

# Security Issues for Third Party Games: Technical, Business, and Legal Perspectives

Steven B. Davis, IT GlobalSecure Inc. and  
W. Joseph Price, Kelley Drye Collier Shannon

## Overview

Security is a growing issue in the gaming industry and is of particular concern for games from third party developers and outsourced services or products. Game security incidents have grown into a costly problem. Whether it is the compromise of the game code during development or the customer support costs associated with game exploits, security failures can delay product launches or add unexpected millions to customer support costs. These problems are exacerbated by the nature of third party relationships in the game industry. Outsourced products and services can also introduce expensive risks.

Not everything, however, is bad news. The growth of the game industry may open up new revenue streams for game developers and publishers – especially those who consider security in their game designs.

## The State of Game Insecurity

Game security incidents have grown from a couple of incidents a year to every two weeks in 2005 and more than one a week in 2006. These have ranged from code compromises of major titles like Half Life 2, Grand Theft Auto, and Halo 2 to serious hacks that have undermined online play for games on PCs, consoles, and handhelds. Traditional piracy continues to worsen with piracy problems already for the Xbox 360 and HD DVD and Blu Ray under attack while massively multiplayer online games (MMOs) have also been the victims of server piracy, griefing, and gold farming. These incidents cause more than bad publicity; they can cost millions (and millions) of dollars and may ruin the reputation of a game franchise.

While the game industry does attempt to track piracy, there are no formal statistics or loss estimates from game security failures. The observed costs are quite clear, however. Several games that have had their code compromised during development have been delayed by months. The added costs associated by extending a development project for a couple of months are annoying, but the delay in earning revenues can be staggering. Consider a major game title that earns \$50 million in its first month of release – such a game may effectively “lose” a million dollars for each month that it is delayed.

Online games that use subscriptions, virtual asset purchases, or other business models face substantial costs from cheating and hacking problems. Unlike a traditional computer game where most of the sales are made within a month of launch, online games are designed with lifecycles of 18 months to 5 years or more. As such, controlling customer support and operational costs is essential. A company that is running a licensed online game believes that they are losing 10 to 20 percent of their revenues *per month* because of security problems. This probably doesn't fully capture the impact of lost customers and bad word-of-mouth.

## Security Accountability in Third Party Development

Third party developers are motivated to get their game out as fast and as cheap as possible and are typically held accountable for delivering a “great game.” Since the bulk of the fees that these developers earn are from completion of the title, their motivation to address lifecycle and operational issues like security, support, and other services is low. Publishers and developers need to cooperate to ensure that security issues are adequately addressed during the development process.

The computer game industry is changing from a business where a flashy box and some hurried reviews will sell a product. Games no longer have a 30-day sales cycle, but are moving to a long-term relationship via an online service. Unfortunately, game development licensing needs to catch up with these changes. While the only security issue that used to be important was fighting, now piracy, cheating, griefing, and other issues are more important. The game publisher needs to provide an ongoing operational infrastructure to support the game. Customer support, server operations, and ongoing engineering, patching and maintenance have changed games into services. The nature of the business relationship and deliverables between a game developer and publisher must change to match this model. Solid engineering, good design, infrastructure costs, life cycle costing and management now matter. Publishers must rethink their relationship and contracts with developers so that business needs match with contracts.

Interestingly, there are collateral benefits to these changes. Simply providing an online game service can be a powerful anti-piracy tool, as Blizzard demonstrated with Battle.Net. Also, multi-player gaming means that when a friend introduces a new game to his buddies, his buddy is more likely to buy the game so that they can play together, not just borrow the initially purchased copy.

Factoring in security issues into the game development process is one way to reduce lifecycle costs and risks. Game publishers should engage a “layered approach” when working with developers and end users. Security risks (which translate into costs) should be considered at each stage of game development. The later security is considered, the more expensive it is going to be ... and the publisher will ultimately pay for security failures – one way or the other.

Today, for games from third-party developers, the software is typically provided “as is,” in terms of security. During discussions with developers, many have said “security is the responsibility of the publisher.” For console games, developers and publishers have relied on the security provided by the platform – a strategy that has not had good results so far. So, with everyone placing the security responsibility on everybody else, the security “ball” simply gets dropped.

When there are security failures, the publisher is the one who pays.

If the publisher insists on a security solution, and is willing to pay, developers will apply resources to security, just as they do for animation, art, and game play. In contracts, the publisher could assure that its developers agree to appropriate indemnification for security issues.

