Cybersecurity . . . How Important Is It?

By Judge Herbert B. Dixon Jr.

When several unrelated high-profile events occur within a short interval relating to a single topic, folks might want to take notice of the issue and consider the possibility that the topic might be really important. Several events during a three-week interval this summer caught my attention and inspired me to write this column. First, the president of the United States took the unprecedented step of writing an op-ed piece for the *Wall Street Journal*. Second, the person who heads both the National Security Agency and the newly created U.S. Cyber Command appeared as the guest speaker at the annual convention of extremely talented computer hackers. Third, newly installed American Bar Association President Laurel Bellows announced the priority issues to be addressed during her presidential term. And, lastly, a nationally known technology writer was the subject of and wrote about a very disrupting and embarrassing personal experience. The topic in each of these high-profile events? Cybersecurity—also associated with variations of the name such as cyberwarfare, cyberterrorism, and other cyber-names that refer to computer hackers stealing, sabotaging, crippling, or destroying someone's computer operations or digitized files.

The President of the United States Writes an Op-Ed on the Importance of Cybersecurity

During the summer of 2012, President Barack Obama wrote an op-ed article in the *Wall Street Journal* to urge passage of the Cybersecurity Act of 2012, a bill pending in the Senate to establish cybersecurity standards to prevent large-scale cyberattacks on the nation's critical infrastructure.[1] The president wrote about the possibility of unknown hackers inserting malicious software into the computer networks of private-sector companies that operate most of our transportation, water, and other critical infrastructure (including electrical grids) and the nation's financial, energy, and public safety systems. The president warned that foreign governments, criminal syndicates, and lone individuals probe our financial, energy, and public safety systems every day. He gave an example of a water plant in Texas that disconnected its control system from the Internet after a hacker posted pictures of the facility's internal controls. And, in urging enactment of cybersecurity legislation, the president wrote about recent penetration of the networks of companies that operate natural-gas pipelines. He noted that computer systems in other critical sectors of our economy, including the nuclear and chemical industries, were being increasingly targeted. The president proffered that taking down vital banking systems could trigger a financial crisis; that the lack of clean water or functioning hospitals could spark a public health emergency; and that the loss of electricity could bring businesses, cities, and entire regions to a standstill. Finally, to emphasize his demand that Congress pass the Cybersecurity Act, the president drew an analogy that because nuclear power plants must have fences and other defenses to thwart a terrorist attack, water treatment plants must test their water regularly for contaminants, and airplanes must have secure cockpit doors, it would be the height of irresponsibility to leave a digital backdoor wide open to cyber adversaries.

U.S. Intelligence Agency Leader Is Featured Speaker at Computer Hackers' Convention

Another news item I noted during this one-month interval was about Gen. Keith Alexander, who heads both the National Security Agency and the newly created U.S. Cyber Command. He made an unprecedented appearance as the featured guest speaker at the 20th annual meeting of one of the oldest and largest gatherings of computer hackers, the DEF CON® Hacking Conference.[2] Gen. Alexander spoke about his support for the Cybersecurity Act of 2012 and the country's need for the skills of the white hat hackers[3] to secure cyberspace. In several speeches leading up to this appearance at the DEF CON conference, Gen. Alexander spoke about a 17-fold increase in cyberattacks on U.S. infrastructure since 2009, going from nine in 2009 to more than 160 in 2011. He was concerned that increases in foreign cyberattacks on the United States were aimed at "critical infrastructure." And, on an ominous note, Gen. Alexander estimated on a scale of 1 to 10 that the nation's preparedness for a large-scale cyberattack was "around a 3."[4]

ABA President Adopts Cybersecurity Priority Initiative

At home in the American Bar Association during this same one-month interval, ABA President Laurel Bellows announced cybersecurity as one of her priority initiatives.[5] She created a task force to help identify and address the cybersecurity and cyber-espionage challenges posed by criminals, terrorists, and hostile nations to our own country's security, as well as to that of private industry and law firms. The task force is charged with reviewing potential cybersecurity threats and national plans to confront them; reviewing information-sharing practices between and among government and private industry; reviewing the legal framework for addressing cybersecurity, particularly in the context of a substantial cyberattack on critical infrastructure; and providing advice on best practices to help law firms protect their clients while safeguarding U.S. interests.

Prominent Technology Writer Is Victim of Malicious Hacking

The last of the four matters that caught my attention was a series of blog posts

and articles by and about an epic hacking experienced by Mat Honan, a prominent and highly respected technology writer.[6] It seems that Honan was playing with his infant daughter one evening when his iPhone suddenly powered down. After he plugged it in to recharge, the iPhone spontaneously rebooted to the initial setup screen. He discovered that his iPhone was blank. It was missing all its data! Honan went to his iCloud account to restore his phone, but he could not gain access to that account. Next, Honan opened up his MacBook and received an iCal message advising that his Gmail account information was wrong. Then, the MacBook's screen went gray and asked for a four-digit PIN (personal identification number). Honan had no idea what this request for a four-digit PIN was about because he had never established such a PIN.

