Your Presenters

Bob Chaput, CEO & Founder  
MBA, CISSP, HCISPP, CRISC, CIPP/US  
• 35+ years in Business, Operations and Technology  
• 25+ years in Healthcare  
• Executive | Leader | Entrepreneur  
• MBA, Mathematics  
• Certified | Key Healthcare Executive | Key Thought Leader  
• Responsible for largest healthcare datasets in world  
• Numerous Technical Certifications (MCSE, NOCA, etc.)  
• Experience and Focus: Healthcare, Financial Services, Retail, Legal  
• Member: AIPR, CHA/AMIA, HIMSS, IQA, HCCA, KPM, IAC, ACF

Mary Chaput, Chief Financial and Compliance Officer  
MBA, HCISPP, CIPP/US, CIPM  
• 25+ years in Health Care  
• 15+ years as CFO of public company, 12+ years with GE  
• Former VP/CFO and Compliance Officer for Healthways, Inc.  
• Former VP/CIO for Cerner Research, Inc.  
• Business executive – 15+ years of ergonomic and international financial management & operational experience  
• BA Mathematics, MBA, MS Financial Management Program  
• Expertise and Focus: Healthcare, Due Diligence, Risk Management, Analytics, Legal  
• Member: AIPR, HCID, CHI/AMIA, HIMSS, IQA, HCCA
Learning Outcomes

- Provide an overall 6-point program for building a cyber risk management case for action
- Learn the danger of using "industry" data breach costs per record
- Prepare to calculate the cost of a data breach specific for your organization
- Determine how to choose cost factors relevant to your organization
- Use breach cost for your organization to build the business case to strengthen your cyber security program

Discussion Flow

1. Problem
2. Solution
3. Results
4. Resources

Changing Landscape Driving Cyber Risks

Cybersecurity risk management programs in healthcare are simply not keeping pace with the evolving threat landscape.
“First, Do No Harm.”

~ Hippocrates, 4th Century, B.C.E.

With the Digitization of Healthcare, We’ve Discovered New Ways to Create Harm

It’s a Patient Safety Issue - Connect the Dots!

Confidentiality Integrity Availability

Quality and Safe Care Access to Care Timely Care

Not an IT Problem!

Patient Safety – Quality of Care – Patient Satisfaction Issues

<table>
<thead>
<tr>
<th>Bad Things Emanating from COMPROMISE OF</th>
<th>CONFIDENTIALITY</th>
<th>INTEGRITY</th>
<th>AVAILABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Theft</td>
<td>Incorrect Diagnosis</td>
<td>Delayed Admission</td>
<td></td>
</tr>
<tr>
<td>Reputational Damage</td>
<td>Incorrect Treatment</td>
<td>Delayed Diagnosis</td>
<td></td>
</tr>
<tr>
<td>Relationship Damage</td>
<td>Incorrect Prescriptions</td>
<td>Delayed Surgery</td>
<td></td>
</tr>
<tr>
<td>Employment Damage</td>
<td>Incorrect Billing Charges</td>
<td>Delayed Prescriptions</td>
<td></td>
</tr>
<tr>
<td>Financial Damage</td>
<td>Contaminated Clinical Trial</td>
<td>Delayed Discharge</td>
<td></td>
</tr>
<tr>
<td>Anxiety</td>
<td>Identity Theft</td>
<td>Diagnosis Errors</td>
<td></td>
</tr>
<tr>
<td>Depression</td>
<td>Reputational Damage</td>
<td>Treatment Errors</td>
<td></td>
</tr>
<tr>
<td>Suicide</td>
<td>Death</td>
<td>Death</td>
<td></td>
</tr>
</tbody>
</table>

It's a Patient Safety Issue - Connect the Dots!

Confidentiality Integrity Availability

Quality and Safe Care Access to Care Timely Care

Not an IT Problem!

