The Need for Security Integration with Outsourced IT services
(The loss of communication synergy caused by outsourcing)

Dated: 1/27/2004
Author: Kent E. Chadrick
Version: GSEC Practical Assignment v1.4b Option 1
****

Introduction:

You've seen that IBM commercial where the fat man is in the psychologist office. He states he has a dream where he is the most famous magician. He accomplishes dissecting his best customer but he has a dilemma – he can't put the customer back together again. The psychologist answer – "you have an integration problem". That is exactly what my company is suffering with and from the numerous magazine articles that I have read many companies suffer the same. Security Integration is a problem for many companies that have outsourced major areas of their Information Technology (IT) services. Unfortunately, security posture is one of the first significant areas that suffer from integration issues. Over 55 billion US dollars were lost in 2003 from virus attacks.[1] Since 2001 over 90 billion US dollars have been lost with monetary damages increasing per year. We are gaining increased security awareness but not necessarily improved security posture. "Security has emerged as one of the most important issues of 2003. Looking to next year, it will again be a priority for all CIOs. With that in mind, in the last 12 months, what has emerged as the overwhelming failing of the security industry?"[2] What emerged from this question is the critical need of governing our processes and organization by integrating security risk assessment – our security posture, with our everyday business pulse. The business process drives the required integration; the integration drives the types of security placeholders - security posture validates and ensures protection of the business process.

No longer can security take a back seat to our business processes. Further security must be integrated into the very fabric of our common processes. Outsourcing security IT services will require an even greater commitment on management and their employees to properly and effectively communicate security issues and concerns. The lack of comfortable security posture is captured in a Business Wire survey where 52% of CSOs and senior security executives were only somewhat confident that their security activities are effective. Further, 45% felt their companies were playing catch up and 15% were falling behind.[3] Security is here to stay requiring daily actions and constant risk mitigation. Security posture is a business process and the better we accomplish it the more communications synergy we will achieve. Our last hurdle will be to integrate security with outsourced identities to obtain communications synergy. An analysis at what security integration and posture provides and how those concepts apply to typical IT areas in the outsourcing process is required. This analysis will require managers to change their cultural and organizational concepts.

Integration Complexity

Integration is one of the highest levels of IT skills to achieve. Second to none are security skills. IT service providers who know they truly have these skills are looking for companies that will respect and hence pay for that knowledge. Knowledge is truly powerful and outsourcing for that knowledge will be costly. If your company is like mine – where your operational processes change constantly, your need for dependable, reliable and stable integration is paramount. Having a proper security posture engrained with the integration is critical. Integration ensures databases communicate across platforms and operating systems. Integration focuses on the key processes in data exchange and manipulation. Integration articulates what values are critical and secure before the next system process executes. Why do many companies assume the outsourced vendor will properly weigh and value these integration points? It is your business process that should dictate the type and complexity of your IT system. It should be your company that thoroughly understands these integration points since these points define your most critical process areas. Was it not our business processes that drove the IT world to where it is now? Was it not our need to exchange data accurately, securely and timely that provides IT the means to continuously revolutionize our processes?

You can't outsource the very reason you exist as a company nor can you concerning the service you provide. It would be obvious business suicide. So you must ensure that you continually invest in people who are willing to make the integration points and security posture their mission. This mission is the unsung and neglected foundation for your company's survival and success. Unfortunately, most companies will not pay the price for those quality outsource services nor will they keep people in-house for the integration mission, as a result you have the piecemeal or devalued IT solution. Both can be a disaster for your companies IT security posture. Even non-IT companies can have catastrophic results when security integration is not aggressively pursued. "The Blackout of 2003, during which an estimated 50 million people lost power, showed that the North American power grid is susceptible to failure. Energy companies face increasing pressure to dramatically improve the security and reliability of the utility infrastructure to ensure economic stability."[4]

After initially outsourcing most companies will naturally lose their in-house expertise. In addition, many IT outsourcing contracts do not provide the level of security detail you need to make IT assessments. Many companies inherently put themselves in a position where they can no longer effectively assess their security posture. These realities are where communication synergy can be lost. Synergy is where the total is greater than the sum of its parts. Synergy is where we obtain our best value.

