Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Security Challenges of Offshore Development

This paper will attempt to take a small step in raising the security community's awareness of growing security risks related to off-shore development by examining some of the issues and potential threats. It is beyond the scope of this paper to provide solutions for security risks associated with offshore development.

Copyright SANS Institute
Author Retains Full Rights

AD

The Security Challenges of Offshore Development

By Rob Ramer

Software development is now a global process. Hundreds of U.S. corporations are turning to offshore software outsourcers to maintain their core systems as well as develop new applications. India alone exported over $5 billion dollars of software in 2000, over 65 percent of this went to the United States.[i] Software outsourcing companies have set up offshore development centers (ODC) in many other Asian countries such as Pakistan, Malaysia, China, and the Philippines. Other popular destinations include Israel, Ireland, Mexico, Russia and Chile. These countries offer low costs, valuable trained personnel, and English language capabilities. Their facilities employee thousands of programmers who develop software applications for U.S. companies.

Excellent illustrations of such facilities are the technology parks that India has developed to aid software-exporting companies. Software Technology Parks of India (STPI), headquartered in New Delhi, is an umbrella organization with eleven facilities throughout the country. Each technology park provides for a software company's infrastructure needs by guaranteeing a supply of electricity, high-speed telecommunications links, and even hardware and network capabilities. STPI provides services for more than 450 companies.[ii] The growth of software exports from these parks grew at an annual rate of 65 percent during the nineties. Each STPI houses multiple offshore development centers.[iii]

An ODC may be a dedicated facility for one client or it may produce software for multiple clients. System requirements and specifications are normally developed by analysts working at the client company and then coded by programmers at an ODC. The ODC is usually connected to the home computer system through leased lines, through a Virtual Private Network (VPN), or sometimes directly through the Internet. The link to the ODC creates several potential vulnerabilities for the client's system. Vulnerabilities include Trojans or viruses embedded in the software, unauthorized access by ODC personnel into parts of the client network, and intrusion of the client system by a hacker who has penetrated the ODC defenses.

At the same time that software development has become a global industry, there are growing incidents of cyber warfare. After the emergency landing of a U.S. surveillance plane on Hainan Island, Chinese and American hackers declared war on each other, attacking websites in opposing countries. Such attacks increased from two or three incidents per day before the incident to 40 to 50 immediately following it.[iv] In October 2000, a wave of denial of service attacks and network penetrations has spread through the Middle East. Hackers attacked both the Israeli Defense Forces and the Foreign Ministry websites. The Foreign Ministry site crashed and the Defense Forces shut down their website as a defensive measure. U.S. organizations that support Israel were also attacked.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

US government and private security consultants warned that such attacks could spill over to other American companies.[v] On September 11, 2001, the unthinkable happened to the physical security of our nation. Given our country's newly heightened security consciousness, there will be greater attention to network security. Still, U.S. corporations are struggling to establish effective security practices within their own companies. When a company out-sourced a software project in the past, it rarely examined the security practices of the offshore outsourcing company. Whether this will change in the future depends on education of the security community, consumers and producers of offshore software, and our political leaders.

One of the great attractions of offshore outsourcing is the comparative price advantage compared to on-site development. Improved security will add to costs and both clients and vendors may be tempted to cut corners, despite the recent upsurge in terrorism. Few analysts have examined the security implications of global software development. The topic deserves in depth research, analysis, and increased visibility.

This paper will attempt to take a small step in raising the security community's awareness of growing security risks related to off-shore development by examining some of the issues and potential threats. It is beyond the scope of this paper to provide solutions for security risks associated with offshore development.

The Risks of Offshore Development

Whether engaged in global software outsourcing or not, each company must assess the threats to their computer systems and the actual risks that they face. Threats include viruses, denial of service attacks, network intrusions, fraud, and sabotage by disgruntled employees. It is, of course, impossible to defend against all possible threats and therefore each company must analyze its actual risks. The investment in computer and network security must be commensurate with the actual risks.

Risk analysis and determining appropriate counter measures is necessary for all companies. However, the picture becomes much more complicated for a company that is using an offshore development facility. There are several complicating factors:

- *Loss of control* – By outsourcing, a client loses control over the conditions under which its software is developed. A link with an ODC opens a broadband communications channel directly into the client system. The company's security personnel lose the ability to regulate authentication of users at the ODC.
- *Network complexity* - Configuration management of expanding and ever changing networks is a challenge for most security departments. Maintaining an understanding of normal traffic patterns becomes almost impossible when an ODC is thrown into the mix. If the development center produces software for multiple clients and does not isolate the networks connected to each client's system, configuration management becomes an impossible task.
- *Clashing security policies and procedures* - The client and the ODC may take varying approaches regarding known vulnerabilities, intrusion detection, or

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

perimeter defense. These discrepancies could easily create vulnerabilities for both the client and the offshore vendor.

