Technology
A more effective, simple and cost efficient approach to protecting critical enterprise data

- Consulting • Technology • Outsourcing
It's not news to executives that their companies' information is under attack, and that this threat has become increasingly sophisticated and more pervasive. Today's cyber thieves are extremely adept at using the latest tools and technologies to expose and exploit even the smallest vulnerabilities in companies' defenses.

What may be a revelation, however, is the size of the gap between the level and nature of the threat and the capabilities companies have in place for securing their information. Accenture research and client experience have found that while companies have been busy innovating and growing their businesses, the vast majority of their efforts to protect sensitive information have not kept pace.

Consider, for instance, the case of mobile banking. In response to marketplace demand, banks have been rolling out applications that enable customers to conduct transactions via their mobile devices. However, while mobile banking represents a tremendous business innovation, banks' security infrastructures as currently constructed never envisioned mobile banking. Therefore, the data exchanged via mobile banking transactions is at a higher risk to be compromised by hackers with access to sophisticated tools.

Collaboration is another example. The success of the modern global enterprise hinges, in many ways, on how well a company employs innovative technologies and business structures to help employees and trading partners access and share critical information—and ultimately to make better decisions. The automobile industry, where close collaboration with suppliers is a way of life, is a prime example. However, many companies do not have in place the level of data protection commensurate with the extent of information sharing that is common today.

In short, the failure of security efforts to keep pace with business innovation, combined with the increasing sophistication and prevalence of threats to critical information, has put many companies in a risky position.
Why companies struggle to respond to the threat

Companies are struggling to respond to the threat to their information for many reasons. One reason is a reliance on security standards to set the bar for what is considered sufficient protection. Conceptually, standards are a good thing, as long as they remain current and relevant. Unfortunately, the standards for information security—on which certain industry regulations and security hardware and software products are based—were developed more than 15 years ago and have not been updated appreciably since. Yet during that time, companies have continued to innovate (think cloud computing, trading partner collaboration and mobility, for instance). They now engage in practices for which those security standards were never designed—a fact that has not gone unnoticed by criminals, who are quick to exploit vulnerabilities.

In addition, companies don’t have the appropriate processes in place to distinguish the relative importance of each type of data they generate and store, a determination that is crucial to constructing appropriate security measures.

In our experience, most companies generate and collect three categories of sensitive information (Figure 1), each with a different value to the enterprise.

Regulated information

In this category is the type of data people most often think of when the subject of information protection is raised. This is also the category of data that historically has garnered the biggest headlines when compromised. Regulated information includes personally identifiable information (PII) such as contact information; social security numbers; financial information, such as banking or credit card numbers; and medical records. When such data is compromised, enterprises can experience a range of negative consequences, including public outrage, lawsuits, fines, and loss of brand equity and consumer trust. Recent high-profile breaches underscore the magnitude of the threat to regulated data.

Confidential organizational information

Confidential organizational information—which includes such things as marketing plans, financial projections, sales reports and M&A discussions—also is key to an enterprise. However, while authorized access to confidential organizational information can drive greater business productivity, leaks of this type of information can have varying impacts on the business, ranging from public embarrassment to catastrophe.

---

**Figure 1. Three categories of sensitive information**

<table>
<thead>
<tr>
<th>Intellectual property</th>
<th>Confidential organizational information</th>
<th>Regulated information</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Patent and copyright information</td>
<td>• Unreleased financial data</td>
<td>• Sensitive personal data</td>
</tr>
<tr>
<td>• Trade secret</td>
<td>• M&amp;A strategy and plan information</td>
<td>• Education or professional information</td>
</tr>
<tr>
<td>• R&amp;D data</td>
<td>• Sales and pricing data</td>
<td>• Health-related information</td>
</tr>
<tr>
<td>• Knowledge objects</td>
<td>• Tax information and data</td>
<td>• Detailed transaction information</td>
</tr>
<tr>
<td></td>
<td>• Litigation information</td>
<td>• Services or subscription information</td>
</tr>
<tr>
<td></td>
<td>• Job and employment information</td>
<td></td>
</tr>
</tbody>
</table>
A prime example is a company discussing the possibility of acquiring another firm. For competitive and strategic reasons, those discussions must be kept secret until an agreement is reached. Details on the proposed merger are known generally only to a small number of people in the acquiring company, the target, and their respective law firms. If these discussions become public, the parties could experience short-term damage (such as loss of trust among employees and negative publicity that undermines the brand), as well as long-term loss of competitive advantage, market position or strategic advantage. They also could invite potential investigations from regulators if any of these companies publicly trade their stocks.

**Intellectual property**

Arguably the most critical type of information in many enterprises is intellectual property (IP). Companies today are more likely to compete on the strength of their innovation and intellectual property. This type of information includes such things as blueprints for a new product design, the recipe for a market-leading food or beverage, the design of a new computer chip, and proprietary software code. Such trade secrets typically account for two-thirds of the value of information portfolios for some companies, as determined by a March 2010 Forrester Report Research.\(^1\)

The threat of having critical IP stolen and used by another company is real and growing. "Every year, an amount of intellectual property many times larger than all the intellectual property contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government agencies," U.S. Deputy Secretary of Defense William Lynn noted in a recent article he wrote for *Foreign Affairs*.\(^2\) According to FBI estimates, $600 billion worth of IP is stolen every year from U.S. businesses.\(^3\) Having critical IP fall into the hands of an unauthorized party, such as a competitor, can have a devastating effect on an enterprise’s business, including loss of differentiation, market share and shareholder value.

However, because all companies are different, the value of specific types of data is not consistent from organization to organization. Multiple factors—including a company’s industry, business model and specific competitive situation—heavily influence the importance of data to a specific company.

Consider the case of automobile companies. One might think that the design of a new car would be IP worth protecting—and conceptually, it is. However, from a car company’s perspective, new-car designs actually are not that sensitive. Automakers know that competitors can gain access to IP simply by reverse-engineering a product once it hits the market. Such “teardowns” of a new car by competitors are common and can reveal considerable intelligence on what went into the design of the vehicle.

Similarly, at companies that develop genetically modified crops, one might intuitively expect that the DNA sequencing that produces those plants would be “crown jewels” that should be protected at all costs. But in reality, anyone could go into a field where such crops are growing, cut a sample, analyze it in a lab, and identify the sequencing.

In both the preceding cases, IP that might be considered highly sensitive in some companies is not due to the nature of those industries and their products. However, in such companies, while a product’s design may not be as valuable—and, thus, worthy of protection—how that product was built is.

For instance, Rolls Royce’s Trent aircraft engines long have been considered the gold standard for such products. Yet these engines are not market leaders because of their designs. Rather, it is Rolls Royce’s unique process for manufacturing the ceramic blades that give Trent engines a performance advantage over competing engines.

The question is: can companies accurately distinguish between data that is vital to secure and that which is not? In Accenture’s experience, the answer often is no. We have found that companies consistently overestimate the importance of their data—typically believing between 40 percent and 50 percent of the data they generate and collect is highly sensitive. In extreme cases, companies actually believe all of their data is sensitive and worthy of protection. In reality, for most companies, only about 5 percent meets that criterion.

But even if they intuitively know that some data is more important than other, many companies do not have the tools or resources to identify different levels of sensitivity across their sets of data. As a result, they secure all data at the same level. Besides the expense and complexity of this approach, this means companies are over-protecting some data while under-protecting other, more critical data. With a more realistic view of sensitivity levels, companies could implement a far less complex, more cost efficient, and more effective security architecture.

Here’s a real-life example: A pharmaceutical company faced the challenge of protecting one type of highly sensitive data that was not legally allowed to be transmitted in any way across country boundaries. Unfortunately, the company found that not only had some of this data leaked out of its host country, it also had essentially spread to other locations of the company around the world. An audit firm suggested the company would have to upgrade its entire global security environment to address the situation—an effort the firm estimated would cost $80 million to $90 million. The company’s CIO decided to get a second opinion. Working with Accenture, the company determined that although the data in question was, indeed, spread globally, it was largely duplicative data. Accenture recommended the company instead consolidate all the data onto one server, disconnected from all networks, in a single highly secure physical location. This option not only resulted in even better protection than the initial recommendation but was also a lot more cost efficient.
A new approach to security

The pharmaceutical company example illustrates how an organization could be misled into thinking security is too huge, complex and costly a problem to address. We believe the most effective approach to security is the simplest: Concentrate first on stringently protecting what is really important, and then apply measures to the other types of data that are commensurate with their value to the enterprise. Such an approach should be based on a holistic perspective that considers the entire lifecycle of information (create, process, store, transmit, and destroy); is information-based, rather than system-based; and recognizes that “an information type may pass through multiple systems, multiple business processes and multiple storage media over its lifetime and hence be subject to differing risks.” (Figure 2).

