ANSWERING SECURITY QUESTIONS. QUESTIONING SECURITY'S ANSWERS

JANUARY 2010

GOING INTERNATIONAL

COMPUTER SECURITY ALERT

Computer Security Institute, 11 West 19th Street, New York, NY 10011, 212-600-3026, csi@ubm.com

What To Learn From Google About Security and Privacy Management in an International Business

In December, 34 high-profile companies—including Google, Adobe, Juniper, Symantec, Dow Chemical and Northrup-Grumman—were victims of a well-orchestrated series of sophisticated, targeted attacks that aimed to abscond with the companies' intellectual property. Google also discovered that the attack had led to the breach of two Gmail users' account information, but not the content of the users' e-mail messages themselves. During the investigation, Google became aware that several other Gmail users' accounts had been breached "routinely," likely due to a clever phishing campaign that specifically targeted human rights activists and international journalists who cover Chinese affairs.

Although the attacks were sophisticated and worrisome, it was the incident *response*, not the incidents themselves, that caused political and economic ripples across the globe.

Not only did Google publicly announce the attacks (when there were no regulatory compliance requirements that they do so), they hinted that the attacks were committed on behalf of the Chinese government (despite the lack of concrete technical evidence to support that claim), they announced that they might cease their practice of self-censoring Google.cn search engine results (thereby incurring the considerable displeasure of the Chinese government) or simply shut down business in China (at least the search engine part of the business), and, rumor has it, began investigating the possibility of insider collusion, suspending the network access rights of some Google China employees (and giving the rest of the staff the day off and tickets to see *Avatar*).

CONTENTS

What followed was a media tempest: Google was alternately showered with laurels for taking a bold stand against censorship, disparaged for dressing up a business decision in the costume of morality, questioned about how exactly stopping censorship was supposed to improve the security of Google's mail servers, and shrugged off by Bill Gates who said they were getting a lot of credit for doing nothing. United States Secretary of State Hillary Clinton alluded to the case during a public speech about Internet freedom, urging The People's Republic of China to investigate the security incidents at Google. China's *Global Times* impugned Clinton's speech in a Jan. 22 editorial, writing "The U.S. campaign for uncensored and free flow of information on an unrestricted Internet is a disguised attempt to impose its values on other cultures in the name of democracy." Strain was added to already precarious relations between the United States and The People's Republic of China. Meanwhile, in stark counterpoint to the praise of human rights organizations, Germany issued reminders that, by European standards anyway, Google is no paragon of social responsibility. Two German publishing companies slapped Google with fresh anti-trust suits, the German Minister of Justice publicly warned that Google was collecting too much information about people and being insufficiently transparent about the fact, and the CEO of another German publisher verbally sparred with Google's chief legal officer about fair business practices, raising the eyebrows of attendees at the DLD conference in Munich.

It's certainly made for stimulating reading. It's a reminder—invigorating us and exhausting us, in turn—that this humdrum, workaday, information security thing we do is actually a matter of great consequence. It's an intriguing case that business leaders, security leaders, privacy officers, corporate lawyers and public relations officers should study together.

What, though, is the lesson? What are we to learn from this rumpus that changes how information security professionals do their jobs? Certainly this case contains a few choice field notes about incident response, the increasing sophistication of targeted attacks, the perils of not-early-enough adoption and the risks of relying too heavily on cloud computing when the cloud provider might up and leave the country.

Yet perhaps the two key lessons the security manager should draw from this experience and follow when one's organization is endeavoring to do business in a new country are to first, know the local law and culture, and second, know thyself.

When in Rome...

When in Rome, do as the Romans do. The borderless nature of the Internet makes this advice difficult to follow—when you're *in* Rome you may very well be in Sparta, Constantinople, Thebes or any other ancient city at the very same time. Nonetheless, it is essential to be well-acquainted with Roman law *before* you make the first visit.

"I totally agree," said Xuxin "Max" Xu, security management manager of AIA Group, the pan-Asian arm of life insurance company AIG. "There are too many things on the to-do list for a company who wants to expand international business, but, understanding and complying with local law is always the top priority." Xu brings new perspectives to the international security conversation and the Google China discussion, being that he is both a security professional based in China, and that he was recently the senior manager of security and compliance at Freeborders, a China-based offsourcing and offshoring firm.