Security Posture

Opps! We didn't get that antivirus loaded like we wanted. Why hasn't my antivirus signature been updated? I don't understand – how did they gain access to our infrastructure by TELNET? Why is our Web servers continuously being probe and attacked? Has your company experienced any of these trials? These types of problems will cause significant operational disruption. Consequently, it is imperative to minimize these failures. As companies outsource their IT requirements, security risk and assessment must be included in the process and ensured a daily operational reporting and accounting. Studies have concluded that in order for outsource providers to stay competitive they will become more vertical experts combining both business and technology skills.[5]

Vertical alignment would mean understanding a process from beginning to end to include the security posture of that process. The aspect of vertical alignment is a major culture and organizational change. In the classic sense outsourcing meant allowing vendors to provide services independent of the companies services. For example, having an independent trucking company that ships your product. Vertical alignment would place emphasis on a complete process. The antivirus process for instance, would involve the company's user desktop to the processes in which updates where acquired and disseminated. The administration of user desktop computers may still be a function of the company, but the antivirus service would be outsourced. Vertical alignment would ensure that the user desktop is getting signature updates. If not, they would report discrepancies and possibly deny network access until compliance thus ensuring the integrity of the network as a whole. In the past the vendor would provide the signature update but not have the processes in place nor the authority to enforce compliance. Similarly, the company now has their own metric to track, which is the timely and accurate dissemination of signature updates.

Vendors who do not provide this type of integrated security with accountability will be hard pressed to continue business. Vendors need to improve on integration and security as a required service foundation. It is of little service to be a web provider when your company cannot ensure effective customer business integration in a secure manner. Vendors must become vertical process providers. Synergy can be obtained by the application of vertical alignment and expertise and the necessary culture and organizational changes required to support this application. There are common IT areas that companies usually gravitate to outsourcing: Network perimeter security, network design and operating systems and vulnerability assessment to include threat management. A look unto these IT areas can give us a better understanding of the need for security integration and the improved communications synergy available.

Outsourced Boundary Protection

Centralized management, network perimeter security, server consolidation and resource alignment are common terms heard within company walls for outsourcing. Although network perimeter security – boundary protection (BP) has been subject to outsourcing, the concept of including BP as a portion of a greater security process is fairly new. The industry is now using terms like Managed Security Services (MSS) but the process is the same integrated security:

> "Here, a corporation may choose to design and deploy security through a security or networking team. Historically, the security team has inserted dedicated security devices, such as firewalls, into the network infrastructure, while the networking team has activated security capabilities on existing networking devices, such as access control lists on routers. Since each group has a different set of priorities, coordinated security may be lost. A more effective and efficient approach, and one that an executive can use to make an immediate difference, is to create a team which combines both networking and security responsibility and skills, tasked with deploying both dedicated and integrated security systems. This maximizes the probability of a consistent security design, policy and implementation".[6]

Boundary Protection Example

My company decided to centralize our BP services. Although still technically within the company the new central BP is outsourced. Each major site can no longer manipulate nor access our firewalls and proxy servers. Thrown in for good measure is the Service Delivery Point (SDP) routers. So basically we control no external IT system. Even going into this new process we knew the outsource vendor did not have the same level of technical expertise we currently possessed. This change follows what other major companies are experiencing. Further still, we discovered that there are two outsourced groups managing the BP. Some have access to all, but others can only do firewalls or maybe routers. Yes, vendors do outsource as well. So it should be of no surprise if you find subcontractors within your IT primary contract.

IT security experts know time is money and money can't fix lost data. Quick reaction, documented procedures and log captures are critical in times like these. It is the quick reaction and procedures that help us when a virus like Welchia comes along. Well our outsourced friends got an F for effort and execution. In fact, we have the documentation that proves the virus came across an internal link to none other than – bingo the outsource location. Yes, they had the virus two days before letting any subordinate locations know. Yes, they had seen alerts and alarms from our location. But they sent a request for investigation and correction to us. Only we no longer have the equipment and tools for use to accomplish the request. TCPDUMP was a critical tool embedded on the firewalls. Real time analysis of input/output traffic even specifying TCP ports, hosts and interfaces could be accomplished on the firewalls – the ones we don't control anymore. This is a loss of synergy costing us dearly in security posture.

