Clyde Hewitt
Ken Lobenstein
Jon Sternstein
Angel Hoffman

Biomedical Device Security
Session Overview

- Inadequate biomedical device security was once an unaddressed security pain point that grew with the computerization of critical point-of-care electronic equipment. The good news is that as cyber security awareness grows, healthcare organizations are partnering with medical device vendors to secure and test their products. This session will explore medical device trends and recent collaborative successes, along with ways that healthcare providers can drive advances in medical device security and patient safety.
Session Objectives

- Describe the respective responsibilities of both manufacturers and healthcare organizations that use the devices.
- Enumerate recent successes of manufacturers and healthcare organizations working together to improve biomedical device security.
- Discuss opportunities for healthcare providers to drive change in the medical device security status quo.
Disclaimer

• The views expressed in this presentation represent the speakers and to not reflect the views or opinions of their respective organizations
Discussion Flow

Hackers & Security Officers (Jon)

Regulators & Manufacturers (Ken)

Providers & Patients (Angel)
Medical Device Safety and Security (MeDSS)
AMC Security Conference

Deloitte & Touche LLP
June 2016
Introductions
Agenda

What are we going to talk about today?

- Evolution of medical devices
- Medical device cybersecurity landscape
- Industry response
- Product Security Program Framework
- Medical Device Security Program Framework
- Takeaways

Today's objective:
- Explore the medical device cybersecurity landscape and steps that can be taken to increase the security posture
Medical Device Evolution
Early Electrocardiograph

Developing For Reliability vs. Developing For Security

**Yesterday**

- Fixed function
- No local data storage
- Very limited “connectivity”
- Interaction requires physical access

**Today**

- Complex and changeable algorithmic driven behavior
- Sensitive data storage
- Interoperability requires network connectivity
- Remote access

Better Care & Lower Cost

New Risks!
It is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

In comparison, not having cybersecurity is similar to walking into a bank without cameras, security, or safes and being able to take the money.

Networked Medical Devices
- Connection is wired or wireless
- Communication via public internet, private network or point-to-point connection

Mobile Medical Apps

Remote Monitoring

Implantables

Diagnostics

Databases (PACS)

Capital Equipment

The Challenges with Expanded use of Networked Medical Devices
- More devices are becoming connected medical devices
- Varied responsibilities for purchase, installation and maintenance of medical devices
- Variable control over what is placed on the network
- Inconsistent training and education on security risks

Common Vulnerable IT Components

<table>
<thead>
<tr>
<th>Device Software</th>
<th>Firmware</th>
<th>Removable Media</th>
<th>Physical Access</th>
<th>Database and/or Storage</th>
<th>Clinical Applications (e.g., Treatment Planning Software)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Support/Maintenance</td>
<td>Device Hardware</td>
<td>Network Access/Firewall</td>
<td>Operating System</td>
<td>Ports/Interface</td>
<td></td>
</tr>
</tbody>
</table>

Cybersecurity
- It is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access
- In comparison, not having cybersecurity is similar to walking into a bank without cameras, security, or safes and being able to take the money.
Medical Device Cybersecurity Landscape
Recently, hackers are taking control of hospital networks using malware and demanding money to release control. This greatly impacts the providers as patients have to be directed to other hospitals since many of their devices and patient records are unavailable. Eventually, the hospital either has to pay the money, or completely reset their IT systems, including potentially buying all new infrastructure equipment.

Everyday, people download new smartphone apps without thinking, but there is a hidden danger. Apps from unknown sources can come infected with malware that can take over personal, and work email accounts, allowing hackers to use them for their to access sensitive information or send links to spoofing websites.

