Living With Licenses And Software Control

Gary Audin

As the telephony world moves to a software model, you'll be dealing with new problems—including version control and the proliferation of patches.

The video game Pac Man had the player, through the little round yellow character, devouring the screen items. If you were not fast enough, you lost. I would try again and do better, but I never became proficient.

The same can be said about VOIP software releases, versions and patches. The software comes at you. You install the software for new features and functions, or hoping that you have avoided or fixed a functional or security problem. When you are finished with the software installation, more arrives—especially patches.

You will never be quite sure if you have won or lost the software update game. But if you do not take control of the software installation process, then it will control your time and budget and lead to a lot of user dissatisfaction.

To learn the details of exactly what you face, we sent a detailed software survey out to 12 VOIP/IP-telephony vendors to collect information relating to the impact that software changes would have on the enterprise. Avaya, Nortel, Alcatel-Lucent, Inter-Tel, Aastra Intecom, NEC and Sphere Communications responded. Cisco, Siemens, 3Com, Mitel and ShoreTel did not respond to the survey.

Information was collected from the non-responding vendors' websites to attempt to complete the picture. Although not all respondents answered all questions, enough information was collected to satisfy the goals of the survey.

The survey results were not collected to compare one vendor to another. The survey was concerned with the enterprise issues that surface with all the changes that the enterprise has to confront as software is produced by the VOIP/IP-telephony vendors.

Gary Audin is a communications consultant and trainer (for BCR *VOIP seminars) and has a blog at www.voiploop.com and technical tips at www.searchvoip.target.com. He is a regular speaker at the VoiceCon conferences.*

TDM vs. IP-PBX Software

Software management feels like a plague to some, a career's work to others. You may be remembering the old TDM days when there were few software changes, one or two per year. You could be 2 to 4 years behind in the software upgrades of the TDM system and you were not unique.

In contrast, the VOIP/IPT systems and their endpoints seem to be a moving software target, a target that is changing its form and emphasis over time. All we can predict is there is no end in sight for the VOIP/IPT software upgrades and patching problems.

Distributing software can be overwhelming. While upgrading the server is not so daunting an undertaking, once you add in the updates to the gateways and phones, the task escalates in size. One Windows-based IPT vendor has received as many as 75 operating system vendor patches in one year. IT departments can receive 3,000 to 4,000 patches for all their software-based IT systems in a year.

What Do The Vendors Call It?

For starters, make sure you and the vendor agree on software definitions. I have been confused, and learned that vendors use the terms *release, version* and *patch* differently. Here are some general definitions:

1. Release = A major modification to the existing software; may include feature and function additions and changing the operating system.
2. Version = A minor set of upgrade software. May include new features, functions, fixes, etc.
3. Update = Modification to a release (a less commonly used term).
4. Patch = Usually a problem fix with no new functions; however, one vendor also defines patches for:
—Firmware
—Product improvement
—Interoperability
—Customized product improvement paid by customer
—Diagnostic (to trap a specific event)

Think of the *releases* and *versions* as strategic

Software Control

The total cost of ownership (TCO) for VOIP/IPT becomes hard to predict in a world of software charges, because not all the software element charges and installation costs can easily be predicted. The vendors did not have many suggestions for the enterprise to predict an accurate TCO.

Avaya suggested the following should be included in the TCO analysis:

- Frequency of major or release upgrades and minor or version upgrades (mandatory vs. optional)
- System down time during a major or release upgrade—how long? How many employees affected?
- Can voice calls be preserved during a minor release or version upgrade, to minimize down-time?
- Availability of software tools to remotely install software patches without a technician onsite.
- License cost of a major or release upgrade vs. minor or version upgrade
- Number of servers requiring upgrades.
- Cost of an on-site technician to upgrade/maintain these systems?
- Whether patches require system downtime or not.