As Xu and any other compliance officer will tell you, data privacy and security laws vary greatly from country to country, and it is imperative to plot where each nation's law sits on the spectrum from privacy to security. Where you map that nation's laws on the privacy-security continuum will both answer and raise essential questions about your security program.

For example, what data are you permitted to collect? ("Data," meaning anything from personally identifiable information about your customers, to PII about your personnel, to intellectual property, to access logs, to search history, etc.) How long are you permitted to retain it? How long are you required to retain it? How must that data be stored and secured? Under what circumstances can the government subpoena this data?

No doubt you've already thought of those questions, being that regulatory compliance has become so part and parcel of the security manager's job. There are, however, plenty of other questions that may be a bit more, well, foreign, to you.

Like: are your security tools legal? Certain penetration testing tools may violate section 202(c) of Germany's penal code, which makes it an offense to create, obtain or distribute any computer program that violates German cybercrime laws. Or… what if you're not allowed to use encryption?

Ulf Löfven, currently CEO of Swedish firm Ekelöw Infosecurity, encountered just that sort of conundrum in his considerable experience working in the security and fraud field in international organizations. On a visit to Singapore, where Löfven's (former) company was just about to launch a mobile stock trading app that had already found success elsewhere, Löfven discovered that business in Singapore was going to be very bad indeed—because the encryption algorithm the app

used was prohibited. When attempting to download the encryption software from his hotel room in Singapore, Löfven received an error message stating that the use of encryption algorithms and encryption software that had not first been approved by Singapore government security authorities was not allowed for use within Singapore territory.

Of course, *doing as the Romans do* extends beyond simply following the local law—something Löfven learned in rather startling fashion during a project in India. "I worked in New Delhi with an operator that had huge fraud problems," Löfven said. "Very early I found that they were not really eager to *fix* the problems. After having been there some time I got closer to the fraud manager. One day he said 'Ulf, if I fix this problem too well, then the mafia will come in here, point a gun to my head and tell me not to be *too* efficient.'"

Löfven advises "Get very familiar with the local environment and the habits. This does not of course mean to just give in to these threats; but it is vital to really understand what risks you're dealing with."

One way of gaining such familiarity with the local culture is to hire a local staff; but Löfven suggests against doing this too soon. "If possible, I would not hire local staff initially," he said. "To do that in a proper way takes a long time, especially in a country where you don´t have the natural connections or network to the right people."

Xu is more encouraging. "Having businesses in China, we are talking about a market that has a totally different cultural background, compared to North America," he said. "I always suggest these companies to have a localized team first." Xu added that the cost of IT staff in China is much less expensive than it is in North America, so "why not?" (Google, it is rumored, suspects that some of its Chinese employees may have colluded in the December attacks. More on this below.)

Any of these legal or cultural considerations could have significant impacts on the fundamental decisions you make about your security architecture: how you partition data assets, how you monitor activity, whether or not you set up separate data centers within the physical borders of the country, what kind of local staff you'll need, how you configure identity and access management tools, and much, much more.

As for Google China, the search engine adheres to the country's Internet censorship policies, which require that search results be filtered so as not to include any content that the Chinese government has deemed to be harmful to the People's Republic of China. Falling under this description are content regarding the Falun Gong movement, content regarding the Tiananmen Square protests of 1989, and content that support the independence movements of Tibet and Taiwan.

Google similarly edits search results to comply with other nation's laws. For example, in accordance with local laws, Google's changed their German and French search engines to remove references to some sites that contain hate speech or deny that the Holocaust ever occurred. In accordance with the United States Digital Millenium Copyright Act, Google has removed references to some sites containing content that criticized the Church of Scientology and used some of the Church's proprietary content without authorization.

Google had opted to do as the Romans do, and it seemed the company was committed to doing business in China, on Chinese terms…until Jan. 12.

When the Romans attack

Jan. 12 Google's Senior Vice President of Corporate Development and Chief Legal Officer David Drummond posted a blog entry titled "A New Approach to China." I recommend reading the full post at http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

Wrote Drummond: "In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google."