If we had control of our firewalls – we would have executed multiple tasks simultaneously; TCPDUMPS, Access Control Lists (ACL), Port redirects, and detail logs. We would have pinpointed the type, area and gravity of our security posture. We would have at least two days worth of time. Did I mention that phrase about time? The correct security posture and process should have executed something like this: On day one the central BP notices malicious traffic (ping bombs). They perform the analysis utilizing the firewall tools. They send out a notice to subordinate locations stating the problem to date and to ensure a specific virus definition be validated on all systems (part of that integration thing again). If necessary segment external connections until the necessary virus correction can be obtained.

Unfortunately, every aspect of the security posture was compromised; Inadequate Firewall expertise with the lack of understanding critical integration point and the responsibility of managing that point such as, security notifications and dissemination of immediate actions required, validation of required action and process improvement if necessary. Our outsourced contract did not ensure vendor documentation and dissemination to dependent companies. The Service Level Agreements (SLA) were only concerned about services and not the security posture required to support those services. In our case even the parts weren't accomplished let alone the total – so forget the synergy. Synergy here would have been reaction time and thorough execution of security assessment and mitigation.

IT is converging toward better firewalls and their capabilities. Application-level firewalls are critical today in intrusion detection and blocking application level attacks. These attacks exploit normal and usually approved protocols. When the data is reassemble the attack becomes evident such as buffer overflow vulnerability for a web server. Application-level attacks are some of the most difficult to protect against. Consequently, companies need to be preparing themselves to purchase, implement and integrate these application-level devices within their IT systems. Although these devices stand as fierce warriors at the gates of many companies, too many times enemies find the back door. In our case the back door was subordinate traffic links we trusted. Today's security posture requires a reassessment on what a trust network is especially if users travel with their computers and can bypass the perimeter with application level viruses like Code Red.[7] Assessment of what our companies are actually trusting and hence the vulnerabilities we are susceptible to would be an excellent application of security integration.

Outsourced Network Design and Operating System (OS) support

Have you ever spent a significant amount of time with vendors discussing, identifying, designing IT systems for future capacity and capability thus enhancing your business processes? Have you then watched in utter amazement as reality set in punctuating that the designed did not work as advertised? Worst, you realized where in the determination of business processes, the lack of effective communication materialized either by terminology, actual processing or control. This scenario happened often without outsourcing. With outsourcing this phenomenon will cost you money to fix and a probable security nightmare. "Half of this year's IT outsourcing projects will be tagged as losers by senior decision-makers for not delivering on bottom-line promises, said research firm Gartner. Outsourcing is prone to failure because of breakdowns in communications between outsourcing providers and their clients, Gartner said."[8]

Network Design Example

It took over two years for my company to implement Windows Active Directory (AD). We painstakingly reviewed, documented and simulated the effects of migrating from Windows NT4 to Windows 2000. We discussed and chose the Domain model, established the Organizational Units (OU) and the effects on critical core services such as Domain Name Resolution (DNS), Window Internet Name Service (WINS) and email. Everyday tasks typical for system administrators were reviewed and thought out. Again these services were to be centrally controlled, managed and administered. We would retain control only on our specific OU. The problem in a nutshell was the fact that we never fully obtained our goal of an AD enterprise. The concept failure seems to be lost for upper management. Yes we run client side Windows 2000 Professional. We also have Windows 2000 servers – but still running in mixed mode. Our glitch was the fact that our security posture and processes of email prevented us from migrating to Windows 2000. Further still, the cluster solution provided by the outsource vendor was at best-antiquated and at worst just plain myopic. The cluster was unstable, unreliable and now definitively dead. So we are in some kind of holding pattern. Not NT and not 2000. Our failure to properly ensure our outsourced solution indeed supported all of our services is unacceptable. But for the outsourced solution to be one of shortsighted and realistically never supportable is equally damaging. Yet this integration issue is nothing in comparison to the loss of quality, level of service, security and overall performance of our network.

