

Meet CFUS



Joseph C. (Joe) Hibbitt
Principal, President
Los Angeles, California



Manny Mangahas
Principal, VP—East Coast Operations
Clifton, Virginia (Washington DC)



Burnie Reed
Principal, VP—Midwest Operations
Dallas, Texas

CFUS Update!

Industry: Automotive

Provided database architecture support for a multinational project. Drafted business requirements. Translated to functional and technical specifications. Implemented into the database architecture.

Technology : Oracle

Industry: Entertainment

Determined end user service level agreements and implemented within an operations and maintenance contract.

Technology: Custom Oracle CRM

Teleworkers Feel Safe, Threaten Network Security

Business employees working remotely say they believe the Internet is getting safer. But they're actually one of the reasons it's so unsafe, according to a new study.

The study, conducted by researcher Insight Express and sponsored by Cisco, polled 2,000 remote access workers in 10 countries. Most of the respondents (56 percent) said they felt the Internet was safe in 2007, as opposed to 48 percent in 2006.

Ironically, as was the case in [the earlier 2006 study](#), the results found a wide gap between teleworkers' perceptions about security and the reality.

Worse, they themselves are evidently contributing to the problem, thanks to unsafe activities.

The study found that remote workers regularly engage in risky behavior -- opening e-mails from unknown sources, using corporate PCs for personal activities and "hijacking" their neighbors' Wi-Fi connections.

Forty-four percent of global respondents in 2007 said they felt it was acceptable to use their employer's PC for personal activities, down slightly from 45 percent in 2006.

The U.S. trended in the opposite direction, however. Forty percent in 2007 admitted to misusing an employer-owned PC for their own purposes -- a sizable increase from the 29 percent reported in 2006.

More specifically, 43 percent of respondents worldwide admitted to doing personal Internet shopping on their corporate PC, a small increase from 39 percent the previous year.

In the U.S., that figure is again far larger. Respondents admitting to shopping online with their employer's PC rose to 62 percent in 2007, up from 46 percent the year before.

Other unsafe behavior included allowing non-employees to share an employer-owned PC. On a global basis, 21 percent of respondents admitted to the practice -- up from 20 percent in 2006. Additionally, 12 percent

worldwide said they helped themselves to a neighbor's Wi-Fi connection, a 1 percent increase from the previous year.

The study also examined respondents' motivation for engaging in behavior that potentially undermined the security of their PC and corporate network.

Twenty percent of the study's respondents reported using their corporate PC for personal online shopping because of a lack of time -- they'd never complete personal chores if they didn't do them while "at work."

Respondents also had an answer for why they shared their employer-owned PC with friends and family: 32 percent of those polled said they simply didn't see anything wrong with the practice.

When it came to reasons why they "borrowed" their neighbor's wireless Internet connectivity, some 22 percent of respondents claimed they couldn't tell whether they were using someone else's Wi-Fi or their own.

With so many users engaging in risky activities, it seems odd that believe security is actually improving. What's behind such a disparity?

Patrick Gray, senior security strategist at Cisco, sees a decreasing sense among remote workers, ensuring that they fail to remain diligent.

"We haven't seen major worms in a few years -- things have changed with the bad guys going underground using more stealthy methods," Gray told *InternetNews.com*. "With this reduction of gross attacks, we have a false sense of security among the user population."

The recent Storm worm has not proven a wake-up call because it's not of the same category as the Zotob, Blaster and Sasser worms of the past, Gray said. Those worms

were harmful in that they shut down computers, so infection proved impossible to overlook.

"Storm is insidious in the fact that people don't know they are being compromised," he added.

Users also fail to understand the security implications of some of their behaviors, Gray said. For instance, remote workers may not know there are risks in just visiting a Web site, so they might not think much of using an employer's PC for shopping or other personal activities.

In some cases, teleworkers will disconnect from their corporate VPN to shop online, then reconnecting afterward, Gray said. However, doing so could mean the user brings malware with them once they reconnect, endangering the corporate network.

Workers may not be wholly at fault for failing to understand how their actions could threaten network security. Instead, their companies' IT administrators could bear some responsibility because they haven't done an adequate job explaining the problem, according to John Stewart, Cisco's chief security officer.

In a Webcast discussing the study's findings, Stewart said IT professionals industry-wide still have a long way to go in explaining to employees why they should take caution in their activities, whether at home or in the office.

"We still haven't done enough," Stewart said. "The whole concept of 'work versus home' is completely disappearing in front of our eyes. We've got to remember we're crossing the chasms of 'work versus play' and they're becoming the same thing."

