THE OFFICIAL PUBLICATION OF THE CHANNEL PARTNERS CONFERENCE & EXPO

VOLUME 2, ISSUE 5, JULY 2012

Channel Partners™

www.channelpartnersonline.com

$9 US

CLOUD SECURITY

A SPECIAL ALL-DIGITAL, GREEN ISSUE

Locking Down THE CLOUD WORKSPACE

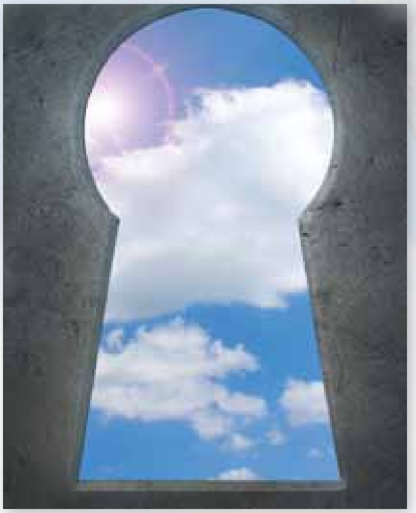
IN THIS ISSUE:

CONTENTS

www.channelpartnersonline.com

July 2012

Channel Partners



OPINION

FEATURES

Is Cloud Ready or Risky?

While cloud is ever-present in the tech lexicon, more than half of IT pros who responded to a May 2012 survey from Wisegate said it's "too risky for prime time" and only suitable for commodity applications like CRM and email. Security is still a major concern, the poll found.

Certainly, security cannot be ignored, but it's also not insurmountable. It's not wholly different from securing on-premises systems, experts say; it's just that the perimeter has changed. In addition, many companies find that their cloud service provider does a much more diligent job of managing security than they can do as an individual organization.

This digital issue takes a look at the security profile of predominant cloud architectures as well as the all-important and vulnerable endpoints, plus it offers advice for questions to ask cloud providers and ways to counter customer concerns. It also reviews the top threats and governance areas as identified by the Cloud Security Alliance.

As always, we would welcome your feedback on the content and the digital issue experience. You can contact me at khenderson@vpico.com or on Twitter.

Enjoy!

Khali Henderson

KHALI HENDERSON
Editor-in-Chief
Twitter: @khalihenderson

MOREINFO

RESEARCH

Cloud Computing 'May Be a Lot of Hot Air'

IN THIS ISSUE
Table of Contents p. 2 ■ Top 7 Security Threats p. 6

In here, our cloud has your customers covered.

Increase flexibility and efficiency with AT&T Cloud Solutions. In order to keep on top of customer concerns about their data, they need storage that can adjust to meet their demands. AT&T Cloud services allow customers to store data in one of two U.S.–located AT&T Data Centers, on a virtualized infrastructure that's monitored 24/7, 365 days a year, and incorporate physical and network-based security. With AT&T managing the infrastructure, your customers can manage their business data cost effectively and feel confident while doing it. To see what a network of possibilities can do for your business, visit **att.com/inthecloud**.

Already a Solution Provider? Contact your Channel Manager to learn more about selling AT&T Cloud Solutions. Interested in becoming an AT&T Solution Provider? Visit att.com/alliance for more information.

It's the AT&T network – a network of possibilities.

Rethink Possible®

TOP 7 THREATS to Cloud Computing

To help organizations in making educated risk-management decisions regarding their cloud adoption strategies, the Cloud Security Alliance has compiled a guide to the top cloud computing threats. The list is a companion to "Security Guidance for Critical Areas in Cloud Computing," the industry standard catalog of best practices in secure Cloud Computing. The top threats, as excerpted from the CSA report, "Top Threats to Cloud Computing," Version 1.0, include in no particular order:

1 Abuse and Nefarious Use of Cloud Computing

IaaS providers offer their customers the illusion of unlimited compute, network and storage capacity — often coupled with a

IN THIS ISSUE
Editor's Letter p. 4 ■ Critical Security Control Areas p. 12 ■ Table of Contents p. 2

"frictionless" registration process where anyone with a valid credit card can register and immediately begin using cloud services. Some providers even offer free limited trial periods. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors and other criminals have been able to conduct their activities with relative impunity. PaaS providers have traditionally suffered most from this kind of attack; however, recent evidence shows that hackers have begun to target IaaS vendors as well. Future areas of concern include password and key cracking, DDOS, launching dynamic attack points, hosting malicious data, botnet command and control, building rainbow tables and CAPTCHA solving farms.

2 Insecure Application Programming Interfaces

Cloud Computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency.

3 Malicious Insiders

The threat of a malicious insider is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance.

To complicate matters, there is often little or no visibility into the hiring standards and practices for cloud employees. This kind of situation clearly creates an attractive opportunity for an adversary — ranging from the hobbyist hacker, to organized crime, to corporate espionage, or even nation-state sponsored intrusion. The level

IN THIS ISSUE
Editor's Letter p. 4 ■ Critical Security Control Areas p. 12 ■ Table of Contents p. 2

of access granted could enable such an adversary to harvest confidential data or gain complete control over the cloud services with little or no risk of detection.

4 Shared Technology Vulnerabilities

IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (e.g., CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multitenant architecture. To address this gap, a virtualization hypervisor mediates access between guest operating systems and the physical compute resources. Still, even hypervisors have exhibited flaws that have enabled guest operating systems to gain inappropriate levels of control or influence on the underlying platform.

A defense-in-depth strategy is recommended, and should include compute, storage and network security enforcement and monitoring. Strong compartmentalization should be employed to ensure that individual customers do not impact the operations of other tenants running on the same cloud provider. Customers should not have access to any other tenant's actual or residual data, network traffic, etc.

> A defense-in-depth strategy is recommended, and should include compute, storage and network security enforcement and monitoring.

5 Data Loss/Leakage

There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. Loss of an encoding key may result in effective destruction. Finally, unauthorized parties must be prevented from gaining access to sensitive data.

The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment.

IN THIS ISSUE
Editor's Letter p. 4 ■ Critical Security Control Areas p. 12 ■ Table of Contents p. 2

6 Account, Service & Traffic Hijacking

Account or service hijacking is not new. Attack methods such as phishing, fraud and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks.

Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

7 Unknown Risk Profile

One of the tenets of Cloud Computing is the reduction of hardware and software ownership and maintenance to allow companies to focus on their core business strengths. This has clear financial and operational benefits, which must be weighed carefully against the contradictory security concerns — complicated by the fact that cloud deployments are driven by anticipated benefits, by groups who may lose track of the security ramifications.

Versions of software, code updates, security practices, vulnerability profiles, intrusion attempts, and security design, are all important factors for estimating your company's security posture. Information about who is sharing your infrastructure may be pertinent, in addition to network intrusion logs, redirection attempts and/or successes, and other logs.

Security by obscurity may be low effort, but it can result in unknown exposures. It may also impair the in-depth analysis required highly controlled or regulated operational areas. **CP**

MOREINFO

WHITE PAPERS

Security Guidance for Critical Areas in Cloud Computing

Top Threats to Cloud Computing

SOURCE

Cloud Security Alliance

IN THIS ISSUE
Editor's Letter p. 4 ■ Critical Security Control Areas p. 12 ■ Table of Contents p. 2

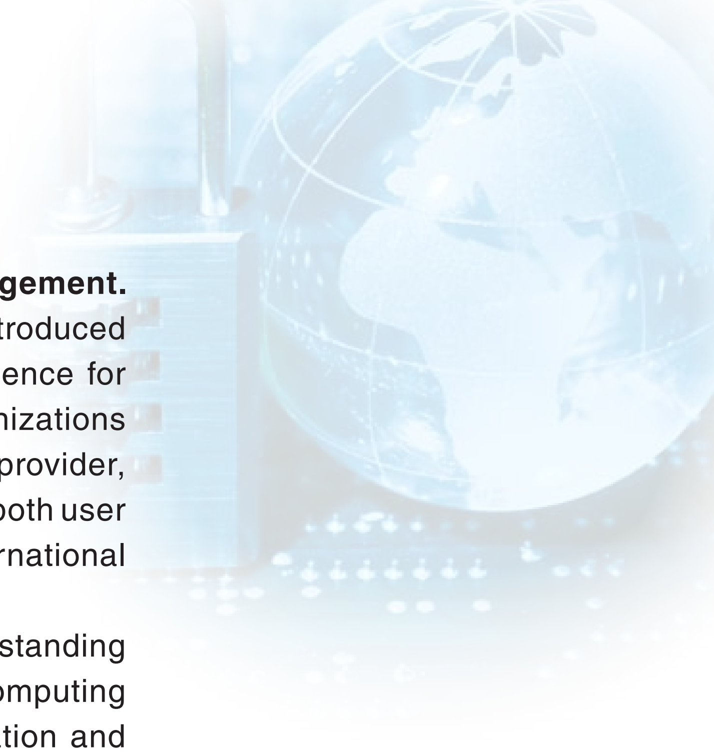
Critical Control Areas for Cloud Security

Security controls in cloud computing are, for the most part, no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models and the technologies used to enable cloud services, cloud computing may present different risks to an organization than traditional IT solutions.

The Cloud Security Alliance has identified 12 domains, addressing both the strategic and tactical security "pain points" within a cloud environment. The domains are divided into two broad categories: governance and operations. The governance domains are broad and address strategic and policy issues within a cloud computing environment, while the operational domains focus on more tactical security concerns and implementation within the architecture.

They include the following, as excerpted from the CSA guide, "Security Guidance for Critical Areas of Focus in Cloud Computing," Version 3.

IN THIS ISSUE
Top 7 Security Threats p. 6 ■ Securing Different Cloud Types p. 16 ■ Table of Contents p. 2



GOVERNANCE DOMAINS

Governance and Enterprise Risk Management. Governing and measuring enterprise risk introduced by cloud computing, including legal precedence for agreement breaches, ability of user organizations to adequately assess risk of a cloud provider, responsibility to protect sensitive data when both user and provider may be at fault, and how international boundaries may affect these issues.

Legal and Electronic Discovery. Understanding potential legal issues when using cloud computing include protection requirements for information and computer systems, security breach disclosure laws, regulatory requirements, privacy requirements, international laws, etc.

Compliance and Audit. Maintaining and proving compliance when using cloud computing, including evaluating how cloud computing affects compliance with internal security policies, as well as various compliance requirements (regulatory, legislative, and otherwise). This domain includes direction on proving compliance during an audit.

Information Life Cycle Management. Managing data that is placed in the cloud, including identification and control of data in the cloud, compensating controls that can be used to deal with the loss of physical control when moving data to the cloud as well as data confidentiality, integrity and availability.

Portability and Interoperability. Evaluating the ability to move data/services from one provider to another, or bring it entirely back in-house as well as interoperability between providers.

> Because of the cloud service models employed, the operational models and the technologies used to enable cloud services, cloud computing may present different risks to an organization than traditional IT solutions.

OPERATIONAL DOMAINS

Traditional Security, Business Continuity and Disaster Recovery. Assessing the impact —

IN THIS ISSUE
Top 7 Security Threats p. 6 ■ Securing Different Cloud Types p. 16 ■ Table of Contents p. 2

risks increases and decreases — of cloud computing on operational processes and procedures used to implement security, business continuity and disaster recovery.

Data Center Operations. Evaluating a provider's data center architecture and operations to identify common data center characteristics that could be detrimental to ongoing services, as well as characteristics that are fundamental to long-term stability.

Incident Response, Notification and Remediation. Ensuring proper and adequate incident detection, response, notification and remediation at both provider and user levels.

Application Security. Securing application software that is running on or being developed in the cloud, including whether it's appropriate to migrate or design an application to run in the cloud, and if so, what type of cloud platform is most appropriate (SaaS, PaaS, or IaaS).

Encryption and Key Management. Identifying proper encryption usage and scalable key management both for protecting access to resources as well as for protecting data.

Identity and Access Management. Managing identities and leveraging directory services to provide access control.

Virtualization. Evaluating the use of virtualization technology in cloud computing, including risks associated with multitenancy, VM isolation, VM co-residence, hypervisor vulnerabilities, etc. This domain focuses on the security issues surrounding system/hardware virtualization, rather than a more general survey of all forms of virtualization. **CP**

MOREINFO

WHITE PAPERS

Security Guidance for Critical Areas of Focus in Cloud Computing

SOURCE

Cloud Security Alliance

IN THIS ISSUE

Top 7 Security Threats p. 6 ■ Securing Different Cloud Types p. 16 ■ Table of Contents p. 2

Motorola Solutions PartnerEmpower™ Program

MAKE THE MOST OF OPPORTUNITY

Today is another opportunity to close the big deal. To set yourself apart from competitors. To build long-lasting relationships with customers. To bring true innovation to burgeoning markets. Are you ready?