Today we fully understand that a "mixed" mode AD is not much different than a characteristically NT4 domain. WINS is still predominantly used in server-to-server resolution. Since WINS cannot be parsed our central outsourced folks are in control of this resource. Every time we need to remove or add a server to the domain we must coordinate by phone and/or email to accomplish the task. Essentially every entry in WINS concerning the given server must be deleted. Tombstoning does not work in this scenario.

Since Dynamic Host Control Protocol (DHCP) dynamically registers users/computers to DNS and WINS, we have similar issues with these services. Have you tried to track down and computer who's antivirus is not updating? If you use the ping (– a option) you get one name. Then reverse resolution will give you another name. Is this the sort of integration and security posture that provides a better value added service with respectable response time in any given security incident? Unfortunately the performance is unacceptable and many companies have to develop convoluted processes and work-arounds in order to keep current operational levels. What we are left with is requiring additional time to perform the same system administration functions. Our centralized outsource administration is no smarter nor capable and in fact must perform reoccurring and remedial tasks based on flawed system migration, execution and integration. Does that sound like synergy to you?

Outsourced Vulnerability Assessment

One of the most critical elements for security integration is the need to establishment a process of assessing your network vulnerability. Vulnerabilities are network loopholes caused by software bugs and programmers back doors that could allow hackers unauthorized assess. These vulnerabilities would include desktop OS vulnerabilities to infrastructure platforms such as Cisco and Marconi products. The vulnerability assessment (VA) process is an almost daily accumulative testing of every network device under your control. It is the primary heartbeat advertising potential security threats and compromises to your IT systems. "It's important to locate where information is stored, understand the security measures in place that guard that information, and identify vulnerabilities and suspect configurations that place information at risk."[9] No quality company that relies on IT systems for the success of their business could do without VA. Therefore, any company outsourcing IT services would require the VA process to be integrated in daily performance and status reporting. VA is a perfect example of vertical alignment discussed earlier. VA is applied at every major IT level such as, infrastructure, OS and application. Further, many VA systems will pose as the hacker executing a series of attacks to gain access to vulnerable devices. This is why VA is a significant tool to integrate into your IT systems. VA systems provide some of the best value synergy to an IT system.

Having a VA system does not provide absolute security. Security integration will have to consider the effects running such a processes will have on the IT system. Again required process identification, implementation and control are paramount. It is possible that the VA system will actually induce the security risk you were trying to avoid. Honestly though, that type of failure is from our management process not the VA system itself. In order to obtain an accurate assessment of the network, you need to task that network. Tasking the network will reveal network and security relationships that even the best IT integrators would miss. Consequently, managers need to test, evaluate and validate VA systems before full implementation. This process is continuous since vulnerabilities are constantly being update.

Intrusion Detection Example

Our company utilizes Internet Security System (ISS) for our vulnerability assessment. Currently this product has over 13,000 vulnerabilities, threats and security checks that can be performed on IT systems.[10] We outsource our vulnerability assessment as a means for unbiased assessment. Unfortunately, we experienced a Denial of Service (DoS) attack on our infrastructure system caused by ISS scans. We were still in our VA validation process when we became aware that an ISS scan was being performed causing a complete network infrastructure collapse. Although this is obviously an undesirable result, the failure stemmed more from our lack of communication sharing of when and where the scans were taking place than the ISS system itself. The ISS system performed an invaluable security integration service by discovering an unknown vulnerability.

The ISS database determined that our Marconi system was a Unix-based system, but for good measure ISS runs all vulnerabilities against a platform. This aspect of ISS is absolutely wonderful. It is from this aspect of ISS that we discovered an unknown vulnerability for Marconi. The Marconi device (ESR) was vulnerable for a Microsoft Internet Explorer (IE) and Internet Information Server (IIS) Code Red attack. In fact, this attack developed into a persistent DoS attack. After running the BackdoorCodered2 (scan # 6992) virus against the ESRs , the supervisor modules would lockup without recovery. Rebooting the device was the only corrective action. This vulnerability has now been updated in the CANS. In addition, we no longer use this Marconi code since Marconi has fixed the vulnerability.

