

Information Protection for Corporate Governance

Identify, Control And Audit The Flow Of Confidential Corporate And Board Information, To Ensure Confidentiality And Demonstrate Proper Corporate Governance And Compliance



OVERVIEW

The board of directors and members of the executive management team receive and create large amounts of confidential information such as: board meeting minutes, earnings reports, revenue plans & forecasts, sales pipeline, new business opportunity plans, operations strategies, and strategic business plans. These plans are among a company's most important assets. When such information is improperly disclosed, a company can suffer a competitive disadvantage, lost sales momentum, and damage to its reputation.

Failure to comply with requirements like Section 406 of Sarbanes Oxley (SOX), Securities and Exchange Commission (SEC) or the New York Stock Exchange (NYSE), rules for protecting confidential corporate data can decimate a company's stock valuation.

Codes of conduct govern senior financial officers in public companies, and the more stringent requirements of the NYSE corporate governance listing standards govern personnel of listed companies. These NYSE listing requirements specify that companies must ensure employees, officers, and directors maintain the confidentiality of information entrusted to them, including all non-public information that might be of use to competitors or harmful to the company and its disclosed customers. These requirements also stipulate that these companies must implement procedures and compliance standards that will facilitate effective protection of confidential information.

THE SOLUTION

The NextLabs Corporate Governance & Confidential Information Protection Solution manages the protection, sharing and communication of board-level information. It persistently protects confidential information wherever the user is located, ensures user adherence to policy, and educates board members and executive management on the correct usage of confidential information. This is accomplished in a non-intrusive and intuitive way.

The solution is an integrated data protection solution that combines multi-channel communications control, information rights management, virtual information barriers, and host-based data loss prevention technologies with application, document, and device control capability. It performs real-time policy evaluation on or off the network. This comprehensive approach improves compliance and mitigates information risk. This is the only available solution that controls information sharing across communication and collaboration channels.

The solution also makes internal and external collaboration among the corporate governing body safer and more secure, automating safe handling of confidential board information and ensuring proper access and protection of applications and data.

SOLUTION HIGHLIGHTS

- Leakage of confidential board information
- Improves corporate governance by minimizing information risk for all levels of communication
- Reduces audit cost up to 90% and improve compliance by 4x
- Automates up to 90% of the information protection and handling procedure with 100% user satisfaction
- Seamless protection and interactive workflow offer ease of use and a high degree of coverage
- Rapid, proven implementation with central management and ease of maintenance to ensure quick ROI
- Best practices, reusable policy libraries, and user assistance to improve TTV and lower TCO

The NextLabs Corporate Governance & Confidential Information Protection Solution scales to meet the information protection requirements for board members and executive management team by working seamlessly with all applications. It is easy to use and maintain.

The Solution Addresses the Following:

Information Duplication: A key issue that often leads to leakage of confidential information is uncontrolled duplication of information.

Protection of Corporate Governing Body Document Repository: Materials created by and received from the board of directors and executive management team members, including sensitive company information, must be protected. Role-based access control must be managed to control access to the repository to maintain confidentiality of the documents.

Removable Media Usage: One of the common ways confidential information is lost by board members and/or executive management copying files to USB thumb drives and losing them. Another risk is a member of the corporate governing body inserting infected USB drives into their systems, and infecting other members.

Communication: Many leaks of confidential information happen as the corporate governing body members inadvertently send confidential information to unapproved users. To prevent such occurrences, the Solution includes policies to govern Email and IM usage.

Laptop Protection: The Solution prevents Administrators from accessing confidential board information on laptops when the laptop is maintained or repaired.

Secure Portal: The Solution provides a secure portal for enabling collaboration among the board of directors and the executive management team.

Application Control: Board data could be leaked or confidentiality may be compromised without application control. The Solution protects against such leakages.

Information Rights Management: Board data should be protected based on its content and context. The information access should be limited based on time and role.

Auditing and Reporting: The Solution provides comprehensive reporting of all access and usage of confidential board information to support Information Governance initiatives. The Solution offers a customizable compliance dashboard showing key parameters such as attempted violations, top user access, and effectiveness of the policies.

The Solution includes Pre-Built Policy Applications

The NextLabs Corporate Governance & Confidential Information Protection Solution meets requirements of:

- **Secure Vault:** Providing a secure location on the local drive for storing board information to protect against unauthorized access.
- **Secure Communication Channel:** Providing a secure channel for receiving board package. Information and sending confidential board requests to other board members, executive management team, and legal counsel, preventing usage of unapproved communication channels such as Yahoo!, Gmail, or instant messaging.
- **Secure Collaboration:** Establishing a secured portal where information access and usage is monitored and secured.

- **Approved Application:** Allowing only company-approved applications to access and share the board data so that it is protected against any inappropriate disclosure.
- **Approved Usage:** Printing documents or copying data to removable devices, such as USB drives, without compromising security and confidentiality.

SOLUTION DEPLOYMENT: HOW TO GET STARTED TODAY

NextLabs implements the solution by using expert product knowledge and a services best practices methodology. NextLabs can also assist clients with identifying their controlled data, as well as defining information control policies.

Step 1: Requirements Gathering

NextLabs works with you to understand your infrastructure, and security and policy requirements.

Step 2: Risk Assessment

We help you discover and identify your current risks to help prioritize Solution requirements.

Step 3: Policy Configuration

Policies are designed and electronically codified using NextLabs' suite of Information Risk Management software, along with any custom Policy Assistant automation.

Step 4: Install Policy Enforcers

Policy Enforcers are deployed across applications and systems, if applicable to requirements.

Step 5: Knowledge Transfer

NextLabs will conduct knowledge transfer training to ensure your team possesses the expertise to appropriately maintain and manage the solution.

ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM. For more information on NextLabs, please visit <http://www.nextlabs.com>.