Maximizing the value of a data protection program

Insights on governance, risk and compliance

June 2014
The rising costs and increased media coverage of data breaches and the continued escalation of threats facing organizations has led to information security, particularly data protection, being discussed at the highest level. Boards and audit committees are expecting their information security functions to proactively report on the capabilities, maturity and effectiveness of their data protection activities.

Whether an organization's business risk relates to the protection of customer data, proprietary information or intellectual property, implementing technology forms only part of the solution designed to prevent, detect and respond to data loss events. Technology implementations can be costly and many organizations complain they have not seen the value of data protection tools demonstrated after implementation. Too often, information security functions struggle to make effective use of data protection tools, and expensive products turn to shelf-ware.

EY has worked globally with clients to help implement data protection programs, and we have consulted with many organizations after data protection technology implementations to help them realize better value from their investments. Common mistakes that organizations make include:

- Viewing data protection as a technology problem and not involving the business
- Protecting all information with the same controls
- Not engaging users in data classification and data protection processes
- Investing in specific capabilities while ignoring other immediate risks
- Focusing disproportionately on prevention controls and not investing enough in detection and response capabilities
- Not customizing processes and technology for their environment
- Forgetting about maintaining technology and processes after the initial setup

Our goals with this report are to share insights and lessons learned from our experiences, and to help organizations maximize their technology investments by following four key steps:

1. Building a data protection program that is aligned to the business
2. Implementing an effective program structure
3. Spending time, energy and money protecting the data that matters most
4. Changing the business culture and measuring performance to achieve sustainability
Understanding your business is the foundation of an effective and efficient data protection program.

Technology implementations often fail to deliver their promised benefits because organizations do not configure the tools to protect the information within the organization that is truly valuable. With limited resources to configure and manage tools, organizations must ensure that time spent monitoring the movement of information in and out of their environment is focused on the information that matters most.

Understanding compliance requirements and business drivers

There are two common drivers for data protection programs:

1. Complying with legal, regulatory or industry compliance requirements to protect specific data types, such as credit card numbers and national identification numbers
2. Protecting data that is essential to the organization’s ability to win in the marketplace (e.g., intellectual property, trade secrets, proprietary information, and merger and acquisition plans)

There are several types of regulatory and compliance requirements related to data protection; this includes industry-based regulations and laws, which require the protection of certain types of personally identifiable information (PII). While many of these regulations are subject to interpretation on the details of what types of technical controls are required, all regulations require these types of data to be protected from inappropriate access or disclosure.

Organizations in regulated industries, such as health care, financial services and retail, are implementing data loss prevention technology and other technical controls to protect PII. Additionally, many organizations have contractual agreements in place with customers and business partners, which require specific data protection controls to be in place; for example, many financial services organizations now require vendors to implement data loss prevention technology to monitor and prevent sensitive data from being transmitted through unencrypted channels such as email.

Data protection life cycle

Starting with understanding the business and designing protection and monitoring controls based on this knowledge helps to focus the data protection program on the data that matters most.
Data protection in a globally collected world

The privacy regulatory landscape is changing rapidly and many organizations are unprepared. For example, a new European Commission pan-European data protection regulation will replace the current Data Protection Directive (95/46/EC (1995)) and its 32 local implementations. The final regulation is likely to strengthen the rights of data subjects and impose increased fines. Other proposed aspects of the new regulation include giving individuals the “right to be forgotten,” requiring that explicit consent be obtained before processing personal information, and the requirement that every organization processing personal data of more than 500 persons appoint a data protection officer.

Just as the EU seeks to improve its data protection regulations, in the Asia-Pacific region, the Asia-Pacific Economic Cooperation (APEC) organization has developed a voluntary, certification-based system. Known as the Cross-Border Privacy Rules (CBPR) system, it enables organizations doing business in the 21 participating APEC countries, which includes the US, to establish a consistent set of data privacy practices.

As regulators around the world seek to bolster requirements for privacy program accountability, the differences among regulations continues to diminish. This is good news for organizations seeking to develop encompassing privacy programs that achieve accountability, governance and monitoring objectives. This comprehensive approach addresses a wide range of compliance requirements rather than focusing privacy efforts on specific, jurisdictional regulations.

Business leaders can help prioritize the types of information that are most valuable to the organization, such as:

- **PII for individuals**
  - Names, addresses, email addresses, phone numbers and demographic information
  - Social security numbers and other national identifiers
  - Banking information and credit card numbers
  - Personal health information (PHI)

- **Intellectual property**
  - Product designs
  - Source code
  - Pending patents
  - Formulations
  - Manufacturing process instructions and procedures
  - Research and development results and analysis
  - Exploration data
  - Scientific papers

- **Proprietary information**
  - Customer lists
  - Pricing, cost and sales information
  - Pre-released financial results
  - Merger and acquisition information
  - Third-party contracts
  - Strategy and product roadmaps
  - Bid plans

Gaining an understanding of the data that matters most may sound simple, but being specific is the key to success. Data owners often speak in general terms about the data they believe should be protected, such as by responding that all source code or product designs are sensitive. However, is the design of a product that has been on the market for five years really as valuable as a cutting-edge product in the early stages of the product development cycle?

Thinking like an outsider can help to highlight types of information that are most likely to be targeted. Here are examples of questions that should be discussed with data owners:

- What data would hurt us the most if it fell into the wrong hands?
- What information gives us competitive advantage in the market?
- What data would someone want to steal?
- What knowledge makes us better than our competition?
- Where are we investing in research and development?
- What would we be very embarrassed to lose?
- What data would trigger compliance requirements?
Enabling the data protection program with an effective structure is an important step in making sure the right stakeholders are engaged in a productive way.

Below are two examples of program structures that illustrate the ways different structures can be effective for different types of organizations:

- For organizations focused on protecting personally identifiable information, a top-down strategy and approach, which involves working with relevant departments such as the legal, compliance, internal audit and privacy functions to determine which types of data need to be protected may be sufficient. Workshops with key stakeholders in each relevant part of the business can be used to gain consensus and develop a prioritized strategy for protecting sensitive data.

- By contrast, organizations focused on protecting intellectual property, proprietary information or other unique datasets, should develop a top-down strategy and data protection governance framework supported by a bottom-up program for engaging business unit leaders in classifying data generated in their functional areas. Engaging the right level of stakeholders within the business units is critical, and it is imperative that consistent guidance, training and enablers be provided to the business.

Successful programs generally require:
- A centralized governance model
- A global program framework (policies, procedures and guidelines)
- Centralized support of the technology solutions employed
- Centralized event triage and response
- Documented processes for event escalation and workflow
- Business unit ownership of data classification activities
- Business unit engagement to provide data protection requirements and to respond to identified events

Don’t fall in love with tools – support technologies with effective processes and people

A common mistake in data protection programs is assuming that technology will be a magic bullet. Often tools are configured and left to the IT department to manage, forgetting that the business, not IT, has the knowledge needed to appropriately classify and assign risk to incidents.

The most successful data protection programs have well-designed processes with both IT and business resources assigned. IT can manage the tool and provide basic incident evaluation, forwarding incidents to the appropriate business unit for investigation and resolution.

Business process leaders evaluate incidents, assign the risk rating based on the sensitivity of the data exposed and lead corrective activities.
Create a data classification framework that enables users to identify, label and protect sensitive data

Most organizations have some type of data classification policy in place. However, a significant percentage would readily admit that their classification policy is nothing more than a piece of paper, and that their classification guidelines are not reflected in the behavior of users.

Many organizations have created policies that define classification levels in generic terms but without additional guidance, these policies are often misinterpreted. Mapping specific datasets or data types to the classification levels established is critical. It is important to provide clear direction about the types of data that belong in the highest (and most sensitive) classification levels to avoid over classification.

A data classification framework consists of several components, including:

1. **Data classification policy** defines the scope, responsibilities, and other governance requirements within an organization to effectively manage the implementation of varying levels of data protection for different types of information.

2. **Data classification scheme** determines the tiers of data and associated levels of protection and describes each level in terms that are meaningful to the organization.

3. **Data labeling guidelines** give instructions for labeling information (most commonly files and folders) in a way that makes it easy for users to visually determine the classification level of a document and enables automated tools, such as data loss prevention (DLP) systems, to programmatically identify sensitive documents and protect them accordingly.

