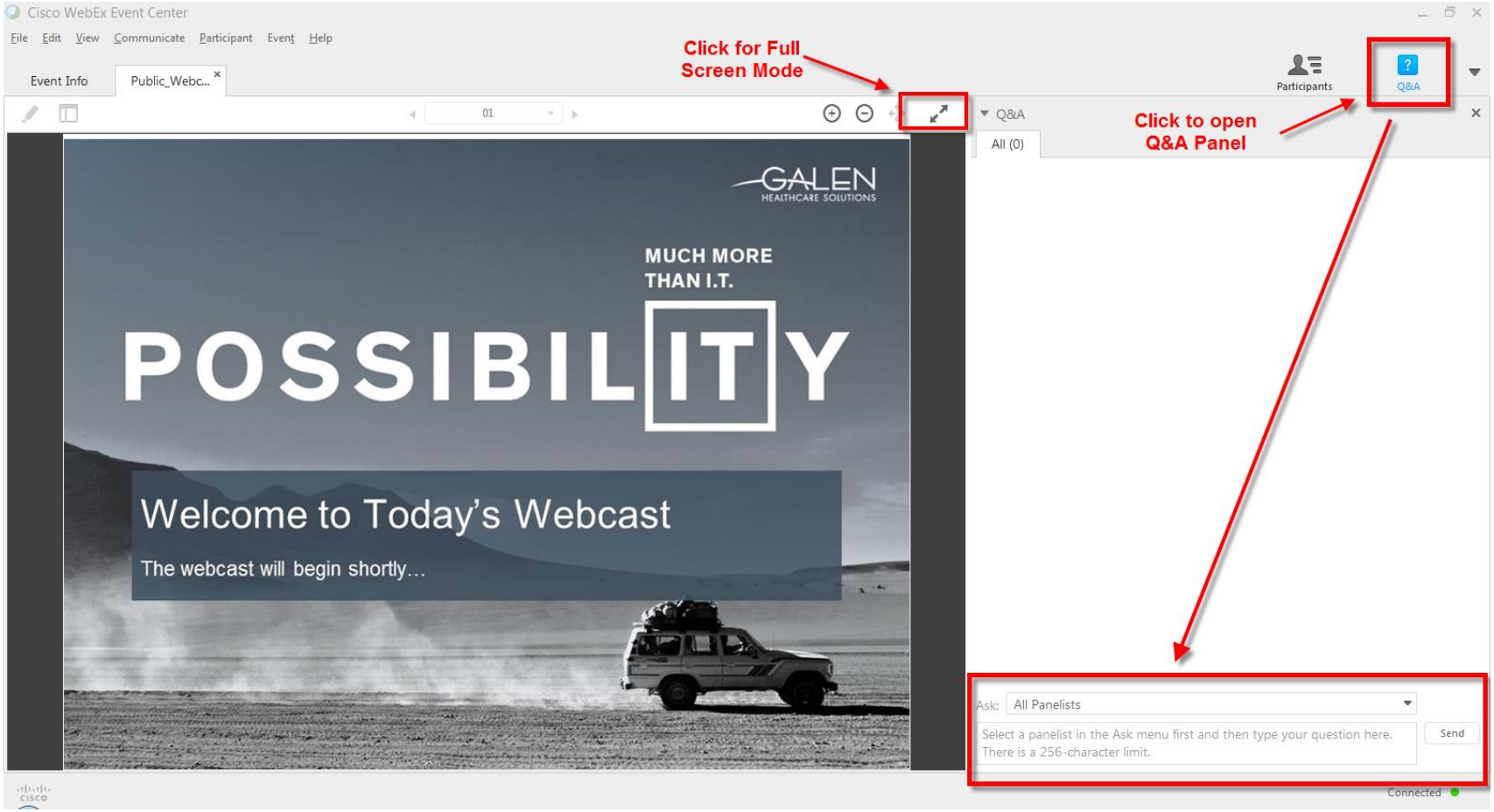
GALEN
HEALTHCARE SOLUTIONS

Health IT Security

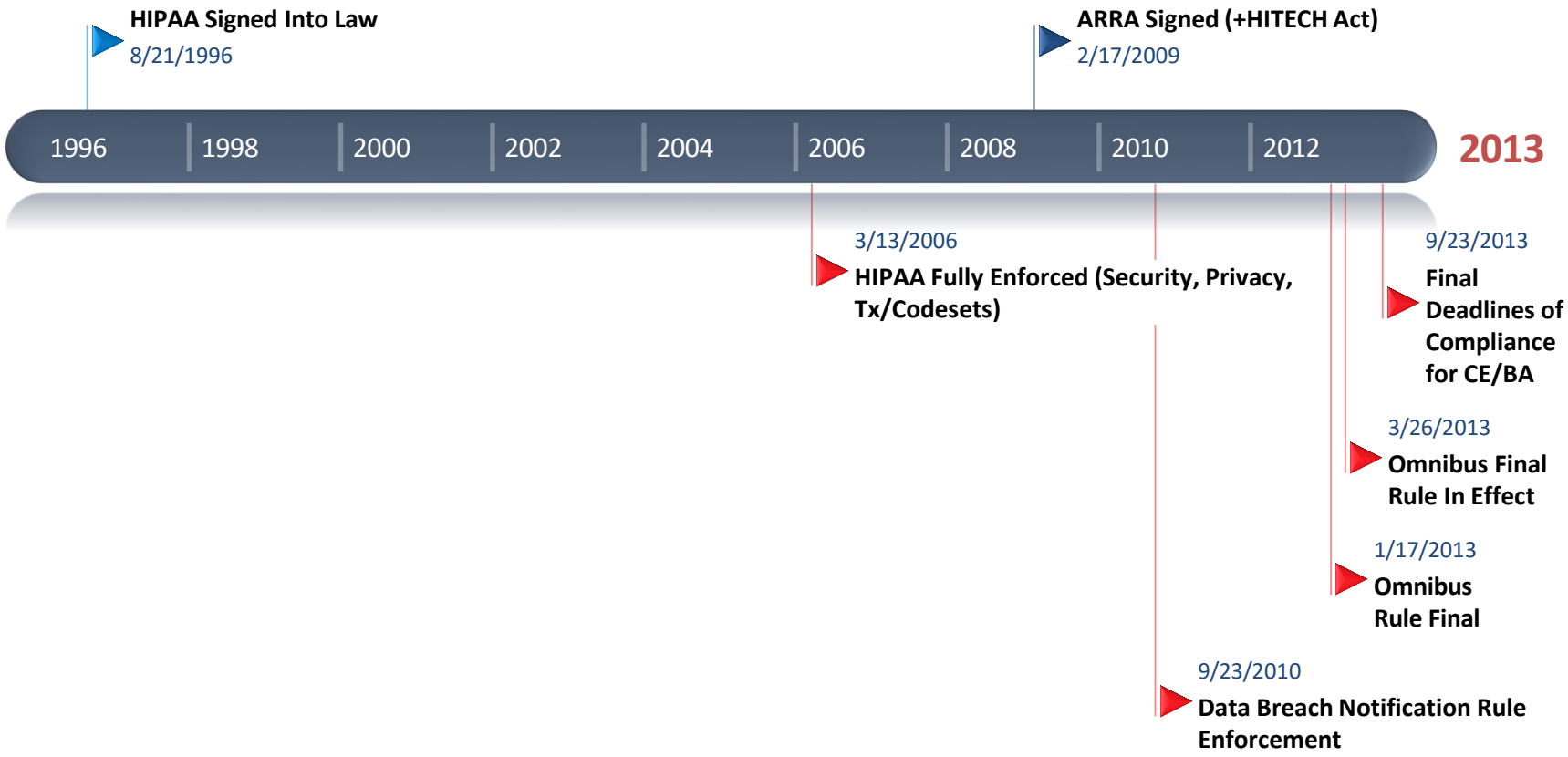
Your phone has been automatically muted. Please use the Q&A panel to ask questions during the presentation!



Agenda

- Legal Timeline
- Current Law
- Threats
- General Best Practices
- The Cloud!
- ISV Evaluation

Legal Timeline



Current Law

- Omnibus Rules Take Precedence
  - Breach Notification
  - Business Associates
  - Penalties
  - Privacy Rules
  - Teeth

Breach Notification

- No thresholds for reporting (used to be 500+)
- Virtually all breaches are now reportable
- Risk analysis can mitigate exposure

Business Associates

- Mostly the same rules apply as to Covered Entities
  - All of the Security Rule
  - Most of the Privacy Rule
    (if contract involves Privacy Rule obligations)

- Many BAAs needed to be updated
  - Specifically note Security & Privacy Rule adherence
  - Specify any delegation of Privacy Rule compliance

Business Associates

- BAs are contractually AND directly liable for violations
- BAs liable regardless of contract with CE
- BAs are liable for the actions of their sub-contractors
- Subcontractors are BAs
- CE is ultimately responsible as well

Penalties

- Didn't Know: $100-$50k *per patient*
- Reasonable: $1k-$50k *per patient*
- Willful/Corrected: $10k-$50k *per patient*
- Willful/Uncorrected: $50k *per patient*
- Yearly Max Per Calendar Year: $1.5mm
  (For same provision)

