Georgia Department of Community Health

Cyber & Information Security

Board of Community Health Meeting December 11, 2014

Presented By: Sherman Harris

Office of Information Security

Date: 12/11/14

Regulatory Requirements

- HIPAA Privacy & Security
- Social Security Administration Security Standards
- HHS/CMS Security Requirements & Standards
- FISMA/NIST Security Standards
- FBI CJIS Security Standards
- State Security Standards
- IRS Federal Tax Information (FTI) Security Standards

Information Security

- What is Information Security?
  - Is it a Technology Issue or a Business Issue?
    - Who Owns the Security Risk to the Department, Business Programs and Data in the Organization?
      - How Does the Office of Information Security Assist the Departmental Leadership Team and Business Owners with Managing Business Risks to their Business Programs and Data?
        - » Governance
        - » Compliance
        - » Policies & Standards
        - » Business Technology Procurements, Contracts, etc.

Business Risks

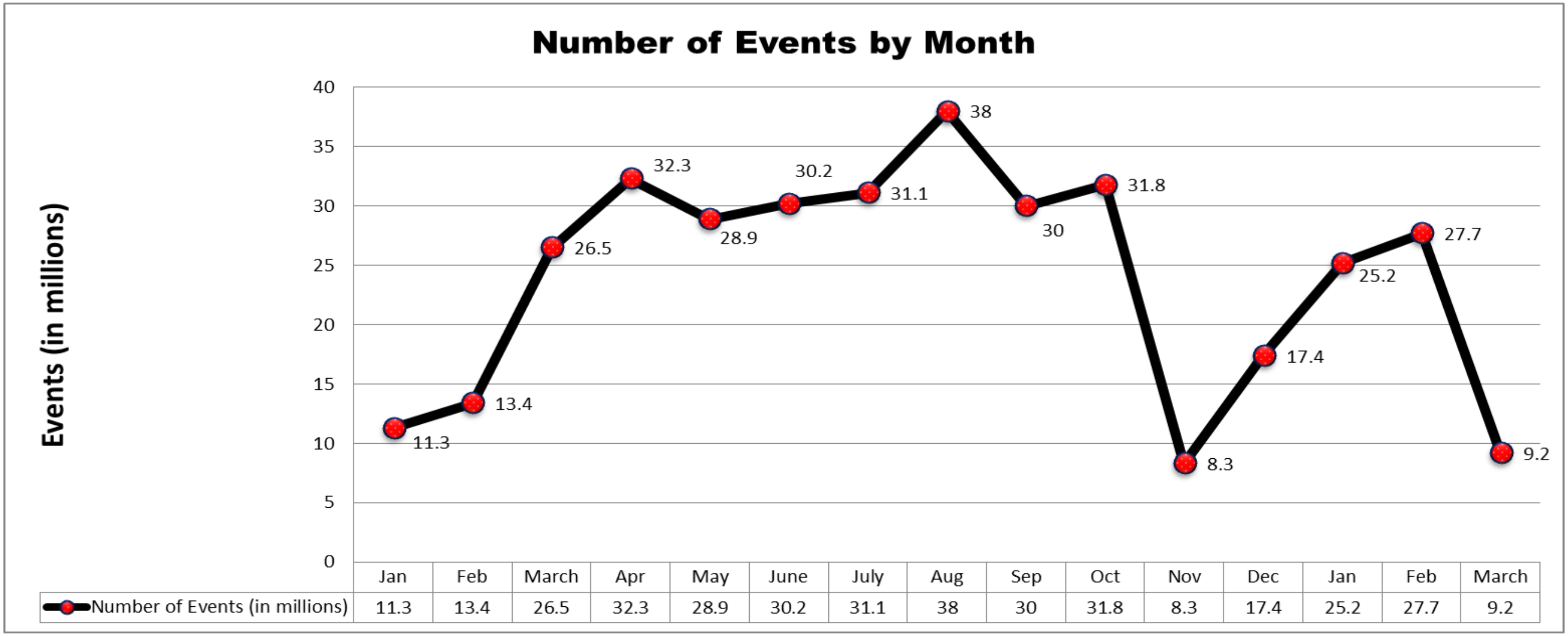
- Business Risks to Information and Data Security Include:
  - ePHI Data Security Breaches
  - Immediate HHS/OCR Notification (Greater than 500 Affected Members)
  - Health Plan Member Notifications, Credit Monitoring, etc.
  - Potential Civil Monetary Fines & Penalties
  - Federal Funding Impacts
  - Impact to Data Sharing Agreements (e.g. CMS,SSA,IRS, etc.)
  - Damage to Image and Reputation of Department (Priceless)

Cybersecurity Risks

- Cybersecurity Risks to Business Programs Include:
    - Network Cyber Attacks
    - Malware Introduced via E-Mail and Internet Downloads.
    - Use of Non-secure WiFi Connections for State Business.
    - Cyber Attacks against Healthcare Business Associates with whom we Share Data: Vendors, CMO's, Pharmacy Drug Partners with Insufficient Security Controls, etc.
    - Cloud Computing Security Standards Not Implemented.

Blocked Cyber Attacks

Intrusion Trends: Jan 2013- March 2014



	Jan	Feb	March	Apr	May	June	July	Aug	Sep	Oct	Nov	Dec	Jan	Feb	March
● Number of Events (in millions)	11.3	13.4	26.5	32.3	28.9	30.2	31.1	38	30	31.8	8.3	17.4	25.2	27.7	9.2

- This document is protected from disclosure by O.C.G.A. 50-18-72(a)(25)(A)(i) (2013) and should be kept confidential to protect the interests of the public.

Georgia Department of Community Health

BUSINESS RISK LEADERSHIP PARTNERS

- Office of Information Security Business Risk Partners Include:
  - Commissioner’s Office
  - Department Management Team (Division Heads)
  - HIPAA Privacy & Security Officer, Sharon King and HIPAA Privacy & Security Specialist, Latrice Thomas
  - Legal Team
  - Office of Inspector General
  - Business Program and Data Owners (Medicaid, SHBP, etc)
  - Procurements Team

OIS BUSINESS PARTNER SUPPORT

- How we assist Leadership and Business Partners with managing program risks:
    - Work daily with State Technology Service Provides, Vendors, State and Federal Business Associates and others to ensure your Data is protected.
    - Implement Security Governance Structure to ensure that Business Compliance Requirements are continually met by the Department, the State, Business Associates, Third-Parties and others with whom the Agency does Business.
    - Address appropriate Security Standards and Requirements in all Business Program Initiatives, Projects, Procurements, Contracts, Grants, and Data Sharing Agreements, etc. involving the use of Technology.
    - Assist with keeping Federal Program Funding and Data Sharing Agreements in Place.
    - Assist with keeping the Department out of the News Media.
    - Audit to Ensure Compliance (Continuous Monitoring).

SECURITY BOTTOM LINE

- How Can We Simplify this Message and Reduce it to the Bottom Line?

  - SECURITY “GOOD” ☺

  - NO SECURITY “BAD”☹

QUESTIONS

- Are There Any Questions?