4. **Data handling guidelines** provide specific requirements for protecting data according to its classification level. For each classification level, data handling guidelines define how data must be stored, transmitted and processed.

5. **Data classification mappings** can be used by data owners to link datasets or data types to classification levels. These documents explain to a particular business unit, team or project, what types of data are considered sensitive and are useful in both providing guidance to the support teams that manage data protection technical controls and providing guidance to the users that work with the relevant information.

Implement a data classification scheme that fits the business

There is not a one-size-fits-all approach to data classification systems. The number of data classification levels which are appropriate depends on the type of organization and the data protection strategy.

In practical terms, data classification focuses on:

- The most sensitive data – data that would cause great harm to the organization if inappropriately disclosed
- Unrestricted data – data that can be shared and does not carry control restrictions
- Data in between with a range of sensitivity

The data in between really determines how many classification levels are appropriate. Three-, four- and five-tier classification systems are common. So which is the right answer? As usual, it depends on the circumstances, but each classification level should have unique handling guidelines and protection requirements. A key point to remember is that if you are not going to treat the data differently, there is no reason to have different levels.

It is common to see organizations focused on protecting PII and meeting regulatory requirements implement three- or four-tier systems. Five-tier systems are common in industries that produce intellectual property such as the technology, chemical, manufacturing, and oil and gas sectors.

The following data classification case study illustrates an example of a four-tier classification system.
Important tip: use colors along with words

In the example classification scheme shown above, you will notice colors used instead of words to express the classification levels. Many organizations are implementing color-based schemes because they help users differentiate between levels. Terms such as “Secret”, “Restricted”, “Classified”, “Critical”, “Confidential”, “Proprietary” and “Private” can all mean the same thing in their simplest forms – that they are not for public consumption. However, these terms, and others frequently used, can be misinterpreted by users, while the color schemes are easy to understand and distinguish.

Additionally, embedding the color in document labels along with the words can help automated systems such as DLP more accurately distinguish between true classification labels and uses of words such as “Confidential” in documents.

**Classification level** | **Description** | **Example data types**
---|---|---
**Red** | Highly sensitive information, which must be restricted to only authorized individuals. | High-value intellectual property (e.g., new product formulations, process design, source code and engineering information) which should not be shared with any third parties. Protected PII such as SSNs, credit card numbers, combinations of names and addresses.

**Yellow** | Sensitive internal data, which must be restricted to only authorized users and approved third parties. | HR data, payroll data, internal memos, business plans, operational procedures, sales and contracting information.

**Green** | Non-sensitive internal data. | Individual test results, raw test data and process diagrams for commonly available products or technology. Aggregated/sanitized personal information.

**White** | Information suitable for public release. | Marketing materials, job postings, published financial reports.

Data labeling tools allow or force users to select the appropriate classification level of a document when it is created or saved; these tools apply a visual label and a metadata tag to a document. Data labeling tools are also used to classify emails, which can feed other security tools to prevent sensitive emails from being transmitted to non-approved devices and recipients.

**Metadata tags:** Metadata tags are normally not visible to the user and are applied by a data tagging tool by inserting special information into the metadata of a file. While these types of tags do not promote user awareness, the metadata tags allow automated solutions to accurately identify the document or message's classification level. Tags can be manually applied, selected when saving a document or automatically applied by security solutions based on location, keywords or other factors.

**Effectively use labels and tags**

Data labels and tags are the building blocks for effectively classifying data, which can then be used to improve user awareness, measure compliance and enforce policies automatically. Labels and tags are used to clearly identify a document's classification level.

**Labeling and tagging methods:**

![Visual labels](image)

**Visual labels:** Visual labels are markings in a document that are applied to the document's cover pages, headers, footers, and background (watermark). An example could look like: [Top Secret (RED) Do Not Distribute].

**Keep data classification mappings current**

The value of data can change over time, especially for organizations that produce intellectual property, perform research and development and execute frequent, sensitive financial transactions. While certain closely guarded secrets maintain their value (think of the formulation of your favorite soft drink), many others lose value as time passes (like the source code for your first computer’s operating system).

**Data owners** – the business users that create and monetize information – must keep data classification guidance up to date, or gradually too much information will be marked as sensitive, reducing the program’s effectiveness. Changing classification levels on data sets is expected: it keeps users engaged in the classification process and it keeps the focus of the data protection program on the data that matters most.
Document and assign key roles and responsibilities

All users within an organization and relevant third parties that are provided access to data have a role to play in data protection. Key responsibilities should be documented to avoid confusion and help provide clear accountability.

Responsibilities that should be defined include:

- Writing, reviewing and approving data protection policies, procedures and standards
- Providing training
- Defining high risk data and communicating handling requirements to the data protection program and data handlers
- Classifying sensitive data as it is created and updated
- Designing security technology solutions to protect the movement, storage, and processing of data
- Configuring and maintaining data protection technology
- Monitoring technical controls and alerts generated by data protection systems
- Validating alerts and escalating events as appropriate
- Responding to escalated events and policy violations
- Keeping up to date with regulations and privacy laws
- Reviewing contracts and facilitating non-disclosure agreements (NDAs) with third parties to validate appropriate data protection clauses and audit rights are included
- Conducting independent reviews to validate compliance with security policies and procedures
- Providing metrics and reporting to stakeholders to allow for increased awareness, evaluation of program effectiveness and continuous improvement

Data protection should be a business-wide focus

The people responsible for providing data protection controls are normally not the people generating the data that is most valuable. Without effective communications between the business, other stakeholder groups and IT, the data protection program’s chances for success are minimal.

Involving users in data classification, asking the right questions to the right people, and establishing roles and responsibilities are all critical steps in creating a sustainable data protection program.
Once the data that is most valuable to the organization is understood, IT can select and target controls to apply more protection to this information. While certain controls, such as firewalls, provide a level of protection across the enterprise, other data protection controls, such as DLP technology, should provide targeted protection for only sensitive data.

Organizations should adopt a strategy that fits the unique needs of the business; for example, organizations with very mobile workforces and sensitive data contained in many unstructured files and systems, should place high importance on endpoint and mobile device controls, such as hard drive encryption, mobile device management and external media control.

Furthermore, the types of sensitive data that must be protected should be considered in the overall data protection strategy.

Organizations focused on protecting predictable and consistent data types, such as PII (e.g., credit card numbers, national identifiers, bank account routing numbers), can achieve significant risk reduction quickly using built-in policies in DLP.

In contrast, built-in DLP policies are not as helpful to organizations focused on intellectual property protection: for these organizations, DLP systems cannot accurately detect high risk data unless data classification processes have been implemented with visual or metadata labels.

All organizations should be aware that privacy regulations and requirements could hinder their desired security approach; e.g., security tools that monitor the use of the data by authorized users can trigger privacy concerns and can be delayed, limited or stopped by regulators, unions and works councils.

The model below illustrates focus areas for mitigating the risks of data loss.

EY's data protection control model

Data governance

| Policies and standards | Identification | Risk assessment | Classification | Architecture | Quality |

Data protection controls

Data in motion
- Perimeter security
- Network traffic monitoring/blocking
- Web content filtering
- Data collection and exchange
- Messaging (email, IM)
- Remote access

Data in use
- Privileged user monitoring
- Workstation restrictions
- Application controls
- Data labeling/tagging
- Removable/external media control
- Export/clipboard/print control

Data at rest
- Encryption
- Obfuscation/tokenization
- Mobile device protection
- Network/server repository control
- Physical media control
- Archive, disposal and destruction

Data in use

Structured data

Unstructured data

Detect and prevent inappropriate transfers of sensitive data from the internal network to the internet

Data-in-motion refers to data in transit between systems, such as between a user’s computer and an external web site.

The key objectives for protecting data in motion include:

Ensuring authorized transfers of sensitive data are appropriately encrypted

Users should be provided with the ability to encrypt sensitive data using approved methods; this will allow for secure transfer of sensitive information to authorized third-party recipients. Ideally, organizations should provide users with encryption technology that can be decrypted by the Information Security function to validate that the technology is used for valid business purposes. Organizations should consider blocking...
non-authorized forms of encryption, particularly encrypted file containers such as ZIP and RAR files, as a means of preventing data exfiltration. Additionally, regular transfers of sensitive information through automated processes to third parties should be encrypted.

- **Detecting and preventing sensitive data loss events**
  Use technology, such as DLP technology, to detect and prevent sensitive data from being sent externally using insecure methods. DLP technology can be used to force encryption for sensitive data or to prevent specific content from leaving via Internet communications such as email, web sites, and file transfers. There are many ways to configure DLP policies to detect sensitive data — remember to focus on the data that matters most to the organization.

- **Using content filtering and firewalls to block high risk sites and services**
  Organizations should carefully evaluate and control network egress. Systems such as proxy servers and firewalls can be used to prohibit users from accessing known malicious sites, file sharing sites and personal email services. Additionally, applications such as instant messaging tools, or specific components of websites such as Facebook messaging, can be blocked. Organizations should also consider blocking access to sites and applications that allow encrypted data exfiltration, such as file sharing sites that are not authorized for business use.

### Controlling the cloud

Adoption of cloud-based services presents challenges when trying to use data protection and security technology. In the past, information security solutions have relied on the use of on-premise solutions for monitoring data in motion and protecting data at rest. As more services and data storage move to the cloud, this architecture is no longer viable in many cases.

Using cloud-based email providers demonstrates the problem of getting DLP technology in a position to be able monitor or remediate improper data transmittal. In cloud-based email environments, typically an additional network route must be configured to capture the data for DLP technologies. The data must be sent from the cloud provider back to the internal network to utilize DLP technology; this can add latency and cost to the process while diminishing some of the benefits of using cloud providers by having to route the traffic through the datacenter.

In this rapidly emerging area, cloud to cloud DLP technology, DLP as a managed service, and improved capabilities to support DLP functionality within cloud email and storage offerings, are all helping to address these challenges.

Information Rights Management (IRM) products have also advanced significantly and can provide an effective mechanism for protecting unstructured data regardless of how it is transferred or where it is stored. Files such as Microsoft Office and PDF files can be encrypted and protected by IRM solutions, enabling security controls to move with the files. These tools can be used to: revoke access to users who no longer require it; prevent unauthorized users from accessing the content; track the locations where files have been accessed; prevent copying, pasting and printing; and offer other powerful features.

In an age of borderless IT environments, this type of portable security architecture will provide more and more value.
Identify and secure data at rest

Data at rest describes data stored on disk: it includes both structured data stored in databases and unstructured data, such as Microsoft Office files, stored on file servers, network shares and collaboration tools.

Effectively managing data at rest requires addressing data whether it is stored in structured repositories, unstructured repositories, and on workstations, servers and mobile devices.

An effective data at rest program should:

- **Develop and maintain an inventory of high risk data repositories**
  It is difficult to protect information without understanding where it is, where it should be, and where it should not be. Organizations should maintain an inventory of data repositories and systems, including applications, such as SAP, and unstructured repositories, such as network file shares. The inventory should document repositories where sensitive data is authorized for storage and locations where sensitive data is often is, but should not be, stored. Non-production systems should also be considered if they contain production data or intellectual property.

- **Actively scan common repositories to identify sensitive data stored in unprotected locations**
  Users often save sensitive documents to publicly accessible file shares for convenience and for collaboration with users in other departments. Sensitive files in these accessible locations should be regularly identified and moved to secure locations. Users should be trained to use secure methods of collaboration; remember that it is important for secure, user-friendly collaboration methods to exist, or users will develop their own methods for collaboration.

- **Establish data owners for sensitive data repositories and data sets**
  Analyze data access and usage to determine the users who regularly create and access sensitive information. Use this information and gather business stakeholder input to establish accountability for classifying data sets, reviewing and approving access to sensitive repositories, training data handlers, and promoting a culture of data protection.

- **Carefully manage access permissions for secure data repositories**
  Whether data is stored in databases, applications or unstructured systems, if the location is approved for sensitive data storage it is vital that access is regularly reviewed and approved by data owners to ensure that access is limited to authorized individuals with a business need-to-know. Additionally, provisioning access to these systems and repositories should be appropriately managed. Do not forget that “read only” access is just as important as “write” access when it comes to protecting the confidentiality of information.

