Security and Risk Management Strategies

In-Depth Research Overview

# Implementing Security Controls in Outsourced and Offshore Environments

Version: 2.0, Feb 21, 2008


## AUTHOR(S):

**Eric Maiwald**
(emaiwald@burtongroup.com)

## Additional Input:

Fred Cohen


## TECHNOLOGY THREAD:

**Risk Management**

## Conclusion

Many enterprises use outsourcing and offshoring to more efficiently perform noncritical commodity functions. However, outsourcing introduces risk to the enterprise, and proper controls must be used to mitigate the risks to an acceptable level. While technical controls can be used to manage some types of risk, their effectiveness degrades with increased information technology (IT) outsourcing. Management and contractual controls are a must and should dovetail with vendor management activity and legal team advice. IT teams will apply different strategies for outsourcing, depending on whether it's a technical-team decision or management edict.




BURTON GROUP 7090 Union Park Center · Suite 200 · Midvale, Utah 84047 P 801.566.2880 F 801.566.3611

www.burtongroup.com

# Publishing Information

Burton Group is a research and consulting firm specializing in network and applications infrastructure technologies. Burton works to catalyze change and progress in the network computing industry through interaction with leading vendors and users. Publication headquarters, marketing, and sales offices are located at:

**Burton Group**
7090 Union Park Center, Suite 200
Midvale, Utah USA 84047-4169
Phone: +1.801.566.2880
Fax: +1.801.566.3611
Toll free in the USA: 800.824.9924
Internet: info@burtongroup.com; www.burtongroup.com



Burton Group's *Security and Risk Management Strategies* service provides objective analysis of networking technology, market trends, vendor strategies, and related products. The information in Burton Group's *Security and Risk Management Strategies* service is gathered from reliable sources and is prepared by experienced analysts, but it cannot be considered infallible. The opinions expressed are based on judgments made at the time, and are subject to change. Burton offers no warranty, either expressed or implied, on the information in Burton Group's *Security and Risk Management Strategies* service, and accepts no responsibility for errors resulting from its use.

---

If you do not have a license to Burton Group's *Security and Risk Management Strategies* service and are interested in receiving information about becoming a subscriber, please contact Burton Group.

# Table Of Contents

# Synopsis

With the substantial potential for cost reduction, performance improvement, and economies of scale, outsourcing and offshoring have become more than just fads for enterprises. Of course, outsourcing is not a new idea—enterprises have been outsourcing almost since the beginning of commerce for the simple reason that no enterprise does everything on its own. Most of what enterprises outsource is noncritical, commodity functions for which there are multiple suppliers.

Depending on what is outsourced, the enterprise may be accepting additional risk, and therefore there is a need for additional controls. Risks may come from reliance on a particular vendor, security failures at the vendor, the loss of intellectual property, a loss of creativity in problem solving, a loss of flexibility, or legal and regulatory differences in various locations around the world. There is a difference between performing a function with internal employees at an enterprise-owned facility and having that same function performed by employees of another organization at a facility that is not a part of the enterprise.

Controls are needed to enable the outsourcing relationship. The enterprise must determine the necessary internal and external controls and make sure they are implemented correctly to meet the enterprise's control objectives. The choice of controls depends on what is outsourced. Technical controls such as network zoning, proper authentication and authorization, software testing, and physical security controls can help the enterprise manage its risk, but the more information technology (IT) functions are outsourced, the more the enterprise must rely on managerial and contractual controls.

To properly manage risk, the enterprise should identify a strategy for outsourcing so that it understands the risks involved, as well as which controls are required. Outsourcers with similar control objectives, policies, and procedures are more likely to be good fits for the enterprise than those with dissimilar controls. Enterprises need to determine how they will govern vendors and verify that the proper controls are in place. In the end, the enterprise needs to conduct audits of the vendor's controls and facilities.

# Analysis

Outsourcing is not a new phenomenon. Enterprises have been outsourcing almost since the beginning of commerce, and the reason is simple: no enterprise does everything on its own. Enterprises buy office supplies rather than make their own. Enterprises use other companies to stock vending machines, take care of plants inside and outside the buildings, clean offices, and the list goes on. Most of what enterprises outsource is noncritical commodity functions, and the benefits of this outsourcing go beyond simple cost savings. Depending on what is outsourced, the enterprise may be accepting additional risk, and controls are needed to manage this risk. The risk picture also changes when an enterprise chooses an outsourcer that is not local. In other words, the outsourcer may exist in a different country in a different part of the world. The common term for this is "offshoring," but this term really only applies to enterprises whose presence spans only a single country. For large, global enterprises, this is an exception rather than a norm.

# Reasons for Outsourcing

Generally, commodities are outsourced while noncommodities that bring value to the enterprise are not. Commodities often have multiple suppliers, and it is easy to switch between suppliers. In some cases, outsourcing makes sense and happens naturally. For example having others manage facilities, physical security, and payroll makes sense for many enterprises because of economies of scale. These functions also will not differentiate one enterprise from another.

Noncommodities make the enterprise what it is. Noncommodities are the core competencies of the enterprise, and they differentiate one enterprise from another. It is often difficult to find any suppliers for noncommodities and, therefore, if a supplier is found, it may become a single point of failure for the enterprise.

The desire to outsource may be driven from above. Enterprise executives may determine that outsourcing is a good idea for any of a number of reasons, including the perceived cost savings, executive-level metrics (e.g., revenue per employee), or simply because it is fashionable or trendy. When the desire to outsource is driven from above, information technology (IT) departments will most likely not be given the option to outsource but will be told that outsourcing plans must be created.

Outsourcing may also be driven from the IT department, which may see significant cost savings by outsourcing because a vendor may have significant economies of scale in a particular area. For example, a security service provider that specializes in monitoring intrusion prevention devices may be able to monitor enterprise devices for less money than it would take for the enterprise to hire and retain the necessary staff and equipment to perform the same function. The difficulty in hiring and retaining key staff or expertise is another reason why IT may look to outsource a function. Rarely used technical skills are good candidates for outsourcing, because employees possessing those skills will be difficult to retain and keep busy and interested.

Enterprises that are experiencing high employee turnover or that foresee high turnover may find a benefit in outsourcing because the inconvenience associated with hiring new employees will be transferred. An example of this is a large enterprise that faced a mass exodus of IT employees with mainframe expertise. The enterprise was preparing to offer early retirement to employees, and the IT department was expecting to lose its entire mainframe team. Rather than reconstitute the team, the IT department found a vendor to take over management of the mainframes.

An enterprise IT department may see benefits to outsourcing when faced with new projects or requirements. Faced with the need to meet Payment Card Industry (PCI) requirements or new requirements for availability of a data center, the IT department may view outsourcing as a lower-cost alternative to meeting the requirements. In this case, the vendors will advertise their existing infrastructure and show how using the vendor allows the enterprise to meet the requirements on day one.

# Benefits of Outsourcing

Reasons for outsourcing were discussed in the previous section, but does outsourcing really provide these expected benefits? Outsourcing can provide benefits. Certainly there are cost savings. One large enterprise that outsources software development projects found that not only does the vendor provide a cost savings on a cost-per-hour basis but, by structuring the contracts correctly, the enterprise was able to better manage project schedules—which, of course, also helped manage project costs.

Vendors that already have the staff, expertise, and equipment to provide a function can bring systems and projects on line faster than if the enterprise built the entire system from scratch internally. Outsourcing may increase the ability of the enterprise to respond to changing conditions or new markets. The enterprise is taking advantage of the efficiency associated with the outsourcer.

Enterprises that outsource may be able to take advantage of location benefits. Different parts of the world have different labor rates and costs of living. By making use of outsourcers in different parts of the world, the enterprise may be able to take advantage of lower labor rates or perhaps gain access to different markets for goods. Expanding the locations where an e-commerce function is provided may also yield multiple Internet access points, which may provide higher overall bandwidth and higher availability.

The key to gaining benefits from outsourcing is to make sure that the relationship between the enterprise and the outsourcer is easily untangled and that adequate financial protection and verification of proper function is provided.

# Risks of Outsourcing

There are differences between internal employees working at internal facilities on internal projects and employees of another organization performing similar tasks at another location. The enterprise may lose the ability to control behaviors and decisions about technical and nontechnical protective measures. The protection posture of the enterprise changes with outsourcing because elements of risk management, information security operations, and other security processes are placed out of control of the enterprise. The controls that the outsourcer puts in place may be different than those used by the enterprise, and the enterprise will need to adjust its own controls to deal with the new situation.

The first question to ask when talking about outsourcing is: What is being taken out of the hands of managers and employees who are bound to the enterprise's normal operation and locations on a regular basis and put into other hands? For simple outsourcing (e.g., transfer of shipping duties from internal workers to suppliers), the issues are relatively simple to understand and straightforward to deal with. But not all outsourcing is this simple. In IT, things like operations of systems (including networks and databases), software development and support, helpdesk operations, and data center operations are increasingly being transferred to outsourcers. These transfers involve many different things, such as intellectual property, knowledge needed to operate the enterprise, and sensitive information. These are the very things that form the core of information-related risks to the enterprise, and, as a result, they are important to clearly understand in order to meet the resulting risk management changes in the information protection arena.