As a member of the Motorola Solutions PartnerEmpower™ Program, you will be. PartnerEmpower provides a path to business growth through access to our top-ranked mobility and communications products, tools that help you drive sales, and the backing of a vendor that highly values its channel.

Team with Motorola Solutions today. Together, we can achieve new levels of success while helping customers rise in the moments that matter.

To get more information, visit us at **www.motorolasolutions.com/partnerempower**

PartnerEmpower™

Securing Public, Private & Hybrid Clouds

By Jebb Dykstra

When I ask a customer or a partner if they are ready to move to the cloud, I see a wrinkled brow. When I say security, either a look of fear crosses their face or their eyes glaze over. I am almost always speaking to a very technical audience. Confusion, fear and frustration aside, cloud is happening now — to such an extent that the federal government has issued a Federal Cloud Computing Strategy and said that cloud computing is a "profound economic and technical shift ... ." As both consumer and enterprise customers migrate to using and delivering cloud services, cloud security issues cannot be ignored. In his lecture at UCLA on Amazon Web Services Cloud, Dr. Werner Vogels, CTO of Amazon and the technical lead of the world's leading cloud service provider, said, "At the end of each presentation, I face three questions: one, security; two, security; three, security." Make no mistake about it, cloud security is critically important.

IN THIS ISSUE
Critical Security Control Areas p. 12 ■ Securing Cloud Endpoints p. 22 ■ Table of Contents p. 2

What complicates the cloud security issue is that different cloud architectures raise different questions, which lead to different answers. A silver bullet for cloud security does not exist. One must take into consideration whether you are dealing with a private, hybrid or public cloud. In a traditional data center, the goal is to keep the bad guys out. In a cloud, you do not have a traditional perimeter to defend (i.e., a moat around your data center). Therefore defending your territory is much more difficult. In the cloud, your exposures multiply and risks are increased. In a data center, you own the servers (and virtual machines if you choose to virtualize). In a cloud, you usually lease the servers and virtual machines. In most cases, you only control the virtual machines. This causes great anxiety when determining how and when to move the cloud. Your control over the environment in the cloud is greatly reduced, which leads to risk and exposure.

> In a traditional data center, the goal is to keep the bad guys out. In a cloud, you do not have a traditional perimeter to defend.

THREE MAIN ARCHITECTURES

So how do you resolve this loss of control, while still feeling good about migrating services and applications to a secure cloud?

When facing a decision of migrating software or services to the cloud, the first order of business is to seek out best practices and experts. One of the best resources for cloud computing best practices is guidance provided by experts engaged by the Federal Government at The National Institute of Standards and Technologies (NIST). NIST has published numerous reports on cloud computing and cloud security. Many of the leading reports can be found at NIST's website. In addition, with a quick search query and a phone call, you will likely be able to interview numerous consulting agencies as to how they can best serve your needs by securing your data, software, services and applications in your cloud of choice.

The National Institute of Standards and Technologies (NIST) defines six different types of cloud architectures. However, these different architectures are variations on the themes of private, hybrid or public cloud. The variations include whether the servers, hypervisors, operating systems, virtual machines or cloud are on-premises, off-site or a multitenant/shared community. In each circumstance, cloud security will be handled differently.

IN THIS ISSUE
Critical Security Control Areas p. 12 ■ Securing Cloud Endpoints p. 22 ■ Table of Contents p. 2

According to NIST, a hybrid cloud is defined as two or more independent facilities bound together, such as an on-premises data center bound to private or public cloud infrastructure.

Private Cloud. For many considering a migration to the cloud, private clouds are a welcome relief because the loss of control is mitigated to the greatest degree. Private clouds generally are defined by NIST and Wikipedia as cloud infrastructure operated and dedicated to a single tenant. The servers and the virtual machines are not shared with any other organization. This makes private clouds typically the most secure and usually the first step for an enterprise to the cloud. In some cases, you may even own the servers, the virtual machines and the cloud may even be located inside your data center. If this is the case, then the security architecture is similar to a traditional data center in terms of "defending the perimeter." However, depending upon how much control you cede to the cloud provider (or managed service provider) for a private cloud, instead of taking direct responsibility for cloud security, you may end up auditing or reviewing your cloud provider's security practices to ensure your software, services, applications and data are secure.

Hybrid Cloud. According to NIST, a hybrid cloud is defined as two or more independent facilities bound together, such as an on-premises data center bound to private or public cloud infrastructure. In a hybrid cloud, you face a dual approach to security. As described above, you can protect your data center infrastructure in the traditional approach — "secure the perimeter." But you cannot treat your bound private cloud or public cloud infrastructure with the same security approach. You must define the type of cloud infrastructure you have architected. What is it that you are protecting? Are you protecting just the virtual machines as described above? Or is there more, such as the hypervisor or the OS? Who is responsible for the firewalls? What about the application stacks? Who is going to be responsible for updates on the app stacks? Do you monitor your own app code? Will you have to manually track all of these activities? Is it automated? You do not need to know all of these answers, but someone has to be able to answer them.

Public Cloud. A public cloud raises different security questions than if you are using a private or hybrid cloud. If you are reselling Google Apps, IBM's Lotus Live, Microsoft's Office365, HP or Oracle (or any other large company's software or cloud services), then you probably are thinking you don't have to worry about security

IN THIS ISSUE
Critical Security Control Areas p. 12 ■ Securing Cloud Endpoints p. 22 ■ Table of Contents p. 2

since that is their problem. You take it for granted that they have it covered. To some extent, this may be perfectly reasonable, especially when dealing with household. However, many of the above questions can and should be posed to your public cloud provider.

At some point, just letting the large software or cloud provider handle cloud security will not be enough if you are dealing with any reasonable-sized customer or a complex cloud applications that knit together different software products. Selling cloud services is rarely one dimensional and usually multiple vendors are involved. Expect that your customer will demand you answer their cloud and security questions in specific detail. This happens the moment you let them know the cost of such cloud services. Complex cloud security questions arise with even small customers, not always because of their size, but also because of the size of their customer base.