Penalties

- Worse when policies are missing / inadequate
- Intent matters

Entity	Fine	Details
CIGNET	$4.3mm	Online database / significant negligence
Alaska DHHS	$1.7mm	Unencrypted USB drive, few policies / risk analysis
WellPoint	$1.7mm	No AuthN/Z for large DB / significant negligence
BCBS of Tennessee	$1.5mm	57 unencrypted HDs stolen
Mass Eye & Ear	$1.5mm	Unencrypted laptop stolen / poor policies & risk analysis
Affinity Health Plan	$1.2mm	Lack of proper equipment disposal
South Shore Hospital	$750k	Backup tapes lost in transit

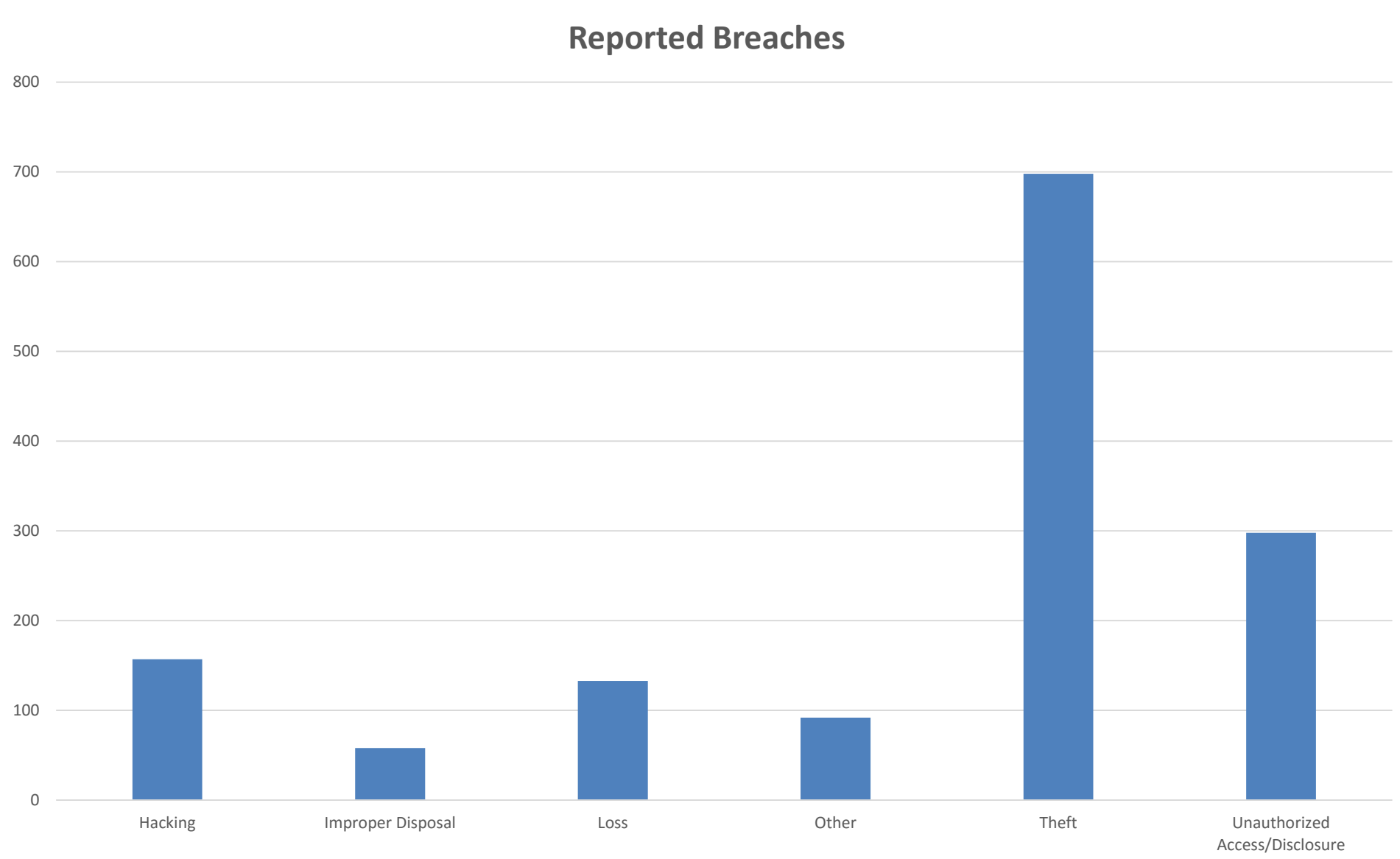
Privacy Rules

- Expanded Guidelines
  - Marketing / Communications
  - Disclosure for purposes
    - Remuneration / payment
    - Student immunization enforcement
    - Health plans
  - Privacy policies

