FTR Now

Protect Your Domain Name from Rogue Departing Employees

Date: July 10, 2008

We have recently helped a number of our clients retain and regain control of registered domain names that have either been threatened or taken by departing employees. We suggest you take steps to control against this risk.

WHAT'S IN A NAME?

A domain name may seem like a simple piece of intellectual property, but once in use, it is a critical means by which an organization operates.

The harm from losing control of a domain name goes beyond those organizations that rely on their websites to conduct transactions. Any corporate website has significant reputational value. It is a sign that an organization is "open for business," and if it is taken down unexpectedly a whole range of stakeholders can be left with questions about an organization's trustworthiness and stability. The targeted organization is left with a communication crisis without its best means of mass communication. Damage to reputation in the eyes of current and potential customers, vendors, financers and employees can be significant and permanent.

Lost control of a domain name will also usually result in the loss of an organization's e-mail system. And without its primary means of communication, the targeted organization will suffer harms that go far beyond inconvenience. As with the loss of a website, an organization whose e-mail system is taken down unexpectedly will suffer damage to reputation. And in organizations that use e-mail in critical business systems, loss of e-mail will also cause significant operational risks.

WHAT'S THE THREAT?

Let's go through some domain name basics to better understand the threat.

To start, people do not own domain names. Rather, they register them through organizations called "registrars" in order to gain an exclusive right of use.

Registrars are responsible for maintaining the official record of a domain name's registration, including the legal entity with the right of use – the "registrant" – and the person who controls the domain on behalf of the legal entity – the "administrative contact."

Registrars also commonly control a domain name's "domain name system" or "DNS" record. The DNS plays an important traffic control function on the internet. If the DNS record for a domain name is set properly by a legitimate holder, the DNS will direct internet traffic addressed to the domain name to the holder's intended website and e-mail server. If not, the legitimate holder's website and e-mail server will essentially be unreachable.

Given what is at stake, one would think that registrars would have highly sophisticated systems for securing domain name registration and DNS records. Unfortunately, this is not the case.

There are only three pieces of information upon which the most common security system employed by registrars relies – a username, a password and an administrative contact e-mail address. Although this may vary depending on the type of domain name, generally, a person with knowledge of a domain name's username and password and with control of its

administrative contact e-mail account can make critical changes to a domain name's registration and DNS records without any further proof of authorization. That is, a registrar will not ordinarily check with a second person or take other steps (like asking for proof of authorization by board resolution, for example) before a person with access to this security-sensitive information (normally the designated administrative contact) is allowed to transfer a domain name's registration to an unrelated company or entity. This means that authorizing the wrong person to act as an administrative contact is a major security gap for domain name control.

The following scenario is not hard to imagine.

A technical employee registers the domain name on behalf of his employer. He lists himself as the administrative contact or maybe even registers the domain in his own name. Nobody thinks twice about this because domain name administration is believed to be a technical matter, and when the employee is eventually terminated (in unpleasant circumstances) he takes the domain and his exclusive knowledge of all usernames and passwords with him.

The employer now has no control over the domain, and its corporate website and e-mail system (with 400 plus e-mail accounts) are exposed to a potential malicious attack. When the employer eventually discovers its predicament it appeals to its registrar, but the registrar stays neutral in property disputes and will only give control back to the employer if it receives a court order.

WHAT RIGHTS DO YOU HAVE IN YOUR DOMAIN NAME?

Having a clear right to exclusive use of a trade name that corresponds with a corporate domain name can be a basis for re-gaining control of a stolen or lost domain name. If Hicks Morley, for example, discovered that a departed employee had registered "hicksmorley.com" in her name, it might be able to have the name transferred back into its name based on its longstanding use of the distinctive trade name "Hicks Morley" and its longstanding use of design marks that feature the words "Hicks Morley."

Although trade-mark protection is important, it may not be a sufficient basis for a remedy in all cases of domain name theft.

In fact, in most cases of departing employee domain name theft, a trade-mark claim (if it exists at all) will be secondary to a stronger claim based on control over the domain name itself. The primary claim in its essence is as follows: "(1) You registered it for us in the course of your employment, (2) had control of it for us, (3) had no authority to transfer it beyond our control for any purpose and (4) had a duty to give it back when we asked for it." This claim (which is based on legal obligations that flow from the employment contract and the law of trespass to property) is much stronger than a trade-mark claim because it does not depend on establishing of any of the prerequisites associated with a trade-mark claim such as distinctiveness and prior use in commerce.

As practitioners who practice in employment law and litigation and who do not advise on the specialized law of trade-marks, the point we wish to make is that the protection of your domain name is as much a matter of managing employees as it is managing intellectual property. If you can manage employees to lay the basis for the four-part claim we have described above, you will protect yourself from employee domain name theft.

WHAT ARE PRACTICAL STEPS FOR PROTECTING A DOMAIN NAME?

There are many more things you should do to protect your domain name than we can cover in this bulletin, but by controlling for the risk of loss to a rogue departing employee you will close a significant security gap. In this regard, we have four suggestions.

1. Always ensure the domain is registered in the company name. From a registrar's view, you do not have any right to control a domain name for which you are not the "registrant," so an employee should never be allowed to register a

domain name in his or her own name. Never! And if you do not know whether your website is currently registered in the company name, do a check right now by going to any registrar's website and searching the publicly-available record for your domain name. In common parlance, this is called doing a "whois" lookup.

2. Control the user name, password and administrative contact e-mail. We have searched, but have not been able to find a registrar willing to offer a system for authorizing changes that involves two people (so they can watch each other). This means any employee with your security-sensitive domain name information will likely have an ability to make unilateral changes to your domain name registration record in order to deprive you of control. Hence, the fewer employees with this information the better and such employees should be both senior and trustworthy.
3. Record the authorization. Your ability to prove that you have a right to your domain name that supersedes any right enjoyed by the employee who administers it for you will depend on the circumstances in which you have assigned that employee his or her duties. Make sure it is clear that your domain name administrator only controls the corporate domain name in the course of his or her employment duties and on the company's behalf. Ideally, you will address the risk of domain name theft in the employment contract, job description and in all written instructions. Also, do not let an employee pay the registration fees for a domain name on the company's behalf. Never!
4. Choose a registrar within the province that will help in the event of trouble. Most registrars will stay neutral after a domain name is hijacked and will only turn it back after a court order. With this in mind, you should still pick a registrar who is accessible by phone, has a physical presence nearby and at least expresses a commitment to provide information should you have a problem. Since you will benefit from a court order that binds the registrar in the event of theft, you should pick one resident in the province.

HOW LONG WILL IT TAKE TO OBTAIN A COURT ORDER?

If your website and e-mail server goes down, the best means of securing prompt relief is to file a court action and seek an order to restore the domain to your control. To succeed, you must show (1) that there is a serious issue to be tried, (2) that you will suffer irreparable harm if relief is not granted and (3) that the balance of convenience favours the granting of relief.

Although it should be relatively easy to meet the three-part test for an order in most cases, obtaining an injunction is never an easy feat. All the ordinary litigation risks are amplified because of the rush to court. Also, even if evidence can be marshalled and materials prepared quickly, it can take time to secure an available judge. The time-to-court risk will vary depending on the court in which you file your action, but in Ontario will likely range between one and five days.

The expectable time delay in recovering a stolen domain name means two things. First, you should have an emergency/contingency plan in place that identifies who does what in the event your domain name is stolen. And second, where the costs of disruption are expected to be high, if you anticipate a problem with an employee who has control of a domain name you should consider preparing for an injunction in advance of any confrontation. The cost of preparing for the worst and not having to act may outweigh the downside risk.

CONCLUSION

Domain name theft by rogue employees is a real problem with extreme consequences. As we have explained, it is also very unlikely that your registrar is watching your back. We encourage you to take the steps needed to minimize your risk. We would be glad to help.