- **Encrypt sensitive data stored on all devices, which can be taken off-site**
  Mobile devices, workstation hard drives, removable media and backup tapes should be encrypted if these devices can be removed from the organization’s facilities.

- **Remember about structured data**
  While certain end user computing applications, such as Microsoft Office products, are prevalent, it is also common for sensitive data to be stored in structured databases and applications. Having data owners provide information about the structured repositories and applications that contain this information will help to avoid missing weak points for data leakage. For example, it is common within the chemical industry for sensitive intellectual property to be stored in ERP systems. Forgetting these systems and focusing only on unstructured data repositories can result in gaps in data protection program coverage.
Control endpoints, including workstations and mobile devices

- **Implement endpoint/host DLP software**
  Endpoint DLP software provides the ability to control egress through removable media and printing. Additionally, endpoint agents can track sensitive content, even if files are compressed, encrypted or accessed through applications such as web browsers; this provides the ability to control data uploads to encrypted websites.

- **Evaluate applications to identify unnecessary data extraction features**
  Many applications provide “export,” “save” and “reporting” functions that allow users to perform mass extracts of information from the underlying database. Organizations should be aware of these capabilities and should restrict these functions for users that do not require them to perform their job responsibilities.

- **Limit user privileges on workstations**
  Controlling endpoint privileges can significantly reduce the risk of data loss. Blocking access to unnecessary peripherals and media is an important consideration for organizations without endpoint DLP. Additionally, removing local administrator rights on workstations is a critical step in defeating advanced malware and preventing lateral movement within a network. Many organizations are now implementing temporary privilege escalation tools to allow users to obtain elevated permissions only when needed.

- **Promote strong controls for mobile devices**
  Mobile devices can be significant vectors for data loss. Native functionality on many mobile devices do not provide adequate security features to protect sensitive information. Mobile device management (MDM) software can enforce strong password controls, detect if the mobile device has been “jailbroken,” and provide secondary authentication and encrypted containers for sensitive business applications.

Organizations should take a comprehensive look at data loss risks to differentially invest in the right areas

It is expensive to deploy the most advanced technologies and the most mature processes in every business area. Understanding the external threats that face the organization, identifying potential motivations for malicious insider activities, listening to feedback from the business, and benchmarking against peers can help to prioritize investments. However, a single weakness can be exploited to cause a significant data loss event; as a result, organizations must take a balanced approach to managing risks to provide a solid foundation across the board while developing advanced capabilities in strategic areas.
Fix broken business processes

Effective data protection controls often lead to the identification of broken business processes; examples include: HR departments exchanging benefits enrollment data with third-party benefits providers through unencrypted email; the use of insecure protocols, such as telnet, for application access; and users emailing sensitive files to their personal email addresses to work from home on the weekend. By identifying the root causes associated with data protection issues, broken business processes can be identified and remediated. Identifying these types of processes and practices can be a quick win associated with DLP technology deployments and can significantly reduce the risk of data loss for organizations.

Involves the business in incident response

Business stakeholders have a significant role to play in incident response. When data loss incidents are identified, appropriate stakeholders should be engaged to provide effective and efficient management of incidents and to help ensure compliance obligations related to breach management are met.

Additionally in day-to-day operations, the individuals responsible for reviewing alerts generated by security tools may not have the business context to accurately classify and assess the severity of a potential incident, so structured processes for escalating events to stakeholders and data owners for review should be in place to:

- Allow stakeholders to provide input to whether or not events are truly incidents that require action
- Take over the handling of a validated incident when appropriate
- Own remediation activities to address broken business processes and correct identified issues

Build a culture of data protection

Organizations that implement data protection technology and processes learn a lot about the behavior of their users, compliance with information security policies, data flows within the organization, and the interaction between internal groups and third parties. The knowledge gained through these processes should be used to help improve security awareness and policy compliance.

Methods for using this knowledge to improve the culture include:

- Providing targeting training to policy violators when data loss events are detected
- Embedding “lessons learned” and real examples into onboarding training for new hires and annual refreshers
- Disciplining users for malicious activities or repeated negligent practices
- Studying incident trends to provide organization- or department-wide training to address common problems
- Sending communications to user communities to highlight problem areas and relevant policies which are frequently violated
- Reporting incident metrics by user groups to executive leadership to highlight groups that require improvement
How do I know if my data protection program is working?

Establishing meaningful metrics provides an organization with the ability to be able to measure the effectiveness of its data protection program.

It is important to determine which information provides actionable information that can help improve user awareness, event response processes, policies and mitigating controls. Example metrics are provided in the table, at right.

Report to the business and continually improve

Metrics should be reported to the appropriate data protection governance body; this group should include business unit representatives and stakeholders from groups, such as internal audit, legal, compliance and HR functions. Business leaders can use the metrics to improve user awareness in their teams, provide guidance for policy improvements and give feedback on the overall value of the program. Trend analysis should also highlight the improving nature of the program; examples include: demonstrating the reduction of DLP false positives, the reduction of accidental data leakage events over time, and increases in the percentage of labeled or classified unstructured documents.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trainable events by group</td>
<td>For a given period of time, the number of non-malicious DLP events that required providing instructions and/or point in time training to a user.</td>
</tr>
<tr>
<td>User awareness level</td>
<td>After each training session, the percentage of employees who did not pass testing on the training content.</td>
</tr>
<tr>
<td>Events by root cause</td>
<td>The number of incidents by root cause type over a given period of time. Common root causes include improper data classification, auto-generated business reports not reviewed by appropriate personnel, inadvertent disclosure, transferring sensitive data over unsecured communication channels, etc.</td>
</tr>
<tr>
<td>Top policy violators (by individual or group)</td>
<td>For a given period of time, identify the individuals and/or groups that generated the highest volume of validated DLP events.</td>
</tr>
<tr>
<td>Resource utilization</td>
<td>For the prior month, the total number of hours spent on data protection event handling divided by the number of working hours per week.</td>
</tr>
<tr>
<td>Incident handling efficiency</td>
<td>For a defined period of time, the average time required to investigate and resolve an incident.</td>
</tr>
<tr>
<td>DLP event volume</td>
<td>By month, the list of all validated events for the previous 12 months, by policy or rule.</td>
</tr>
<tr>
<td>Regulatory compliance level</td>
<td>For a given period of time, the number of incidents by regulatory compliance requirement (e.g., PCI, HIPAA, etc.)</td>
</tr>
<tr>
<td>Data classification trends</td>
<td>For specific file types (Word, PowerPoint, Excel, PDF, etc.) the percentage of detected files that contain the organization's data classification labels.</td>
</tr>
</tbody>
</table>
### Business value

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifies needs for prioritized training; targeted training can be provided to groups and departments with high event rates.</td>
</tr>
<tr>
<td>Evaluates the effectiveness of data protection training materials and delivery.</td>
</tr>
<tr>
<td>Identifies significant reasons for event generation, which can lead to improved training, correcting broken business process and identification of high value mitigating controls. Requires event review team to close incidents with root cause indicator.</td>
</tr>
<tr>
<td>Identifies individuals that require direct training or disciplinary action. This can also highlight groups that handle significant volumes of sensitive data and those which need top-down improvement and communications. Embedding data protection measures into annual performance measures can be a powerful incentive to understand and apply data protection policies and data handling guidelines.</td>
</tr>
<tr>
<td>Estimates the number of employee weeks per month dedicated to data protection event handling.</td>
</tr>
<tr>
<td>Evaluates compliance with acceptable service levels for event resolution. This can be split into time to initial evaluation and time to closure if validated events are escalated to secondary parties for closure.</td>
</tr>
<tr>
<td>Provides insights into the types and volumes of data loss events over time. Grouping by policy or rule provides specific details about the trends for specific types of sensitive data.</td>
</tr>
<tr>
<td>Identifies potential compliance issues, such as unencrypted credit card numbers stored in unstructured files.</td>
</tr>
<tr>
<td>Provides information about the percentage of unstructured files that contain classification labels. This can be combined with other policies to determine a percentage of files that contain sensitive data and have been labeled with a classification level.</td>
</tr>
</tbody>
</table>

**To stay relevant, the data protection program must keep up with the business**

Organizations are not static. The value of information changes frequently, and in some cases continuously. If the data protection program doesn’t change to continue to focus on the data that matters most, the value provided by the investments in technology, people and processes will decline over time. Providing metrics to the business, addressing broken business processes and providing regular training help users and data owners to stay engaged. These activities increase communications and can help the data protection program to stay relevant.
Data protection is a business issue – not an IT issue

For complex organizations with many types of sensitive information, taking data protection for granted is a recipe for disaster. Even organizations with strong information security teams, cutting edge tools and mature processes can be victimized by data loss events. Whether people act carelessly or with malicious intent, users with authorized access present a huge challenge. To meet this challenge, organizations need to be able to apply additional safeguards and increased monitoring of the data that is most important to protect.

Without input, sponsorship and direction from the business, information security professionals cannot strategically align controls and monitoring capabilities to the data that matters most. Additionally, unless end users actively participate in identifying and labeling sensitive information, data protection program investments may yield little practical value.

**Business leaders:**
Set the tone and build a culture of data protection.

**Data owners:**
Get involved – it’s your data!

**Information security professionals:**
Walk across the aisle and ask the right questions.

### Key questions for business leaders

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are you confident your intellectual property, trade secrets, proprietary information and customer data are protected from insiders?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are your regulatory and compliance obligations for data protection and privacy being met?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does your Information Security function understand what data is most valuable to the business? (Have you told them?)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is your data classification policy more than just a piece of paper? Has it been implemented and embedded into your culture?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have your investments in data protection people, processes and technology demonstrated tangible value for your business?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you know what success looks like? (Do you know if your program is working?)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If one of these questions has been answered with “No,” it is time for you to take action.
Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our Insights on governance, risk and compliance series at www.ey.com/GRCinsights.
At EY, we have an integrated perspective on all aspects of organizational risk. We are the market leaders in internal audit and financial risk and controls; and we continue to expand our capabilities in other areas of risk, including governance, risk and compliance as well as enterprise risk management.

We innovate in areas, such as risk consulting, risk analytics and risk technologies, to stay ahead of our competition. We draw on in-depth industry-leading technical and IT-related risk management knowledge to deliver IT controls services focused on the design, implementation and rationalization of controls that potentially reduce the risks in our client’s applications, infrastructure and data. Information security is a key area of focus where EY is an acknowledged leader in the current landscape of mobile technology, social media and cloud computing.
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2014 EYGM Limited. All Rights Reserved.

EYG no. AU2498
ED none

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com/GRCinsights

About EY’s Advisory Services
Improving business performance while managing risk is an increasingly complex business challenge. Whether your focus is on broad business transformation or more specifically on achieving growth, optimizing or protecting your business, having the right advisors on your side can make all the difference.

Our 30,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and exceptional client service. We use proven, integrated methodologies to help you solve your most challenging business problems, deliver a strong performance in complex market conditions and build sustainable stakeholder confidence for the longer term. We understand that you need services that are adapted to your industry issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where your strategy and change initiatives are delivering the value your business needs.

To find out more about our Risk Advisory services could help your organization, speak to your local EY professional or a member of our global team, or view: ey.com/advisory.

The leaders of our Risk practice are:

<table>
<thead>
<tr>
<th>Global Risk Leader</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Paul van Kessel</td>
<td>+31 88 40 71271</td>
<td><a href="mailto:paul.van.kessel@nl.ey.com">paul.van.kessel@nl.ey.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Area Risk Leaders</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jay Layman</td>
<td>+1 312 879 5071</td>
<td><a href="mailto:jay.layman@ey.com">jay.layman@ey.com</a></td>
</tr>
<tr>
<td>EMEIA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jonathan Blackmore</td>
<td>+44 20 795 11616</td>
<td><a href="mailto:jblackmore@uk.ey.com">jblackmore@uk.ey.com</a></td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Iain Burnet</td>
<td>+61 8 9429 2486</td>
<td><a href="mailto:iain.burnet@au.ey.com">iain.burnet@au.ey.com</a></td>
</tr>
<tr>
<td>Japan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yoshihiro Azuma</td>
<td>+81 3 3503 1100</td>
<td><a href="mailto:azuma-yshhr@shinnihon.or.jp">azuma-yshhr@shinnihon.or.jp</a></td>
</tr>
</tbody>
</table>