Other tips and questions that need to be considered:

- Determine whether the software change is mandatory or optional and for how long (months, a year).
- When is the software no longer supported?
- Can you do a single total change or do you have to enter each piece of software separately, in the proper sequence?
- Have you budgeted the staff hours and system down time?
- Hot fixes can be chained, that is, several can be installed without a reboot.
- Even if no exploit has yet been reported, install the patch within 48 hours.
- Ensure deployed patches:
  - —Are consistent
  - —Have status tracking
  - —Have error logging

The Software Change TCO

The total cost of ownership (TCO) associated with software changes will be higher than most enterprises anticipate. There is always something missed or forgotten. There will be the cost of the software, usually only for the releases. Then comes the time it takes for the enterprise staff to learn about and prepare for the software installation. A channel/reseller will probably be required for the actual installation, and there will be channel/reseller charges even for the installation of "free" software patches. The number of sites and endpoints will increase the overall bill.

Software changes may also require some equipment changes. It is somewhat common that the existing hardware does not contain enough memory for the software. This is expected in the server, but the gateways and IP phones may also be affected. In one case, an enterprise had to purchase the next bigger (in memory) IP phone to implement some new security features.

When there are many endpoints and sites to change, it may be wise for the enterprise to purchase a test server, gateway and at least one of each IP phone deployed. These can be used to test the software changes and ensure that the enterprise has the correct procedures in place for successful software deployment. See the accompanying "Software Change TCO Worksheet" for a listing of the TCO cost elements for one year□

The Software Change TCO Worksheet (for one year)

1. Training cost for staff X number of staff to be trained _____
2. Cost of releases X number of sites or endpoints _____
3. Channel software installation charges per site or endpoint
   - Release installation _____
   - Version or minor release installation X number of versions _____
   - Patch installation X number patches or service packs _____
4. Staff-days of enterprise staff preparation X labor cost per site or endpoint
   - Release installation _____
   - Version or minor release installation X number of versions _____
   - Patch installation X number patches or service packs _____
5. Hardware costs (memory, processor.....) per site or endpoint _____
6. Test site and endpoint hardware and software costs _____

TOTAL ANNUAL COST _____

Make sure your RFP fully defines the term "release"

software changes. Implementation should be reviewed and planned; it is not obvious that either a release or version should be immediately installed. Patches, on the other hand, are tactical fixes and small changes. Patches should not include new functions or features, nor should they affect previously installed and successfully operating software.

Unfortunately, some vendors' regression testing (ensuring the software does not change or turn off existing features and functions) is poor. Releases, versions and patches should be tested, or the enterprise should wait to learn others' experiences installing the new software.

Software Is Licensed

One of the respondents, Sphere Communications, pointed out that there are other issues relating to VOIP/IP-telephony software. For example, expect that the software will be priced and governed by licenses. Sphere suggested that additional areas of software interest to the enterprise are:

- What is the vendor's licensing structure?
- How many major capabilities does an enterprise user get with a single license?
- What are the license combinations (e.g., 6-line phone = ? licenses; 6-line phone + softphone = ? licenses; 6 line phone + softphone + WiFi Phone = ? licenses).
- Are licenses perpetual, annual?
- How does the vendor license users versus ports (gateways, for example)?
- What is the licensing-key mechanism for the software?
- Are there other shared-use features that are licensed?

The point Sphere is making is that the TCO for software will vary from vendor to vendor depending on the vendor's software licensing structure (also see "Software Control."). The software packaging will affect the software procurement, and will influence if and when software upgrades will be implemented. These licensing questions will be addressed in greater detail in an upcoming issue of *BCR*, and in the VoiceCon Fall 2007 conference breakout session called "Pricing and Licensing: Paying How Much for What?" (see www.voicecon.com/sanfrancisco).

The Software Release

A software release is a significant piece of software. All the vendors were asked about their definitions of a release and how many have been offered since January 2005.

Aastra Intecom defines two release types, major and baseline.

- A "Major Release" is the addition of features. This type of release requires a retrofit, which will require a system cold start to implement the new features and table sizes. In Aastra Intecom parlance, this is noted as a full number change: e.g., Pointspan 3 to Pointspan 4.
- A "Baseline Release" is where bug fixes are installed. It does not require a retrofit. An upgrade from Pointspan 3.0 to 3.1 would be a baseline upgrade. This could also contain minor enhancements that do require a cold start.