(“Indemnification” is a contractual method of accepting responsibility when a problem occurs.)

If this is not possible, the publisher could insist that the developer deploy security that the publisher has rights to and prefers, as part of the game. In other words, the developer should consider incorporating its own security solutions that it believes are good enough warranting a tight indemnification or give the publisher the ability to require its preferred security solution to be incorporated as part of the game.

## **End-User Security Risks**

Publishers need to consider how potential security flaws will impact consumers. For example, a game run on a PC that introduces a security flaw could make the game publisher a plaintiff's lawyer dream and publisher's nightmare. The Sony-BMG Rootkit scenario, where Sony-BMG's music software installed an "anti-piracy" software tool that introduced potential security vulnerabilities was bad, but it could have been much worse if Sony's security tool had been used to deliver a virus or other malware. The publisher should make sure that features and security code do not create new security problems, provide reasonable disclosures to end users, and put potential hackers on notice that access to game code is not permitted (sounds obvious, but this legal element will help in court). Lawsuits are putting publishers on notice that they have an issue; notice-based liability requires the publisher to react.

## **Code Theft and Development Security Practices**

The process of developing and supporting games has grown steadily more complex. Localization, audio, and art may all be developed by different companies. This requires increased formalization of security processes to protect the game project.

Code theft has become a notable, and highly preventable, security vulnerability for the games industry. The "garage engineering" mentality is still too prevalent in an industry with multi-million dollar development budgets and gross revenues for individual games over one hundred million dollars. A game's code-base and art assets are just too valuable to be left easily accessible on the Internet – especially in an industry that regularly complains about losing millions and millions in sales to piracy.

Even worse, these problems are largely preventable. Traditional information security practices such as firewall, intrusion detection systems, good configuration management systems and even simply disconnecting high value data from the Internet are widely available and relatively inexpensive.

A notable complicating factor is the rise of distributed development and outsourcing in the games industry. More sites, more companies, and more people inherently create more risk. There are a variety of criminal laws addressing code theft. Which section of the criminal code that will apply depends on the circumstances of the crime. A common criminal law prohibiting most types of hacking is the Computer Fraud and Abuse Act ("CFAA") (18 U.S.C. § 1030). Most of the CFAA's provisions prohibit unauthorized "access" to a "protected computer" coupled with other conduct.

A proactive security strategy is needed to manage these risks. First of all, don't provide full access of high value data to everyone. If a person, or company, can't access data, they can't compromise it. Second, make people and organizations accountable. Implement tracking and logging mechanisms – if a problem occurs, it is possible, and preferably easy, to find the culprits. Fire people, fine companies. Publicly. Finally, have a recovery plan in place in case of theft or disaster. Games are major businesses – they should implement good back up strategies and have disaster recovery plans in place, as well as insurance and other measures to manage business risks.

Hackers and other data intruders are subject to criminal and civil liability. There are at least forty federal statutes that can be used to prosecute cybercrime, victims can sue under a variety of civil

theories. But hackers are difficult to identify or subject to the jurisdiction of the United States. Even worse, they are typically what lawyers refer to as “judgement proof” – not worth suing because they do not have enough money to pay damages.

A better target for a lawsuit is the entity that failed to prevent the security breach, or otherwise covered up an issue causing more damages in the long run. These entities are deeper pockets for plaintiffs, and sometimes easy targets. In general, courts will impose some form of liability on the person in the best position to prevent losses, particularly if they are aware of the security issues. The best legal defence, therefore, is to avoid security breaches. Security bonding and insurance (if available) may also help.

Issues will arise, however, and there are specific laws to meant to preserve intellectual property and network integrity. Owners of intellectual property (such as game code) can seek protection through trade secrecy, patents, copyrights, and other legislation tailored to their particular industries. In the DeCSS cases, for example, the DVD Copy Control Association (“DVDCAA”) tried to stop distribution of DeCSS through state trade secret law, while Universal and other studios invoked the DMCA, a federal copyright and anti-circumvention statute. These techniques only supplement good business strategies and effective technical measures. It is an open question whether the DVD industry “won” the war against DeCSS or whether the decreasing prices of DVDs had a more significant impact on reducing piracy.

## **Security Accountability in Third Party Licensing**

Online games are increasingly seen as good licensing opportunities. Potential game publishers/operators get a completed title and developers open up new royalties. However, licensees are obliged to operate and support these games and security problems can turn a potentially profitable license into a costly support and marketing nightmare.

