Disgruntled employees and Intellectual Property Protection
Dan Morrill
April 2006

Don't always think in a straight line.
**- *The Way of the Spear***

The greatest knowledge is knowing what intellectual property you own, and where it is located on the network. The next greatest knowledge to know is what controls, technology and processes stand between that data and both insiders and outsiders. The way that intellectual property theft happens can come along a number of various tangents. However, the disgruntled employee is fast becoming the avenue of choice for loosing intellectual property. There is at least one excellent example, in the Sony DRM root kit that could provide a viable avenue for the disgruntled employee to take advantage of the network, and its computing systems.

While some data may be lost due to an honest mistake, posting something early on a web site, or accidentally loosing a laptop. Angry, disaffected employees are also a risk for loosing data to the outside world. The vectors for inappropriate data loss can be as simple as an employee who is angry at management for what ever perceived issue that is posted on a blog. To data that is deleted across the enterprise framework without adequate backups of that data to restore the company back to operation.

There are also employees that seek out to deliberately ruin the corporate image that exists for the company. Elite web hosting was targeted by a former employee that hacked their way into the systems in 2000.

> "For Elite Web Hosting in Orlando, Fla., September, 2000, was a nightmare. A disgruntled former employee allegedly hacked into the company's computer system without authorization. He then allegedly sent e-mails that contained vulgar language and implying that Elite was moving into the Web porn business to every Elite customer. The missives further claimed that the company's majority owner, Augustino Mireles, had been raiding Elite's coffers for personal use. The impact on Elite was immediate. Thirty steady customers jumped ship, each taking $5,000 per month in revenue from Elite's cash flow. Elite owner Mireles brought in Advanced Computer Investigations (ACI), a computer-security company. Its assignment was to bolster the company's defenses against hackers and ensure that the former employee could not get back into the system". (Business Week, 2000).

Disgruntled insiders is not as unrealistic as people may think, nor is it far fetched to think that anyone in the organization would be willing to bring it down or hurt it. News services are rife with information such as the Elite Web hosting company, that result in the total loss of the company. Corporate reputations are hard won, and easy to loose. The reputation that the corporation has is just as important as any other for of property that a company may have. Intellectual property that is deliberately sold as with Omega engineering:

> “In 1998, a network administrator for Omega Engineering was accused of activating a digital time bomb that destroyed the company's most critical manufacturing software programs. The company claimed more than $10 million in damages and lost productivity. The jury found the administrator guilty.” (Network Computing, 2000)

The numbers are staggering about the impacts of loss of intellectual property, and many small companies cannot afford to loose their competitive edge, nor can they truly afford the raw costs of having to start all over again. Larger companies have more intellectual property to protect, and more ways of loosing that property. Disgruntled employees have a number of motivations, and usually can justify their actions by circular logic, including “the company can afford it”. The ability of people to believe that the company “owes them” goes a long way in justifying the acts. As well people’s personalities will change from their standard personality, and they will trial the attack before it is fully implemented. Mangers should be on the look out for alterations in behaviors, and in finding unexpected software on computing systems like the existence of hacker tools, server software, and other applications that should not be on the computers in question. As well, managers should be looking for large transfers of data out of the company network that are unexplained, or not to the usual trusted trading partners, or along known VPN links.

This is not the only way that intellectual property can escape the company. The use of USB devices, DVD and CDR write drives, all of the technological ways of moving data from point to point all can be controlled using various technologies like Tablus, Cisco, and others. This can lead to management decisions as to how best to control the movement of intellectual property within the organization, as well as with trusted trading partners. Even trusted trading partners need to take into account proper management of intellectual property as shown by Microsoft’s experience with this issue with the loss of Windows NT and Windows 2000 source code, because a trusted trading partner did not have suitable technology or controls to prevent the loss.