Avaya defines two release types as well, but the content of releases is different:

- "Major Release" means a major change to the licensed software that introduces significant new features and functionality. A major release is typically denoted by a change in the digit(s) to the left of the first decimal point (e.g., [n].y, where [n] is changed)
- "Minor Release" means a minor change to the licensed software that introduces a limited amount of new features and added functionality. A minor release is typically denoted by a change in the digit(s) to the right of the first decimal point (e.g., n.[y], where [y]is changed).

Inter-Tel has four types of releases that vary in magnitude:

- "Major Releases" referred to by version, (such as v2.0) contain major new features.
- "Minor Releases" (such as v2.1) usually consist of minor features and a roll-up of software corrections recently released in maintenance releases or emergency releases (see next two bullets).
- "Maintenance Releases" consist only of software corrections and feature tweaks that relate to the quality of the product.
- "Emergency Releases" are created for specific customers, to deal with specific issues. These are not charged for, and if the fix is found to be of benefit to other customers, it is added to the next maintenance release.

Alcatel-Lucent defines Major, Minor and Maintenance releases similar to Inter-Tel, but does not have an Emergency release designation. **NEC** has only one type of release. **Nortel** did not make any differentiation among releases.

Given these varying release definitions, it becomes incumbent on the enterprise to fully define the term release in the RFP and subsequent contract for the IP-telephony procurement.

Cisco is a bit unusual. Cisco's Unified Communications Manager (formerly Call Manager) has a release and version series, 4.X, that operates with Windows. The 5.X release and version series operates on a Linux platform. Since it has been Cisco's practice to not support more than two releases, will it drop the 5.X series when it issues a new 6.X series? Or will Cisco have to support the 4.X, 5.X and 6.X releases? I do not think that the 4.X series will be discontinued soon—there are many enterprises that, as policy, do not want Linux systems in their IT environment. No other vendor appears to have this release problem.

Overall, the number of releases was not large. Most vendors have issued two major releases since January 2005, so the enterprise should anticipate a major release about once a year.

The impact of a release, however, can be sig-

nificant (for more, see the sidebar, "Planning, Testing, Deploying"). There is always the chance that part of the release will not work. The enterprise should allocate time and staff to testing the release before implementation. This could take several staff-days before the enterprise is confident in the release. The staff-days may be allocated from the internal IT organization, or this may be a (paid) service from the channel or partner that implements the release.

Another factor is the possibility of interruption of the PBX operation. A major release will have to be carefully scheduled, because the implementation of the release can require that the server be off line during implementation, which of course means that there will be no telephone service during this time.

You can avoid this interruption if you have two servers, a primary and backup—but then there will be no backup operation during the installation. Also, the two-server configuration will have to proceed through two implementations, during both of which processes you'll be without backup. And only upgrading one server isn't an option; generally, the primary/backup synchronizing operation will not work if only one of the servers is upgraded.

To learn more about planning for the upgrade, go to your vendor's website. It may contain time planning information for how long the server/gateway/phone will be down for the installation. But remember that the time estimates may be optimistic; the enterprise staff may not be as qualified as the vendor estimate assumes.

Informing The Customer

Another question we posed in the survey is, "How does a customer learn that a release is coming, and how are the release costs charged to the customer?" Some responses:

- **Sphere** does this through its Software Assurance program. As part of the program's annual fee, the customer has access to all the releases. Customers can self-install a release if they complete Sphere's Certification Course.
- **Aastra Intecom** customers are alerted to new software via roadmap discussions at the vendor's user group meetings. Fix lists are distributed to the user group as well as to all Aastra Intecom field managers. Notification is also given through Prod-

You need a software maintenance agreement in order to anticipate TCO

Planning, Testing, Deploying

When planning for the patch, here are some questions to ask and pointers to remember:

1. Make sure you understand the function and operation of the patch.
2. What will the patch solve?
3. What servers and endpoints will be affected?
4. Is a reboot required after installation?
5. Can the patch be uninstalled?
6. If the patch fails, how can the server and endpoint be recovered?
7. Is there a test platform available for testing the patch?
8. Interrogate the vendor to determine how well the regression testing was performed. You do not want to be the vendor's software test bed.
9. Whose operating system patch should you install: the original software vendor's (Microsoft) or the VOIP/IPT vendor's?
10. Define the extent of the patch and the recommended time frame for installation. Extent can range from a critical to an informational patch.
11. Set up an internal change control procedure for all patches.

When testing and deploying the patch:

1. Ensure that the test environment simulates the targeted server and endpoints.
2. Verify that the patch delivery process was successful.
3. There should be no significant issues after the patch is installed on the server and end-points.
4. Determine that none of the already successful features and functions, installed before the patch, are changed in a detrimental manner.
5. Remember that two servers with different patch levels can stop communicating with each other after one of them has the patch installed and the other server is one patch behind.
6. Demonstrate that the patch can be removed in case there are problems with it.
7. Verify the patch installation.
8. Review the patch status and formally document and report the completion of the successful patch.

Patches are commonly included in the next release or version of the software so that the enterprise does not have to install the patches separately. One vendor, who has now fixed the problem, was shipping systems without the latest patches. This required the channels/partners to perform the patch installation and incur the labor cost.

Look into how your IT department handles patching. It already has some mechanism for patching that may be the model to use for VOIP/IPT patching. Those who have responsibility for core voice functionality may even want to consider outsourcing the VOIP patching problem to the IT department.

Patches can take anywhere from 10 to 60 minutes to install after the preparation has been completed□

Patches may be general or security-related

uct Notes distributed to customers. An annual software agreement can cover the release costs. Alternatively, customers can pay for the features activated, and for the number of users.

- **Nortel** normally works through channels that are issued a Product Bulletin and Knowledge Transfer Kits (sales and marketing information). The channel in turn communicates with the end user, Customer Forums, Channel Forums and trade shows. The cost of the new releases can be covered by purchasing a Software Release Subscription (SRS). Customers can install releases if they have the proper training and accreditation.
- **Avaya**'s Manufacturers Support Policy specifies support (software enhancements and bug-fixes) for the current Major Release and one prior Major release. Avaya provides six months' notice of end of manufacturer support of a major release. Major releases are chargeable to a customer; minor releases are an entitlement after purchase of the major release. Avaya also offers upgrade protection plans that allow software upgrades via paid subscriptions (three-year agreement).
- **Inter-Tel** informs the enterprises through their resellers. Major releases are charged to the customer, while minor, maintenance and emergency releases are free.
- **Alcatel-Lucent**'s Key or Large Accounts have a Direct Touch representative or Global Service Manager in charge of delivering information to the customer. Alcatel-Lucent has mainly indirect distribution through certified business partners, who are supposed to announce the release. Alcatel customers can subscribe to a Software Evolution Service to cover the cost of releases.
- **NEC** publishes "Dear Associate" letters, which are sent to their Associate Partners. End user customers and consultants may also register to receive these letters. NEC offers a Software Subscription which covers software-only upgrades (not installation). Any hardware changes required by the upgrade are chargeable to the customer.

The vendors recommend the customer use a software maintenance agreement to cover the costs of new releases, as this is the only way to anticipate the software cost in your TCO calculation. Each vendor has a different program for release notification that must be spelled out in the RFP and subsequent contract.

Release costs can be controlled, but only through a software maintenance agreement. Any additional hardware you may require in order to implement a new software release will be a separate charge, and not covered by the software subscription agreements.

What's A Version?

