Security in the new information age: Striking a balance between risk and opportunity

Introduction

Collaborative projects like the Human Genome Project (HGP) would not have been possible without the Internet and distributed computing systems. Innovations like these blur all types of boundaries: physical, social, and even competitive. Like the HGP, companies now reap the same rewards that come from collaboration by sharing systems and data. This kind of sharing is the keystone of the new information age.

The information age has shifted focus from physical assets to connectivity and information assets. The competitive differentiator is now about expanding connections beyond company walls, and sharing ideas and data with partners, suppliers, and increasingly customers. Data now flows in and out of the business in enormous volumes and rates. It is more difficult to control where data ends up and who has access to it—in short, to safeguard information assets.

Advances in technology and means of delivery also bring changes to the business. There is a lot of interest in cloud computing and for good reason. Cloud computing allows companies to flexibly outsource IT infrastructure to providers and leverage economies of scale to control costs. However, cloud computing is relatively new and there are substantial concerns around security—some warranted and some not—but all addressable.

Security risks are rising with the growing volumes of unstructured data – the data that commonly appears in Web pages, presentations, white paper, marketing materials, e-mails, etc. In fact, IDC reports that over 95% of all digital data is unstructured. Text, audio, and visual data is growing at an astounding rate and most of it is not contained in an easy-to-manage database. Anyone can now easily create and distribute content. Consequently, files containing sensitive information can be leaked, either accidentally or intentionally.

In many ways, new technologies have made doing business easier. But these same technologies have made securing the business more difficult. Identifying and tracking information present ongoing challenges, forcing IT leaders to think creatively to pre-empt new threats. And, while it’s important to understand the risks and opportunities that new technologies present, it’s also important to clearly distinguish between real and perceived threats. Ultimately, every threat depends on the unique risks it creates for the organization, and it must be evaluated and addressed within this context.

Trend #1 Collaborative Development: Protecting from the inside out

The pace of innovation today has caused many companies to realize the value of collaborative development. Through partnering or outsourcing, companies can work together, sharing...
expertise and data to take advantage of market opportunities. This type of collaboration can enable companies to respond to customer needs more efficiently and effectively than they could in isolation.

Global connectivity allows outsourcing, both onshore and offshore, to flourish as a way to offload tasks or supplement IT resources. Outsourcing firms are showing up in every industry and support a variety of business activities, including IT. While not all outsourcing work is collaborative development, using outsourcers can greatly increase the speed in implementing new business capabilities.

Many companies have realized the benefits of reduced costs by hiring specialized skill sets only when needed, shifting fixed costs to variable, and creating the ability to scale resources up or down as required. Companies bring in outside experts to help with product development, strategies, R&D, and other business development functions. Previously viewed as a tactical move, outsourcing is now being seen as a long-term business strategy.

Collaborative development is not only limited to outsourced resources such as skilled contractors and consultants. Companies are now recognizing the power of joining forces with business partners and suppliers. These synergistic partnerships create more efficient business processes that can reduce time to market, help control inventory costs, and speed up new product innovation. By sharing resources, capabilities, expertise, data, and even access to the customer base, partners can work together to do more than they ever could individually.

Risk Assessment

The 2009 Verizon Business Data Breach Investigations Report (DBIR) found that 32% of data breaches involved business partners. Additional findings show that many attacks originated from network connections, data, systems, and user privileges that companies weren't even aware existed. With more companies allowing their business partners to access systems and data, these numbers may easily increase.

These shared connections and access to data are happening in all parts of the business in most industries. For example, medical transcriptionists download patient data, transcribe it, and send back the updates to the originating care providers. Sales departments provide outside dealers with access to customer and prospect lists. And, the supply chain network is being tightly integrated so that wholesalers and retailers can help manufacturers balance supply with demand much closer to real time. Over time, it’s difficult to track what data and connections still exist outside the company boundaries.

Vulnerabilities can be found in the most obvious ways. For example, partner access that remains available long after a project or relationship is terminated or when data is retained in systems after it was no longer needed. Some audits have found examples where partners who were supposed to have access only to specific machines were given access to the network through a VPN. This situation inadvertently gave them much wider access. The DBIR finds that 67% of breaches could have been prevented if the owners were simply aware of the data’s existence on the breached systems.