Is Apple's iPhone 2.0 Good Enough For Enterprises?

A developer of enterprise mobility software has expressed doubts that Apple's iPhone can cut it in the enterprise due to a number of issues, all of which Apple can change, but in doing so are anathema to how the company operates.

Ahmed Dattoo, vice president of marketing of Zenprise, a developer of software for enterprise [BlackBerry](#) users, said he would welcome the opportunity to support the iPhone in the enterprise but has his doubts it will make much headway.

"The question that needs to be asked is, is the 2.0 software going to be good enough to take on RIM at the enterprise level?" he told *InternetNews.com*. "It doesn't look it. Is it good enough to get at the small and medium-sized business market? Probably. They have different requirements."

Apple (NASDAQ:AAPL) did not return calls seeking comment for this story. The company had its big enterprise roadmap event

last week where it [unveiled details](#) of its software development kit (SDK) and support for Microsoft's Exchange Server. CRM and SaaS provider Salesforce.com announced support for the iPhone and two large corporate customers, biotech giant Genentech and Nike, said they already had iPhone deployments underway.

"The iPhone is a watershed event in mobile computing for corporations," said Todd Pierce, vice president, of corporate IT at Genentech, in a statement. "Genentech's pilot with iPhone has shown its potential to be the most useful business mobility tool we've ever used. We now have 3,000 planned for deployment based on how easy and simple it was to integrate iPhone with our corporate email system."

IDC analyst Sean Ryan, said Apple's support of Exchange was important to get the iPhone consideration among enterprise buyers, but nothing special. He notes that Nokia, Palm, Symbian, HTC and other mobile players

already support Exchange and its ActiveSync technology for connecting to corporate email systems.

"In the mobile enterprise it's not just about the device, but about the platform and the support system," said Ryan. "The iPhone has a lot of cachet, but there are many challenges to wide corporate adoption. It's a premium-priced device with limited device management." With Exchange, IT can shut down an iPhone that's lost or stolen, but other mobile devices have more extensive management capabilities.

Ryan also said the market for enterprises devices like smart phones is still at a very early stage and the iPhone is very new. "Apple has an opportunity but RIM, Nokia, Microsoft and others aren't going to sit still."

Dattoo of Zenprise laid out four distinct areas he thinks Apple must overcome to make the iPhone a true success in the enterprise. The problems range from technical to perceptual.

The first is that Apple is viewed as a consumer product, and firms that play in both spaces, consumer and enterprise, use separate brands. "It's rare to see a company pulling off operating in the enterprise space and consumer space with the same product," said Datoo.

The second is support. Apple is a relatively small company with modest support infrastructure. Where would an enterprise customer go for help, AT&T or Apple? Over the years, RIM built out a significant support

structure, which Apple will need. "To be a mainstay in the enterprise, you need a support model conducive to an enterprise model," said Datoo.

The third problem is security. The iPhone's internals are not documented or exposed. Datoo said it's not even possible to get at basic internals, like the battery levels or signal strength meters. Many features, like Bluetooth and the camera, can't be locked down. Also, the iPhone is managed through iTunes, which many enterprises have banned

from their computers. None of this, he said, will sit well with enterprise customers.

Finally, there is support. Datoo cited a Gartner study that put total cost of ownership for a mobile phone at between \$1,300 and \$2,600, with about 50 percent of that cost going to IT and user administration. iPhone has no remote administration features, no visibility into the device, which means a lot more time would be needed to be spent diagnosing problems.

Target Heart Rate Zone Training

Target Heart Rate Training is a systematic method of improving your cardiovascular fitness. The body's organs and muscles change in response to the demands placed on it. By exercising at sufficiently intense levels, you can overload your cardiovascular system. During rest, your body adapts to strengthen the cardiovascular system. Over time, your heart becomes more efficient at delivering the oxygen and fuel required by the muscles to maintain this higher level of performance. The skeletal muscles also become better at extracting oxygen from the bloodstream. With continued consistent exercise, the cardiovascular system continues to consistently improve.

How do you know how hard you are working out? Physiologists have discovered that the rate of oxygen used by the muscles during exercise is the best measure of aerobic work. An individual runs on a treadmill while the heart rate and the volume of inhaled and exhaled air are sampled and measured. The difference between the volume of oxygen inhaled and exhaled during the test is what the muscles used to burn fuel (mostly carbohydrates and fat). The rate of this oxygen consumption, in liters per minute, is called VO₂. The test is performed at progressively more difficult levels until the individual reaches his or her maximum capability. This maximum rate of oxygen consumption is called the VO₂(max).

The VO₂ method is the most accurate way

to determine exercise intensity. However, it is not without some serious drawbacks. It requires expensive equipment, trained personnel, and specialized facilities... These tests are expensive. Another drawback is that you can't take this specialized and bulky equipment with you when you work out. (This stuff ain't portable.)

This brings us to the second best way to measure exercise intensity - your heart rate during exertion. The heart rate is much easier to measure than VO₂ but it is a very good approximation of VO₂. It has been observed that the relationship between the percentage of VO₂(max) and the percentage of maximum heart rate is very predictable. Studies consistently show the 55% VO₂ (max) corresponds to approximately 70% maximum heart rate for most individuals. This means that if you know your maximum heart rate (the fastest your heart rate is capable of pumping), you'd have a convenient method of monitoring your workouts.

To accurately determine your maximum heart rate, there are specialized facilities with bulky and expensive equipment that require trained personnel available to you for a price. You can determine your maximum heart rate by undergoing an exercise stress test. If you choose this route, it is important that you undergo a physical examination prior to the test, especially if you are over 35. Many trainers have also developed tests that you can perform to estimate your maximum heart

rate. For instance, one test could involve having you step up and down on a stool at a certain rate for pre-determined durations while the trainer monitors your heart rate.

Knowing your maximum heart rate will allow you to estimate where you can train to bring about cardiovascular improvements. But since a stress test isn't practical for most individuals, physiologists have developed a number of formulas for estimating maximum heart rate without actually requiring you to take your heart rate up to potentially dangerous levels. The maximum heart rate formulas provide an approximation of your true maximum heart rate. But by estimating conservatively, you can use these estimates as the foundation for monitoring your exercise intensities.

Once you've determined your estimated maximum heart rate, you can construct a "target zone" for your workouts. Normally, trainers specify "zones" for you to work in. This is because the human heart rate changes continuously. It would be virtually impossible to maintain any selected heart rate. In addition, it takes a while for the heart to "come up to speed." For these reasons, a "target heart rate zone" has evolved to become the most practical method of measuring exercise intensity.

Target heart rate zones are expressed as a percentage range based on your maximum heart rate. Your trainer (or your software) will convert these percentages into a target heart rate ranges specific to you. For instance, your goal may be to maintain your heart rate of between 124 and 144 bpm (beats per minute). For tracking purposes, you would most often only track the duration of your exercise in which you were between your minimum and maximum heart rate goals (your duration "in the zone").

Most training schedules incorporate different types of workouts (e.g. long, slow distance, high intensity intervals). You can construct different target zones depending upon the type of workout you are performing. Heart rate monitors can help you stay in that zone so that you can achieve your goal

for that workout. Modern heart rate monitors can tell you "duration in zone" - the amount of time you were in your target heart rate zone. Some will even beep when you are above or below your selected training zone. This makes it far more convenient to track your workouts. These heart rate monitors usually have a sensor that mounts around your chest and a computer that mounts in a watch-like case on your wrist.

Target heart rate training lets you track improvement over time. This is indicated by a gradual reduction in your resting heart rate. Another indicator of improvement is that you'll need to perform at higher levels to perform the same exercise at the same heart rate range as before. For instance, you may find that you need to run on a treadmill at say, 4.5 mph to stay in your target heart

range when you first start out. You will find that over time you will have to run at, say, 4.8 mph to get your heart to stay inside your target heart range. Paradoxically, over time, you have to perform at higher levels to exercise the same amount.

Target heart rate training provides a scientific approach to tracking your improving levels of fitness. With a decent heart rate monitor, it becomes easier to monitor your workouts. It allows you to measure exercise intensity independently of what activity is being performed by focussing on heart rate as the measure of exercise intensity. If you haven't been making the kind of progress you know you are capable of, you might consider this methodical approach to improving fitness.

Contact CFUS (corporate)

The CFUS Corporation * 4859 West Slauson Ave. Suite 219 * Los Angeles, California 90056
323.298.8502—office * 310.388.5988—fax * info@cfus.com * <http://www.cfus.com>

Story Credits:

<http://www.internetnews.com/infra/article.php/3726216/Teleworkers+Feel+Safe+Threaten+Network+Security.htm>
<http://itmanagement.earthweb.com/erp/article.php/3733221>
<http://www.nutribase.com/thrt.shtml>