

BLOG POST

10 Million More Reasons to Pay Attention

October 30, 2014

Remember when you were a kid, and everybody was getting ready to play kickball, and there were two captains, and the captains started picking teams, and you kept not getting picked, and then there were just two people left, and you didn't want to be the last one, and ...

Wait, what? No! I am *not* speaking from personal experience! Moving on.

Well, that kid who doesn't want to be picked last? Yeah, that's the FCC. And the sport's not kickball, but data security. Everybody's weighed in on cybersecurity. Just take a look:

- **[FDIC Chairman Martin Gruenberg](#)**: “[I]nternet cyber threats have rapidly become the most urgent category of technological challenges facing our banks. The large number and sophistication of cyber attacks directed at financial institutions in recent years requires a shift in thinking.... it needs to be engaged at the very highest levels of corporate management. (September 22, 2014.)
- **[FTC Chairwoman Edith Ramirez](#)**: “The Commission’s 50 settlements with businesses that it charged with failing to provide reasonable protections for consumers’ personal information have halted harmful data security practices; required companies to accord strong protections for consumer data; and raised awareness about the risks to data, the need for reasonable and appropriate security, and the types of security failures that raise concerns.” (April 2, 2014.)
- **[SEC Commissioner Luis Aguilar](#)**: “Given the significant cyber-attacks that are occurring with disturbing frequency, and the mounting evidence that companies of all shapes and sizes are increasingly under a constant threat of potentially disastrous cyber-attacks, ensuring the adequacy of a company’s cybersecurity measures needs to be a critical part of a board of director’s risk oversight responsibilities. (June 10, 2014.)
- **[DOJ Assistant Attorney General for National Security John Carlin](#)**: “[I]t’s not fair to let the private sector face these threats alone. You are on the front lines of these battles, but we are with you and committed to working with you to protect networks, identify perpetrators, disrupt their efforts and hold them accountable. At the DOJ, it’s among our top priorities.” (October 28, 2014.)
- **[NY Superintendent of Financial Services Benjamin Lawsky](#)**: “Cybersecurity is one of the most important issues the Department of Financial Services will face as a regulator in the months and years ahead across the entire financial system. And you will be hearing a lot more from our agency about this in the near future.” (October 20, 2014.)

- My colleague, [Michael Pegues](#): “Have you read about all of this personal information being stolen? I’m telling you, the whole world went downhill when people gave up on the abacus.”

Okay, I may have made the last one up. But anyway, with the FDIC, SEC, FTC, DOJ, and New York having a grand old time at the bar, you have to figure that the FCC was trying to figure out how to join the conversation without making it too obvious that it hadn’t really come up with anything as of yet to contribute. And I may be [anthromorphizing](#) here, but I think the conversation went like this:

FCC: “Hi guys!”

FDIC: “Oh. Hey.”

FTC: <sigh>

SEC: “Hey.”

DOJ: <grunt>

NY: “Hi there! How are you! I’m New York! Nice to meet you! I like to regulate everything everywhere at any time! Because I’m New York! Want to join us? Here pull up a chair!”

FCC: “Sure! I’d love to! Hey, I was just thinking about you guys when I dropped a [\\$10 million fine for data privacy violations](#) the other day.”

FDIC/SEC/FTC/DOJ (chorus): “Check please!”

That’s right: The FCC has joined the data security arena by popping a pair of two telecom companies with a \$10 million fine for storing personally identifiable customer data online without firewalls, encryption, or password protection. Ouch. According to [Travis LeBlanc, the FCC’s top enforcement official](#), “This is unacceptable.... This is the first data security enforcement action [by the FCC], but it will not be the last.”

Cue the ominous music!

Pretty simple takeaway here, friends, no? If you use – no, if you *have* — a computer at your workplace and have not thought about cybersecurity, you’re going to need to get with the program. Because it is only a matter of time before someone gets into your systems and a regulator wants to talk to you. Maybe even more than one.

Maybe even <gasp!> New York.