BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms.
AGENDA

- Today’s Cyber Threat Landscape
- Cybersecurity and the Healthcare Sector
- Cybersecurity and Risk Mitigation
- Conclusion
TODAY’S CYBER THREAT LANDSCAPE
Nearly 80% of organizations [surveyed in the U.S.] have been victim of a cyber attack during the past 12 months and nearly 50% have been victim of a ransomware attack.

Internal actors were responsible for 43% of data loss, half of which is intentional, half accidental.

This year, companies that had data breaches involving less than 10,000 records, the average cost of data breach was $4.9 million and those companies with the loss or theft of more than 50,000 records had a cost of data breach of $13.1 million.

Between January 2015 and June 2016, there has been a 1,300% increase in identified exposed losses, a combined exposed dollar loss of more than $3 billion.
DATA BREACHES BY THE NUMBERS

48% caused by malicious or criminal attacks

$4 million average cost of a data breach

29% increase in total cost of data breach since 2013

$158 average cost per lost or stolen record

$355 average cost per lost or stolen record in healthcare organizations

2016 Data Breach Study: Global Analysis, Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, June 2016
The FBI estimates that ransomware this year will generate $1 billion for criminals.

Businesses stand to lose much more from hacks—at least $400 billion globally.

The cyberdefense, cyberforensics and cyberinsurance industries are projected to be worth nearly $200 billion annually by the close of the decade.
MOTIVATIONS AND INCENTIVES

Political-Ideological

HACKTIVISM
Hacktivists might use computer network exploitation to advance their political or social causes.

TERRORISM
Terrorist groups might seek to sabotage the computer systems that operate our critical infrastructure.

Nation-State

ESPIONAGE
Nation-state actors might conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.

WARFARE
Nation-state actors might conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.

Criminal

CRIME
Individual and sophisticated criminal enterprises steal personal information and extort victims for financial gain.

INSIDER
Insider threat actors typically steal proprietary information for personal, financial or ideological reasons.
TARGETED DATA

- Personally Identifiable Information (PII)
- Payment Card Industry (PCI)
- Protected Health Information (PHI)
- Business Intelligence MPNI
- Intellectual Property (IP)
- Defense, National Security, Critical Infrastructure
ANATOMY OF A HACK

RECON - INITIAL COMPROMISE - ESTABLISHFOOTHOLD - ESCALATE PRIVILEGES - MOVE LATERALLY - INTERNAL RECON - EXFILTRATE DATA - MAINTAIN PRESENCE
CYBERSECURITY & THE HEALTHCARE SECTOR
PRE-CONFERENCE SURVEY PARTICIPANTS

ROLE WITHIN THE ORGANIZATION

- **39%** Executive Leadership
- **28%** Board Member

SIZE OF FACILITY

- **82%** Up to 99 Beds
- **16%** 100+ Beds
TO WHAT EXTENT DO YOU THINK YOUR ORGANIZATION IS EXPOSED TO CYBERSECURITY RISK?

Significant

Somewhat

Nothing Unusual

Not Sure

78%
RANKING OF TOP 5 GREATEST CHALLENGES

1. Operational Sustainability & Viability
2. Regulatory Changes & Reimbursement
3. Cost Containment & Management
4. Value-based Reimbursement
5. IT Capabilities
6. Capital Issues
7. Need for Technology--Telehealth
8. Compliance Associated with Regulatory Pressures
9. Cyber Threats
HOW HAS YOUR ORGANIZATION ADDRESSED THE CHALLENGE?

CONDUCTED HITRUST AND/OR CYBER ASSESSMENT

- 55% “Yes”
- 37% “Not sure”
- 8% “No”
WHO IS RESPONSIBLE FOR ADDRESSING CYBER THREATS?

- Chief Technology Officer (CTO)
- Chief Information Officer (CIO)
- Board and Executive Team Together
- There is no single individual leading this effort
- Chief Financial Officer (CFO)
- Chief Executive Officer (CEO)
- Board of Directors
- Chief Operating Officer (COO)

There is no single individual leading this effort.
HEALTHCARE CYBER INCIDENTS

OCR Reaches $400,000 HIPAA Settlement for Failure to Update Business Associate Agreement

Advocate Health Care hit by $5.55M fine for HIPAA violations
August 2016

New York Hospital to Pay $2.2 Million Fine for Allowing Filming of Patients Without Consent
ProPublica, April 21, 2016, 12:40 p.m.

