IT ADVISORY SERVICES

The changing lens of information security

kpmg.com
The changing lens of information security

Enabling business via information protection programs

Contents

- The new view of information protection 4
- A matter of timing 5
- Technology as a business enabler 6
- Regulatory and cultural shifts 7
- Technology's next wave 9
- A look at our clients’ results 10
- How KPMG can help 11
The quality and integrity of corporate information is vital to an organization’s success. If it is lost or stolen or its integrity is compromised in any way, the damage to an organization’s reputation and revenue stream could be irreparable. So, with threats to corporate information on the rise and information portability proving to be an essential business need, it’s not surprising that protecting this information is a top priority for today’s business leaders. And it is a priority that presents daunting challenges, especially amid today’s turbulent market environment. Due to increasing pressure to significantly reduce costs and improve performance, to adhere to increasing regulations, and to respond to rapidly changing business needs, information protection is on the cusp of an evolutionary era that has the potential to redefine the culture, strategy, and function of IT within an organization.

Information protection is moving beyond the traditional view of security at the perimeter level—where barriers, such as firewalls and antivirus software, aim to surround and protect the network—toward a more strategic focus on protection at the data level. And the change could not be more dramatic. Whereas traditional security relied on a rigid fortress of architecture, the new era of information protection must be more nimble and nomadic in nature, heavily dependent on flexibility, scalability, and accessibility to meet the ever-changing business needs of a global marketplace.

This calls for a complete change in mindset. Creating a more malleable information protection system requires rethinking the information protection strategy in a way that derives the most business benefit for an organization. This involves the restructuring of people, processes, and enabling technologies to strategically align with business goals. It also means that compliance, the driver of former information security models, will now serve a mandatory yet peripheral role in the new information protection design. The goal of this new model focuses on aligning security with the core requirements of the business to derive the most business value.
A matter of timing

While securing information is largely being driven by a sense of urgency from the business, the current market environment adds to existing pressures. As a result of the troubled economy, aggressive cost-cutting initiatives are underway in almost every area of an organization, including IT. Executives are being asked to scale down resources, reduce headcount, and lower overall cost of ownership. At the same time, IT security is facing a staggering growth in very real threats from a variety of sources including hackers, disgruntled layoff victims, and unscrupulous employees. Meanwhile, increased and changing regulations further complicate matters. Amid such change, information security must reflect the same level of efficiency as the business. So the timing for this transformation is less than ideal.

As a result, business and IT executives are grappling with questions and decisions on how to best move forward.

• What should the 21st century IT security model look like?
• What are the metrics? And how do we know these should be the metrics?
• As firewalls and other technology become dated, what types of access management technology will prevail to meet the needs of a changing security model?
• What are the new revolutionary technologies that will drive cutting-edge security?
• Will the desired technology adequately meet both business and security needs?
• How do we gain efficiencies in our processes while still maintaining compliance?

These and many other questions are being explored while the pressures to enact change are intense. And, the mandate is very clear: do more with less. And do it now.
Technology as a business enabler

Digitalization and globalization have forever changed the dynamics of doing business. As business continues to evolve, so must the security function put in place to support and protect it. Hence, there is a distinct need for nimbleness and agility in an organization's future information protection strategy. As organizations realign to become more efficient, the same expectation exists for information protection to become more efficient. There is a growing demand for increased flexibility, integrity, scalability, and accessibility of information that has changed the way organizations view information protection. It's not about technology; it's about deriving the greatest business benefits by utilizing technology.

Organizations today not only want but need to enable business with technology that improves operational functionality, data availability, and optimizes performance while safeguarding the information and reducing costs. As a result, the future-forward focus relies on more of an information-centric security model, in which it is not necessary for you to go to the data but rather for the data to come to you. As oceans of data continue to overflow and overwhelm organizations and the demand for anytime/anywhere access increases, the network-perimeter security model appears impractical to sustain.

New technology exists that is able to meet the business needs as well as the bottom line, but the ability to provide adequate security must also be factored into the equation. An information security strategy must be supportive and reflective of supporting business and strategic goals and be developed in a manner as dynamic as the business needs it to be, while adequately protecting the information.

The challenges are significant. Business models are constantly changing and evolving—even on a daily basis. That means that the information security program must be able to do the same. As a result, executives are going to need to find the right strategic solution for their organization that will provide for the securing of information while still allowing the business to respond to its current needs. The ability to figure out that strategic formula for an organization will depend on a variety of factors, needs, and tolerances specific to the organization. It may require a third party or business partner relationship in order to support the business being nimble without relying on technical architecture or cumbersome policies and procedures. In some cases, the new business model will dictate less security than before.

As a result, a changing scenario from risk elimination toward risk management arises. In essence, today's security organization should abandon the worst-case scenario approach that led to an inflexible architecture and should look to take a risk-appropriate scenario approach that provides for exceptions and contingency plans. This new model assumes that all data are not created equal and that they do not demand the same level of information protection. The difficulty lies in defining and providing the appropriate level of security for specific information while simultaneously allowing the business to be responsive and agile. And yes, this may mean that organizations will no longer assess “everything” but instead will need to place the emphasis on the value of the information.
Regulatory and cultural shifts

Changing the view of information protection from a technology function to a strategic business imperative is just one of many hurdles facing the IT staff. After rising to the challenge of Sarbanes-Oxley (SOX), IT executives are aware of the significant changes that regulations may impose on operations. Amid economic reform, IT executives are bracing for a new wave of regulatory challenges to take hold. Many industries are already facing intense scrutiny from regulators, which makes data integrity and security policies more relevant than ever.

These laws enact international and industry standards that include:

- ISO 27000 series
- National Institute of Standards and Technology (NIST) 800-53
- Payment Card Industry (PCI) Data Security Standard
- Payment Application Data Security Standard

Pressure from government, trade associations, shareholder bodies, and regulatory authorities indicates that the secure management of business data remains a primary corporate responsibility. There are already numerous industry regulations, including SOX, the Health Insurance Portability and Accountability Act (HIPAA), the HITECH provisions of the Act, and PCI standards, to name a few, that require the implementation of several rigorous safeguards to protect sensitive data. The new processes within a revised security program should take this into account as new regulations come down the pike. Yet, as previously noted, the priority and focus on compliance in the new information protection strategy will shift. It will be more about streamlining, automating, and controlling the function to meet the necessary standards rather than allowing compliance to drive the process.

Additionally, as IT becomes more of a strategic enabler for business, there will be a cultural shift where both IT and the business take an interactive role in driving the overall strategy. Moreover, CIOs and CISOs, who were sometimes viewed as technology personnel, are increasingly taking on business roles and are playing a prominent role in the strategic planning and business decisions of an organization.

A host of regulations

The ever-evolving regulatory landscape has a significant impact on IT security and operations. Some examples of recent regulations that likely require operational changes to maintain compliance include the following:

- Code of Federal Regulations (CFR) 21, Part 11
- Computer Security Act of 1987
- European Union Data Protection Directive
- Federal Information Security Management Act (FISMA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Health Insurance Portability and Accountability Act (HIPAA)
- Homeland Security Act
- Independent country data privacy laws, such as Japan’s Personal Information Protection Act
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)
- Office of Management & Budget (OMB) Circular A-127
- OMB Circular A-130
- Presidential Decision Directive (PDD)-63
- Sarbanes-Oxley Act (SOX)
- Security Management Act
IT and other business counterparts should collaborate more interactively with one another and as a result, their strategic alliance will positively impact the bottom line. It’s important to acknowledge that while business needs are driving these cultural shifts, the new roles for technology will help create value for the business rather than just preserve it.

As businesses undergo sweeping changes, new control models and risk management mechanisms will be required to preserve and create value through strong information protection models, right-sized to fit emerging business processes. The following represent leading practices in information protection moving forward.

**Enterprise View of Risk and Control Value**
- Evaluate and risk-rank business processes including business value estimations
- Consolidate asset management and combine with risk scoring
- Develop tiered models of control coinciding with protection requirements

**Changes in Business Models**
- Create or enhance security-focused vendor management program
- Define trust levels and protection strategies for virtualization and cloud computing

**Targeted Attacks**
- Utilize enterprise risk tiers to apply controls and processes across classifications
- Update training and awareness to include social engineering attack and defenses
- Implement additional end-point controls as necessary

**Increased Insider Risk**
- Assess control processes for manual user activity and automate where possible
- Implement role-based access control and consolidated access management systems
A process-driven strategy includes dynamic applications where business processes can be easily created and changed. However, this also generates major change management, service management, and compliance challenges for an organization. Transactional security can become very complex, very fast. A variety of technology solutions are available that are designed to help address such challenges.

However, allure from a cost perspective comes from next-generation technologies such as virtualization and cloud computing, which continue to garner attention of both business and IT circles. And, there’s good reason. These technologies not only have the potential to reap significant cost savings but also can cause reductions in required space, resources, and energy without the need to add equipment or staff. Hence, the business case for these trends is powerful: optimize performance, reduce resource consumption, and increase scalability. However, security has to be addressed proactively in the procurement and configuration and cannot be after the fact.

