Digital Dilemmas:
Protecting your Digital Property

Part 1 of a Series on Digital Assets (May 7, 2014)

Protecting Personal Information

The extent to which we interact with digital information is increasing quickly. Smartphones are nearly ubiquitous and can now track our whereabouts, decide what advertising we receive, control our homes' thermostats and even water our lawns from the other side of the world. Many of us now have a digital "presence" through the likes of social and professional networking sites, blogs, discussion boards, and on-line games. Our digital-selves persist after we log off and even after we die. And of course, there are now digital assets that carry real economic value. While largely beneficial, this digital immersion raises a host of new questions about security, legal rights and governance.

A subsequent installment of this series will address planning for our digital assets but this bulletin focuses on security, which has yet again been in the headlines recently with the emergence of the Heartbleed bug and the Internet Explorer bug.

Internet Explorer Bug

What is it?

A major bug was discovered in Microsoft's Internet Explorer web browser over the course of the past few weeks. The bug affected all versions of Internet Explorer and allowed attackers to install malware on your computer to steal personal data, track online behavior, or gain control of the computer. The bug was so severe that the United States and British governments recommended that people temporarily stop using Microsoft Internet Explorer.

Microsoft recently issued a 'patch' to fix the bug for Internet Explorer versions 6 through 11 (essentially all versions of the browser currently in use). Most Microsoft Windows users have "automatic updates" enabled, which will download and install the patch without the user having to take any action. To ensure that the patch is downloaded, though, you should visit the Microsoft website and search for any available software updates.

Windows XP

Note, as well, that Microsoft recently stopped supporting its oldest operating system, Windows XP. Although Windows XP is over twelve years old, some outlets have reported that 26% of all Windows users are still using the operating system. If you are still using Windows XP, be aware that, except for the patch described above, Microsoft

will no longer be releasing security updates to the operating system. We suggest upgrading the operating system if possible, or, if not, purchasing a new computer.

Heartbleed Bug

What is it?

Last month, a serious encryption flaw in the coded language used by many popular websites and encryption services was discovered. Called the Heartbleed bug, the flaw potentially exposed private account information – user names, passwords, credit card numbers and banking information – over a two year period.

While we immediately think of our email accounts and on-line banking as areas of vulnerability, the Heartbleed bug's reach extends much further than that. Certainly, many websites use the coded language that the bug targets, but so do numerous other electronic devices, such as televisions and wireless routers.

It is not clear if the sensitive information was indeed taken by anyone, but the ability to access it caused numerous tech firms and website owners to patch their systems. Some companies, including the likes of Apple and Dell, just updated certain of their products last week to address the security issue. As of April 17th, there were still over *150 million* vulnerable apps running on the Android platform. The fallout from the Heartbleed bug is likely to continue for the foreseeable future as companies patch their systems and address the breaches that did occur.

If you have been waiting to address the problems caused by the Heartbleed bug, now is the time do it.

What can you do?

From a consumer's perspective, addressing the flaw is largely out of our hands. We are reliant on individual companies to update their sites and software and investigate potential breaches, and on developers of the web language itself to address the problem.

That said, there are certain precautions that all of us should immediately take to guard against harm caused by the Heartbleed bug and minimize the potential for future security leaks.

- First, take a moment to assess what you use.
    - *What websites do you regularly use that require log-in information or have sensitive data, like a credit card number, stored on them? What electronic devices are in your house, including less obvious ones like a television?*
- Second, once a company has patched its site, you should change your password.
    - *An internet security firm recently reported that the 1000 most widely accessed websites have all been fixed, which means that it should be*

safe to change your password on most sites. Any password changed before the flaw is patched will still be vulnerable. Perform a quick web search to see if a company has updated its website; many will not proactively disclose this to you because they do not want to draw attention to their vulnerability in the first place.

- Third, update software.
    - *For devices running software, like a phone, cable box, e-reader or computer, you should update the software when such updates are available. Providers generally will alert you when new software is available (think the Windows updates that appear in the lower right hand corner of your computer, or Apple using a pop up message that appears on your phone).*
- Fourth, be proactive.
    - *As you continue to log-in to websites over the next few weeks, simply remember to check if you've updated your password. For some sites, like that of a specific retailer, we might not log-in all that often, so as you do, be sure to update your information.*
- Fifth, be vigilant.
    - *Proactively check your credit card and banking accounts over the next several months and be watchful for any irregularities, and periodically review your credit report.*

We advise you to change your passwords for all sites that you regularly use and continue to monitor your bank accounts and credit cards over the next several months for any unusual charges.

For more information please contact your Hemenway & Barnes attorney or the author of this advisory:

Dennis R. Delaney
Hemenway & Barnes LLP
60 State Street, 8th Floor
Boston, MA 02109
617-557-9722
ddelaney@hembar.com
www.hembar.com

Kevin M. Ellis
Hemenway & Barnes LLP
60 State Street, 8th Floor
Boston, MA 02109
617-557-9736
kellis@hembar.com
www.hembar.com

Hemenway & Barnes LLP