Cyber Attack Nets 4.5 Million Records From Large Hospital System

So It WAS Ransomware: The Implications of the Attack on MedStar Health
April 4, 2016

HealthCare.gov hacked over the summer: ‘There was a door left open’

Maryland’s Cignet Health to Pay $4.3M for HIPAA Violation

Medical records exposed in massive Sony hack

Medical records exposed in massive Sony hack

FBI warned health care providers 10 months before Anthem cyber attack
industry unprepared for even basic cyber threats

USPS Hack: Healthcare Information of 485,000 Employees Leaked

Health care records make fertile field for cyber crime
A HOLISTIC APPROACH

1. Strategy & Program Design
2. Data Privacy
3. Risk Assessment
4. Incident Response
5. Cyber Threat Intelligence
6. Information Governance
7. Cyber Insurance
8. Information Security

CYBER RISK MANAGEMENT
HOLISTIC APPROACH
INFORMATION SHARING CHANNELS
THREAT INTELLIGENCE

Private Sector Threat Information + Government Classified and Unclassified Evidence and Intelligence = Cyber Threat Intelligence
GUIDANCE FROM THE FBI

18 October 2016
Alert Number
161018-001

Please contact the FBI with any questions related to this PIN Report at either your local Cyber Task Force or FBI CYWATCH.

Cyber Criminals May Increasingly Target Healthcare Savings and Reimbursement Accounts to Commit Fraud

Summary

The FBI assesses computer intrusions against companies providing third party administrator (TPA) services to business clients for employee insurance plans, particularly Health Savings Accounts (HSAs), may indicate a trend that could increase over the next two years.

Health Savings Account Cards Used for Fraud

Many TPAs offer HSA benefit cards to simplify the reimbursement process for plan members. HSA accounts may be an attractive target for cyber threat actors because of the lower degree of scrutiny by account-holders compared to regular bank accounts. Instead of the member paying out-of-pocket expenses and waiting for reimbursement, the transaction is processed at the merchant/provider counter utilizing a credit card linked to the member’s health benefit account.
DIGITAL ASSET VALUATION

THREE PRINCIPLES OF DIGITAL ASSET VALUATION FOR CYBER INSURANCE

1. Consider who gets value from the asset.

2. Understand the role your digital assets play in creating economic value / generating revenue.

3. Look forward - valuing your digital assets requires an outward view (previously invested costs to create the asset are “sunk”).
DIGITAL ASSET VALUATION

UNDERSTANDING THE VALUE OF DIGITAL ASSETS

Intrinsic
Critical element that allows the digital asset to exist in the first place (e.g. the person, binary data, physical object, legal contract etc.)

Extrinsic
Opportunities to leverage the digital asset making it more useful to prospective users
DATA CLASSIFICATION

Identify
- Data assets
- Data custodians

Plan
- Create classification framework
- Develop protection profiles

Act
- Review and analyze report(s)
- Readjust framework and re-classify data as needed

Classify
THREAT + VULNERABILITY + CONSEQUENCE = RISK
CHALLENGES TO THE HEALTHCARE SECTOR

- Legacy computer systems
- Multiple wireless networks - open networks
- Internet enabled medical devices - wireless connections
- Mandatory transition from paper to electronic health records
- “Bring your own device” (BYOD) policy
- Only sector which stores and combines PII, PHI and PCI
- Mergers & Acquisitions create PHI inventory challenges
- Victims are often unaware when PHI is stolen
- Third party vendors with network access
- Higher payout on the black market
- Cybercrime displacement from financial services
HOW CYBERCRIME AFFECTS THE HEALTHCARE INDUSTRY

Protected Health Information (PHI) is monetized and exploited for:

- Medical Device Fraud
- Prescription Fraud
- Healthcare/Medicaid Fraud
- Identity Theft
- Tax Fraud
- Unknown Exploitation

Protected Health Information (PHI) is 10-70x more valuable to fraudsters than credit card information.

- Patient Names/DOB
- Blood Types
- Policy Numbers
- Billing Information
- Diagnoses Codes
Advocate Healthcare Network (Advocate) was investigated by HHS - Office of Civil Rights after submitting three breach notification reports.

- In August 2016 it was announced that Advocate settled potential HIPAA penalties for $5.55 million
- Advocate has to adopt a corrective action plan
- Combined breaches effected ePHI of approximately 4 million individuals - Included PII and demographic, clinical, health insurance information
- Advocate failed to:
  - Conduct an accurate and through assessment of potential risks and vulnerabilities to all ePHI
  - Implement policies and procedures and facility access controls
  - Obtain satisfactory assurances in the form of a written business associate contract (third-party vendor management)
  - Reasonably safeguard an unencrypted laptop left in an unlocked vehicle overnight
Payment Transformation, M&A Activity and Other Activity Generating New Cyber Risks
THE MOVEMENT TOWARD CLINICALLY INTEGRATED CARE

Various forces—including the move toward payment tied to quality and longer episodes of care—are driving clinical integration across provider types, leading to new and more complex data sharing and integration requirements for providers.
CLINICAL INTEGRATION

STRATEGY TO OPERATIONALIZE

Aligning all providers in an integrated network requires a new focus on information governance and an understanding of where clinical partners stand in various factors that could generate risk.
THE TRANSITION TO VALUE BASED CARE?