Many computers and medical devices are running ancient software that have multiple vulnerabilities. In addition, poor cyber awareness of manufacturer and hospital personnel gives attackers additional opportunities to take control of systems.
### Overview of Medical Device Cyber-threat Environment

<table>
<thead>
<tr>
<th>Threat actor (attacker)</th>
<th>Attacker end-goal</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee/Contractor</td>
<td>Harm to reputation of the provider</td>
<td>Patient safety</td>
</tr>
<tr>
<td>Organized Crime</td>
<td>Harm to reputation of the manufacturer</td>
<td>Disruption of clinical operations</td>
</tr>
<tr>
<td>Hacker</td>
<td>Personal satisfaction</td>
<td>Damage to the device</td>
</tr>
<tr>
<td>Malware author</td>
<td>Patient injury</td>
<td>Unauthorized disclosure of PHI/PII</td>
</tr>
<tr>
<td>Aggrieved party</td>
<td>Sale of PHI/PII²</td>
<td>Disruption to other hospital IT systems</td>
</tr>
<tr>
<td>Security researcher</td>
<td>Leverage device as an attack platform</td>
<td>Regulatory</td>
</tr>
</tbody>
</table>

*Note that this is not an exhaustive list of threats, impacts and attacker motivations*

---

² Protected Health Information/Personally Identifiable Information
Today’s Cybersecurity Landscape

- Medical device manufacturers are in various stages of implementing “security-by-design”
- No specific standards for “security-by-design” so device manufacturers are taking different approaches
- Healthcare providers are raising the bar regarding what they consider “adequate security controls” for medical devices that sit on their networks
- The US Food and Drug Administration (FDA) has issued a guidance on the “postmarket management of cybersecurity in medical devices”
- IoT and medical device cybersecurity are getting more press and news coverage
- The FDA and Congress are calling for action on healthcare’s preparedness to ransomware along with other cybersecurity threats following an increase in attacks

Overview of FDA’s Cybersecurity Guidance
FDA Premarket Guidance on Medical Device Cybersecurity

Three takeaways from the “Guidance”:

• Manufacturers should address cybersecurity during the “design and development” of the medical device

• The scope of the “Guidance” covers the following:
  - 510k, de novo submissions, pre-market approvals (PMAs), product development protocols, and humanitarian device exemption

• The FDA is looking for the following in their review of the above submissions:
  - A specific list of cybersecurity risks that were considered in the design of the device and a list, and justification for the cybersecurity controls that were established for the device;
  - A “traceability matrix” that links the actual cybersecurity controls to the cybersecurity risks that were considered;
  - A summary describing the plan for providing validated software updates and patches as needed throughout the lifecycle of the medical device to continue its safe and effective use;
  - A summary describing controls that are in place to help medical device software remain free of malware, especially from the point of conception to the point at which that device leaves the control of the manufacturer; and
  - Device instructions for use and product specifications related to recommended cybersecurity controls appropriate for the intended use environment.

The FDA recommends that medical device manufacturers consider the cybersecurity framework core functions to guide their cybersecurity activities: Identify, Protect, Detect, Respond, and Recover (found in NIST’s Framework for Improving Critical Infrastructure Cybersecurity).
Four takeaways from the “Guidance”:

• Medical device security is a shared responsibility between medical device manufacturers and healthcare providers

• The scope of the “Guidance” covers the following:
  ▪ Medical devices that contain software (including firmware) or programmable logic and software that is a medical device

• Critical components of cybersecurity risk management program include:
  ▪ Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk
  ▪ Understanding, assessing, and detecting presence and impact of a vulnerability
  ▪ Establishing and communicating processes for vulnerability intake and handling
  ▪ Clearly defining essential clinical performance to develop mitigations that protect, respond, and recover from cybersecurity risk
  ▪ Adopting a coordinated vulnerability disclosure policy and practice
  ▪ Deploying mitigations that address cybersecurity risk early and prior to exploitation

• Manufacturers should participate in cybersecurity ISAOs for sharing and dissemination of cybersecurity information and intelligence

The FDA recognizes that medical device cybersecurity is a shared responsibility between stakeholders including healthcare facilities, patients, providers, and manufacturers of medical devices.
Product Security
Deloitte Advisory Product Security Approach

- Analyze/Measure
  - Product Security Risk Assessment
  - Product Security Technical Testing
  - Product Security Program Assessment
  - FDA Cybersecurity Support

- Transform
  - Product Security Strategic Planning
  - Product Security Program Development
  - Product Security Program Implementation

- Sustain
  - Collective Threat Intelligence
  - Product Security Training and Communications
  - Periodic Reviews and Monitoring

Phases/Time:
- Stage 1: Initial
- Stage 2: Developing
- Stage 3: Defined
- Stage 4: Managed
- Stage 5: Optimizing