Cloud security cannot to be ignored or taken for granted. Depending upon your cloud of choice, your answers to cloud security will be slightly different. But by following some of the best practices suggested by NIST and by taking a proactive approach to security in the cloud, you will be ready for this profound economic and technical shift to cloud computing securely. **CP**

Jebb Dykstra is CEO of Meetrix Communications. An entrepreneur and IP/software lawyer for the last 16 years, he has worked with venture capital-backed companies including Meetrix Communications (AVG Ventures), OneStop Internet (Bessemer Ventures/Fung Capital), Education Revolution (acquired by Camelback Education), Universal Business Matrix (DFJ), Unidym (Arrowhead Research), FastPoint Games (DFJ, DFJ Dragon and Mission Ventures) and Coax Corporation (Southridge Capital). Previously, Dykstra worked for Irdeto Group (part of the Naspers Group), Howrey & Simon and PriceWaterhouseCoopers (now a part of IBM). He currently teaches cyber security law and cloud computing law at the University of Denver as an adjunct professor.

MOREINFO

ARTICLE

The Rise of the Cloud Integrator

BLOG

Cloud Jumps the Chasm: Are Solution Providers Ready for the Road Ahead?

SOURCES

Meetrix Communications

NIST

IF YOU WANT YOUR DATA TO BE SAFE, DON'T WORRY. WE USE PROTECTION.

Data is precious. Every bit and byte is someone's brainchild. Which is why we protect them like they were our own. We have four geographically diverse SSAE16 datacenters for worry-free cloud computing and app delivery. We offer remote backup to make sure there's a secure mirror image of your on-site data. And we have high-speed fixed wireless Internet/ VoIP backup, plus redundancy and forwarding options for landlines. It's like bubble wrap for electrons. Safety first.

TelePacific®
TELEPARTNER PROGRAM
Simplicity. Support. Succe$$.

Become an Agent | Learn about our SSAE16 datacenters

A network solutions provider serving businesses nationwide 877-GO-AGENT TelePacificAgent.com

Securing Cloud Endpoints

By John Eldh

Symantec commissioned the "2012 Endpoint Security Best Practices Survey" to see how IT is coping with endpoint security.

A new era in IT service delivery has dawned with the rapidly increasing adoption of cloud computing, and with it come concerns about safety in hosted environments. This technology is doing more than just transforming the data center. It is revolutionizing business processes and the way businesses are interacting with their clients. This marked change in how businesses will operate presents channel partners with several significant opportunities – including how to secure your customers' endpoints with the proliferation of the cloud.

Symantec commissioned the "2012 Endpoint Security Best Practices Survey" to see how IT is coping with endpoint security. The findings show a wide variance between how the best and worst organizations handle endpoint security. Ultimately and not surprisingly, those organizations employing best practices are enjoying dramatically better outcomes. Following are key findings of our survey.

IN THIS ISSUE
Securing Different Cloud Types p. 16 ■ Security Questions to Ask p. 28 ■ Table of Contents p. 2

The typical organization incurred $470,000 in losses due to endpoint cyber attacks in the past 12 months.

Top-tier organizations fare better against attacks. The organizations that had deployed more comprehensive security technologies and practices were better prepared and better able to thwart attacks, and reduce the amount of money and time spent doing so. The top-tier companies were 2.5 times less likely to experience a large number of cyber attacks, and 3.5 times less likely to experience downtime.

Top-tier companies only experienced 21 percent of the downtime of the lower-tier businesses — a total of 588 hours compared to 2,765 hours.

Top-tier organizations employ the latest in endpoint protection technologies and practices. We asked survey respondents what precautions they were taking to protect their endpoints. Based on the safeguards, policies and procedures they employed, we were able to divide businesses into three tiers of preparation, and compared the organizations that were in the top tier with those in the bottom tier to see what distinguishes them from each other.

Among these top performers, nearly 100 percent indicated they keep their endpoints — including virtual and physical servers, virtual and physical desktops, laptops/netbooks and mobile devices — somewhat or completely updated with current operating system and application updates through the entire organization.

These companies not only have deployed virus and spyware protection across nearly all of their virtual and physical endpoints, they also have deployed firewall protection, intrusion prevention systems, and tools to prevent unauthorized copying of data to and from peripheral devices such as USB drives. Nearly all of these top-tier companies also indicated that a wide range of endpoint security safeguards and technologies are somewhat-to-extremely necessary, including encryption, access control, data loss prevention and reputation-based security.

Finally, 99 percent of these top performers provide some form of employee security training, with 82 percent doing so at least once a year.

Attacks against endpoints are costly. The first thing we asked about in the survey was the cost incurred in dealing with a variety of endpoint-focused cyber attacks. We defined cyber attacks as attacks (either from inside or outside the organization) on the computer network, website, desktops and mobile devices, and virtual servers and desktops. Examples could be viruses, spam,

denial-of-service attacks, theft of information, fraud, vandalism and so forth. We then asked the respondents to indicate the costs they experienced as a result of cyber attacks on their endpoints.

Combining the frequency of attack (what percentage of respondents experienced each type of attack) with the magnitude (the average cost for each type of attack), we were able to determine that the typical organization incurred $470,000 in losses due to endpoint cyber attacks in the past 12 months.

The most common consequences of attacks were forced dedication of IT manpower to remediate affected endpoints; the loss of organization, customer or employee data; and damage to the organization's brand and reputation.

There is no single solution that will prevent all attacks, and companies should not rely solely on endpoint security technology for protection.

There is no single solution that will prevent all attacks, and companies should not rely solely on endpoint security technology for protection. To reduce the risk of a successful cyber attack, here are some steps any organization can take that will reassure your customers that their business-critical applications are safe in hosted environments:

•*Assess the risk.* It's vital that businesses identify and classify confidential information. They must know where sensitive information resides, who has access to it, and how it is entering or leaving the organization. In addition, businesses should continually assess their network and endpoints to identify possible vulnerabilities.

•*Minimize the risk***.** Businesses must implement a multilayer protection strategy to minimize the risk of exploited endpoints. In addition to traditional antivirus, firewall and host intrusion-protection technology, they should deploy the latest innovations in endpoint security, such as reputation-based security and real-time behavioral monitoring. These newer technologies provide additional efficacy in the battle to thwart many new cyber attack strategies. Finally, businesses must patch applications and systems regularly.