Mitigation Strategies

Before entering into a partnership, companies need to assess the potential security risks. If not managed carefully, giving access to systems and allowing partners to access or move data will have enormous risks. It’s imperative to know who will be accessing the information, what kind of security is employed on the partner side, what data they will access, and how long they can keep any downloaded data on their own system. It’s important to wrap security features around the sensitive data itself using methods like encryption and digital rights management (DRM) to provide a stronger means of access control.

Once the risks and vulnerability points are identified, formal policies must be put in place and agreed to by the partner. This should document the “who, what, when, why, where, and how” regarding access and data usage. DRM can help manage these policies by specifying and enforcing usage rights. Even if the data falls into the wrong hands, if the user doesn’t have the “key” the data remains encrypted. In addition, it’s important to run policies and processes to verify business partners also have adequate security in place. These partners need to provide assurance that they are not interacting with compromised hosts and that data is not being used outside of the agreed-upon scope and purpose.

Stringent processes, including partner assessments and periodic audits, should be implemented to reveal any policy compliance issues and potential threats to the organization. Companies should
do regular sweeps of user accounts to remove any expired accounts and identify any unauthorized accounts. These audits will detect whether this data is still available in the partner’s system. Whenever possible, audits should be automated to proactively identify and respond to any policy violations. There will always be risks in allowing partner access and integration, but these can be controlled with methods such as DRM, documented controls, and periodic audits.

**Trend #2 “Anything as a Service”: Think big, start small, deliver securely**

Just about any IT function can be subscribed to as a service these days. Applications, like customer relationship management, made the Software as a Service (SaaS) model an increasingly commonly accepted business practice. Now there are services to manage IT infrastructure, communication, network, platform and other IT functions—practically “anything as a service,” which is also known as XaaS.

These XaaS offerings provide a number of benefits, including reduced barrier to entry and increased business agility. Because the infrastructure is owned by the provider, there are little-to-no capital expenses involved. Costs are also reduced when the infrastructure is shared among several users, also known as multi-tenancy. The pay-as-you-go cost model allows additional resources to be deployed as needed, something CFOs find very attractive.

With business models and technology changing so quickly, keeping the infrastructure current becomes a greater challenge. Making big investments in technology can be risky as it can become obsolete before the full business value is ever realized. Because XaaS can scale quickly, it allows IT leaders to think big, start small, and deliver quickly. These services allow business leaders to create strategies with great potential and quickly test them on a small scale to see if they justify further investment.

These services have evolved and coalesced with concepts like virtualization, collocation, application services, and outsourced hosting, to enable cloud-based services. Virtualization technologies support cloud computing by logically separating the underlying resources so that multiple instances can run on the same hardware. Increased bandwidth provides the speed necessary to make cloud computing a viable business option.

Once regarded as hype, cloud-based services are now becoming increasingly viable and accepted as mainstream options. Gartner predicts that between 2008 and 2013, cloud-based computing services are forecast to grow from $0.66 billion to $6.8 billion for a compound annual growth rate (CAGR) of 59.5%. With more and more of the IT environment moving to the cloud, Gartner also predicts that by 2012, 20% of businesses will own no IT assets.

**Risk Assessment**

Even though many IT leaders are starting to see great value in cloud-based services, fears over security remain a central issue. In a 2009 IDC survey, 87.5% of respondents listed security as their primary concern with cloud technologies.

The security threats in the cloud are primarily the same threats facing in-house systems and infrastructure, but with a few exceptions. One of the biggest concerns with cloud-based services is multi-tenancy. Multi-tenancy allows physical sharing of software and hardware, with only virtual boundaries. This means the data from multiple companies may reside on the same server. These virtual boundaries can cause concern for IT and business leaders responsible for data. Additional security risks include:

- Number of cloud provider staff with access to the data
- Physical location of the data
- Ability to meet security standards and regulations
- Strength of the disaster recovery
- Long-term viability of the provider itself

Though most cloud service providers offer various levels of security, it is the internal IT group that is ultimately responsible and must deal with the fallout of a security breach. That kind of accountability without control can be unsettling, so it’s critical to thoroughly interview cloud providers on the short list. The potential for risk depends greatly on the cloud service provider.

**Mitigation Strategies**

Before implementing a cloud-based service, companies need a formal process and set of standards for evaluating cloud service providers. At a minimum, cloud security should offer standard protection such as firewalls, intrusion detection and prevention, and user authentication.
However, cloud environments are more complex to secure, given the potential to share infrastructure and applications, and their connection to the Internet. Companies should be aware of the additional security requirements.