So in summary our VA system provided realtime vulnerability assessment to include the capability to assess unknown vulnerabilities. Our security integration suffered since we did not ensure our management process included notification of scan execution. That disconnect allowed three DoS attacks on our infrastructure, which effectively brought all network services down. Fortunately, we still were validating the outsourcing performance and therefore could deduce the cause. Finally, our VA system allowed an improvement to not just our infrastructure but also any Marconi customer using the current code. The end state is that we have better communications synergy by using our VA management process. We obtained better protection of our infrastructure.

Conclusion

So what is the bottom line for companies today that outsource IT services? How do companies gain communications synergy? Where is the game plan that is simple, focused and doesn't need a rocket scientist to figure out? How do corporate managers ensure their business process will benefit the most out of IT without compromising their security posture? How do they protect what is crucially their business intelligence – even from the outsourced vendor? The simplest answer is that they must ensure they have as a business partner, someone with high-level IT integration with accountability. This support doesn't have to consist of personnel by the dozens. It could be in-house or outsourced having only one or two key personnel. These individuals will be your company's security integrators responsible for interweaving IT security throughout your business. They will help you obtain your best value IT contracts:

> "Not surprisingly, the poll shows a direct correlation between security confidence and an organization's level of security investment. CSOs who reported being extremely or very confident in their security measures were those with the highest budgets. Incidentally, this group also boasted the lowest number of cyber crime incidents and monetary losses as a result of those incidents."[11]

These individuals will have the knowledge, experience and performance record of not only IT services, but also the capacity to successfully integrate business processes and keep those processes secure. They would be held accountable to the company. They would hold vendors accountable by providing metrics to the company and vendors. The most ironic aspect of security integration that companies need to understand is that the solution lies with human intervention. The answers cannot be found by a single IT system or device. Complete integration of man and machine through out the business culture and organization will provide the level of security posture required in today's IT world. The results will be communication synergy.

List of References

[1] "55bn virus damage costs for businesses last year"
URL: http://www.silicon.com/software/security/0,39024655,39117842,00.htm (19 Jan. 2004).

[2] "Taking the industry's pulse" *Computing Canada*. Vol 30 No. 1
URL: http://www.itbusiness.ca/index.asp?theaction=61&lid=1&sid=54385&adBanner=Training (16 Jan. 2004).

[3] Business Wire URL:
http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20040126005442&newsLang=en (26 Jan. 2004).

[4] Erickson, Brian. "Key Trends for Utilities in 2004"
URL: http://www.energypulse.net/centers/article/article_display.cfm?a_id=592 (19 Jan. 2004).

[5] Picarille, Lisa. "The Secret to Successful Outsourcing" *Destination CRM*.
URL: http://www.destinationcrm.com/articles/default.asp?ArticleID=3773 (19 Jan. 2004).

[6] Burman, Tushar. "Managed Security Services: Outsourcing mantra"
URL: http://www.securesynergy.com/media/newsitems/0057-03/0057-03.htm (2 Jun. 2003).

[7] Weisman, Robyn. "Deepening the Firewall: Exclusive Interview with NetScreen Executive Officer David Flynn" *Ecommerce Times*. URL: http://www.ecommercetimes.com/perl/story/32533.html (8 Jan. 2004).

[8] Keiser, Gregg "Gartner Says Half Of Outsourcing Projects Doomed To Failure"
URL: http://www.crn.com/sections/BreakingNews/dailyarchives.asp?ArticleID=40804 (26 Mar. 2003).

[9] "Identifying the real threat" *Network Magazine.*
URL: http://www.networkmagazineindia.com/200211/inperson2.shtml (Nov. 2002).

[10] Internet Security Systems URL: http://xforce.iss.net/xforce/search.php

[11] Business Wire URL:
http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20040126005442&newsLang=en (26 Jan. 2004).