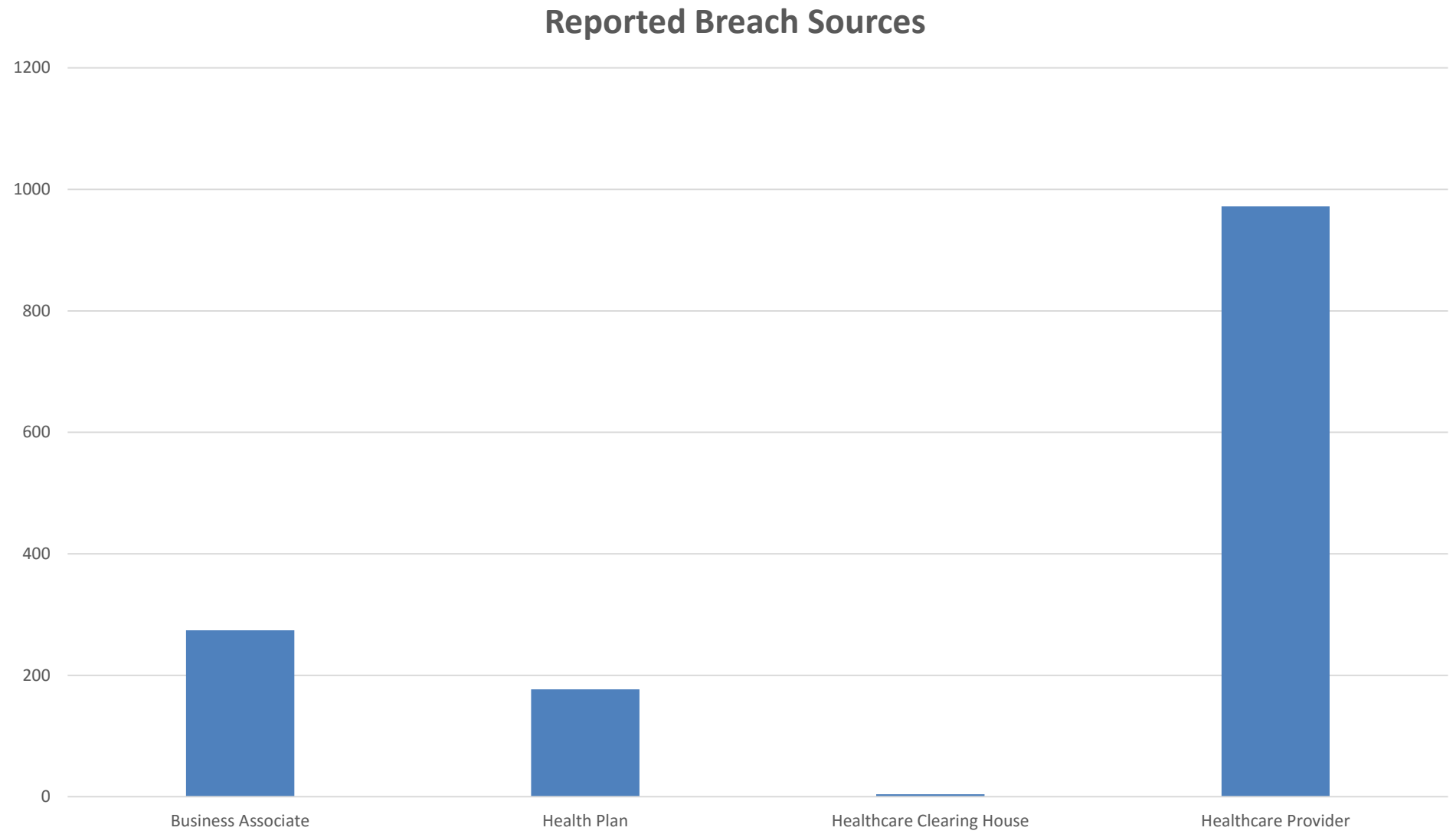
Threats

- Hacking
- Physical theft
- Employee / BA misuse
- Negligence / loss / etc.

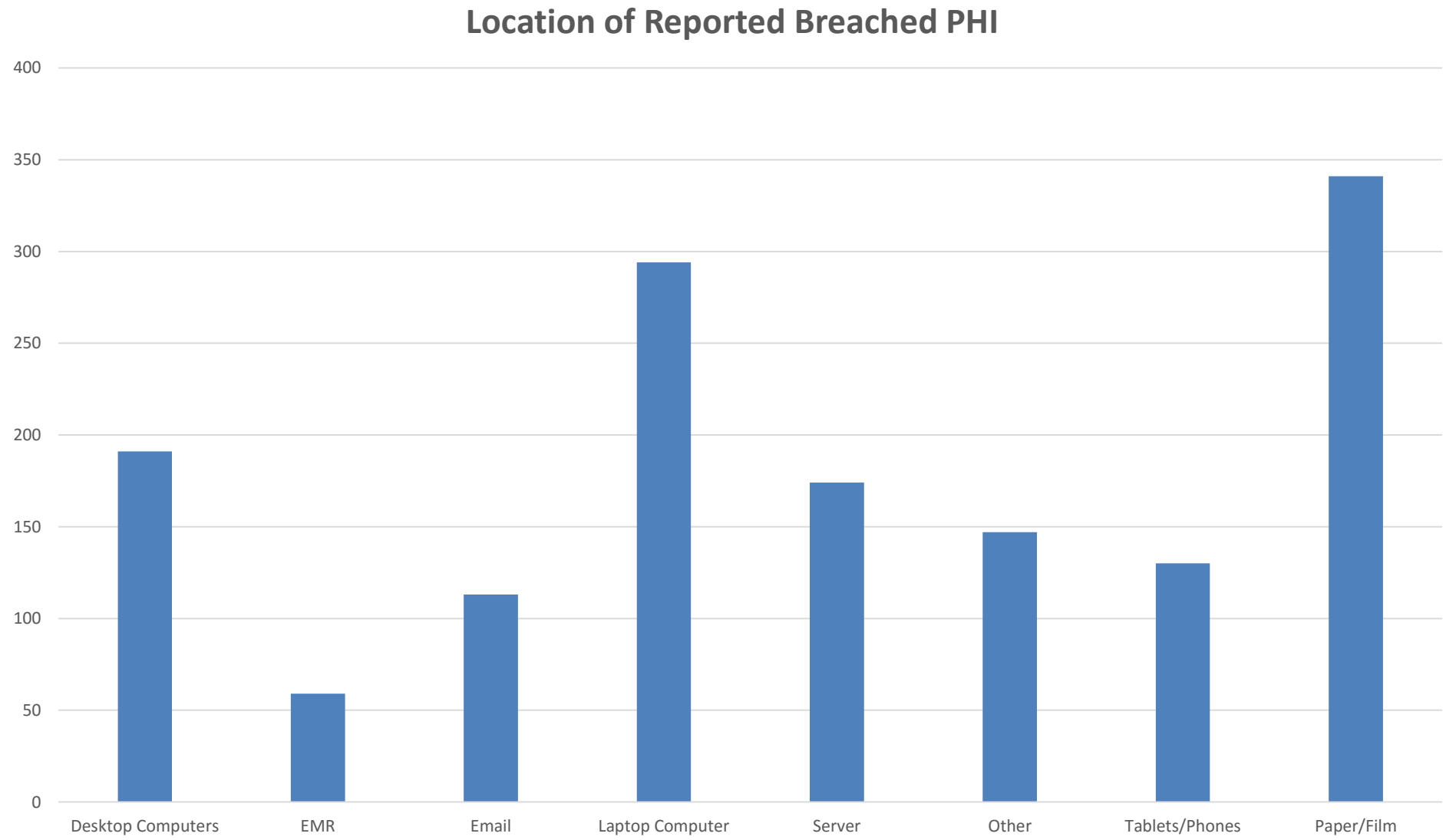
Threats



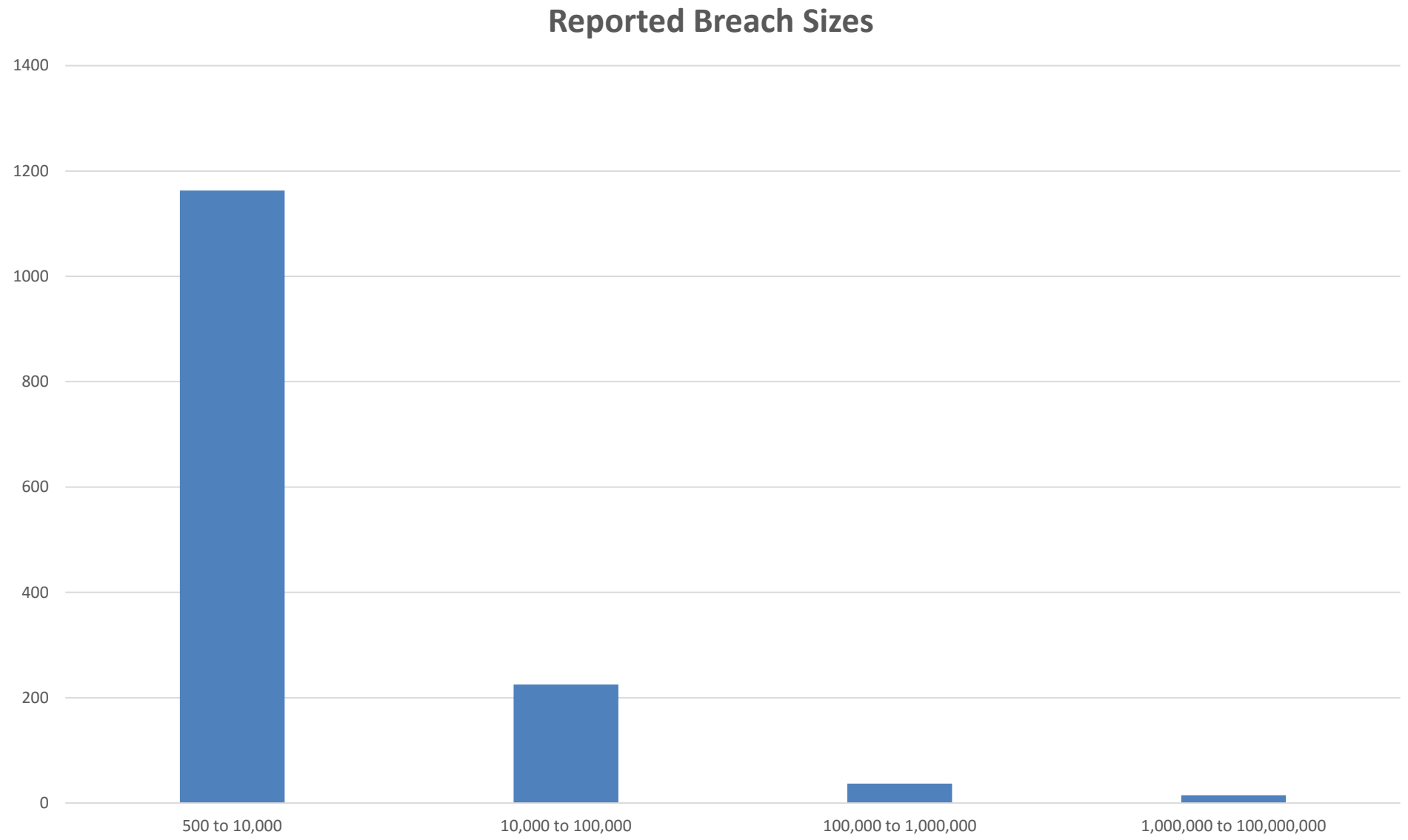
Threats



Threats



Threats



General Best Practices

- Risk Mitigation
  - IT
  - Physical Security
  - Risk Assessments
  - Employee Education / Training
  - BA / Vendor Selection

- Penalty Mitigation
  - Documentation!
    - Policies
    - Risk Assessments
    - Meeting minutes
    - Demonstrate intent

Risk Mitigation - IT

- Encryption
  - At rest (BitLocker, Sophos, etc.)
    - *Includes servers, mobile devices*
    - *Must be able to prove encryption*
  - In motion (TLS / HTTPS)
    - *Includes "internal" communications*
  - Don't forget 3rd parties
    - Email, file sharing, etc.
  - Secure the cryptographic keys!
    - Consider 3rd party "secrets" service

Risk Mitigation - IT

- Infrastructure – The Perimeter
  - Firewalls
    - Intrusion detection
    - Stateful packet inspection & filtering
    - Subscription-based updates
  - Modern VPNs
    - IPSEC or SSL
    - *Not* PPTP
  - Restrict WAP
    - WPA2/EAP
    - Segmented guest networks

Risk Mitigation - IT

- Infrastructure – Inside
  - Antivirus/Malware Detection
  - Centralized AuthN/Z
    - Active Directory / ADFS
    - *Never* share accounts
    - Multi-factor whenever possible
    - Minimal access profiles
    - Industry standard password, lockout, expiration, etc. policies
    - Clear off-boarding procedures
  - Patching / Change Control
  - Restrict USB / external devices
  - Network segmentation
  - Email

Risk Mitigation - IT

- Infrastructure – Continuity
  - Ensure availability of PHI
  - Ensure care can be provided
  - Highly available servers (clusters, farms, etc.)
  - Hot secondary data centers
  - Software based continuity solutions
  - Backups
    - On & off site
    - Encrypted
    - TEST THE RESTORE!
  - *Fully documented*

Risk Mitigation – Physical Security

- Room / Device Locks
  - Secure areas (server rooms, backup storage)
  - Desktops, laptops, tablets
  - Server cases (case intrusion sensors)
- Building Access & Identification
  - Front desk / guard
  - Keycode / Fob policies (off-boarding)
- Beware of Social Engineering
  - Walks in, grabs laptop, leaves
  - Walks in, drops off malware in USB key, leaves
  - Help desk “forgot password” calls
  - Phishing via email, social media, etc.

Risk Mitigation – Risk Assessment

"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization]."

- Section 164.308(a)(1)(ii)(A) - Security Rule

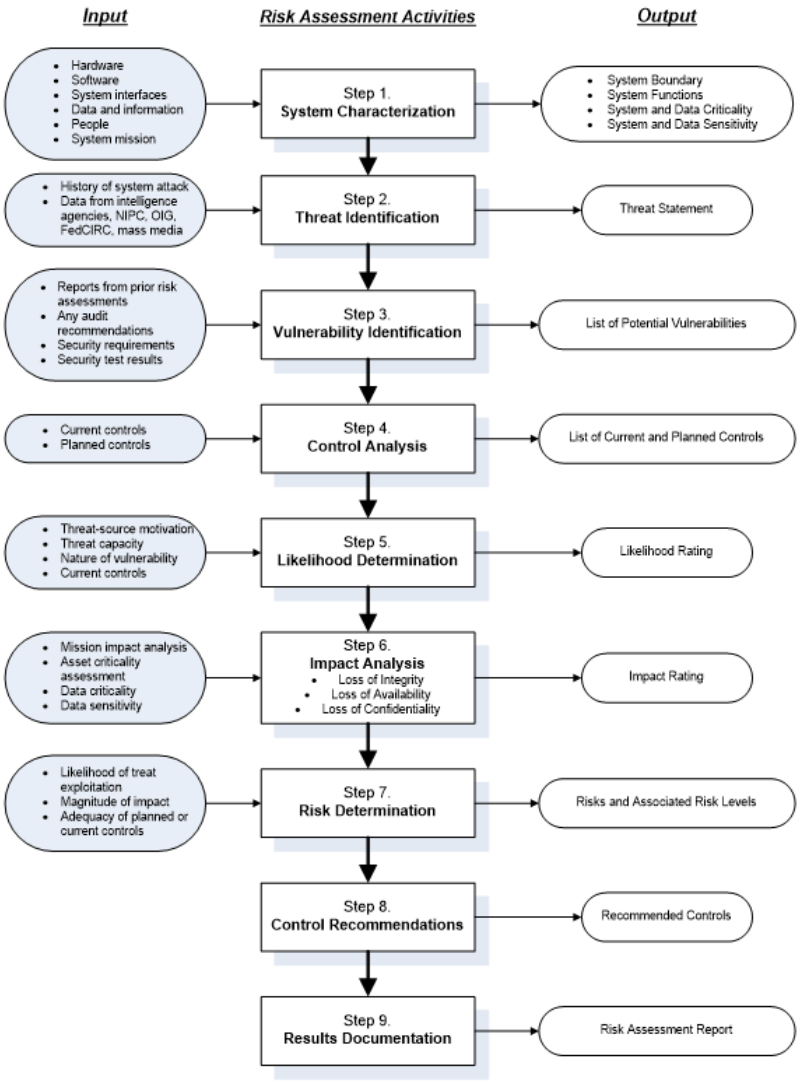
Risk Mitigation – Risk Assessment

- Done “as needed”
- Anytime risks may have changed
- Keep full meeting notes
- Sign off by PO/SO, CIO, CTO, etc.
- Can be done internally or with an outside party

Risk Mitigation – Risk Assessment

- Identify all sources of e-PHI, both internal and external
- Catalog threats to each source
  - Human (inappropriate access, hacking, etc.)
  - Natural (earthquakes, hurricanes, etc.)
  - Environmental (backup degradation)
- Document ways to mitigate risk and lay out a plan to implement

Risk Mitigation – Risk Assessment



This flowchart was taken directly from NIST SP 800-30

Risk Mitigation – Risk Assessment

- Assessment drives changes in:
  - Employee screening policies
  - Physical security measures
  - Backup procedures
  - Application of encryption
  - Authentication & authorization procedures
  - Business associate assessments
  - Etc.

Risk Mitigation – Employee Training

- Bi-Yearly
- Written policy acknowledgements
- Privacy training
  - Ideally tailored to specific job roles
  - Stress implications of violation
- Violation reporting policies
- Social engineering / general security

Risk Mitigation – BA / Vendors

- Demand and review all policy documents
- Keep up-to-date BAAs in addition to MSAs and other contracts
- Pay special attention to any that host or transmit PHI outside of environments in your direct control
- Should be a significant element of risk assessment

Penalty Mitigation

- Documentation
- Documentation
- Documentation

The Cloud!

- Providers starting to support healthcare scenarios
  - Microsoft Azure
  - Amazon AWS
  - Boutique Providers / Aggregators
- Must offer BAAs
- Compliance depends on usage
- Are they safe?

The Cloud!

- Why are they more secure?
  - Economies of scale
    - Azure by the numbers
      - $10+ billion invested
      - $1.5+ billion/year revenue
      - 6+ million requests per second
      - 2+ million databases
      - 500,000+ websites
      - 30+ trillion stored objects
  - This is their primary business

The Cloud!

The Cloud!

- Why should you still be cautious?
  - Big target / greater reward for hackers
  - Easy to use in a non-compliant way
    - Many vendors likely hope you won't ask
  - Demand transparency

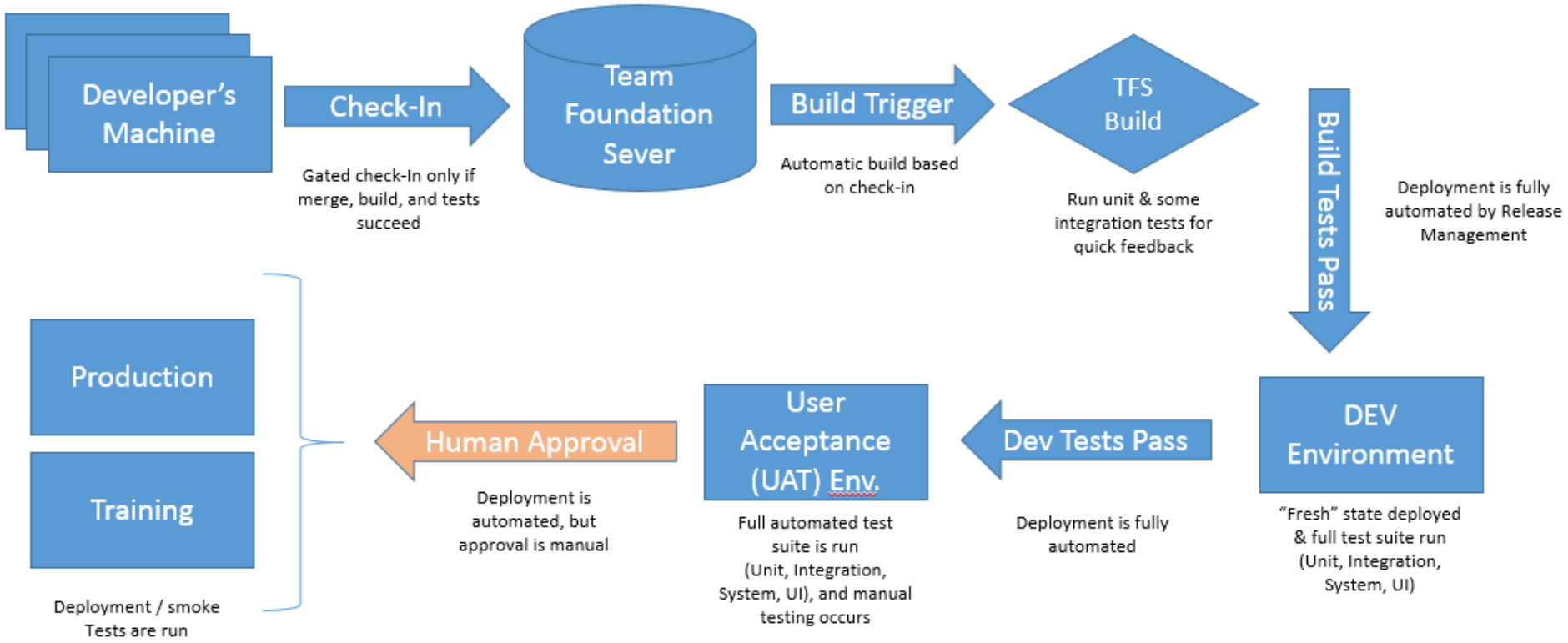
Software Vendor Selection

GALEN HEALTHCARE SOLUTIONS

- Software Development Lifecycle
  - Process
  - Security reviews & analysis
  - Testing process
    - Manual testing
    - Code coverage
  - Automation
  - Pipeline Access control

Software Development Lifecycle

GALEN HEALTHCARE SOLUTIONS



Resources

- Legislation / HSS / ORC
  - http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
  - http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
  - https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf
  - https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
  - https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the#h-95
  - http://conference.himss.org/HIMSS13/pdfs/7.pdf
  - http://www.poynerspruill.com/publications/Pages/SummaryofNewHIPAARules.aspx
  - http://wedi.org/forms/uploadFiles/35FE700000100.filename.7.26_Combined.pdf
  - https://www.truevault.com/blog/what-is-the-penalty-for-a-hipaa-violation.html
  - http://hipaacow.org/resources/hipaa-cow-documents/risk-toolkit/
- IT
  - https://technet.microsoft.com/en-us/library/bb735870.aspx
  - http://www.gfi.com/blog/the-ultimate-network-security-checklist/
  - https://aws.amazon.com/compliance/
  - https://azure.microsoft.com/en-us/support/trust-center/

Thank you for joining us today.

To access the slides from today's presentation, please visit:

http://wiki.galenhealthcare.com/Category:Webcasts

For additional assistance or to request information about our many services and products, please contact us through our website:

www.galenhealthcare.com