Maturity Levels:
Deloitte Advisory Product Security Program Framework™

Medical Device Manufacturers

- Governance
  - Marketing Leadership
  - Legal Leadership
  - R&D Leadership
  - Privacy Leadership
  - IT Security Leadership
  - Regulatory Compliance Leadership

- Operating Components
  - Security Risk Management
    + Product Security Requirements
    + Security Risk Assessment
    + Technical Testing
    + Third-Party Component security
  - Security Event Handling
    + Threat Intelligence
    + Patch & Vulnerability Management
    + Product Security Incident & Event Management
  - External Communications
    + Product Security Attributes
    + Vulnerability Communication
    + Inquiry Response
    + Regulatory Submissions
    + Security Authorization
  - Security Education & Training
    + Security Awareness
    + Secure Development
    + Program Processes
    + Product Lifecycle
  - Program Monitoring
    + Key Performance Indicators
    + Product Inventory
    + Program Audit Framework
    + Program Assessment Framework

- Conception → Analysis → Design → Build → Test → Manufacture & Market → Post-market Surveillance → End of Life

- Quality Management System (QMS)
  - Infrastructure and Security Components
  - Security Engineering
  - Industry & Organizational Context
Deloitte Advisory Medical Device Security Program (MDSP)™

Governance

Safe and Secure Medical Devices

Cybersecurity Steering Committee

Governance and Leadership

Information Security
Clinical Engineering
Physicians
Nursing staff
Procurement
Legal & Compliance as needed

Operating Components

Security Risk Management
+ Medical Device Security Requirements and Baselines
+ Security Risk Assessment
+ Third-Party Security

Security Event Handling
+ Threat Intelligence
+ Patch & Vulnerability Management
+ Medical Device Security Information & Event Management

External Communications
+ Medical Device Security Attributes
+ Information Sharing
+ Medical Device Inquiry Handling
+ Vendor Collaboration

Security Education & Training
+ Security Awareness
+ Secure Design
+ Program Processes
+ Medical Device Lifecycle

Program Monitoring
+ Key Performance Indicators
+ Medical Device Inventory
+ Program Audit Framework
+ Program Assessment Framework

Foundational Components

Centralized Document Repository

Infrastructure and Security Components

Security Engineering

Industry & Organizational Context

Acquisition
Testing
Implementation
Maintenance
Disposition

Healthcare Providers
Takeaways
Get involved with NH-ISAC\(^4\) and medical device consortia

- Sharing of cyber threat intelligence about fielded networked medical devices will be critical in understanding the current threat environment, modeling the changing cyber threat landscape and helping to create future security standards for medical devices.

Assess the cybersecurity risks of your medical device IT environment

- Implement a strategy to assess cybersecurity risks and mitigate patient safety impacting cyber risks first.
- Leverage technologies designed to identify advanced persistent threats (APT) that may have already bypassed your primary defenses.

Adopt a secure development lifecycle (SDL)

- “Build-in” security in the early requirements/design phases of new medical devices (or iterations of existing medical devices);
- Embed SDL into the “dna” of your product development teams.
- Healthcare providers should seek to understand if medical technology companies are embracing “security by design”.

Monitor the FDA’s direction on medical device security

- Currently, the FDA is leading the way regarding medical device security; other international regulatory agencies will likely follow suit.
- Continue to monitor the FDA’s direction and additional guidance on cybersecurity that may be forthcoming.

Takeaways
Some important actions for you to own

\(^4\) NH-ISAC—National Health – Information Sharing and Analysis Center
Medical Device Security

SECURITY OFFICER’S VIEWPOINT

JON STERNSTEIN – STERN SECURITY
Agenda

- Malware Threat
- Security Roadblocks
- NCHICA on FDA Guidance
Medical Device Malware

“The type and breadth of incidents has increased,” said William H. Maisel, chief scientist at the FDA’s Center for Devices and Radiological Health. “Now we’re hearing about [incidents] weekly or monthly.”
Medical Device Malware

- Cardiac catheterization labs shutdown
  - 2010-2011 Several Hospitals Affected
  - Malware caused downtime
  - Patients Redirected to separate hospital
Medical Device Malware

- Intensive Care Fetal Monitors Infected
  - Beth Israel Medical Center
  - Devices could not record any data
  - “Manufacturer refuses to allow OS updates or security patches”
Antivirus Misconfiguration