Monthly costs due to security problems of 10 to 20 percent or more, as noted in the example above, can suck all of the profit out of a licensed game service. In Sony Online Entertainment’s report on its experiment with Real Money Transactions, they found reductions in overall customer support costs of 40 percent simply by supporting these transactions internally. The key to successful licensing is to control support costs and security problems can be a major driver of a game’s support costs. Cheating, griefing, and hacking or even the perception of cheating, griefing, and hacking can become major problems for any game service.

A key part of the due diligence process for licensing any game should be to determine support costs and risks. Games developed in sophisticated markets like Korea are likely to be thoroughly “tested” by griefers, cheaters, and hackers. It is highly worthwhile to research the “security state of the game.”

Another question that is important is accountability for security. This issue cuts both ways. The game developer may be concerned that the licensee does enough to protect the source and executable code that they provide while the licensee may be rightly concerned about who will fix security problems (and who will pay to fix those problems). NCSOFT’s server code was compromised, apparently in China, and turned up in several places, including a pirate service in the US that was shut down recently by the FBI. Conversely, NetDevil had the code for its City of Heroes server compromised – one wonders how a licensee would feel about paying its fees when the risk of a pirate service has increased due to this failure. In Korea, a number of game companies outsource security to specialty security service providers (in the US, the only

commercial game security service provider is Even Balance with its Punkbuster security service). When licensing a game that uses such a service, it is probably preferable to include the security service in the prime contract with the game company to have unified responsibility for security (and, since the total payments are larger, a bigger “stick” to push for better security support).

An interesting collateral issue is the issue of replacing a licensee. The long saga of The9 and their battle with Blizzard over the licensing of the Burning Crusade expansion to World of Warcraft in China is an interesting example. The companies worked out their issues, but Blizzard was quite unhappy for a long time with the quality of service that The9 was providing to World of Warcraft’s Chinese customers.

## Service Provider Security Issues

Games are no longer simply sold in a store. There are electronic distribution services, online game services, payment processors, game arcade operators, and even security service providers. The security performance of these companies can have serious implications for the success of a game. Outages, such as that recently experienced by Valve’s Steam online game distribution service, as well as more conventional security requirements can affect all of these businesses. The situation can be complicated further by having many companies, subcontractors, products, and service providers involved – and when there is a security problem, they will all be pointing their fingers at each other or at you.

If you are lucky, legal issues are raised just before signing the contract for software or services. Typically, however, security only becomes a consideration when a breach occurs. In a perfect world, every contingency will be in mind when initially negotiating the contract. In the real world, a breach will occur in a way not entirely anticipated, and will be complicated by confusion and split responsibilities between the affected parties and other product and service providers.

Given these circumstances, it is wise to keep four issues in mind when licensing software or services. The licensor and the licensee should consider: (1) *licensee rights*: the licensor will want an assurance – and the licensee should also confirm for its own purpose – that the licensee has the rights to what it is licensing, including all of the elements it relies upon to deliver the product (for example, consider sublicenses when relying on other licensed work); (2) *damages*: consider worse case scenarios and who you are dealing with; a licensee that cannot (or will not) provide damage relief should expect to provide its product at an appropriately discounted rate because the licensor will have to spend money elsewhere in anticipation of a breach (if the security software firm, for example, is a small company with little or no assets, then its breach conditions or warranty might only be as good as its insurance policy, if any, which should be requested to be part of the agreement); (3) *warranty*: anything short of an express warranty, created by an affirmative statement, description, or promise in the license (such as an express warranty as to the security capabilities of hardware or software) will give a licensor pause; and (3) *breach and termination*: consider how you can get out of the license agreement, particularly when a breach occurs, and also consider what damages might be available upon breach.

Reviewing the license in the context of a security breach will likely be as complicated an effort as when initially negotiated. There are few laws and regulations to apply in this area of law. Liability will likely rest with the entity that is contractually liable, **if there is one**.

If there is a lawsuit, it will be crafted around how the security breach occurred. Good logs and tracking mechanisms are necessary to even begin such a suit. These records need to be created, stored, and handled in a manner such that they can be used in court. Consider the forensic issues before an incident occurs. If the license grants rights for software or services “as is,” then there are no guarantees, such as the existence of an express or implied warranty (this is often found in a paragraph in all caps in the agreement). If there is any available warranty, it will be, at best, in a legal grey zone – the license may provide a degree of a warranty, complicated by limited indemnification rights, and subject to third party licenses that no party ever read.

Damages for breach of warranty are generally different than breach of contract. It is common to have exclusive remedies applicable to contractually promised express warranties if, for example, the hardware, software, system, or service fails to comply with an express warranty. For these reasons, the breach of contract and breach of express warranty claims are generally treated as separate claims, even where the express warranty claim arises under a contract between the parties.

Service providers (e.g., ISPs) may find themselves part of a lawsuit whether or not they “should” be included. The quickest way to get out is to have something clear to give to the court that cannot be attached by the plaintiff or other defendants. In that manner, service providers will want to take full advantage of a legal immunity available to them (47 U.S.C. § 230), and confirm that immunity in the service agreement.

The model to engage is the “conduit.” With the law and typical service contracts on their side, ISPs will escape liability, which will likely run to another party. A slight warning is warranted to those ISPs that move from the conduit role and add functionality. Even a recent case in California confirming the broad application of immunity included a footnote indicating that any involvement by the ISP that is extensive could void the immunity. That leaves the door open for liability if the service provider provides security functionality, and fails.

The contract should be the security measure of last resort. First, design the business so that it has robust security; second, have clear accountability by any external parties; third, have a solid technical solution; and finally, paper it over as well as you can with good contracts and licenses.

## **Long Tail Opportunities**

There is an emerging area that game publishers and developers have not fully exploited or considered in their games – secondary commercial game licensees. There are companies that would like to operate tournaments, contests, and simply for-pay online services with existing games in the same geographic market as the basic game. This may require more rigorous security design to allow effective competitive play or simply an alternate version tied to the commercial service. However, they can add additional sales and extend the life of a game with minimal additional development costs.

Also, there are game cafes and account-based licenses. Most US and European games are licensed on a per-copy basis while in Asia games are typically licensed by usage. The lack of recognition of these different license regimes during business planning has made it much more difficult for games to reach both markets.

Finally, integrated online game services such as Turner’s GameTap may extend the life of a game and open up a new revenue stream – especially, if planned for from the beginning.

All of this raises an interesting development and licensing strategy. The film industry has, for years, pre-sold rights to different markets during the development stage. Game companies could potentially reach out to these various markets noted above for funding – spreading their development costs and reducing risks.

Gamers have little or no loyalty to developers, much less publishers. Another area that has been poorly developed, but which could have security benefits, is a publisher-wide online infrastructure. A lobby service, ranking system, and online store, are all features that can help strengthen a publishers brand and create a direct link with its customers. Also, these services can have a substantial anti-piracy and overall security benefit by creating an enduring relationship with players.

## Conclusion

The rapid growth and huge changes in the game industry in the past several have opened up some significant, and expensive, security holes. There are more companies involved, there is a lot more money involved, and there are many, many, more things that can go wrong. Simply being aware of the potential security impacts of these new business configurations will be a good step. A proactive security strategy can reduce risks and even open up new opportunities.

## Questions and Comments

Please address questions and comments for Joseph Price (legal), an attorney at Kelley Drye, and Steven Davis (technical and business) to [ceo@secureplay.com](mailto:ceo@secureplay.com). Steven Davis, CEO of IT GlobalSecure, maintains a blog, PlayNoEvil (<http://www.playnoevil.com/>), which contains the reference incidents, materials, and articles cited throughout this paper.

## Authors

### ***Steven Davis, CEO, IT GlobalSecure Inc.***

Steven Davis, CEO of IT GlobalSecure, leads the [SecurePlay](#) game security product development, IT and game security engineering services and training. He writes a blog on game security on other industry issues at: <http://www.playnoevil.com>. Mr. Davis' twenty years of expertise includes security leadership positions at NSA, CSC, Bell Atlantic, and SAIC. He worked on Nuclear Command and Control, Key Management Systems, and other security systems for the government and commercial customers. He holds a BA Mathematics from the University of California-Berkeley and obtained his Masters Degree from George Washington University in Security Policy Studies. He holds several patents for innovative security solutions.

### ***W. Joseph Price, Attorney, Kelley Drye Collier Shannon***

Mr. Price's legal practice is concentrated on e-commerce issues with a focus on business transactions for developed and developing entities and specialized litigation. He represents clients in matters involving internet-based service providers, content providers, technology-based enterprises, VoIP services, telecommunications carriers, as well as purchasers of such products and facilities. Mr. Price's litigation experience includes the representation of clients in federal and state courts, including the defense and resolution of investigations and enforcement actions

initiated by State Attorneys General and federal regulatory agencies, such as the FBI, FTC and FCC.