•*Education is crucial.* Businesses should also train employees on the risks and what they need to do for safe computing, and hold them accountable. Eighty-two percent of top-tier companies provide security training to their employees annually, compared to 66 percent of bottom-tier businesses.

IN THIS ISSUE
Securing Different Cloud Types p. 16 ■ Security Questions to Ask p. 28 ■ Table of Contents p. 2

•*Be prepared.* It's important to prepare for the inevitable by creating a full incident response plan. It's also vital to occasionally practice implementing the plan. When the time comes to put the plan into action, it will help businesses by improving their response time and will ensure a more complete response.

Following these steps will keep you ahead of the curve in securing your customers' endpoints, and it frees your customers to focus on the most vital part of their IT infrastructure: the data they need to run their business. It also provides a solid foundation to ensure that adaptation for future needs will be as smooth as possible. Establishing cloud security from day one will maximize your customers' — and your — ability to compete in the 21st century marketplace. **CP**

MOREINFO

BLOG

Cloud Security Starts at the Endpoint

RESEARCH

Survey: Cloud Adoption Very Slow

2012 Endpoint Security Best Practices Survey

SOURCE

Symantec Corp.

John Eldh is vice president of channel sales for the Americas at Symantec Corp., where he is responsible for the security company's enterprise channel and distribution strategy, as well as partner programs for all market segments, including SMB, midmarket, public sector, VARs and national partners. During his seven years at Symantec, he has held sales leadership positions. Most recently, he was vice president of sales for Symantec.cloud and was responsible for architecting the group's go-to-market and channel strategy.

IN THIS ISSUE
Securing Different Cloud Types p. 16 ■ Security Questions to Ask p. 28 ■ Table of Contents p. 2

WHERE DO YOU FIT IN THE LOOP?

The worlds of telecom and IT are coming together. Be a part of the mix in Orlando this September.

Are you an early-adopter who is already selling complete business productivity solutions? Or are you an IT/VAR or telecom agent who is ready to take the next step and diversify your revenue? Wherever you fit in the converging channel, the Channel Partners Conference & Expo is right for you.

REGISTER EARLY for the **Conference & Expo Package**. You can save up to $50 while getting access to the education, networking and solutions you need.

This premier package give you access to:

- The Expo Hall featuring the top exhibitors in the industry
- Four concurrent education tracks
- The Keynote Address
- The Keynote Roundtable
- The Opening Reception
- Two Continental Breakfasts
- Vendor Presentations

The convergence of the channel is happening.
Take advantage of it. Define your place in the loop.

IT
Channel Partners
Conference & Expo
TELECOM

Visit our all-new website at
channelpartnersconference.com

Enabling the Converging Channel
September 12-14, 2012
The Peabody Orlando

15 YEARS OF CHANNEL LEADERSHIP

Questions to Ask Cloud Providers About Security

By Jim Lippard

Gaining efficiency and reducing costs are clear benefits driving the movement of IT infrastructure into the cloud, while security is the main worry that prevents it. But asking the right questions can help you to not only reduce your risks, but enable you to control them more effectively than you can with an on-premises IT infrastructure. The business continuity and disaster recovery benefits of geographic distribution may be obvious. Perhaps less obvious is that a provider may be able to use its economy of scale to hire specialized expertise, as well as solve particular problems common to many customers within a particular niche or vertical market. By asking the right questions, you can find a provider with contract terms and SLAs that establish the foundation for a sound and trusted business relationship.

IN THIS ISSUE
Securing Cloud Endpoints p. 22 ■ Countering Customer Objections p. 34 ■ Table of Contents p. 2

Your first questions should be directed to the customer: What is the nature of the data and services they plan to move to the cloud, and what would be the impact to the business if a breach exposed them to the public, to other customers sharing the same infrastructure or to the provider? The answers to these questions will help you to ask the right questions of the service provider regarding its architecture, deployment models and controls. It is important to keep in mind that your clients customers and suppliers are still going to hold them responsible for what happens to information they provide — whether it's managed in-house or by a third party.

> It is no longer a question of whether your organization will suffer a breach, but when and how quickly you will notice and respond.

CONTROLS & GOVERNANCE

The next questions are for the provider, particularly about how it can provide assurance that the client's requirements are met on an ongoing basis.

What visibility will you have into the effectiveness of the security controls of the solution? What logs and reports will you (and your auditors) be able to access? What certifications are held by the provider, and are there any audit reports that you can review? Do you have any audit rights?

What SLAs are provided and are they negotiable? What remedies are offered in the event that SLAs are not met?

Insight into the overall security stance of the provider, and its compatibility with your client's, may be gained by asking open-ended questions about the provider's security controls — namely, what are they? An answer in vague generalities is less acceptable than specifics, which make reference to particular security standards and frameworks, and a few such references is less acceptable than an ability to offer details about what is actually in place to meet them. A provider with an SSAE 16 audit of their data center is better than one without. Better still is a provider who can provide you with the appropriate type of Service Organization Control (SOC) report for the service being provided (SOC 1 for financial auditors, SOC 2 IT auditors, SOC 3 for more general audience) and (for SOC 2/3) covering the relevant Trust Services Principles for the type of data and service involved.

IN THIS ISSUE
Securing Cloud Endpoints p. 22 ■ Countering Customer Objections p. 34 ■ Table of Contents p. 2

Channel Partners
SOLUTION CENTER

Hosted Voice for Your Clients

Your customers look to you to provide answers. This FREE Channel Partners Solution Center focuses on the key benefits of switching to hosted voice with an ROI calculator, whitepapers, case studies and videos.

MegaPath

FIRST, PROVIDE US WITH A FEW DETAILS.

