Behavioral Analytics in Your Healthcare Privacy and Security Program

May 12, 2017
Agenda

• What are Behavioral Analytics?
• Where do Behavioral Analytics fit in?
• Why Behavioral Analytics?
• The People Security problem
• Lessons Learned
• Practical Examples of Behavioral Analytics
• People Security Vision
• Takeaways
Speakers

John Houston
Vice President, Information Security and Privacy, and Associate Counsel
University of Pittsburgh Medical Center

Kurt J. Long
Founder and CEO
FairWarning
What are Behavior Analytics?

Offers profiling and anomaly detection based on a range of analytics approaches, usually a combination of:

1. Basic analytic methods (rules, signatures, pattern matching, other)
2. Advance analytics, algorithms, machine learning

Example techniques:
1. Statistical analysis
2. Data visualization
3. Trends

Application Security Layer

**PERIMETER SECURITY**

**NETWORK SECURITY**

**ENDPOINT SECURITY**

**APPLICATION SECURITY**

**PEOPLE**

**PHI**

Behavioral Analytics
Use Cases
• Patient Investigations
• Forensics
• OCR Audit Controls
• HIPAA Governance
• eDiscovery
Use Cases
• Patient Investigations
• Forensics
• OCR Audit Controls
• HIPAA Governance
• eDiscovery

Use Cases
• Information Security Insights
• Insider Threats
• Compromised Credentials
• Predictive & Preventative

PATIENT PRIVACY MONITORING

BEHAVIORAL ANALYTICS

DETERMINISTIC
BASED IN LAW

PROBABILISTIC
INFORMATION SECURITY
Why Behavioral Analytics?

Misuse of ePHI is prevalent

- IRS Tax Fraud
- Medical Identity Theft
- ID Theft
- Fraud

- Opiate Prescriptions
- Claims Modification
- ‘Snooping’
- Inadvertent Breaches
Cybersecurity & People

Source:
People Security Problems

Verizon Breach Report 2017

“Healthcare has the unenviable task of balancing protection of large amounts of personal and medical data with the need for quick access to practitioners. Internal actors are well represented with employees accessing patient data out of curiosity, or to commit identity fraud.”

“Insider misuse is a major issue for the Healthcare industry; in fact it is the only industry where employees are the predominant threat actors in breaches. Interestingly enough, Figure 20 shows the insiders’ motives are almost equally divided between financial and fun. This is a product of a lot of sensitive data that may be accessed by legions of staff members containing PII —that is perfect for identity theft— and medical history (sometimes of friends or relatives), that is very tempting for enquiring minds (that want to know!).”

Definitions

1. **Unknown User** means – no information other than user ID and password.

2. **Poorly Known User** means – insufficient information to contact user in any way.

3. **Identity Intelligence** - Understanding who the user is, what the user’s role is and what assets the user has access to (and that such access is appropriate).
Collaboration, Legacy Application Architectures and M&A Activity Lead to People Security Problems
Collaboration, Legacy Application Architectures and M&A Activity Lead to People Security Problems

- Non-Employees w/ Access
- Vendors
- Contractors
- Affiliate Physicians

Healthcare System Network:

- Employees
- Non-Employees
- Employees w/ Access
- Ad
- Vendors
- Contractors
- Affiliate Physicians
- Cerner
- MEDITECH
- Epic
- Allscripts
- Office 365
- Salesforce
- eClinicalWorks
- STREAMLINE HEALTH
- GE Healthcare
- athenahealth
- Others

3rd Party Physicians and Diagnostic Clinics, Affiliates...
Collaboration, Legacy Application Architectures and M&A Activity Lead to People Security Problems

- Identity Intelligence
  - e.g. Lawson + AD
  - Application Access Logs
  - Discover & Correlate
    - Well known users
    - Poorly known users
    - Ungoverned users
    - Untrained users

Healthcare System Network:

- Non-Employees w/ Access
- Vendors
- Contractors
- Affiliate Physicians
- Employees
- 3rd Party Physicians and Diagnostic Clinics, Affiliates...

APPLICATION ACCESS LOGS

- AD
- Local Users

- Cerner
- MEDITECH
- Epic
- Allscripts
- Office 365
- eClinicalWorks
- athenahealth
- Others
Healthcare Struggles with User Identity Management

Overall 29% of users are poorly known in major EHR vendor 1
Overall 13% of users are poorly known in major EHR vendor 2
Overall 32% of users are poorly known in major EHR vendor 3

Example 55% Overall unknown users in primary EHR of this small-sized care provider in the West
Example 786 Unknown users have access to financial system of this mid-sized care provider in the North East

Source: Based on FairWarning Identity Intelligence deployments of nearly 1 Million monitored users across 50 care providers
Lessons Learned

Security and Compliance Gaps Due to Poor Identity Intelligence

• Multiple userids across applications and systems which are uncorrelated negatively impact the efficiency, accuracy of reporting and analytics and audit controls

• Shared, recycled and training userids are frequently the source of security gaps and compliance violations

• Poorly correlated userids result in the inability to detect access after termination and other Access Rights Management requirements

False Positives and Undetected Incidents Due to Poor Identity Intelligence

• Poorly known and unknown users are often intentionally ignored in privacy monitoring causing security and compliance gaps

• Poorly known and unknown users generate large volumes of false positives because Title, Department, Facility Location, etc can not be used for filtering
Use Cases
• Patient Investigations
• Forensics
• OCR Audit Controls
• HIPAA Governance
• eDiscovery

Use Cases
• Information Security Insights
• Insider Threats
• Compromised Credentials
• Predictive & Preventative

IDENTITY INTELLIGENCE
ABOUT YOUR USERS
People-Centric Security – Trust but Verify®

Gartner illustrates the principle of inverting the traditional, control-centric security approach to one that focuses on people.
Example One

Shared or Compromised Credentials
Example Two

Data theft by registration desk or others
Example Two

Data theft by registration desk or others
Example Three

Risky phishing behavior
Example Three

Risky phishing behavior

Link Clicked
Example Three

Risky phishing behavior
People Security Vision

EHR & Clinical Application Monitoring
- Alerting
- Reporting
- Salesforce & Healthcloud
- Office 365
- Real-Time

Governance
- Investigation Management
- Risk of Compromise
- Audit Response
- Notification & Disclosure
- Training Results

EHR & Clinical Application Behavioral Analysis
- Statistical Deviation
- Trending
- Visualization
- Workforce interaction with care provider enterprise

Investigations, Forensics, e-Discovery

Dynamic Identity Intelligence

Machine Learning

Predictions

Filtering

Engagement

Salesforce & Healthcloud
Office 365
Real-Time
Training Results
People Security
People Security
Takeaways

1. Behavioral Analytics are powerful and important for security and privacy programs
2. Behavioral Analytics are supplemental to your existing Audit Controls, Forensics, and eDiscovery capabilities
3. The quality of Identity Intelligence is core to your security and compliance controls
4. Start with focused use cases
5. Behavior Analytics are Probabilistic as opposed to Deterministic
6. People Security should be part of an overall program emphasizing identity intelligence, scalable governance, training and monitoring

For more information visit:
- Gartner articles: Understanding Insider Threats, & Market Guide for User and Entity Behavior Analytics
- FairWarning.com: FairWarning Patient Privacy Intelligence & Patient Privacy Intelligence Whitepaper: The Intersection of Compliance, Legal and Information Security
Ethical Considerations

See FairWarning at the Global Healthcare Privacy Summit

Discussions exploring the "Ethical Considerations of Artificial Intelligence in Healthcare Privacy and Security Programs"

Health Summit Featured Speakers:

Kurt J. Long
Founder and CEO
FairWarning

Isabelle Falque-Pierrotin
Article 29 Working Party Chair
European Union & Authority (CNIL) President
French Data Protection

Kate Black
Privacy Officer and Corporate Counsel
23andMe

Clint Phillips
Chief Executive Officer and Founder
Medici and 2nd.MD

Julian Ranger
Executive Chairman and Founder
Digi.me

Dr. Nikolaus Forgó
Data Protection Officer, Chief Information Officer, Law School Professor and Dean of Students, and Director of L3S and the Institute for Legal Informatics at the University of Hanover

Randy Farmer
Chief Operating Officer
Delaware Health Information Network

David Huseby
Security Maven
The Linux Foundation’s Hyperledger Project

Kay Firth-Butterfield
Executive Director of AI-Austin and Executive Committee Vice-Chair of The IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems