

it

Channel Leadership/Trusted Advisor Series

security
CONSULTANT

October 2006

The Security Resource for Solution Providers

**Business
Continuity For
the Real World****Acceptable Risks
Acceptable Losses****TAC**
The
Advisory
Council

Beth Cohen is the Thought Leader for Hot Technologies at The Advisory Council (TAC) and President of LUTH Computer Specialists.

CONTRIBUTORS**Array Networks**
Michael Stewart**Cisco Systems**
Alex Thurber**Grisoft**
Larry Bridwell**Juniper**
Stephen Philip**RSA**
Michael Ross**SonicWALL**
John DiLillo**Trend Micro**
Nancy Reynolds**Westcon**
Laurie Usewicz**INSIDE:**

- Business Protection Basics
- Systems Backup and Restore
- Disaster Recovery
- Protecting Every Dimension
- Planning for the Unthinkable

**CMP**
United Business Media

Author's Spotlight



Beth Cohen, Thought Leader for Hot Technologies at The Advisory Council (TAC) and President of LUTH Computer Specialists, has more than 20 years experience in creating and supporting corporate IT infrastructure for different industries, including architecture, construction, engineering, software, telecommunications, networking and research. TAC 9 (www.TACadvisory.com) represents "The Next Generation of IT Advisory Services," utilizing thought leaders and experts in assisting IT to generate business value while ensuring success. As Director of Engineering IT at BBN, Cohen participated in the creation of the Internet. Specific expertise includes security, scalable robust IT architectures, operating systems, desktop support, process improvement, program management, IT/business alignment and integration of networks, applications and systems. Cohen has earned degrees from Rhode Island School of Design and Boston University and holds an MBA from Bentley College and a Graduate Certificate in Computer Science from Harvard University.

Email your inquiries and comments to Beth at editor@itsecurityconsultant.org

Effective Business Continuity: Disruption Not Disaster

Most companies are more concerned with weathering disaster and data loss than maintaining 100 percent uptime. But creating a viable data protection and business continuity plan presents an enormous challenge—and an enormous opportunity for solution providers with the skills and savvy to make survivability their stock in trade.

There has been so much talk in the press in the past few years about disaster recovery and business continuity that most companies have at least gotten the message they need to do something about it. Unfortunately, while there is plenty of fear-mongering from vendors and press alike, as most company executives and IT managers quickly discover, planning for uncertainty and risk management can be a complex and expensive proposition. All this means there are opportunities for knowledgeable solution providers to help clients cut through the conflicting messages and deliver appropriate data security technology and protection services.

For large companies with deep pockets or compelling reasons, like multinational financial institutions or telecommunications giants,

full hot-standby data centers and high-availability business continuity plans might be the right solution. The average solution provider's customer, however, is more interested in weathering disaster and data loss without going out of business than in maintaining 100 percent uptime through a Category 5 hurricane. With the help of a capable solution provider, some smart planning, and a deep understanding of real business requirements and risk tolerance, it's possible to put together an affordable business protection plan that will work for most businesses.

Everyone understands that major natural calamities like tsunamis, hurricanes and floods, as well as man-made devastation including radiation or chemical leaks, blackouts, wars and terrorist attacks are highly disruptive. Yet even a seemingly small problem

like a power outage can cause major business disruption if it takes out a critical server at the wrong time. It can be equally devastating if a trusted employee suddenly quits and takes the only copy of the client list to the competition.

We are living in an increasingly insecure world, with data security threats coming at businesses from all directions. According to MI5, the British security agency, every year nearly one in five businesses suffers a major disruption. Even if major disasters account for only 2 percent to 5 percent of all data loss, when they do strike, they can be devastating, both to seemingly immune multinational and to companies not directly in the data business. For example, the Loma Prieta earthquake in 1989, which wiped out downtown Santa Cruz, Calif., resulted in approximately \$6 billion in direct physical damage and \$10 billion in total economic losses. Ultimately, over 36 percent of the Santa Cruz business community was destroyed or suffered serious damage directly or indirectly from the event. Many businesses had not done enough business continuity and data protection planning and did not have the staying power to survive the physical and economic blow.

Last year one of my data protection clients, a large construction company, discovered the hard way that most computer systems are not designed to take direct lightning strikes. You might think that a construction company could function without its computer systems—after all you don't need a computer to hang drywall. But as company executives quickly discovered, they were unable to order

materials or bill customers. Because the executives had not been willing to procure the correct level of secure data protection for the company, the data recovery process took weeks instead of the days or hours it should have. In the end, they suffered economic losses in the hundreds of thousands of dollars. For my client, it was an expensive lesson in the fundamental differences between business continuity and disaster recovery.

No smart business executive would think of running a company without liability, fire and flood insurance. Given the number of highly publicized disasters in the past few years, solution providers and their customers should have a high degree of interest in data protection and business security. After all, planning for a major disruption is widely regarded as good business sense from a risk mitigation perspective. Think of it as simply a basic business continuity insurance policy.

Too many companies are afraid to create appropriate business continuity plans because secure disaster recovery and business continuity solutions are considered expensive and risky -- a difficult problem for companies to navigate themselves. For example, many professional services companies, such as legal, engineering and architectural firms, find that all of their intellectual property resides on computers and networks they don't understand well. When disaster strikes without proper secure disaster recovery and business continuity plans in place, these companies are at risk of going out of business simply because they are not technologically sophisticated enough to know what to do.

This precarious situation represents a huge opportunity for solution providers to create secure disaster recovery solutions for their client companies. Given the complexity of the problem and the limited access to important skills and resources, savvy solution providers can create a compelling set of consulting services for their customers. Knowledgeable solution providers can help enterprises secure their data and protect it from catastrophe by offering packages of integrated disaster recovery and business continuity planning services.

Business Protection Basics

To be able to offer these types of services credibly, solution providers must have a solid understanding of the important differences between data archiving, business continuity and disaster recovery. Before delving into the technical details of creating different types of solutions, it is essential to understand the basic terminology. It's equally essential to understand the conceptual differences between systems backup and recovery, archiving, disaster recovery and business continuity:

- **Data loss event (DLE):** Each system and data set can be associated with detrimental events that determine how a system will fail, the likelihood of that failure, and the type of loss. In the case of the front end of a Web-ordering system, failure might mean the loss of a few records. In the case of a back-end system failure, an entire database of customer records might be lost.
- **On a larger scale,** a solution provider needs to assess the likelihood that a business system will be affected by a disastrous event. If a company has

continued on p. 4



westcon
networking together®

Laurie Usewicz
VP and GM, Security Sales
www.securitypoint.westcon.com

Giving Resellers the Tools They Need to Succeed

At Westcon we're committed to helping resellers deliver prevention and mitigation solutions that correspond exactly to their customers' needs. Our goal is to be a trusted advisor and partner, enabling you to broaden or deepen your security offerings and supply your customer with the best-of-breed security solutions.

Because of the rapidly changing differences in how networks must be protected today, IT departments are struggling to stay ahead of corporate needs. With SecurityPoint, Westcon enables resellers to differentiate themselves from their competitors and truly protect their customers, moving them beyond simply defending the perimeter.

Westcon's technology experience and expertise allow us to customize vendor-agnostic end-to-end solutions that are easy to deploy, easy to manage, and easy on the budget. Westcon's SecurityPoint program brings to bear all the tools and resources our customers require to succeed in the security marketplace.

The best way to demonstrate Westcon's commitment to your success is with our six-step custom selling program, which combines online tools, processes, and product expertise:

Whether a Westcon reseller uses one step or all six, our goal is the same: Spend time with resellers and customers to tailor a solution that's on target.

continued from p. 3

located its data center in the basement of a building on the banks of the Mississippi, water damage risk is considerably higher than if the same data center is located outside the flood plain.

- **Recovery Point Objective (RPO):** This involves determining how much data loss is tolerable. The value of the RPO often changes depending on the desired scenario of data loss and recovery. Most companies would be more than happy to recover their data from a week ago in a major catastrophic event that affects thousands of other businesses, yet would not want to lose more than 15 minutes of information in the case of a localized systems failure.
- **Recovery Time Objective (RTO):** How fast does a given system need to recover from a data loss? For many companies, the exchange server must be configured to attain "five-nines" data and systems availability. That essentially means an RTO measured in seconds rather than days. The value of the RTO will often drive important decisions regarding systems architectures to meet requirements for high data availability and strong security.

It is important to clarify the distinction between data protection and security products that deliver disaster recovery and high-availability systems intended for data retention and archival purposes. The functions are related but have very different usage, hardware and software requirements. Each approach represents increasingly complex and sophisticated architectures to solve the same basic problem: how to secure and protect the enterprise from data loss.

Systems Backup and Restore

The first step for a solution provider in creating client-facing data protection services is to apply traditional systems backup methodologies to protect client businesses at the most basic level. Conceptually, systems backup processes create copies of client data on alternative media, so that the working system where the data normally resides is no longer a single point of failure.