Drummond did not share details about the type of Google intellectual property that was stolen; he focused instead on the type of information the attackers were trying to obtain from Google users. He wrote:

> Second, we have evidence to suggest that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists. Based on our investigation to date we believe their attack did not achieve that objective. Only two Gmail accounts appear to have been accessed, and that activity was limited to account information (such as the date the account was created) and subject line, rather than the content of emails themselves.
>
> Third, as part of this investigation but independent of the attack on Google, we have discovered that the accounts of dozens of U.S.-, China- and Europe-based Gmail users who are advocates of human rights in China appear to have been routinely accessed by third parties. These accounts have not been accessed through any security breach at Google, but most likely via phishing scams or malware placed on the users' computers.

Drummond went on to say:

> These attacks and the surveillance they have uncovered—combined with the attempts over the past year to further limit free speech on the web—have led us to conclude that we should review the feasibility of our business operations in China. We have decided we are no longer willing to continue censoring our results on Google.cn, and so over the next few weeks we will be discussing with the Chinese government the basis on which we could operate an unfiltered search engine within the law, if at all. We recognize that this may well mean having to shut down Google.cn, and potentially our offices in China.

Google did briefly cease censoring search results on Google.cn, but later began censoring again, and are reportedly undergoing conversations with the Chinese government to discuss the possibility of legally running an unfiltered search engine of some ilk.

Drummond's post sparked a great deal of political discussion and a great deal of security research.

Security researchers counted that, in addition to Google, at least 33 other large companies were similarly attacked (and their intellectual property compromised), as part of a large operation dubbed "Operation Aurora" by security firm McAfee.

The Aurora attackers compromised clients by way of drive-by downloads of a modified version of the Hydraq Trojan that exploited an HTML object memory corruption vulnerability in Microsoft's Internet Explorer 6 Web browser. The compromised clients then communicated with command-and-control centers in Taiwan and the United States; these C&Cs have not been operational since Jan. 4.

Microsoft, it turns out, had known of the Internet Explorer vulnerability since Aug. 26, when it was reported by Meron Sellem of Israeli firm BugSec (CVE 2010-0249). Microsoft was planning to release a patch as part of the regular patch cycle in February, but instead issued the patch Jan. 21 as an emergency security update for all versions of Internet Explorer. (Before the patch was made available, officials in Germany, Australia and France cautioned citizens against using Internet Explorer, and downloads of competing browsers, Opera and Firefox, increased in those countries.)

Although Drummond did not exclusively come out and blame the Chinese government for the attacks, the implication was present in his words.

Others, however, speculated whether or not the evidence was strong enough to prove that the attack derived from Chinese sources at all, much less the government itself.

(Are you sure they were the Romans?)

Criminal hackers (like the Operation Aurora team) use an assortment of methods to obfuscate the true source of an attack—a fact of which forensics experts and law enforcement officials are all too aware. In place of inarguably damning forensic evidence, the most powerful factors pointing to China are a) the type of information the attackers were looking for—human rights activists and international journalists covering the China beat—and b) the type of information the attackers must have had in order to successfully carry out the attacks.

In a Jan. 18 report, Reuters referenced two anonymous sources that hinted that insiders at Google China might have participated in Operation Aurora:

> The sources, who are familiar with the situation, told Reuters that the attack, which targeted people who have access to specific parts of Google networks, may have been facilitated by people working in Google China's office.… The sophistication in the attack was in knowing whom to attack, not the malware itself, the analysts said. Local media, citing unnamed sources, reported that some Google China employees were denied access to internal networks after January 13, while some staff were put on leave and others transferred to different offices in Google's Asia Pacific operations. Google said it would not comment on its business operations.

Jan. 20, Joe Stewart, director of malware research with SecureWorks, provided another piece of evidence that he argued supported the theory that the Operation Aurora attacks were carried out by hackers in China. In a blog piece titled "Operation Aurora: Clues in the Code," Stewart explained that the modified Hydraq Trojan used in the Aurora attacks used an unusual cyclic redundancy check algorithm that Stewart believed to be "virtually unknown outside of China." "In my opinion," Stewart wrote, "the use of the unique CRC implementation in Hydraq is evidence that someone from with the [People's Republic of China] authored the Aurora codebase." (Read the full piece at http://www.secureworks.com/research/blog/index.php/2010/01/20/operation-aurora-clues-in-the-code/.)

