Cybersecurity & Public Finance

Todd C. Kinney *and* Nicole P. Moriarty

January 17, 2020 | HFA Institute 2020 (Washington, DC)

KUTAKROCK

kutakrock.com

Vulnerabilities for Public Entities

- Housing Finance Agencies have to be concerned about:
  - Protecting HFA funds
  - Protecting borrower and other sensitive data
  - General HFA operations and environment
- Open records and open meeting laws make public entities particularly susceptible to attack
- Cybersecurity issues may impact public and investor trust and issuer credit ratings
  - Cost of responding (often a function of preparedness)
  - Short-term stability and long-term health

Mitigating Cybersecurity Risk

- Training
- Technical tools
- Verification
- Act fast
- Insurance
- Sharing cyber experiences … and resources

Disclosures and Credit Ratings

- Balance between transparency and security and SEC trends
- Growing position that cybersecurity disclosures are material to investors
- Key questions to deal with both disclosure and rating issues:
  - Have you assessed and identified your risk and gaps? How and how often?
  - Are you prepared? How can you demonstrate preparedness (e.g., written plans)?
  - Do you have personnel dedicated to information management or cybersecurity?

Keys to an Effective Cyber Program

- An effective organizational privacy and data security risk management program requires
  - Fostering an organizational culture in which privacy and data security are valued and promoted
  - Providing adequate financial and human resources to build out and maintain a robust information security management program
  - Enforcing programmatic policies and procedures
- Without the full support of management, in these three key areas, effective risk management simply cannot occur

Management Buy-in

- Strategies to foster management engagement:
  - Create a management-level information Security Risk Management Committee
  - Require management participation in security awareness training
  - Track and report security incidents to management on a regular basis
  - Bring in the insurance brokers and underwriters to talk about information security risk mitigation
  - Quantify the risk in monetary and regulatory (penalty) terms

Security Awareness Training

- Privacy and information security training is one area where 100% participation should be mandatory, since organization-wide security is only as good as your weakest link
- Training should be used to communicate and explain company policies that require employee implementation
- Incorporating into training plenty of real-world examples of information security catastrophes is a great way to heighten awareness of the risks!
- Small, digestible content can help reinforce that privacy and data security are an important part of the organizational culture (at least new hire, annual, and refresher training)