All the vendors consider a version to be a smaller change in software that does not warrant a full release. The number of versions supported is essentially unlimited. Normally there is no charge for a version, though if it is installed by a channel or partner, there will be a labor cost for the installation. Some specifics:

- **Sphere** defines "versions" as a subset of a release. They have issued one such minor release since January 2005.
- **Aastra Intecom** uses the term "Baseline" release to cover what can be called a patch. There have been five since January 2005.
- **Nortel** defines a version as a post-release that provides incremental features and functions to meet customer or market-specific needs. There have been two server/gateway versions and several for IP phones since January 2005.
- **Avaya** defines a version as a minor release. There has been one since January 2005.
- For **Inter-Tel**, the terms *release* and *version* are synonymous. There have been 8 to 10 smaller "maintenance releases" since January 2005.
- **Alcatel** also defines versions as minor releases. There have been two minor releases each for the OmniPCX Office and the OmniPCX Enterprise products since January 2005.
- A version for **NEC** refers to the software feature level, for example: R-18, R-19, R-20.5,etc. (this numbering system is unique to NEC). A software version may be active in multiple releases of hardware. NEC has issued six versions since January 2005.

Since *versions* are, for most vendors, a form of software release, versions bring with them the same installation issues we discussed for releases. Most vendors have issued four to six version (minor) releases since January 2005—not a large number. But it does mean the enterprise should anticipate a version every four to six months in addition to the major release (Table 1).

The impact of a version can also be significant. There is always the chance that part of the version will not work, so the enterprise should allocate time and staff to test before implementation. This could take several staff-days, once again incurred either by internal employees or as a paid service. As with releases, you may also have to bring down the PBX during the installation.

TABLE 1 A Year in the Life of Software

Month	1	2	3	4	5	6	7	8	9	10	11	12
Releases (1)				^								
Versions (2 to 4)		^							^			
Patches (4 to 10)	^		^		^	^	^	^	^			

Patching, Patching And Patching

Patch management has been an IT problem and topic of discussion for years (See "Patch Management Tools"), and now the patching problem has come to the voice environment. In one telecom managers' focus group, patching was the most frequently discussed complaint. There will be patches to the servers, gateways, hard phones and softphones. Patches can be needed for the operating systems, protocols, features, functions, administration and applications.

So what exactly is a patch? The definition at www.webopedia.com is "a fix to a program bug. It may also be called a service patch. A patch is an actual piece of object code that is inserted into (patched into) an executable program. Patches are typically available as a download."

Most enterprises divide patches into general and security patches (See "Security Patches: The Headache," p. 56). The security patches should receive priority.

Patching is always a difficult issue. Some considerations:

- Enterprises don't patch enough. The overload of patches being issued causes enterprises to delay or ignore some patches.
- Conversely, enterprises may also patch too much. Not all patches are necessary—but it can be difficult to determine which to install.
- Viruses infect faster than ever. In fact, as soon as a security patch is announced, the enterprise's vulnerability to security breaches will increase until the security patch is installed.
- Patches don't always work. For example, the day Windows XP was announced, Microsoft announced two Windows XP security patches that, it turned out, did not work.
- Enterprises don't test the patches. Patches have been issued that turn off previously successful application functions and features.
- Patches are necessary, but as noted above, the volume is out of control. Some vendors avoid publicly stating the number of patches delivered because the more patches issued, the lower the confidence in the vendor's products.

Now the next question is, where do you get the patches? This also depends on the vendor:

1. Most vendors offer the patches through channel partners; in some cases, going through the channel partner is mandatory.

2. When the customer owns and maintains the VOIP/IPT devices, certified staff members can access the patch library to determine whether the patch is appropriate—but they may not be able to download the patch (depends on vendor).

3. Some vendors will not allow the customer to even view the patch library, requiring all patches to pass through the channel or through the vendor maintenance arrangement.

4. Some endpoint patches can be stored on the call server and are downloaded automatically when the endpoint registers to the server.

Some vendor responses about patches:

- A **Sphere** patch may include a fix, feature, etc., however a patch is typically reserved for providing an urgent repair that is service affecting. Customers are notified through email or through the company's Technical Assistance Center (TAC). There was no comment from Sphere on the number of patches issued.
- **Aastra Intecom** uses the term Engineering Change Order (ECO) instead of patch. They have issued 31 ECOs since January 2005.
- **Nortel** includes firmware, product improvement, interoperability, customized product improvement paid by the customer, as well as diagnostics (to trap a specific event) as patches. So patches do not always equal fixes; Nortel declined to specify how many patches had been issued.
- **Avaya** issues patches as Product Correction Notices (PCN). Customers subscribe to email notifications of patches. Avaya typically issues 3 to 4 service packs per year containing 10 to 20 fixes each. Not every service pack needs to be installed by every customer.
- For non-urgent conditions, **Inter-Tel** refers to a patch as a maintenance release. Emergency releases cover system stability or performance. There have been 10 maintenance releases since 2005.