Patient Safety – Quality of Care – Patient Satisfaction Issues

<table>
<thead>
<tr>
<th>Bad Things Emanating from COMPROMISE OF</th>
<th>CONFIDENTIALITY</th>
<th>INTEGRITY</th>
<th>AVAILABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Theft</td>
<td>Incorrect Diagnosis</td>
<td>Delayed Admission</td>
<td></td>
</tr>
<tr>
<td>Reputational Damage</td>
<td>Incorrect Treatment</td>
<td>Delayed Diagnosis</td>
<td></td>
</tr>
<tr>
<td>Relationship Damage</td>
<td>Incorrect Prescriptions</td>
<td>Delayed Surgery</td>
<td></td>
</tr>
<tr>
<td>Employment Damage</td>
<td>Incorrect Billing Charges</td>
<td>Delayed Prescriptions</td>
<td></td>
</tr>
<tr>
<td>Financial Damage</td>
<td>Contaminated Clinical Trial</td>
<td>Delayed Discharge</td>
<td></td>
</tr>
<tr>
<td>Anxiety</td>
<td>Identity Theft</td>
<td>Diagnosis Errors</td>
<td></td>
</tr>
<tr>
<td>Depression</td>
<td>Reputational Damage</td>
<td>Treatment Errors</td>
<td></td>
</tr>
<tr>
<td>Suicide</td>
<td>Death</td>
<td>Death</td>
<td></td>
</tr>
</tbody>
</table>
Why Do We Do What We Do?  
Creating a Safer Environment for Patients

Evolving Focus

2010

2015

Patient Safety

Security & IRM

Compliance

48 OCR Actions ... 5 already in 2017 / 13 in 2016

- 48 OCR Cases
- 38 Involving ePHI / Risk Analysis
- 34 Adverse Risk Analysis Findings
- 32 Adverse Risk Management Findings

Organizations Struggling with Basic Information Risk Analysis / Management
- Not asset-based – systems / apps / technology that create, receive, maintain or transmit ePHI
- Not comprehensive enough – every asset in every LOB in every facility in every location
- Not detailed enough - not considering every asset threat vulnerability scenario
- Not following OCR/NIST guidance / 9 essential elements
- Not enough documentation / evidence of vibrant ongoing program

The Single Biggest Decision Your Organization will Make Regarding Cyber Risk Management is ...

... How Your Organization will Conduct Cyber Risk Management ...

Many Organizations Struggle to Justify, Fund, Establish, Implement and Mature their Cyber Risk Management Programs ...
Begin With the End in Mind

Assume:
- Breach of 10,000 Records
- Cost Per Record Breached = $402.00
- Annual Rate of Occurrence (ARO) = 50% = once every 2 years

Then:
- Single Loss Expectancy (SLE) = 10,000 x $402.00 = $4,020,000
- Annual Loss Expectancy (ALE) = SLE x ARO = $4,020,000 x 50% = $2,010,000

Questions:
- Would you invest $500,000 in controls to avoid a $2,010,000 ALE?
- Would you invest $2,000,000 in controls to avoid a $2,010,000 ALE?
- If the ARO of 50% was wrong, could that affect your decision?
- If the SLE of $4,020,000 was wrong because the $402.00 was wrong, could that affect your decision?

Our Focus: Impact / Cost Per Record Breached

Discussion Flow

1. Problem
2. Solution
3. Results
4. Resources

How to Build Your Cyber Security Business Case

1. Form and charter a cross-functional task force of key, peer stakeholders (e.g., Legal, Finance, HR, Risk Management, Compliance, IT, Privacy, Security, Clinical, Quality, etc.)
3. Research OCR Resolution Agreements / Corrective Action Plans (48 as of this writing) and identify those most relevant, relatable to your organization. Analyze and summarize top 5 most relevant cases and “Lessons Learned”.

https://www.ansi.org/standards_activities/standards_boards_panels/idsp/protected_health_information.aspx
How to Build Your Cyber Security Business Case

4. With the help of your Executive risk broker, identify the connections between privacy/cyber risks, patient safety and your professional liability coverages (e.g., Med Mal, EPLI, D&O, cyber liability, etc.)

5. Complete three current state assessments; strategic, tactical and operational:
   1. Complete an objective, current state, strategic assessment of your information risk management (IRM) maturity
   2. Complete an objective, current state, tactical 10-point assessment of your privacy/security compliance and cyber risk mitigation program.
   3. Critically evaluate your latest operational risk analyses vis-a-vis emerging HHS OCR “Standards of care.”