ROI CALCULATOR

See How Much Your Customers Save By Switching Today

Follow the steps in this ROI Calculator to see how much your customers can save on Hosted VoIP

MegaPath

Practical Guidance for Purchasing Hosted Voice Solutions

WHITEPAPERS

Covering topics such as:

- Countdown to Satisfaction:
  Top Considerations in Choosing a Hosted VoIP Provider
- Hosted Voice for the SMB Distributed Workforce
- SMB Cost Savings with Hosted Voice
- Voice Services – Quality of Service and Technology

MegaPath

VIZIOSoft Builds Client Relationships, and Its Business, with Hosted Voice and Data Service from MegaPath

CASE STUDIES

- VIZIOSoft Case Study
- Gorilla Tango Case Study

SPONSORED BY

MegaPath™
DATA · VOICE · SECURITY

Find the complete Solution Center at:
www.channelpartnersonline.com/solution-centers.aspx

What certifications has its staff earned? Does the provider employ dedicated security staff with industry certifications, as well as engineers with vendor-specific certifications? Does the provider also employ business process people with ITIL or ISO 20000 IT service management knowledge? How does the provider do change management?

The data your client stores in the cloud may be sensitive proprietary information, or it may include personally identifiable information subject to breach laws or other regulatory requirements.

DATA PROTECTION

The data your client stores in the cloud may be sensitive proprietary information, or it may include personally identifiable information subject to breach laws or other regulatory requirements. You need to ask questions about how that data is protected. How is it secured in transit, both en route to and from the provider, as well as when it moves within a virtual environment? How is it secured at rest? Is encryption used, and how are keys managed? Are there solutions available where you control the keys, so that the data is not visible to the provider? What controls protect your data from unauthorized modification or destruction? How are security profiles associated with the data maintained when the data moves from one environment to another? How is data destruction ensured when the data is removed or upon termination of the contract? Do you retain ownership and control over the data so that you can remove it in a usable, portable form for use with another provider?

IDENTITY & ACCESS MANAGEMENT

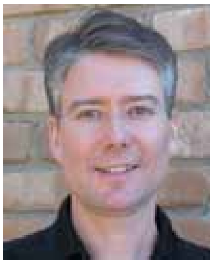
Your client's data in the cloud environment will need to be used in some way, directly or indirectly, by individual users. How will the provider authenticate those users and monitor their activity? Ideally, you want to reduce the complexity of user management, perhaps by using a form of federated identity based on SAML (such as Active Directory Federation Services) or OpenID, which can also help with visibility. What mechanisms are available to control access for authorized users to cloud resources, at what level of granularity, and with what audit trails?

IN THIS ISSUE
Securing Cloud Endpoints p. 22 ■ Countering Customer Objections p. 34 ■ Table of Contents p. 2

INCIDENT RESPONSE

In the last several years, reports of major breaches at prominent companies have made it more and more evident that preventive controls are never sufficient. It is no longer a question of whether your organization will suffer a breach, but when and how quickly you will notice and respond. The importance of detective and corrective controls, as well as having a strong incident response capability, cannot be underestimated. You'll want such capabilities from the cloud service provider, and some open-ended questions will help set the stage. What are your incident response capabilities? Have you had any breaches, and, if so, what did you do? Both of these are great initial questions. It's important to ask about change management (again) and configuration management, how does the provider recognize when unauthorized changes occur? A provider that is unwilling to talk about such details is probably unsuitable as a trusted partner managing your most critical data.

These questions are just a start. Ideally, you'll want to familiarize yourself with documents on the risks of cloud computing, which cover the above areas (taken from section 4 of NIST 800-144) and others, such as the white paper noted in the column to the right. **CP**



Jim Lippard is a senior product manager for security products at EarthLink IT Services. His career began in information technology as a systems developer on the Multics operating system, where he participated in the reviews and testing that led to the first B2 security rating from the National Computer Security Center. He held security operations and architecture leadership positions at Primenet, GlobalCenter, Frontier and Global Crossing, and did R&D work at Genuity. He was the technical editor for "Extreme Exploits: Advanced Defenses Against Hardcore Hacks" and contributed the entry on botnets to the "Encyclopedia of CyberCrime."

MOREINFO

WHITEPAPER

NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing

SOURCES

EarthLink Business

ITIL

IN THIS ISSUE
Securing Cloud Endpoints p. 22 ■ Countering Customer Objections p. 34 ■ Table of Contents p. 2

Selling Techniques Immersion Center

A Free Resource To Help You Diversify Revenue and Sell New Products & Services

The Selling Techniques Networking event at the Channel Partners Conference & Expo in spring offered channel partners – agents, VARs and dealers – the chance to come together and discuss successful sales of emerging products and services such as:

- Cloud Computing and Communications
- Conferencing and Collaboration
- Hosted VoIP
- Ethernet
- MPLS
- Wireless/Mobility
- SIP Trunking
- UC
- Energy

This Immersion Center includes six reports with input from those discussions, on-site polling and secondary research.

Find the new techniques you need to close your next big sale. Visit the Immersion Center today at **www.channelpartnersonline.com**

SPONSORED BY:

AireSpring Altēva COMMUNICATIONS. UNIFIED. SIMPLIFIED. IN THE CLOUD. COMMUNICATION CMS MANAGEMENT SERVICES IBM Quest TECHNOLOGY MANAGEMENT FOR BUSINESS questsys.com sidera networks simplewan viawest Centered Around You

Countering Customers' Cloud Security Concerns

By Sanjay Srinivasan

The forecast for cloud security should read "sunny and clear" but enterprises looking to adopt cloud-based IT and communications services continue to deal with uncertainty about whether the services they receive and, more importantly, any of their content is truly secure. They certainly recognize all the other business benefits of cloud based services (including but not limited to access to services and information wherever you are, business continuity in the event of a disaster, opex vs. capex and others) but balk at signing on until they are comfortable that the services are secure. This provides a great opportunity for service providers to differentiate themselves from others in the area of cloud security using a combination of technology, messaging and most importantly education about cloud security. It is the author's opinion that FUD is probably the biggest contributor to an enterprise's insecurity about cloud security. The remainder of this article outlines some strategies to use to overcome objections about cloud security.

IN THIS ISSUE

Security Questions to Ask p. 28 ■ Contacts p. 40 ■ Table of Contents p. 2

The list of strategies actually begins with an observation: The very same decision makers that struggle with this question for their businesses use cloud-based services in their personal lives and do so with some of their most critical private information — online banking is an example. Consumers believe this to be secure and that belief is not coming from them having any deep dive into the bank's cloud design — that belief may largely be coming from the fact that the banking industry is regulated and that someone else is ensuring that everything is secure. As we look into this deeper, it will be apparent that third-party testing, certification and compliance will be a key strategy toward overcoming objections.

Many enterprises believe that their computing or communications is more secure when it remains entirely on their premises or if they build a private cloud. While it is technically feasible for enterprises to design a solution that is secure, the operational aspect of the IT and communications services over time result in security becoming

Overcoming Insecurity About Cloud Security

Strategies for overcoming objections about cloud security include:

- **Addressing the FUD that exists about cloud security by separating fact from hearsay**
- **Highlighting the fact that security breaches largely come from operational issues vs. technology issues and that enterprises aren't as well equipped to stay on top of operational practices**
- **Explaining that service providers are often required to have regulatory compliance audits and approvals in place to sell services to specific verticals. As a result, all their customers receive the benefit**
- **Stressing that service providers are more plugged into the hacker world than are enterprises and hence remain current or ahead of the state of the art**
- **Reminding enterprise decision makers that they have adopted cloud-based services in their private lives and should consider applying the same decision-making process toward deciding whether cloud-based services are right for their enterprises**

IN THIS ISSUE
Security Questions to Ask p. 28 ■ Contacts p. 40 ■ Table of Contents p. 2

Channel Partners
Whitepapers

DISCOVER
New Solutions.
BE A
Trusted Advisor.

White Paper

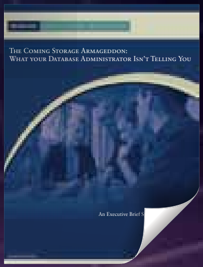
Storage-efficient Data Protection and Retention

Storage-Efficient Data Protection and Retention

Businesses are creating data in unprecedented volumes, varieties and velocities. Tapping into the value of that so-called Big Data is critical – so critical that companies have a very limited tolerance for downtime. At the same time, budget constraints make ensuring data is available and backed up is a challenge that will only worsen. This whitepaper discusses data protection and retention tools that meet the current market demands for faster, smarter and cheaper.

In this whitepaper, experts:

- Assess Data Growth's Impact on Data Protection and Retention
- Weigh The Dilemma of Minimizing Risk Versus Minimizing Cost
- Review IBM Portfolio Solutions Addressing Data Protection and Retention


The Coming Storage Armageddon: What your Database Administrator Isn't Telling You

An Executive Brief

The Coming Storage Armageddon: What Your Database Administrator Isn't Telling You

The truth is that data growth is outpacing our ability to process, analyze and store it. Enterprise storage needs are growing at 40 percent per year.

The unbridled data growth and inefficient storage can cause application performance problems. This whitepaper explores how to redesign storage by:

- Reducing the amount of data to be stored
- Storing data in the right place
- Optimizing the existing storage environment

Sponsored by:
IBM

Get your FREE copy of these featured Whitepapers at
www.channelpartnersonline.com/whitepapers

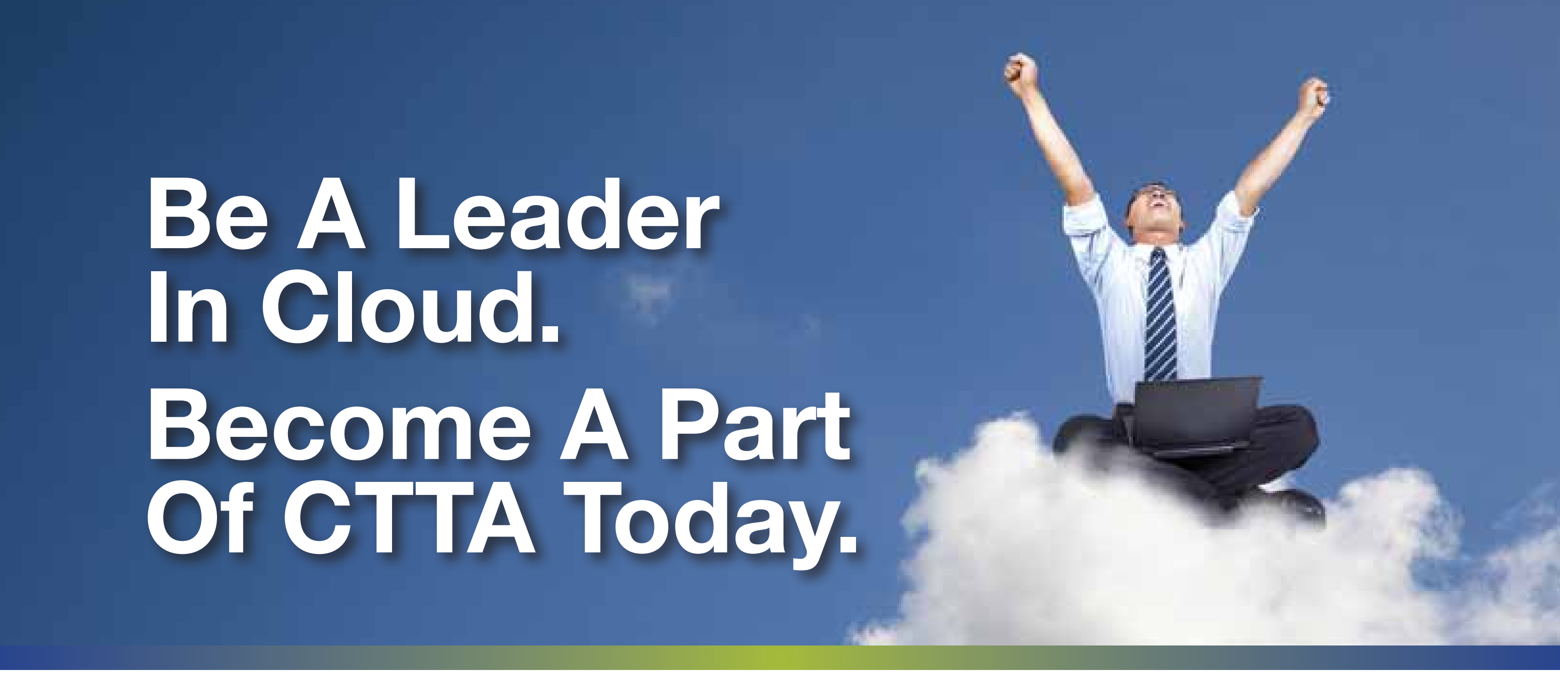
increasingly lax. This degradation often comes from process engineering failures — weak passwords, password change policies that were strong when they started but succumbed to user pressure and eased up on the policies, amongst others. Enterprises in the SMB sector often do not have the budgets and the resources to ensure that security practices are being stringently followed; in fact they may not even know that this is not happening, as there is no formal audit process in place. By comparison, service providers can offer cloud services that are built around stringent security requirements including ongoing compliance audits and reports.

