Pete Burke on Cybersecurity and the Law

Why the People Need WWII-Type Cybersecurity Drills

Edmund B. (Pete) Burke is an attorney whose special experience is in the areas of software and technology law and e-commerce.

UBIQUITY: How did you first get interested in cybersecurity?

BURKE: Somewhat by accident. I had a couple of cases involving the Federal Computer Fraud and Abuse Act, and naturally developed further interest in cybersecurity, and cyber terrorism to boot. Cyber terrorism issues certainly have become a lot more pronounced and important since September 11, and I think it's an area that's largely ignored by the general populace.

UBIQUITY: How would you characterize your own specialty?

BURKE: Computer technology law, software information law. Legal issues and computing.

UBIQUITY: These cases you mention came up in what way?

BURKE: I had a couple of clients who had been hacked, as well as some who wanted some advice on establishing internal procedures against disloyal employees, for instance, who were, or might have been, engaging in hacking.

UBIQUITY: So how did you approach these subjects?

BURKE: Just through general reading, and research on the Internet, and I came to the conclusion that our cybersecurity as a nation is extremely vulnerable. This is appreciated by the government, which has established several offices that deal with this problem, but I don't think the general populace is particularly attuned to the entire question of cybersecurity and what we're now calling cyber terrorism. I think there's been a lot of interest in hacking -- that is to say, random acts by various people who aren't necessarily combined in an organization but who hack either for personal gain or sometimes just for the thrill of it. Most of the stories we've seen in the press have related to what we would call hackers, but we fail to appreciate the real risk that's posed to our economy and our social system by coordinated attacks by a better trained and more dedicated enemy who is intent on crippling our information technology facilities.

UBIQUITY: Why hasn't it happened already?

BURKE: Although not on a very large scale, we have had some various cyber attacks, including ones against government facilities. Granted, we've really not had a major league catastrophe and or even one that's gained much public attention, such as September 11th has, but that kind of catastrophe may be just a matter of time. The Internet creates such an opportunity for terrorists that we should be astonished that we haven't suffered an information-system Pearl Harbor yet.

UBIQUITY: What might an information Pearl Harbor look like?

BURKE: Perhaps a coordinated and systematic attack over a considerable period of time, by organized cyber terrorists working under the direction either of foreign governments or foreign terrorist organizations, with specifically the intent to impair or cripple our information systems. The ways that can happen are innumerable. Denial-of-service attacks would only be one of many attack strategies. I think we'd also look for coordinated attacks against thousands of important facilities -- including private corporations as well as government facilities -- for the purpose of bringing those systems down or just creating enough havoc and chaos so that they're continually in a state of disrepair.

UBIQUITY: What do you think is the reason that companies and people don't take many steps to do anything about it?

BURKE: Actually, I think many companies have taken serious steps, but the general populace is largely unaware of the degree of the risk, or even the threat. It's common for people to have all sorts of spyware and other unauthorized programs on their computers, and some of those could easily be malicious. We've not appreciated that cyberspace is really an extremely important national resource that should be protected and husbanded, as we do our national parks or other important resources. The great tradition in the Internet and computing has really been to see the Internet as the Wild West. What do you need to get on the Internet, after all? You don't need any sort of permission from anyone; all you need is an Internet connection and a computer that you can get in your local Best Buy store. We're eventually going to have to look at some social decisions about having to trade off, perhaps, what we view as our inherent freedoms to use the Internet, against security.

UBIQUITY: What kind of tradeoff?

BURKE: Well, there's no requirement or even any sense that people should have any sort of education or training before using the Internet. We wouldn't think of letting people use our highway systems without having some sort of training. In fact, every state requires that drivers be licensed -- that they pass a specific test to be permitted to drive a car. Our cyberspace is just not generally viewed as a national resource that we need to protect. Anyone can use it with absolutely no training or supervision. We wouldn't think of allowing our highway systems to be used like that, and we accept the notion that some sort of supervision is required to be able to use the roads, because in doing so you pose a danger to other people.

UBIQUITY: Is that the essence of the problem -- untrained users?

BURKE: I think it's a large part of it. There's no general national program to try to educate users, other than some rather episodic government attempts to sponsor seminars and spread information. People are largely unaware of the risks that their own systems impose on the Internet. As I say, we still view the Internet as the Wild West, with cowboys riding across the range, free to go wherever they want and do whatever they want. Sure, there are some restrictions imposed by the law about hacking into other people's systems, but these are not effective sanctions, and we don't have a sufficient "war mentality" about the Internet. We fail to appreciate that it is extremely vulnerable to terrorist attack, and the general public treats it with more or less indifference. We take it for granted. During wartime, at least in World War II, we had civil defense. We designated civilians who were charged with responsibilities and organizing civil defense and acting even as air-raid wardens. We

have nothing like that in computing. It hasn't come to us yet that we have this incredibly vulnerable resource that can be attacked by our enemies. We're just completely ignorant or complacent about that.

UBIQUITY: And what would you propose as a solution?

BURKE: The first step probably has to come from the government, and we need to escalate cybersecurity in terms of our national priorities. How many times during the recent presidential debates did either candidate mention the issue of cyber terrorism as a threat to the nation, as a component of the war on terrorism? To me, that should be at the top of the list, but it certainly was not on the list of anybody's important issues. But it is at least as important to our security as the war in Iraq.

UBIQUITY: You talk of the need for giving people better training, which sounds a bit like computer literacy programs. How would you judge the success of the various computer literacy programs that have been developed over the years?

BURKE: I'd say moderate at best. I don't know that people in general even appreciate that when they using their computer systems to engage in Internet commerce they are participating in an overall system that could be collapsed through a series of dedicated attacks. Our computer literacy programs are focused more on teaching people to be more effective with computers in a general way. But even though people are familiar with things such as anti-virus programs, industry surveys show that most people don't use those very regularly. All of the efforts are episodic and uncoordinated. Someone in authority must announce that this is an important issue for our national security. This is as important as having a strong military, this is as important as having a vibrant economy, this is a part of an infrastructure that supports our entire way of life. And we can no longer take it for granted.

UBIQUITY: Suppose we could make you the czar of a new program to accomplish this?

BURKE: No, I think it needs to stem from the presidential level, not just from the government bureaucracy, because it's really a matter of public awareness, concern and attention. And in our system, when you really look at it, that's what a President is for. There already are government officials who are charged with these responsibilities, but it doesn't get any degree of public attention, simply because the horrible thing hasn't happened yet. You know, we always wait for the horrible things to happen, and then we get real concerned about them. But we haven't had an information Pearl Harbor -- we haven't had days or weeks of impossible Internet service throughout the country; we haven't had thousands and thousands of people's homes, computers, files and financial information corrupted in a single attack; we haven't had banks being overloaded by thousands and thousands of e-mails and telephone calls from customers whose accounts or ability to connect to the Internet has been disrupted. The possibilities are really beyond imagination, and the challenge is not so much a need to establish government programs or bureaucracies but to create an overall public awareness that cyber terrorism is a real issue. It is one that we're very vulnerable to and that is going to happen. I don't know how someone just looking at the world as it is, and at the Internet as it is, can fail to believe that we are going to be attacked, seriously and catastrophically. Before the United States entered World War II it was appreciated by our political and military forces that the Japanese were planning to attack, but we didn't know where, and we didn't know when. Few people really expected an attack on Pearl Harbor, which was

not the most obvious target. We're just cruising for the same sort of incident with our information security, and I'm chagrined that the highest leadership in this country shows no interest in trying to educate the public.

UBIQUITY: So what would you do?

BURKE: I would say, "Mr. President, I want you to call a news conference call tonight for 8 o'clock. I want you to notify all the networks, tell everyone this is critically important for our national security. And address the nation and say, 'My fellow citizens, we face a tremendous threat to our national security and economy and to our entire way of life. We desperately need your help. We need for every American to do his or her part, and for that purpose I'm taking the following actions...'" Because of the pervasiveness of computers, the problem is too big for government to handle by itself, so we need organized citizens' committees and citizen actions that are sanctioned, sponsored and supported by the government. We're in a war condition. We just haven't been attacked yet, so we don't appreciate that. As always happens, we won't until we have another Pearl Harbor. I just wish we could learn from our own history.

UBIQUITY: You don't think this is an area where the level of required expertise is really fairly high?

BURKE: That's a good question. Many people in the overall computing community don't possess sufficient expertise, and that's part of the problem. We have millions and millions of casual Internet users, and, returning to the highway analogy, we have millions of people driving around in automobiles with no idea what speed limits are, how to signal for a left turn, what to do if they get in an accident, and so forth. They don't even have any real appreciation of the risk involved.

UBIQUITY: But in the case of cars the risk is generally a fairly limited one, just involving a few cars at a time.

BURKE: Right, and because of the nature of the Internet, it's as if we had millions of people driving on the road at the same time -- they all get into one tremendous traffic accident that jams our national highway system. We see our national highway system as a defense resource. The Interstate Highway Act requires that at least 1 mile out of every 5 miles of Interstate highway be straight; the reason for that requirement is so that the highway can be used as a landing strip in time of war. People have forgotten that part of the motivation for creating an interstate highway system was for our national defense. But now the Cold War is over and we have a diffuse and dispersed enemy now, rather than one that's personified in the Soviet Union, and we're complacent about it. I want the President to stand up and say, "Don't be complacent. We're at tremendous risk, we're incredibly vulnerable in innumerable ways. In the not-too-distant future, organized groups of cyber terrorists -- who are well-financed and who are not just a bunch of random kids running around -- with sophisticated tools and knowledge are going to engage in coordinated and sustained attacks on our information system and resources in an attempt to cripple and destroy us."