6. Present Findings, Observations and Recommendations to C-Suite / Board. Request approval to build Plan of Action and Milestones (POAM), to include your Phase 1 proposed budget.

Industry/Expert Collaboration

Table of Contents
1. The Progression of the Health Care Ecosystem
2. The Evolution of Laws, Rules, and Regulations
3. PHI Data Breach Landscape
4. Threats and Vulnerabilities
5. Safeguards and Controls
7. Data Breach Costing Framework
8. Calculating the Cost of a PHI Breach
9. Finale
10. Appendices

Back to Likelihood and Impact

What ....
• Bad Things Could Happen?
• Vulnerabilities Exist?
• Offsetting Controls or Safeguards Exist?
• Is the Likelihood of that Bad Thing Happening?
• Is the Potential Impact if the Bad Thing Happens?

Think Like Your Insurance Carrier:
Frequency and Severity!
Risk Equation...were it this simple...

\[ \text{Risk} = f([\text{Asset} \times \text{Threat} \times \text{Vulnerability}] \times \text{Controls}) \times ([\text{Likelihood} \times \text{Impact}]) \]

In What Controls Should We Invest $ to Reduce Likelihood and/or Impact?

Risk Management Objectives

What is risk exposure after applying a control?

Determining Likelihood

What ....

• Bad Thing Could Happen?
• Vulnerabilities Exist?
• Offsetting Controls or Safeguards Exist?

• Is the Likelihood of that Bad Thing Happening?
Likelihood of a Bad Thing Happening?

Risks to Health Information are Accelerating...

- Breaches are UP
- Ransomware is UP
- Hacking attacks are UP
- Complaints are UP
- Fines & Penalties are UP
- Phase II OCR Audits are UNDERWAY

It's a matter of when, not if...

Enforcement is Increasing...

OIG's Recommendations to OCR:
1. Strengthen oversight of compliance
2. Improve investigation processes and documentation
3. Develop an efficient search and tracking system
4. Fully implement a permanent audit program

Developing Your Business Plan...

What ....
- Bad Thing Could Happen?
- Vulnerabilities Exist?
- Offsetting Controls or Safeguards Exist?
- Is the Likelihood of that Bad Thing Happening?
  - Is the Potential Impact if the Bad Thing Happens?
Accretive Health Share Price & Story

Cost Per Breached Record By Industry

Industry/Expert Collaboration
Repercussions...

Cost of PHI Breach

Reputational Repercussions

Financial Repercussions

Legal/Regulatory Repercussions

Operational Repercussions

Clinical Repercussions

Time to get to work....


Reputational Repercussions and Considerations

Relevance Considerations
- Type of Business (CE or BA)
- Availability of Competitive Alternatives
- Acceptability of Competitive Alternatives

Impact Considerations
- Size of the Breach
- Sensitivity of Data
- Demographics of Affected Individuals
Abnormal Churn Rates

“The biggest financial consequence to organizations that experience a data breach is lost business. Following a data breach, organizations need to take steps to retain customers’ trust to reduce the long-term financial impact.”

Sensitivity to Privacy Matters – Demographics Matter

Cost of Replacing Staff

Recruiters Charge 20-35% of Starting Salary

Not including advertising, administrative time, and interview costs
Financial Repercussions and Considerations

Relevance Considerations
- Size of Breach
- Complexity of Breach
- Strength of Safeguards
- Type of Company (public or private)
- Breached Party (CE or BA)

Impact Considerations
- Size of the Breach
- Type of Breach (intentional vs. non-intentional)
- Further Disclosure
- Type of Data (financial as well as health)

In the Model: Financial Repercussions

Remediation
- Detection/Escalation Cost
- Credit Monitoring
- Identity Theft Monitoring

Mitigation
- Encryption
- Replacement of Stolen/Lost Asset
- Workforce Training
- Lost Productivity

