

7 Steps to information protection

7 Steps to information protection

Executive summary

Vulnerability, risk, and information protection challenges

Every organization is at risk of confidential information loss. Billions of dollars worth of profits, competitive advantage, reputation, and market share are at stake. Today's highly competitive business environment intensifies the vulnerability and risk. Global operations, with outsourced and off-shored business functions, spread the vulnerability. Tools for accessing and distributing information, such as the Internet and mobile computing devices, exacerbate the risk.

Information vulnerability and risk come from both malicious and unintentional disclosures by employees and partners; unintentional disclosures are usually the larger problem. Reducing these risks and vulnerabilities is now both a business imperative and a legal mandate as recent regulations impose obligations on organizations to protect certain types of information.

Global corporations and government organizations require more than network security and access control to guard their confidential data. They must protect the information itself, inform the behavior of those carrying the information, have visibility regarding where their confidential data resides on their network, have influence over where that data is going, and implement a policy for managing it. A strategy that balances the organization's legal and business needs to protect information with the competing interests to share it is vital.

7 steps to information protection

Information protection strategy best practices involve a cross-functional team that:

1. Assesses risks
2. Identifies and classifies confidential information
3. Develops information protection policies and procedures
4. Deploys technologies that enable policy compliance and enforcement
5. Communicates and educates stakeholders to create a compliance culture
6. Integrates information protection practices into businesses processes
7. Audits so that stakeholders are held accountable.

This paper reviews these seven best practice steps highlights the role of technology in achieving each one.

7 steps to information protection strategy best practices

Unlike the recent past, best practices now involve using technology to efficiently establish and reinforce each of the seven foundational building blocks of an information protection strategy. The sections that follow focus on the objective, the first step toward achieving the objective, and the use of technology to facilitate achieving the objective for each of the seven steps.

1. Assess risks
2. Identify and classify confidential information
3. Develop information protection policies and procedures
4. Deploy technologies that enable policy compliance and enforcement
5. Communicate and educate stakeholders to create a compliance culture
6. Integrate information protection practices into businesses processes
7. Audit and hold stakeholders accountable.

S
T
E
P
1

Assess risks of information loss and compromise

Objective:	Determine information protection strategy approach and priorities
First step:	Conduct a risk assessment and survey
Technology:	Use data loss prevention software to conduct a data loss risk assessment

A risk assessment and management survey starts the process of developing, updating or strengthening an information protection strategy and determining which approach is most appropriate for the organization.

Software tools allow an organization to determine where confidential information is located and how it is or might be accessed and transmitted electronically from the organization's network. The chart below summarizes the objectives of the risk assessment workshop or survey, and the software tools.

	Risk Assessment Workshop or Survey	Technical Risk Assessment— Software Tools
Objectives:	<ul style="list-style-type: none"> • Identify which information should be protected • Apply classification(s) to distinguish types of confidential information • Determine perceived risks and severity of information loss • Identify existing information protection policies, procedures and practices • Identify business processes that are perceived to create high risks of information loss • Determine awareness of incidents of information vulnerability, loss and compromise • Understand the organization’s risk tolerance • Understand priorities and preferences for resources, communications and tools that may reduce information vulnerability • Quantify and qualify the risk of confidential information loss 	<ul style="list-style-type: none"> • Locate confidential data on the network • Determine who has access • Demonstrate the flow of information internally • Provide evidence of information being sent by and to unauthorized users • Identify business processes that may cause information loss • Document at-risk confidential data • Quantify risk of non-compliance • Provide a record of information flow from inside the network to outside the network

A cross-functional information protection team works most effectively to synthesize the results of the risk assessment, management survey and software risk assessment tools. The team typically consists of representatives from Legal, IT and Corporate Security, with involvement from representatives of business units, such as Research and Development, Marketing and Customer Engineering, and representatives from Compliance, Human Resources, Corporate Communications, Audit, Competitive Intelligence, or Risk Management, among others, depending on the contribution that they can make to the priorities of the information protection strategy.

The three products of a risk assessment—risk assessment and survey results, the report of results from the technical risk assessment, and the team’s syntheses and recommendations—provide the basis of a compelling presentation that will help executives understand the need to invest in an information protection strategy.

Given rapid changes in the types of information that bring value to an organization, advancements in technologies that put information at risk, and collaborative working relationships that put those risks in the hands of individuals around the globe, most companies benefit from conducting an annual risk assessment.

S
T
E
P

2

	Define confidential information and assign appropriate levels of protection to it using classifications
First steps:	• Update information classifications based on best practices • Identify confidential information • Apply classifications
Technology:	Use software to locate, automatically label, and enforce procedural requirements associated with each classification

Identify and classify confidential information

The second fundamental building block of any information protection strategy is the determination of which information is worthy of what type of protection, and which information must be protected by law. This can be achieved by defining and applying information classification categories. For information classification best practices, see http://www.pro-tecdata.com/consulting/consulting_classif.php.