> “Early reports indicated, and Microsoft later agreed, that the real source of the leak was Mainsoft, a San Jose, Calif.-based maker of software to port Windows applications to other platforms, including Unix and Linux. A statement attributed to Mainsoft chairman Mike Gullard said, "Mainsoft has been a Microsoft partner since 1994, when we first entered a source code licensing agreement with Microsoft.” (Searchwinit, 2004)

Protecting intellectual property means that you should trust people, but people are not all equally trust worthy. Companies should also trust their trading partners, but not all trading partners are equally trustworthy. Intellectual property in the hands of a company that does not have adequate controls, or controls similar to the originating company can have unintended consequences not just to the trading partner, but to all the companies in the productivity chain. These kinds of consequences are usually not thought about when a person in the company starts out, nor do they see themselves as criminals, or otherwise

doing anything wrong. Rather people who do this kind of intellectual property theft often see themselves as doing good, or saving the company from a gross mistake, or otherwise striking back at management or co-workers that are non responsive to what ever the person thinks needs to happen.

McAfee issued a report in 2005 that described some of the common issues that companies face when dealing with their own internal computing systems.

- One in five workers (21%) let family and friends use company laptops and PCs to access the Internet.
- More than half (51%) connect their own devices or gadgets to their work PC.
- A quarter of these do so every day.
- Around 60% admit to storing personal content on their work PC.
- One in ten confessed to downloading content at work they shouldn't.
- Two thirds (62%) admitted they have a very limited knowledge of IT Security.
- More than half (51%) had no idea how to update the anti-virus protection on their company PC.
- Five percent say they have accessed areas of their IT system they shouldn't have. (McAfee, 2005)

As well, McAfee has also quantified a system of four major personality types that inhabit a company's security infrastructure.

- The Security Softie – This group comprises the vast majority of employees. They have a very limited knowledge of security and put their business at risk through using their work computer at home or letting family members surf the Internet on their work PC.
- The Gadget Geek – Those that come to work armed with a variety of devices/gadgets, all of which get plugged into their PC.
- The Squatter – Those who use the company IT resources in ways they shouldn't (i.e. by storing content or playing games).
- The Saboteur – A very small minority of employees. This group will maliciously hack into areas of the IT system to which they shouldn't have access or infect the network purposely from within. (McAfee, 2005)

Various organizations report the incidences of disgruntled workers and internal hacking are on the rise. No company wants to have this kind of information out on the internet, nor do they want to have their customers know that their data has been exposed due to a bad hire. While companies rightly focus on the outsider as a primary entry point by using firewalls, antivirus, anti spyware, patch management and other technologies, the insider is often overlooked. As technology becomes harder to crack from the outside, it is more effective to come at a company from the inside, using any vector from social engineering, bribery, blackmail, even getting contractors or new full time employees to take a second job with a person who wants the companies data.

With all these threats, and various ways of going about getting data in and out of the network, the solution seems like it would be difficult and costly to implement. Intellectual Property protection should be in line with the estimated dollar cost should the data be lost, or otherwise accidentally disclosed or intentionally disclosed. While no solution is perfect, information security personnel rather need to set up speed bumps that will discourage all but the most dedicated internal hackers. Most people who are internet and not internet savvy or hacker savvy will attempt one or two tools, and if they do not work, then they will abandon the process. Simple controls and processes can go a long way to reducing these kinds of threats.

Personnel:

- Do not use group accounts; each person should have their own account on the network
- When using service accounts passwords should be highly complex and stored in a password vault
- No person should have access to a service account, domain administration, root, enterprise administration account or otherwise without a solid check out procedure
- Do not store critical passwords in spreadsheets on a network share
- Have Human Resources policies that have clear and direct consequences including termination for releasing or otherwise compromising computer passwords or sharing user accounts
- Do background checks on all incoming employees to the company
- Do credit checks on all incoming employees to the company
- If they blog and disclose it, read what they write about with a critical eye as to what kind of employee the person would make. Is their blog full of angry statements or self aggrandizing statements? Blogs are an excellent way of discovering the personality behind the person
- Talk to their references that they provide on their resume (and be careful not to commit any HR violations)
- Trusted trading partners should also have their own accounts on the network
- Trusted trading partners should be on their own VPN, and access should be limited by IP address to what resources the trading partners need
- Monitor sharp and sudden changes of peoples personality, if uncomfortable, put the personnel on a special project that reduces the risk of loosing data and reduces their permissions on the network
- Be prepared to work with law enforcement if needed
- Be prepared for news services to find out that there has been a hacking attempt and to ask questions
- Be prepared to handle questions from members of the companies, investors, investing houses, and other interested parties
- Have a fully cognizant legal person ready in case of a intellectual property or company wide event that would lead to the loss of data