The protection posture of the enterprise changes with outsourcing because elements of risk management, information security operations, and other security processes are placed out of the control of the enterprise. At the very least, risk is controlled differently than it would be for internal systems. By looking in detail at each of these issues and identifying the differences, issues can be listed and addressed with compensating controls, where appropriate. The *Security and Risk Management Strategies* overview "A Systematic, Comprehensive Approach to Information Security" provides a structure for getting at these issues.

Different types of outsourcing may create different types of risk for the enterprise, including but not limited to:

- **Getting too involved with, or too dependent on, a vendor:** Outsourcing works best when the outsourced function is a noncritical commodity. An enterprise that outsources critical IT functions may end up at the mercy of the outsourcer. Should the outsourcer fail to deliver the necessary service, the enterprise may suffer negative consequences.

- **Security failure at the vendor:** The outsource vendor may have control over sensitive information and, if the vendor fails to protect the information, the enterprise may suffer regulatory penalties or reputation damage. For example, there have been several stories of vendors that, by misplacing a backup tape or laptop, lost sensitive enterprise information. While the outsource vendor's name is usually mentioned in such situations, due to various breach-notification laws it is the enterprise that must notify customers.
- **Loss of intellectual property:** Sensitive enterprise information may be transferred to the vendor because the vendor needs the information to perform the outsourced function or simply because the information will reside within the vendor's facilities. Access to the information is now under the control of the vendor, and it may be disclosed to unauthorized individuals without the enterprise's knowledge.
- **Loss of creativity:** Employees add value to the enterprise by finding creative solutions to problems. The solutions may increase the intellectual property of the enterprise or they may simply be more efficient and therefore less expensive. When an enterprise outsources a function, the incentive to do things better may disappear. Even if the incentive does not disappear, the vendor (rather than the enterprise) will be the beneficiary of the creativity.
- **Distance and time:** Depending on the location of the outsource vendor, there may be risks associated with distance and with time differences. For example, if an enterprise outsources software development to a vendor on the other side of the world, it may be difficult to have face-to-face meetings to go over requirements and solve problems. The time difference between locations may limit phone or video conferences. Overall, these issues may limit enterprise oversight of the project.
- **Loss of flexibility:** Enterprises may lose flexibility when a function is outsourced because the vendor will likely meet the explicit requirements of the contract. Changes to the contract will require change orders and additional costs, and the process to implement a change order may reduce the ability of the enterprise to respond to changing business requirements.
- **Knowledge and expertise stays with the vendor:** Knowledge gained by outsourced workers resides with the vendor and not with the enterprise. So, as employees learn better processes, this knowledge will not become part of the enterprise corporate memory but will instead become part of the vendor's corporate knowledge. The same is true for security awareness and the effectiveness of the security culture. The enterprise will rely on the security culture of the vendor. For example, IT architects need to be aware of emerging threats and vulnerability so that their planning can take these things into account. If day-to-day management of IT systems is outsourced, the architects may lose insight into the latest attacks and, therefore, the architects may be less effective.
- **Legal and regulatory differences:** Laws and regulations differ across the world, and these differences may increase the risk to the enterprise. For example, it may not be possible for an enterprise to monitor the activities of an outsourcer's employees in a different country due to privacy laws in that country. is especially noted for prohibitions on employee monitoring. Alternatively, laws around intellectual property theft may not provide sufficient deterrent in some parts of the world.
- **Cultural differences:** Values often differ according to culture. Enterprises that assume that the cultures of their primary locations are the same as those in other parts of the world may find that some controls they rely on don't work in the same way or provide the same level of risk mitigation. For example, in some countries, patriotism or loyalty to a clan or regional group may outweigh concern about breaking the law.

How these risks materialize is affected by a number of factors, including the sensitivity of the outsourced activity, its criticality to the business, the degree to which the outsourced activity is commoditized so that suppliers can be replaced, and the degree to which carrying out the outsourced activity requires architectural coupling with the enterprise.

In the end, the risks of outsourcing are influenced by the reasons the enterprise saves money by outsourcing. If the vendor can perform the function for less, they are more skilled, the workforce is less expensive, they have economies of scale, or the savings result from not carrying out the same level of control the enterprise would carry out.

# Controls for Outsourcing

Enterprises deal with risk in different ways. An enterprise can avoid risk by not entering a business area or not performing a function. In the case of outsourcing, an enterprise may choose to avoid risk by keeping the function in house. An enterprise can attempt to transfer risk with an insurance policy or by using contracts and statements of liability to transfer risk to the vendor. Of course, not all risk can be transferred—after all, it is still the enterprise's reputation and brand that is at stake—and most vendors will try to manage and control their own risks and, therefore, will be unlikely to accept excessive risk.

Risks that cannot be avoided or transferred must either be accepted or mitigated. Acceptance of risk depends on the risk appetite of the enterprise. Some enterprises may be willing to accept significant risk if the cost savings (i.e., the potential reward) is great enough, but most will attempt to mitigate the identified risks. The decision on how to handle the risks of outsourcing will be made by the enterprise's executive management. Decisions about which controls to use may be left to other departments (e.g., IT) once the overall decision has been made. More detailed information on the risk management decision can be found in the *Security and Risk Management Strategies* overview "A Systematic, Comprehensive Approach to Information Security."

Controls are needed to enable the outsourcing relationship. The enterprise needs to know what the controls are and if they are sufficient to meet the enterprise's control objectives. Controls also must be monitored to make sure they are effective and in place.

The choice of controls depends on what is outsourced. For example, technical controls may be very useful if certain application development is outsourced. However, technical controls begin to lose their usefulness as a greater part of the IT department is outsourced, because the expertise to monitor the controls—not to mention the access necessary to use the controls—may be transferred to the vendor.

As more and more IT functions are outsourced, monitoring the vendor and auditing the vendor's controls become the dominant risk mitigation mechanisms for the enterprise.

## Policies, Standards, and Procedural Controls

For any outsourcing relationship:

- Control standards must be compatible between the enterprise and the vendor
- The implementation of policy must be compatible between the enterprise and the vendor
- Hiring procedures at the vendor must meet the enterprise's hiring standards
- Testing procedures and change control must be made to include both the enterprise and the vendor
- procedures must be updated to include dealing with the vendor in an outsourced environment

Differences in organizational policies between the enterprise and the outsource vendor will cause the enterprise to suffer. If the vendor has more lenient policies in some area, the enterprise does not meet the same standards for outsourced work as for internal work (and therefore risk may be too high). If the vendor has stricter policies, it presumably charges more to carry them out, and the enterprise could pay less by reducing those policy requirements at the vendor.

Looking for vendors that apply similar control standards will help to locate compatible vendors. More details on enterprise control standards can be found in the *Security and Risk Management Strategies* overview "Enterprise Security Control Standards: Which Ones and Where They Apply." The vendor may have standards that are applied to all customers. It is very difficult to get a vendor to change its standards, and any additional controls will add to the overall cost.

Differences in policy between the enterprise and the vendor may dictate compensating controls so that the mismatches are addressed. These controls may be technical, managerial, or contractual. Changes to policies will result in changes to controls, and if the vendor changes a policy, the change should not be implemented until the enterprise has made its changes to the controls.

## Technical Controls

Technical controls are control mechanisms implemented as part of IT technology and systems or as part of the physical environment in which the IT systems exist. Technical controls require the enterprise to have the necessary expertise to properly implement and manage the installed products. Monitoring will also require sufficient staff to identify and respond to events in a timely fashion. For these reasons, technical controls can only provide risk mitigation if the enterprise retains sufficient IT access and resources. See Table 1 for examples of technical controls, how they might be used, and their possible limitations.