UBIQUITY: The not-too-distant future?

BURKE: Yes. If thoughtful people don't believe that, they are dreaming in a Pollyanna state of mind. Our information systems are too rich a target for our enemies to

ignore them very much longer. We should be astonished that an information Pearl Harbor hasn't already happened.

UBIQUITY: But what about a solution that would require highly coordinated activity from millions upon millions of people?

BURKE: That's the essence of the problem. We're not ready for the solution because it's not in our history or nature to undertake sufficient measures until we suffer a catastrophe. Look at our Pearl Harbor experience. If you look at how our national perceptions changed after Pearl Harbor, it's really pretty astonishing. We even went so far as to have concentration camps for people who might be considered the enemy, and those procedures were sustained by the courts of the time on the ground that national survival trumps, in critical times, some of our freedoms. We have always cherished our freedoms, but sometimes it becomes necessary to make compromises with those.

UBIQUITY: What specific freedoms would have to be reconsidered?

BURKE: Well, let's return once more to the driver's license analogy for inspiration. Is it really unreasonable to establish a national rule saying that in order to use the Internet a person has to undergo some sort of training or licensing procedure?

UBIQUITY: But wouldn't the training be beneath a fairly low threshold? For example, the licensing procedure would not require a computer science degree.

BURKE: Certainly not, but it would entail people demonstrating an awareness, an ability to use the basic home protection mechanisms that we have. And of course the requirement would be difficult to enforce, because -- even if you had a licensing scheme -- how are you going to stop unlicensed users? It would be a very difficult problem, undoubtedly, but it's an awareness and attitudinal issue. It's important to have a statement that our information infrastructure is a critical national resource and your government needs citizen help to protect it. We should be asking people to help not simply because it benefits them personally, but as a patriotic move to help protect a valuable resource of their country.

UBIQUITY: What would the citizen cyber soldier actually do?

BURKE: The citizen soldier would, first of all, have some responsibility to establish well-recognized security procedures for his own home computing environment. That seems to be an obvious first step. I think we would also have more public education on a community level of users who would combine and coordinate with each other to ensure that their own resources are relatively safe, and are not being high-jacked for terrorist attacks. We would want to educate people on what to do upon the occurrence of an information Pearl Harbor. Ask the average people who are using the Internet about what they would do if the country suffered an Internet catastrophe that affected their accounts: what would be their first reaction? The fact is, we have no idea what they would say or do. In the same way that we have plans for disaster relief when we have hurricanes or other natural disasters, we need to have plans to recover from an information disaster and have those plans recognized by the populace.

UBIQUITY: What about yourself? How do you feel that you are positioned to cope with such an occurrence?

BURKE: Probably better than most, but I'm not sure what I would do in an Internet catastrophe that prevented me from using e-mail or using the computer to do banking or transact business over the Internet. I'm a regular user of anti-virus, anti-spyware, and anti-adware programs, I use firewalls, and I'm fairly consistent in trying to protect my own resources. But what I would do if we suffered a national information catastrophe? I'd be running around complaining like everyone else that my system wouldn't work, I couldn't use e-mail, I couldn't transact business, all of my accounts were closed. I'm not claiming to be a saint by any means. I am observing that we need a plan, the populace needs to be aware of it, and to work on some level of preparedness.

UBIQUITY: You mentioned the civil defense measures taken in World War II, such air-raid wardens looking for German planes in the sky. What would be analogous in the new world of cyber terrorism?

BURKE: That's an excellent question. I'm sure there are government planners who would be far more adept at figuring those things out than I would, but I would advocate some sort of drills as were conducted in World War II. And I think the populace generally participated in those without questions, and without holding a grudge about it, because it was deemed an important thing to do for the protection of the country – not just for their own safety, but for the country. If a threat is perceived as real most people will respond positively and patriotically. We just don't yet perceive it to be a threat. It's terrible to think that we'll have to suffer first, before we're psychologically prepared to take those kinds of actions. Right now I think I'm just one of some voices in the wilderness. I'm afraid that the voices may get louder some day, when we suffer some sort of real, sustained catastrophe, and are not prepared to deal with it or even to face it.

END

More information on Edmund B. (Pete) Burke may be found at www.burkefirm.com

Source: Ubiquity, Volume 5, Issue 40, December 14 - December 23, 2004