- Hemo Monitor Downed by Antivirus Software
  - Hemo monitor lost connection during cardiac catheterization procedure
  - Down 5 minutes while the patient was sedated
  - Had to reboot machine
  - Product security recommendations explicitly stated specific files/folders could not be scanned
Security Roadblocks

- Vulnerability Scans Prohibited
- No Antivirus
- No Security Patches
FDA Guidance

- Manufactures should adopt “Cybersecurity Framework”
- Address cybersecurity both premarket & postmarket
- Recertification not needed for security updates
NCHICA Response

- Recommendation vs. Requirement
- Penalties
- Publically disclose non-compliance
- Eliminate unsupported software
- Allow Security Testing
References

- Medical Device Malware [https://www.washingtonpost.com/national/health-science/facing-cybersecurity-threats-fda-tightens-medical-device-standards/2013/06/12/b79cc0fe-d370-11e2-b05f-3ea3f0e7bb5a_story.html](https://www.washingtonpost.com/national/health-science/facing-cybersecurity-threats-fda-tightens-medical-device-standards/2013/06/12/b79cc0fe-d370-11e2-b05f-3ea3f0e7bb5a_story.html)


REGULATIONS, SECURITY AND SAFETY

Angel Hoffman
Owner/Principal
Advanced Partners in Health Care Compliance
THE FDA’S GUIDANCE

January 15, 2016, the U.S. Food and Drug Administration (FDA) published a draft guidance titled, *Postmarket Management of Cybersecurity in Medical Devices*

This is following a number of reports of medical devices being hacked, and threatening the security of hospital computer networks.

FDA’s position – medical device security is a shared responsibility of both the device manufacturer and the medical facility using the equipment.
FDA RECOMMENDATIONS

- Companies should adopt the NIST *Framework for Improving Critical Infrastructure Cybersecurity*

- Manufacturers should develop comprehensive cybersecurity risk management programs

- Manufacturers should take a more proactive approach
CURRENT STATUS

- Today’s medical devices are designed to be networked
- To facilitate patient care
- Networked devices incorporate software that may be vulnerable to cyber security threats
- Vulnerabilities may pose risks to patient safety and the effectiveness of the medical device, requiring ongoing monitoring
PROACTIVE VS REACTIVE

Historically, the healthcare industry has been more reactive in their approach to addressing issues of all types.

In this scenario, a more proactive approach would include:

- Monitoring cybersecurity information sources to identify and detect cybersecurity vulnerabilities and risks
- Knowledge of the impact of vulnerabilities; assessing and detecting their presence
BEING PROACTIVE (CONT’D)

- Development and communication of organizational processes for vulnerability intake and handling

- Address and clearly define clinical performance, to mitigate risk and to protect, respond and recover from cybersecurity threats

- Develop policies and procedures and train employees

- Deploy mitigation strategies to detect cybersecurity risks early and prior to exploitation
NEED FOR STRONGER PROTOCOLS

Due to recent events…stronger medical device security protocols are needed.

July 2015 – Department of Homeland Security and FDA warned providers to avoid using and infusion pump due to a vulnerability which allowed hackers to gain remote control of the device.

Unauthorized users could change the dosage the pump delivers, leading to potential complications and/or death.
HOSPIRA SYMBIQ INFUSION PUMP
ANOTHER EXAMPLE

In 2010 – a New Jersey VA catheterization lab closed temporarily, when the computerized devices were infected with malware.

Risks:

- Too risky to take a chance to perform any procedures under this predicament; patients could face complications or death

- Potentially caused delay of care with individuals needing an emergency cath procedure (e.g. cath lab to surgery)
PATIENT SAFETY

Overall, the concern for patient safety should be the primary concern.

Everyone is a patient at one time, whether inpatient or outpatient.

Changing a patient’s weight could deliver too much or too little medication (multiple IV medication dosages are based on Kilograms).

Too much IV pain medication could cause respiratory depression, from which a patient could respiratory arrest and eventually die.

An insufficient amount of IV medication in an uncontrolled and sustained rapid heart rate could result in damage to the heart.
Implantable and Other Devices

As technology moves forward, this will become an increasing concern:

Pacemakers

Implantable cardioverter defibrillators (ICDs)

Insulin Pumps (e.g. security researcher, Jerome Radcliffe, demonstrated how he could wirelessly hacked into his own pump)

Also, patient monitors, infusion pumps, ventilators, and imaging machines have the technology to becoming wireless

Incorporating information from wearable devices into EHR

Information shared with Health Information Exchanges (HIEs) has the potential to impact multiple organizations
HOSPITALS

Hospitals under attack:

- Hollywood Presbyterian Medical Center in LA paid $17,000 in bitcoins to hackers in order to get their EHR back online.

- MedStar Health had 10 hospitals come to a standstill when their EHR went down.
FDA RECOMMENDATIONS FOR HOSPITALS

- Restricting unauthorized access to the network and networked medical devices.
- Making certain appropriate antivirus software and firewalls are up-to-date.
- Monitoring network activity for unauthorized use.
- Protecting individual network components through routine and periodic evaluation, including updating security patches and disabling all unnecessary ports and services.
- Contacting the specific device manufacturer if you think you may have a cybersecurity problem related to a medical device.

To assist in reporting a specific medical device vulnerability, contact ICS-CERT at 877-776-7585 or ics-cert@dhs.gov.
CLOUD STORAGE

Questions/Concerns:

Will there be an increase in vulnerabilities with more EHR data being stored here?

What about a potential for an increase in breaches?

If large corporations (e.g. retail) are having issues controlling information being hacked, how will healthcare succeed?

Healthcare has more information than retailers and banks.
PROBLEMATIC

Internet of Things (IOT):

- As this becomes more common, incidents with hackers will continue to increase (e.g. insulin pump)
- Leaving a wider opportunity for entry points into a system
- Use of medical devices using/collecting PHI could lead to opportunities for identity theft and/or global spying
WHAT ABOUT NATIONAL SECURITY?

U.S. National Security Agency (NSA) can use information for both domestic and international spying - known due to Edward Snowden, whistleblower in 2013.

Use in foreign intelligence…the NSA is researching the possibilities for exploiting internet connected medical devices from thermostats to pacemakers.

May be easier ways to obtain information than through medical devices, but just knowing the possibility exists is concerning to healthcare providers.
Angel Hoffman
Owner/Principal
Advanced Partners in Health Care Compliance
FDA RECOMMENDATIONS

- FDA guidance published - following a number of reports of medical devices being hacked and threatening the security of hospital computer networks.

- Companies should adopt the NIST *Framework for Improving Critical Infrastructure Cybersecurity*

- Manufacturers should develop comprehensive cybersecurity risk management programs

- Manufacturers should take a more proactive approach
CURRENT STATUS

- Today’s medical devices are designed to be networked

- To facilitate patient care and improve overall quality of care

- Networked devices incorporate software that may be vulnerable to cyber security threats

- Vulnerabilities may pose risks to patient safety and the effectiveness of the medical device, requiring ongoing monitoring
Historically, the healthcare industry has been more reactive in their approach to addressing issues of all types.

In this scenario, a more proactive approach would include:

- Monitoring cybersecurity information sources to identify and detect cybersecurity vulnerabilities and risks
- Knowledge of the impact of vulnerabilities; assessing and detecting their presence
- Impact to patient care, expected outcomes, morbidity and mortality
WHAT CAN BE DONE?

- Development and communication of organizational processes for vulnerability intake and handling

- Address and clearly define clinical performance, to mitigate risk and to protect, respond and recover from cybersecurity threats

- Develop policies and procedures and train employees on them

- Deploy mitigation strategies to detect cybersecurity risks early and prior to exploitation

- Work collaboratively, across departments and avoid working in silos
NEED FOR STRONGER PROTOCOLS

Due to recent events…stronger medical device security protocols are needed.

July 2015 – Department of Homeland Security and FDA warned providers to avoid using an infusion pump due to a vulnerability which allowed hackers to gain remote control of the device.

Unauthorized users could change the dosage the pump delivers, leading to potential complications and/or death
HOSPIRA SYMBIQ INFUSION PUMP
ANOTHER EXAMPLE

In 2010 – a New Jersey VA catheterization lab closed temporarily, when the computerized devices were infected with malware.