Honan knows a lot more about his digital devices than the average consumer. During his years as a technology writer, he has met many knowledgeable persons working in the technology manufacturing and service-providing industries. He reached out to them, and some were able to assist in his effort to reclaim his digital life. With their assistance, he slowly regained access to his various devices and accounts.

Once Honan restored his iPhone data, he found he could not make or receive calls because not only had he lost access to his Gmail account, but also to all other Google services, including his Google Voice account, which was connected to his phone. When Honan finally regained access to his Twitter account, he found horrific damage, namely, racist and homophobic Tweets and taunting messages under his Twitter name aimed at other hackers. Honan later learned that many of his followers and friends were trying to alert him that his accounts had been hacked. Understandably, he did not receive these messages until later because he was locked out of his accounts. There were many more indignities that Honan suffered trying to put his digital life back together that I don't need to detail here. You get the point.

As a result of this experience as a hacking victim, Honan was missing a tremendous amount of data and documents, including irreplaceable pictures of family—his daughter's first year and relatives who had passed—and eight years of messages in his Gmail account. Later, Honan learned that the real objective of the hacker was access to Honan's Twitter account. Later, the hacker contacted Honan through Twitter bragging about his accomplishment and also expressing regret for the severe disruption to Honan's life. Honan learned that the hacks were not exotic and sophisticated computer hacking techniques but exploitation of known weaknesses by the hacker while armed with easily acquired information—a billing address and the last four digits of a credit card on file.

At the risk of oversimplification, this is how Honan's digital life started to unravel. The hacker first came across Honan's Twitter account, which then led to Honan's personal web site, which then led to his Gmail address. The hacker went to Google's account recovery page and entered Honan's Gmail address. This revealed a partially obscured Me.com alternative e-mail address that was set up for account recovery. This revelation was a clue to the hacker that Honan had an Apple ID account. At some point in the process, the hacker called Amazon claiming to be Honan and requested to add an additional credit card to the account (a fake credit card number). After Amazon accepted the new credit card number, the hacker immediately called back to Amazon advising that access to the account was lost. The hacker provided Amazon with the new credit card number that was given in the previous call and the billing address and then requested to add a new e-mail address to the account. Next the hacker accessed Honan's Amazon account on the Internet requesting a password reset e-mail, which he received. After gaining access to the Amazon account, the hacker was able to see the last four digits for all credit cards on file for Honan. Next the hacker called Apple tech support with Honan's address, Apple ID, and last four digits of credit cards and reported that he could not get into his Me.com e-mail. In response to this call, Apple issued a temporary password, which allowed the hacker to permanently reset Honan's Apple ID password. Later, the hacker saw a Gmail password recovery e-mail in the Me.com mailbox. Gaining more information along the way, the hacker then reset Honan's Twitter password and then used iCloud's "Find My" tool to remotely wipe Honan's iPhone, iPad, and MacBook. Finally, the hacker deleted Honan's Google account. Honan learned that although the hacker's ultimate target was the Twitter account, the purpose of the data destruction in the various devices was to make it difficult for Honan to get back into this Twitter account.

The good news? Honan eventually recovered a significant amount of his data, documents, and information after employing the services of recovery specialists to resurrect, to the extent possible, the erased data and documents from his computer hard drive. The data recovery folks were able to recover Honan's prized photo with his then-newborn daughter.

What Are We Mere Mortals Supposed to Do?

There are thousands of reported instances where the computer systems of major businesses have been hacked. There are also thousands of instances of computer hacking of major businesses that have not been reported, due to either embarrassment or ignorance that hacking has occurred. The instances of cyberattacks are neither rare nor benign. They are persistent

Judge Herbert B. Dixon Jr. is the technology columnist for *The Judges' Journal*, co-chair of its Editorial Board, and a member of the ABA Journal Board of Editors. He sits on the Superior Court of the District of Columbia and is a former chair of the National Conference of State Trial Judges. He can be reached at Herbert.Dixon@dcsc.gov. Follow Judge Dixon on Twitter @Jhbdixon.

and potentially destructive. They include unexpected e-mail attachments from unknown individuals containing malware designed to steal or destroy your digital files and destructive e-mail attachments and Internet links that appear to be from trusted friends. Cyberattacks have been waged against every type of institution in the United States, e.g., federal agencies (including the CIA and the FBI), cybersecurity companies, defense and intelligence contractors, the United Nations, banks and other financial institutions (including Nasdaq, VISA, Mastercard, and Paypal), social media sites (including Facebook and LinkedIn), and law firms (which are particularly valuable targets because of the client information contained in the law firms' files).