| **Technical control** | **Use** | **Limitations** |
|---|---|---|
| Content control<br><br>(Also see the *Security and Risk Management Strategies* reports "Document Management Security: Not Receiving the Scrutiny It Should" and "Controlling Information with Network Content Filtering" and the *Security and Risk Management Strategies* overview "Rights Management: Driving Security to the Data.") | Limiting how sensitive information may be used or what information may be sent out of a network. | Rights management products are still in their infancy. Encryption may prevent network content monitoring from seeing sensitive information |
| Network zoning<br><br>(Also see the Reference Architecture technical position " Zones.") | Can be used to limit where outsourcer employees can go on a network. Especially useful for cases where the outsourcer requires access to enterprise systems. Zoning at the vendor may be used to limit mixing of enterprise data with other customers. | Enterprise network must be configured to separate systems to be accessed by the vendor from other systems. Vendor zoning must be monitored and audited. |
| Network controls<br><br>(Also see the *Security and Risk Management Strategies* reports "Network Intrusion Detection and Response: More Than Just Speed Bumps on the Network?" and " Enterprise Firewalls and Perimeter Architecture.") | Firewalls and intrusion detection and response systems can be used to limit network traffic and to monitor for unauthorized traffic. | Encrypted traffic can prevent inspection by network devices. |
| Authentication, authorization, and access control<br><br>(Also see the *Identity and Privacy Strategies* reports " Privileged Account Management: Addressing the Seedy Underbelly of Identity," " Understanding Role Management Applications: No Pain, No Gain," and " Fine-Grained Authorization: New Products Move a Step Closer to the Holy Grail of Identity Management" and the *Identity and Privacy Strategies* overview "Strong Authentication: Increased Options, but Interoperability and Mobility Challenges Remain"). | Can be used to limit access by outsourced employees when accessing enterprise systems. | Requires procedures to be updated so that outsourced employees can be provisioned and deprovisioned. Should be coupled with appropriate logging mechanisms. |

| | | |
|---|---|---|
| Virtualized desktop environments<br><br>(Also see the *Security and Risk Management Strategies* overview "Attacking and Defending Virtual Environments.") | Can be used to limit how an outsourced employee accesses internal enterprise systems. May reduce the likelihood of malicious software infections and of unauthorized copying of sensitive information. | Requires stable communications. The work of outsourced employees must be compatible with the environment. |
| Technology to obfuscate data or generate appropriate test data | Used to provide data for testing applications. | Test data must be able to completely exercise the application. Obfuscated data must be modified so that obvious patterns are obscured. |
| Application testing during the software development lifecycle<br><br>(Also see the *Security and Risk Management Strategies* report "Web Application Testing: Protecting the Front Lines" and the *Application Platform Strategies* overviews " SDLC Infrastructure: Supporting the Development Process" and "To Err Is Human, So Test That Software .") | Used to verify that applications do not have obvious vulnerabilities before deployment. | Application testing may not find all problems and intentional attempts to install back doors may go unnoticed. |
| Log monitoring or security event/information management systems<br><br>(Also see the *Security and Risk Management Strategies* report "SIEMese Twins: The Security Information Management and Security Event Management Markets.") | Used to monitor activity on systems and network devices. | May lose its ability to provide a complete picture if the outsourced vendor controls administrator accounts on systems and network devices. |
| Physical security controls | Used to monitor employees at the outsourced vendor and to provide a deterrent to unauthorized behavior. | Generally controlled by the vendor and not by the enterprise. Deterrent may fail if the vendor does not use it appropriately or if the culture does not put stock in the penalty. |

| | | |
|---|---|---|
| Encryption<br><br>(Also see the *Security and Risk Management Strategies* report "Database Encryption: The Hot Topic in Structured Information Protection" and the Reference Architecture technical position "Encryption.") | Used to protect information for remote access (e.g., virtual private network [VPN]) and for protecting data at rest. Can also help to control information when hardware reaches the end of life at the vendor. | Encryption may require key management, and the key management may be the responsibility of the enterprise. |

**Table 1:** *Examples of Technical Controls*

## Management Controls

No matter how you slice it, management is important in order to mitigate risk, and the need for management is essentially identical whether an enterprise is outsourcing a function or not. If outsourcing reduces management control, then that loss of control must be compensated for by some other control (e.g., technical or contractual) or the enterprise will be at increased risk.

Proper management of projects and operations means that requirements are defined clearly, results are reported and monitored, and quality is verified. The following three conditions must continue when an enterprise outsources a function:

- The enterprise must clearly state all requirements. For operations, this may include availability requirements (see the *Security and Risk Management Strategies* overview "Beyond Denial of Service: Is Availability a Security Issue?") and response times. For development projects, detailed requirement documents should be prepared and discussed with the vendor.
- The enterprise must define reporting requirements so that progress can be tracked. Ideally, specific metrics are identified and reported by the vendor. The enterprise will establish a monitoring framework so that management is kept up to date on the status of projects and operations. A reporting mechanism for incidents must be established with appropriate contacts identified.
- The enterprise must verify the quality of the product provided by the outsourcer. This may be in the form of application testing, operational systems testing, response testing, or audits.

Management is important so that there is some enterprise control over workers. When a function is performed by enterprise employees, management exercises control over the employees through rewards and penalties that can include terminating the employee. To provide the same type of control over workers who are employees of an outsourced vendor, the enterprise must exert influence over how the vendor's employees are rewarded and penalized. The enterprise will also need to validate that the vendor's hiring practices meet the enterprise's requirements.

The employee dynamic at the vendor is also important from a management perspective. Employees will want to perform interesting work or else they will get bored and look for other positions. High turnover at the vendor will impact the enterprise and, therefore, the enterprise should examine how the vendor manages its employees. Does it address the turnover issue? Is there a mechanism for advancement? Is there any feeling of loyalty between the employees and the vendor? One large enterprise noted some success in creating a team spirit with the vendor's employees by bringing groups to the enterprise's facilities for training. Over the course of the training sessions (which lasted several weeks), the enterprise tried to make the workers feel that their work was important, and this appeared to increase enthusiasm for the work.

The enterprise must also manage the impact of outsourcing on enterprise employees. Depending on the type of outsourcing, key employees may be replaced and the transition will need to be managed so that key expertise is not lost before the vendor is able to take over the activity. The loyalty of existing employees who remain may also change as they see how other employees were treated. This may impact the ability of various departments to maintain a sufficient quality of work.

Depending on the functions outsourced, perception of the enterprise may change within the local community. A large number of unemployed workers may cause the community to look at the enterprise as less than desirable, and this may increase other risks for local facilities and workers. The enterprise must manage the relationship with the community so that risks are minimized.

The primary management control will be auditing, because auditing and monitoring will replace day-to-day management oversight of workers. Contracts must be written to allow audits of the vendor. But to make use of the control, the enterprise must do the audits. Audits will incur additional costs and will reduce overall cost savings associated with outsourcing, but they are crucial.

## Contractual Controls

When an enterprise uses contractual controls, it exchanges managerial and technical controls—which it used to have when the function was internal—for legal controls over the vendor. The enterprise is attempting to transfer some risk to the outsourced vendor. To do this, the enterprise must take appropriate steps to ensure that the contract has adequate controls and places liability on the outsourcer. It also requires that the vendor is large enough to sustain the loss associated with the liability and to somehow make the enterprise whole. As much as every enterprise would like to transfer risk in this manner, not all risk can be transferred, and any outsourcer worth working with will also be taking appropriate steps to manage its risk. A vendor is very unlikely to accept a risk for which it does not have adequate controls.

Contractual controls can work where the outsourced activity is well defined and when success criteria are determined and agreed to by both sides—for example, with a service level agreement (SLA) that defines a level of availability for an application. In such a case, both the enterprise and the vendor understand what it means to have the application available because the criteria are clearly defined. The vendor will then take appropriate steps to manage risk so that it can meet the terms of the SLA. At the same time, the vendor understands its potential liability because the penalties for insufficient performance are well defined.

Regulations and laws vary around the world. In order to make sure contracts properly manage the enterprise risk, the enterprise's legal staff may need to engage legal expertise in various locations around the world to make sure it understands local laws and contractual requirements.

It is often believed that the customer has ultimate power in dealing with a vendor because the customer can always find an alternative if the original vendor fails to perform. While this is true, the ramifications of changing vendors may be hard for an enterprise to swallow, depending on the function that is outsourced. In the case of commodities, where there are multiple vendors and where the enterprise has not become too entangled with the vendor, it is certainly possible for the enterprise to change vendors. Examples of this include such things as cleaning services and security guards. However, as the enterprise begins to outsource IT functions, the situation begins to change.

For certain types of IT outsourcing, the enterprise is likely to find multiple vendors. An example is application development—many vendors are willing to develop applications for an enterprise. If one vendor does not perform properly, finding another is not difficult (although some costs and scheduling delays may be incurred, depending on the project's status when the switch occurs). In fact, it may even be possible to move the function back in house if the skills and employees continue to be employed by the enterprise.

However, the greater the amount of IT that is outsourced, the greater the difficulty in moving to another vendor or moving the function back in house. It's not impossible—some large enterprises have successfully pulled IT functions back in house—but it can be quite difficult. If an enterprise has outsourced all IT functions, it no longer has a large IT staff and may no longer own the IT infrastructure. Reconstituting both will take time and a careful transition plan.

# Recommendations

The following sections detail general recommendations related to risk management when outsourcing and offshoring. More detailed recommendations for particular outsourcing activities can be found in the *Network and Telecom Strategies* Methodologies and Best Practices (MBP) document "Public or Private, Build or Buy: Who's Building Your Enterprise Network?" the *Application Platform Strategies* overview "Software Development Outsourcing and Offshoring Risks and Rewards," and the *Security and Risk Management Strategies* MBP document "Considerations for Risk Management When Choosing Software as a Service."

## Identify an Enterprise Strategy for Outsourcing

While outsourcing is sometimes looked at as a tactical solution, it is really part of an overall enterprise strategy for improved performance or cost savings. Outsourcing to meet short-term needs without an overall strategy may expose the enterprise to unnecessary risk. The enterprise should identify criteria that make projects or functions good outsourcing candidates. Performing a business impact analysis will give insight into the value and downtime risk associated with each business process. This information can be invaluable in building the outsourcing strategy.

## Governance

As part of the outsourcing strategy, the enterprise should determine how it will govern vendors. The enterprise should determine who will be responsible for monitoring the vendor, how the vendor will be monitored, and what internal processes and procedures must be changed to accommodate outsourcing. It may be appropriate for the enterprise to create a vendor governance group or team to monitor vendor compliance with contract terms. Ideally, the team will be cross functional and will include IT, legal, and contracts representatives. Proper governance will also require the enterprise to maintain some level of IT expertise internally to properly perform the monitoring function.

## Do Your Homework

When enterprises look for vendors in parts of the world with which they are unfamiliar, they must do the necessary homework. Different parts of the world have different laws, regulations, and cultural norms. There are differences in governments and the stability of power and other infrastructure. For these reasons, enterprises should consider engaging firms that specialize in identifying vendors with specific skills and that can guide the enterprise through local issues.

## Analyze the Risk

Enterprises also should conduct a risk analysis before determining that a function is an outsourcing candidate—and also before engaging with any vendor. The organization should identify the controls required to manage the risk of outsourcing a particular function. It should also identify risks associated with particular vendors, as well as the compensating controls required to manage the risk sufficiently.

## Policies, Procedures, and Standards

It is recommended that enterprises look for vendors that use control standards similar to those the enterprise uses internally. They should examine the vendor's policies, procedures, and standards to ensure compatibility with the enterprise's internal policies, procedures, and standards. When an incompatibility is noted, the organization should identify the necessary control changes to properly manage risk. The organization should also identify the vendor's internal governance processes.

## Conduct Site Visits

When considering a vendor, organizations should take the time to visit the vendor's facilities. Ideally, this will be part of the risk analysis phase. Site visits allow the enterprise both to see how controls are implemented and to get a better understanding of how the vendor does business. In many cases, a vendor management team may be officially tasked with the visit, in which case the enterprise should ensure that the team has the appropriate set of security questions, benchmarks, and other things to look for.

## Limit Numbers of Vendors

Investigating and monitoring vendors is expensive and time consuming. The organization should consider working with a smaller number of vendors so that costs are reduced and the enterprise's ability to influence the vendors is increased. The enterprise should also be mindful of risk aggregation issues and higher switching costs if the vendor pool becomes too small.

## Engage the Legal Staff

The enterprise's legal staff should be engaged in any outsourcing project. The enterprise should understand limitations of contracts and what types of risk can and cannot be transferred. The enterprise must understand the options available once a contract has been signed.

## Changes in Policies, Procedures, and Control Standards

The enterprise must understand the ramifications of changes in policies, procedures, and control standards both at the vendor and within the enterprise. Changes on either side of the relationship will need to be reconciled for an effective protection program.

# The Details

When looking at the situation in many countries today, one gets a sense of the impact of outsourcing and offshoring on local economies, but business can rarely afford to pass up cost-saving opportunities. From a competitive standpoint, outsourcing must be addressed. The risk questions that must be answered largely deal with the difference between the offshore or outsourced worker and the employee working in the central office.

## What's the Difference?

Fundamentally, security requirements remain the same regardless of which organization the employees work for or where they are physically located. That is, a business process that involves information technology (IT) and people has essentially the same utility to the business and requirements for risk management regardless of who the people are and what the technology is. So, in order to understand the risks, one must drill down into the real security requirements and how they can be achieved by different combinations of people and technologies. Security requirements come from a risk analysis of the five security objectives: confidentiality, integrity, availability, use control, and accountability. More details on security objectives can be found in the *Security and Risk Management Strategies* overview "An Objectives-Based Assessment Framework for Security Solutions." Some security requirements may not be achievable by some combinations of people and technology, and these combinations can be excluded. Other combinations may increase costs, thus altering the business utility of those combinations and placing other combinations in a more favorable light.

The system that combines technologies and people to assure content utility—as discussed in the *Security and Risk Management Strategies* overview "A Systematic, Comprehensive Approach to Information Security"—is of most value.

## Outsourcing

Outsourcing has occurred since enterprises decided not to seek to own the entire means of production, natural resources, sales, distribution, and every other facet of their operations. This was a change in the early twentieth century associated with antitrust cases against companies like Standard Oil, which owned and was forced to release its network of oil field leases, drilling platforms, refineries, delivery mechanisms, and gasoline stations all over the United States and much of the world. Outsourcing is in place anytime an enterprise uses services from another organization that it could perform internally.

A fundamental thing to understand about outsourcing is that commodities are commonly outsourced while noncommodities—the intellectual capital of the enterprise that brings much or most of the value to the enterprise—are not. The value of most enterprises far exceeds the value of physical plant plus inventory. Much of the value is in the intellectual property of the enterprise, which does not end at patents, copyrights, trade secrets, and trademarks. Most intellectual property resides in the brains of enterprise employees (this is often called "institutional knowledge"). Outsourced worker intellectual value resides with the outsourced vendor, not with the enterprise.

From a security standpoint, the loss of intellectual investment includes the enterprise's security culture—the awareness, knowledge, processes, and procedures used in day-to-day operations. In fact, enterprises that outsource must also rely on the vendor's security environment. Outsourcing has potentially devastating implications for enterprises when that outsourcing comprises the enterprise's meaningful intellectual capital.

But true commodities—whether goods (e.g., paper, or ink) or services (e.g., common parts of order processing and delivery of goods around the world)—are highly amenable to outsourcing.

In the extreme, an enterprise can outsource everything. This is called an investment firm, or sometimes a holding company. The assumption in this overview is that the enterprise has some set of functions that it does internally and which comprise the key aspects of the enterprise's value.

## Offshoring

Offshoring introduces a different set of issues than other types of outsourcing: It increases distance and, therefore, time delays associated with physical events, and it introduces regulatory, cultural, and other similar issues. No matter where the enterprise starts or has its primary location, when it offshores operations, it is moving those operations to another part of the world. It should be noted that large enterprises that already exist in multiple countries will not view offshoring the same as enterprises that primarily exist in one or two countries. The motivations for offshoring include financial benefits associated with different labor rates and reduced regulatory requirements, and, perhaps as important, access to large markets in those locations.

From a security standpoint, a wide variety of valid and invalid issues are brought out in discussions. People tend to like people they think are similar, and, of course, this makes offshoring introduce racial issues. Similarly, people tend to like and want to deal with people that sound and behave like they do, which means that cultural issues and speech patterns are often reasons for opposing offshoring. Although speech patterns are typically not security concerns, cultural issues often are real security issues because different cultures produce people with different behavior patterns, and security depends on the behavior of workers in order to provide necessary security controls. Cultures and governmental structures also dictate standards of due care and diligence, which means that, in order to meet local standards of due care, an enterprise may have to work more or less strenuously. Continuity and stability of government, potentials for military conflict, and other similar issues are also important.

When outsourcing and offshoring are combined, even minor issues with offshoring are exaggerated because they interact with outsourcing problems to exacerbate the situation.

## Management

Outsourcing reduces normal management control over personnel and business decisions and thus increases the need for compensating controls. For example, the difference between the enterprise managing the IT department and having an outsourcer do the same thing can arguably be codified in terms of the precise management roles, responsibilities, reporting chains, ability to make changes, and all other aspects of management that exist within the enterprise. When the IT department is owned by the enterprise, the enterprise can hire and fire, promote, demote, or carry out any other personnel lifecycle controls it wishes without appeal to any other body (subject, of course, to regulatory requirements).

Outsourcing arrangements don't always allow the buyer to determine who is hired and fired, promoted, demoted, and so forth, within the outsourced vendor's organization, and this is presumably part of the overhead saved by the enterprise in outsourcing. But someone has to do it, and if it saves money to have someone else do it, either they do it better than the enterprise can because they are more skilled, they have some economy of scale, or the savings result from not carrying out the same controls the enterprise would carry out—in which case, compensating controls are needed. Raises, bonuses, and all manner of rewards and feedback are provided through management, and when management is ceded to another organization, the enterprise loses not only the ability to influence worker behavior, but also the feedback it otherwise gains from having management in touch with the workers. The enterprise should specify who will and will not work on projects, and it should implement controls to ensure compliance with its wishes.

Another element of control that is commonly lost concerns who, what, where, why, when, and how workers may carry out tasks. When an enterprise outsources work to other enterprises, the vendors generally take over control of these facets of the work, and this means that they can no longer be used as a basis for effective discrimination between appropriate and inappropriate behavior. Although this is not universal, it is certainly commonplace. Of course, when someone else pays for workers inside the enterprise facilities (e.g., bank tellers or assembly line workers at a factory), the enterprise may have its management in place for those workers, and this dramatically increases the level of control over what is available for outsourced teams with their own management working offsite.

If the business model is such that the enterprise pays for goods and checks on the quality of those goods per specifications and utility, and if there are many suppliers available, then the enterprise can reasonably control the quality of goods produced. But if the number of suppliers is small or sufficient quality control is not in place, then the enterprise will likely suffer.