However, this theory was later refuted in a Jan. 26 report in U.K.-based technology news site, The Register. According to The Register, the algorithm had actually "circulated for years on English language books and websites, casting doubt on claims it provided strong evidence that the malware was written by someone inside the People's Republic of China…In fact, the implementation is common among English-speaking programmers of microcontrollers and other devices where memory is limited." (Read this in full at: http://www.theregister.co.uk/2010/01/26/aurora_attack_origins.)

One last tenuous tie to China: according to documents obtained by the Christian Science Monitor, at least three U.S. oil companies—Marathon Oil, ConocoPhillips and ExxonMobil—were hit by very similar, "Aurora-style" attacks in 2008, and some of the breached information was apparently sent to computers in China.

''Any accusation that the Chinese government participated in cyberattacks, either in an explicit or indirect way, is groundless and aims to discredit China,'' an unidentified ministry spokesman said,

Leave Rome?

Regardless of whether or not the Aurora attacks were committed with the approval of the Chinese government, the possibilility of Google leaving the Chinese market stirred up passions.

For threatening to back out of the China market, Google was ardently praised by human rights advocacy organizations, including Amnesty International and the Electronic Frontier Foundation. Yahoo! also came out praising Google's actions, but Yahoo's Chinese partner, the Alibaba Group, quickly followed up by calling Yahoo's comments reckless, stating: "Alibaba Group has communicated to Yahoo! that Yahoo's statement that it is 'aligned' with the position Google took last week was reckless, given the lack of facts in evidence."

U.S. Secretary of State Hillary Clinton alluded to the Google situation during a Jan. 21 speech about Internet freedom she delivered at the Newseum in Washington, D.C. In her speech, Clinton compared Internet censorship to the Iron Curtain that was symbolically demolished with The Berlin Wall. From her speech:

> The new iconic infrastructure of our age is the Internet. Instead of division it stands for connection, but even as networks spread to nations around the globe, virtual walls are cropping up in place of visible walls. Some countries have erected electronic barriers that prevent their people from accessing portions of the world's networks. They've expunged words, names and phrases from search engine results. They have violated the privacy of citizens who engage in non-violent political speech. These actions contravene the Universal Declaration of Human Rights [proclaimed and adopted by the General Assembly of the United Nations in 1948], which tells us that all people have the right to seek, receive and impart information and ideas through any media and regardless of frontiers. With the spread of these restrictive practices, a new Information Curtain is descending across much of the world.

(Watch the full speech on the U.S. Department of State's YouTube page, at http://www.youtube.com/watch?v=ccGzOJHE1rw.)

The Chinese newspaper the *Global Times* responded to Clinton's speech in an editorial Jan. 22, writing: "The U.S. campaign for uncensored and free flow of information on an unrestricted Internet is a disguised attempt to impose its values on other cultures in the name of democracy."

Some have argued that Google is using the global debate about freedom of speech as a way to gussy up an otherwise plain economic decision to abandon a market they've failed to dominate. Google is *not* the leading search engine company in China—that position is held by Chinese search engine company Baidu, which claims about 60 percent of China's Internet searches. Nonetheless, it's no small thing being number two in the country that is home to a rapidly growing population of Internet users that is already bigger than any other nation's worldwide. According to figures released Jan. 15 by the China Internet Network Information Center (CINIC), 384 million Chinese people use the Internet; this number is nearly 30 percent larger than CINIC's count of 298 million last year. Further, market leading search engine Baidu may be experiencing a bit of a rough patch. Two of Baidu's senior officials—chief technology officer Yinan Li and chief operating officer Peng Ye—announced their resignations (both citing "personal reasons") this January; shares of Baidu Inc. fell 6.5 percent after Li's resignation. Whatever Google's reasons, if the company walks out on a market with so much potential, it will be a major business decision.

Maybe you just shouldn't go to Rome in the first place

If Google leaves China, will it be a moral decision? Will it be a business decision? Does it matter?