Thus, if a company has extra copies of its data stored on tape or disk, it can be restored to another system if the main system fails. For many companies, this translates into securing data simply by backing it up to tape using common applications like Symantec or Legato. Today, the target media is typically some kind of removable optical or tape system, but various kinds of tapes, DVDs, CDs, floppies, USB flash and optical drives have all been used for backup over the past 20 years. Recently, with the falling prices and increasing reliability of disk drives, a popular option has been to save the data on virtual tape libraries, that is, disks or RAID arrays configured to look like a tape drive to the backup software. Some companies are offering hard disks in a tape cartridge package. Given the limitations of this approach for disaster recovery or business continuity, putting a hard drive into a tape cartridge is a misplaced use of new technology.

The advantage of using the backup-and-restore approach is that it is a technologically well understood and mature architecture used by companies for more than 30 years. There

continued on p. 6

**GRISOFT**
AVG Anti-Virus

Larry Bridwell
VP of Communications
www.grisoft.com

Sophisticated Protection Against Sophisticated Viruses

Virus threats have become both more subtle and more complex. The reason we no longer see regular bulletins about virus outbreaks is that predators don't want to announce themselves. They are more interested in using Trojan horses, password-stealers, and spyware, which can surreptitiously track and steal data.

That makes it much more difficult, time consuming, and costly to uncover and recover from these viruses. It also means that our customers and partners need to know they're working with a company that continuously invests in R&D and not only sales and marketing—a problem that plagues many technology firms experiencing rapid growth.

Grisoft is an engineering company with a serious commitment to customer support. The key is to target specific customers, like consumer, SMB and enterprise, and then give them the best possible product with the right amount of support.

Grisoft is recruiting new partners and resellers, and we offer competitive benefits. Grisoft's AVG Anti-Virus, Anti-Malware, and Internet Security Suite are low on system resources and easy to use. We provide 24/7 technical support via e-mail. Our reseller program is having great success due to our commitment to R&D and ongoing enhancements to customer and partner support.

continued from p. 4

are many time-tested and reliable backup applications to choose from, all of which will backup a system's data and catalogue the directories and files to allow for relatively simple file restoration. If a client company is looking for an inexpensive and mature technology to protect its basic systems data, and it is not overly concerned with recovery speed, high RPO values or reliability, then a backup tape system combined with an off-site storage rotation will deliver basic functionality. For added security, many backup software vendors are now including encryption overlays in their products.

On the other hand, the disadvantages of this approach are also legion. It has been estimated that over 60 percent of all attempted tape restores fail. If all the records are on a single type of backup medium and software, the task is somewhat simplified, but it is important to confirm that old tapes are still readable by the equipment. Many companies find that over time, their 8-mm and 4-mm DAT drives get out of alignment and are no longer able to read tapes created on other drives or in some cases, on the same drive after it has been repaired and realigned.

Another major problem with the traditional approach to backup is the amount of time to recover a system. Recoveries from tape media can take days. If a company has suffered a major loss event involving many systems, the recovery can quickly become overwhelming, even assuming the tapes were taken to a secure

off-site location. The CIO of a major Boston hospital system estimated that not having a hot backup site for its major systems meant that a major data center outage would result in a time to recovery measured in weeks. Even a single system failure would take more than a day just to retrieve the media and restore the files from the off-site tapes. This is an unacceptable situation for hospitals due to the critical roles they play in any disaster scenario.

Too many companies, both large and small, are still relying on these old-fashioned, slow, unreliable backup systems as the basis for their disaster recovery contingency plans. Smart solution providers can easily build profitable businesses offering better data protection systems and packages to client companies using more modern architectures and approaches that deliver higher security, availability, reliability and faster recovery times.

Archiving

Unlike backup and restoration, where the objective is to recover the entire system in its most recent stable state, the purpose of archiving is to protect data for historic, regulatory and audit purposes. While the files may or may not be important, they are generally not saved for recovery purposes. Archiving systems must have the ability to retain vast amounts of data in a searchable form. Often the time to recovery can be sacrificed in exchange for more sophisticated data-mining features. While Sarbanes-Oxley only requires the retention of financial

continued on p. 8



Michael Ross
VP Americas Channel
www.rsasecurity.com

Giving Back to the Channel

Losing data due to a security breach, especially one caused by a preventable spyware attack, can have a substantial negative impact on a company's reputation. Consider what would happen if your network was down for a day. Imagine if your closest competitor got hold of your customer database or your sales strategy. Could you afford these losses?