So the need for management is essentially identical whether outsourcing or not, and if outsourcing reduces management control, then that loss of control must be compensated for by some other control or the enterprise will be at increased risk.

Offshoring on top of outsourcing typically creates a variety of management issues associated with cultural differences and distance. From a security standpoint, the location of management and workers is relatively unimportant. However, cultural differences in management style make the job of the security department more complex because different influence methods are required in different cultures. Because management control is firmly within the enterprise, regardless of where the enterprise operates, and the management feedback process remains available in offshore locations, management issues are relatively negligible. The one area in which this is somewhat painful is the 24-hour nature of global enterprises, but this is not particularly a security issue.

Another approach to offshoring is to create wholly owned subsidiaries in each region or offshore area. In this case, independent management structures are sometimes used, but because of the desire to share elements of operations and gain efficiencies, there are strong similarities between the management structures in the subsidiaries. This approach tends also to focus on business areas rather than things like technology support or other IT aspects of the enterprise. It is rarely advisable to split the IT function across subsidiaries, and it is rarely done. Subsidiaries often gain significant degrees of autonomy over many IT functions.

When outsourcing is also offshored, the time and distance, time zone, and linguistic issues exacerbate the lack of control, making it harder and more expensive to get involved with management issues at the outsourcer.

## Policy

Enterprises set policies according to their executive management desires and needs. They decide on factors like compliance stance, appeals process, and so forth at the top management level, and these result in policies that are enforced throughout the enterprise. For example, if a policy states that a particular process is required in order to hire someone, then human resources (HR) is responsible for meeting that policy; if the policy states that confidential information will be limited in distribution, then it may well be up to the IT department to implement the controls for this policy requirement.

Policies are often also set as a result of using policy standards, following processes defined for an industry, based on top management or ownership, and so forth. Whatever the policies, they result in internal requirements for carrying things out within the enterprise in particular ways. Presumably, there are reasons for the selections of policies, and these reasons are presumably business reasons such as those identified in this overview. When outsourcing, the business reasons do not change. Therefore, policies should remain the same. But what if the vendor has different policies?

The simple answer is that the business suffers because of differences in organizational policies between the vendor and the enterprise. If the vendor has more lenient policies in some area, the enterprise does not meet the same standards for outsourced work as internal work. But if the vendor has stricter policies, it presumably charges more to carry them out, and the enterprise could pay less by reducing those policy requirements at the vendor. Unless the outsourced vendor has only one customer or all of its customers have identical policies, some customers will have mismatches. This approach is taken in some industries such as financial services where regulatory and industry groups largely force the hands of suppliers to meet specific security standards and compatibility requirements.

Mismatches produce more than just differences in business efficiency. In the case of information protection, they can create mismatches in interfaces between systems that cause protection to fail.

As in the management arena, policy differences dictate compensating controls so that any mismatches are addressed. This means that policy changes must also result in control changes and that policy changes by the vendor must not be completed until the enterprise has made and tested the control changes. Otherwise, there will be gaps in the compensating controls. Similarly, any policy changes at the enterprise must be examined for changes in the compensating controls.

When outsourcing is offshored, the increased complexity and differences in policies are greatly exaggerated as well. For example, cultural differences in some venues may result in apparent agreement to almost any requirement, but reality will not reflect the identified policies. Audits that turn up deficiencies may cause expressions of regret and attempts to delay meaningful change. Some cultures allow this, and it remains to be seen if economic changes will force changes in local laws and regulations to improve accountability.

## Standards

Standards in this context indicate control standards, or specifications of how policies are carried out within the enterprise (see the *Security and Risk Management Strategies* overview "Enterprise Security Control Standards: Which Ones and Where They Apply" for more information). Although policies should change rarely, responsibility for control standards is most often given to titled individuals such as the chief information security officer (CISO), chief information officer (CIO), or in some cases, a director of risk management or someone within the legal department. These individuals promulgate control standards to indicate the specific needs for controls associated with meeting specific policies. For example, a policy might say that all systems must be backed up if they contain valuable enterprise data, and that the rate of backup must reflect the value of the data. A control standard might then define specific control requirements for specific classes of systems. For example, systems identified as critical enterprise applications might have to be backed up to a different site in some timeframe, and so forth. These control standards reflect the generic version of how a policy is carried out by the enterprise.

Even if the outsourced vendor has the same policies as the enterprise, incompatibilities in control standards can lead to catastrophic results. For example, if internal high-value systems must have backups at sites more than 250 miles away based on a threshold of total system loss yielding more than $100 million in losses, and the outsourcer simply has three facilities in a region, all within 100 miles of a central point, it cannot fulfill this control standard, and the business may lose more than $100 million the next time a hurricane or earthquake damages the outsourcer's locations. But it would not have harmed them to the same level if they had met the enterprise control standards.

Control standards such as these are almost never reconciled with outsourced efforts, resulting in potentially dramatic differences in control standards and the effectiveness of controls for meeting the specific needs of the enterprise. As with policies, control system incompatibilities can cause systemic weaknesses. In addition, changes in control standards at either side must be reconciled for an effective protection program. Change management must be in place if the process is to be successful.

Control standards generally guide choices about prevention versus detection and response, response times, processes for identifying event sequences of potentially serious negative consequences, processes that support risk management efforts, and so forth. The disintegration of control standards between the enterprise and outsourced vendors results in a disintegrated control standards set and likely significant control failures in issues that cross the enterprise boundary. Control standards often also address decisions about emphasis on integrity, availability, confidentiality, use control, and accountability, and different emphases may result in different outcomes.

## Procedures

Procedures are specific things done by individuals associated with specific system types in order to achieve the control objectives. For example, a procedure designed to cover the requirement for retention of system audit information might include a series of steps that identifies audit trails on systems prior to their installation and configures those systems to send those audit trails to a remote audit server in order to secure them for future use, which includes regular searches for patterns of known attacks and deviations from normal operation. Procedures are also adapted for systems and circumstances, and this does not create any unusual problems associated with offshoring. However, there are significant procedural issues associated with local laws and operations. For example, procedures for incident responses will involve different government agencies and bureaucratic reporting responsibilities, and reporting procedures will differ depending on shared resources such as central HR departments across the world and the delays associated with time differences. But these are all variations within the normal range of what a security program has to deal with, and they are not particularly more challenging in the offshoring environment than in the more localized enterprise; there are just more of them.

In outsourced environments, the enterprise almost never controls vendor procedures to this level of clarity. Differences in how identical controls standards are implemented can create incompatibilities. For example, when the enterprise is required to search all records for information related to a specific transaction, it may not be in possession of all of those records because they may exist at the vendor's facility. Although some enterprises may view such a situation as freeing them from reporting responsibilities, they are on highly dubious ground in believing that this reduces liability. Differences in how the outsourced vendor stores data, retention times for specific items in specific forms, and other technical implementation details make some processes more or less expensive than others.

As a rule, the procedural differences for accomplishing the same control objectives make relatively little difference whether outsourced or not, assuming the control standards are properly done and thorough.

## Documentation

Documentation is a vital part of the feedback and assurance process associated with information protection, and it provides, among other things, the ability to independently verify that activities have been carried out and that individuals are accurately depicting those activities. Documentation of policies and control standards, as well as the reporting they require prior to acting on events, are also vital to the proper operation of security processes.

Typically, outsourced contractors that work off site have whatever documentation the outsourced vendor provides, and whether the vendor provides documentation to the enterprise is a matter of contract. In most cases, the level of documentation provided in outsourced contracts is very limited. For example, detailed processes undertaken in investigating incidents are not usually provided to the enterprise. This is problematic because the enterprise is unaware of the particulars of what took place in those incidents and the changing nature of the threats faced. It also becomes difficult or impossible for the enterprise to verify the coordination of documentation with procedures and to verify that the procedures are carried out as documented.

Presumed but unverified documentation is inadequate to assure that required business functions continue to be carried out. In fact, documentation alone doesn't suffice. People willing to use a computer to steal funds are not likely reluctant to lie in their documentation. Real criminals attack real systems, and insiders are often involved. Without the ability to verify documentation, its utility is minimized.

## Auditing

Auditing outsourced vendors is often problematic, and contracts often restrict access. In much of the world, banking regulations, healthcare-related regulations, and various controlled aspects of industries (e.g., drug manufacturing) mandate audits that generate reports and results that are sometimes made available as part of fulfilling contractual or regulatory requirements, but this is a far cry from internal auditors' job of assuring that protection meets enterprise needs.

When internal auditing is not available to outsourced systems and processes, management can no longer monitor the effectiveness of controls. Consequently, there is no certainty available to management other than whatever risks are contractually transferred to the vendor. Many risks can be transferred to vendors, but this requires the enterprise to take appropriate steps to assure that the contract has adequate controls and liabilities to the vendor, and that the vendor is large enough to sustain the loss associated with any harm to the enterprise. In most cases, liabilities are limited, leading to continuing acceptance of all residual risk from an unknown level of protection in the vendor.

One thing often forgotten in discussion of these issues is that people are not always sincere, honest, or well intentioned. Internal auditing catches insiders preparing to perform—or having already performed—illicit acts that harm the enterprise. Without the internal audit capability in place and active at the appropriate level of detail, insiders do not get caught and losses to the enterprise increase (even if they are hard to directly detect and associate with a cause).

Because vendors wish to protect their income, they have strong motivation to cover up insider attacks to retain a positive image with their clients, and they may not care to audit for impacts of insider abuse. They have little to lose if an insider gets away with illicit activity unless the client finds out about it. If an outsourcer reports an insider attack to a client, it risks potential liability and damage to its reputation.

Although some would assert that this lack of trust is inappropriate in a polite business context, the facts remain the same whether ignored or not.

When offshoring is mixed with outsourcing, auditing problems increase. Because of the distance, language, and cultural issues, it is far harder and more expensive to audit distant places not under your control. Auditors who don't know the local language and come from a different culture are very hard pressed to convey questions effectively and understand answers. Even if contracts allow some level of audit from the enterprise, distance and lack of access limit the amount of work likely to get done per unit time.

In most cases, external auditors end up being the only option for an offshored outsourced effort, and external audit firms have many of the same internationalization problems that enterprises do. Auditors in Pakistan are Pakistani, and auditors in China are Chinese. Unless they share a common corporate culture, the differences are problematic.

## Testing

Protection testing is executed poorly, but most large enterprises engaged in substantial use of IT for handling medium- or high-consequence business functions, and most enterprises with centralized patch and configuration management, have some level of testing process associated with change management and implementation of new technologies into existing infrastructure.

Testing requirements for most enterprises are codified in approval processes and technical process controls associated with change management. But outsourcing agreements rarely cover the change management process associated with functions provided by the vendor. Some vendors practice rigorous and sound change management, configuration management, and testing. But in other cases, errors introduced by vendors' change processes have caused large-scale outages for many companies as incompatibilities or lack of adequate training produces users who don't know how to use altered systems. In addition, changes to network components with incompatibilities have caused large-scale network outages, and unmanaged change often causes outages.

If the outsourced vendor does not have an integrated change management and protection testing process that meets enterprise standards and that includes testing in enterprise environments, changes at the outsourcer could cause serious outages and loss of integrity, confidentiality, accountability, and use control. This is all the more important in larger outsourcing arrangements where, for example, networks and systems are managed by outsourced providers. Incompatibilities could result in large-scale, enterprise-wide outages in such arrangements, and they commonly result in minor outages and incompatibilities.

Testing is not limited to infrastructure components. Applications that are developed by an outsourced vendor must be properly tested before being put into production. Data used for testing should reflect real-world data, but confidentiality requirements will likely limit access to the data for workers who are not employed by the enterprise. Procedures and mechanisms for obfuscating real data or creating false data for testing must be maintained by the enterprise.

In essence, the integrated testing requirements of the enterprise must be maintained to the extent that enterprise systems integrate with outsourced systems, and internal testing at the vendor must be adequate to meet availability requirements of the enterprise typically codified under the outsourcing agreement.

## Technology

Technical safeguards must be matched in order to have effective protection across interconnected systems. For example, if business content must be protected in a trusted network zone because of enterprise security architecture needs, and if it must communicate with an outsourced system, equivalent controls are needed on the outsourced vendor's side to avoid exposing the enterprise trusted zone to external attack and defeat of zoning requirements within the enterprise architecture. System placement and trust are fundamental issues in the zoning architecture. This happens often when outsourced or offshore personnel are allowed virtual private network (VPN) access into a trusted zone without the same identity proofing and host security controls used for employees. More information on network zoning can be found in the Reference Architecture technical position "Zones."

The requirement for effective protection is not limited to zoning architecture, of course. When the enterprise's and outsourced vendor's architectures are intertwined, common requirements may need to be applied to other elements of security architecture. Depending on how the vendor's IT environment is coupled with the enterprise's, incompatibilities could degrade enterprise IT security. Also, some security requirements follow sensitive or critical data wherever it is handled, regardless of the technical coupling between internal and outsourced systems.

Architectural incompatibilities may arise out of policy differences, compliance stance, or other principles reflected in Burton Group Reference Architecture. In one case, this problem showed up rather clearly when outsourced HR functions were examined prior to an audit only to find that the vendor did not protect workers' personal information as strictly as the enterprise. The enterprise eventually required contractual changes that forced the vendor to implement controls compatible with the enterprise—including encryption capabilities not previously in place. The contract changes substantially increased the cost of the outsourced work, making it far less of a cost reduction than it was originally considered to be.

Offshoring has many technology implications, including but not limited to issues of time and time differentials, reliability, encryption, information sharing restrictions, volumes of data transferred, and cost of communications and infrastructure—all of which have substantial impact on information protection.

Time delays associated with distance are problematic when transaction processing and similar near-real-time activities are required in high volume. Availability is far harder to maintain at a distance because more intervening elements can cause failures. As things like traffic rerouting and Internet traffic interfere with transaction and other related processing, the cost/performance tradeoff is impacted by distance. This also impacts costs in terms of time delays associated with encryption. As distance and intervening infrastructure delays decrease available time, the ability to use encryption technology is altered. Availability is also impacted by distance, and, because availability is a key security objective, distance effects must be accounted for.

When offshoring and outsourcing are combined, these problems are far more severe because of the lack of control over outsourced technical decisions. Although agreements about performance can be (and are) made as part of service level agreements (SLAs), the lack of control places far more responsibility on the enterprise to adapt to the outsourced vendor rather than promoting the kind of mutual adaptation that occurs within enterprises. This is not to say that outsourcers are not very accommodating. Many of them are. But they don't have to be to the same extent as employees, and this increases the potential for issues.

## Personnel

Many consider outsourcing personnel issues far more important than any other issues with outsourcing. The lack of control over the individuals working on enterprise efforts is more than just the management issue identified previously. It goes directly to the trust issue. There is a widespread but often inadequately justified sense that enterprise employees can be trusted while vendor employees cannot be trusted to the same degree. It's a matter of loyalty, where employees are expected to be loyal to their employers while outsourced personnel, even when they are long-term workers working full-time for the enterprise, have at least mixed loyalties with some or most of their loyalty to their employer as opposed to the enterprise. Clearly, the employees had better have loyalty to their employer, or they would be untrustworthy; that is, when the interests of the enterprise and the outsourced vendor do not strictly align, the enterprise suffers. This is often controlled by designing a growth path for vendor employees covering a particular client's needs. This benefits both vendor and client. It limits turnover, and the client retains access to individuals it has probably provided training for. But because the vendor may have different executive management goals, the rewards may not be adequate compared to other opportunities that enterprise management is not aware of. Because outsourcer management is on the other side of the negotiations table, the enterprise cannot reasonably know how and why it makes its decisions or trust that other motivations won't win out.

Personnel processes are also used within the enterprise for associating trust level with workers, and to the extent that they are carried out and can be verified by the enterprise, they are certainly appropriate. But problems arise in terms of trust of the vendor as well as the workers they identify. For example, all personnel processes that integrate with identity management (IdM) provide the means for authorizing workers to work. If the vendor's HR department decides to grant workers access to enterprise systems, it can do so, and the enterprise can do little or nothing about it if authorization has been outsourced. The vendor will argue, and rightly so, that it needs to be able to control its employees to be effective as a business, but will it take the expedient route when access is needed in the middle of the night and an authorized worker is not available or is more expensive? Even if the contract specifically forbade use of someone who had not been background-checked or pre-authorized, one could imagine outsourced personnel at midnight believing it is in their best interest to conceal the problem from the enterprise.

The notions in this section may upset many readers, particularly managers who are responsible for outsourcing and who cannot see the difference between their HR department and the outsourced HR department. There is some validity in this perspective. But in the security business, it must be assumed that people aren't always good and don't always do the right thing. Even when they are trusted, the enterprise must be able to verify what they do. Like certain business partners who have taken and sold internal information from their business partners, sabotaged companies they partnered with, and committed all manner of other offenses, insiders can also be malicious. In fact, they are responsible for most losses from information security incidents today.

But the loss of control and loyalty associated with outsourcing, particularly when existing workers are transferred to the outsourced vendor—which then changes their benefits, management, and employment contracts—can be extremely problematic. Some will be upset, others will be happier, and others will remain loyal to their former employer. All are potential problems that must have compensating controls to ensure that the enterprise's HR processes and their effects on controlling employees are compensated for in contracts with vendors.

Even if the outsourcer has equivalent or identical HR controls, loyalties are mixed. But if the controls differ and the enterprise cannot exert the same level of control and standards at the vendor that are in place at the enterprise, including having the ability to limit changes to those controls, then compensating controls and the capability to compensate at the rate of change at the vendor are necessary.

One of the key issues associated with offshoring, especially in cases where national sovereignty or security are concerned, is loyalty. Although outsourcing challenges loyalty to enterprise or vendor, in the national security context, additional nationalistic, religious, or other loyalties come to the fore with higher priority.