- *Threats to a company's intellectual property* - Offshore development creates risks to a company's intellectual property because trade secrets, customer data, and financial information are often made available to a foreign company whose employees are not subject to U.S. laws. A company's worst nightmare is losing their intellectual property when they go offshore since it would require international litigation, a process that could take years of effort while the damage is immediate.
- *Legal issues* – As mentioned, different laws govern offshore vendors. The issue is not contract enforcement as much as data security because most vendors are affiliated in one way or another to U.S. corporate entities. However, the laws applying to protection of data are often non-existent in the offshore country. Another legal complication is presented by the new U.S. data privacy laws such as Graham-Leach-Bliley that requires U.S. financial corporations to protect the data of their customers.[vi] Few measures are required to ensure that offshore development centers are abiding by these laws.

Loss of control

When a company has its software produced in an overseas development center, it defines the performance requirements but it gives control over how the software is developed to the overseas vendor. Clients spend hundreds of thousands of dollars testing software applications to ensure that they meet requirements. Rarely, however, do security departments inspect the code for Trojans, viruses, or embedded Easter eggs - code that performs unspecified or even illicit activities. Virus scanners identify and sanitize widely known viruses, but they will not find code specifically designed to sabotage or provide particular information. Given the sophistication with which terrorists have infiltrated the aviation industry in the United States, such activities are real risks that security departments must now guard against.

Clients establish direct links between an ODC and their host system for a number of reasons. Some offshore teams carry beepers and provide real-time applications support. Other teams log-on to the host system during night and uses test environments to code and test programs. These programmers have authorization to update data files and system libraries needed to maintain the applications they support. The ODC network has direct access to the host computer. Some companies use development centers in foreign countries for critical operations. These companies include many leading American railroads and airlines.[vii] The vast majority of offshore developers are honest IT professionals happy to have the opportunity to work for a U.S. company. However, the catastrophic events at the World Trade Center and the Pentagon, show to what lengths terrorists have gone to cause damage to U.S. interests. It would be much easier to penetrate the security of an offshore development center and implant some code time bombs that would later cause chaos for a U.S. company.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

A client company also loses control over authentication of users logging in from the ODC. Software developers are normally given user ids with broad authority. The same is true for offshore developers. However, the client company has no control over the physical security of the ODC. Could people off the street or from another office or a team working on a competitor's system walk in and start using a workstation? Company security personnel have no way of knowing if the offshore developers are sharing passwords. They usually have no idea of what the vendor's perimeter defenses are. Vendor's security policies are rarely examined for issues such as connecting to the Internet at the same time they are logged on to the client host system.

Network complexity

Configuration management is a challenge within s single company's network. Linking the host computer with an ODC exponentially increases the complexity of the task. Depending on the methods beings used, an ODC link can mean an unknown network is linked into the heart of the client company network.

The impact of an ODC link can certainly be minimized by a defense in depth techniques. The development environment being used by the ODC can be placed in a DMZ of its own. Then communications with the rest of the network can be routed through firewalls that are specially programmed to monitor the specialized traffic involved in the project. This is not the usual pattern in offshore projects. Instead, offshore programmers are routinely treated as remote developers. They usually have to pass through a perimeter firewall but then they have the same access as on-site developers. The primary defense against unauthorized intrusion is authentication based on passwords and authorization rules. Password cracking tools such as LophtCrack can resolve most passwords within a few minutes.

As we have seen, developers are normally granted a wide degree of authority to update system libraries. Password authorization as the primary defense may be appropriate within the perimeters of a corporate network. Network security services can determine the normal traffic patterns of a programmer and monitor other activities such as Internet connections. Known vulnerabilities can be corrected and regular anti-virus updates and other defensive measures can be insured. An ODC connection bypasses all of these measures leaves multiple channels for hostile penetration of the host system. A developer in an ODC maybe be conscientiously doing his job. Still, while he is coding and testing he could also chatting on a website that would be off limits to an on-site programmer. An attacker could use the open http connection to the workstation to implant a Trojan in the host system or map the corporate network. Alternatively, a rogue developer could implant malicious code into a program that works perfectly.

