

OUTSOURCING AND OFFSHORING: THE BENEFITS AND RISKS

From Tough Times Rise New Opportunities

Challenge

For outsourcing to work, a certain amount of control must be given to the contracted outsourcer. By granting the level of access, network, application security, and data privacy become a major concern that the contracting company must meaningfully address

Solution

Juniper Networks has recognized the security risks faced by those organizations that have taken advantage outsourcing and have architected a solution to comprehensively address the damaging security holes that expose organizations to unacceptable risk.

Benefits

Juniper's security solutions provide outsourcing organizations with peace of mind to:

- Grant the right level of access to each individual
- Support for all devices whether they are company or third party devices
- Provide instantaneous identification and appropriate mitigation of the most complex attacks
- Ensure a sitewide view with real-time and historical reporting for security or compliances purposes

Now more than ever, the business environment in which we operate tests even the strongest organizations. A confluence of challenges—including tight economic conditions, increased competition, and rising business costs—combine to act as a catalyst for organizations to look for and implement new and innovative ways to gain a “competitive edge” in order to survive.

One method that has received increased attention—and adoption—is outsourcing, which is also commonly referred to as business process outsourcing (BPO). Several of the most common models of BPO include:

- **Offshoring** – Traditional outsourcing in which a company is contracted far outside of the country of the original outsourcing company
- **Nearshoring** – Offshoring in which a company is contracted outside of the originating company's country—in a country that is close to the outsourcing company's country of business

Another form of offshoring is when a company or organization—rather than contracting with a third-party, offshore organization— hires staff in an offshore country to work directly for it. This has been referred to as subshoring. It provides the company with a greater amount of control and employee ownership than usually found in a typical outsourced or offshore relationship.

There are a number of regions and specific countries around the globe that have a vibrant, growing outsource business. Among countries that have a strong outsource or offshore business market, India maintains a commanding lead with an estimated \$30 billion in estimated revenues expected from offshoring in 2008¹. Other locales—such as China, Eastern Europe, the Philippines, Morocco, Egypt, and South Africa—have also become prime destinations for outsourcing and offshoring.

Outsourcing operations are also generally conducted through one of the following three business models²:

- Transactional BPO handles one aspect of a business process only.
- Niche BPO carries out three or four aspects of a business process.
- Comprehensive BPO handles both transactional and administrative tasks in a business process and takes 70 percent responsibility of the output.

¹ Nasscom BPO Newline, The Indian BPO Sector Dealing with the Challenges, January, 2008

² www.tutorial-reports.com/business/outsourcing/bpo/models.php?PHPSESSID=4abf87ff79522c29129ecb5f704568a1

The Emerging Joys of Outsourcing

In order to drive additional revenue and improve margins within today's ever-changing mobile network business climate, mobile service providers (MSPs) must be able to provide value-added services to their customers. To meet the accompanying network requirements, operators must cost-effectively transition to and implement each critical feature of the next-generation, high-performance IP/MPLS mobile network—including the mobile backbone; mobile backhaul; security; Authentication, Authorization and Accounting (AAA); Fixed Mobile Convergence (FMC); and session border controller (SBC).

Forrester Research notes that in 2006, U.S. companies outsourced over 130,000 jobs, moving many of these jobs offshore. Projections indicate that this number will increase to more than 3.5 million U.S. jobs moving offshore by 2015³. But, this should come as no surprise. Outsourcing and offshoring enable an organization to subcontract a portion of its business processes to a contracted company that can perform the desired functions better, faster, and usually at a fraction of the cost. The benefits of outsourcing and offshoring business processes for the originating company include transferring some of the risk associated with the processes to the contracted company, while simultaneously realizing a substantial cost savings. Additionally, the originating, outsourcing company can enjoy increased flexibility by investing less in certain areas of its business, which may not be its strongest—outsourcing these processes can eliminate distractions and enable the originating company to focus on its core business. BPO also allows the originating, outsourcing company to be more agile when market conditions demand organizational changes, such as reductions in force (RIFs).