Further, it's no longer possible to sweep a spyware attack under the proverbial rug. Various disclosure laws require customers to be notified whenever a company experiences a data breach.

Data breaches can lead to dire financial consequences, such as negative association with a corporate brand. They also can reveal that a company is noncompliant with regulations and initiatives like HIPAA (Health Insurance Portability and Accountability).

Channel partners should look for security solutions that repel data attacks and document the failure of those attacks. Such information is especially important when the attack comes in the form of spyware. In addition, standalone products can usually offer significantly more focus than a products suites.

continued from p. 6

records, to simplify the archiving process companies are often archiving all records for seven years.

The key to maintaining good, secure archives is the ability to restrict record access based on roles and sophisticated search functionality. For example, if a company was faced with a sexual harassment suit, the search function should be able to find messages based on keywords. Yet for security and confidentiality purposes, it should only allow access to the records by the person's manager and the HR staff.

Another often overlooked problem is that tape management and backup software like Symantec and Legato tend to be oriented toward creating tapes designed to be used for system recovery rather than for archival purposes, so it is not uncommon for it to take extraordinary amounts of time to find small amounts of data or a few files. For example, if a company's tapes were all created and labeled by machine name, and the machines had a mix of engineering documents, financial records and random e-mail archives, the ability to retrieve a given piece of data could be seriously compromised. If the tapes are organized by project, year or some other more meaningful way, then retrieval time could be significantly reduced if the purpose of the backup was to retrieve individual files or directories rather than entire systems.

At the 50,000 foot level, data archives can be thought of as information that becomes increasingly less relevant over time. Current financial records are highly valuable and must be fully

protected, while 15-year-old records are mostly of historical interest, and unless there is a pending lawsuit, of little actual value to the on-going operations of a company. At the same time, as the content of the tape archives are aging out, the tapes themselves are slowly deteriorating, and the equipment to read the tapes is becoming less able to read them. Think about it -- even if your customers could retrieve their records from 18-year-old nine-track reel-to-reel tapes, unless the records were maintained in ASCII text format, they are unlikely to still have the application that could properly read and interpret the data. Over time, as the cost of retrieval rises, the value of the data drops. At some point, which will vary on the type of data and company policy, the cost of maintaining the archives will exceed the value. When that point is reached the tapes can be safely destroyed and discarded

For security and regulatory reasons, companies are often struggling with how to maintain long-term archives of encrypted yet valueless data on aging equipment readable only with obsolete applications. With increasing pressure from government agencies to maintain these records, this problem is only going to get worse over time. There are already arguments in the data storage community related to where these massive archives should reside. Arguments for maintaining them online to address searchability and compatibility issues raised by staying with tape formats are countered by the enormous costs of maintaining hundreds of terabytes of rarely accessed data. A knowledgeable

continued on p. 10



Alex Thurber
 Director of Security and Data
 Center for Worldwide Channels
www.cisco.com

Self-Defense: The Only Protection Against Security Threats

Security continues to be a top of mind concern at companies of all sizes. Threats are more sophisticated. Network topologies are more complex, which makes them harder to defend. There's so much connectivity and so many laptops that the traditional network perimeter has disappeared. IT can no longer expect to have physical control of its assets.

What's needed is a comprehensive solution, one that deals equally effectively with physical issues, porous perimeters, and access control. It must be able to identify and neutralize threats on its own; by the time human operators respond, it's too late. It must be collaborative, which rules out a collection of point products. And it must implement security everywhere: off-site locations, the network, and all connected devices.

Cisco's Self Defending Network is the only solution that can meet those requirements. That's because we began as a networking company and have always known that security must be integrated seamlessly into the network.