Notification
- Affected Individuals
- Media
- Attorney Fees

Changing Ba
- Due Diligence
- Transition

Credit & ID Theft Monitoring

Wide Range: $10 - $25/month/person

## Elements of Notification Costs

<table>
<thead>
<tr>
<th>Notification to Affected Individuals</th>
<th>Over 500 records</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Set Up of Contact Databases</td>
<td>Notification to Media</td>
</tr>
<tr>
<td>• Message Development</td>
<td>• Identification of Local Media</td>
</tr>
<tr>
<td>• Legal Review</td>
<td>• Message Development</td>
</tr>
<tr>
<td>• Printing</td>
<td>• Legal Review</td>
</tr>
<tr>
<td>• Postage</td>
<td>• Inquiry Response Time</td>
</tr>
<tr>
<td>• Assembly</td>
<td>Notification to HHS</td>
</tr>
<tr>
<td>• Call Center Support</td>
<td>• Content Development</td>
</tr>
<tr>
<td></td>
<td>• Legal Review</td>
</tr>
<tr>
<td></td>
<td>• Inquiry Response Time</td>
</tr>
</tbody>
</table>

**PR and/or IR Campaign**

<table>
<thead>
<tr>
<th>Content Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal Review</td>
</tr>
<tr>
<td>Advertising</td>
</tr>
<tr>
<td>Inquiry Response Time</td>
</tr>
</tbody>
</table>

## Cyber Liability Insurance – Common Coverage

- Cyber insurance very focused on healthcare
  
  - Significant competition between insurance companies
    
    - Health care system 10,000 employees
      
      - $10MM limit
      
      - Deductible of $250,000 - $500,000
      
      - Premium $175,000/year - $225,000

- Coverage:
  
  - 3rd party liability: $10MM with sub-limits of $2MM for breach response and $250K for defense costs
  
  - Breach response coverage: notification, crisis management (PR & law firm guidance), ID theft monitoring, forensics, fix-ups, fines and penalties, credit card fines & penalties, government regulatory settlements (not fines and penalties), consumer redress


## The Cost of Changing Business Associates

- Cost of Time on RFP and Due Diligence on New Vendor
- Legal Costs negotiating BA Agreement
- Cost of Transition (Duplicate Cost during Transition to New Vendor)
- Incremental Higher Annual Cost of New Vendor

CHECK YOUR BUSINESS ASSOCIATE AGREEMENTS FOR INDEMNIFICATION
### Legal & Regulatory Repercussions and Considerations

**Relevance Considerations**
- Size of Breach
- Public vs. Private Company
- Strength of Compliance Program
- History of Previous Breaches
- Board Oversight
- Residual State of Affected Individuals
- Accreditation Requirements

**Impact Considerations**
- Size of the Breach
- Type of Breach (intentional vs. non-intentional)
- Type of Breach (malicious vs. non-malicious)
- Type of Data (financial as well as health)
- Demographics of Affected Individuals
- Celebrity Status of Affected Individuals
- Resident State of Affected Individuals

---

### Settlement $ and Settlement # of Cases Are Increasing

**Settlement Totals per year ($000s)**
- 2008: $100
- 2009: $2,250
- 2010: $1,035
- 2011: $6,166
- 2012: $4,850
- 2013: $3,741
- 2014: $7,940
- 2015: $6,193
- 2016: $23,505
- 2017*: $11,796

**Average /Settlement ($000s)**
- 2008: $100
- 2009: $2,250
- 2010: $518
- 2011: $2,055
- 2012: $970
- 2013: $748
- 2014: $1,134
- 2015: $1,032
- 2016: $1,808
- 2017*: $23,505

*2017 data thru 4/12/17

### Class Action Lawsuits $1,000-$2,500 per record

- St. Joseph Health System-$7.5MM Settlement+$7.5MM attorney fees
- State of Texas – 3.5 MM state employees
- Stanford Hospital & Clinic - 20,000 patients
- Sutter Health Hit With $1B Class-Action Lawsuit
- Patient files $20M lawsuit against Stanford Hospital
- TRICARE Health Management Sued for $4.9B
- AvMed Health sued over 'one of the largest medical breaches in history'
- Emory Healthcare Faces Class-Action Suit Over Data Breach

Court widening view of data breach damages, lawyers say
St. Joseph Health System Sets Class Action Lawsuit over Data Breach

“St. Joseph Health System settled with a cash payment of $7.5 million to participating settlement class members. The court documents also indicate that St. Joseph spent an additional $7.5 million on identity theft protection, $13.0 million to institute policies to comply with federal & state, and $7.5 million in attorney’s fees... And, $2.1 million OCR Settlement...”

