DIMACS Highlight: Discussion of Online Security

[October, 2014] On October 9, 2014, DIMACS Director Rebecca Wright testified before members of the New Jersey State Legislature on issues of cybersecurity. Wright was invited to testify before the NJ Assembly Homeland Security and State Preparedness Committee about cybersecurity threats and protecting the public from such threats. Her testimony came in the wake of recent high-profile security breaches at Home Depot and JP Morgan Chase, the latter of which may have compromised information related to 83 million accounts. In her testimony, Wright advised that cybersecurity is complicated and providing protection requires ongoing vigilance throughout the cybersecurity ecosystem. Failing to implement adequate security is becoming more costly both to businesses and to individuals.

New Jersey State House by Marion Touvel via Wikimedia Commons

She advocates that individuals follow commonly given advice to practice good password hygiene, install anti-virus software, check credit and bank statements regularly, and be wary of emails claiming to be from financial institutions. She says that businesses should make security a priority throughout the company. While many businesses have been slow to adopt new security solutions because of their cost, Wright suggests that, with the escalating cost of breaches (both financial and reputational), businesses may gain a competitive advantage from providing strong security to customers. She also notes that the government can play a role in providing guidance to businesses and must play a role in protecting infrastructure.

New Jersey State House, General Assembly Chamber by Niagara via Wikimedia Commons

Wright was also one of four invited contributors to the October 4 “Room for Debate” feature of the New York Times. Also spurred by recent data breaches, the four discussants addressed what it would take to make bank accounts and credit cards secure. All four noted that U. S. businesses have been slow to adopt new technology that allows replacement of traditional credit cards with more secure cards implanted with security chips. Such cards are already used throughout Europe and have been since the 1990s. Plans are now underway in the U. S. to move to E.M.V. technology, a global standard for chip-based cards that makes use of cryptographic authentication, by October 2015. While not without its own risks, if properly implemented, this will raise the bar for attacks and reduce the overall security

risk to customers. As the discussants noted, moving to E.M. V. is a first step, but additional measures that limit retailers' access to purchasers' private data are both needed and available.

Related Links:

- DIMACS: dimacs.rutgers.edu/
- Rebecca Wright: http://www.cs.rutgers.edu/~rwright1/
- Wright's full testimony to the Assembly: http://www.cs.rutgers.edu/~rwright1/Publications/Wright-NJ-testimony-2014-10-09.pdf
- Room for Debate: http://www.nytimes.com/roomfordebate
- Cybersecurity activities at DIMACS: http://dimacs.rutgers.edu/SpecialYears/2011_Cyber/