This column is not intended to enlighten government agencies or major businesses. I am writing for mortal individuals like myself and readers of this column. To the extent that I have gained your attention, let me be the first to advise that achieving cyber-safety in today's world by totally disengaging from e-mail and the Internet is not a practical solution. So, the next best thing is to adopt cybersecurity practices that will enhance your chances of avoiding cyber-victim status. Some of the practices are commonsense, some are easy to implement, and others will be a nuisance. Here are a few suggestions:

- Don't use the same password on multiple accounts, services, and devices. Once the hacker has obtained that password, it will be among the first to be attempted with future hacking attempts directed at you.
- Install antivirus software. Hasn't everyone done this? And download the latest virus definitions frequently.
- Establish answers to password retrieval questions that are likely unknown to a hacker or anyone who has conducted research about you.
- Use complex passwords with numbers, symbols, and uppercase and lowercase letters. For example, we have learned from a review of more than 6 million leaked LinkedIn passwords that the four most common passwords in that database were "password," "123456," "12345678," and "1234."[7] According to the Web site howsecureismypassword.net, any of these passwords could be cracked almost instantly by a knowledgeable professional or novice with the correct tools. The same goes for any password that is a mere series of numbers (including telephone numbers, dates, house numbers, etc.), a series of letters, or a word from a dictionary. Also, merely adding your initials to a set of numbers would extend the cracking effort from nearly instantaneous cracking to about 19 seconds of effort. On the other hand, if you use numbers, symbols, and uppercase and lowercase letters, something like "1234hBd$#@!" ("1234," followed by my initials "hBd" with one letter capitalized, followed by "$#@!," which is 1234 in reverse holding the shift key), it would take a desktop PC about 4,000 years to crack the password. If my initials were all lowercase or uppercase, that would drop the time to crack the password down to 48 years. And, yes, a longer password with similar variations is more secure. If I merely add an additional four digits (year, house number, last four digits of a telephone number, etc.) to establish a password of "1234hBd$#@!2012," the Web site howsecureismypassword.net advised me that it would take a desktop PC 157 billion years to crack the password (if only I should live so long).
- Enable two-step verification if available. Google offers this option whereby you enter your password and a second verification code is sent to your cell phone or generated by an app on your smartphone. Dropbox offers a similar option.
- If you think you will have difficulty keeping up with all those complex passwords, install a password keeper app or program. Some basic programs can be obtained free. And they are much more secure than writing the passwords on sticky notes that you put on your desk or computer monitor.
- Ignore e-mails from banks and other financial institutions that tell you your account has been frozen because, when you click the link, you will be directed to a fake Web site, which will capture and use your ID and password once you try to sign in. If you want to satisfy yourself whether the e-mail is a scam, pay a personal visit to your financial representative (or, at a minimum, make a telephone call to them to ask about the e-mail you received). The same advice goes for e-mail attachments or Internet links in an e-mail from folks you don't know. Also, be sure to exercise caution with e-mails from people who you do know, especially when the e-mail is not typical of the type they have sent you in the past. If you are the least bit suspicious, reply to the e-mail or call the friend to see if he or she actually sent you the e-mail. Your contact with the friend about the suspicious e-mail you received may be the friend's first notice he or she has been hacked.
- Lastly, back up your digital files. You've heard this before. Mat Honan, the technologically astute hacking victim discussed earlier, embarrassingly admitted that he failed to make a backup copy of many of his treasured personal files. Now, after his experience as a victim of malicious hacking, he backs up his digital files in multiple locations.

A hint to the wise is sufficient. ■

Endnotes

1. Barack Obama, Taking the Cyberattack Threat Seriously, WALL ST. J. (July 19, 2012), http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html.

2. Lucian Constantin, NSA Chief Asks Hackers at Defcon for Help Securing Cyberspace, PC World, July 28, 2012, available at http://www.pcworld.com/article/260007/nsa_chief_asks_hackers_at_defcon_for_help_securing_cyberspace.html.

3. "White hat" hackers are persons who can identify a security weakness in a computer system or network but, instead of taking malicious advantage of it, expose the weakness in a way that will allow the system's owners to fix the breach before others can taken advantage of it. White Hat, Searchsecurity (June 2007), http://searchsecurity.techtarget.com/definition/white-hat.

4. David Sanger & Eric Schmitt, Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure, N.Y. Times (July 26, 2012), http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html.

5. American Bar Association Names Illinois

Lawyer Laurel Bellows President, ABA (Aug. 7, 2012), http://www.americanbar.org/groups/leadership/office_of_the_president/laurel-bellows-biography.html.

6. Mat Honan, How Apple and Amazon Security Flaws Led to My Epic Hacking, Wired.com (Aug. 6, 2012), http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all.

7. Similar research regarding four-digit ATM, debit card, and mobile phone PINS reveals that over 1 in 10 people use the PIN "1234."