Open Sesame: Who Sees What?

By Chuck Adams, Cisco IBSG Innovations Practice

Protecting valuable customer information is one of the most important IT responsibilities in any organization—from doctors' offices and hospitals, to financial institutions, to retailers. Traditionally, customer data, and all other information resources, were housed and processed in on-campus data centers under the watchful eyes of IT and security managers. Firewalls were placed around the perimeter of the enterprise to keep intruders out and data in. Maintaining strong protection at the border was enough to safeguard the most sensitive data. Unfortunately, this is no longer the case.

Today, enterprise borders are permeable, or even nonexistent. It is not unusual for important information resources—data services, applications, networking, storage, web services, and development services—to reside outside the traditional enterprise perimeter. Virtualization and cloud services have created a highly distributed environment in which data and processes might be hosted on virtual machines or "in the cloud" anywhere in the world. Increasingly, IT leaders are responsible for protecting data, applications, and processes that are outside their direct realm of control.

Upholding the Customers' Trust

Consumers routinely entrust personal and private information to the entities with which they do business, having no idea where that information will go, who will have access to it, or how it will be used. They give banks their social security numbers. Retailers know their credit card numbers and buying preferences. Healthcare institutions collect vital personal information and store it in electronic health records. In all these cases, the task of the IT security executive is the same: to uphold the trust of the customer by protecting this personal data, whether it resides in the enterprise or in the cloud.

Sometimes they fail. In June 2010, AT&T inadvertently exposed the e-mail addresses of more than 100,000 iPad 3G customers, including U.S. government and military users.[1] Hackers have accessed hotel, restaurant, and grocery store computers, putting hundreds of customers at risk of credit card fraud. Banks have lost laptops containing unencrypted customer account information. Healthcare organizations have inadvertently released confidential patient information. According to the Privacy Rights Clearinghouse, more than 500 million identity-specific records have been compromised in the United States since 2005. [2] This total does not count millions of other instances in which confidential information

was leaked that did not include account numbers, social security numbers, driver's license numbers, or other information that could enable identity theft.

Opportunity: Develop a Holistic Strategy for Embedded Security

Security failures can happen anywhere: in the enterprise, in the cloud, and wherever an employee or partner can access sensitive information via a smartphone, laptop, tablet, or other portable device. Whether the security leak is due to a stolen BlackBerry, a lost flash drive, or a compromised cloud environment, the ultimate responsibility lies with the enterprise that has been entrusted with the customer data. As the borders of the enterprise become more permeable, security professionals are responsible for protecting sensitive data that may be distributed throughout an infrastructure owned and managed by multiple vendors and service providers in multiple locations. This presents an opportunity to design and implement a comprehensive risk-management strategy that embeds policy-based security controls throughout the information architecture. By embedding security across the extended environment, rather than just at the borders, enterprises can ensure a blanket of protection for their valuable customer information.

Complication: "The Cloud" Extends Across a Patchwork of Local Jurisdictions, Regulations, and Standards

That comprehensive blanket of protection must extend to the cloud. When companies outsource data storage, subscribe to cloud-based applications, or scale their networks via infrastructure as a service, they really don't know where their information will reside, or what subcontractors may touch it. Customer management software may be hosted in Bangladesh or Brazil. Technical support representatives may access customer data from India or Ireland. Product development platforms may be distributed from Tennessee to Taiwan.

Each of these different geographies and jurisdictions has a different set of regulations and standards within which cloud service providers operate. Europe has more stringent privacy regulations than much of the rest of the world; California's laws are more rigorous than those of most other states. But in some parts of the world, data hosting or cloud service providers may be virtually unregulated, or regulations may not be enforced. How can an IT executive be sure that customer data remains secure—wherever it is?

Solution: Borderless Security for Borderless Networks

As network borders continue to expand across multiple geographies, devices, technologies, and vendors, security must also expand across these same frontiers. Security policy and protection must reach into every corner of the far-flung network where customer data might be stored or processed. Securing information resources in an increasingly borderless world begins with an overarching network architecture that enables IT to efficiently manage access from multiple locations, from multiple devices, and to applications that can be located anywhere. The key element in providing this sort of secure, scalable access is a policy-based, information-centric security architecture that allows IT to implement controls and enforce policy throughout this network—from server, to infrastructure, to client. To accomplish this, security must be integrated into the very fabric of the architecture, not something that is added on.

Enterprises must then extend this blanket of protection to encompass all vendors and service providers that may touch the enterprise information, including the subcontractors and hosting services they may employ. They should investigate potential cloud service providers thoroughly and demand information about the hiring, training, and oversight of vendor employees who have privileged access to their sensitive data. They also need to understand the vendor's data protection schemes and operational continuity procedures. Compliance with specific standards and regulations should be required in the contractual agreements enterprises make with their vendors.

It is the responsibility of enterprise IT professionals to ensure that vendors comply with all appropriate privacy standards defined by their organizations, not just the local regulations of the jurisdiction within which they operate. They should consider compliance with ISO2700 data security standards as a baseline requirement for their vendors. On top of that are various national or regional regulations, such as those contained in the U.S. Sarbanes-Oxley legislation and California's security-breach notification requirements. The third layer of compliance is composed of industry-specific privacy regulations, such as those contained in the U.S. Health Insurance Portability and Accountability Act (HIPAA), and in the Gramm-Leach-Bliley Act regulating financial services. On the global front, the Payment Card Industry (PCI) Security Standards Council continues to define more rigorous standards for all involved in processing major credit card transactions. Enterprises should expect full compliance with this complex regulatory framework to be verified by regular independent audits.

Benefits: Flexibility and Efficiency, with Full Data Protection

For organizations that carefully ensure the security of their cloud-hosted information, the benefits are many. With cloud services, enterprises can respond quickly to unusual spikes in demand without making additional capital investments. They can subscribe to special application services delivered over the network without having to manage and maintain those applications. And they can use the cloud as a development platform for additional applications that run on the cloud infrastructure. They can access virtually unlimited storage capacity and computing power, on-demand, and pay only for what they need.

While we have focused largely on the risks associated with cloud computing, there are also a number of security benefits.[3] For example, the large-scale implementation of most cloud providers' services makes it more affordable for them to hire a large staff of security professionals and to deploy the most effective and advanced security practices available. Their larger scale also makes it easier to dynamically allocate resources for filtering, traffic management, identity verification, data encryption, and other measures. This offers multiple response choices for certain types of security issues, and creates more resilient services.

Furthermore, because security is one of the most important factors in selecting a cloud-computing vendor, cloud service providers view ironclad security as an important competitive advantage. In many cases, especially for small and medium-sized companies, the security measures available through cloud computing vendors will be more effective and affordable than their in-house security services. And if there *is* a data breach, it will be easier to gather and retain log files and other evidence.

Conclusion

CIOs should begin to evaluate their current information security architecture and prepare to transform their role and organization. Begin by taking the following steps:

- Work directly with security managers to design a comprehensive and holistic strategy for information security, with a minimum goal of compliance with ISO27000 standards and any additional requirement that are applicable
- Determine the most critical types of information and design commensurate information security policies and controls to actively protect each. Where information is destined for an external enterprise, design contractual controls to ensure information security to the same degree as within your enterprise
- Thoroughly investigate potential cloud vendors to ensure robust security capabilities and compliance with all appropriate standards and regulations, and prepare to routinely audit their performance
- Transform security-management procurement processes and purchasing criteria to focus on interoperability and alignment with the security strategy; include the right to audit and evaluate audit results in contracts with vendors

Keeping customers' trust means keeping their data secure, whether it is in the enterprise data center, or in the cloud. IT executives should take a comprehensive risk-management approach to their own networks, and then contractually extend that blanket of protection to all the vendors and service providers that touch their sensitive information resources.

For more information, please contact:

Chuck Adams
Business Resiliency Solutions Manager
Cisco Internet Business Solutions Group
cjadams@cisco.com
+1-512-340-3430

Endnotes

1. "AT&T Security Breach Exposes iPad 3G Customer Data (Updated 2x)," Jason D. O'Grady, ZDNet, June 10, 2010.
2. "Chronology of Data Security Breaches, 2005-Present," Privacy Rights Clearinghouse, http://www.privacyrights.org/data-breach#CP, September 16, 2010.
3. For a more complete description of these benefits, see "The Security Benefits of Cloud Computing," Cloudtweaks, August 15, 2010 (http://www.cloudtweaks.com/2010/08/the-security-benefits-of-cloud-computing/)

Cheri Goodman of Cisco IBSG provided writing and editing assistance for this paper.

More Information

Cisco Internet Business Solutions Group (IBSG), the company's global consultancy, helps CXOs from the world's largest public and private organizations solve critical business challenges. By connecting strategy, process, and technology, Cisco IBSG industry experts enable customers to turn visionary ideas into value.

For further information about IBSG, visit http://www.cisco.com/go/ibsg.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**