Enterprise loyalty varies dramatically according to the nature of the enterprise. In government agencies, military organizations, national laboratories, and enterprises that support those entities, national interests and national loyalties are and will continue to be key issues. This extends to those who work for those entities, suppliers, contractors, and so forth. In this sense, offshoring is far more problematic than outsourcing.

All of this has a major impact on information protection because loyalty is the major basis for trusting that workers will do what they are supposed to do. Although fear sometimes keeps workers in line, and the notion that work is an exchange for pay is supposed to create feedback that favors more loyal workers, the notions of loyalty between businesses and workers has been dramatically reduced in recent years as more and more work is offshored. Thus, offshoring creates a reduction in trust between workers and enterprises, and this creates still more personnel-related issues, even for workers who are not part of the offshoring. Many workers also believe their work will soon be offshored, and this brings out racist, religious, or nationalistic loyalty issues.

Cultural issues are also critical to offshoring personnel matters. Background checks have widely varying utility, and different methods are available in different regions and nations. Although a criminal records check in the United States might be meaningful for select individuals and crimes, in other locations, completely different results, costs, limitations, and records are available. In some cases, governments provide corporations with direct information on who to hire, leading to planted intelligence operatives. In others, governments refuse to provide any information on their populace, leading to private investigative processes to replace records checks. Cultural issues can also result in nepotism, caste-based hiring and promotional decisions, and a wide range of other issues that affect the ability to control workers and their behavior by making security behavior part of the feedback process related to personnel. Regardless of the culture at the enterprise's headquarters, there are increased complexities associated with having multiple interacting cultures. This is faced by all global enterprises, but not all enterprises are global, and offshoring is an act of globalization.

One of the most common mistakes enterprises make is assuming that vendor employees' economic interests are stronger than interests such as nationalism, religion, or family ties. The notion that loyalty comes from higher pay rates is generally flawed, whether at the national policy level or at the individual employee level.

When offshoring and outsourcing are combined, all notions of loyalty to the enterprise must be assumed to have disappeared because the enterprise and the workers are so far removed from each other. The interaction is purely an exchange in which each party acts in its best interest. And if outsourced, offshored workers have insider access to critical enterprise content, the enterprise cannot ignore the increasing likelihood that workers could take advantage of opportunities to earn more by abusing this access.

## Physical Security

When vendors do not work on the enterprise's premises, physical security is the vendor's responsibility. If the physical security processes and systems are not adequate, the enterprise suffers, whether it owns and operates them or not.

In the physical security arena, there are many opportunities for enterprises to use outsourced data center services that are far better at physical security than the typical enterprise is. Most enterprises are relatively easy to penetrate, but many large data center providers have physical security systems that are very effective against certain classes of external threats. However, this is offset to some extent by the aggregation of risk associated with multiple enterprises being collocated within an outsourced facility, and many outsource contracts are not for data centers alone. The issue of risk aggregation associated with multiple enterprises accessing a facility can be limited to some extent by buying a more expensive suite with a better physical boundary, as opposed to simply renting a cage within a large area of cages. On the other hand, a large outsourced data center may be an attractive target for a large-scale attacker such as a military operation. But the second issue, that many outsourcing arrangements do not involve secure data center operations, is far more problematic.

Physical security varies greatly from company to company and site to site, and it is common to find vendors using whatever facilities are available to support their contract fulfillment. This may range from home workers who have almost no serious physical security but are generally obscured from being targeted, to rented office space in buildings that have minimal security and many renters, to owned facilities with varying degrees of physical protection, to high-quality, well-protected data centers and operating facilities. Unfortunately, few contracts with vendors detail the specific facility to be used. Unless the contract includes specifics of the physical security requirements, outsourced vendors may use any or no physical security in any or all of their facilities, and this will be out of the enterprise's control. Again, the lack of control issue arises. There are, of course, exceptions. Securities industry players are sometimes quite specific about physical security, access to the site, and other similar issues.

Another vital thing to understand about physical security is that it closely interacts with information security and is increasingly being integrated with information detection and response regimens. Incident handling will deal with the integration effects; however, the fact that an attack sequence may be stopped by a combination of physical and informational barriers or other combinations of physical and informational elements of the protection posture means that when one barrier changes, the other may have to change in order to provide compensating controls. A physically secure room, if there is such a thing, can replace many other controls (e.g., console login limitations, dial-in access limitations on maintenance ports, and local passwords), but if the physical control goes away or changes, the other controls are no longer in place. Physical changes must be coordinated with operational changes, and if they are split across the outsourcing arrangement or if the vendor is more or less diligent in this interaction, the consequences to the enterprise may vary from excessive costs to increased consequences from attacks.

Lifecycle issues are also important in the physical arena, and, as in the other physical issues, most contracts do not cover the lifecycle issues associated with things like vendor equipment containing enterprise data. For example, if the de-commissioning process does not include physical removal of disks or other similar changes to operations, then security will be lost. Again, the issue is control over the physical aspects of the data and system lifecycle for outsourced equipment and content held by the outsourced vendor.

Outsourced guard services are quite common but, again, when these guards have access to sensitive facilities, contracts rarely cover the issues associated with inappropriate acts by guards when those acts are at a level of harm associated with large-scale events. A guard who is paid a few dollars an hour in the United States, and for whom the enterprise pays less than $20 per hour to the guard company, cannot always be expected to resist bribes of $500 to $1,000 to allow someone to go through the trash. Yet outsourced guards are very common in enterprises. The risks associated with these guards are usually compensated for with other controls for high-value situations, but they often remain a weak link in the protective chain.

Distance is an impediment in physical security because of the time it takes to get from place to place and the need for increasing numbers of hands and infrastructure elements in contact with content and mechanisms. Restrictions on what products may be purchased and deployed (and where) may prevent the use of more trusted mechanisms and operating environments, as well as contributing to the inability to control the distribution and transportation process. Border crossings, as well as import and export laws, may limit available technical solutions. Distribution of key materials and similar procedures cannot involve personal contact, and this means that other sorts of authentication must be trusted to a larger degree.

Difficulty in securing at a distance for the information arena is far easier than in the physical arena. For example, response forces have to be local to meet most physical timing requirements, which means that much of the physical security overhead must be present at the offshore site. The physical security director or chief security officer cannot show up at the offshore site for a surprise visit very easily or rush there in response to an incident—in the best-case scenario, it would likely take 24 hours to arrive. So some sort of local physical security presence is required for offshoring. Many companies outsource this locally, but this is problematic because it is so hard to get a handle on what vendor to trust with global physical security. There are companies that do global physical security and intelligence work, but they are typically far more expensive than employees doing the same work. And those companies also offshore the work around the world, although they have done it for many years and have established methods and personnel.

Cultures vary greatly across the world. For example, the same physical searches and ever-present video cameras that work in the United States don't work in the rest of the world. There are countries where almost anything goes, and others where very few methods are allowed. In some locales, people will refuse to enforce management mandates if they are undesirable or culturally taboo. Religious and gender/sexual issues vary greatly by country, and this leads to different physical security issues such as facial coverings that prevent certain kinds of biometrics.

The legality of exporting images is not universal, so pictures taken in an industrial plant in some countries cannot be sent to other countries. This disrupts use of automated camera systems and limits investigation to local forces. Investigations generally require licensure, and this is also local (typically to a level of a state or region). This means local investigative teams are required in many jurisdictions. If matters ever get to court, local testimony will be in the local language and it will be hard to get people to accept the testimony of someone from another country over the word of local countrymen. Loyalty to nationality usually exceeds loyalty to some legal structure.

Controlling physical things at a distance is generally harder than doing so locally. Redundancy must be increased in some way to compensate for the inability to assure controlled communications at a distance. Fail-safes must be designed to deal with communication delays and failures so that proper behavior of the physical security system can be assured at a distance, even in the face of physical attack.

Governments differ in their support for enterprise protection programs. Some friendly governments will provide the security and other personnel for a plant and give the enterprise no choice. Other governments offer no support except when someone calls the local police, and then the response time may be very slow, particularly for cases in which attackers have suppressed police response in advance of an attack (e.g., a large-scale theft). Physical attacks against facilities that manufacture expensive equipment sometimes involve heavily armed gunmen in well-coordinated attacks. Local police will have no feasible response to this in many places around the world, and by the time the army arrives the thieves will be long gone. For information attacks, it wasn't long ago that the United States and the European Union (EU) had little or no response from government, and a break-in at a data warehouse facility is likely to get a detective from the burglary squad to show up within a few hours rather than an elite response team that shows up in a few minutes.

There are still many places in the world where government control is limited, and government overthrows happen in various places several times per year—either by sheer force or by bloodless revolutions. When governments and their policies change, this can have dramatic impacts on physical security issues associated with offshored work and workers. Xenophobes may threaten workers and foreign policy may interfere with business success. Access to the entire country may be limited, imports and exports may be cut off, and there may be telecommunications takeovers (as is common when governments change). The idea that an enterprise might somehow have the political power to fix these things is often found to be false.

Another area often ignored is the protection of the computing environment (e.g., power, cooling). Environment is critical for the operation of IT and environmental controls and requirements (or the lack thereof) may lead to the need for special protection for IT as well as workers.

When combining offshoring and its issues with outsourcing at a distance, these problems tend to multiply. Although some outsourcing to offshore entities may improve physical security issues and friendliness with local authorities, the lack of control very often produces environments with little or no real physical security except when the audit team arrives, which is generally known well in advance.

## Incident Handling

Outsourced vendors have every reason not to report incidents to the enterprises they serve. If they appear to be perfect, they are more likely to retain the contract. If the enterprise doesn't know about the incident, how can it hurt the enterprise? Sadly, the answer is that it can hurt a great deal—it can even put the enterprise out of business.

Detection and reaction to incidents, as well as adaptation of IT in response to the changing nature of incidents, are all vital elements of normal information protection. Although some enterprises outsource these functions to specialized companies, these sorts of arrangements almost always have very explicit sets of issues addressed, provide the enterprise with full details of all incidents, provide very specific instructions on actions in automated or externally handled response activities, and have intervention by the enterprise for incidents beyond what is expressly identified for outsourced handling. Enterprises are granted better access to the information from most vendors than they could ever have on their own because the vendors tend to be more thorough and detail oriented, retain enormous volumes of data, and analyze it very quickly and with greater expertise. These services tend to provide only technical responses to technical network and system attacks and do not handle internal attackers or misuse very well. Further, they don't interact directly with HR or other business processes, and they are therefore very valuable for very limited niches.

But when outsourcing goes beyond this very vertical incident-detection and response-handling niche, the situation is far different. The times associated with detection and response is closely tied to consequences to the enterprise, but unless there is very close collaboration with the outsourced vendor, these sorts of closely tied event-sequence approaches are doomed to fail. Enterprises often have closely held secrets regarding business processes that are not shared with vendors, and this leads to situations in which, even if the vendors wanted to do the best job feasible, they could not. Splitting responsibilities, limiting information, and other related issues associated with partial outsourcing are clearly problematic in the incident response arena.

Generally, issues like disaster recovery planning and the broader business continuity planning end up unresolvable in dealing with high-consequence event sequences where responsibility involves the vendor unless there is very tight integration between outsourcers and the enterprise.

Again, in the commodities arena, things like telecommunications services have enormous risks associated with disasters, so enterprises often choose to have multiple suppliers and practice disaster-recovery and business-continuity plans that allow them to switch suppliers and infrastructures quickly enough to meet recovery requirements. But comparable capabilities are rarely available in the noncommodities arena because noncommodities are not readily replicable. This approach to all outsourcing is appropriate, if only to prevent failure of the outsourced vendor from leading to failure of the enterprise. The lack of direct control over personnel and their locations and collocation is problematic in assuring continuity. Business-continuity planning and disaster-recovery planning must be verified to meet enterprise requirements whether outsourcing is involved or not. But in many outsourcing scenarios, this sort of analysis and process is simply unavailable.

Incident handling, both in the physical and informational arenas, becomes harder at a distance, particularly when there are many time zones between locations. On the other hand, the use of incident-handling teams around the world can make 24/7 availability far easier to achieve with everyone working daylight shifts in their area and providing coverage for the rest of the world. When there are global incidents, this means that someone in a very distant location will be in direct control of the entire enterprise infrastructure. From a risk-aggregation standpoint, this may be unacceptable, so limits on this sort of activity may also be required.

In many large enterprises, significant global information security incidents result in deployment of their global reaction force, which means waking people from all over the world to participate in decisions and carry them out locally. For offshoring, this is simply part of working at a high level for a global enterprise. But, if mixed with outsourcing, it may not be part of the contract, and waking a business partner's executive in the middle of the night may not be something that saves money in contract negotiations. Distance means time; however, in most network incidents, the time between locations around the world is not long enough to make a significant difference in response, unless the distance also leads to communications failure—which it often can. Different locations have different quality services, and these differences in quality, response time, and so forth cause availability issues that are particularly problematic in incident handling.

There are also many types of incidents that rarely happen to an enterprise unless offshoring is undertaken. These include international political incidents, wars and insurrections, and instabilities in governments. Enterprises that are not already global in nature have their local insurrections and political issues, and have adapted to them over their growth from a startup business into an enterprise. For those offshoring, there are more of these things, plus international political issues, to consider. For example, if a U.S. company offshores to the Middle East, political turmoil is likely to be normal. Problems get worse when there are invasions and wars involving the United States and local governments, and these issues have to be dealt with as part of the price of offshoring. Trade disputes between the EU and the United States have come and gone, and, depending on the industry, offshoring has been very damaging. Political friendships that seem like they will never end often end very quickly with a change of government or a single dramatic incident. These represent large-scale risks to enterprises because they can result in incidents that cannot be easily compensated for unless the offshored business is an entity unto itself and the rest of the entities forming the enterprise are only mildly co-dependent.

## Knowledge and Awareness

Within an enterprise, knowledge and awareness levels are controlled and measured in order to ensure that individuals know how to do their jobs properly. Specifically, in the security arena, awareness programs for all workers are used so that they know how to behave in specific circumstances. But when some of the workers are outsourced, the awareness program has to somehow be extended to them; and because they often work in different environments, the same rules may not apply. So, either the enterprise has to adapt awareness programs to the outsourced environment and the vendor program has to be approved by the enterprise, or the awareness program will not do the job it is supposed to do. And, of course, when multiple enterprises use the same vendor, the vendor must have either a dedicated staff for each enterprise, multiple and likely confusing awareness programs, or it will have a different awareness program than that needed by the enterprise. Awareness and user behavior are critical to enterprise protection. To the extent that it differs, different protection measures and architectures may also be required.

Training and education levels are critical to the effectiveness of enterprise protection programs. While many vendors have better security training and knowledge levels than enterprises, not all do. It is the responsibility of the enterprise to assure that the training and knowledge levels of vendor workers are adequate to the needs of the enterprise for information protection. This implies feedback from the vendor to the enterprise that allows the enterprise to test training and awareness levels of the vendor as part of the contract.

The whole point of an awareness program is to create a social environment and behavioral pattern that acts to improve the effectiveness of the protection program without worsening the rest of the social environment. Pleasant, friendly, safe, and secure are the goals. This requires different specific actions in different locations around the world, but it still deals with the same general issues. Some things need not be said in all places, while other things need to be emphasized in some cultures more than in others. This cultural deviation in awareness programs needs a set of experts who can translate the overall goals of the program and detailed content into not only the language, but also the social mores of the cultures that functions are being outsourced to.

## Organization

The type of organization involved in an outsourcing effort can also be problematic for security considerations. Entities can be public, private, government, for profit, nonprofit, of varying size, managed with different structures, and operated in different ways. Organizational differences are enormously problematic for information protection. In most enterprises with very different divisions, there are significantly different protection programs in those divisions. Operating those programs is far more complex than for enterprises with unified organizational structures and social mores.

In outsourcing arrangements between companies with substantially different organizational structures, different protection programs must be integrated in order for the outsourced functions to be integrated with internal needs. Conversely, in internal systems with different cultures and structures, the divisions tend to operate separately. The reason outsourced work often has to be integrated more than internal divisions is that outsourcing takes portions of the work from a business unit, splitting the business unit into controlled and uncontrolled parts.

# Conclusion

Many enterprises use outsourcing and offshoring to more efficiently perform noncritical commodity functions. However, outsourcing introduces risk to the enterprise, and proper controls must be used to mitigate the risks to an acceptable level. While technical controls can be used to manage some types of risk, their effectiveness degrades with increased information technology (IT) outsourcing. Management and contractual controls are a must and should dovetail with vendor management activity and legal team advice. IT teams will apply different strategies for outsourcing, depending on whether it's a technical-team decision or management edict.

# Author Bio

**Eric Maiwald**

**Vice President and Service Director**

**Emphasis:** Information security architecture, perimeter security, enterprise security management, infrastructure protection, mobility and mobile security

**Background:** 20 years of experience in enterprise information security as a security officer and consultant (with Fortrex Technologies) for large financial institutions, healthcare providers, services firms, and manufacturers. Extensive experience in the security field performing assessments, policy development, architecture design, and product implementations. Also has experience as a product manager for Bluefire Security Technologies.

**Primary Distinctions:** Respected speaker on enterprise security topics and Certified Information Systems Security Professional. Named inventor of several patents: "Apparatus and Method for Providing Multi-level Security for Communications among Computers and Terminals on a Network," "Using Trusted Associations to Establish Trust in a Computer Network," "Apparatus and Method for Providing Network Security," and "Method for Establishing Trust in a Computer Network via Association." Author of "Network Security: A Beginner's Guide, Security Planning and Disaster Recovery," (with William Sieglein); and "Fundamentals of Network Security," all published by Osborne/McGraw-Hill.