Do enterprises patch too much—or not enough?

Patch Management Tools

The typical IT department has to contend with Patch Tuesday from Microsoft, as well as patches from their many software vendors. There can be several thousand patches a year to consider and install. This problem has stimulated the creation of patch management tools, which help organize, control, inventory and distribute patches. A well-designed tool will:

- Have scanning flexibility to identify and locate missing patches.
- Have comprehensive scanning to eliminate false positives that can create wasteful efforts.
- Be efficient to deploy.
- Be as up-to-date as possible in scanning for patches and determining need for them.
- Provide detailed reporting on software patch conditions.

More than a dozen such tools are on the market, and vendors have information on their websites. The following vendors are listed not as a recommendation, but they do have useful information for understanding the issues and methodologies for good patch management:

- Shavlik Technologies (www.shavlik.com)
- Encora Software (www.encora.com)
- Blue Lane Technologies (www.bluelane.com)
- Patchlink Corp. (www.patchlink.com)
- NetClarity (www.netclarity.com)□

Security patching should be proactive, not reactive

Security Patches: The Headache

Security is the most anxiety-producing patch problem. Security patches can be found on the VOIP/IPT vendors' sites. The vendor sites are usually more current than the sites listed below. Nevertheless, the public security vulnerability sites have hundreds of known VOIP/IPT patches, and they include:

- **http://cve.mitre.org, Common Vulnerabilities and Exposures (CVE)**—A dictionary of publicly-known software security issues that is maintained by Mitre for the U.S. Department of Homeland Security. As of mid-June 2007, this site had nearly 22,000 listed software security patches, of which about 500 dealt with VOIP, IP-telephony and related signaling protocols.
- **http://nvd.nist.gov, National Vulnerability Database (NVD)**—A list of publicly-known software security issues that is maintained by the National Institute for Standards and Technology (NIST), also for Homeland Security. The NVD includes the CVE dictionary mentioned in the previous bullet. As of mid-June 2007, this site had nearly 25,000 listed software security patches, of which about 150 dealt with VOIP, IP-telephony and related signaling protocols.

The NVD site has existed since 1999. It is only within the past three years that this site has included VOIP/IPT vulnerabilities. The NVD site gathers information directly from 10 other sites and indirectly from 50 more sites. It provides links to patches and directions for limiting the dangers. A significant value of this site is the severity rating given to the patches. Each security vulnerability is assigned a rating using the Common Vulnerability Security Scoring system (CVSS). A rating of 7 to 10 means immediate action should be taken. Most patches rate 5 or lower on severity□

- **Alcatel-Lucent** patches only bugs. There is no published policy for the patch delivery. Maintenance patches are shipped every 4 months for a given release.
- **NEC** uses the term patch as well. NEC considers the number of patches proprietary and did not provide a patch issuance figure.

Conclusion

The patching problem will not go away. If history is any guide, VOIP/IPT patching will continue, especially for security purposes.

Patches that fix a problem other than security can be selectively inserted into the system and endpoints. Security patching, on the other hand, should be proactive, not reactive. There will be cases when a defensive approach must be taken, when a critical security incident arises. Security patches are designed to terminate vulnerabilities and mitigate the possible risk that the server and endpoints will be compromised□

Companies Mentioned In This Article
3Com (www.3com.com)
Aastra Intecom (www.aastraintecom.com)
Alcatel-Lucent (www.alcatel-lucent.com)
Avaya (www.avaya.com)
Cisco (www.cisco.com)
Inter-Tel (www.inter-tel.com)
Mitel (www.mitel.com)
NEC (www.nec.com)
Nortel (www.nortel.com)
ShoreTel (www.shortel.com)
Siemens (www.siemens.com)
Sphere Communications