Risks:

- Too risky to take a chance to perform any procedures under this predicament; patients could face complications or death
- Potentially caused delay of care with individuals needing an emergency cath procedure (e.g. cath lab to surgery)

Result: All of which jeopardizes both patient safety and the bottom line – too costly related to patient lives as well as overall productivity
Overall, the concern for patient safety should be the primary concern.

Everyone is a patient at some time, whether inpatient or outpatient.

Changing a patient’s weight could deliver too much or too little medication (multiple IV medication dosages are based on Kilograms).

Too much IV pain medication could cause respiratory depression, from which a patient could respiratory arrest and eventually die.

An insufficient amount of IV medication in an uncontrolled and sustained rapid heart rate could result in damage to the heart.
As technology moves forward, this will become an increasing concern:

Pacemakers

Implantable cardioverter defibrillators (ICDs)

Insulin Pumps (e.g. security researcher, Jerome Radcliffe, demonstrated how he could wirelessly hack into his own pump)

Also, patient monitors, infusion pumps, ventilators, and imaging machines have the technology to becoming wireless

Incorporating information from wearable devices into EHR

Information shared with Health Information Exchanges (HIEs) has the potential to impact multiple organizations
Hospitals under attack:

- Hollywood Presbyterian Medical Center in LA paid $17,000 in bitcoins to hackers in order to get their EHR back online.

- MedStar Health had 10 hospitals come to a standstill when their EHR went down.
FDA RECOMMENDATIONS FOR HOSPITALS

- Restricting unauthorized access to the network and networked medical devices.

- Making certain appropriate antivirus software and firewalls are up-to-date.

- Monitoring network activity for unauthorized use.
Protecting individual network components through routine and periodic evaluation, including updating security patches and disabling all unnecessary ports and services.

Contacting the specific device manufacturer if you think you may have a cybersecurity problem related to a medical device.

Notifying the FDA

To assist in reporting a specific medical device vulnerability, contact ICS-CERT at 877-776-7585 or ics-cert@dhs.gov.
CLOUD STORAGE

Questions/Concerns:

- Will there be an increase in vulnerabilities with more EHR data being stored here?
- What about a potential for an increase in breaches?
- If large corporations (e.g. retail) are having issues controlling information being hacked, how will healthcare succeed?
- Healthcare has more information than retailers and banks.
PROBLEMATIC

Internet of Things (IOT):

- As this becomes more common, incidents with hackers will continue to increase (e.g. insulin pump)
  
- Leaving a wider opportunity for entry points into a system
  
- Use of medical devices using/collecting PHI could lead to opportunities for identity theft and/or global spying
WHAT ABOUT NATIONAL SECURITY?

U.S. National Security Agency (NSA) can use information for both domestic and international spying - known due to Edward Snowden, whistleblower in 2013.

Use in foreign intelligence…the NSA is researching the possibilities for exploiting internet connected medical devices from thermostats to pacemakers.

May be easier ways to obtain information than through medical devices, but just knowing the possibility exists is concerning to healthcare providers.
THE FUTURE OF HEALTHCARE

Relies on:
- Our ever vigilant watch
- Ongoing commitment
- Never taking your eye off the prize
- Putting patients before money: ETHICS
- Doing the right thing! (don’t put money before integrity and quality)

We are **changing the world** through medicine and technology

But at what cost to…
human life, privacy, dignity and financial theft?
Post Lunch Brain Stretch
Audience Participation

- With biomedical devices embracing the Internet of Things, how does this impact our healthcare organization structure?
- Will biomedical engineering stay in a separate business unit or become part of the IT area of responsibility?
- Will the scope of the security officer’s responsibility expand to meet the larger risk area?
- Whose responsibility is it anyway to secure these systems?
- With certain wearable devices becoming more prolific, will the line between EHR and PHR be defined more by policy than technology?
- What role do we expect our EHR vendors to play in this space?
Audience Participation

• Open Discussion
Backups

• Legal Stuff Follows
This presentation contains general information only and Deloitte Advisory is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte Advisory shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, “Deloitte Advisory” means Deloitte & Touche LLP, which provides audit and enterprise risk services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. Deloitte Transactions and Business Analytics LLP is not a certified public accounting firm. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.