

Whack-A-Mole Security: Bad Policy, Bad Legislation

BY DANIEL CASTRO | NOVEMBER 20, 2009

The recent disclosure of a confidential Congressional document has at least one congressman calling for a ban on peer-to-peer (P2P) file sharing software, but a closer look at the problem reveals that this effort would merely be treating the symptoms, not the disease.

First some background. Last month the Washington Post revealed that more than thirty members of Congress and staffers were under investigation for possible ethics violations, including for “accepting contributions or other items of value ... in exchange for an official act.”¹ While this revelation was shocking, perhaps even more shocking was the means by which this information was leaked—the information was downloaded from the Internet. As detailed by the Washington Post and the Committee on Standards of Official Conduct in the U.S. House of Representatives, a low-level committee staffer had saved a copy of a confidential House ethics committee report on her personal computer while working from home.² Unfortunately, the staffer was also running a peer-to-peer file sharing program and inadvertently saved the file in a folder that was shared with other users. By saving the file in a shared folder, the staffer made the document available to all other users on the publicly accessible file sharing network. While only one report from July was reported by the Washington Post,

the Standards Committee noted that the potential disclosure involved several confidential documents.

The initial reaction from House leaders was tempered. The Standards Committee issued a statement reminding House Members, Officers and employees to maintain good information security practices when handling sensitive materials and noted that “no matter how robust our cybersecurity systems are, they remain subject to individual error.”³ The statement also emphasized that the disclosure took place on the staffer’s personal computer, that the staffer was no longer employed by the committee, and that no House information systems were compromised.

Case closed? Not so fast. Some members of Congress are jumping on the media attention surrounding the ethics leak to enact a legislative ban on peer-to-peer file sharing software. Rep. Edolphus Towns (D-NY) has introduced the Secure Federal File Sharing Act (H.R. 4098) which would prohibit the use of peer-to-peer software on all computer systems run by the Federal government or its contractors. In addition, the legislation directs the Office of Management and Budget (OMB) to address the use of P2P software on the home computers of government employees used for work purposes. To be fair, this is not a completely reactionary move.

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington and in the states.

For more information, contact ITIF at 202-449-1351 or at mail@itif.org, or visit www.innovationpolicy.org.



Congress has held a number of hearings over the years detailing instances of sensitive and confidential information being revealed over peer-to-peer networks—including Social Security numbers, financial records, and even location information about a safe house for the first family.⁴ In fact, the latter incident spurred Rep. Towns to first announce his call for a ban on the use of peer-to-peer software on all government networks.

It is hard to fault the Congress for misunderstanding the problem when some of the press reports surrounding the incident have often been misleading or inaccurate. In fact, most of the press seems to blame the disclosure on the peer-to-peer software, rather than on human error or the bad policies and practices that led to the disclosure. And some reports are simply erroneous and reflect a poor understanding of the technology. For example, according to the Wall Street Journal, by using a peer-to-peer network the staffer “allowed someone to hack into her computer and obtain the document.”⁵ That’s like saying by publishing an article on its website, the Wall Street Journal allowed its readers to hack into their web server and read the news.

To be clear, using peer-to-peer file sharing software exposes users to a number of risks. First, P2P software is often used by Internet users to download and distribute copyrighted content, an illegal act for which individuals can and should be held responsible. Second, the files shared on P2P networks often contain malware—viruses, spyware, and other malicious software that can steal the user’s private data and turn an infected PC into part of a botnet. But peer-to-peer software, by itself, did not cause the confidential Congressional document to be leaked to the press.

Some have argued that peer-to-peer software presents a unique threat because users are often unaware that the software is sharing files on their personal computer.⁶ For this reason, Reps. Mary Bono Mack (R-CA), John Barrow (D-GA) and Joe Barton (R-TX) introduced the Informed P2P User Act (H.R. 1319) earlier this year which would require peer-to-peer software to give users conspicuous notice and obtain consent before sharing files from a user’s PC. First, most file sharing software does not share your entire hard drive, but just a few select folders. In addition, P2P software is already evolving and responding to their users’ de-

mands for more control and notice over how files are shared and preventing accidental disclosure of private information. Finally, while more notice may reduce some accidental file disclosures, incidents such as the recent leak of Congressional documents stem from misconfigured settings or operator error, not a lack of notice.