Cloud security is multi-faceted and should be offered in a layered approach—physical security, network security, operating system security, and data security. Credible cloud providers should be able to describe the security features of each layer. At the very least, they must be able to show where data resides, how it is protected, and how access is managed. The more detail a potential vendor can provide, the easier it will be to determine the real risk of moving a specific application or data center into its cloud.

As much of the security concerns center around data, it’s important to know:

• Who has access and how are they vetted?
• What data security technologies such as data loss prevention (DLP) or encryption are used, especially in the case of multi-tenancy?
• Is the data completely deleted when the user deletes it from the application?
• How many copies of the user’s data are kept and where is it stored?
• What is the vendor’s privacy policy? Is customer data ever used for promotional purposes?
• How are investigations/audits handled on shared infrastructure?
• Are tested encryption methods used in the case of multi-tenancy?

Individual organizations will continue to be responsible for meeting regulatory and industry compliance requirements. Yet with cloud computing, the burden for maintaining security systems in the cloud will fall on the service provider. For this reason, it’s important to select providers that have security expertise in PCI DSS, HIPAA, GLBA, EUDPD, and other security initiatives.

Companies should also ask the cloud provider if it receives regular security assessments from third parties or internal security teams. Companies should then choose providers who have been certified with information security standards such as PCI, SAS70, HITRUST CSF, and ISO27001. Also, it’s very important to check if the provider has a plan for responding to security incidents and what the response time to critical threats is. Experienced providers will have a strong service level agreement and a solid track record of proven security practices.

**Trend #3 Unstructured Data and Secrets: Securing informal intelligence**

Today, most data is no longer available solely in large structured databases or corporate-controlled applications. It is now also found on file shares, laptops, handheld devices, online applications, social networks, cloud-services, and other third-party systems. This is especially true for unstructured data.

Organizations are beginning to see the power in extracting intelligence from unstructured data. This is now being done by combining expressions of both traditional, structured data, such as a customer list, with unstructured textual data, such as call center notes. New semantic tools enable textual analysis to uncover trends in conversations. The exploding numbers of social networking and Web 2.0 tools, including blogs, RSS feeds, Twitter, and Facebook, represent increased information opportunities for marketing, product, and customer service managers. This contextual intelligence gained from the combination of structured and unstructured data yields richer insights that help with analyzing the correlation between customer sentiment and buying behavior.

As search methods for intelligence in unstructured data matures and becomes more effective, the value of this unstructured data will increase. For example, information can be gathered from data created by customers discussing products and services in public forums, employees posting to social networking sites, and companies revealing technical approaches and strategies in various media. These factors create an informal intelligence that companies may not be aware is available.

**Risk Assessment**

Identifying and securing sensitive information in unstructured data are critical. E-mails, blogs, online communities, and social networking sites are all places where sensitive customer data and intellectual property data can be leaked, either accidently or on purpose. Given that an estimated 80% of the enterprise data growth in the next five years will be unstructured data, security risks can no longer be ignored.

Unstructured data and increased data volumes present major risks. The first, and probably most likely, is the unintended leakage of secretive information and intellectual property. This information, often referred to as “secrets,” has intrinsic value for the company. It comes in the form of new...
Security in the new information age: Striking a balance between risk and opportunity.

Product details, source code, construction plans, factory layouts, sales and revenue forecasts, and other types of competitive intelligence.

The second risk comes with another type of sensitive information, sometimes called toxic data, which predominantly carries value for people outside the organization. Examples of toxic data include all data that is regulated, including personally identifiable information. Customer data is naturally part of this category as it often is subject to privacy regulations. Leakage of this data can result in regulatory fines and public relations issues.

A recent risk has developed with the advent of mashups. The same technology that allows companies to quickly gather and analyze information on the Internet is now being used for malicious purposes. Mashups, the ability to combine different types of data, allow an independent piece of data can be linked up with other pieces of data to create information the company may not want available. While this has been done manually for several years as part of competitive intelligence practices, it can now be done much quicker with automated tools that comb through unstructured textual data.

Mitigation Strategies
Securing vast amounts of unstructured data in places both inside and outside the control of corporate IT poses a huge security challenge. Companies should start with a data governance program that develops rules and policies that define proper usage and distribution of sensitive information. These rules must then be enforced. Leading organizations apply a combination of technical tools and methods such as data loss prevention (DLP) and training, resulting in internal certification or data-specific clauses in employment contracts.

The first step in securing unstructured data is through a data discovery process that identifies the types of at-risk information and where that information is created, stored, and moved around. Unstructured data resides in places like e-mails, presentations, medical records, legal contracts, design specs, and sales forecasts. In addition, external connections such as social networking, chat, blogs, and community forums should be identified to understand what information is produced and how available it is.

Having a comprehensive understanding of the existence and use of unstructured data will help with the next step—establishing policies. These policies should protect privacy and intellectual property, and also protect connections that could potentially be attacked by hackers or viruses. All employees should receive training to help them understand the risks to both themselves and the company, and how they can help identify and protect against potential threats and leaks.

Once the unstructured data landscape has been mapped and policies developed, technology such as DLP, encryption, and digital rights management (DRM) can be used to monitor and protect the data. DLP monitors data in use, data in motion, and data at rest and uses a set of rules that consider the data type, originator, recipient, and destination to assess security risk in context. Encryption protects the data from being used by an unintended recipient, and DRM controls who or what may have access to the data—and for how long.

Security for unstructured data will look different in every company. It will be influenced by the company’s data management maturity, level of risk, and company culture. What will be the same is that securing unstructured data will take a layered approach—one that includes policies for access and use, processes that include training and communication, and technologies to enforce these policies and processes.

Conclusion
Innovations in technology now allow employees to collaborate more easily with partners and customers and take advantage of shared resources. This means information flows more freely both inside and outside corporate firewalls. Partners and suppliers access company systems and pull data, IT groups take advantage of cloud computing services to reduce costs, and the volume of unstructured data continues to grow.

Successful companies will embrace these new business trends in ways that benefit the business, while balancing the additional risks that might be introduced. To achieve this balance, IT leaders must continue to track both advances in technology and changing business needs. Security risks must be continually assessed and security leaders will need to always be diligent about managing these risks.

It’s essential to stay on top of current security trends and best practices to meet and beat the latest...
challenges that continue to evolve. At the same time, it’s important to separate the real risks from the theoretical. This is not always easy and IT leaders should seek help from experts.

Whereas security used to reside in the backroom of IT, it’s now taking center stage in corporate boardrooms—and for good reason. Recently publicized data breaches have had catastrophic impacts to the companies’ reputations and stock prices. Security managers need to rise to the challenge by engaging with the various business unit leaders to understand new risks and collaborate on security strategies.

In the end, 100% security cannot be guaranteed, nor is it a reasonable expectation. Each company will need to sit down and have an educated discussion about the risks, the costs to address risks, and the level of restrictions built into security policies. In short, security leaders need to balance the risk with the business opportunity.

**Verizon Business can help you balance the opportunities and risks of the new information age**

This era of collaboration provides new opportunities that each come with its own level of risk. Verizon has over 15 years experience assessing risk, designing and implementing global security solutions, and providing ongoing threat management to companies and government agencies around the world. In addition, Verizon offers secure cloud computing services.

To learn more about security and cloud solutions, contact your Verizon Business account manager or visit www.verizonbusiness.com/thinkforward/

---

1. IDC White Paper sponsored by EMC, As the EconomyContracts, the Digital Universe Expands, IDC, May 2009
6. Technology Trends You Can’t Afford to Ignore, Gartner Webinar, Nikos Drakos, Raymond Paquet, July 1, 2009
8. Technology Trends You Can’t Afford to Ignore, Gartner Webinar, Nikos Drakos, Raymond Paquet, July 1, 2009

---

**About Verizon Business**

Verizon Business, a unit of Verizon Communications (NYSE: VZ), is a global leader in communications and IT solutions. We combine professional expertise with one of the world’s most connected IP networks to deliver award-winning communications, IT, information security and network solutions. We securely connect today’s extended enterprises of widespread and mobile customers, partners, suppliers and employees—enabling them to increase productivity and efficiency and help preserve the environment. Many of the world’s largest businesses and governments—including 96 percent of the Fortune 1000 and thousands of government agencies and educational institutions—rely on our professional and managed services and network technologies to accelerate their business. Find out more at www.verizonbusiness.com.