Virtualization allows multiple virtual machines to run on a single physical machine. By pooling resources, it provides a cost-effective way to increase efficiencies. Essentially, virtualization severs the link between location (hardware) and application (software) releasing workloads to run on virtual machines. Cloud computing goes further and removes the link between ownership and control by making physical location ambiguous. Cloud computing involves the outsourcing of computing capacity to third-party services over the Internet. It is a pay-as-you-go strategy where you use IT services as you need them. This allows for IT services such as computational power purchasing, disk storage, collaboration, application development, and customer relationship management to be managed remotely and purchased on demand. There is no need to invest in additional servers or infrastructure over time because these solutions are flexible and scalable. They can address short-term initiatives and requirements as well as deal with the ebbs and flows of business cycles. However, in the case of cloud computing, where the data reside, who has access to them, and when, are not always identifiable.

Therein lies the problem. While it is challenging enough to share information with business partners and established third parties, the blurry characteristics that make up “the cloud” allow for the use of nontraditional vendors that may be unknown entities to an organization. Seemingly, there’s a lack of concern surrounding cloud security, which could put an organization at great risk as well as fail to meet specific regulatory requirements for sensitive data.

As cloud computing and virtualization technologies continue to develop, whether or not they can measure up to the practical needs and expectations of an organization’s information protection strategy will likely be determined on a case-by-case basis.
A look at our clients’ results

Client situation #1:
A FORTUNE 25 corporation seeks to combine information protection efforts following mergers.

Challenge
A FORTUNE 25 corporation had recently completed several major merger activities. As a result, the company ended up with four major security offices representing four major service lines, based upon geographic and regulatory boundaries. In addition to being an expensive way to operate, this distributed approach also prevented the organization from effectively leveraging shared services and technology centers.

KPMG services
KPMG was engaged to assist with developing a wide-ranging information protection strategy for the combined entity and identified a multiyear road map for transition including metrics to monitor success. KPMG then assisted with deployment of new supportive business processes and enabling technologies to support the strategy including identity and access management, risk assessment, and proactive monitoring.

Result
The company reduced its security operational budget by greater than 40 percent while increasing the committed service level and supporting additional business priorities.

Client situation #2:
A FORTUNE 100 financial services company seeks to improve information security to meet new regulatory requirements.

Challenge
After completing several major mergers and divestiture activities, a FORTUNE 100 financial services company faced several challenges meeting a host of new regulatory requirements. The company found itself being regulated in new fashions and by new entities yet had no additional funding to spend on information security on an ongoing basis.

KPMG services
KPMG was engaged to assist with developing security program capabilities around core information security functions. KPMG designed the program and associated processes, and is currently assisting the company with the implementation of the program, processes, and supporting tools.

Result
With a new system in place, the company was able to maintain current annual spending on information security while increasing compliance activities to meet its current regulatory needs.
How KPMG can help

KPMG can help improve the effectiveness of your information protection program by assisting your organization in enhancing the cost of security, reducing risk, and making compliance easier to demonstrate. But most importantly, it can help you provide your company with better business enablement capabilities. KPMG’s approach to information protection balances preserving and creating business value. Our multidisciplinary team recognizes that organizations want to protect and maintain the integrity of information while leveraging its strength as an asset to provide measurable benefits.

To help protect your information assets, KPMG professionals focus on:

- Protecting and controlling electronic records and critical information assets
- Strengthening the processes and technologies used to manage employee, customer, and business partner electronic identities
- Linking and coordinating IT compliance efforts through streamlined approaches to lessen their impact on business process owners
- Understanding and improving business resiliency processes and technology to reduce the risk of unintended business disruption
- Developing a strategy that can enable/enhance security to achieve your organization’s value creation goals
- Understanding, prioritizing, and mitigating the risks associated with the use, transfer, storage, and management of critical information assets
- Building and maintaining industry-appropriate control frameworks and information governance mechanisms to manage and control information where privacy concerns, regulatory concerns, business process integrity, or critical business decisions impact the value of the information to the business

With our ability to see the broader issues, your organization can benefit from advice that is grounded in business perspective, objectivity, and impartiality.
Contact us:

For more information about KPMG’s Information Protection and Business Resilience practice, please contact:

Greg Bell
Global Leader, Information Protection and Business Resilience
T: 1 404-222-7197
E: rgregbell@kpmg.com