But the legislative response from Rep. Towns is more troubling. The congressman has argued that “We can no longer ignore the threat to sensitive government information that insecure peer-to-peer networks pose. Voluntary self-regulations have failed so now is the time for Congress to act.” However, the committee staffer revealed confidential information by mistakenly saving the document in a shared file folder. This mistake was human error. If the staffer had accidentally emailed those documents—say by inadvertently clicking on the wrong attachment—would members of Congress now be calling for a ban on email? Of course not. The underlying problem is not that the staffer was running a P2P program on her computer, but that the sensitive documents had virtually no access controls on them to prevent their unauthorized use. After the staffer was allowed to take the document home as an unsecured file, the confidential information could have been leaked in many different ways—from a lost USB drive to a stolen laptop to a snooping roommate. If the file would have even had basic password protections enabled, probably none of the ensuing drama would have happened. A properly encrypted file, even if lost or made publicly available, would remain secure and confidential.

Unfortunately, this type of response is typical when organizations face a data breach, as executives scramble to fix the immediate problem without taking time to understand the bigger issues. This whack-a-mole approach to information security problems is bad strategy for an organization and bad policy for the Congress. Good information security practices depend on IT leaders forming a solid understanding of risk and taking action to manage those risks. For example, in this case, the risk here is not peer-to-peer file sharing, but rather inappropriate disclosure of confidential information. A better approach would be to review the policies and procedures for access to confidential information. Questions to ask include:

- Who should be given access to sensitive information?
- Should employees be permitted to take sensitive documents out of the office?
- If so, what controls are in place to ensure that the data stays secure?
- If not, what controls are in place to ensure files remain in the office?
- Are sufficient penalties in place to punish those who violate these policies?
- Are the known risks acceptable, and if not, what else should be done?

Certainly people are not perfect and some data breaches will still occur even with better policies and technology. And prohibiting P2P software probably makes sense for most agencies, but it is only a small part of a bigger problem. Rather than narrowly focusing on P2P, policymakers should be promoting broad strategies for sound information security policies across government. For example, rather than legislate that

government IT executives should have a full accounting of P2P use on their network, they would be better off mandating that these IT executives need to have information security programs in place that give them detailed network intelligence so they can inventory what applications are running on their computers and track suspicious outbound and inbound network connections. In addition, government-wide policies should be developed to promote secure teleworking. As teleworking becomes more common the perimeter for enterprise security becomes wider and the amount of control that IT administrators can exert over remote PCs becomes weaker, thus creating a new threat environment. Government best practices in this area would be helpful to small and large businesses in the private sector.

Policymakers should use this experience as an opportunity to push for substantial progress on information security practices, not merely small mandates banning a particular type of software.

ENDNOTES

1. Carol D. Leonnig, “7 on defense panel scrutinized,” *Washington Post*, October 30, 2009, <http://www.washingtonpost.com/wp-dyn/content/article/2009/10/29/AR2009102904699.html>.
2. Ellen Nakashima and Paul Kane, “Dozens in Congress under ethics inquiry,” *Washington Post*, <http://www.washingtonpost.com/wp-dyn/content/article/2009/10/30/AR2009103001959.html>.
3. “Statement of the Chair and Ranking Republican Member of the Committee on Standards of Official Conduct Regarding Cybersecurity Issue,” Committee on Standards of Official Conduct, October 29, 2009, <http://ethics.house.gov/Media/PDF/Press%2010-29-2009.pdf>.
4. Jaijumar Vijayan, “Details on presidential motorcades, safe house for First Family, leak via P2P,” *ComputerWorld*, July 29, 2009, http://www.computerworld.com/s/article/9136053/Details_on_presidential_motorcades_safe_house_for_First_Family_leak_via_P2P.
5. Brody Mullins, “Leak Offers Rare Peek at Congressional Ethics Probes,” *The Wall Street Journal*, October 31, 2009, <http://online.wsj.com/article/SB125694460088919841.html>.
6. Mary Bono Mack, “P2P survival guide: what users must know,” *The Hill*, May 5, 2009, <http://thehill.com/opinion/op-ed/8129-p2p-survival-guide-what-users-must-know>.