Technology is available to discover, monitor, enforce, and prevent information sharing based on the organization's information classifications. Best-of-breed products are policy driven and can effectively implement and reinforce information classifications for electronically stored and transmitted information. Software tools can establish varying degrees of protection according to the procedural requirements associated with each data classification.

One procedural requirement that is common to all classifications is applying a notice, such as "Company Confidential", to confidential information. Automated tools ensure that confidential materials in electronic form are identified with a notification stating their appropriate classification.

Develop information protection policies and procedures

	Develop policies and procedures that define responsibilities for protecting confidential information
First steps:	<ul style="list-style-type: none"> • Compare existing company information protection policies to best practices • Develop policy updates based on best-in-class policy models
Technology:	Use pre-packaged and configurable policy templates to create policies for automated tools

An overarching information protection policy statement summarizes the organization's commitment to protecting confidential information, including personal and private information and confidential information received from third parties that is subject to a nondisclosure obligation. This policy typically references other policies and procedures, such as the policy defining each of the confidential information classifications, and the applicable protection procedures.

Best practice information protection policies and procedures address unique audiences and subjects. For example, most companies have one policy or procedure that addresses both employee and management responsibilities for protecting confidential information. A different policy or procedure may address the treatment of information based on its classification while yet another policy may describe the information security protocols on the organization's network.

Automated policy builders create policies to take advantage of software tools that contribute to policy compliance and enforcement. These software tools:

- Protect data wherever it is stored or used
- Discover and protect confidential information exposed on file servers, databases, Microsoft® SharePoint®, Lotus Notes®, Documentum®, LiveLink®, web servers, Microsoft® Exchange, end-user laptops and desktops, and other data repositories
- Discover and inventory confidential data stored on laptops and desktops and prioritize high risk endpoints for additional protection
- Monitor and prevent data loss on the network including email, IM, Web, Secure Web (HTTP over SSL), FTP, P2P, and generic TCP
- Monitor and prevent confidential data from being copied to USB, burnt to CDs/DVDs, downloaded to local drives, attached to network transmissions, or encrypted or concealed using high risk applications
- Automatically enforce policies.

Policy builders provide configurable, pre-built templates that are based on compliance requirements, industry best practices and acceptable use standards. Once these policies are in place, you can use the software tools to measure risk reduction, demonstrate compliance, and automate remediation.

STEP 4 enforcement
Deploy technologies that enable policy compliance and automatic

	Adopt and deploy technologies that enable policy compliance and automatic enforcement
First steps:	Review current technologies and assess the costs and benefits of options
Technology:	Use software to enable, enforce, and reinforce appropriate storage and use of confidential information

A policy without compliance and enforcement is dangerous. Lack of policy enforcement degrades policy credibility both in the eyes of those responsible for compliance and in the eyes of the law. One organization that prided itself on the policies developed by its information protection team was stunned to discover that their policies were used by opposing counsel as evidence of a failure to protect information in a trade secrets case. Opposing counsel was able to argue that the organization’s information protection program was “confused and confusing at best” since the rather strict organization policies had not been enforced.

Technology solutions do more than enable policy compliance and enforcement; technology can alter user behavior. In the same way that people tend to become more vigilant when they know that they are being recorded by a camera or audio recorder, we become more vigilant about protecting information when we know that technology is keeping track of what we are doing with it.

Security access controls, authentication software, encryption, DRM, and firewalls are some of the technologies that provide the IT security infrastructure that protects organization information.

Monitoring software is a technology that can enable, enforce and reinforce the appropriate behavior of users. For example, monitoring software can be used to keep track of where, when and how insiders transmit confidential information. The software can enforce policy compliance by preventing the transmission of confidential information by certain users to other users, to an Internet web site, or to a competitor.

One software solution, such as that offered by Vontu (see <http://www.vontu.com>), combines endpoint and network-based software to prevent wrongful disclosure of confidential information while automatically enforcing data loss prevention policies wherever data is stored or used.

Using technology is important for both business and legal reasons. From a business perspective, technologies can ensure that protections are applied consistently and effectively. It takes only one loose lip to sink a ship and it takes only one confidential product plan sent to a competitor to turn an organization's success into failure. Technology solutions are available to reduce the risk of these calamities. Most leading organizations rely on technical security precautions to prevent or reduce many of their significant information loss risks.

As the use of technologies becomes a recognized best practice, it is emerging as a legal requirement for establishing reasonable measures to protect trade secrets. If an organization cannot meet the requirement of demonstrating "reasonable measures", the organization will have no legal recourse in the event that their information is lost, stolen, or compromised.

5 Communicate with and educate stakeholders to create a compliance culture

	Inform employees and stakeholders of their responsibilities to protect information; motivate information protection behavior
First steps:	• Draft key messages • Develop training • Establish an ongoing communication campaign
Technology:	Use technologies that provide notification of information protection policies and reinforce the communication campaign

Technology contributes significantly to information loss prevention in large part by ensuring that information is accessible only to authorized users and that, when authorized users share that information electronically, they do so according to organization policy. No amount of technology security can perform the entire job. Information security technology is only effective in a corporate culture where users take personal responsibility for protecting the organization's valuable intellectual assets.

Best practices for communication and education that create a compliance oriented culture focus on both content and process. The message to employees and stakeholders must be clear: protecting information is everyone's responsibility. Failing to fulfill that responsibility could destroy the organization.

Education and training must teach stakeholders how to fulfill their responsibilities, from classifying confidential information to collecting it from customers at the conclusion of project meetings. Training must also familiarize users with the information security tools and technologies that will help them fulfill their information protection responsibilities.

Even annual training will not likely keep pace with information risks and opportunities for reducing those risks. An information protection awareness communication, such as a monthly bulletin that highlights specific risks and provides tips on reducing those risks (see <http://www.pro-tecdata.com/iptips/index.php>), keeps information protection top-of-mind.

Training and ongoing awareness communications are essential to creating a corporate culture that respects and protects confidential information. Yet nothing is more effective than a reprimand immediately after one has inappropriately shared information. Technology that instantly notifies the user, at the time that he or she violates a policy, delivers a powerful message of deterrence.

STEP 6 Integrate information protection practices into businesses processes

	Make information protection integral to the way the organization operates and does business
First steps:	<ul style="list-style-type: none"> • Identify key business processes where information is at risk • Develop a plan for integrating appropriate information protection practices into those processes
Technology:	Use software to enforce business process re-engineering for information protection

Both a goal and a result of applying information protection best practices is that they become integrated into the operations and business processes of an organization. Information protection procedures should not burden employees, most of whom have an already full work load. It would be futile to expect consistent and comprehensive information protection if information security is the extra step that gets in the way of what needs to be accomplished.

Instead, the organization's stakeholders should operate in a culture of compliance, where protecting information is integral to every aspect of the business, including researching potential new products, developing marketing plans, analyzing financial reports, making sales calls, selecting facilities, manufacturing products, procuring supplies and interviewing job applicants. The procurement department should consider purchase orders incomplete until the vendor has signed a nondisclosure agreement. Software should automatically prevent project plans from getting through the organization's network to a competitor.

Broken business processes often create the highest risk of information loss and compromise. In one software organization, every engineer had access to every line of code for every project. Simple access control software can be used to change a business process that makes the organization's crown jewels vulnerable. Monitoring technologies are available to ensure automated integration of information protection procedures into the work flows involving electronically stored or transmitted data.

Audit and hold stakeholders accountable

	Examine current practices and remediate deficiencies
First steps:	• Establish audit parameters and methodology • Conduct audit to assess compliance with information protection procedures and practices
Technology:	Use automated monitoring and auditing tools

The purpose of the audit is to ensure that the information protection procedures and practices adopted by the organization are being implemented consistently and effectively. Once the core infrastructure of an information protection strategy is in place, an audit determines if the intentions behind each of the information protection initiatives has been successfully carried out.

In one recent audit, an organization discovered that photographs of its manufacturing facility were available on the Internet despite its policy prohibiting photography in any of its manufacturing sites. After an investigation, the audit group discovered that camera phones were not only allowed in the facility, but that the organization was issuing camera phones as standard cell phones to its employees. Once this inconsistency was revealed, the audit committee was able to recommend corrective action.

Technology enables another kind of audit. Specifically, discovery and monitoring software allows an organization to keep track of who is sending what to whom electronically, and when and where that material is sent. This kind of tracking provides valuable audit reports:

- Benchmarking risk reduction trends over time, at the SBU or department level
- Compliance reports addressing Sarbanes-Oxley, GLBA, HIPAA and other legal obligations
- Incident reports with detailed information for investigations, classifying each incident by level of severity, to drive enforcement and remediation.

Discovery and monitoring software also helps an organization determine the effectiveness of its policies and training. An initial technical security risk assessment of a telecommunications organization indicated that information was being transmitted to unauthorized users on a regular basis. Following the risk assessment, the organization developed a policy, mandated information protection training, and implemented monitoring software, to keep track of their highly confidential information. The telecommunications organization then conducted an audit. The results of the audit showed that, while the monitoring software was effectively preventing employees from sending confidential information to unauthorized users, employees continued to attempt to send confidential information inappropriately.

It is not sufficient to rely on technology to prevent information loss. An employee who does not respect and protect information will likely put it at risk by sharing it in hard copy, verbally, or in some other manner, even if the technology to prevent unauthorized electronic transmissions is in place.

The function of the cross-functional, interdisciplinary team is to ensure the effectiveness of the organization's information protection strategy, in part by using technology as a tool to enable effective information protection.

Contact us for more information or assistance.