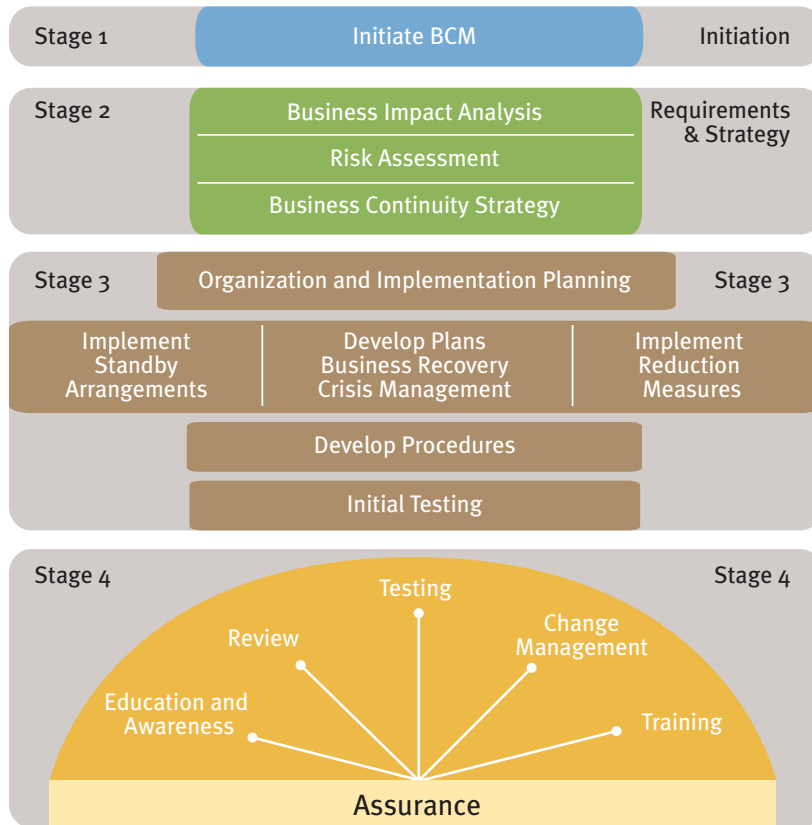
We offer our channel partners two distinct advantages: the most advanced technology available and an award-winning partner program that has been singled out by *CRN*, *VARBusiness*, and others.

There is something else we offer our channel partners: a name and reputation that can open virtually any door.

Sponsored by **INGRAM MICRO**

continued from p. 8

Four Stages to Survivability



Crafting a full-fledged business continuity plan can be a daunting affair. Breaking the plan down into logical steps takes much of the effort out of evolution.

Source: <http://www.insight.co.uk/bcm/>

solution provider can help companies choose the appropriate approach based on the specific requirements of a given situation.

Of course, the problem of retrieving data from old media represents a real opportunity for highly specialized solution providers that are willing to

maintain old equipment and legacy applications. These companies can offer data recovery services for desperate companies -- for a price. The state of New Jersey hired a solution provider to recover, at great expense, the school records of thousands of students after a major crash brought down a key mainframe server. The

continued on p. 12

**SONICWALL**

John DiLillo
Vice President
of Worldwide Sales
www.sonicWALL.com

A Full-Spectrum Approach to Security and Partners

SonicWALL understands that anyone connected to the Internet, whether as an individual or as part of a company, is under constant attack. Treating security as a one-time solution, as many vendors do, can't safeguard against threats that change every minute. Through its unified threat management solutions, SonicWALL delivers ongoing updates to over 500,000 systems worldwide, ensuring that our customers are always protected, even from zero-day events.

SonicWALL offers a broad spectrum of solutions for small and mid-sized organizations that includes comprehensive network security, secure content management, email security, and continuous data protection. Our dynamically updated solutions are designed to be easy to manage and cost-effective for companies of all sizes.

Nearly all our hardware products also serve as platforms for renewable software and services subscriptions, which gives our partners profitable recurring revenue opportunities. That's one reason our partner program has gained a high reputation within the channel community. More importantly, we treat our partners as our customers, not as an extension of our sales force. We sell exclusively through the channel, and we won't introduce products unless we're convinced our partners can make a profit with them. The channel is our sales force. We do everything we can to help partners build their business, offering development, collateral, and other marketing support. What's more, we constantly reevaluating our program to make sure it's up to date.

continued from p. 10

data recovery solution provider had specialized equipment that could read the data directly from the disks, bit by bit. While that scenario might seem extreme, the alternative—trying to rebuild the records from paper archives—was even more costly and time consuming.

Disaster Recovery

When there is a major calamity, after the staff has been accounted for, the next step for most companies is to immediately implement their disaster recovery plans. If they are well organized, they will be able to recover by using a combination of technologies and processes and quickly get back to some semblance of normal business. Too many companies find that what they thought was a thorough recovery plan fails when it counts. A well-prepared solution provider can help its clients avoid such painful and expensive scenarios by offering thorough and feasible disaster recovery plans and services.

As an example of the opportunities available to solution providers, Sungard has built a profitable business unit around the idea of creating cold, warm and hot failover sites for their global enterprise customers. For Sungard's clients, the costs of such services are more than offset by the risks of data loss in the face of calamity. Several major Wall Street financial institutions successfully used Sungard's services after the September 11 terrorist attacks.

