NCSHA

HFAs AT THE CENTER

AUSTIN 2018 ANNUAL CONFERENCE & SHOWPLACE

Information Security

David Hebert

Managing Director of I.T.

New Hampshire Housing

What Must Be Secured and Protected?

C.I.A. Triad

- **Confidentiality** – of PII and BCI
- **Integrity** – of Authority information systems, data and content
- **Availability** – of information systems

Threats to Information Systems

- Unauthorized access and use, theft of information
- Intentional or accidental disclosure
- Modification, destruction, sabotage
- Disruption

Threat Vectors

#1 - Employee inattentiveness (ex. Accidents, social engineering, phishing)

#2 - Virus or systems hacker attacks

#3 - Physical theft (laptops, devices)

Risks to HFA's?

- Liability – costly negligence claims, mishandling of PII
- Public Relations – reputational damage
- Business Interruption – systems/data unavailable or unreliable
- Others – extortion, ransom

2009 – First NHHFA Formal Assessment

- **Technical Controls Review**
  - Penetration tests – ability to execute malicious code on systems
  - Anti-virus
  - Firewalls
  - Patch management
  - Encryption
  - Password policies
  - Intrusion detection – network logging and monitoring

- **Operational Controls Review**
  - Classification of data
  - Computer/internet use policies
  - Portable device use policies
  - Access policies – least privileges
  - Visitor access
  - Separation of duties
  - Clean desk policies
  - Material controls (electronic & hardcopy)
  - Communications (emailing, faxing, wireless, remote access)
  - Recovery & continuity capabilities
  - Incident reporting & handling
  - Employee awareness training

Recommendation→ Formal Information Security Program

- Formed cross divisional Information Security Committee
- Goal: Develop and implement policies that balance secure handling of information with organizational productivity, and govern toward effective compliance.
- VERY CHALLENGING!

Security Committee

Cross-Operational Security Officers:

- Managing Director Assisted Housing
- Managing Director Administration/HR
- Financial Controller
- Director Homeownership Lending
- Managing Director IT (Chair)
- Director Multi-Family Asset Management

Information Security Handbook

- Follows NIST guidelines
- 70+ pages, covers 3 areas:
  - Management Controls
  - Operations Controls
  - Technical Controls
- Discussions + Deliberations + Decisions
  - Exhaustive weighing of restrictive policy vs. worker productivity
  - Focus on “Due diligence” policies and practices
  - Many business process scenarios to consider, balancing policy vs agility

ONE YEAR IN THE MAKING!

2012 Another Third-Party Security Assessment

- Ethical hacker
- Penetration testing again
- Online Lending web application testing
- Scanned entire network for vulnerabilities
- Detailed review and enhancements to new Security Handbook
- Social engineering – phone attacks, some employees fooled!
- Results: detailed report of critical-high-medium-low vulnerabilities to fix
- **Recommendation: Formal ongoing employee training & awareness program**

2015: Assessing Service Providers?

- Third party providers who take custody of PII (30 +)
- Comply with same due diligence policies as the Authority?
- How to audit or assure compliance?
- Contracted a security firm to assess one new provider
- Developed questionnaire to probe current/future vendors
- Attempts to get the vendor responses were difficult at best
- Engaged an attorney for recommendations
  - Revised Confidentiality & Security Agreement, attached the questionnaire
  - “If provider has passed an SSAE – 16 Soc Type 2 or an ISO 27001 audit no further assessing needed”

2016 - KnowBe4

- Subscribed to KnowBe4 - computer based online awareness training
- Videos, games, quizzes, phishing/vishing exercises
- Phishing tests
  - KnowBe4 – common for 30% casual employee clickers
  - We started at 16% employee clicks (doing internally driven training)
  - Got as low as 3% employee clicks (with subscription to KnowBe4 modules)
- Bottom line – Repetitive, frequent training REALLY HELPS to get employee's attention!

Presently

- Completed new updates and revisions to the Security Handbook
- Upcoming – Release to employees along with announcing new "Digital Workplace" Access Anywhere policies
- Budgeted - another external security assessment, pending many in process changes to systems environment.