The Downsides of Outsourcing

To realize the full benefits of outsourcing and offshoring, it is essential for the originating organization and contracted offshore company to operate in an environment where both realize mutual benefits. And while many outsource partnerships are successful, many originating, outsourcing companies—as well as the companies to which they outsource their business processes—can expose their business to substantial risk.

In order for an outsource or offshore partnership to work seamlessly, a certain amount of control must be given to the contracted outsourcer or offshore company. From a network perspective, these remote outsource partner locations can be established, and access privileges may be granted to restricted applications and data located on the originating company's network. With this level of access, network and application security and data privacy becomes a major concern. There is hardly a day that passes where we do not learn of a new, colossal security breach driven by outsourcing, off or nearshoring, or

subshoring that affects a major global organization. This is not because security for outsourcing is lacking, but it is because the nature of the threat has changed.

Security was originally architected with the belief that the threat was always looking in from the outside. That is, threats historically were found outside of the network, and were trying to get into the network. With outsourcing, we have permitted outsourced partners and subcontractors—most armed with third-party, unmanaged devices—to access our networks, applications, and data, effectively bypassing our network perimeter security. These contracted outsource partners and subcontractors are now, in effect, permitted onto networks similar to a trusted user with a managed device.

In the case of organizations that hire and furnish offshore sites with their own staff, these new employees are truly trusted users with managed devices. However, most of the same issues and problems faced by originating companies when working with third-party, contracted offshore partners are not alleviated and can sometimes be exacerbated when dealing and working with these new offshore employees.

Outsourcing can produce a myriad of different security risks, but they boil down to two major types of threats:

1. The “good” outsource partner accidentally puts an outsourcing company—or even its own company, whether it is the outsource partner or an offshore extension of the originating company—at risk by unknowingly doing something wrong. The “something wrong” can be accessing the originating company's network with an infected device, sending data to the wrong location, or even misplacing a PC or some other form of digital media.
2. The “bad” outsource partner intentionally puts an outsourcing organization—or its own company, whether that is the outsource partner or the originating company in the case of an offshore division or staff—at risk by exposing, stealing, and/or reselling confidential assets. The motivation can be for a variety of reasons including mischief, retribution, extortion, or even for profit.

OUTSOURCING HALL OF SHAME

Large, multinational oil and gas exploration company: An offshore vendor stole the social security numbers of employees and used them to file for unemployment benefits.

Major U.S.-based metropolitan hospital: The records of nearly 50 patients were posted to a publicly available Web page as a result of an outsourcing error.

Major worldwide financial institution: It lost hundreds of thousands in customer funds, which were stolen by an offshore outsourcing vendor.

³ <http://www.msnbc.msn.com/id/12745020>

Major payroll and benefits services company: With the scope of this breach still unclear, the personal information of state employees may have been compromised based on a security breach of payroll and benefits systems that were improperly subcontracted to an off-shore company.

Regardless of intent or relationship, the danger to an originating, outsourcing company remains the same: Their network perimeter has become porous, and given the type of network security deployed, it becomes nearly impossible to defend against malware, trojans, keyloggers, spyware, and worms when outsource partner devices have been allowed to bypass all of the company's existing perimeter network security. It is impossible to defend a perimeter when you cannot delineate exactly where the perimeter is.

The Juniper Solution: Addressing the Outsourcing Threat

Juniper Networks® has recognized the security risks faced by those organizations that have taken advantage of the benefits outsourcing and offshoring have to offer. We have architected an answer to help those organizations plug the highly volatile and potentially most damaging security holes created or exacerbated by outsourcing and offshoring, which can expose their organization to unacceptable risk.

Several key tenets are employed to architect Juniper's solution, including:

- There must be access to the right information and applications, given to the "right" people, whether they are local or remote. The heterogeneous audience that comes as part of an outsourcing contract demands that granular access control ensures only authorized personnel are allowed access to only the resources they require to be productive, and nothing more. Locking down everything else helps limit network, application, and data exposure—and ensures that confidential data and key intellectual property (IP) remain secure.
- Employees or BPO personnel will sometimes commit a breach with the data to which they rightfully have access. It is essential to log who is accessing what, and when. Moreover, reporting information must be complete, easily accessible, and simple to understand. This provides the virtual paper trail necessary to quickly react to any potential breach both from a security and compliance perspective.
- Employees of outsource or offshore partners may access data and applications on your network with third-party and unmanaged devices. Some of the biggest insider breaches are a result of an infected endpoint contaminating a network. Ensuring that a device is clean before it comes on

your network can help ensure your network stays clean. This is done by making sure that endpoint devices—particularly those of outsource or offshore partners—are clear of infection from viruses, keyloggers, trojans, worms, and other malware before they gain access to your network. If a device—dependent of whether it is a corporate device, or a third-party or unmanaged device—is found to be infected, it is important to limit its access (that is, quarantine the infected device) until it can be "cured" (that is, remediation is complete). To guarantee minimal disruption, automatic remediation—where the infection or inability to meet corporate security or access policy is addressed automatically, without human intervention—is best to ensure that a device used by an outsource or offshore partner is clean and meets your security and access policies. However, self-remediation may also be indicated, where employees of your company or outsourced employees are able to take actions on their own to cleanse their infected devices, and attain or regain network access as quickly as possible.

- Compartmentalization via network segmentation enhances security by ensuring that once on the network, employees and outsourced personnel are not given free reign of the applications and data on the network. Encryption further secures data in transit to ensure that it cannot be compromised or hijacked while in transit either to local or remote locations, as well as inside the network itself.
- Visibility and control must be complete. It is impossible to find or report on security without a single and comprehensive view of the network, both from a real-time and historical perspective. Aside from saving on OPEX costs, it is the only way of getting an accurate picture on the security posture of the organization.
- "Rearview mirror" security is a thing of the past. It is no longer acceptable to wait weeks to months in order to ascertain that a breach has occurred. Detection, mitigation, and reporting on potential breaches must occur in real time. This means that the various deployed security elements must work together and collaborate to root out attacks that are stealthy, sophisticated, and built to evade traditional security point products. It also means automating the tedious process of log correlation, which is still largely done on an ad hoc or manual basis.
- Violations do not always require a complete shutdown. Blocking traffic every time a suspicious incident occurs simply does not address the requirements of today's high-performance business and can result in business grinding to a halt. Rather, it is essential to take the "appropriate response" based on the violation that has occurred. This may include actions such as rate limiting, reporting, quarantine, or update.

Summary – Securing the Benefits of Outsourcing

The good news is that Juniper Networks has done the heavy lifting for you when it comes to securing your business—particularly your network, critical applications, and sensitive data—against the risks and threats that are presented by any outsourcing or offshoring situation.

Led by Juniper Networks Adaptive Threat Management Solutions—which work across heterogeneous network environments by delivering adaptability, scalability, visibility, and investment protection to provide comprehensive network and application access control and security—Juniper offers a complete solution to address and mitigate the risks and treat the most common threats prevalent in an outsourcing or offshoring arrangement. Integrating and interoperating with Juniper’s complete portfolio of award-winning access control and security products, Adaptive Threat Management Solutions are the foundation through which organizations can enjoy the fruits of BPO while successfully defending their network and business from the outsource and offshore threats that can directly and most severely impact their business.

Next Steps

For more information about Juniper Networks products and services, please visit www.juniper.net.

For additional information about Adaptive Threat Management Solutions, please visit: www.juniper.net/adapt

To purchase Juniper Networks solutions, please contact your Juniper Networks sales representative at 1-866-298-6428 or authorized reseller.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Corporate And Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King’s Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airsides Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
Fax: 35.31.8903.601

Copyright 2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. “Engineered for the network ahead” and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.