The Network – Delivers!

Record Software Non Compliance Settlement

$3,467,000

(Not counting an additional $10 - $15 million in hidden costs!)

Software Piracy Enforcement Audits Get More Lucrative Every Day!

In September, 2007, the Business Software Alliance (BSA) announced a record anti piracy settlement of over $3,467,000. The claim involved an "undisclosed international media company" that we'll call ***Target IMC***. Realistically, the underlying costs of this single punitive copyright compliance audit event—the costs you never see published—easily exceeded $10M-$15M. Read on to discover how your company can be exposed to this type of software piracy audit. As well, we discuss how *Target IMC* could have prevented, or at very least minimized, the financial impact of their ineffective software asset management techniques.

Nearly 50% of the companies we encounter inform us that their management of copyright protected software is excellent. Some claim their company is too small to be noticed by the software piracy audit teams. Some claim their company is too small. Unfortunately, none of these three claims is generally based in quantifiable fact—the only facts the software piracy auditors will accept. In other words, these companies are living in a fantasy world of denial—a world that will rapidly fall apart when the copyright violations auditors come calling.

So? How did *Target IMC* become mired in their personally customized software piracy punitive purgatory? More importantly, how could this same nightmare happen to you?

1. **All you have to do is use technology**. Ownership of desktop computers, notebooks, servers, PDAs, cell phones, smart phones, answering systems, printers, copiers, fax systems, even a simple radio—can set you up for an up-close and personal encounter with the software piracy enforcement auditors or the literally dozens of related copyright audit teams. ***The Network*** *trains your personnel to recognize and mitigate costly technology-related risks.*
2. **If you own the hardware, you are definitely responsible** for the materials loaded on that hardware. This means that ANY operating system, software, font, graphic, music, video—even gaming—products on your systems—and please don't fall for the, "We don't permit games on our systems," fantasy. Let us repeat this critical issue: ANY of these products can and will expose you to software piracy and/or copyright enforcement audits. ***The Network*** *delivers core tracking procedures that enable you to maintain maximum control over tech evolutions.*

3. **All you have to do is grow**. Every time your technologies change—or every time someone changes them—you expose yourself to new and frequently invisible software piracy or copyright-related risks. ***The Network*** *delivers simple, low-cost procedures you can use immediately to monitor the growth of enterprise technologies—minimizing the losses common to ineffective asset management.*
4. **All you have to do is misplace your trust**. Unless your organization has established an *effective* life cycle management program for both software and hardware, anyone within the enterprise can set you up for a punitive audit.

> **Real World** – A confidential spokesperson for *Target IMC* implied that their non compliance exposure could be traced to a single individual who "(*failed?*) to keep us compliant and manage our software assets."
>
> Does anyone want to place odds that some semi-clueless software asset manager has been targeted as a convenient scapegoat? Think we're crazy? Check item number 5 below.
>
> If this company had used the techniques delivered by ***The Network*** to effectively manage its technology assets, they could have minimized the impact of this anti piracy audit—as in knocking down their potential lost revenue by somewhere around 3.4 to 10 million dollars! The key word here is "effective"—and unfortunately very few companies use a truly effective software asset management process.

5. **All you have to do is fail to pay attention**. We have known a distressingly large number of software asset managers, technology asset managers, or copyright compliance assurance professionals who have repeatedly informed us that executive management of their company is playing the license compliance shell game. These executives are well aware of the risks of software piracy; They're well aware of the occurrence of copyright non compliant events within their enterprise; They have been repeatedly informed of existing risk issues; Yet, they still fail to take action or empower anyone else to take action putting an end to the non compliance. ***The Network*** *shows you how to avoid this costly trap.*
6. **All you have to do is miss a single important software piracy exposure factor**. Just one simple mistake can wreak havoc across your entire enterprise. Many times the non compliance mistake is innocent—but just as many times it is blatant software piracy. Either way, unless your asset managers thoroughly understand the exposure factors, you get to be a constantly paranoid audit target. *Unless you contact* ***The Network*** *to discover proven methods for minimizing these common & expensive errors.*
7. **All you have to do is fail to comprehend the sheer power of the enforcement industry players**. Get this straight: There are more than 26 enforcement groups in the United States—over 100 globally. Every single one of these groups is aggressively hunting you and your company. They offer your employees whistle-blower rewards of up to $1 million for reporting your activities.

These folks have regional, national, and international law behind their actions. In other words: ***You WILL NOT WIN a confrontation with them.*** *Contact* ***The Network*** *to discover how you can stonewall the predatory software piracy auditors.*

Real World – *Target IMC* was hit with what is referred to as a forced software piracy audit—a raid. This is absolutely THE most costly license non compliance confrontation. ***The Network*** *delivers the knowledge you need to avoid this incredibly expensive hit to your bottom line as well as head-off the collateral damage to your enterprise reputation.*

Here's your recap: To minimize your exposure to software piracy audits:

- You absolutely must set in place a genuinely effective technology asset management program across the enterprise.
- You absolutely must recognize that the copyright enforcement industry players are sitting on a literal gold mine of easy audit targets.
- You must understand and remain constantly aware of your real world exposure and you have to stand up and take genuine action to minimize that exposure.
- Realistically, if you purposely violate copyright, you deserve to become a software piracy audit statistic. If, on the other hand, you are simply guilty of just plain lousy software asset management, wake up and smell the blood in the water. Failure to do so will ensure that you, too, will become a victim of predatory enforcement audit practices.

By the way: When *Target IMC* was audited and paid their $3,467,000 in fines, they honestly believed that they'd seen the end of their software piracy woes. ***They were categorically wrong***: Their settlement represents the interests of only four copyright holders—ONLY FOUR. How many other rather aggressive software publishers have products on the systems of *Target IMC*? How long will it take these, and dozens of other, copyright holders to identify this international mystery media company and invoke their own "right to audit" clauses?

There is plenty of non compliance blood in the complex sea of license compliance assurance. The audit sharks are circling… Unless you take the right action and take it right now—today—your journey into software piracy purgatory has only just begun.

The Network *provides you with the unique and proven solutions that you vitally need to help avoid this costly series of license non compliance events…*

Any questions? Feel free to ask. We'll do our best to provide an accurate and timely answer.