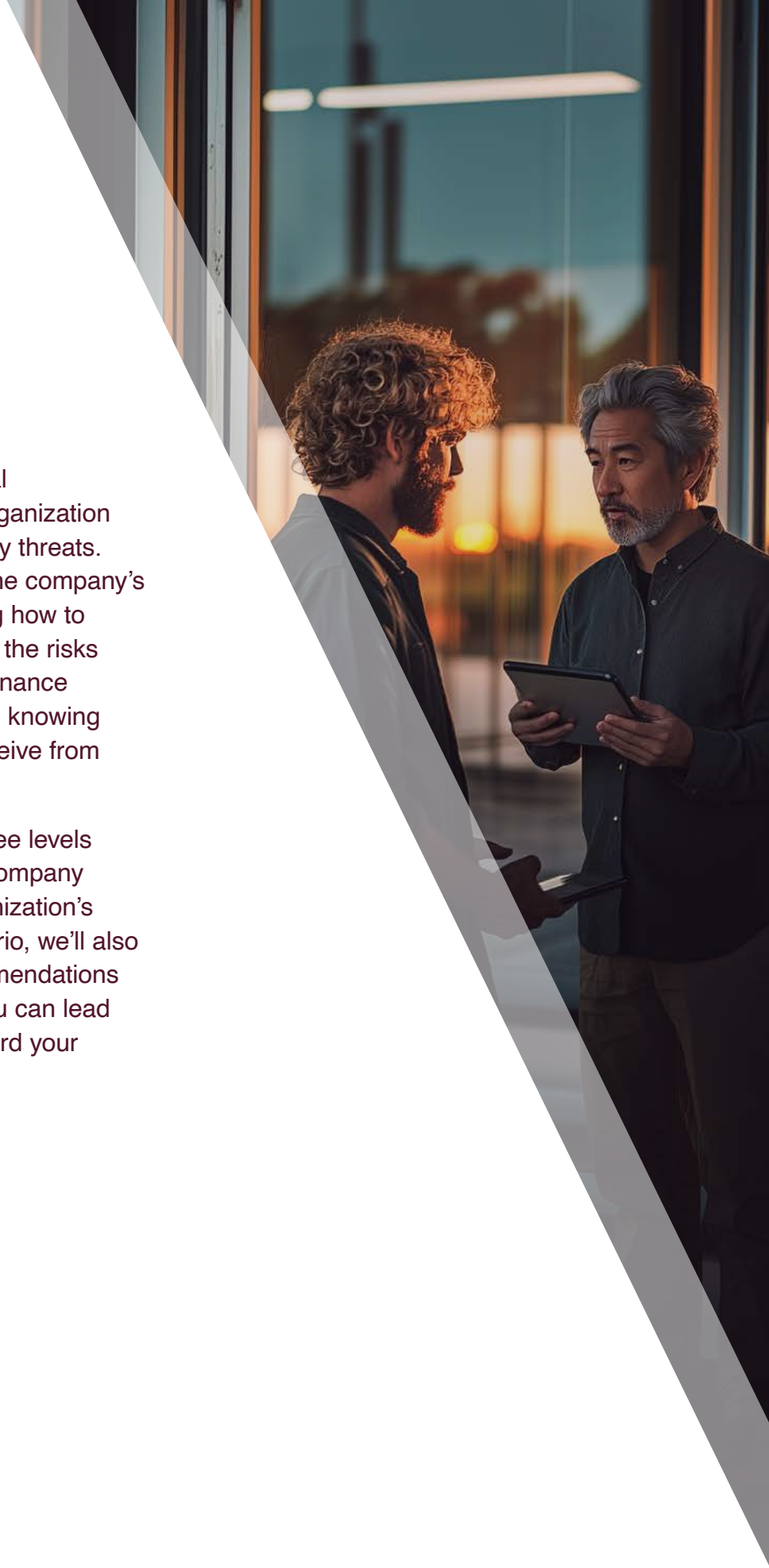
F12.net

BOARD MEMBER INSIGHTS

How to Respond/ Govern Based on Your Company's Cybersecurity Posture



As a board member, one of your critical responsibilities is ensuring that your organization is protected from evolving cybersecurity threats. This requires not only understanding the company's cybersecurity posture but also knowing how to govern and guide leadership based on the risks you face. Effective cybersecurity governance involves asking the right questions and knowing how to interpret the responses you receive from management.

In this guide, we'll walk through the three levels of responses you might receive from company leadership when discussing your organization's cybersecurity posture. For each scenario, we'll also provide actionable governance recommendations to ensure that, as a board member, you can lead confidently, mitigate risks, and safeguard your organization's future.

1 **What are the most critical cybersecurity risks we face**, and how does leadership ensure these risks are being addressed at all levels of the organization?

- **Best-Case Response (Best-in-Class)**: Leadership provides a comprehensive risk assessment outlining the specific cyber threats the company faces, including emerging AI threats. They have a proactive cybersecurity program integrated into the overall risk management process, with regular updates at all levels of the organization.
  - **Actionable Recommendation**:
    1. Continue to support leadership's cybersecurity investment.
    2. Schedule **annual board reviews** of the evolving risk landscape.
    3. Encourage **continued education** for the board on cybersecurity developments.
- **Middle-Case Response (Needs Improvement)**: Leadership acknowledges some risks but has only **partial coverage** (e.g., they've addressed common threats like phishing but haven't fully considered AI-driven attacks). They plan to improve policies and update security systems, but gaps exist.
  - **Actionable Recommendation**:
    1. Mandate a third-party cybersecurity audit.
    2. Set specific deadlines for leadership to address gaps and report progress.
    3. Allocate budget for upgrading tools and for training staff.
- **Worst-Case Response (Nightmare)**: Leadership seems unaware of current threats or dismisses them, saying cybersecurity is IT's responsibility without a clear understanding of the risks. No formal risk assessments have been done.
  - **Actionable Recommendation**:
    1. Insist on an **immediate audit** by a specialized cybersecurity firm.
    2. Convene an **emergency meeting** with the CISO (or hire a virtual one if needed).
    3. Develop a **cybersecurity action plan** with strict timelines for implementation and regular board updates.

2 How frequently are we conducting risk assessments, and are these assessments including emerging AI-driven threats?

Best-Case Response: Leadership explains that **risk assessments are conducted quarterly** and AI-driven threats are actively being monitored and mitigated. A dedicated team continuously evaluates emerging threats.

- **Actionable Recommendation**:
  1. Ensure the board receives **quarterly cybersecurity reports**.
  2. Advocate for **ongoing AI-driven threat scenario planning**.
  3. Encourage participation in **industry threat intelligence networks**.

Middle-Case Response: Risk assessments are conducted annually, and while AI is on their radar, they've only recently begun exploring AI-related threats. The assessments cover the basics but need to go deeper into emerging risks.

- **Actionable Recommendation**:
  4. Push for **more frequent assessments**—at least semi-annual.
  5. Mandate **AI-focused cybersecurity training** for key personnel.
  6. Support **investment in AI detection tools** to proactively address threats.

Worst-Case Response: Leadership admits that no formal risk assessments have been conducted recently, and they have little understanding of AI-driven threats. They assume **existing firewalls and antivirus software** are sufficient.

- **Actionable Recommendation**:
  7. Require an **immediate risk assessment** by external experts.
  8. Build a **cybersecurity incident response team** with AI capabilities.
  9. Establish a **cybersecurity budget** and ensure its integration into the overall business risk management plan.

3 **Do we have an up-to-date incident response plan**, and how often is it tested through real-world simulations or tabletop exercises?

Best-Case Response: Leadership presents a **detailed incident response plan** that is updated regularly and tested through **quarterly tabletop exercises** and **real-world simulations**. All levels of the organization are involved, and results are used to improve the plan.

- **Actionable Recommendation:**
  1. Ensure **continuous improvements** to the plan.
  2. Include **board-level participation** in at least one annual tabletop exercise.
  3. Encourage the use of **external evaluators** to test the plan's effectiveness.

Middle-Case Response: There is a **basic incident response plan**, but it hasn't been tested in over a year. Leadership is aware that it needs updating and plans to schedule exercises in the near future, but nothing is currently in motion.

- **Actionable Recommendation**:
  1. Set a **deadline for immediate testing** of the plan.
  2. **Mandate regular updates** to the plan based on industry standards.
  3. Require **quarterly simulations** moving forward, ensuring the board gets a post-exercise debrief.

Worst-Case Response: Leadership admits that there is no formal incident response plan, and testing has never been done. The team relies on a reactionary approach, assuming IT will handle any breaches as they occur.

- **Actionable Recommendation**:
  1. Demand an **immediate development** of a formal, comprehensive incident response plan.
  2. Institute **emergency training** and tabletop exercises as soon as the plan is created.
  3. Recommend appointing a **dedicated cybersecurity leader** if one doesn't exist to oversee the incident response.

4 How do we assess and manage cybersecurity risks from third-party vendors, and what is our process for continuously monitoring these risks?

- **Best-Case Response**: Leadership provides a **thorough third-party risk management process**, including vendor audits, real-time monitoring, and specific contract clauses that outline cybersecurity responsibilities. Continuous monitoring tools are in place.
  - **Actionable Recommendation**:
    1. Ensure **third-party risk assessments** are reviewed by the board annually.
    2. Push for **automated monitoring tools** to stay ahead of risks.
    3. Recommend **independent audits** of key third-party vendors.
- **Middle-Case Response**: Third-party risks are evaluated at the time of onboarding, but **ongoing monitoring is limited**. Leadership acknowledges the need for more frequent reviews but hasn't implemented continuous monitoring tools.
  - **Actionable Recommendation**:
    1. Encourage **investment in automated vendor risk monitoring**.
    2. Require **semi-annual reviews** of third-party vendor security.
    3. Update contracts to include more **robust cybersecurity clauses**.
- **Worst-Case Response**: Leadership doesn't have a formal third-party risk management process. Vendors are chosen based on price or performance without any **cybersecurity vetting**. There's no plan to manage third-party risks.
  - **Actionable Recommendation**:
    1. Immediately initiate a **third-party vendor risk audit**.
    2. Establish a **cybersecurity vetting process** for all new and existing vendors.
    3. Hire or consult with a **vendor risk management expert** to set up continuous monitoring.

5 How are we ensuring compliance with relevant cybersecurity regulations (e.g., PIPEDA, GDPR), and do we conduct regular audits to maintain compliance?

Best-Case Response: Leadership provides clear documentation of **regular audits**, including internal reviews and third-party assessments, demonstrating full compliance with regulations like **PIPEDA, GDPR**, and other applicable standards. They have a compliance officer or team responsible for monitoring changes in regulation and adjusting policies accordingly.

- **Actionable Recommendation**:
  1. Ensure that **compliance reports** are reviewed by the board annually.
  2. Encourage a **proactive approach** by staying ahead of changing regulations, particularly as they evolve to cover AI-related threats.
  3. Suggest an annual **external audit** to verify ongoing compliance.

Middle-Case Response: The company conducts **occasional audits**, but only reacts to regulatory updates when required. Compliance is **basic** and not integrated into broader business processes. There is a lack of proactive monitoring for new or upcoming regulations.

- **Actionable Recommendation**:
  1. Mandate a **more frequent audit schedule**—preferably semi-annually.
  2. Appoint a **dedicated compliance officer** or third-party advisor to stay ahead of regulatory shifts.
  3. Conduct **gap analyses** to identify areas where compliance could improve, particularly regarding evolving international standards.

Worst-Case Response: Leadership is **unaware of specific regulations** or hasn't conducted a compliance audit in years. They assume that because the company hasn't faced penalties, compliance isn't a priority.

- **Actionable Recommendation**:
  1. Implement an **immediate regulatory audit** to assess vulnerabilities.
  2. Hire or contract a **compliance officer** if one isn't already in place.
  3. Create a **compliance framework** and ensure all staff are trained on the necessary standards to maintain ongoing compliance.

6 **What measures are we taking to build a cybersecurity-aware culture throughout the organization**, and how often do we provide employee training on cybersecurity best practices?

Best-Case Response: Leadership presents a detailed **employee training program** with regular **cybersecurity awareness campaigns**, mandatory **phishing simulations**, and role-specific training across the organization. Employees are regularly tested, and results are used to improve training content. The program is embedded into the corporate culture.

- **Actionable Recommendation**:
  1. Have the board participate in the **same training** to show commitment.
  2. Encourage leadership to **continually update the training** to reflect emerging threats, including AI-driven attacks.
  3. Suggest using **external cybersecurity awareness platforms** to ensure best-in-class employee training.

Middle-Case Response: Training is conducted on an **annual basis**, but it's basic and doesn't include regular testing or simulations. Leadership acknowledges that while some employees are aware of best practices, cybersecurity isn't **embedded in the culture**.

- **Actionable Recommendation**:
  1. Push for **quarterly training sessions** and regular phishing tests to improve employee engagement with cybersecurity.
  2. Suggest implementing a **real-time training platform** that can evolve as new threats emerge.
  3. Request leadership include **cybersecurity KPIs** in performance evaluations to drive accountability.

Worst-Case Response: Cybersecurity awareness isn't part of the culture, and no formal training is provided to employees. Leadership assumes that the IT department handles everything and that most employees don't need to know about cybersecurity.

- **Actionable Recommendation**:
  1. Demand **immediate implementation** of a cybersecurity awareness training program.
  2. Begin **phishing simulation tests** to measure employee awareness and readiness.
  3. Build cybersecurity training into the **onboarding process** for all new employees and make it a regular, required event.

7 How do we evaluate the cybersecurity risks posed by AI and automation in both our defenses and potential vulnerabilities?

Best-Case Response: Leadership explains they are already **integrating AI and automation** into both defensive cybersecurity and threat detection, with a focus on machine learning algorithms that detect anomalies. They regularly assess AI-related vulnerabilities and have invested in **automated response tools**.

- **Actionable Recommendation**:
  1. Encourage continued investment in **AI-driven detection tools**.
  2. Ask for **quarterly briefings** on how AI advancements are being incorporated into cybersecurity strategies.
  3. Suggest ongoing collaboration with **AI-focused cybersecurity firms** to stay ahead of emerging threats.

Middle-Case Response: AI is **on the radar**, but they've only just begun exploring its potential in cybersecurity. They are considering implementing AI tools but haven't yet integrated them into everyday defenses.

- **Actionable Recommendation**:
  1. Push for **immediate adoption** of AI-driven cybersecurity solutions.
  2. Recommend leadership set up an **AI task force** to focus on integrating automated defenses.
  3. Request an outside consultation with **AI experts** to evaluate the company's current approach and future AI needs.

Worst-Case Response: Leadership has no real understanding of how AI could pose a threat or be used in cybersecurity. They dismiss AI as something "**in the future**" or too technical for current needs.

- **Actionable Recommendation**:
  1. Demand **immediate AI training** for leadership to understand the current risks and opportunities.
  2. Engage with an **AI-driven cybersecurity firm** to begin developing an AI-integrated strategy.
  3. Insist on a **cybersecurity risk assessment** that includes specific focus on AI and automation vulnerabilities.

8 **What are the most critical cyber security risks we face,** and how does leadership ensure these risks are being addressed at all levels of the organisation?

Best-Case Response: Leadership conducts thorough, **regular risk assessments** covering specific and emerging cyber threats, such as AI-driven attacks, ransomware, and supply chain risks. Their proactive cybersecurity programme is deeply integrated into the overall risk management structure, with clear communication across all levels of the organisation.

- **Actionable Recommendations**:
  1. Continue the board's support of **ongoing cybersecurity investments**.
  2. Schedule **quarterly board reviews** of the evolving risk landscape.
  3. Promote **board education** on new cybersecurity developments and emerging threats.

Middle-Case Response: Leadership recognises some risks but offers **only partial coverage**—addressing basic threats like phishing, while **under-preparing for advanced or emerging risks**. They plan to bolster policies and update security systems, but gaps remain in comprehensive threat monitoring and resilience testing.

- **Actionable Recommendations**:
  4. Mandate an **external cybersecurity audit** to identify coverage gaps.
  5. **Set specific timelines** for leadership to report progress on risk mitigations.
  6. Allocate resources to **enhance cybersecurity tools** and staff training.

Worst-Case Response: Leadership admits that they have **no formal vendor risk assessment process**, and they trust their vendors without conducting any due diligence. Vendors with access to sensitive data are **not monitored for cybersecurity risks**, and the **company lacks contractual safeguards** in its agreements with third parties.

- **Actionable Recommendation**:
  7. Implement an **immediate audit** of all vendors to assess cybersecurity risks.
  8. Establish a **formal vendor risk management program**, including regular reviews and compliance checks.
  9. Update all vendor contracts to include **mandatory cybersecurity standards** and penalties for non-compliance.

9 How are we managing and mitigating the legal and financial risks associated with a cyber incident, including potential litigation and regulatory fines?

- **Best-Case Response**: Leadership outlines a **comprehensive cyber risk management plan**, including **cyber insurance**, **legal protections**, and **contingency funds** set aside for regulatory fines or litigation. They have a dedicated team that constantly reviews legal implications and adjusts based on evolving cyber risks.
  - **Actionable Recommendation**:
    1. Encourage **regular reviews** of the company's cyber insurance coverage to ensure it is up-to-date and comprehensive.
    2. Push for continued **legal readiness drills** to prepare for potential cyber litigation.
    3. Ensure the company's **incident response plan** includes provisions for rapid legal and financial mitigation actions in the event of a breach.
- **Middle-Case Response**: The company has basic cyber insurance and legal protections in place but hasn't reviewed them recently. Leadership acknowledges that some gaps exist, particularly regarding newer risks like **AI-driven attacks** and **ransomware**.
  - **Actionable Recommendation**:
    1. Mandate a **thorough review** of cyber insurance policies and legal coverage.
    2. Encourage leadership to work with external consultants or law firms to **strengthen protections** against newer risks.
    3. Push for an updated **cyber risk mitigation plan**, including budget allocations for potential regulatory fines and legal fees.
- **Worst-Case Response**: Leadership has no **cyber insurance** or dedicated legal resources for cybersecurity incidents. They assume that general insurance will cover any issues, and they have **no contingency plan** for regulatory fines or legal action.
  - **Actionable Recommendation**:
    1. Immediately acquire **cyber insurance** with coverage for breaches, ransomware, and regulatory fines.
    2. Engage a **legal team** specializing in cyber risk to create a mitigation plan.
    3. Allocate funds in the budget for **cyber-related financial risks**, including potential litigation and fines.

10 **How do we ensure senior leadership and board members are trained in cybersecurity**, particularly regarding spear phishing and targeted attacks?

Best-Case Response: Leadership describes a regular **cybersecurity training** program specifically designed for senior executives and board members, including real-world simulations and testing for **spear phishing** and other targeted attacks. They are also involved in **tabletop exercises** to prepare for breaches.

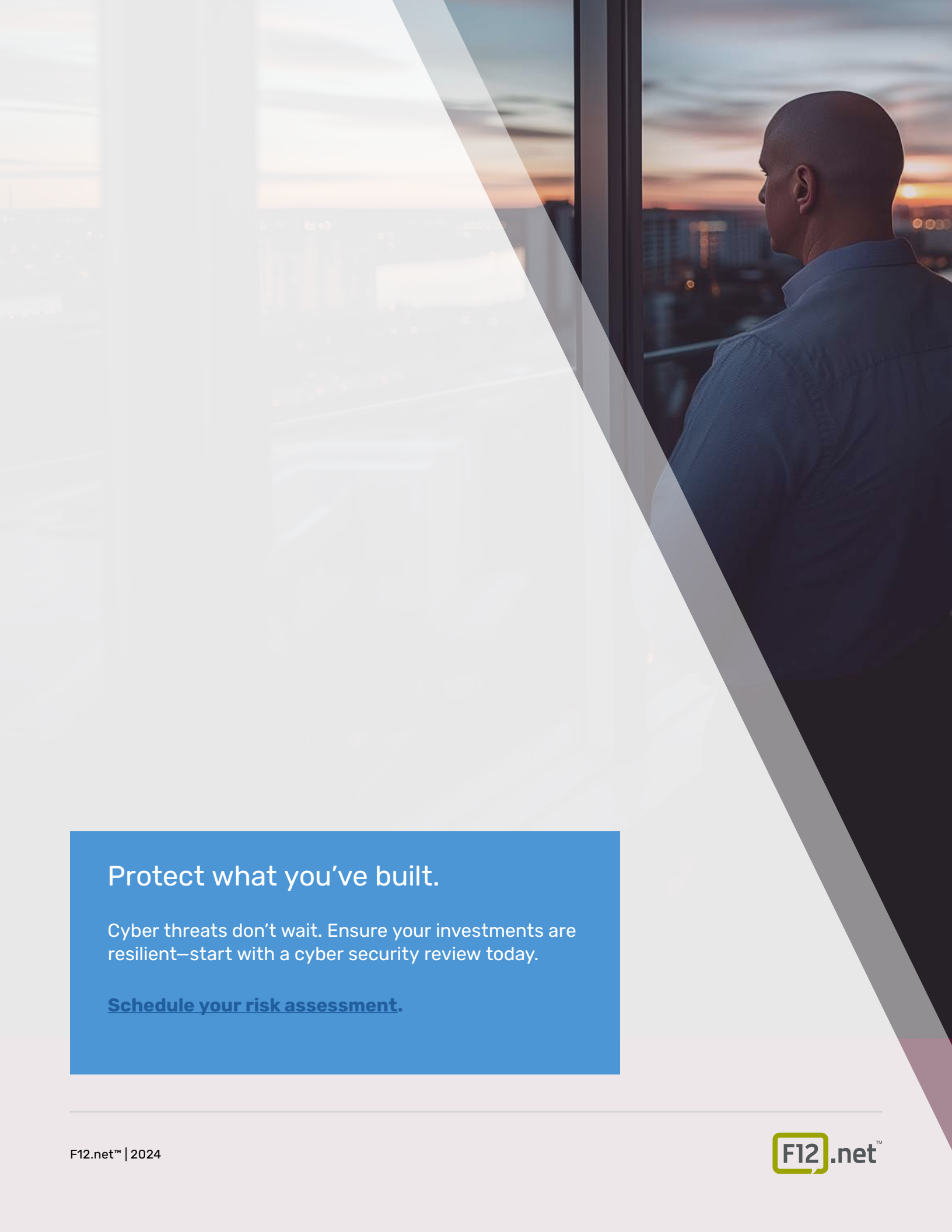
- **Actionable Recommendation**:
  1. Continue regular **board-level cybersecurity training** and ensure it evolves with the threat landscape.
  2. Ensure board members are included in **annual incident response exercises**.
  3. Regularly review and update **executive-level phishing simulations** to reflect the latest threats.

Middle-Case Response: Senior leadership and board members receive **basic cybersecurity training**, but it's infrequent, and simulations specifically targeting their roles are rare. They are aware of spear phishing, but no real emphasis has been placed on training them to deal with these attacks.

- **Actionable Recommendation**:
  1. Require **quarterly training** specifically designed for board members and senior leadership.
  2. Implement regular **spear phishing simulations** focused on executives.
  3. Integrate **executive training** into the company's broader cybersecurity awareness program, ensuring it's tailored to the unique risks they face.

Worst-Case Response: Leadership admits that **no formal training** has been provided for senior executives or board members, assuming that only IT staff need this level of education. They are unaware of the risks associated with **spear phishing** or targeted cyberattacks on leadership.

- **Actionable Recommendation**:
  1. Immediately implement a **cybersecurity training program** tailored to the board and C-suite.
  2. Conduct an **executive-targeted phishing simulation** to assess vulnerabilities.
  3. Schedule **annual cybersecurity briefings** for the board with external experts to ensure they are well-informed on the latest threats.



Protect what you've built.

Cyber threats don't wait. Ensure your investments are resilient—start with a cyber security review today.

Schedule your risk assessment.