Are you prepared for a Ransom Attack?

Downtime Preparedness for IT, Clinical and Business Operations
How a CIO Can Prepare

Presented by:

Sandra Murray, MBA, PMP, CISM
Joy Bauer, RN-BC, PMP, CPHIMS, CHTS-CP, CMUP
Directors, HealthNET Systems Consulting, Inc.
HealthNET
SYSTEMS CONSULTING INC

Your CATALYST to Quality Care and Financial Performance Using Information Technology

Healthcare Data Analytics

System Implementations

IT Strategy and System Selection

| 1990 Massachusetts S Corp. MBE Certified | Dedicated to Healthcare Over 400 clients | Independence & Knowledge of Major Software Products |

Strategy | Project Leadership | Technology and Analytics | Professional Resources | Systems
Presenter Introductions

Joy Bauer, RN-BC, PMP, CPHIMS, CHTS-CP, CMUP

- 30 year clinical informaticist and IT systems professional
- Roles include clinical and IS leadership, large-scale system implementation management, interim CIO
- Adept at complex problem solving around technology, infrastructure, privacy and security

Sandra Murray, MBA, PMP, CISM

- 25+ year IT leadership professional
- Multiple leadership roles managing information systems technical teams
- Project leadership roles include large scale system implementations and optimizations, merger and acquisitions, system selections
- Credentials Certified Information Security Manager and ITIL certification
Downtime Preparedness
How a CIO Can Prepare

Learning Objectives:
• Statistics and examples of recent downtime events
• Why Healthcare systems are targeted at an increased rate
• Components of a downtime policy and procedure
• Ensuring patient care and business operations can continue
• Guides to help you prepare for downtime
Healthcare Statistics

• Ransomware up 89% from 2016 to 2017
• Costs expected $11.5 billion in 2019
• 70% of incidents originated by phishing emails
• #1 in cyber attacked industry
• 45% of ransomware attacks in 2017
• Average cost is $1.4 million dollars to recover
• On average 308 days to discovery of events
Examples

**Alabama**
- Sarrell Dental - two week down
- DCH Health System - 3-system hospital 2 weeks doors closed
- Springhill Memorial

**California**
- Hollywood Presbyterian Medical Center - Feb 2016
- Alvarado Hospital Medical Center - malware disruption
- Chino Valley MC and Desert Valley Hospital

**Maryland**
- MedStar Health - 10 hospitals and 250 OP sites went to paper

**Indiana**
- Kings Daughters Health — went to manual process

**Massachusetts**
- Partners
- New Bedford

**University of Connecticut**
Why Healthcare

Last and Fast
- Greater than 80% growth in use of EHR since 2004
- Implementation outpaced security measures

Rich $$$ data
- PII and PHI
- Proprietary clinical research
- Personnel can be a risk

Broad and Diverse relationships
- Billing companies
- Insurers
- Providers
  - M&A, divestures, decommissions

Dealing with Patient Life
What Makes Downtime So Complex

Awareness

Response and Repair

Data recovery

Training

Different facilities geographically dispersed

Different EHR infrastructures

Age of equipment
What Makes Downtime So Complex

Dependent on outside vendors
  • Telecomm
  • ISP
  • Cloud
  • Third party solution providers
  • Service Level Agreements

Continuing care of critical patients
  • New research shows critical heart patients care declines
  • Having work arounds for technology dependent care
Downtime Planning and Process

- IT Governance is essential
- IT Governance is essential - not a typo
- You have a downtime plan covering entire organization
- Executive leadership has reviewed departmental policies
- Do you have a plan?
  - What is the maximum amount of time you have planned to be down
  - Does execution of your plan meet your RTO (Recovery Time Objective)?
  - Does it meet your RPO (Recovery Point Objective)?
- Plan for data restoration
- You have a resource plan to execute all of the required activities
Downtime Planning and Process

- What happens if an internal disaster is called during your downtime
- You have current downtime forms for essential processes
- Do your providers and staff know how to work from paper?
  - Do you have downtime documentation, order, and result tools?
  - Are all shifts prepared?
  - Have you practiced with off sites and all hour shifts?
- Do your providers and clinicians know how to work without technology
  - Equipment
  - POC testing
  - ICU procedures using technology
Downtime Planning and Process

- Know your organization – governance, reporting structure
- Written procedures and policies
  - who to contact
  - visual diagrams
  - communication teams - external and internal
  - legal team engaged - determine if the incident reportable
  - insurer-keep track of financial costs
- Drills
- Lessons Learned reviewed and included in policy/practice
Ensuring Your Business Remains Operational

- **Paper processes known and available**
  - Registration
  - Documentation
  - Orders
  - Billing
  - Time keeping
  - Payroll

- **Ongoing internal and external communication -TRUST is KEY**
  - Communicate to public
  - Communicate minimum twice daily to providers
  - Communicate to internal staff routinely
  - Communicate honestly as to data and uptime expectations
Ensuring Your Business Remains Operational

• **Resources**
  - Leadership to make decisions
  - Management to guide staff and resources
  - Front line staff to perform patient care
  - IT and IS staff to remediate current situation
  - IT and IS staff carry on with the daily operations as possible

• **Clinical Care**
  - Manual equipment for routine care (VS, cardiac pressures, ect.)
  - Drills and checks to ensure staff competent
  - Forums to discuss concerns for care
  - Alternative plans for critical processes
Planning Resources

- **NIST**
  
  https://www.nist.gov/services-resources
  
  https://www.nist.gov/cyberframework

- **SAFER Guides**
  
  https://www.healthit.gov/topic/safety/safer-guides

- **HIPAA Guide**
  

- **AHIMA – Plan B**
  
  http://library.ahima.org/doc?oid=95715#.XbmjH55YZhE

- **Risk Assessment**
  
Notes & Links

- https://www.massgeneral.org/disaster-medicine/assets/PDFs/Downtime%20Toolkit.pdf
- 10 Sickening Healthcare Ransomware Statistics 2018 [Infographic] – Kraft
- Ransomware in Healthcare Facilities: A Harbinger of the Future?
- Reviewing Downtime Procedures Are Essential | HIMSS
- Three Ways to Improve Your Security Incident Response Plan – HIMSS