NEXTLABS®

White Paper

Automated Information Handling

Now An Enterprise Can Actively Control Information Handling To Promote Business Efficiencies and Control Disclosure Risks

Executive Summary

Today's companies maintain diverse business relationships inside and outside the enterprise. With increased mobile users and data, portable devices, partners, and remote workforces, risks are growing over sensitive business information. No longer can exposure be classified as either an inside threat or external attack. Rather, companies must now consider how an extended enterprise can effectively maintain proper information handling and disclosure across dynamic networks where workflow, collaboration, and risk management is now complex.

As companies continue to add new information resources to empower employees, uncertainty increases over how to handle data properly. Traditional "lock down" security measures can restrict employees from easily collaborating with internal teams, partners, outsourcers, and remote users. Alternatively, granting document and application rights to access and use files can help guide proper handling, but often these IT controls lack an awareness of the proper business conditions that determine acceptable use. A user's credentials, the data class or computing device, present location for doing business, time of day, and other variables often determine the severity of the risk.

As a result, authorized users with correct entitlements to sensitive data, who attempt to support corporate policies and procedures, are often forced to make discretionary policy decisions that result in handling information improperly, including misuse or unintended actions that can harm business momentum and integrity, and violate regulations.

The risk of mishandling sensitive data can now be quickly removed or decreased. NextLabs' Information Risk Management solution uses an extensible platform approach that allows information controls to be quickly digitized and codified by expressing familiar business language terms, and deployed across points inside or outside the enterprise. Companies protect information integrity and optimize procedures by using controls that automate policies for what, where, when and how data is to be used appropriately and by which users, without affecting productive business activities when automation is applied. If required, controls automate information use procedures based on policy evaluation to simplify workflow.

This white paper introduces the concepts behind automated information controls, today's business risks when relying on manual policy approaches, typical automation scenarios, and the benefits for automating policies and procedures. The overview will help business executives and policy planners to better understand automated information handling across an extended enterprise to protect data and improve business efficiency.

BACKGROUND

Today's organizations maintain a set of policies and procedures that direct the company for how sensitive data is to be used properly in support of productive business goals. Policies and procedures also exist to help control risks that are exposed when data is handled and disclosed improperly. When data is misused or negligence occurs, it could lead to loss of intellectual property, conflicts of interest between project teams within the organization, or violations of industry or internal regulations that can generate costly fines and remediation expenses.

Unfortunately, relying on manually enforced "paper" policies and the goodwill of employees to always interpret policy correctly are not reliable, effective, or legally defendable positions when policy violations inevitably occur. More often, executives are being held directly accountable by regulators, shareholders, government agencies, and similar bodies when data is compromised internally or externally, with results that include decreased shareholder value, bad PR, lost competitive momentum, and even jail time.

Why are Manual Business Policies Hard to Enforce?

With risks to sensitive data growing, business planners are realizing their jobs are increasingly difficult when attempting to ensure consistent controls across a dynamic enterprise. Policies and procedures, codified in handbooks, are translated into IT controls or communicated during employee trainings. But system rules and education do not always accurately capture what the policy planners intended, leading to unknown results when users interpret policies and information handling becomes discretionary.

A company policy such as, "HR teams cannot disclose social security numbers outside the company" will often get translated into an access control at a network gateway on a set of HR data or an employee rule discussed during training, without capturing the business conditions that determine appropriate use scenarios for proper disclosure. For example, it may be appropriate for an HR Director to share data in a benefits plan during specific time periods, over properly-secured communications channels, with benefit plan administrators. However, today, companies often compromise by either locking down data with excessive security controls or, alternatively, accept an open environment that lacks the control granularity to ensure risks are actively managed within context.

Enterprise policy planners need business policies and procedures to be accurately and quickly automated across their information network to ensure proper handling, without slowing down normal business flow. Information controls that automatically understand when data handling and disclosure is appropriate to business circumstances can avoid arbitrary "lock down" security approaches that cripple productivity. When policies are applied, in business terms, to accurately describe and automate controls, without forcing end users to make discretionary policy enforcement decisions, companies can achieve a closer alignment with their intended business objectives.

