Practical Cyber Security Governance: A Guide for Hospital Boards and Executives

KEVINMAGEE

kevinmagee.com

Executive summary

Hospital Board members have long been responsible for protecting their organizations from complex risks associated with quality, patient safety, and evolving medical innovations.

Yet today, there is a troubling tendency to view cyber security as fundamentally different and separate from other risks facing organizations, and therefore best left to staff who have the experience and operational expertise to address it.

The reality is that cyber security can no longer be ignored or treated separately, as it can, and will, present ongoing and evolving risks that endanger both patient safety and financial stability within health care organizations.

The trouble is… most board members don't have the necessary depth of experience and expertise in cyber security that they may have in other relevant and traditional areas of governance. Financial skills, for example, are much more universal and easier to develop and improve upon due to the ubiquitous nature of the topic. There are an abundance of courses, books, magazines, newspapers etc. devoted to finance that are easily accessible and comprehensible for the layman…

But where does one begin to learn about malware, encryption, middleware, and public clouds – and at a level of understanding that pertains to the role of a governor rather than a computer scientist?

This short guide won't provide you with all the answers when it comes to cyber security, but what it will do is better prepare you to ask some of the right questions.

Contents

What's the worst that can happen?

Without warning, your organization is hit with a catastrophic ransomware attack. Most of the critical digital systems that your hospital needs in order to provide even the most basic levels of patient care are now offline.

Your CEO receives a ransom note via email demanding thousands of Bitcoins. If no payment is sent, the message warns that the attack will continue indefinitely and the hospital may never regain access to much or all of the compromised data, including sensitive patient records.

The Chair calls an emergency meeting of the Board.

Board Chair: "I have a motion on the floor that we instruct the CFO to transfer $3.4 million into a digital cryptocurrency called Bitcoin. This will facilitate a ransom payment to an unknown criminal or criminal organization that has seized control of our critical systems and completely crippled our ability to function. Furthermore, there is no guarantee that paying the ransom will allow us to reverse the damage."

Would anyone care to second this motion?

I certainly wouldn't.

What really did happen?

Think this situation is completely fictional and could never happen to your organization?

Consider that, in early 2016, Hollywood Presbyterian Medical Center in Los Angeles was hit with malware that shut down organization-wide access to email, digital patient records, and some Internet-connected medical devices for nearly two weeks. It's believed the hackers had originally demanded $3.4 million USD; the hospital eventually paid 40 Bitcoins (approximately $16,900 USD) to have its systems restored.

So while the opening situation above is actually fictional, it is in fact based on a true story and more importantly, it's not at all inconceivable that this very situation or something like it could also happen to your organization.

So what happens next?

Let's break down the components of what our fictional board of directors is up against:

1. A catastrophic breach has just occurred and the organization is completely crippled. Emotions are running high, bordering on panic, and no one has any context or experience that can be applied to comprehend the situation, let alone provide strategic guidance and sound governance. This is the worst possible state for making a critical decision, particularly without some sort of plan in place to help guide the process.

2. Is it even possible to transfer $3.4 million USD into Bitcoin? How exactly would we accomplish this? What are the risks associated with doing so? Does the organization have that kind of cash immediately available should it decide to pay the ransom? What effects will the loss of these funds and the decision to pay the ransom have on the organization long term? For example, diminished patient confidence, possible lawsuits, and unknown impacts on employee morale. And then there's the question: will it invite

copycats once we've demonstrated we're willing to pay?

3. Is it even legal to pay a ransom? Someone better get legal on the phone…

4. How can we even be certain that the people demanding the ransom are in fact the people directing the attack?

5. What would happen if the organization paid the ransom and the attackers either didn't fix the problem or, worse still, demanded more money?

How would our fictional Board, CEO, and CFO possibly untangle all of this and make good decisions under the glaring spotlight of intense media attention?

The answer is: they can't and they won't.

And a final thought… even if the motion were to pass, how exactly would the CEO and CFO actually go about implementing the directive from the Board?

From worst-case scenario to better cyber security governance

While there is no way whatsoever that any organization can prepare for every possible cyber risk scenario, the fact remains that cyber security risk can no longer be considered an operational matter or simply an "IT thing."

And the worst time for the board to start thinking about cyber security governance is certainly after an attack has already occurred.

What are the key responsibilities of the Board?

Just as in financial operations and other areas of enterprise risk management, when it comes to cyber security, the board of directors has "risk oversight" responsibility but does not actually operationally manage cyber security risk.

The board is, however, responsible for setting strategic priorities and then ensuring that management is implementing and reporting regularly on the implementation and effectiveness of processes, policies, controls and other key performance indicators, which would include notification of breaches or other material risks.

Directors owe a duty of care and must ensure that, should a privacy or security breach or some other cyber security related event occur, they have already taken in good faith all steps possible to protect the organization, including the following:

1. Has your board appropriately assessed all of its cyber security-related risks? What reasonable steps have you taken to evaluate those risks?

2. Have your board appropriately prioritized cyber security risks, from most critical to non-critical? Are these priorities properly aligned with corporate strategy, other business requirements, and a customized assessment of your organization's cyber vulnerabilities?

3. What actions is your board taking to mitigate cyber security risks? Do you have a regularly tested, resilience-inspired incident response plan with which to address cyber threats?

The five principles of responsibility

The National Association of Corporate Directors has nicely distilled these responsibilities down to five principles:

PRINCIPLE 1: Directors need to understand and approach cyber security as an enterprise-wide risk-management issue, not just an IT issue.

PRINCIPLE 2: Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

PRINCIPLE 3: Boards should have adequate access to cyber security expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.

PRINCIPLE 4: Directors should set the expectation that management will establish an enterprise-wide, cyber-risk management framework with adequate staffing and budget.

PRINCIPLE 5: Board discussion of cyber risk management should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

Complete details on these principles are available in the NACD Director's Handbook on Cyber-Risk Oversight.

What does good cyber security governance look like?

The boards of organizations that are successfully providing a high degree of structured oversight in regards to cyber security risk have a few things in common:

1. They have progressed from sporadic to no engagement on the topic (perhaps annually or when IT is looking to make new capital purchases) to receiving regular reports from management that include metrics and performance against key performance indicators.

2. In some cases, a committee of the board has direct responsibility for tracking cyber security risk, but in most cases, the entire board is engaged in cyber risk oversight.

3. They regularly engage outside experts for updates, training and benchmarking.

4. They educate themselves and research all possible relevant information related to the challenges and risks faced by the organization in order to demonstrate that in reaching a decision they have considered all reasonable alternatives.

5. They vigorously probe and challenge management with well-informed questions.

Questions Directors can ask to assess the Board's level of "cyber literacy"

1. As a board, are we demonstrating the appropriate level of due diligence, ownership, and effective management of cyber security risk that we owe to our organization as governors?

2. To what degree has our board discussed cyber security risk management and threats to our organization over the past year?

3. To what degree has our level of concern about cyber security risk increased/decreased over the past year?

4. Is our prioritization and level of engagement on the topic of cyber security consistent with our perceived level of overall risk to the organization?

5. Does our board need to play a more active role in determining our organization's cyber security strategy? If so, in what way?

6. What aspects of cyber security governance, strategy and risk management should be dealt with by the board, and what aspects should be delegated to committees of the board?

7. What metrics and other means of reporting do we require from management and how frequently are we reviewing this information? Is the degree of reporting and frequency aligned with our overall prioritization of cyber security risk management? To what degree do we feel the information provided is accurate and trustworthy?

8. Do we have sufficient cyber security expertise represented at the boardroom table? Is cyber security expertise adequately represented in our board member skills matrix requirements?

9. Do we understand and can we differentiate between our cyber security needs as an organization and our compliance requirements to external governing bodies?

10. Have any of our board members attended formal governance training specific to cyber security risk management? Should this be a requirement/option for some or all board members?

11. Have any of our board members attended formal personal digital security training? Should this be a requirement/option for some or all board members?

12. Are the methods we use to distribute sensitive and confidential materials to board members aligned with our organization's overall cyber security policies and procedures? Examples: risk associated with a board member's use of personal email accounts to receive confidential documents? Or encryption, storage and archiving of files and documents on personal devices?

13. Do we fully comprehend that board members are likely to be high-priority targets of cyber attackers and why?

Questions Directors can ask regarding the overall cyber security posture of the organization

14. Do we have a full and accurate understanding of the impact on our organization's reputation or very existence if key sensitive information held by the organization is accessed or stolen, or if critical systems are compromised?

15. In management's opinion, what is our overall cyber security maturity level as an organization? How do we compare to organizations similar in size and complexity in our industry?

16. How is accountability determined for managing cyber risks across our organization? Does this include management's accountability for business decisions that may introduce new cyber security risks?

17. What are the most critical cyber security risks to our organization as identified by management?

18. How many attacks does our organization experience each day/week/month and how many of these are successfully blocked?

19. Has the board been informed of any or all cyber attacks or breaches that have already occurred (successful or otherwise), how severe they were and the resulting impact to the organization?

20. What do we consider our most valuable and essential physical assets? How do our information technology systems interact with these assets? Examples: heating and cooling systems, manufacturing or medical equipment?

21. What do we consider our most valuable and essential digital assets? Examples: our network, databases, applications, email and other communication systems.

22. Do we have a digital asset inventory or "balance sheet" that catalogues and prioritizes the value, operational significance and interdependencies of all of our digital assets?

23. Are we investing appropriately in protecting our network, computing devices, Internet-connected devices and data relevant to their value and criticality to the operation of our organization? How do we evaluate and measure the results of our decisions?

24. Do we consider cyber security a part of our overall strategic and operational business decisions? Examples: procurement, supplier contracts, mergers and partnerships, third-party access to systems and insider risk?

25. Do we have the right people with the right skills and experience in place to implement, manage and operate our cyber security programs now and into the future? What, if any, are the gaps and what is management's plan to address them?

26. Do we have the right reporting structure in place to ensure there are no conflicts of interest that may be detrimental to the organization? For example, should the Chief Information Security Officer report to the Chief Information Officer, the Chief Financial Officer or the Chief Executive

Officer? What are the risks, challenges and benefits associated with our current reporting structure?

27. Is our organization adequately adhering to current cyber security related legislation and compliance requirements? Are we monitoring potential imminent legislation and preparing proactively for future requirements?

28. What is the liability exposure to our Directors related to cyber security risk?

29. Are we dependent on specific vendors for our overall cyber security posture? How confident are we that we have the right vendor partnerships in place to meet our needs? Do we know the technology road maps for our most strategic cyber security vendors and do they align with our projected future needs?

Questions Directors can ask related to cyber security insurance

30. Does our organization have adequate insurance that covers cyber incidents; do we know what exactly is covered and to what extent? Is our insurance coverage aligned with our overall cyber security risk management strategy and appetite for organizational risk?

31. Is our cyber security insurance provider responsible (or willing to be responsible) for incident management until a situation is resolved?

32. Has our cyber security insurer provided a list of approved vendors who will directly manage and resolve cyber incidents should they occur?

33. Have the vendors that we currently engage with or have contracted to resolve cyber incidents been approved by our insurer? Will our insurer pay for these services if they are ever required, and are there any approvals or documents required in advance?

Questions Directors can ask before a cyber attack or breach incident occurs

34. How will we know if we have been hacked or breached, and what makes us certain we are capable of identifying such an event should it occur?

35. What are our most critical vulnerabilities related to cyber security and how could they be exploited by either external or internal threats?

36. Which threat actors are most likely to attack our organization and for what purposes?

37. If a hacker wanted to do the most damage (financially, reputational, etc.) to our organization, how would they likely go about doing it?

38. How does our organization go about identifying, classifying and prioritizing cyber security risks, and how is our organization managing these risks?

39. How is our organization managing cyber security risk in relation to all other enterprise-wide risk? To what degree is cyber security risk integrated into an overall approach to risk management?

40. To what degree has our organization assessed insider threats, both intentional and unintentional?

41. When was the last time we conducted an independent external assessment of our cyber security defenses, policies and procedures?

42. When was the last time we conducted an active cyber security penetration test? What were the results? How was the information provided used to improve our organization's overall security posture?

43. Have our auditors identified any cyber security related deficiencies in regard to our organization's internal controls over financial reporting? If so, what are they and how are they being addressed?

44. Do we keep secure off-site backups of critical data? How current are these off-site backups?

Questions Directors can ask about cyber security risk management strategy

45. On what points do management and our information technology/security teams disagree about overall cyber security strategy, policies or posture?

46. What are the leading industry practices for cyber security risk management?

47. What frameworks or methodologies has our organization adopted to manage enterprise-wide risk and to what degree?

48. Have we implemented a systematic cyber security framework, such as the NIST Cybersecurity Framework?

49. Have we conducted a full cyber security risk assessment of our organization? How often is this process completed? Has the methodology, process and results of the assessment been reviewed and vetted by external experts and to what degree? What steps have been taken by management to improve our overall cyber security posture as a result of the most recent risk-assessment process?

50. Do we have an enterprise-wide, independently budgeted cyber security risk management team? Is the budget adequate to meet the objectives set by management and the board? How is it integrated within our organization's overall enterprise risk-management process?

51. Do we have appropriate risk management strategies in place for both general organization-wide cyber security, as well as more advanced strategies for protecting our most critical physical and digital assets? What are these strategies and how do they differ?

52. Do our organization's outsourced providers, contractors and other third-party providers have adequate cyber security controls and policies in place? How are these controls monitored? Do their policies align with our organization's expectations and to what degree are any deficiencies putting us at risk?

53. Do we have an ongoing, organization-wide security awareness training program? How is this implemented and

by whom? How effective is the program and how is this measured? How are we ensuring that the training is current and relevant to employees and our organization's current and future needs?

Questions Directors can ask about insider threats related to cyber security

54. What are the industry-leading practices for managing insider threats? To what degree have we adopted these practices and, in management's opinion, how effective are they? What are the gaps, if any, and what is management doing to address them?

55. How do key functions (Information Technology, Human Resources, Legal, and Compliance) work together to create a culture of cyber security awareness and personal responsibility for cyber security?

56. Does the organization have written policies that cover appropriate employee use and access to data, applications and devices? How effective are these policies and what is our current overall level of compliance? How are employees informed and trained regarding the details of these policies? How are these policies enforced?

57. Do we encourage a safe environment for employees to report cyber security incidents, even if they are self-reporting accidental or unintentional incidents?

58. Do we conduct regular training for our employees on how to implement our organization's cyber security policies, as well as how to recognize, identify and report potential threats and vulnerabilities to management?

59. Have we adapted and updated our Human Resources policies, such as background checks, new-employee orientation, training, employee exit interviews, etc., to incorporate our cyber security programs and policies?

60. How do our information technology operational controls, including individual access restrictions, encryption, data backups, monitoring and inspection of network traffic, etc., help to protect against insider threats?

61. Do we have an insider-incident activity plan that spells out how and when to contact our legal department, law enforcement and/or other authorities, and whether to explore legal remedies?

62. Do we have a policy on how to deal with situations related to extortion and cybercriminal activity, such as Ransomware, that have a material impact on our ability to continue the regular operations of the organization? Has this policy or topic been reviewed or investigated by our legal department and are our policies fully compliant with all laws and legislation to which we are subject?

63. Do we have in place an acceptable-use policy that details what employees may and may not do with the work-related devices they use, including such aspects as acceptable use of the Internet and web browsing, email and the installation of non-approved software and applications?

64. Do we have policies in place related to remote work and travel that detail where

and how employees should use work-related devices, and how employees should connect to our organization's network? Examples: use of unsecured public WiFi, use of a VPN to connect from any remote location, permission to take devices home and to travel outside of the country where laws regarding communication protocols and encryption may differ from the jurisdiction of their regular workplace.

65. Do we have policies in place related to employee use of personal devices for work-related activities, commonly known as Bring Your Own Device (BYOD)? How does employee use of personal devices impact our organization's overall cyber security posture?

66. Do we have policies in place related to the management and acceptable use of social media accounts operated on behalf of the organization?

Questions Directors can ask about incident-response preparedness

67. What do we, as an organization, believe constitutes a "material cyber security incident or breach"?

68. Does our organization have a cyber security incident response plan? What was the process involved in developing this plan? What cross-organizational departments and stakeholders assisted in the development of the plan?

69. What actions, events or circumstances will result in activation of our incident-response plan?

70. To what degree can we rapidly contain damages and mobilize response resources when a cyber incident occurs? How are we certain of this and what are we doing to continuously improve our ability to respond?

71. To what degree has our plan been vetted by external experts, tested and exercised? How often does this occur?

72. For significant cyber attacks or breaches, what is our public relations and communications plan?

73. Under what circumstances will law enforcement or other government agencies be notified of a cyber attack or breach?

74. How does our incident response team work with the organization's broader enterprise risk function?

75. How is our cyber security incident response plan integrated with other plans related to disaster recovery and business continuity?

76. Do we encourage our technical staff to enter into information-sharing exchanges and educational activities with other organizations in our industry in order to benchmark, learn from others and help identify emerging threats?

Questions Directors can ask about contracting third-party assistance

77. Should a cyber incident occur, in addition to external legal counsel, do we have relationships established with independent security experts and

forensic investigators, crisis communications advisors and law enforcement? Who is responsible for establishing and maintaining these relationships?

78. What non-disclosure or other legal agreements do we have (or need to have) in place in order to immediately leverage third-party assistance should a cyber incident occur?

79. Do we have protocols and policies in place related to when and how to engage third-party assistance as part of our overall incident response plan?

Questions Directors can ask regarding supply-chain threats

80. Do our vendor agreements create new legal risks or additional compliance requirements related to cyber security?

81. How do we balance the financial opportunities (lower costs, improvements to efficiency, etc.) created by greater supply chain flexibility with potentially higher cyber risks?

82. How much visibility do we currently have across our supply chain regarding cyber security risk exposure? What controls, if any, do we have in place to monitor and mitigate these risks?

83. How is compliance with our organization's cyber security policies and requirements built into contracts and service-level agreements with our suppliers? How are they enforced?

84. Do employees of our suppliers have direct access to any of our systems? How is their access monitored and controlled? Examples: remote updates to information technology equipment, access to HVAC systems for maintenance monitoring, and direct access to our ERP or procurement systems.

85. What do we require of our supply chain and other third parties regarding notification of data breaches to their systems or other related cyber incidents that could have a material impact on our organization?

86. Are we indemnified against cyber security incidents on the part of our suppliers/vendors?

87. Do we indemnify our suppliers/vendors against cyber security incidents?

88. What are our supplier's responsibilities during a cyber attack? How are these responsibilities outlined in our incident response plans? Have these responsibilities been adequately communicated and acknowledged by our supply chain partners?

Questions Directors can ask after a cyber security incident has occurred

89. How did we learn that the cyber incident occurred? Were we notified by an outside law enforcement agency, or was the incident discovered internally?

90. Who is aware of the incident? What are their names and their organizational or legal affiliations?

91. Have we activated our incident-response plan? Is it working as planned?

92. Who is designated as the primary incident response coordinator?

93. What is the schedule of regular progress updates to the board? Who is responsible for these updates and by what means will they be communicated?

94. Who is authorized to make decisions regarding the affected operations?

95. What impact did the cyber incident have on our ability to maintain normal business operations?

96. Has the cyber incident been contained? How are we certain this is the case?

97. What, if anything, are our strategic cyber security vendors doing to assist us in containing the cyber incident? Are they meeting their contractual obligations to our organization?

98. What systems or data have been affected and to what degree? Are we certain that we are aware of all systems and data that have been compromised? How are we certain this is the case?

99. What information has been accessed or stolen, and what is the sensitivity of that data? Is any of the data classified as regulated data? Examples: credit card data, personal health information, etc.

100. What notifications regarding this incident need to or have already been made? Examples: law enforcement, regulatory agencies, media, etc.

101. What vulnerabilities in our systems or policies were exploited that allowed the incident to occur?

102. What steps are management taking to make sure this type of cyber security incident does not happen again?

103. What can we do to mitigate any losses caused by the incident?

104. Will there be any possible or expected litigation against our organization as a result of the cyber incident? Is our legal team actively investigating/preparing for these possibilities?

105. What overall damage has been done to the reputation of our organization? Examples: consumer confidence, employee moral, media exposure, etc. What are the long-term implications of this damage and what can be done to mitigate or repair the damage?

Helpful Cyber Security Governance Resources

eBooks

- Director's Handbook on Cyber-Risk Oversight (NACD)
- Governance Series – Navigating the Digital Age (NYSE/Palo Alto Networks)
- Information Security Governance: Guidance for Boards of Directors and Executive Management 2nd Edition (IT Governance Institute)

White Papers

- Connecting the dots: A proactive approach to cybersecurity oversight in the boardroom (KPMG)
- Partnering for Cyber Resilience Towards the Quantification of Cyber Threats (World Economic Forum)
- Guide to INFORMATION SECURITY FOR THE HEALTH CARE SECTOR (eHealth Ontario)
- Cybersecurity: What the Board of Directors Needs to Ask (ISACA)
- Cybercrime and Other Threats Faced by the Healthcare Industry (TrendMicro)
- 2017 Scalar Security Study – The Cyber Security Readiness of Canadian Organizations
- Governance of Cybersecurity: 2015 Report (Georgia Institute of Technology)
- THE ACCOUNTABILITY GAP: CYBERSECURITY & BUILDING A CULTURE OF RESPONSIBILITY (Nasdaq/Tanium)
- Cybercrime: an overview of incidents and issues in Canada (RCMP)
- The Global Risks Report 2017 – 12th Edition (World Economic Forum)
- Health Warning: Cyberattacks are targeting the health care industry (Intel Security)
- 2016 Internet Organised Crime Threat Assessment (Europol)
- 2016 Cost of Data Breach Study: Canada (Ponemon)

Cyber Security Governance Websites

- NIST Cybersecurity Framework
- HITRUST Alliance
- HIMSS Cyber Security HUB

Relevant Canadian Websites

- Public Safety Canada
- Public Safety Canada – Report a Cyber Security Incident
- CRTC Spam Reporting Centre
- Canadian Anti-Fraud Centre
- Canadian Cyber Incident Response Centre
- Office of the Privacy Commissioner of Canada
- Information and Privacy Commissioner of Ontario

Cyber Security and Privacy Legislation

- Overview of privacy legislation in Canada
- Canadian Law - Digital Privacy Act
- Canadian Law - Personal Information Protection and Electronic Documents Act
- Ontario Law - Personal Health Information Protection Act

About the author

Kevin Magee is a member of the Board of Directors of the Brant Community Healthcare System as well as a senior sales executive and cyber-security professional.

Currently, he leads the Ontario sales and engineering teams of Gigamon Canada, a Security Delivery Platform company headquartered in Santa Clara California.

Kevin has held previous positions leading the Public Sector vertical team at Palo Alto Networks and Healthcare teams at Oracle Canada and Hewlett Packard Canada.

Before changing careers to join the ranks of major corporations, Kevin held CTO and Vice President level positions with several technology startups focusing on healthcare and security solutions.

A very active and enthusiastic participant in the Canadian startup community, he has severed as a Mentor and Entrepreneur in Residence at Laurier University's Launch Pad program, as an Advisor in the Life Sciences and Healthcare practice at MaRS, as an advisor to Hacking Health Canada, as well as guest lecturing and advising on curriculum development for cyber security, cybercrime and security awareness programs for several Canadian colleges, universities and industry associations.

He writes, teaches and speaks extensively about cyber security governance, security awareness, cybercrime, healthcare and entrepreneurship and blogs regularly about these topics at kevinmagee.com

kevinmagee.com