- Have more than one person doing the same job, have key person insurance in the event of a loss of key personnel
- Have policies and procedures for contractors, trusted trading partners, and regular employers that clearly spell out requirements for internet access
- Have a clearly designated process for releasing data onto web sites, and other company properties that can be accessed by the general public

Technological controls

- Use software that limits access to USB, CDRW, and DVD-RW drives on computing systems. They should only be unlocked when adequate need has been established for them
- Always test backups, conduct a quarterly emergency drill where complete loss of computing systems are effected, and how to recover from any disaster
- Log all security events on a network and use a collation engine to sort through them looking for locked passwords, escalation of privilege, and other signs that someone may be trying to figure out the security mechanisms of the network
- Watch for very large transactions off the network that would indicate an off hours or very large data transfer off the network.
- Be able to attribute events to IP, System name and IP address, login for all suspicious events on the network
- Verify all data on the network and have more than one person filling any particular technological function
- Conduct regular software inventories using a tool like SMS or other software inventory tool
- Check all contractor equipment to ensure that it meets company standards. If there is software that is not normal for the company, or their equipment has hacking tools or other tools, have them remove it.
- Develop a “VPN Jail” for all unknown systems that connect to the network when someone first connects a new system to the network.
- Keep abreast of hacker tools, and other technologies that can enhance or defeat the companies current security mechanisms
- Monitor search engines, peer to peer networks, and other networks for the existence of the companies intellectual property

These solutions do not have to be costly to implement, but do require coordination at the management level to make the process successful. As with all new policies and technological controls, feasibility studies will help the company determine which controls and processes make financial and business sense. Management and senior Management coordination are also required to make these processes and changes successful. Companies should also be evaluating their perceived risk along with actual defined risk.

Perceived risk is when the company thinks that there could be a violation of data because of inadequate controls either personnel or technological. Actual risk is when data is discovered leaving the network, or found on the internet. Management should designate a team to review all personnel and technological controls and then develop a threat

scenario based on the likelihood of something happening. From that scenario, controls and technology should be reviewed that will mitigate or reduce the risks that the company deems likely to have happen. No process should be undertaken without management, and in many cases, HR and Legal review.

Test case: Sony DRM six months later

Its been almost six months since the revelation of Sony's DRM project from First4Internet became public and the EFF has released more information on the ramifications and outcomes of using the DRM schema that first4internet used. For those that did not follow the case, or are unaware of it, the premise of the Sony DRM was that it would hide itself on a person's computer so that they would be unaware of it. Some very clever security researchers, Ed Felton and Alex Halderman who according to best resources found it first but waited for legal determination to report it (they have a history), and then publicly released by Mark Russinovich.

The issue really is not that someone used DRM; the issue is that the DRM altered the users' computer in ways that the average computer user could not hope to remove, let alone discover. As well, because it was publicly released, the DRM schema used could be used to hide other programs on a person's computer, and the hackers had a field day with it. As unintended consequences of the Sony DRM process, World of Warcraft game cheaters who ran game cheat code did hide their code within the confines of the Sony DRM module, so that the program could not see the anti cheating mechanisms that WoW came out with, to make game play fun for everyone. Hackers began to hide their code within the confines of the Sony DRM module as well like Breplibot.c. The DRM that was released had some very serious unintended consequences that anyone who makes or uses DRM need to be aware of. Companies should use the Sony case as a backdrop for the public and security researchers view into the programs that are dropped on someone's computer in an effort to protect source code, or source files, in this case music.

