Let the Buyer Beware!

Ransomware & Cybersecurity Threats Create Peril to Health Care M&A Transactions

March 30, 2017

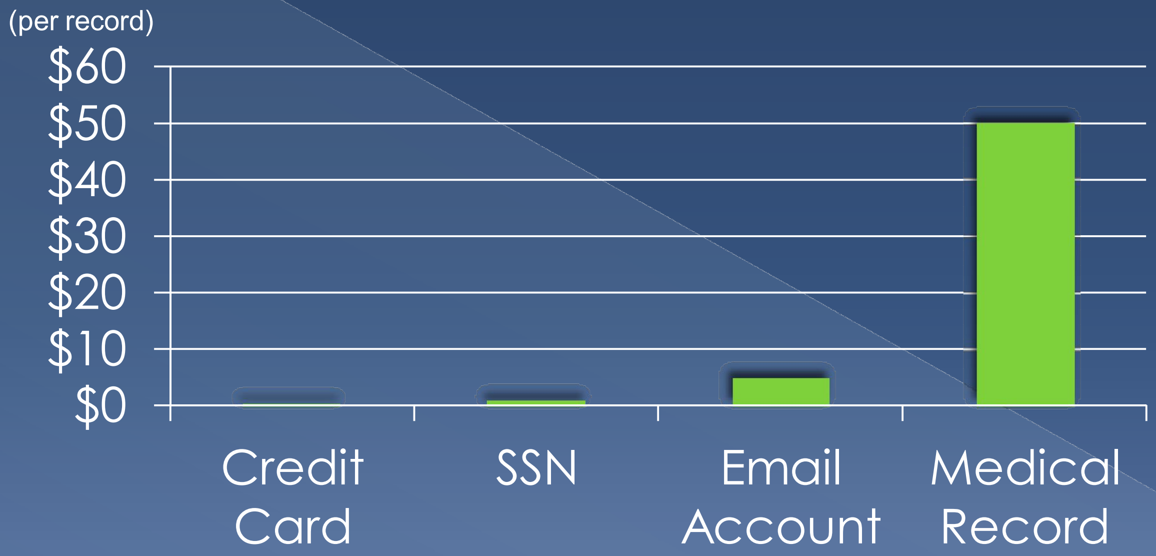
Lisa J. Acevedo, Esq., CIPP/US, CIPP/E, **Shareholder and Co-Chair, HIPAA/Health Information Privacy and Security Practice**, Polsinelli PC.

David Holtzman, JD, CIPP/G,
VP Compliance Strategies, Cynergistek

Health Care Cybersecurity Threats—Phishing Attacks and other Hacking, Malware, Ransomware, etc.

- EHR data is more valuable on black market than financial data
  - Medical data theft more difficult to detect than credit card theft—thieves have longer to “milk” the data.
    - Can be used for many fraudulent purpose, e.g. File false claims, use to get drugs/devices which can be resold.
- According to many security experts, the health care industry has underspent on security so is more vulnerable.
- Health care providers are the perfect target for ransomware attacks

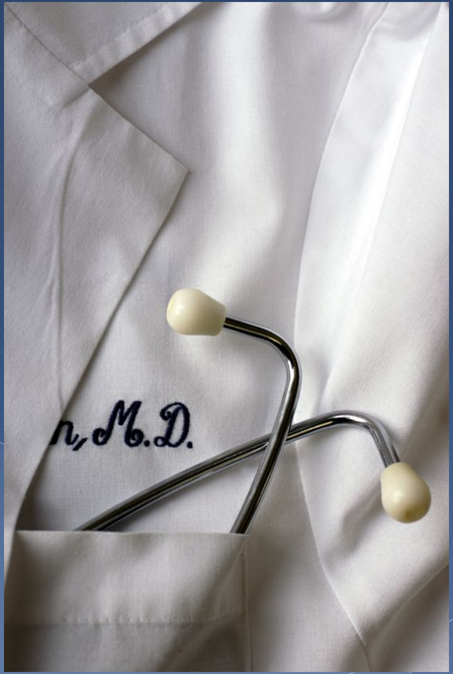
Black Market Value of Stolen Data



Sources: http://histalkmobile.com/2014-a-perfect-storm-for-data-breaches/
http://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/

Health Care M&A Backdrop

- Changes in economics and new payment models fuel mergers, acquisitions and other transactions
  - Many involve physician practices, large multispecialty groups with clinics, ASCs, other health care facilities, etc.
  - Deals may be structured as an asset purchase to limit liability
  - Regardless of deal structure, EHRs are generally a key component & asset



Why Information Security Challenging to Healthcare

1. The prime directive. First priority is taking care of patients, and we need quick and easy access to information to do that.
2. Innovation. A never-ending stream of new IT products and services are promising to improve the delivery of care.
3. Complexity. Hundreds to thousands of applications must work together seamlessly, but also must be secured.
4. Costs. Healthcare organizations are under pressure to reduce costs, and incremental spending to address security can be a tough sell.

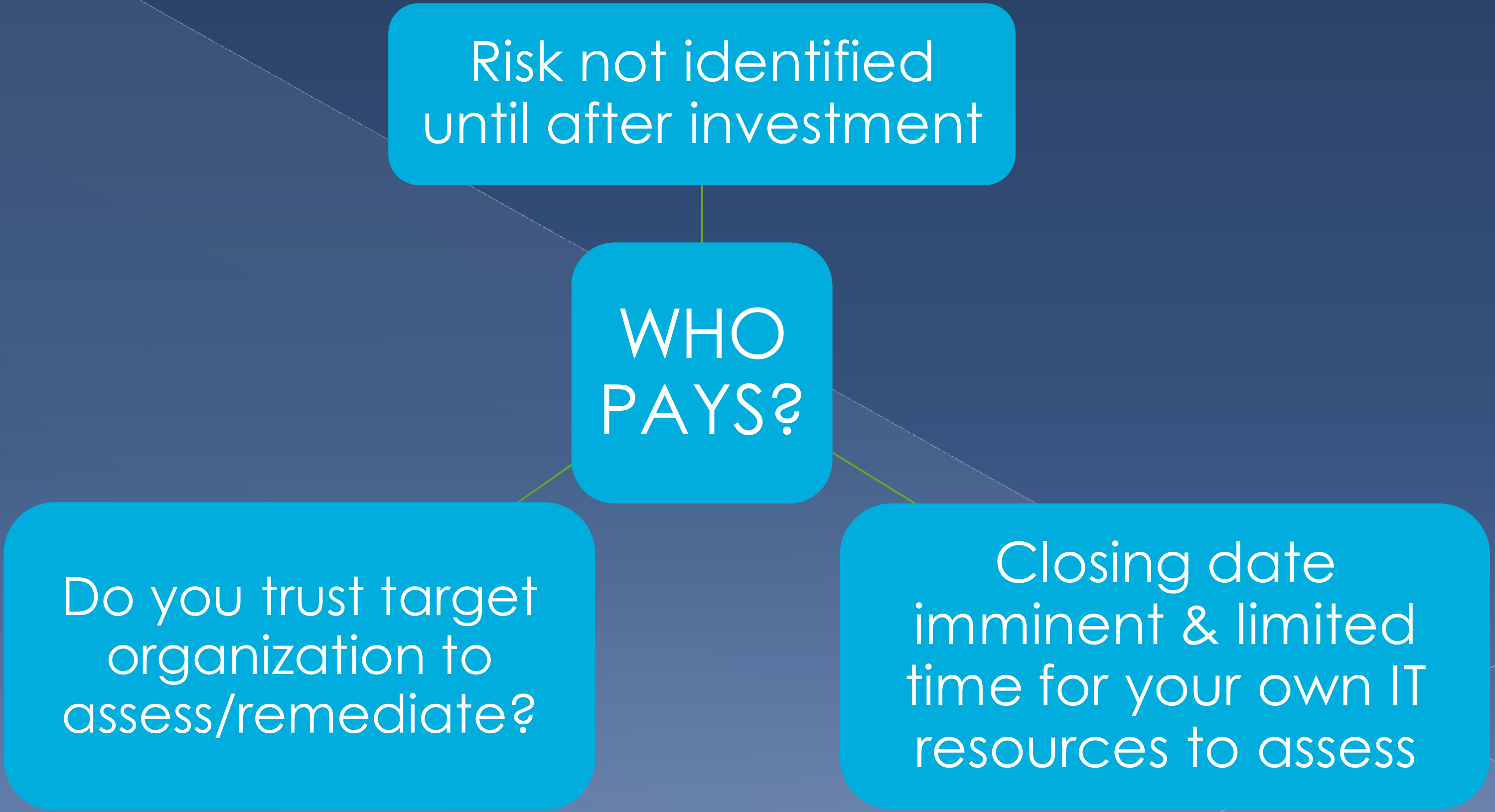
Cybersecurity Threats Risky for Deals

- Many target organizations have not conducted an adequate Security Risk Analysis and have not identified/implemented a Risk Management Plan
- Target organizations may have been subject to ransomware or other cyberattacks, determined them not to be reportable and did inadequate remediation to EHR systems
- HIPAA has not traditionally been considered to create high risk in deals and traditional due diligence investigations are often not structured to **timely** identify the new cybersecurity risk
  - Asset purchase structure thought to address compliance risks---not true any longer

Unidentified Cybersecurity Threats Adversely Impacts Deals

- Not Factored Into Key Front-End Decisions
  - Purchase Price
  - Post-Close IT Remediation Budgets
  - Closing Date

What is the Impact?



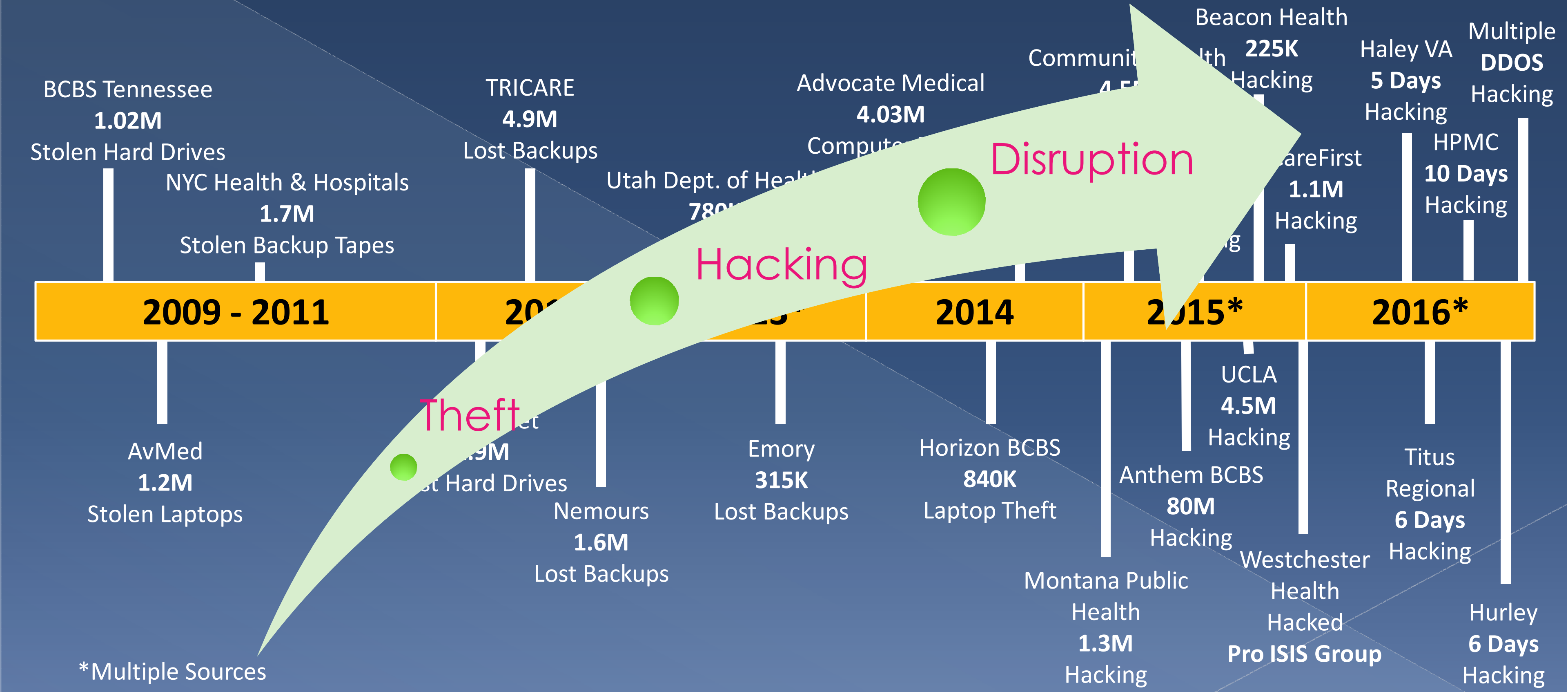
Risk not identified until after investment

WHO PAYS?

Do you trust target organization to assess/remediate?

Closing date imminent & limited time for your own IT resources to assess

Evolving Healthcare Threat Landscape



BCBS Tennessee
1.02M
Stolen Hard Drives

AvMed
1.2M
Stolen Laptops

NYC Health & Hospitals
1.7M
Stolen Backup Tapes

TRICARE
4.9M
Lost Backups

et
.9M
t Hard Drives

Nemours
1.6M
Lost Backups

Utah Dept. of Heal
780

Emory
315K
Lost Backups

Advocate Medical
4.03M
Compute

Horizon BCBS
840K
Laptop Theft

Communit lth
4.5
g

Montana Public
Health
1.3M
Hacking

Anthem BCBS
80M
Hacking

Beacon Health
225K
Hacking

UCLA
4.5M
Hacking

areFirst
1.1M
Hacking

Westchester
Health
Hacked
Pro ISIS Group

Haley VA
5 Days
Hacking

Titus
Regional
6 Days
Hacking

HPMC
10 Days
Hacking

Multiple
DDOS
Hacking

Hurley
6 Days
Hacking

*Multiple Sources

System Acquisition/Integration Issues

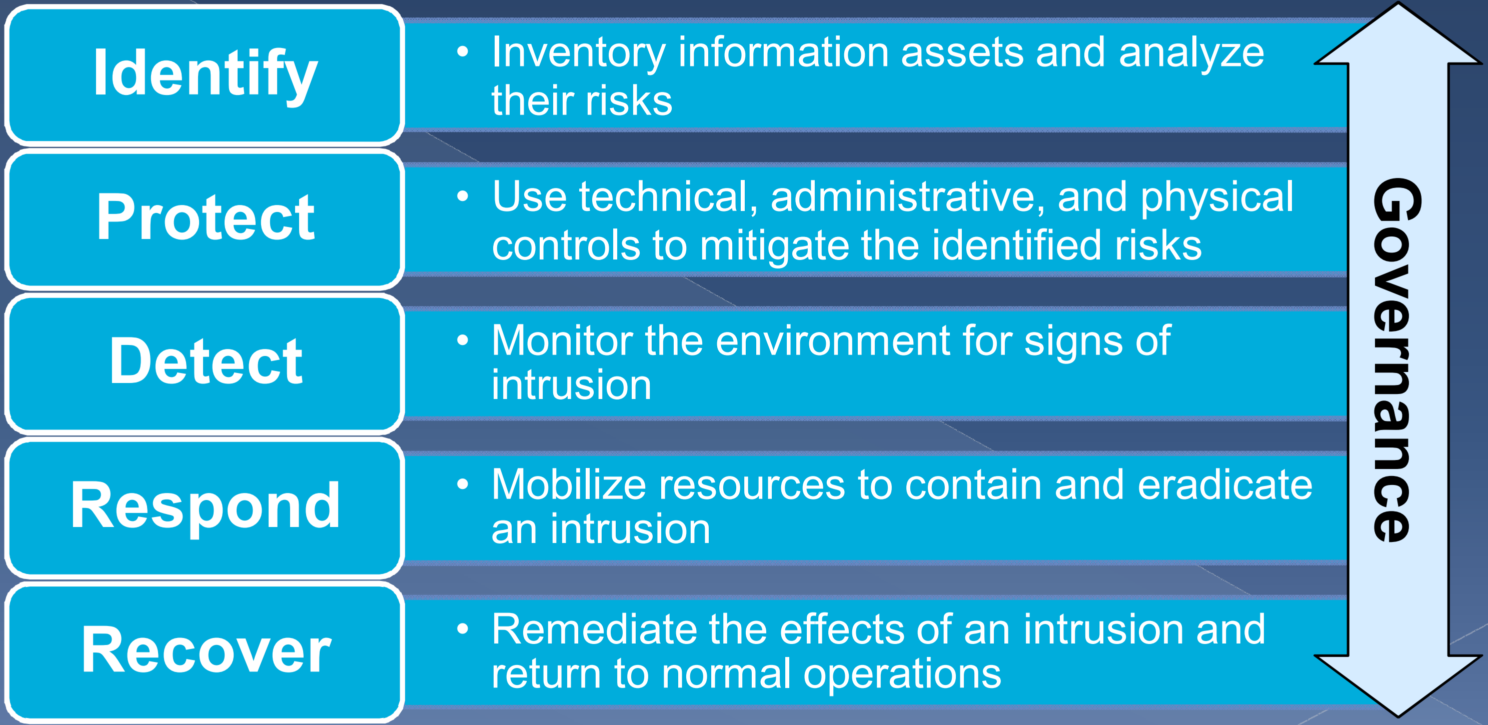
- Legacy systems
- Multiple wireless networks
- Internet enabled medical devices
- Multiple to electronic health record systems
- BYOD prevalence
- Stores & combines PHI, PII & PCI
- Identified but unaddressed high & critical risks to data
- Third party vendors w/ network access
- Clashing organizational cultures and priorities

Start With Risk Assessment

WE'LL NEED A RISK ANALYSIS ON THIS PROJECT BEFORE I CAN APPROVE IT.
www.unitedmedia.com
S. Adams
RISK 1: INDECISIVENESS
RISK 2: OVERANALYSIS
RISK 3: CLUELESSNESS
RISK 4: MICROMANAGEMENT...
CLICK CLICK CLICK
© 1997 United Feature Syndicate, Inc.
11/8/97
I DON'T UNDERSTAND THESE RISKS.
THAT'S NUMBER THIRTY-SIX.

Credit: http://dilbert.com/strips/comic/1997-11-08

Assess for Today's Cybersecurity Threat



Identify
- Inventory information assets and analyze their risks

Protect
- Use technical, administrative, and physical controls to mitigate the identified risks

Detect
- Monitor the environment for signs of intrusion

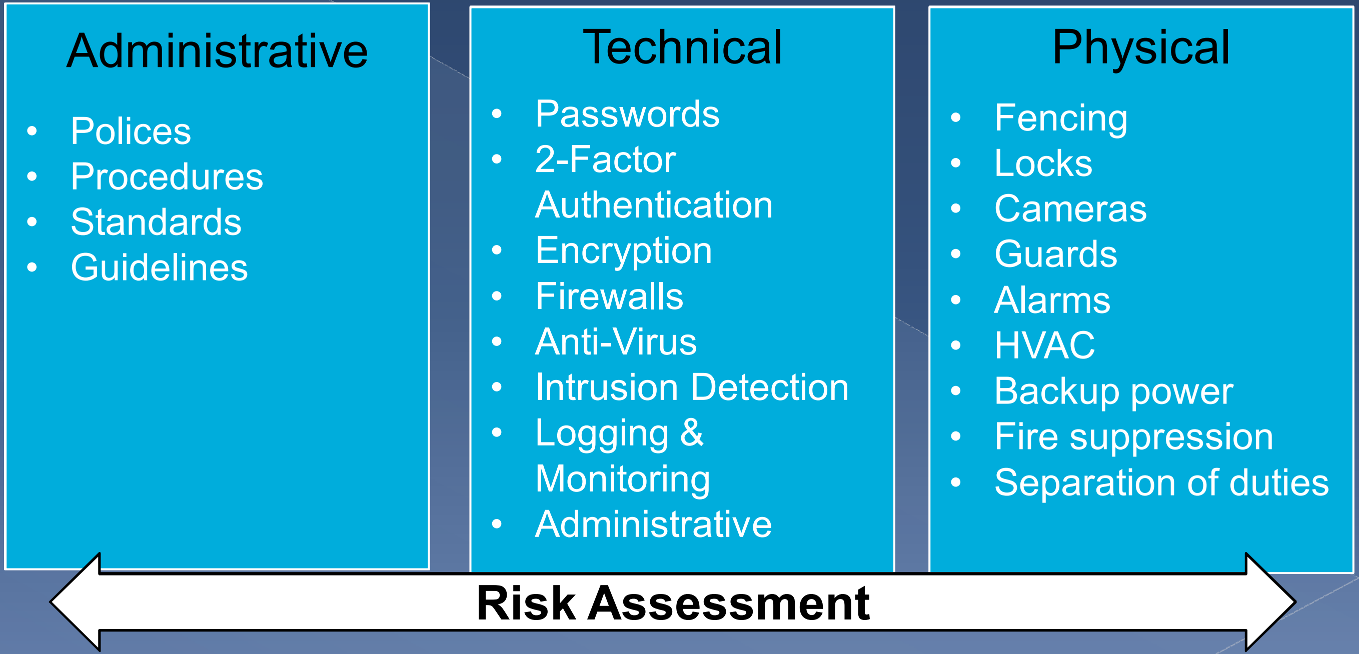
Respond
- Mobilize resources to contain and eradicate an intrusion

Recover
- Remediate the effects of an intrusion and return to normal operations

Governance

NIST Cybersecurity Framework http://www.nist.gov/cyberframework/

Examples of Security Controls



Administrative

- Polices
- Procedures
- Standards
- Guidelines

Technical

- Passwords
- 2-Factor Authentication
- Encryption
- Firewalls
- Anti-Virus
- Intrusion Detection
- Logging & Monitoring
- Administrative

Physical

- Fencing
- Locks
- Cameras
- Guards
- Alarms
- HVAC
- Backup power
- Fire suppression
- Separation of duties

Risk Assessment

Key Steps to Address Cyber Risk

- Identify This New Risk and Address Early
  - Educate business leads, deal teams, on costs associated with cybersecurity risks so that they can proactively address in initial strategy
  - Restructure diligence process to facilitate proactive and early identification and assessment of cybersecurity and other privacy/security risks
- Address cybersecurity risks and plan to address proactively in the deal document

Questions?

David Holtzman
david.holtzman@cynergistek.com

Lisa Acevedo
lacevedo@polsinelli.com