Most disaster recovery systems are designed to replicate an entire system

so it can be rebuilt as quickly as possible with minimum data loss. A high availability system adds the valuable feature of allowing automatic and/or instantaneous failover to a fully functional and secured standby replica of the system. Key features include the ability to roll the system back to a known stable state and automated failover mechanisms. Some companies with an extremely low tolerance for system failure and extremely large budgets use a combination of clustering, redundant systems and fully replicated remote hot sites to meet their five-nines availability requirements.

Business Continuity

What is often overlooked is that disaster recovery and business continuity have essentially opposite objectives. While the purpose of a successful disaster recovery plan is to rebuild business infrastructure after a loss as quickly as possible, a good business continuity plan is designed to keep a company functional through a major internal or external disruption. Business continuity extends far beyond technological solutions into human resources, supply-chain and customer issues. After all, if your client's staff is unable to access systems, and suppliers cannot deliver goods, it doesn't matter how many nines their data center can guarantee -- the business is still not functional.

Since business continuity planning is much harder and vastly more expensive to implement and difficult to understand, many companies tend to develop strategies for disaster recovery, without realizing potential

continued on p. 14



Nancy Reynolds
 VP North American Channel
 Sales & Marketing
 www.trendmicro.com

**Making Reseller Success
 A Strategic Initiative**

“Who’s got your back?”

That’s a good rule of thumb for channel resellers evaluating potential partners. Think of it this way: You need a trusted partner that’s as committed to your success as you are to your customers’.

Resellers need to be aware of three key considerations when selecting a technology partner. The vendor must have the requisite resources to support you fully. It must be committed to building its business through a network of alliances. And it must be able to demonstrate long-term profitability.

Trend Micro offers its resellers solid, innovative technology and a rich array of resources that makes it easy to succeed. Our inside sales reps provide presales support whenever it’s needed. Our field salesforce is there to generate leads for our resellers.

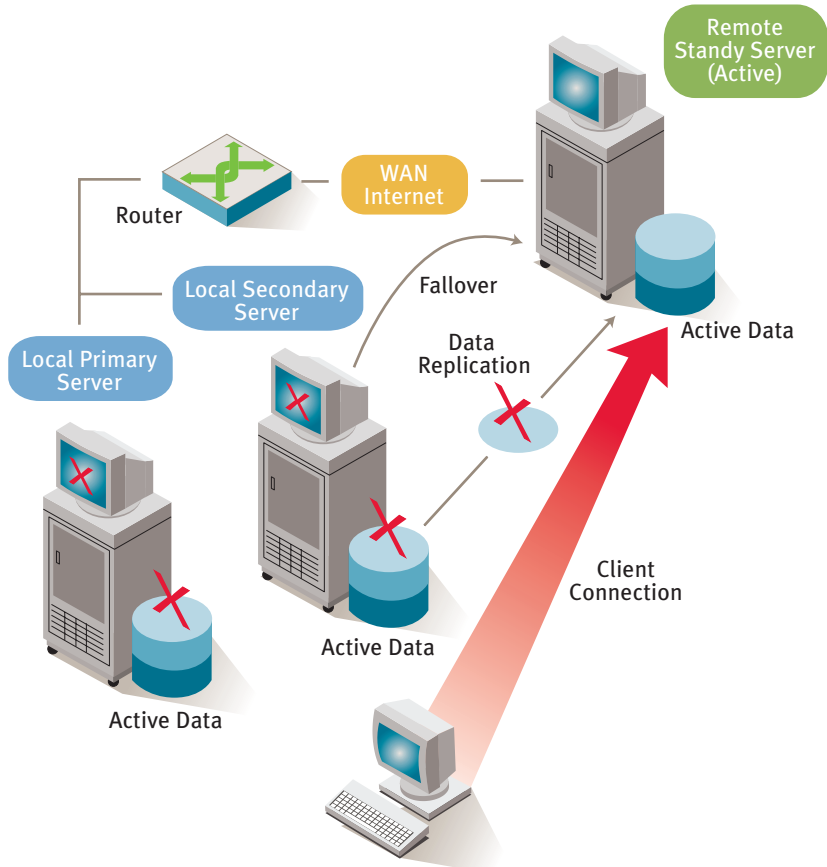
Further, since Trend Micro’s sales are 100 percent channel, our resellers know we’re working with them 100 percent of the time. They never have worry that someone wants to steal their customers.

The quality and breadth of Trend Micro’s alliances indicate the widespread acceptance of its solutions. Cisco Systems, for instance, OEMs our products as part of its Self-Defending Network.