Security policies & procedures

Security reviews are rarely required before an offshore development contract is signed. The assumption is that the vendor has an effective security policy. Even if the vendor has a good policy on paper, the tough question that must be asked is how vigorously is it implemented. A security review is the only valid way to answer this question. The review need not be a full-scale audit. As with all security investments, the activity should

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

be commensurate with the risks involved. The review should consist of a thorough examination of the security policies. It should also analyze the procedures in place to implement the policy and it should asses how well the policy and procedures are actually implemented. An independent security analyst who is able to ask the difficult questions should conduct the review, rather than relying on questions to the vendor sales team. An important factor of such a review is an investigation into how the vendor has dealt with known vulnerabilities. In addition to a security review of the ODC, it is critical that the client company involves its own network security personnel in all technical decisions regarding connectivity between the ODC network and the client's system.

Legal and intellectual property issues

The protection of intellectual property is primarily the duty of a company's legal department. Still, network security must also take an active role since theft of a company's trade secrets is most likely to occur using digital media. The main security goals here are in one sense the reverse of the normal approach of protecting the host from attack. When protecting intellectual property the first task is to identify the data files that must be protected and then access must be restricted. Next, the means by which this information can be removed from either the host site or the offshore development facility must be analyzed. Such information can be uploaded to a website, transferred through a modem connection, written onto a floppy disk or a CD.

It is essential for a company to analyze the risks that offshore relationships may pose to its intellectual property. The risks vary depending on the software application under development, the character of the relationship with the offshore vendor, and the nature of the corporation's intellectual property. Certain trade secrets, such as chemical formulae or industrial processes can be quickly utilized by competitors. Such information is critical to protect. The strictest security measures must be employed in software development projects that involve easily replicable trade secrets. In fact, such projects ought not to be outsourced at all. Other intellectual property is not as easily stolen. For example, a trade process such as a financial planning methodology, while it should be protected from competitors, takes a considerable time to master. Security measures for offshore projects should fit the risks to a company's intellectual property.

In addition to trade secrets, customer data, and financial information are often exposed during a software development project. Customer data can easily be used for fraudulent purposes and the incident of international Internet credit card fraud is rising rapidly. In a tightly interconnected world financial system, information on the finances of large corporations can be used for insider trading and manipulation of stock prices. The employees of a foreign company are not subject to U.S. laws. Some countries such as India are aware of cyber crime and are beginning to take a few initial steps. However, the criminal justice systems of most Third World countries, lack the technical and legal framework to investigate and prosecute system break-ins or data theft.

Conclusion

Offshore development produces a host of potential vulnerabilities for IT companies. Therefore, security considerations are of utmost importance when a corporation considers

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

the global development option. One security breach threatens the credibility, not only of the IT and network security departments but of the whole company and potentially the nation. Security guarantees must be included in the contract with the offshore vendor, with strict financial penalties for violation. The vendor must ensure that facilities and all personnel adhere to the client's standards as regards the protection of data and other intellectual property. Security personnel should insist that their company's offshore program managers conduct regular security reviews to ensure the enforcement of security policies and procedures.

---

[i] National Association of Software and Service Companies (NASSCOM). N pag. Online. 20 Mar. 2001. <http://www.nasscom.org>

[ii] Software Technology Parks of India. N. pag. Online April 1, 2001. <http://www.stpi.net/scheme/scheme.html>

[iii] Chowdhry, J.A. " Software Technology Parks of India: A Fillip to Software Exports." SiliconIndia, December 1997. N. pag. Online < http://www.siliconindia.com/magazine/Dec97stpi.html>

[iv] Eric Hrovat, "Information Warfare: The Unconventional Art In A Digital World", SANS Reading Room, June 30, 2001, <http://www.sans.org>

[v] Rob Ramer, "Protecting Your Network When Employees Log-in From the Web," November 3, 2000. Wizmo Daily News <http://www. Wizmo.com>,

[vi] "Managing Privacy," The American Banker , <http://www.americanbanker.com>, July 10, 2001.

[vii] Author interviews. January 15, 1997, Nitin Kumar, Indian IT consultant who worked for four years at an ODC that maintained train scheduling applications for one of the five largest American railroads. February 8, 2000, Interview with John Doe, XYZ Airlines, Manager IT – Technical Operations. These systems regulate the maintenance of XYZ's large fleet of aircraft. An Indian company carries maintenance beepers twelve hours a day, installing emergency fixes to the software as well as coding and installing enhancements. Flight Operations also outsources some of their software work to India and the Philippines. XYZ is one of the top ten U.S. airlines. (NOTE: As this paper may be posted on a public website, actual names of the companies and individuals have been changed for security reasons. If SANS instructors grading this have questions, I will be happy to provide additional documentation.)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 23rd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced