Vulnerability Management and Reporting
A Proposed Code of Conduct

David S. Muntz, CHCIO, FCHIME, LCHIME, FHIMSS
HITRUST - Senior Advisor, Public Policy

April 28, 2016, Breakout Session – Texas 1-3
How is This Relevant to Our HIT Environment?
Complexity of the Current Environment

- New models of payment
- Mergers/acquisitions/closures
- Shift in care settings
- Care coordination
- Talent shifting
- ICD-10
- ACOs
- SSP ACOs
- Health Insurance Marketplace
- MU 1
- MU 2
- New proposed rules
- Understanding MU 3
- Beyond MU

- Post-ARRA ONC (termination of grants programs)
- Post-ARRA HIT deployment
- HIPAA regulations
- Cybersecurity
- Biodefense
- Payment audits
- Security audits
- Business Continuity
- Patient and Family Engagement
- Patient matching
- Mobile
- Telehealth
- BYOD
Complexity of the Current Environment

- All other federal and state regulatory requirements, e.g. SGR, quality reporting
- All other internal HIT initiatives
- Post-implementation optimization
- Safety
- Big (eclectic) Data
- Data (value) Analytics
- Talent shortage
- Focus
- Changing roles

- Genomics
- Proteomics
- Precision Medicine
- Nanotechnologies
- Health literacy
- Global competition
- Climate
- Global financial health
- The Value Proposition
- Accelerating speed of change in
  - Information Technologies
  - The healthcare environment
Complexity + Pace of Change

Opportunity
Think Holistically

Success = People + Process + Technology
Think Holistically

Success = People x Process x Technology
Vulnerabilities Exist

Our Shared Challenge: Re-establishing Trust
Definition of Vulnerabilities

- Conditions that might unfavorably impact
  - Development
  - Deployment
  - Nominal operations
  - Products
  - Services

- Vulnerabilities can be
  - Intentional
  - Unintentional
  - Known
  - Unknown

- Elements of products and services that could be affected
  - Security
  - Confidentiality
  - Privacy
  - Integrity
  - Authority
  - Trust
  - Usability
  - Availability
Proposal: Create a Code of Conduct
Why Should Principles Be Adopted?

• It’s the right thing to do.
• Adherence to principles can raise the community standard of care
• An expected set of behaviors can be inferred or defined explicitly
• Information gathered should lead to better production, deployment, and usage of HIT products and service
Guiding Principle

My/Our fundamental objective is to maintain and increase the safety of the healthcare continuum in which we provide health information technology (HIT) products and services for the human health experience.

As a developer of software and/or a provider of software and services used by Healthcare Providers and Consumers, I/we are committed to the following principles.
General Principle

In an effort to deliver safe, defect-free products and services, I/we will employ vulnerability management and reporting practices based on the following principles during the development, deployment, and use of those products and services.

Patient safety is paramount.
Community Responsibility

I/We will aspire to make every participant in the delivery of HIT products and services aware of their individual responsibility to monitor and report on events that may adversely affect safety as they occur for the sake of every member of the community.

As a developer and/or provider of services, I/we must educate our employees and our clients about how to communicate a vulnerability.

As a developer and/or provider of services, I/we recognize that safety can be improved and promoted by communicating vulnerabilities during all phases of HIT, including but not limited to development, testing, deployment, and post-implementation.

As a developer and/or provider of services, I/we recognize that whatever product or service I/we provide is one component of the care continuum and I/we will think about the impact that our products and services have on others, as well as the impact others may have on us.
Blame-free Culture

I/we will treat the discovery of vulnerabilities as an opportunity for improvement.

I/we will address the contributing factors in a constructive manner.
From the National Patient Safety Foundation

Leadership for Organizational Learning

- Characteristics of leadership groups
  - Really cares
  - Welcoming/non-defensive attitude
- Encourages speaking up
- Facilitates communication
- Takes action
- Mobilizes information
- Seeks input
- Practices of leadership groups

Team learning behaviors

Group performance
Sense of Urgency

As a provider of products and services, I/we have a responsibility to manage the vulnerabilities as quickly as they can be validated after they are discovered.

Once discovered, I/we will communicate in clear and concise terms the potential impacts of the vulnerability, and when practical, provide solutions.
Audience Participation
Role of the Government

• Create a voluntary framework that can and will be adopted by all healthcare sector participants. In the event that private sector participation is weak, a regulatory mandate(s) for participation should be considered. The effectiveness of the activities in the healthcare sector should be judged by an independent body of experts and reported to [governmental oversight body].

• Provide legal protection to ensure that all parties are encouraged to report vulnerabilities as they are identified.
Other Questions

• Should a vulnerability management maturity model be developed?
• Should the principles evolve with the industry?
• Does one size fit all? How does size, complexity, or usage impact the principles?
• How do we deal with existing quality and safety reporting processes and organizations not necessarily focused on HIT?
• How does this impact or how is it impacted by Executive Order 13691 – Promoting Private Sector Cybersecurity Information Sharing (EO 9913691)
• How does this relate to The National Health Information Sharing & Analysis Center, (NH-ISAC)
Thank You!

David.Muntz@HITRUSTalliance.org
External Intelligence: 
**Brand & Supply Chain Monitoring**

Nicholas Albright  
Vice President, Security - Anomali
Agenda

• Overview
• Supply Chain Monitoring
• External Threat Intelligence
  • Suspicious Domains
  • Network Cleanliness
  • Social Media and DarkWeb
  • Credential Exposures
• Operationalizing
• Wrap up
Overview

• External Intelligence based Breach Analytics
• i.e. using intelligence about events that may not be observable on your network to detect breaches or other security events
• We apply this beyond your borders to your supply chain
• Types of threat intelligence covered include:
  • Suspicious Domains
  • Network Cleanliness
  • Social Media and DarkWeb
  • Credential Exposures
Defining Your Supply Chain

• Any vendor, partner, or customer that your organization relies or trusts implicitly or explicitly

• Supply chain members are a dependency in your vulnerable graph

• Breaches within your supply chain may impact your organization

• Supply chain examples:
  • Contractors or vendors
  • Software, Third Party Libraries, Remote Access Tools (VPN)
  • Environmental Control
  • Power, Utilities, and Telecomms
  • Computing, Hosting, and ISPs
  • SaaS Services
On Premises Controls

• On Premises Controls will only work for supply chain events within your network
• Code / Library Reviews
• Network Flow and Account Access Reviews
• Internal Pivoting
• Threat Feeds (Your Organization on Block lists, Bad guys accessing your org)
• They cannot detect events occurring outside your network
Zero Premises Controls

• How can you use Your Threat Intelligence solution to identify Supply Chain Threats?

• Zero Premises Controls will extend your capabilities deep within your suppliers infrastructure!
  • Public Credential Exposures (Yourself, Partners, Suppliers)
  • Threat Feeds (External Organizations on Block lists)
  • Shodan/Censys Reviews
  • Suspicious Domain Registrations (Yourself, Partners, Suppliers)
  • Social Media / DarkWeb Monitoring
Supply Chain Threat Intelligence

• Document and Research
• Supply chain company’s security posture?
  • Network cleanliness? Web footprint? (Services/Capabilities)
• Supply chain company compromised?
  • How Recent? Repeated? May put you at risk
• Supply chain company’s brand used to phish you?
  • Pay Special Attention to Service Desk Services!
• Supply chain company being targeted?
  • Examples may not be so obvious
    • DNS Registrars hold the keys
External Threat Intelligence
Suspicious Domain Name Monitoring

• Adversaries register domains mimicking the target’s brand
  • Techniques:
    • **Transforms:** Typosquat, Homoglyph, Character Omission/insertion/swap, etc
    • **Deceptive domains:** vpn-mycompany.com, portal-mycompany.com

• Used to phish you or as C2 domains

• Very effective social engineering tactic

• **Inventory Items:** internal and external domain names, brand names

• **Data Sources:** New Domain registrations, Passive DNS, Virustotal Hunting, URLCrazy

• **Operations:** SIEM integration, Email alerts, IDS Signatures, DNS RPZ
Suspicious Domain Examples

threatststream.com
threatustrwam.com
threatsrreem.com
threatstrr3am.com
threatstr3gm.com
threatsyzeam.com
thpeatstreaam.com
threatstteam.no
threatstream.us
thrratstrwam.com
threatstrstream.org
threattstreamcom.com
threatwtrem.com
threatastream.ca
threattrgam.com
threatststream.com
threatatstream.com
threatwstreams.com

threa4stream.edu
th2eatdstream.com
threatstrewqm.com
threatsrgraem.com
thveatstreaam.com
thbeaystream.com
th2eatstreams.com
threatstreal.se
thpeatstreaam.com
threatatrteam.com
threatstream.se
threadstream.com
theateastreae.com
threatrtrteam.com
thraatstream.ru
thr3atstraeam.com
threatstrem.com
thuatcsdruam.com
threaststream.com

thxaratstveam.com
threa4ststream.com
threatstroasmm.com
threutsatreaum.com
threitsstrearam.com
threestsstream.com
threatstrgams.com
theateatstream.com
threatstteam.com
threaststream.com
threaststrearam.com
threaststreemm.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraam.com
thraatsyraa
Don’t Forget About Dynamic DNS

threatstream.lioha.com
threatstream.meibu.net
threatstream.kz.com.ru
threatstream.gnway.cc
threatstream.ircop.cn
threatstream.igirl.ru
threatstream.newsexstories.com
threatstream.free-stuff.com.ru
threatstream.ledichter.com
threatstream.ggsddup.com
threatstream.yooko.com.ru
threatstream.za.pl
threatstream.servercide.com
threatstream.sxn.us
threatstream.wmdshr.com

threatstream.gnway.net
threatstream.rincondelmotor.com
threatstream.pluginfree.net
threatstream.estr.com.ru
threatstream.teksunpv.com
threatstream.gameyg.com
threatstream.redbirdrestaurant.com
threatstream.linkpc.net
threatstream.support-microsoft.net
threatstream.openoffcampus.com
threatstream.keygen.com.ru
threatstream.cu.cc
threatstream.pornandpot.com
threatstream.informatix.com.ru
threatstream.fuentesderubielos.com

threatstream.9wide.com
threatstream.jaqan.cn
threatstream.hyfitech.com
threatstream.easyeatout.com
threatstream.xicp.cn
threatstream.xenbox.net
threatstream.publicvm.com
threatstream.ven.bz
threatstream.meibu.com
threatstream.aq.pl
threatstream.m3th.org

© 2016 HITRUST Alliance.
Case Study: Suspicious Domain Registration

• Abuse isn’t always about network compromises
• Major US Based Cable and Telecommunications company
• Fraudulent procurement attempt
• Email sent from ${user}@${company}-us.com, but with the correct letter head and markings
• Discovered by SIEM scanning incoming email logs and flagged messages as suspicious
• Security team prevented fraudulent transaction, fraud team seized domain
Network Cleanliness Monitoring

- Systems from your IP space or your supply chain’s showing up as ...
  - Bot IPs
  - Scanning IPs
  - Brute force IPs
  - Spam IPs
- Your webserver hosting malicious content?
- Vulnerable or unexpected services running and discoverable?
- **Inventory Items:** IP Address Space of organization and key executives (if possible)
- **Data Sources:** Threat intelligence feeds, honeypot events, botnet sinkhole, Portscan/Web crawl data
- **Operations:** SIEM integration, Email notifications, passive audits of portscan/webcrawl data
Case Study: Network Cleanliness

• Large Hi-tech firm evaluating IT staffing company for outsourcing some development and IT services

• IT Staffing company would need VPN access and access to our internal IT resources

• Passive vendor audit performed using threat intelligence data and public portscan repository

• Upon inspection, IT staffing company had very poor network hygiene
  • tens of IPs regularly checked in to malware sinkholes
  • tens of IPs regularly scanned honeypot sensors
  • thousands of compromised credentials

• IT staffing company deemed too risky
Social Network and Darkweb Monitoring

- **Inventory Items**: Brand names, key executive names
- **Data Sources**: Social media feeds, Crawling DarkWeb, analysts monitoring darkweb, Google Dorks
- **Operations**: SIEM integration, Email notifications

Credential Exposure
Posting from the Hell
Darkweb forum
Case Study: Social Media/Darkweb Monitoring

- Brand monitoring for Major US Based Retailer
- Discovered a custom built attack tools designed for the sole purpose of brute forcing a specific part of the retailer’s web application
- Provided the sample and a report about what it did, how it worked and who built it to the retailer
Credential Exposure Monitoring

- **Inventory Items**: email domains, email addresses of key executives
- **Data sources**: Paste sites, Google Dorks, Darkweb
- **Operations**: SIEM integration / orchestration system – notify users/reset passwords, Email alerts
Case Study: Credential Exposures

• Brand monitoring for a Major Food and Beverage Company
• Discovered leaked credential exposure from an internal IT wiki page that was accidently exposed
• Company alerted and changed all passwords within 24 hours
• No evidence that these credentials were abused in that time
Operationalizing
Build an Inventory

• Create an inventory
  • Yourself
  • Critical supply chain partners
• The adversaries this, you should too

• Email domains names
• Internal and External domain names
• Personal email addresses of key executives
• Company’s IP address space
• IP address space of key executives’ home networks
• Brand names
• Names of key executives
## Data Sources and Integration Points

<table>
<thead>
<tr>
<th>Data Sources</th>
<th>Integration Points</th>
</tr>
</thead>
</table>
| **Suspicious Domains** | • New domain registration data (Whois)  
• Passive DNS  
• Virustotal Hunting  
• Repeated reviews of DynDNS  | • SIEM integrations  
• Email based alerting |
| **Network Cleanliness** | • Honeypots / C2 Sinkholes  
• Open source threat feeds  
• Spammer feeds  
• Commercial Threat intelligence providers  
• Portscan / Web crawl data  | • Search/Alert on your IP network or your supply chain’s network showing up on these lists.  
• SIEM integrations  
• Email based alerting  
• Periodic review of external internet facing assets |
| **Social Media and Dark Web** | • DarkWeb / DeepWeb Forums  
• Social Media Sites  
• Google Dorks  | • Search/Alert on your brand or your supply chains’  
• SIEM integrations |
| **Compromised Credentials** | • Paste sites  
• DarkWeb / DeepWeb monitoring  
• Google dorks  
• Commercial Threat intelligence providers  | • Search/Alert on your email domains or those of your supply chain  
• Notify users  
• Reset passwords as needed |
Summary

• Organizations must watch more than themselves and their industry vertical

• High Tech Suppliers such as Web and Domain Services, Firewall and Desktop Application vendors are increasingly targeted

• Chatter on social media and DarkWeb forums can provide early warning

• Compromised Credentials may be used by third party contractors on your network

• Passive vendors audits should be part of your procurement process
Nicholas Albright | VP of Security
Anomali
2317 Broadway, 3rd Floor Redwood City, CA 94063
Phone: 1 – 844 – THREATS
HTTPS://Anomali.com