THE INTERSECTION OF COST AND QUALITY

- Value-based care is a structure of health care where reimbursement is based on clinical and financial outcomes.

- The move from volume (fee-for-service) to value (value-based payment) and the importance of outcomes and measurement is having significant impacts on how providers operate, requiring providers to collect and report various health indicators related to care delivery and patient outcomes.

- The goals: improved health outcomes, and appropriate care delivery at a lower cost also necessitates that providers are able to access health information across the continuum of care at the point of service and to track and report health events amongst a network of providers.
PAYMENTS FOR AN EPISODE OF CARE

Bundles align services and payments, crossing all traditional lines into an episode of care. These episodes are 90 days or greater and require coordination across the continuum of care. Under this payment model the hospital owns the entire episode, e.g. a total joint procedure. Aligning with good partners and sharing health information becomes critical to financial success.
102
Hospital transactions announced in 2016

55%
more than the number announced in 2015

- 2016 hospital transactions took a number of forms including mergers, acquisitions, joint ventures and joint operating agreements.

- Although there was a slight dip in 2016 over the previous year, it is expected activity is on the rise and will continue as stable health organizations opt to partner to support the evolving demands of the industry and bolster market essentiality.

- Buyers involved in such transactions will need to consider “cyber security” as part of a more enhanced due diligence process.
TELEMEDICINE IN TRANSFORMING HEALTHCARE

Expanded insurance coverage & growing demand has meant an increase in telemedicine requiring an increased information exchange.

The percentage of providers that have telemedicine programs:
- **72%** of Hospitals
- **52%** of Physician Groups

The number of virtual doctor visits in the U.S.
- **2015**: 1 million
- **2016**: 1.2 million

In 2016, more than 15 million Americans received some kind of medical care remotely. This number is expected to grow by **30%** in 2017.

Physicians are conducting ‘virtual’ doctors visits, communicating with their patients by phone, email and webcam or consulting with one another to support patient care.

Patients are using new devices to relay personal health information to their doctors including blood pressure, glucose and vital signs to better manage chronic conditions at home.

---

American Telemedicine Association (virtual doctor visits); Avizia survey of 280 health-care executives, March 2016 (providers); National Business Group on Health survey of 140 large employers (benefits). The Wall Street Journal.

CYBER RISK

CYBER THREATS CANNOT BE ELIMINATED, THEY CAN ONLY BE MITIGATED

“I always tell [our workers], ‘Don’t ever forget that at the end, we’re dealing with a choice that some human made on a keyboard somewhere else in the world … There was a man or woman on the other end of this.’” - Admiral Michael Rogers, Director, NSA and Cyber Command

“The Russians hack our systems all the time, not just government, but also corporate and personal systems. And so do the Chinese and others, including non-state actors. The point is, cyber will continue to be a huge problem for the next Presidential administration, as it has been a challenge for this one.”

- Hon. James R. Clapper, Director of National Intelligence

“The most significant impact the recent hacker attacks will have on the healthcare sector is that information security will need to be considered as an integral part of the security and operations processes of healthcare organizations. They will need to become more proactive and consider risk as equally as utility.” - Mitch Parker, CISO of Temple University Health System
Where do you Start?

Risk Analysis Requirements under the Security Rule

The Security Management Process standard in the Security Rule requires organizations to “[i]mplement policies and procedures to prevent, detect, contain, and correct security violations.” (45 C.F.R. § 164.308(a)(1).) Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard. Section 164.308(a)(1)(ii)(A) states:

**RISK ANALYSIS (Required).** 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].
CYBERSECURITY MITIGATION

RECOMMENDED RISK ASSESSMENT STEPS

- Awareness & Training
- Policies & Procedures
- Application/System Inventory
- Security Operations Center
- Categorize Data
- Business Continuity Planning
- Cyberinsurance
- Incident Response
- Access Controls
- Configuration
- Spam Filters
- E-mail Detection
- Anti-virus & Malware
- Macro Scripts
- Software Restriction Policies
- App Whitelisting

Page 39
CYBERSECURITY MITIGATION

RECOMMENDED REMEDIATION STEPS

- **ISOLATE** affected computers
- **DO NOT CLEAN OR RE-IMAGE** affected computers
- **CONTACT LAW ENFORCEMENT** and provide relevant logs
- **IMPLEMENT** incident response and BC Plans
CONCLUSION & QUESTIONS
OUR CYBERSECURITY AND HEALTHCARE SERVICES

- Cyber Risk Management Strategy & Program Design
- Cyber Risk Assessment & Security Testing
- Data Privacy & Protection
- Security Architecture & Transformation
- Incident Response Planning
- Business Continuity Planning & Disaster Recovery
- Digital Forensics & Cyber Investigations
- Cyber Insurance Claim Preparation & Coverage Adequacy Evaluation
- Strategy Integration Across Expanding Continuum of Care
JOHN RIGGI
Managing Director
Head of Cybersecurity and Financial Crimes Unit

John Riggi leads BDO’s Cybersecurity and Financial Crimes Unit, having spent nearly 30 years as a highly decorated veteran of the FBI, and serving as representative to the White House Cyber Response Group and Financial Services Steering Committee. At the FBI, he led the development of mission critical partnerships with the healthcare industry, among other sectors, for the investigation and exchange of information related to national security and criminal-related investigations, including developing national strategic initiatives to warn the healthcare sector of specific cyber threats.

Knowledgeable in healthcare operations and infrastructure, he held a national strategic role in the investigation and corporate outreach of every major cyber incident targeting healthcare organizations between 2014 and 2016. He also investigated complex healthcare fraud related financial crimes schemes as an FBI field Supervisor and Senior Agent in New York City. Presently, John on behalf of BDO is leading the American Hospital Association’s (AHA) program to provide cybersecurity risk management training to their 5,000 hospital CEO members. John has also been recently named as a national co-chair and spokesperson for the Health Information Trust Alliance (HITRUST) cyber threat catalogue. A healthcare industry first, the catalogue will document cyber threats which face the healthcare industry and define corresponding controls to mitigate those threats.

In addition, John serves as an official private sector validator for the White House’s Presidential Policy Directive (PPD)-41 on U.S. Cyber Incident Coordination. The PPD is designed to foster an improved working relationship between the public and private sector, understanding that “significant” cyber threats—those that pose at least a demonstrable impact on public health or national or economic security—require greater public-private sector cooperation.
Patrick D. Pilch leads BDO’s National Healthcare Advisory Practice and the BDO Center for Healthcare Excellence & Innovation. He has more than 25 years of healthcare, financial services, operational management and restructuring experience and provides strategy, business transformation, interim management, M&A advisory, restructuring, turnaround, and performance improvement services to assist organizations and their stakeholders. Advising nonprofit, for profit and public healthcare organizations on strategic, turnaround and performance improvement, he conducts operational and financial assessments, develops future state models and roadmaps, and implements alignment strategies across the continuum of care to improve quality and delivery.

He has served as a strategic advisor to hospitals, boards, foundations, and healthcare systems in matters involving mergers, acquisitions, divestitures, real estate holdings, and other assets and restructurings.

Mr. Pilch previously held senior leadership roles in Healthcare Advisory at PWC LLP and Alvarez & Marsal. He also led finance and operations at a technology firm, managing general accounting and M&A activity, and served as interim CFO and COO at a hospital emerging from bankruptcy, through its retention of state licensure and securement of deemed CMS status and Joint Commission accreditation. Formerly Vice President of Managed Care and New Business Development at North Shore-LIJ Health System, he also served in financial advisory services and finance positions while at Greenwich Capital Markets Inc., Salomon Brothers, Inc., and Peat Marwick. Mr. Pilch began his career providing investment banking, structured finance, financial reporting, insurance, healthcare, and bank audit services.

PROFESSIONAL AFFILIATIONS
American Institute of Certified Public Accountants
Healthcare Financial Management Association

EDUCATION
M.B.A., Columbia School of Business B.S., Accounting, Fairfield University
About BDO Consulting
BDO Consulting, a division of BDO USA, LLP, provides clients with Financial Advisory, Business Advisory and Technology Services in the U.S. and around the world, leveraging BDO’s global network of more than 67,000 professionals. Having a depth of industry expertise, we provide rapid, strategic guidance in the most challenging of environments to achieve exceptional client service.

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, advisory and consulting services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 500 independent alliance firm locations nationwide. As an Independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 1,400 offices across 158 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your firm’s individual needs.

© 2017 BDO USA, LLP. All rights reserved.