Appraisers and Data Privacy

Tim O'Brien - Appraisal Summit 2018

Overview

Appraisers have access to a universe of data in our day to day lives. Often times, we may take for granted the amount of data (and its importance) and we need to ensure that we are safeguarding this data consistent with the expectations of our clients and industry best practices.

Notable Data Breaches

1

Yahoo (2013):

One of the largest data breaches known to have been reported. 3 billion accounts compromised.

2

Equifax (2017):

143 million Americans records breached and several hundred thousand identities stolen.

3

Target (2016):

Hackers installed malicious software on POS systems in Target self checkout lanes. 70 Million identities and 40 million credit cards.

4

Sony Pictures (2016-17)

100 terabytes of stones data and monetary damages estimated to be over $100M. Primarily a phishing attack at Sony employees

Data and the Appraiser

- Appraisers have access to large amounts of data. Some of the categories:
  - Public Records
    - **Risk: Low**
      - Data is available generally to everyone
  - MLS data
    - **Risk: Medium**
      - MLS data is member based, however, more and more services seem to be monetizing this.
  - Non-public Information (NPI)
    - **Risk: High**
      - This is data that an appraiser has access to that a normal person would not have the ability to obtain through public access or membership

NPI Data (Non-public)

- Through the course of an appraisal assignment, the amount of NPI data can be much larger than people expect. Examples of NPI Data include:
    - Loan Number (via engagement letter)
    - Phone numbers and email addresses
    - Lockbox information
    - Blueprints and schematics
    - Alarm information and passcodes
    - Financial and asset documentation
    - Social security numbers
- In many cases, the appraiser may not have asked for (or needed) this information, however, once exposed to the information, must take proper care to protect the data.

Best Practices for Data Security

- History has proven that no system is impenetrable for data security. Instead of trying to perfect the ultimate security system, appraisers should rather take steps to be fully aware of the data they must protect and where potential intrusions can exist.
- The first (and most important step) is identifying and communicating with your clients (and their agents) around data security expectations and requirements.
    - What is permissible?
    - Is there a documented policy around data security?
    - What are red flag and/or hot button issues for people that provide the data to appraisers?

Best Practices for Data Security

- Start local
  - How is your data stored? Media? Cloud? Paper
    - How secure are these features?
    - What controls are in place to ensure unauthorized use?
      - Firewalls
      - Encryption
      - Strong password controls.
      - Padlock
      - A big dog?
  - Look at your hardware. What do you use the most?
    - Where is the weakest link in your data chain?
      - Ipad, Iphone, IWatch? Laptop?
  - Understand the security of your network.
    - Are you using a public network? A private network?

Best Practices for Data Security

- Think Global
  - Where does your data go during an appraisal process?
    - Third party software providers/tools
    - Typing services
    - Virtual Assistants
  - How does your data get there?
    - Network strength
    - Public versus private
    - Foreign versus domestic

Hot Button Topics on Data

- Foreign travel and the security of foreign networks.
  - Vacations - we need them and our clients often times demand the 365 day a year appraiser. How do you balance work/life balance?
- Outsourcing functions to virtual assistants outside the United States
  - What control does an appraiser have when the data leaves the US and ensuring it is not used for other purposes? What recourse will an appraiser have if the data is misappropriated.
- Mobile devices and the security of these devices.
- VPN networks routing through foreign countries
  - VPN networks are generally a secure and positive step towards data security. However, routing through other countries opens the appraiser up to both questions and additional liability.

Things to think about

- Data security is a responsibility for all parties with access to confidential information. For an appraiser, this does not need to be a million dollar investment, rather, an annual review of best practices on how data is managed and protected.
- The lack of a data security plan will not protect someone who causes a data breach. The penalties can be both financial (and potentially criminal) depending on the circumstances.
- Proactive communication with clients is one of the most important ways to prevent accidental data breaches. Understanding what your clients require is a key step toward security.
- Look locally and think globally. Understanding where your data goes and what risks are associated with decisions made in the appraisal process are helpful ways to map out a secure structure.

Lunch!