"First of all, I don't believe Google's plan of quitting the China market is mainly because of the individuals' privacy protection issue," said Xu. "It could be *one of* the reasons, but not the main reason. Second, international expansion should start by first learning local law. A company can decide to comply with the local law or give up the local business. It is the company's call. But a company is not the right party to judge whether the local law is reasonable or not."

Or is it?

On one hand, a wildly successful international corporation is probably better-equipped to fight the powers that be than a typical grassroots organization of malcontented citizens. On the other hand, is it ethically defensible for an American company to willfully defy the laws of another country in which it does business, on the basis that freedom of speech is a basic human right? After all, although the authors of the United States Declaration of Independence wrote "We hold

these truths to be self-evident" before declaring that liberty is one of the unalienable rights of all men, and "that to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed," the rest of the world may not necessarily find those truths to be self-evident. "Human rights" and "democracy" are not necessarily one and the same.

An information security director may not necessarily be in a position to decide whether or not their organization will or will not enter business in a new country. Nonetheless, it is important for the security team to be prepared for international expansion; both professionally and philosophically. If possible find out what new regions your company is considering expanding into, do your homework on the local privacy-security culture, and ask yourself: Where do I stand? —*Sara Peters*

Modified System-High Approach For Resolving Incompatible Legal and Regulatory Requirements

by Charles Cresson Wood, CISSP, CISA, CISM

Policy: In July of each year, the Information Security Department must submit to the Chief Legal Counsel a summary of all laws and regulations to which Company X is then required to comply. This summary must include all functional requirements dictated by these laws and regulations, as applied within the context of Company X operations. Within 12 months from the date this summary is approved by the Chief Legal Counsel, all of these functional requirements must be reflected in the Company X Corporate Information Security Architecture and relevant implementation projects.

Rationalizing requirements

For many years, government regulators encouraged businesses and non-profits to be self-regulating. The notion was that these entities knew best how to secure their information, and that the market would discipline those who were remiss in this area. The sheer volume of serious information security breaches and violations now being publicly reported makes it clear that this *laissez-faire* approach has failed, and failed badly. In a catch-up effort to encourage management to adequately address information security matters, regulators at many levels of government are now issuing a variety of laws and regulations. This recent rush to regulate has meant that many organizations must now respond to different, and in many cases divergent, requirements. This is especially the case with those organizations that do business over the Internet, which are, by their very nature, operating in many jurisdictions.

This new reality is confirmed by a brief examination of the laws and regulations related to the public reporting for security breaches. The relevant laws differ not just between countries, but also between states within a country. For example, Massachusetts' Data Security Breach Notification Law is one of 46 such laws in the United States. It requires that an individual, a business, or a government agency with "personal information" related to a state resident, must provide notice to that state resident in the event of a suspected or confirmed data security breach. Most states that have such laws provide an exemption for encrypted data. In other words, if the stolen or exposed personal data is encrypted, then there is no reporting obligation. Some states define encryption as a process that transforms data into an unreadable or unusable form. But the Massachusetts law gets more specific, requiring a 128-bit encryption process for all personal data in transit or in storage. Other states, such as Colorado, grant exemptions to those organizations that are regulated by federal statute, such as those organizations subject to the requirements of the Gramm-Leach-Bliley (GLB) Act.

In light of these and many other potentially conflicting requirements, today's information security professional is left with two difficult tasks: (1) how to determine which of the requirements apply to his or her organization, and (2) how to resolve conflicts between multiple requirements so as to define a unified minimum set of information security requirements. Although this article will focus on laws and regulations, the same approach is applicable to, and should be used with, other information security requirements, such as those appearing in a business partner agreement.

Fluid nature

Information is like water, traveling around and showing up in places you may not expect it to (such as your cellar), and sometimes taking forms that you had not anticipated (such as frozen dew on your steep driveway). Information travels through informal networks, such as gossip channels and Internet-based criminal gangs engaged in intellectual property theft. Information morphs from one form to another, such as from a conversation in the elevator to an e-mail message sent to your manager. While good system design seriously considers many of these possibilities—using so-called "fail-safe" or "fail-secure" design—in reality, there is no way to comprehensively plan for all of these contingencies.

