BIRMINGHAM CONSULTING

Risk Management – Headlines and Tips for Executives

Winter 2026

https://birminghamconsulting.net/

1. **Global movements create personal accountability for leaders and boards**
   Board members and executive management are increasingly being held accountable for information security events by suppliers, customers and regulatory bodies. Global developments, such as Europe's NIS2 Directive, highlight that failure to exercise due diligence can create personal accountability for leadership. Executives and boards should ensure risk levels are documented and regularly reviewed, so informed decisions can be made to mitigate threats and protect the organization… and themselves. Courtesy of *Birmingham Consulting*

2. **Key step in risk management – identify and track your assets**
   Leaders should confirm that their technology or security team maintains a complete information asset inventory, which lists all systems, applications, and cloud services the organization uses. Just as financial accounting tracks assets for an organization's financial health, an information asset inventory tracks all data, including where it is stored, what security measures protect it, and who is responsible for it. Understanding the location, value, and importance of each data asset allows leadership to prioritize protections and make informed risk decisions. Regularly updating the inventory ensures it reflects organizational changes and helps prevent unexpected exposure. *Courtesy of Birmingham Consulting*.

3. **Making risk visible - reporting vulnerabilities and threats to leadership**
   Executives should confirm that their organization conducts formal risk assessments on a recurring basis. The current industry standard is annually, allowing teams to identify vulnerabilities, emerging threats, and gaps in controls before they become issues. Leadership involvement and support is key to ensure findings are acted on and that adequate resources are allocated to address priority risks. Equally important, assessment results should be clearly communicated back to executives and the board, with documented action plans and status updates. Consistent evaluation and transparent reporting reduce the likelihood of surprise incidents and support informed strategic decision-making. *Courtesy of Birmingham Consulting*.

4. **Confirm that third-party vendor risks are evaluated before onboarding**
   All third-party vendors, partners, and even clients, introduce additional risk exposure to your organization. Leaders should ensure all third parties include security, privacy, and operational risks in their assessments before onboarding. It's also a two-way street – ensure that your organization is meeting your customer and client security requirements as well. *Courtesy of Birmingham Consulting*.

5. **"Landmark" cyber security case underscores executive accountability**
   The SEC's 2023 action against SolarWinds and its Chief Information Security Officer (CISO) marked the first time the agency charged a CISO in connection with a cyber security incident, highlighting the serious nature of risk management. For executives and boards in 2026, this case underscores the importance of actively documenting, monitoring, and

communicating cyber security risks. Ensuring that known risks are clearly understood by leadership not only supports regulatory compliance but also enables informed strategic decision-making and strengthens stakeholder confidence. Executive engagement in risk management is now a standard expectation. Courtesy of *Birmingham Consulting*

6. **Reduce risk by controlling who has access to critical information**
   Leaders should confirm whether staff and AI agents' access to sensitive systems and data is regularly reviewed. Limiting access to only those people and agents who require it reduces the likelihood of accidental or intentional misuse, up to and including serious incidents. If it's not reviewed on a recurring basis, changes in staffing, roles, or responsibilities should trigger immediate access updates. When leadership support important processes like these, it reinforces a culture of accountability around data protection. *Courtesy of Birmingham Consulting*.

7. **CPCSC Phase 2 April 2026 - New requirements tied to Canadian defence contracts**
   Organizations bidding on or working with the Government of Canada on National Defence contracts will need to meet new cyber security requirements under the Canadian Program for Cyber Security Certification (CPCSC). Phase 2, running from April 2026 to March 2027, introduces a Contract Cyber Security Risk Assessment and requires businesses to self-assess and provide Level 1 self-attestation in their Canada Buys profile at the time of contract award. The Standards Council of Canada is beginning to accept applications from organizations interested in helping certify compliance and developing the Level 2 certification system. Guidance for Levels 2 and 3 to be shared in due course. Leaders should start preparing now to ensure their teams understand the requirements and can demonstrate compliance when contracts are awarded. Courtesy of *Birmingham Consulting*

8. **Understanding your options for responding to security risks**
   Information security is about managing risk, (because the only way to eliminate your risk is to shut down the business). There are four ways you can strategically respond to risk **- mitigate, avoid, accept or transfer.** Mitigating is preparing for a threat with the goal of reducing the likelihood and/or impact of a particular risk. Avoiding risk refers to removing or preventing the circumstances that create the risk. Accepting risk is a conscious acknowledgement that the risk exists, but deciding it's bearable. And transferring risk can involve shifting the risk from one party to another. The most effective way to transfer security risk is contractually, whereas the most common way to transfer financial risk, is insurance. Courtesy of *Birmingham Consulting*