$37.54 Million and counting... 31,800 records ➔ “$1,200 per record

Operational Repercussions and Considerations

Relevance Considerations
- Sufficiency of Current Resources
- Level of Change in Procedures Required
- Level of Oversight of Compliance Program

Impact Considerations
- Type of Breach (intentional vs. non-intentional)
- Type of Breach (malicious vs. non-malicious)
- # of Additional Resources Needed
- Level of Disruption of Organizational Changes

Clinical Repercussions and Considerations

Relevance Considerations
- Type of Data
- Likelihood of Compromise
- Involvement in Research

Impact Considerations
- Type of Breach (intentional vs. non-intentional)
- Type of Breach (malicious vs. non-malicious)
- Type of Research

http://www.ponemon.org/local/upload/file/Third_Annual_Survey_on_Medical_Identity_Theft_FINAL.pdf
The Home Stretch...

### Clinical Repercussions

- Medical Fraudulent Claims Processed
  - 10,000
  - 30,000
- Average cost per claim
- Total Cost of Fraudulent Medical Claims Processed
- Estimated Incurred Loss/Opinion
  - 3%
  - 5%
- Average cost per claim
- Total Estimated Incurred Loss
- Total Impact of Data Breach

### “Sanity-Check” Your Calculations

**Trends in the frequency of compromised records and customer turnover**

- The more records lost, the higher the cost of data breach. Figure 8 shows the relationship between the total cost of data breach and the size of the incident for a benchmark company in ascending order by the size of the breach incident. This cost component includes the direct and indirect costs of data breach, which increase with the size of the breach incident. The larger the breach, the more the company is exposed to the risk of a data breach with a breach size of more than 10,000 records up to one million.

**Figure 8: Total cost of data breach by size of the breach incident**

- Averages are just that – some will be higher, some lower
- And your cost model includes the “hard to calculate costs” that Ponemon doesn’t include

### Updated Cost Per Record Breached

Assume:
- Breach of 10,000 Records
- Cost Per Record Breached = $707.00
- Annual Rate of Occurrence (ARO) = 50% = once every 2 years

Then:
- Single Loss Expectancy (SLE) = 10,000 x $707.00 = $7,070,000
- Annual Loss Expectancy (ALE) = SLE x ARO = $7,070,000 x 50% = $3,535,000

Questions:
- Now, would you invest $500,000 in controls to avoid a $3,535,000 ALE?
- Now, would you invest $2,000,000 in controls to avoid a $3,535,000 ALE?

What’s the Cost of Breached PHI for Your Organization?
How to Build Your Cyber Security Business Case

1. Form and charter a cross-functional task force of key, peer stakeholders (e.g., Legal, Finance, HR, Risk Management, Compliance, IT, Privacy, Security, Clinical, Quality, etc.)


3. Research OCR Resolution Agreements / Corrective Action Plans (47 as of this writing) and identify those most relevant, relatable to your organization. Analyze and summarize top 5 most relevant cases and "Lessons Learned".

4. With the help of your Executive risk broker, identify the connections between privacy/cyber risks, patient safety and your professional liability coverages (e.g., Med Mal, EPLI, D&O, cyber liability, etc.)

5. Complete three current state assessments; strategic, tactical and operational:
   1. Complete an objective, current state, strategic assessment of your information risk management (IRM) maturity.
   2. Complete an objective, current state, tactical/adaptive assessment of your privacy/security compliance and cyber risk mitigation program.
   3. Critically evaluate your latest operational risk analytics vis-a-vis emerging HHS OCR "standards of care".

6. Present Findings, Observations and Recommendations to C-Suite / Board. Request approval to build Plan of Action and Milestones (POAM), to include your Phase 1 proposed budget.
Discussion Flow

1. Problem
2. Solution
3. Results
4. Resources

Business Outcomes

Stronger Financials ...
Balance sheet, lower cost of capital, competitive insurance rates

Lower Career Risk ...
Confidence, passion, energy, engagement, taking the right risks

Higher Satisfaction ...
Patients, physicians, workforce members, board, investors, community

Increased Quality ...
Access to care, timely care, confidentiality, integrity & availability of information

Fewer/No Breaches, Fewer/No Complaints,
No Failed IRM-related Audits, Preparedness,
Self-Sustaining Organization

Discussion Flow

1. Problem
2. Solution
3. Results
4. Resources
Supplemental Materials

1. The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security
2. Costing Model for Calculating the Cost of a Data Breach for Your Organization
3. Links to OCR Enforcement Actions

Links to Supplemental Guidance from OCR

48 OCR Enforcement Actions ... 5 already in 2017 / 13 in 2016

Organizations Struggling with Basic Information Risk Analysis / Management
- Not asset-based – systems / apps / technology that create, receive, maintain or transmit ePHI
- Not comprehensive enough – every asset in every LOB in every facility in every location
- Not detailed enough - not considering every asset threat/vulnerability scenario
- Not following OCR/NIST guidance / 9 essential elements
- Not enough documentation / evidence of vibrant ongoing program

FEATURED WEBINAR

WHAT OCR EXPECTS IN YOUR HIPAA RISK ANALYSIS:
A Conversation with Former OCR Director, Leon Rodriguez

MAY 3, 2017 | 11am-12:30pm CT

YOU DON'T WANT TO MISS THIS
COMPLIMENTARY, INTERACTIVE DISCUSSION
of OCR’s emerging standard of care in performing the required HIPAA Risk Analysis.

LEARN MORE | REGISTER
Contact

Bob Chaput, CISSP HCISPB CRISC, CIPP/US

bob.chaput@ClearwaterCompliance.com
Phone: 800-704-3394 or 615-656-4299
Clearwater Compliance LLC
http://www.ClearwaterCompliance.com

Please complete the session evaluation – we value your feedback!

1. Are you spending the right amount on your exposures?
2. Are you spending too much on low exposures?
3. Are you spending too little on high exposures?
4. Is the cost of a data breach for your organization known?
5. Is the cost of a data breach for your organization used in decision making?
Classic Risk Response Choices

1. Do you know your Kittens, Mosquitos, Crocodiles and Tigers?
2. Are you spending too much on your Kittens, Mosquitos, Crocodiles and not enough on your Tigers?

Fines and Settlement Agreements are Increasing

July 71, 2016
Multiple alleged HIPAA violations result in $2.75 million settlement with the University of Mississippi Medical Center (UMMC)

- Theft of an unencrypted laptop
- Generic username and password
- No Implementation of Security Violations procedures
- Organizational Deficiencies
- Insufficient Institutional Oversight
- No Risk Management Activity

$2.75MM
3 year Corrective Action Plan

“We at OCR remain particularly concerned with unaddressed risks that may lead to impermissible access to ePHI.”

Fines and Settlement Agreements are Increasing

- Multiple reports of breaches
- Widespread vulnerabilities
- No BA Agreement
- Sensitive Information
- Multiple Risk Analysis – Insufficient Remediation

$2.7MM
3 year Corrective Action Plan

“This settlement underscores the importance of leadership engagement and why it is so critical for the C-suite to take HIPAA compliance seriously.”
Fines and Settlement Agreements are Increasing

August 4, 2016

- Three breach reports
- Failed to conduct risk analysis
- No BA agreement
- Unencrypted laptop in unlocked care
- No policies & procedures or facility access controls

$5.55MM
3 year Corrective Action Plan

“We hope this settlement sends a strong message to covered entities that they must engage in a comprehensive risk analysis and risk management to ensure that individuals’ ePHI is secure.”

State AGs and HIPAA Violations

- New York State – The University of Rochester Medical Center – 3,400 records - $15,000
- Puerto Rico – Triple S Salid – 13,000 records - $6.8MM
- Indiana – dentist - $12,000
- Connecticut – Hartford Hospital and EMC - 8,900 records - $90,000, Health Net - $210,000
- Massachusetts – Beth Israel Deaconess Medical Center - $100,000, South Shore $750,000, Boston Children’s $400,000, 4 pathology practices $140,000
- Minnesota – Accretive Health - $2.5MM

For costing purposes, research fines and penalties in your own state