This discouraging fact means that information security practitioners will probably not be able to keep sensitive, valuable, or critical information within certain walls, such as a subnet on an internal network. This fact also means that it is expeditious to consistently protect all information on an internal network, no matter what the classification of that information may be. For example, if there is a possibility that so-called personal information may travel over the network, then

all traffic can be encrypted. This is conceptually simple, and often simple to implement. This approach, where the most stringent requirement applies to everything, is called the "system-high" approach.

Using an unmodified system-high approach has some other benefits, such as the provision of a unified approach, which makes outsourcing easier. This approach also makes the system integration associated with mergers and acquisitions easier to achieve. Another significant benefit associated with the unmodified system-high approach is the ability to expeditiously acquire information security products and services (every system can be configured and equipped the same way).

Still another benefit is the clarity that goes along with sharing data between departments or other units within the organization. To the extent that security requirements do not change from department to department, to that extent can the interdepartmental sharing of sensitive, valuable, or critical data proceed with neither obstruction or delay.

Perhaps going too far

Unfortunately, the system-high approach is often going to compromise system performance, operating cost, or some other important management objective. For example, if all network traffic is encrypted, response time performance may be notably degraded. The way to strike a workable compromise in many situations is a combination of both approaches, herein referred to as the "modified system-high approach." This combined approach involves defining policies where the requirements specified in certain laws and/or regulations apply only to a certain zone on an internal network, a certain department, a specific system technology, or some other specific situation. In other words, the most stringent of the requirements is selected, but it is applied only to those situations where it is required.

As an example of the modified systems-high approach, consider the case of a health maintenance organization (HMO), which employs clerical personnel who process electronic health insurance claims. The internal database used to store this information could use enterprise rights management (ERM) technology, such that all copies of the database are always stored and transmitted in encrypted format. The computers physically situated in the insurance department could all have active copies of the ERM software, which would allow workers in that department to access the database for normal business activities. Copies of the database that are stored on backup tapes would be unreadable to computers outside the department because the database is stored in encrypted format. Thus if a less than scrupulous worker were to save

the database onto a CD-ROM or a flash memory stick, the worker could not successfully sell the database to a gang involved in identity theft.

Thus a policy could specify that the insurance claim database can be updated only within the confines of the ERM system. Additional controls will be necessary to prevent the personal health information contained in the database from finding its way onto other systems. For example, a content filtering system could be used to block the movement of this information out onto the Internet. The system-high component of this approach is that all insurance claim processing is done in the ERM-assisted database, and all of the personal health information involved is thereby encrypted. The "modified" aspect of this approach is that it pertains only to the insurance department, not to the whole organization.

In a more general sense, if a cost-effective technology, process, or some other approach exists that allows a control to be applied within a certain zone, then the application of the control can be limited to that zone only. But if no such cost-effective technology, process, or other approach exists, or no such approach is known, then the system-high strategy must prevail. The result of this decision-making process should then be captured on a spreadsheet, or in larger and more complex environments, in a dedicated database. Illustrating the fact that this whole requirements management process can get terribly complex, the marketplace now offers a handful of requirements definition and requirements compliance software products. One notable example is the GRC SmartSuite Framework provided by Archer Technologies.

Action-forcing mechanism

The policy in the box stipulates that this requirement evaluation, definition and consolidation work be done annually. As with all policy-writing efforts, it is desirable to establish an action-forcing mechanism, a process that forces this important work to be consistently done. This action-forcing mechanism may, for example, be accomplished by establishing a dependency on a desirable result.

For example, if the information security budget for the following year could not be submitted to top management, without first obtaining the approval of the Chief Legal Counsel, then such a dependency could be established. Since the Chief Legal Counsel needs the above-mentioned analysis of information security requirements, before he or she can approve the proposed information security budget, it is fair to assume that this list of current information security requirements will be diligently prepared each year.

Of course this annual requirements analysis should also have an interface with a risk manage-

ment process. Thus the results of a risk assessment, as well as the results from recent compliance audits, should all be considered when drafting the set of information security requirements to which an organization must comply. An annual process, as defined above, is called for because this list of requirements is fixed, but both information security vulnerabilities and true needs are rapidly changing.