Quickly Automate and Enforce Policies

Business planners must be able to quickly and easily automate information controls for proper data access, handling, and disclosure procedures across the enterprise, regardless of risk origin, physical boundaries, or workgroup and IT complexities. To effectively control risks requires an ability to electronically codify and centrally store business policies that can be applied universally across a complex, heterogeneous organization, without gaps or misinterpretation. Policies deployed and enforced across critical control points, inside and outside the enterprise, must ensure that information handling and disclosure is aligned with business requirements.

Automated Information Controls Require a Business-Level Approach

Policies and procedures must be defined in ordinary business terms to ensure controls directly capture real business scenarios, rather than defined in "machine language" due to infrastructure technology limitations. To effectively automate information handling, policies must be abstracted from the complexities of underlying IT management to be relevant across any applicable information resources, systems, and applications. Users change roles or new employees join the company, new business locations and applications are added, new devices and information handling activities evolve, document formats change over time, and so on. Controls must remain consistent across the enterprise during the entire information lifecycle to prevent risk exposure.

THE BENEFITS OF AUTOMATING POLICIES AND PROCEDURES

With a solution that can easily automate business policies and procedures, companies can manage information risks to:

1. Quickly Protect Business Processes and Workflow

When information handling risks are determined, automated controls can be deployed to avoid the risks of unauthorized disclosure. For example:

- If a team creates a confidential proposal, controls can require management approval procedures when attempting to disclose the file outside the team.
- When a quarterly revenue forecast begins a final review period, a policy can automatically prevent data modifications that would attract regulatory scrutiny.

2. Reduce End User Burden and Uncertainty During Policy Decisions

Users who forget to comply with training or are unaware of business policies can avoid making arbitrary decisions that result in data misuse or casual negligence:

- A user who is unsure whether a project team has changed can automatically have all project files saved to a predetermined, approved storage location, where former team members are automatically restricted from access to that location.

- Executive teams that work on a strategic business plan can have related files automatically encrypted prior to any team distribution to maintain confidentiality.

3. Reduce End User Burden and Uncertainty During Policy Decisions

Users who forget to comply with training or are unaware of business policies can avoid making arbitrary decisions that result in data misuse or casual negligence:

- A user who is unsure whether a project team has changed can automatically have all project files saved to a predetermined, approved storage location, where former team members are automatically restricted from access to that location.
- Executive teams that work on a strategic business plan can have related files automatically encrypted prior to any team distribution to maintain confidentiality.

4. Economize Business Relationships

When new teams are formed or suppliers join an organization, uncertainty may exist for how to best communicate and manage ad hoc workflow between members. Automated procedures can improve collaboration efficiency and support safe workflow:

- A company's outsourcing partner is prevented from distributing product designs unless using secure channels and the client company's specific encryption keys.
- Client files uploaded to a company's common FTP server are automatically moved to the correct recipient's file share folder to avoid any conflicts of interest.

5. Lower Support Costs and Total Cost of Ownership

By automating policies and procedures, companies can avoid discretionary uses of data or applications that may result in support escalation or incorrect behavior:

- An end user, unsure when to delete sensitive data after a confidential project is completed, automatically has the content destroyed using a secure shredder and notified, without an IT inquiry required for how to properly use the application.
- When employees attempt to distribute a confidential file, they are automatically educated with real-time alerts about company best practices and approved applications for sensitive data handling without manual training required.

WHAT ARE THE RISKS FROM MANUAL PROCEDURES?

Automating information controls to minimize discretionary access, handling, and disclosure of sensitive data is important to address the risks that exist today from information leakage, conflicts of interest, negligence, improper records management and retention, and more. These risks, if left unmanaged, can result in costly regulatory fines, remediation expenses, losses to shareholder value, negative PR, lost customer loyalty, and similar decreases in business momentum that impact the bottom line.

Automating policies and procedures can help to eliminate manual guesswork across an organization for how data is to be handled properly. Risks today include:

1. Business Tools without Automated Procedures for Proper Use

Employees are provisioned with business tools that often don't include a guidebook for how to use these tools appropriately for business purposes. For example, using Web browsers is necessary to perform market research, access online sales tools or the corporate intranet. But, at the same time, could be used without controls to download illegal MP3s, browse pornography, or undertake similar activities that are unproductive or create liability. Similarly, tools such as USB drives, smart phones, laptop computers and so forth that drive mobile computing also increase risks when data is stored on or disclosed from these devices without safeguards automatically applied.

Automated policies and procedures across business tools can help guide acceptable uses. Application or device entitlements for proper data use can now be provisioned to ensure productive results; for example, setting limits on Web browser access by automatically enforcing URL filtering during normal business hours for contract personnel, or preventing classes of sensitive data from being copied to portable media without encryption applied. When automated policies and procedures are applied across applications, devices, and similar business tools, end users can remain productive while limiting activities that create risk exposure.

2. Minimizing User Uncertainty for Properly Following Policies

Expecting end users to manually support corporate policy that is put on paper is often unrealistic when given a large number of complex, detailed guidelines to follow. What's more, guidelines constantly change, making it difficult for normal users to stay current.

There is a limit to how well regular education programs can ensure a precise set of best practices is followed if left up to manual interpretation and long-term consciousness. Even for those who understand guidelines within their roles, human error is often inevitable when immediate deadlines, new processes, changing business relationships, and so forth add new variables or complexity within dynamic environments.

By automating policies and procedures based on user roles and delivering real-time education automatically if best practices are not followed, policy planners can help to eliminate user mistakes and reduce the burden on honest employees who strive to follow correct guidelines, but often don't, due to human error and policy complexity.

From the example above, a user who attempts to browse a non-business Web site during non-business hours might be automatically permitted, while also receiving an alert if attempts are made to download inappropriate material that creates liability. Similarly, if sensitive data is attempted to be transferred to a USB drive, encryption can be applied automatically before copying, while still allowing data mobility to proceed.

3. Inconsistently Applied Manual Security Controls

Many security tools exist to help protect sensitive data, however, without automation during the time information is handled, end users may forget, or might not even be aware, that security must be applied. Common examples are digital rights or encryption applied when sensitive classes of data are sent via email or downloaded to portable USB drives. When relying upon users to manually and consistently apply security controls in a bottom-up approach, protection is left uncertain across the organization.

While it is possible to automate security controls such as encryption across entire sets of data for all communication channels or endpoints, this broad approach can also slow business fluidity. Automated policies and procedures that determine when security should be applied will result in a more precise approach to control risks. For example, require encryption for only business-sensitive files transferred to USB devices, while still allowing employees to take ordinary work or personal files to a home office or on the road without slowing down their mobility.

4. Data Retention Policies without Automatically Enforced Guidelines

When relying upon manually-enforced policies, employees will not always know what, where, when, and how data should be retained or archived, or even remember what data was deemed sensitive after time sufficiently elapses. In some cases, retention that is left up to user discretion can even harm a business when archiving inappropriate content. Today, data retention solutions are applied to maintain important data or create mirror copies, but doing so runs the risk of overloading storage servers—retaining inappropriate content such as a user's personal files or unlicensed materials, or other data that is irrelevant, if not harmful, to the business.

Automated procedures applied to data retention are necessary to optimize the preservation of sensitive data. Data retention policies need to incorporate when conditions, such as time, project type and document author, should automatically trigger retention controls to be enforced. For example, when a product design is completed, project files and designs are systematically archived. Or if a CFO publishes a financial statement, the spreadsheet is automatically mirrored to back up media.

5. Data Destruction that Fails to Automatically Control Risk Exposure

Similar to retention, there are conditions when data should be disposed of after its usefulness or purpose has expired. When employees browse a Web site or use an application that contains personal information, a Web browser cache or temporary files may need to be cleared or deleted. Or if users decrypt files and store them on a desktop, they often forget to dispose of the decrypted file properly and/or re-encrypt it back to its original state after a task. These scenarios, if left uncontrolled, create unnecessary risk.

Relying only on manually-enforced policies, employees will not always know when, how or why data should be destroyed or transformed, or even remember what data requires policies applied after time. Moreover, since sensitive data can be duplicated, all copies will need to be identified across a network and disposed of accordingly.

Automated data handling is necessary to avoid risk exposure, especially when time can increase risks the longer that sensitive data is left open to casual misuse. Effective, automated controls for data destruction can be as simple as emptying a cache during browser shutdown after sensitive Web sites are viewed and deleting temp files—or as sophisticated as automatically destroying all remnants of a file that match a profile across the enterprise.

6. Improper Disclosure between Workgroups or Outside the Company

Internal workgroups and/or relationships that exist outside a company where data is shared may create conflicts of interest that are not always understood by workers across an enterprise, even if policies are prescribed on paper for safe disclosure. For example, an outsourced manufacturer could violate a customer agreement or contract if product designs are disclosed with a project manager who also manages a competitive client—or a research analyst could share a report with a "trusted" salesperson that violates regulatory barriers. Similarly, a sales rep could accidentally send files to an incorrect client by typing a wrong recipient name into an email address field.

Automating policies and procedures across dynamic groups and between organizations can prevent conflicts of interest that result from improper handling and disclosure. Automation that ensures communications or distribution channels only allow data sharing or collaboration between authorized persons and recipients, for specific projects, can help take the user guesswork out of following proper disclosure procedures when business relationships are formed dynamically or change suddenly.

7. Improper Data Entitlements for Enterprise Applications

Critical data in a company is often created, accessed, shared, and managed through enterprise applications such as enterprise resource planning (ERP) systems, product life cycle management (PLM) systems, customer relationship management (CRM) systems, supply chain management (SCM) systems, document management systems (DMS), file shares, and collaboration portals (such as intranets and extranets). Access to these systems are often role based, and controlling access at the data level often requires complex provisioning of new roles, manual review of user access requests, or strict control of what data can be uploaded to these systems. These manual procedures are time consuming and error prone.

Automating procedures and information controls of who can access what data in these enterprise applications can help reduce the risk of accidental violations, and encourage proper usage of these enterprise applications, deriving productivity while maintaining compliance. For example, an extranet portal can automatically classify a document that is uploaded to a collaboration site, and deny or approve access to the document dynamically based on policy, instead of blindly allowing all members of the site access to the document.

APPLICATIONS AND EXAMPLES

Automation during information access, handling and disclosure can be effective in a number of business scenarios where information risks need to be reduced across the enterprise. A sample of these case examples follows:

Automatically Monitor Sales Forecasts Submitted for Review

- Automation Goal: Ensure that sales managers only upload forecasts to a secured sales team folder; notify stakeholders (“Sales VP”) when spreadsheets are ready for review. Prevent any further uploads prior to the new start of quarter.
- Result: Avoid improper disclosure of confidential data; allow Sales VP to approve forecasts prior to the new quarter in a timely manner; alert managers with late submissions to request an exemption if not submitted in time.

A company wants to ensure efficient workflow, while also protecting confidentiality. A sales team is prevented from emailing files to unauthorized recipients or using unapproved, unsecured communication channels. Instead, all sales forecast spreadsheets need to be copied to the correct shared sales folder. All sales managers conduct business as usual; if an attempt is made to submit a forecast using improper channels, the sales manager is notified to educate how files are submitted correctly. When files are submitted, the Sales VP is automatically notified that a forecast is ready for review and approval. Any late submissions are automatically logged and managers receive a notification to contact the Sales VP for expedited handling or an exemption.

By avoiding delays or inconsistent submission methods, the Sales VP has a higher probability that the team will conform to company procedures for timely forecasting. Moreover, sensitive files are disclosed properly to avoid unnecessary risks.

Portable media is a necessary tool for today's business environment; however, some data must have additional safeguards. If a company employee wishes to transfer non-business data via FTP, send via email, or copy to CD, security controls are unlikely to be needed. For other classes of data, such as non-critical office documents, a user is allowed to copy data to company-approved media (official USB key, FTP, etc.) with only a notification that best practices recommend applying encryption—in some cases, an employee might avoid this step if data disclosure risk is low, such as sales PowerPoint (presentation) files. However, for specific data such as spreadsheets from the CFO office, technical plans from a CTO, a customer database, and so on, encryption is automatically applied to data while it is being copied, transferred or moved, with an appropriate notification that the user must be aware of special handling procedures.

While data mobility is an important part of business fluidity, it's important to set "speed limits" depending on how sensitive the data is to business. By selectively restricting the flow of sensitive data, a company can find a much needed balance between risk mitigation and efficient productivity.

Automate PII Disclosure to Limit Communications and Persons

- Automation Goal: For any content that is classified as a customer's Personally Identifiable Information (PII), require secure communication channels to be used along with restricted access by only "need to know" employees.
- Result: Only certain groups of authorized employees are free to handle information and disclose it securely to each other, avoiding leakage risks.

Openly being able to view and update customer files is necessary for professionals within healthcare, legal, finance, and so forth. However, not everyone within the same organization needs to access, handle, and disclose this data freely. Among those that should have access, as part of their job authorization, misuse and improper disclosure must be avoided. As such, a designated workgroup is assigned to handle specific classes of data—for example, only senior account reps can access, modify and distribute data contained in a customer record repository or, perhaps, any Excel files tagged as customer confidential, regardless of location. Furthermore, "senior reps" can only email files to each other by using encrypted email, using secure FTP, or transferring data to encrypted USB drives. Because of the high sensitivity, policies and procedures are enforced regardless of the employee's location, inside or outside the enterprise.

Within a workgroup, authorized teams will notice no change to their normal ability to handle data as they deem appropriate; however, when attempts are made to mishandle or disclose data in a manner that puts it at risk, improper methods are denied and automatic safeguards are applied for approved communication or distribution channels.

Prevent Outside Contractors from Downloading Customer Data

- Automation Goal: Outside consultants need the ability to handle company data; however, if there is no requirement to transfer this data outside the company, the risk of disclosure should not be allowed under any circumstance.
- Result: Whether due to negligence or specific abuse, any temporary, contract, or part-time employee cannot casually transfer data outside an organization.

External partners, contractors, and temporary employees can help deliver unique services or provide additional human resources as needed. However, risks can increase when non-trusted or low trust workers handle sensitive data. For employees identified as temporary or guest workers, such as an audit team or support personnel, a company may need to provide open access to sensitive data, but if it is modified or attempted to be copied for external distribution, disclosure must be explicitly prevented. A company must be able to selectively determine which employees and temporary workers are high risks, what data is deemed sensitive, and the precise set of activities that can be performed on the data, under specific conditions. When information is handled inappropriately, the user should be automatically warned; however, if explicit abuses occur, the company may want to prevent the actions, while silently logging and notifying internal investigators for remediation or auditing.

By allowing employees who have limited trust to work freely within defined boundaries, while enforcing explicit barriers when abusive or negligent activities are attempted, a company can monitor, report, and audit any activities that can harm business.

Prevent inappropriate access to Sensitive Product Data

- Automation Goal: Access to product designs (CAD files and parts specifications) on the corporate Product Lifecycle Management (PLM) system is restricted to users with the right project membership, nationality and location to ensure compliance with export regulations and corporate intellectual property mandates. Automatically rights protect product data that is exported from the PLM system to ensure compliance.
- Result: Users can continue to use the PLM system but are automatically denied access to sensitive projects. Exported product data continue to be protected. No manual intervention is needed, and risk of violation is reduced.

Increasingly, companies are designing products in global collaboration with their foreign subsidiaries, joint ventures, and partners. These collaborating parties need access to a common design platform, such as their PLM system. Companies need to ensure that users of their PLM system can productively use the system, but need to restrict access to design data in accordance with multiple security factors, such as their project membership, nationality and location. In addition, companies need to ensure that any exported product data will continue to be protected with rights management. Manually enforcing compliance would be impractical; it would require each user to request a product file, and wait for a manual review before getting access. In addition, relying on users to protect a sensitive exported product file is error prone.

By automating the enforcement, the PLM system can dynamically determine if a user request to access a sensitive product data is in compliance with policy, thus improving productivity and reducing risk. In addition, automatically rights protecting sensitive data improves compliance while reducing the burden on users.

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.