One interesting chain of thought that was brought up in the articles was the idea of competing DRM systems on one computer. If both DRM systems use stealth technology (Root Kit types), and since that kind of technology has to reside in low level functionality of the computer, how would someone go about fixing something like that. First, as much with Microsoft's statement that some computers are so security damaged that they need to be started over again from scratch; two competing root kits that are on the same computer could have devastating consequences for the average user. Let alone these kinds of heavily compromised systems on a corporate network. Information security personnel have a hard enough time with malware from hackers and now they will need to add to that the presence of malware from legitimate companies like Sony. Competing root kits as DRM could seriously destabilize a companies computing systems, and most companies let people bring music CD's into work to play on their company computer.

Information Security personnel are not going to know what was done to the computer, but odds are most likely that in a forensics investigation they will run a root kit tool to see if anything is hiding on the computer. If they find one, depending on the companies

policies, they will either wipe the box, or do a more detailed investigation. Without knowing where the root kit came from, or who put it there, or how it got there, a lot of security resources can be wasted because the software came from someone using DRM technology. Security people will not know that it came from a legitimate company, because no security person will think that way initially, and they will need to instill a company wide investigation because they will think, and odds are most likely that they will find further boxes with the root kit. Major companies are not likely to let anyone know publicly what kind of DRM technology they are using, so there will be no answers in any of the collective malware databases on this kind of DRM. Nor will there be any way that a company can recoup the losses of the investigation, or the wiping of company personnel boxes.

The bad part of all this is that Forensic investigations like this are rare; companies with limited resources, smaller companies will not be able to do this kind of investigative work because it is expensive. The malicious insider could quite literally use the root kit provided by Sony to hide their own programs under the $sys$ directory and load the drivers into the system, all by giving someone a Sony CD with the DRM on it, and say "hey I found this great band".

Now for some good news, there is cheap way of discovering the Sony Root kit DRM module in use on the corporate network. Look for calls to Sony or first4internet in the DNS system, this process was used to make an initial call to find out how many people had been infected by the DRM module. Check DNS entries regularly to see if there is any phone home requests in DNS, and then find the computer on the network. Since there is really no reasonable way to remove it short of Sony's removal tool, it might be better to wipe the box because no one will really know if it is Sony's or a corrupted version of the file. You can also review DNS for entries that indicate computers are going places they should not go. Many programs can dump the DNS cache and Ed Felton, Alex Halderman used this process to determine how many computers were phoning home on the internet, and it has been used successfully. A company to determine if there is activity on the network, quickly and cheaply in the longer run can use this same process. Dumping DNS is something that most system administrators or security personnel should know how to do.

While the use of DRM is expected only to grow, security personnel must be able to determine which computers are infected with legitimate and illegitimate software. Policy and process in a company can help in establishing basic processes, but the security team needs to be ready for the future of DRM, and the ways it will be used, for both legitimate and illegitimate uses.

## Conclusion

The test case shows that legitimate and illegitimate uses of packaged DRM to overcome internal security processes are viable. While Sony's DRM had unintended consequences, and was forced to pay fines and penalties in the ensuing legal fall out from their DRM modules, that DRM system is still out there as independent software. The precedent for

allowing people to use  music CD's at work is well established, so this is a viable vector for people with issues against the company to use commercial products to hide malware. This was established in two cases with malware and the problems with World of Warcraft. Security people need to be aware of both the good and bad uses of commercial DRM packages that may show up on a commercial CD.

References:

http://reviews.cnet.com/4520-3513_7-6388181-1.html

http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html

http://weblog.infoworld.com/foster/2006/04/14_a387.html

http://www.cert.org/archive/

http://www.businessweek.com/bwdaily/dnflash/dec2000/nf20001213_253.htm

http://www.newsfactor.com/perl/story/19419.html

http://www.networkcomputing.com/1123/1123f1.html

http://searchwinit.techtarget.com/columnItem/0,294698,sid1_gci951584,00.html

http://www.theregister.co.uk/2005/12/15/mcafee_internal_security_survey/