Charles Cresson Wood, CISSP, CISA, CISM, is an independent technology risk management consultant based in Mendocino, Calif. The 10th edition of his book titled Information Security Policies Made Easy *contains 1350+ already-written information security policies in both CD-ROM and hardcopy book format (www.informationshield.com). His latest book is* Kicking The Gasoline and Petro-Diesel Habit: A Business Manager's Blueprint For Action *(www.kickingthegasoline.com). He can be reached at ccwood@ix.netcom.com. He has no marketing or promotional relationship with any of the named vendors.*

International Enterprise Considerations for Free and Open Source Software

by Ralph Hughes, CISSP, CSSLP, PMP

Thirty years ago if you gave up any of your personal information to a business, most likely it was neatly typed on high-quality paper and filed away somewhere in a fifth-floor document library never to be heard from again. Do the same thing today and odds are that the same data is typed into a Web form and stored who knows where in who knows what format. There may be two or three live copies, not to mention hundreds more on unencrypted backup media stored at some third-party location. While in-transit, that data may have crossed two or three continents and who knows how many international boundaries.

Pretty cool, huh! Providing security for a global enterprise is a tall order, but as organizations depend less on brick-and-mortar buildings and more on the high bandwidth communications to do business, they also must address the risks. Besides, if you have a company with a Web site, you're global whether you want to be or not. "Global risk mitigation!" you say. "Wow, that must be expensive and hard to do!" you say. Well sure. But it's not impossible, and it must be calculated into the budget. A robust information assurance and security suite can be built by identifying a mix of open-source and commercial products that will play well together; or at least not interfere with one another.

At this point I might run an analysis of which open-source tools might best be used to help secure enterprise operations as they go global. I'm not going to do that here. I started trying to break down all the different operations that would be affected and basically gave up when the list got too long. I think that may be better addressed in a series of topics a bit later. Rather than look at any individual package or tool, I decided to try and address the subject of why some organizations choose to employ free and open-source software (FOSS) and why some do not.

The two common complaints with open-source software are lack of support and concerns with the security (or rather the insecurity of the tools). Is one view right and the other wrong? Probably not. Companies don't (or shouldn't) make decisions at random. Decisions are based on a company's policies and their own capabilities. An organization with a well-established IT department and their own internal support capabilities, for example, probably could not care less whether or

not some Tier 1 help desk was one phone call away. However, they might be concerned with whether or not they could trust company confidential data to a piece of software of unknown or untrustworthy origin.

Supporting FOSS

"There's no such thing as a free lunch." That's a typical cliché, but it's very applicable to the world of open-source software. By far the reason most businesses give for selecting an open-source solution is the fact that it is basically free. Even when there is some support fee involved, it is almost always several orders of magnitude cheaper than the competing commercial product.

Is it really cheaper? If we're looking only at the license fee, definitely; but one thing companies that use open-source software have in common is a built-in technical ability to evaluate, select, deploy, and maintain IT solutions on their own. Maybe they contract our their IT support or maybe they do it in-house, but they are capable of do-it-yourself IT. I would wager that if the sunk cost of in-house IT is taken into account, the cost would be almost the same.

"If the cost is the same, why would anyone choose FOSS over closed source," you might ask. The key adjective in the equation is "sunk." If a company has an established IT department that is already part of the operating budget, then adding one more piece of software for them to support is a no-brainer. That is especially true for FOSS tools that are well-maintained and have an established user community.

However, while the tool's user community may be lively in one country, it may be non-existent in another. So, when considering open-source security tools for your international organization, make certain that there are local user communities—or at least communities that communicate in the local language—to help support the IT staff in all your organization's international offices.

Availability of support, or the lack thereof, is the primary reason given by commercial organizations for their decision to avoid open-source solutions.

A matter of trust

Another prime reason that organizations avoid FOSS is the lack of trust. Open-source development efforts often receive input and support from many different locations all over the world. This leads to a measure of risk that is unacceptable for some organizations. So the question arises, "Are open-source tools all bug-ridden applications built by would-be thieves or worse?" Of course not. Besides, there are plenty of commercial applications that are bug-ridden and written by thieves.

That doesn't stop them from being used by organizations all over the world. In reference to a new software package, I have actually heard the question asked, "It this an open-source application, or is it tested and vetted," as if the two are mutually exclusive. Going through the accreditation process for a FOSS tool is probably no more tedious than it is for a commercial application; maybe even less so. At least with the FOSS tool you have access to the source code. With commercial software you rely solely on the integrity of the vendor.