Finally, resellers need to consider a partner’s profitability. Trend Micro is a global leader in security with two decades of success to build on. We’ve got you covered.

continued from p. 12

Mirroring for Site Fallover



Deploying a local standby server ensures business continuity if a primary server goes dark. Extending this model across the wide area by adding a remote standby server ensures business continuity and data recovery even if an entire site goes down.

Source: http://www.openminds.co.uk/data_mirroring/

problems until disaster actually strikes. As a solution provider, there are many opportunities to help your customers identify their most vulnerable systems and offer comprehensive solutions that will allow them to stay in business without breaking the bank.

Preventing Data Loss

The good news for solution providers is that the technology for deploying comprehensive business protection is available now. The bad news: It’s in bits and pieces. By using a combination of newer technologies and integrating mature architectures

continued on p. 16



Michael Stewart
VP Sales

www.arraynetworks.net

Uncompromising Business Continuity—At a Price That Can't Be Beat

At Array Networks, we define business continuity as secure anytime, anywhere access to mission-critical applications and resources—without interruption. The Array SSL VPN access gateway delivers exactly that, thanks to instant capacity, virtually limitless scalability, and unparalleled performance.

Whatever keeps your client's workforce from getting to the office—from transit strike to Category 5 hurricane—the Array SSL VPN enables all of them to work remotely, without any risk of overwhelming the system or seeing performance degrade. We can support up to 64,000 simultaneous users on a single system, at 10 times the speed and scalability of our closest competitor.

Our commitment to the channel is equally uncompromising. We're transitioning to a channel-centric model. We're turning over established customers, including the largest, to our channel partners. And we deliver support and training through the channel, maximizing the opportunity for recurring business.

Since the Array solution is priced 10 to 15 percent lower than the competition, you enjoy higher profit margins. And we've decided to go with a single distributor: Ingram. That eliminates competition within the channel. That frees our partners to focus on only one thing: their customers. Given our unrivaled price/performance advantage, we believe our solutions can almost sell themselves.

Sponsored by **INGRAM**
MICRO®

continued from p. 14

in new ways, a solution provider can deliver customized and affordable integrated solutions that will add real value to their customers' bottom line, and more importantly, their peace of mind. The trick is integrating the pieces into a seamless solution.

With the cost of storage-area networks (SANs) dropping, and new approaches to WAN replication making it feasible to stuff more data through an Internet connection, it is now possible to secure data more effectively. This means that replication of mission-critical data and systems to a distant data center is both feasible and reasonably affordable.

Protecting Every Dimension

The best way to secure data for any purpose is to keep multiple copies on different media at different locations. Copying important data to distant locations or remote servers over the Internet or private WAN connections is not fundamentally difficult or conceptually sophisticated. After all, sending backup tapes to a secure off-site facility is a time-honored, though slow, method of protecting mission-critical information.

Another way to look at it is if a client keeps copies of its important data at headquarters, a remote location and your secured data center, then they have mitigated their risk of catastrophic data loss. The likelihood that all locations will be affected by even a major disaster is low. If the situation is so dire that all the locations are equally affected, then data loss would be the last thing on your

client's or anybody else's mind.

Breakthroughs in disk technology and falling hardware costs, combined with new compression and caching algorithms to optimize data traffic over a WAN connection, are allowing vendors to create products that finally meet the need for faster, automated, more reliable methods of maintaining replicated data stores in remote locations.

There are four basic types of WAN optimization: network, hardware, file system, and application. Depending on the type of data, amount of redundancy and other complex factors, companies are reporting as much as 80 percent reduction in WAN bandwidth utilization. This has opened up undreamed of possibilities for server and data center consolidation and real-time remote failover for truly high-availability applications. From a management perspective, end-users are already accustomed to accessing Web content from anywhere in the world. As long as the information they require is available in a timely fashion, they don't really need to know or care where the data actually resides.

Since WAN optimization, replication and server consolidation technologies are relatively sophisticated, the best way for companies to ensure a successful WAN consolidation or replication project will produce satisfactory results is to hire a vendor-neutral solution provider with expertise in this area to help with the planning and vendor selection process.

continued on p. 18

continued from p. 16

Planning for the Unthinkable

Once a solution provider understands the different data protection architectures and has mastered the available technologies, the final step is to create a planning methodology to help clients create viable disaster recovery/business continuity plans. While there is no standard best practices methodology, years of disaster preparedness manuals from government agencies and non-government organizations like the Red Cross provide a variety of checklists and planning documentation to help get started with a methodology that targets a specific vertical market.

A well-versed solution provider can help clients identify mission-critical systems and invest resources into protecting those first. A provider needs to determine its clients' tolerance for downtime and data loss, then build the technological solution to meet those requirements.