With an information-centric perspective as the foundation, a company can develop and implement the appropriate measures that maximize access to critical information by those who need it while appropriately mitigating the risks to that information throughout its lifecycle. All of this can be done while reducing the overall cost of information protection for the enterprise. Accenture recommends a four-step framework (Figure 3) to help companies achieve those goals:

Figure 2. Information risk perspectives

![Information risk perspectives diagram](image)

Source: The Information Lifecycle, Information Security Forum, November 2010

Figure 3. Accenture’s information protection framework

![Accenture’s information protection framework diagram](image)
• Create an information protection strategy
• Locate and classify the information that matters most
• Weave information protection into the fabric of the organization
• Develop capabilities to protect information assets

These steps enable companies to achieve early value from their efforts and, more importantly, lay a strong foundation for optimizing and protecting their information assets over the long term.

Create an information protection strategy
A company should view its information protection strategy in the broader context of information management. The strategy should include provisions for enabling business opportunities and mitigating critical information risks.

Two actions are key to developing a sound strategy.

One action is understanding the business-specific needs for information protection. As noted earlier, each organization has unique requirements, including regulatory, financial, or reputational. Thus, the business value and risk of different types of sensitive information can differ dramatically from company to company. For example, one public health organization realized huge service improvements through secure cross-department health record sharing but identified unique protection requirements for records indicating a hospice address or locations of relocated children.

Another important strategy-related action is defining a set of objectives to deliver quick wins and address long-term goals. Information protection efforts should begin by defining some achievable outcomes along an information protection roadmap to demonstrate clear progress and return on investment. Most programs can be created around a particular business requirement while laying the foundation for broader use.

Locate, consolidate, streamline and classify the information that matters most
While a strategy is absolutely essential to effective protection, it often will fail unless a company knows what it should protect and where that information resides. By locating and classifying the information that matters most, a company can ensure that subsequent efforts are appropriately directed to the information that has the greatest value to the organization—and that could have the greatest negative impact on the company if it were to be compromised.

A discovery and investigation effort can help a company identify how information flows through its systems (for example, databases, file servers, and SharePoint sites), business processes and user communities. A company also should recognize that information’s sensitivity (and value) can change throughout its lifecycle as it is enriched and combined with other information. Identifying the extent and nature of this change is only possible through automated and manual analysis of information lifecycle flows.

Once the business understands its information flow, it can define and classify that information. Information should be grouped in easily understandable categories so opportunity and risk owners can establish objectives that enforce information protection policies and drive desired information protection outcomes. For example, government organizations typically use some variation of five categories to classify their data: top secret, secret, restricted, confidential and unclassified. One oil company we know also has five levels: IP (the most sensitive), business critical (such as financial data), boardroom-level (for instance, discussions about acquisitions or joint ventures), commercially sensitive, and non-sensitive.

With information flows confirmed and information classified, a company then can perform a business-focused information impact analysis to identify information with the greatest impact on strategic, tactical and operational objectives. This exercise often can yield surprising results. For example, in many organizations, regulated information tends to get the most attention (and resources designed to protect it), when intellectual property is actually the most critical and should be getting the lion’s share of focus.

As a consequence, organizations should agree on which information matters most and which is less sensitive. Looking at the information lifecycle, most companies should treat information classification not as a static attribute but as a dynamic parameter that gets adjusted through the treatment of information itself.

Weave information protection into the fabric of the organization
While external threats to sensitive information are real and growing, Accenture research discovered that just under half of companies that experienced data breaches found the cause to be employee error or negligence.5 Thus, companies should focus considerable attention on ensuring employees understand the importance of protecting information and have the tools to monitor progress over time.

As early as possible, a company should assign clear ownership for information and ongoing protection by first defining information protection roles and responsibilities. Without basic governance, a company won’t be able to adequately protect sensitive information. And just as information sensitivity and value change over time, the role descriptions and job performance targets of information owners and stewards likely will need to be updated.
As part of the governance process, a company should define and communicate policies for sensitive information types and establish, monitor and measure the processes that enforce them. This is an important prerequisite to not only driving the desired behaviors from employees, but also to refining the appropriate supporting information protection processes and technologies.

A formalized training and awareness effort also can be helpful in cultivating an information protection mindset throughout the organization. Ongoing education of staff, as well as anyone in a company’s extended enterprise with access to sensitive information, is key to preventing actions that can compromise information—whether those actions are unintentional (such as system misconfiguration or poor judgment) or malicious (such as hacking or sabotage) (see sidebar on p 9).