Economies of scale have a big bearing on security as well; providers are able to spread the cost of the technology, process, people and systems across their entire customer base.

Service provider clouds are typically better at balancing security and usability. The easiest way to secure a private cloud is to lock it down like Fort Knox. Even that strategy can backfire if employees get frustrated and look for ways to circumvent security just so they can get access from wherever they are, including their home office, hotel room and airport lounge. The service provider architecture, on the other hand, has to be designed for a Fort Knox-level of security and access, and they are in a better position to establish points of presence wherever their customers are. Economies of scale have a big bearing on security as well; providers are able to spread the cost of the technology, process, people and systems across their entire customer base. In contrast, the enterprise is limited by its size; any extra cost must either make its way into their pricing or cut in to their profit margin — neither being a desirable outcome.

Hackers are almost always a step ahead of the enterprises in discovering and exploiting security loopholes. The typical enterprise does take the normal step of protecting the network using firewalls, intrusion detection and prevention services and similar appliances and services. However, that is only step one in securing the enterprise. It is critical that the enterprise is plugged into the world of hackers to stay current with, if not ahead of, what is happening in the hacker's domain. If the enterprise gets disconnected from this, they will also miss notifications about new threats and how to protect against them. They may certainly think about outsourcing the Security Operations Center function of their organization but that very thought process should also set them thinking about why they would not move relevant portions of their IT and communications into the cloud with a service provider that is

IN THIS ISSUE
Security Questions to Ask p. 28 ■ Contacts p. 40 ■ Table of Contents p. 2



Be A Leader
In Cloud.
Become A Part
Of CTTA Today.

in fact plugged into the hacker's ecosystem 24/7. Once again economies of scale play a pivotal role in enabling the service provider to be in a better position in staying abreast or ahead of the hackers. Service providers may use information they have learned about threats faced by a set of their customers and apply protection against such threats to their entire base of customers.

Service providers also can leverage the concept of standards to their benefit in the area of cloud security. They are plugged into the security standards ecosystem and often guide the development and evolution of these standards. As such they are early adopters of these standards. Having been involved in this effort early lets them properly budget for these costs — a typical enterprise only hears about these developments much later and that may potentially delay adoption as their IT team needs to learn about the change and then figure out how to budget for any additional costs. **CP**

Sanjay Srinivasan is CTO for Telesphere, a provider of cloud communications services, where he oversees engineering and product development. Srinivasan has more than 15 years of experience and expertise in the areas of data networks, voice services and hosted application services. Prior to Telesphere, he served in various capacities with companies such as Hughes Network Systems, AT&T Wireless, Lightedge Solutions and Terabeam Corp. He has a doctorate degree in electrical engineering from the University of Virginia.

MOREINFO

ARTICLES

Countering Objections to Cloud Computing

7 Challenges to Building a Cloud Practice

SOURCE

Telesphere

Channel Partners

www.channelpartnersonline.com

About Channel Partners

For more than two decades, Channel Partners has been the leader in providing news and analysis to indirect sales channels serving the communications industry. It is the unrivaled resource for resellers, aggregators, agents, brokers, VARs, systems integrators, interconnects and dealers that provide network-based communications and computing services, associated CPE and applications as well as managed and professional services. Channel Partners is the official media of the Channel Partners Conference & Expo.

EDITORIAL

EDITOR-IN-CHIEF
Khali Henderson – khenderson@vpico.com, ext. 1678

SENIOR EDITOR
Kelly M. Teal – kteal@vpico.com, ext. 1020

MANAGING EDITOR
Buffy Naylor – bnaylor@vpico.com, ext. 1043

SENIOR ONLINE MANAGING EDITOR
Craig Galbraith – cgalbraith@vpico.com, ext. 1124

BUSINESS & REGULATORY EDITOR
Josh Long – jlong@vpico.com, ext. 1104

CONTRIBUTING EDITORS
Tim McElligott – tmcelligott@vpico.com, ext. 1254
Tara Seals – tseals@vpico.com, ext. 1005

CONTRIBUTORS

Jebb Dykstra
John Eldh
Jim Lippard
Sanjay Srinivasan

PRODUCTION

EXECUTIVE DIRECTOR, MEDIA OPERATIONS Danielle Dunlap
EXECUTIVE DIRECTOR, ART Dolly Ahles
ART DIRECTOR, COMMUNICATIONS Israel Laveaga
ADVERTISING PRODUCTION MANAGER Leez May

SALES/MARKETING

NETWORK LEADER
John Siefert – jsiefert@vpico.com, ext. 1233

STRATEGIC ACCOUNT DIRECTOR
Susan Kostbar • skostbar@vpico.com, ext. 1402

CHANNEL PARTNERS EVENT SALES DIRECTOR
Stacy Whitley • swhitley@vpico.com, ext. 1075

ACCOUNT EXECUTIVE
Andrew Masayestewa • amasayestewa@vpico.com, ext. 1061

MARKETING AND AUDIENCE CONTENT MANAGER
David Hurley • dhurley@vpico.com, ext. 1091

AUDIENCE AND CONTENT COORDINATOR
Lauren Kane • lkane@vpico.com, ext. 1113

REPRINTS & LIST RENTALS
Jennifer Thompson • jthompson@vpico.com, ext. 1170

Subscription Customer Service • 800-581-1811

VIRGO

CHIEF EXECUTIVE OFFICER John Siefert

EXECUTIVE VICE PRESIDENT/CFO Kelly Ridley

CONTROLLER Jennifer Janos

VICE PRESIDENT, HUMAN RESOURCES Heather Wood

PUBLISHED BY VIRGO PUBLISHING, LLC

3300 N Central Ave, Ste. 300 Phoenix, AZ 85012
Tel. 480-990-1101 • Fax 480-990-0819
Website: www.vpico.com

IN THIS ISSUE
Countering Customer Objections p. 34 ■ Table of Contents p. 2