitute for duty. It may well be that the company has great cyber resources in terms of people and budget, but management claims to being cyber secure need to be tested by the board via direct Q&A with both management and outside experts that have done their own evaluation. Insisting on outside experts to look at the cyber posture of the company is not a lack of trust in management. Rather, it is a best practice in cybersecurity and should not be resisted by management.

[35] We recognize that not every board would consider it appropriate to meet with the organization hired to conduct a cyber-readiness and penetrating testing function. However, given the extreme reliance on others for advice related to "duty of care," a board may want to pursue this approach.

[36] See https://www.nacdonline.org/Resources/Article.cfm?ItemNumber=8486

VII. Technology and Other Things to Think About

Cybersecurity is not only complicated, but it is quickly evolving as vendors develop new products and services to counteract the ever increasing attack vectors. Some specific items a board might want to explore further are discussed below:

The Internet of Things*.* This is shorthand for everything having an internet address, reachable via the internet, and enabled via the internet. This trend is unavoidable, but presents new and changing cybersecurity challenges.

Digital Certificates and Keys. These are authentication and encryption software mechanisms to allow and protect access. Typically, companies have done a good job on person-based access, but machine-to-machine access has not had the same focus. Very few CIOs know how many digital certificates they have in use, or have a quality management system for these certificates or encryption keys.[37] Many of the high profile and more recent attacks– e.g., Stuxnet, Snowden, and the NSA attack, and others take advantage of this lack of focus. Many keys in use today have low key strengths and longer expiration limits than are what are written into NIST standards.

Joining a Cyber Group and Sharing Information. Many companies have joined groups of five to ten or more companies that cooperate in sharing cyber knowledge; what works and what doesn't, etc. This process is advantageous because it fits with the need to keep up to date and pursue best practices. Sharing actual attack information is a subject in flux. Everyone agrees that a system to share real-time attack data would be beneficial, but legal and practical problems persist. These are slowly being worked out and ultimately should be another source of progress.

Firewalls. Firewalls[38] are typically software solutions used to protect an area of higher security from an area of potentially lower security. As with all software solutions in the very dynamic world of cybersecurity, they require considerable maintenance in the form of configuration and updates. For high security systems, DHS ICS-CERT[39] recommends that companies explore data diodes—hardware based solutions that offer higher levels of protection. Data diodes can also handle applications that require data collection/processing/result-communication (two way applications) through the use of multiple diodes (i.e. in and out).[40]

Social Media. Social Media[41] encompasses a wide range of possibilities, but for threat-actors it represents a treasure-trove of information to assist in attack design. While many pages have been written on this subject, it might be instructive to consider LinkedIn.[42] Thousands of

[37] See 4 of 34 at http://www.slideshare.net/Prolifics/prolifics-ibm-cybersecurity

[38] Firewalls - http://en.wikipedia.org/wiki/Firewall_(computing)

[39] DHS Industrial Control Systems Cyber Emergency Response Team - https://ics-cert.us-cert.gov/ - referenced 2014-05-18

[40] The authors are writing a paper that will include a more complete discussion of this application in energy.

[41] Social Media - http://en.wikipedia.org/wiki/Social_media

[42] Some companies have issued policies to help reduce this exposure.

security professionals in the utility business have profiles in LinkedIn, many with over 500 connections each. These connections provide access to email addresses for all connections, and often personal email addresses. This information is ideal to construct “Watering Hole Attacks”[43] and other phishing attacks. All an attacker has to do is crack one password[44] to gain access to a lot of data – data that’s perfect to populate sophisticated phishing[45] attacks. Tricking people into providing important cyber information or leveraging social media to do so is called “Social Engineering.”[46] While we recognize LinkedIn as a valuable substantive and networking tool for business people~~,~~ it is critical that safe cyber practices be employed while using social media, including the use of unique and hard to crack passwords.[47]

VIII. Conclusion

Cybersecurity is an extremely complex and ever-evolving area—one that most boards recognize presents highly dangerous risks. These risks require board attention but the problems its poses and potential solutions to them have not, historically, been within the board’s DNA and competency. Generally, as areas of risk to a company come to be identified through an Enterprise Risk Management process, the company develops a gap analysis along with a remediation plan to manage those risks. For some ongoing risks the cycle of risk identification, gap analysis, and remediation is repeated on an annual cycle. While it is critical that cybersecurity risks be handled through the same process, because the needed expertise is often not found on the board, an elevated level of advisor reliance should be considered and, perhaps, more frequent reviews.

Given the fast-changing nature of cyber risk versus other tracked risk items, more frequent review may be warranted in any case. In addition, when recruiting new board members, boards should consider candidates with cybersecurity skills.

* * *

This paper has laid out a number of items for a board to consider in its oversight of a corporation’s cybersecurity program as the threat landscape continuously changes, along with the need and opportunity for mitigation and resiliency efforts. We hope readers with board responsibilities will find this discussion of cybersecurity responsibilities useful and avail themselves of the referehnces cited here. ■

[43] Watering Hole Attacks - http://en.wikipedia.org/wiki/Watering_Hole

[44] No Password is safe from the new breed of cracking software - http://tinyurl.com/n6qnpkd - referenced 2014-05-18

[45] Phishing – see http://en.wikipedia.org/wiki/Phishing

[46] Wikipedia - http://en.wikipedia.org/wiki/Social_engineering_%28security%29 See also: Social Engineering: The Basics - http://www.EnergyCollection.us/Energy-Security/Social-Engineering-Basics.pdf Original referenced 2014-06-01 - http://www.csoonline.com/article/2124681/security-awareness/social-engineering-the-basics.html

[47] A great technique for a hard to crack password is the use the first letter from each word of an easy to remember song lyric, famous quote, or phrase, add punctuation, and convert “to” to “2”, “for” to “4”, “ate” to “8”, etc.. For example: “For me to be safe shouldn’t I use complex passwords?” becomes “4m2bssIucpw?”