Yet even if a company can set in place the right roles and responsibilities, establish strong policies and execute comprehensive training programs, it still can fail to achieve its objectives if it doesn’t know where its efforts have “taken root” and where it still has weaknesses that could leave its information vulnerable. Thus, information protection metrics and reporting are extremely important. Management dashboards and other methods that provide an up-to-the-minute snapshot of progress and status can illustrate where the company has made continuous improvement and help justify additional spending to shore up potential problem areas. It also helps company leadership keep information protection a board-level concern. For example, one natural resources company used executive dashboards to illustrate its starting state of minimum compliance and to track information protection metrics such as risk reduction, performance improvement, and security as a differentiator. This was all tied to real-world business objectives.

Develop the necessary capabilities to protect information assets

At the heart of this step in the framework is determining the technologies and processes that optimally support the company’s information protection objectives. In doing so, a company should take a top-down view of how well-suited it is to support those objectives. Does the organization maximize the business enablement of information? Does it appropriately manage the risks to information? If it doesn’t, what changes would be necessary to get there? In many cases, the answer will involve a revision of the company’s enterprise architecture and continuity plans, which must incorporate key aspects of information protection.

A variety of technologies are available to help companies improve their information security capabilities (see sidebar on p10). However, as important as these tools are, companies also must recognize that developing information protection capabilities is not just a technology concern. To the contrary, it should be a collaborative effort between IT and business to integrate information concepts into long-term planning. As part of that planning, the team should create a road map that aligns short-term and long-term information protection business goals with the company’s overall information technology plans. IT capabilities should directly support information objectives, yet in most companies, IT includes surprising gaps that represent great opportunities for enablement and risk management.

For example, a large supplier of electronic goods established an information protection framework of governing controls based on a four-step approach, considering:

- Classification of assets (not limited to information)
- Target environment (e.g., differentiating less-controlled environments from very secure zones)
- Timing and lifecycle activity
- Involved parties (such as employees, authorities, partners, and customers)

In the course of implementing the framework, the company not only modified operational procedures to govern the flow of information, but also altered application development policies to embed information protection. Such actions effectively implement “information aware” applications and help to mitigate information leaks. They also reach into new, less controllable domains of an information ecosystem, such as outsourced services, clouds, mobility networks and social network integration.

A company should not develop information protection capabilities in a vacuum. Rather, it should understand where it falls on an information protection maturity model for its industry and where it ideally would like to be. Such a discussion must take place at the highest level of an organization—ideally, at the board of directors. While measurement and metrics can demonstrate progress, they alone can’t reveal whether the company is doing enough. Thus, some organizations have found that benchmarking their information protection capabilities against their industry peers can help them better understand their current and target maturity and articulate that clearly to stakeholders. For example, one Asian energy company used an information protection benchmarking exercise to assess areas of deficiency, opportunities for improvement and required investment to reach an appropriate level of maturity. The benchmarking report was presented to executive leadership to justify the tactical and strategic initiatives required to meet industry baseline and good practices.
Accenture research and client experience confirm that an organization's people are the keys to security. Thus, to improve its security posture, a company should focus considerable attention on programs and activities that communicate and raise awareness of the value of security among its workforce.

For example, agricultural company Monsanto in the early days developed a series of vignettes featuring a character named Nelson “who’s always misbehaving when it comes to security,” said Shirley Cunningham, Chief Information Officer at Monsanto. “Nelson helped people more easily engage with the communications and remember the message, as they always look forward to seeing what kind of trouble Nelson will get into each week.” A large bank regularly conducts a “Security Week” to focus attention on the importance of security.

In many cases, companies bifurcate awareness and education programs into two streams: one for senior management and one for employees at large.

Taking awareness a step further is the U.S. Department of Homeland Security (DHS), which requires relevant employees to participate in an interactive training game in which employees must choose the right action when presented with various security-related scenarios. “At the end of the program, employees receive a grade of their performance,” noted Richard Marshall, Director of Global Cyber Security, US Department of Homeland Security at DHS. “Those who don’t pass have their access to information immediately cut off until they complete the training again as necessary and get a passing score.”
Despite technology vendors’ claims, there is no silver bullet for information protection. Organizations typically employ a suite of technologies to address different scenarios and business goals. In almost all scenarios, starting with a robust identity and access management solution is a good first step. However, certain information protection technologies are more appropriate for different scenarios, and having a good understanding of where technology will help or hinder is key to making the right decision.