It's no surprise that among government and defense organizations trust or security concerns are the primary reasons for their decision to avoid open-source solutions or components. International corporations, on the other hand, could conceivably experience business or public relations benefits from the internationally transparent nature of open-source software communities. Going open source is one surefire way of avoiding entanglements with Microsoft, Google and other enormous American software companies that sometimes find themselves in uncomfortable anti-trust conversations abroad.

So what's the answer?

Is there a place for FOSS components in the enterprise? Of course! In all likelihood even organizations that officially disallow the use of open-source software are actually using it in some form without even knowing it. A few well-known examples are in order:

- ❏ The Mozilla Firefox Web browser is released under an open-source license and is currently the only serious competitor to Internet Explorer.
- ❏ Apache Web server, the most popular Web server in existence, is open source.
- ❏ The Eclipse development environment is a widely used, open-source, extensible IDE for Web development.

The key to successfully deploying FOSS tools in any organization is to pick your battles. Regardless of the type of organization, you most likely would never be able to replace all your commercial software packages with open-source equivalents. However, you may find that it is entirely within the realm of possibility to incorporate public license tools into certain aspects of the enterprise. Consider these basic rules:

- ❏ Define your requirements. Know what problem you need to solve.
- ❏ Define your evaluation criteria ahead of time. Do not make it up as you go. You will have a much better chance at a fair comparison this way.

- ❏ Take both FOSS and commercial criteria into consideration. Do not assume that if you put open-source tools up against commercial packages that the commercial tools will always win. Some of them are really lousy.
- ❏ If cost is a factor, don't assume that a FOSS package will always win out because it's free. If you have well-defined evaluation criteria, the software has to do something other than sit there and look cheap.
- ❏ Do not be tempted to incorporate a FOSS package for the "cool" factor. Like everything else, there needs to be a solid business reason for selecting a tools, whether it's free or not. If you want to play with cool toys, save it for your home lab.
- ❏ Search for known vulnerabilities in all the candidate tools—FOSS and commercial. The search capabilities of the National Vulnerability Database (http://nvd.nist.gov) and SecurityFocus (http://www.securityfocus.com) are very helpful here.
- ❏ Finally, and especially if open source is a new thing for your company, get support from your management. Create a plan and clue them in. They say it is always easier to get forgiveness than permission, but getting permission is easier than finding a new job.

Open-source tools and packages do have a place in the enterprise. Odds are that some are already being used, even if the "official" line is that they are prohibited by one policy or another. Deploying FOSS components in a large enterprise will take some work. I would encourage anyone serious about this to take it as an opportunity to build a new capability within the organization. If your company has a trust issue with open-source tools, it provides the occasion to establish better internal certification and accreditation practices across the board. Likewise, if the problem is support, use FOSS as a case to broaden the capabilities of your technical team.

Ralph Hughes has worked in the information technology field for nearly 20 years, specializing in the engineering, development and deployment of business systems for the Department of Defense. His background and experience includes secure system design, development, configuration management and continuity planning for a wide range of systems.

COMPUTER SECURITY ALERT

DIRECTOR ROBERT RICHARDSON
robert.richardson@ubm.com 610-604-4604 twitter.com/cryptorobert

SENIOR EDITOR SARA PETERS
sara.peters@ubm.com 212-600-3066 twitter.com/sarapeters

MEMBERSHIP MARKETING SPECIALIST CAROL LUONG
carol.luong@ubm.com 212-600-3356

Sr. Conference Manager Dina Nicovic
dinamarie.nicovic@ubm.com 212-600-3179

Awareness and Training Pam Salaway
pam.salaway@ubm.com 631-878-2205

Sales Manager Nadine Schwartz
nadine.schwartz@ubm.com 212-600-3363

Event Specialist Rosilia Montalvo
rosilia.montalvo@ubm.com 212-600-3018

For address changes or membership questions, visit www.GoCSI.com/membership, call 212-600-3026 or e-mail csi@ubm.com.

Facebook **LinkedIn** **Twitter**

www.GOCSI.com