WHITE PAPER

CYBERSECURITY AND THE BOARD OF DIRECTORS
TIPS FOR SECURING SUPPORT FOR YOUR CYBER RISK MANAGEMENT PROGRAM

NICK SON | VICE PRESIDENT, CYBER RISK & PUBLIC SECTOR

CHRISTOPHER LIETZ | PRINCIPAL, CYBER RISK ADVISORY

COALFIRE™
North America | Latin America | Europe
877.224.8077 | info@coalfire.com | coalfire.com
# TABLE OF CONTENTS

Overview ....................................................................................................................................3  
Why do boards care about cybersecurity? .............................................................................3  
What does the board need to know? .......................................................................................5  
  - What do we need to protect? ..............................................................................................5  
  - Could a breach or incident happen to us? ..........................................................................5  
  - Can we recover when an incident happens? .......................................................................6  
  - Are we making appropriate investments in cybersecurity? ................................................6  
  - How does our cybersecurity program compare to our peers’? .......................................7  
How can security leaders win board support? .................................................................9  
Conclusion ..............................................................................................................................11
OVERVIEW

Cyber risk is more than a technology issue; it carries enterprise-wide legal, operational, and financial implications that endanger virtually all organizations. For some well-known companies, those risks are no longer theoretical, and they struggle to repair the damage done to their operations, reputation, and profits – a process that often takes years.

Boards of directors have a fiduciary responsibility to understand and manage cyber risk. In fulfilling those duties, they will ask pointed questions of those responsible for managing cyber risk. In this white paper, Coalfire will identify the questions you need to be prepared to answer, as well as key ways to garner board support for your cyber risk program.

WHY DO BOARDS CARE ABOUT CYBERSECURITY?

Tasked with securing the future of the organization, the board of directors is responsible for directing the company’s strategy, overseeing management, and protecting shareholder investments. The board is well-versed in managing financial, operational, and market risks, but has not traditionally considered cyber risk.

The ever-present threat of a cyber attack and new penalties for data breaches (see sidebar) have put cybersecurity on the board’s radar. The National Association of Corporate Directors (NACD) now includes cyber risk oversight as one of its top five areas of emphasis for boards, further highlighting its increasing importance. Cyber risk is no longer a technology problem; it’s a business issue and one that could impact the entire enterprise.

Directors are not confident that their companies could effectively thwart a cyber attack. According to a survey by the New York Stock Exchange, 66% of directors do not believe that their companies are properly protected. Perhaps due to those concerns, 80% of directors report that cybersecurity topics are discussed at nearly every meeting.

---

To manage the risk associated with a cyber attack, leadership must bring together key components of an organization to develop joint ownership of risks and a comprehensive approach to cybersecurity. Having a policy isn’t enough. Companies also need tools, processes, and up-to-date information on the ever-changing threats to their enterprises.

Figure 2: Biggest fear regarding cyber attacks according to a survey by NYSE Governance Services

<table>
<thead>
<tr>
<th>Fear</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brand damage due to customer loss</td>
<td>42%</td>
</tr>
<tr>
<td>Cost of responding to a lawsuit</td>
<td>27%</td>
</tr>
<tr>
<td>Loss of competitive advantage due to corporate espionage</td>
<td>19%</td>
</tr>
<tr>
<td>Regulatory and compliance violations</td>
<td>12%</td>
</tr>
<tr>
<td>Other</td>
<td>0%</td>
</tr>
</tbody>
</table>


5 Ibid.
WHAT DOES THE BOARD NEED TO KNOW?

Directors are responsible for business strategy and resource allocation, and they need information to guide their decisions. They aren’t looking for long explanations filled with technical jargon; they need high-level strategic information from which they can make decisions.

Before you appear in front of a board, be sure you can address these five important questions.

1. WHAT DO WE NEED TO PROTECT?

Before a cybersecurity program can be developed, an organization must determine the assets that are most important to the business and the risks associated with them. Assets should be prioritized based on their relative value to the business.

Tips for answering:

- Avoid having a highly granular list. Classify, summarize, and prioritize the most valuable assets and build your cybersecurity program around them.
- Remember to focus on business assets. Think past physical servers to the underlying data and business processes that create, manipulate, and use it.

Examples of corporate assets

- Trade secrets
- Intellectual property
- Databases
- Networks
- Applications
- Business processes
- Financial assets
- Facilities
- Confidential communications

2. COULD A BREACH OR INCIDENT HAPPEN TO US?

Directors are well-read. They will likely be familiar with data breaches and security incidents that have been in the news, and they will want to know if the same risks threaten their organization.

Tips for answering:

- Demonstrate confidence by being proactive. Analyze situations and factor them into the risk scenarios you are managing.
- Acknowledge that being 100% secure is neither feasible nor affordable. Work with the board and business partners to analyze threats and develop appropriate risk response.

What could the company be susceptible to?

- Fraud and theft
- Loss of sensitive information
- Third-party security lapses
- Disruption
- Harm to reputation
- Fines and penalties
**3. CAN WE RECOVER WHEN AN INCIDENT HAPPENS?**

Most directors believe that cyber incidents are inevitable; it’s simply a matter of when. Be prepared to answer how you will respond to an incident and what recovery will look like.

Tips for answering:

- Confirm expectations regarding risk scenarios, acceptable losses, recovery time, and recovery point.
- Demonstrate that you have a plan, know what resources will be required, and that you have practiced the plan.

![Incident response lifecycle](image)

**4. ARE WE MAKING APPROPRIATE INVESTMENTS IN CYBERSECURITY?**

The board is accountable for the organization’s investment strategy. In years past, information security spending was part of a larger IT-related budget. Not anymore. Gartner estimates that by 2020, IT security spending will grow from $75 billion to $170 billion. With such levels of spending, boards will be more apt to scrutinize investments and actively manage budgets.

Tips for answering:

- Provide information about trends and return on investment.
- Demonstrate with data how the money entrusted to you compares to your peers.

---


Figure 3: Median budget and percentage allocated to security by year by industry

<table>
<thead>
<tr>
<th>IT BUDGET</th>
<th>FY 2014</th>
<th>FY 2015</th>
<th>Projected FY 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial services</strong></td>
<td>$1 million</td>
<td>$500,000 - $1 million</td>
<td>$500,000 - $1 million</td>
</tr>
<tr>
<td><strong>Technology/IT services</strong></td>
<td>$100,000</td>
<td>$100,000 - $500,000</td>
<td>$100,000 - $500,000</td>
</tr>
<tr>
<td><strong>Government</strong></td>
<td>$500,000 - $1 million</td>
<td>$500,000 - $1 million</td>
<td>$1 million - $10 million</td>
</tr>
<tr>
<td><strong>Education</strong></td>
<td>$1 million - $10 million</td>
<td>$1 million - $10 million</td>
<td>$1 million - $10 million</td>
</tr>
<tr>
<td><strong>Healthcare</strong></td>
<td>$1 million - $10 million</td>
<td>$1 million - $10 million</td>
<td>$1 million - $10 million</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PERCENTAGE OF BUDGET ALLOCATED TO SECURITY</th>
<th>FY 2014</th>
<th>FY 2015</th>
<th>Projected FY 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial services</strong></td>
<td>7% - 9%</td>
<td>7% - 9%</td>
<td>10% - 12%</td>
</tr>
<tr>
<td><strong>Technology/IT services</strong></td>
<td>1% - 3%</td>
<td>4% - 6%</td>
<td>4% - 6%</td>
</tr>
<tr>
<td><strong>Government</strong></td>
<td>4% - 6%</td>
<td>4% - 6%</td>
<td>7% - 9%</td>
</tr>
<tr>
<td><strong>Education</strong></td>
<td>1% - 3%</td>
<td>3% - 4%</td>
<td>1% - 3%</td>
</tr>
<tr>
<td><strong>Healthcare</strong></td>
<td>4% - 6%</td>
<td>4% - 6%</td>
<td>4% - 6%</td>
</tr>
</tbody>
</table>

**HOW DOES OUR CYBERSECURITY PROGRAM COMPARE TO OUR PEERS’?**

Benchmarking cybersecurity programs is notoriously difficult. The sensitive nature of the topic leaves many companies reluctant to disclose information. Plus, each organization has a unique asset profile and risk appetite.

However, some level of comparison is possible. Find information on best practices and approaches through trade associations and information sharing groups. Additionally, consider engaging a cybersecurity expert that has experience in your industry and others.

---

Tips for answering:

- Establish goals that are appropriate for your organization and are based on existing frameworks.
- Create your own benchmarks by engaging experts and controls maturity models.
HOW CAN SECURITY LEADERS WIN BOARD SUPPORT?

As a security leader, you need to secure guidance, funding, and ongoing support from your board of directors. To help you earn and sustain that support, consider the following recommendations:

1. **Partner with trusted advisors.**
   The board already has several trusted advisors, and those leaders are your natural allies in cyber risk discussions.
   - Operations executives: Are likely to be the “risk owners” and count on you to help them manage risk.
   - Legal counsel (in-house and/or external): Serve on the board as primary advisors on regulatory and liability matters.
   - Chief audit executive (CAE) and internal auditors: Advise the audit committee and support good governance through audits.
   - CIO and CTO: Select, deploy, and manage the technologies that support the business strategy and need your help to make risk-appropriate decisions.

2. **Have a business conversation.**
   While there are technical elements to a cyber risk discussion, the main focus should be on business and risk. Boards understand risk, controls, roadmaps, and metrics. They don’t want to waste time on jargon-heavy, technical discussions or in-depth descriptions of vulnerabilities. Be prepared to identify roadmaps that will manage risk and create accountability.

3. **Educate.**
   Keeping the board up-to-date on security issues is important. Not only does it help you justify investments and processes, but it can also reduce pushback and questions. Credible resources are available from a variety of sources, including US-CERT and other government entities, research organizations, industry associations, analysts, and vendors. Remember, all information should be translated so it relates to your business and relevant risk management framework.

4. **Focus on risk.**
   Risk is a function of threats, vulnerabilities, exposure, and impact, and it’s typically measured in terms of money. Without a risk context, effective decisions concerning security cannot be made. Furthermore, framing the discussion around risks to the business helps the board establish priorities.

5. **Use proven frameworks.**
   Cybersecurity is not something you can manage exclusively with homegrown constructs and in-house talent. Thankfully, there are a number of proven frameworks and industry associations that can provide guidance and best practices. Choose from a number of different frameworks – all of which help you establish common language, a mechanism for dealing with complexity, and comparison to commonly accepted best practices.
6. **Clarify the difference between compliance and security.**

The board probably knows that compliance does not equal security; however, this fact is worth repeating. Compliance is one of the security risks you have to manage, and the risks associated with noncompliance vary dramatically across industries and situations. Don’t spend all your time and budget on compliance-driven requirements; look at the bigger picture and plan accordingly.

7. **Measure controls using a maturity model.**

After establishing a risk context and framework, the focus should turn to controls. Through a maturity assessment, you can determine the cyber risk program’s current state and identify the proposed future state. This process provides the foundation for an honest discussion with the board and other company leaders. From there, you can set realistic, mutually agreeable goals.

---

Coalfire’s Cyber Risk Program Maturity Assessment provides a high-level evaluation of key elements of your organization’s risk management program. Our experts assess your security posture, compare your environment to similar organizations, and provide a prioritized roadmap.

**For more information, visit:**


---

8. **Measure. Measure. Measure.**

Metrics provide insight that fuels discussion, shows progress, and fosters improvement. When choosing metrics to show the board, choose things that reflect what matters to them. For example:

- Key performance indicators – Use these to demonstrate progress and goal achievement.
- Key risk indicators – Use these to identify trends and warnings.

9. **Perform penetration tests.**

Penetration tests are a required element of most compliance programs, and they can be used to educate your executive team. They simulate real-world adversaries with malicious intent and even insider knowledge. Using results of these tests – as long as they relate to real-world risk – can help educate directors on possible problems and justify funding.

10. **Establish a security governance process.**

A governance program helps ensure a level of shared accountability, executive buy-in, and stakeholder involvement. By establishing a multilevel security program, responsibility is shared across management, which optimizes security resources and increases the effectiveness of the security policy.
CONCLUSION

Boards play an important role in the fight against cybercrime. As a security leader, you have a responsibility to help educate directors and gain their support for cybersecurity initiatives. Be prepared to answer their questions concerning the assets that must be protected, the possibilities of a breach, current investments in cybersecurity, recovery plans, and industry benchmarks. All of these conversations should be framed in business terms, not in technology and jargon-heavy details.

As a leading IT security advisor, Coalfire can help. We deliver the expert advice, assessments, and testing to support board-level discussions and cyber risk program development and implementation.

Learn more at Coalfire.com.

ABOUT THE AUTHORS

Nick Son | Vice President, Cyber Risk & Public Sector
Mr. Son leads Coalfire’s FISMA and FedRAMP solutions business, serving U.S. federal, state, local, and commercial clients. Along with maintaining several security-related certifications (CISSP, CISA, CISM, CPA, and CIA), he has more than 20 years of experience in information assurance and cybersecurity program management and legislative compliance. He is a subject matter expert in the area of FISMA, FedRAMP, and third-party reporting.

Christopher Lietz | Principal, Cyber Risk Advisory
Mr. Lietz joined Coalfire in 2009, and has more than 25 years of business consulting, technology, and security experience. He has served clients in the insurance, retail, consumer products, healthcare, transportation, manufacturing, and technology services industries, and is a skilled communicator, strategist, and operations executive. In addition to a B.S. degree in engineering and an MBA in finance and marketing, he maintains multiple security-related certifications (CISSP, CGEIT, CRISC, CISA, CISM, and CTPRP).

ABOUT COALFIRE

As a trusted advisor and leader in cybersecurity, Coalfire has more than 15 years in IT security services. We empower organizations to reduce risk and simplify compliance, while minimizing business disruptions. Our professionals are renowned for their technical expertise and unbiased assessments and advice. We recommend solutions to meet each client’s specific challenges and build long-term strategies that can help them identify, prevent, respond, and recover from security breaches and data theft. Coalfire has offices throughout the United States and Europe. www.coalfire.com