For example, intellectual property and confidential organizational information can leave an organization through many channels: USB flash drives, email, social networks, and others. Technologies that can be particularly useful to protect these types of information include:

- **Data Loss Prevention (DLP) technologies**—DLP technologies enable an organization to enforce information protection policies through technology that can detect unauthorized behavior, alert appropriate parties and optionally block behavior. DLP technology could silently notify an incident response team if a contractor attempted to email confidential blueprints to his external webmail account, for instance.

- **Enterprise Digital Rights Management (DRM) technologies**—Enterprise DRM can embed information protection into file formats and email for sensitive information types. This enables protection to travel with the data no matter where it resides and be transparent for those with legitimate access. Enterprise DRM could render sensitive research information left on a USB flash drive unreadable should the drive be lost or stolen.

Regulated data, such as payment card data, electronic health records and personally identifiable information is typically aggregated through normal business operations and is transmitted and stored by IT systems targeted by data thieves. Technologies that can help protect regulated data include:

- **Data Encryption**—Enterprise data encryption scrambles information held in storage and when transmitted using persistent or temporary keys. Encryption requires careful planning and operation, as poorly managed encryption can itself lead to data loss. Properly implemented data encryption could thwart data thieves from accessing customer payment card data on lost backup media.

- **Data Tokenization**—Data tokenization solutions replace sensitive data with generated “token” data to reduce security requirements on IT systems but can provide actual values to applications when needed. For example, data tokenization could help an organization dramatically reduce the number of IT systems that electronic health records reside upon, thereby significantly reducing risk and compliance costs.

Confidential organizational information can be challenging to secure because it takes many forms and is accessed by employees from a variety of locations and devices. Technologies that are useful for protecting confidential organizational information include:

- **Remote Desktop Technologies**—Remote desktop technologies enable users to access a remote desktop experience controlled by enterprise IT, similar to using an enterprise-issued PC. Remote desktop technologies can help keep sensitive information off of consumer devices, such as home computers and tablets that may be lacking appropriate protection.

Remote desktop technologies could, for example, enable an M&A team to collaborate on plans in the evenings from the comfort of their own homes and from their own devices.

- **Security Information and Event Management (SIEM) technologies**—SIEM technologies aggregate, correlate, report and alert on security events across a variety of IT systems. SIEM technologies raise awareness of unauthorized access attempts and can provide evidence for compliance audits. For instance, SIEM technologies could detect unusual late-night patterns of sensitive financial information accessed by employees who typically work business hours and alert a security response team.

Of course, these technologies apply to a variety of scenarios not mentioned here and can be mixed and matched with the information types above. Each technology is best evaluated in the context of enterprise architecture where all solutions are traceable to business objectives and aligned to IT strategy.
When the Information Age dawned in the early 1970s, few people fully anticipated how widespread the sharing of potentially powerful information would become, or how sophisticated and prevalent the threats to that information would become over time. Yet 40-plus years later, the unexpected has become commonplace, and companies everywhere find themselves grappling with a challenge that at times can seem overwhelming.

In some respects, the situation resembles going into battle against a modern-day MiG jet in a World War II fighter plane. Like the World War II aircraft, companies are relying on old technology and outdated standards to combat a foe with far superior and more sophisticated equipment. Unless conditions change, it’s easy to predict the ultimate outcome.

That’s why we believe it’s time enterprises rethink their entire approach to information security—focusing on reducing the complexity (and cost) of security by adopting protection measures that are appropriate for each type of data’s sensitivity and overall importance to the enterprise.

Fortunately, information protection tools, practices and strategies are now available to help companies achieve that goal. By judiciously applying these capabilities, companies can keep their most valuable information in the hands of those who can use it to the benefit of the company—and out of the hands of those who would abuse it. They also will be better positioned to capitalize on the power of their digital assets and avoid costly breaches and other events that could damage their brand, compromise customer trust, and erode shareholder value.

Conclusion
Notes

1 *The Value Of Corporate Secrets, A Forrester Consulting Thought Leadership Paper Commissioned By Microsoft And RSA, The Security Division Of EMC, March 2010.*


Contact us

**Bill Phelps**
North America Security Lead
+1 703 947 2586
bill.phelps@accenture.com

**Floris van den Dool**
EALA Security Lead
+31 20 4938058
floris.van.den.dool@accenture.com

**Paul O’Rourke**
APAC Security Lead
+61 3 98387488
p.orourke@accenture.com

About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with approximately 236,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world’s most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$25.5 billion for the fiscal year ended Aug. 31, 2011. Its home page is www.accenture.com.