Make sure the business protection plan includes processes that address staff availability and contingency planning. Even more important and often overlooked is that ongoing disaster training and systems testing must be part of the protection planning process. Any disaster readiness plan will fail if the planning process is treated as shelfware—completed once and forgotten.

Best Practices

- **Determine** your client's business goals and objectives then recommend matching data security and protection solutions.

- **Audit** existing systems before adding additional protection services.
- **Build** the business case for business protection by identifying mission-critical systems in terms of lost financial opportunities.
- **Create** a business prioritization matrix based on the business importance of a given system and the relative difficulty of protecting it.
- **Break** the business protection planning process into pieces to make the project more manageable.

Drilling down into more detail, the first step in the creation of any business protection plan is to inventory and prioritize existing systems. You will need to apply two sets of criteria for each system being evaluated: 1) How important is the system to the business, and 2) How much downtime and data loss are acceptable? Downtime and data loss are often confused, but they are not the same. For example, losing a few random e-mails is probably not as critical as having the system unavailable for some period of time.

The relative costs to address RTO and RPO are quite variable. These are where you can realize the most cost savings by being smart about which systems get the most resources. Instant failover will generally mean investing in a complete load-balanced or standby system in a remote location that is capable of taking on the full system functionality. That means purchasing high-availability network connections and switches. Another

continued on p. 18



continued from p. 18

critical consideration is the probability that a given disaster will occur. For example, the likelihood that the San Francisco Bay Area will become a war zone is lower than the probability that it will have a major earthquake. Both of these possibilities are less likely to occur than a data center generator being hit by a lightning strike or a client's headquarters will suffer an extended power outage.

Summary

- **Know** the critical technical distinctions between data security for business continuity, disaster recovery, and data archiving
- **Recognize** that while technology is certainly part of a data security solution, business protection is not primarily a technology problem
- **Understand** that your client company's successful business protection plan takes into consideration cost, risk mitigation, and technology tradeoffs
- **Think** in terms of delivering integrated business protection solutions, rather than offering your customers a choice of either disaster recovery or business continuity services

The issues of data protection, business continuity, and security are complex and specific to each client company's requirements. The real value a solution provider brings to its clients is the ability to create customized packages that are highly responsive to an individual company's needs. While it is not possible to guarantee 100 percent that a solution provider can build a service that will never lose client data or prevent a major catastrophe, it is

possible to protect a company from disasters using an integrated mix of sophisticated data protection technologies and processes. In the end, it's a win-win situation both for solution providers and for their customers. By having expertise with business requirements and technology, the solution provider is well positioned to offer valuable advice to its customers on how to best apply technology to solve data protection and business continuity needs. ■



Vice President: Joseph Braue
Publisher: Pamala McGlinchey
Sr. Director Project Mgmt: Karen White
Senior Editor: Kate Gerwig
Project Manager: Michelle Somers
Editorial: The Forsite Group
Design: CMP Channel Group Design

For more information jbraue@cmp.com or (212) 600-3114

©2006 CMP Integrated Marketing Solutions. All rights reserved



Stephen Philip
Senior Director, Product Marketing,
Security Products Group
www.juniper.net

Ensuring Business Continuity with Remote Access "In Case of Emergency"

A truly responsive solution provider helps its customers maintain business continuity during any sort of disaster, including a pandemic like the Avian flu. A medical emergency of this sort can force your customers to limit personal interactions among employees, partners, and customers. It also drives the need for ad-hoc remote access, while personnel are quarantined, possibly for extended periods of time.

Juniper Networks Secure Access SSL VPN appliances enable employees to work anytime, anywhere from any device, including unmanaged PCs, mobile phones and PDAs. Customer control at the user, application, and network level, along with a clear view of the security status of end-devices, safeguards resources. And deployment is a snap: Employees only need an Internet connection; there's no need to distribute or deploy software.

If disruptions are widespread, Juniper Networks Secure Access ICE (In Case of Emergency) cost-effectively scales our VPN, so the bulk of your customer's employees can work remotely. ICE maintains productivity and gives IT organizations the peace of mind available only with Juniper's best-in-class security capabilities.

Working with Juniper Networks offers our J-partners unparalleled advantages. Secure Access SSL VPN has led the global market since its first release. It currently services Fortune 100 companies and thousands of enterprises worldwide and is the only SSL VPN to be Common-Criteria certified by the National Information Assurance Partnership.

<http://www.juniper.net/products/ssl/>

Sponsored by **INGRAM MICRO**