eHEALTH INITIATIVE
Real Solutions. Better Health.

Privacy and Security: Enterprise Risk Management and Third Party Risk Management

**Audio for this webinar streams through the web. Please make sure the sound on your computer is turned on and you have speakers. If you need technical assistance, please contact ReadyTalk Customer Care: 800.843.9166.

Housekeeping Issues

- All participants are muted
    - To ask a question or make a comment, please submit via the chat feature and we will address as many as possible after the presentations.
- Audio and Visual is through www.readytalk.com
    - If you are experiencing technical difficulties accessing audio through the web, there will be a dial-in phone number displayed for you to call. In addition, if you have any challenges joining the conference or need technical assistance, please contact ReadyTalk Customer Care: 800.843.9166.
- Today’s slides will be available for download on our homepage at www.ehidc.org

About eHealth Initiative

- Since 2001, eHealth Initiative is the only national, non-partisan group that represents all the stakeholders in healthcare.
- Mission to promote use of information and technology in healthcare to improve quality, safety and efficiency.
- eHealth Initiative focuses its research, education and advocacy efforts in four areas:
  - Using Data and Analytics to Understand and Improve Care
  - IT Infrastructure to Support Accountable Care
  - Technology for Patients with Chronic Disease
  - Connecting Communities through Data Exchange

ANNUAL CONFERENCE 2014

THE ROADMAP TO HEALTHCARE DELIVERY TRANSFORMATION

January 28-29, 2014 | CHAMPIONSGATE FL

Discussion Topics Include:

#eHI2014

- ***Disruptive Innovations in Data and Technology: Lessons Learned from Other Industries***
- ***Leveraging Analytics to Support Population Health***
- ***Privacy and Security: Challenges and Best Practices***
- ***Much More!***

REGISTER NOW ▶

Visit www.ehidc.org for more information.

MEDEANALYTICS® MEASURE. MANAGE. LEAD.

Medicity A Healthagen Business

accenture

eHEALTH INITIATIVE Real Solutions. Better Health.

1EDIsource

RelayHealth

OPTUM™

ANNUAL CONFERENCE 2014

THE ROADMAP TO HEALTHCARE DELIVERY TRANSFORMATION

January 28-29, 2014 | Orlando, FL

Early Bird Rates Expire January 2!

REGISTER NOW

#eHI2014

Sponsorship Opportunities Available!

Exhibit Booths Available!

Visit www.ehidc.org for more information.

MEDEANALYTICS
MEASURE. MANAGE. LEAD.

Medicity
A Healthagen Business

accenture

eHEALTH INITIATIVE
Real Solutions. Better Health.

1EDIsource

RelayHealth

OPTUM

Thank You to Our Sponsor

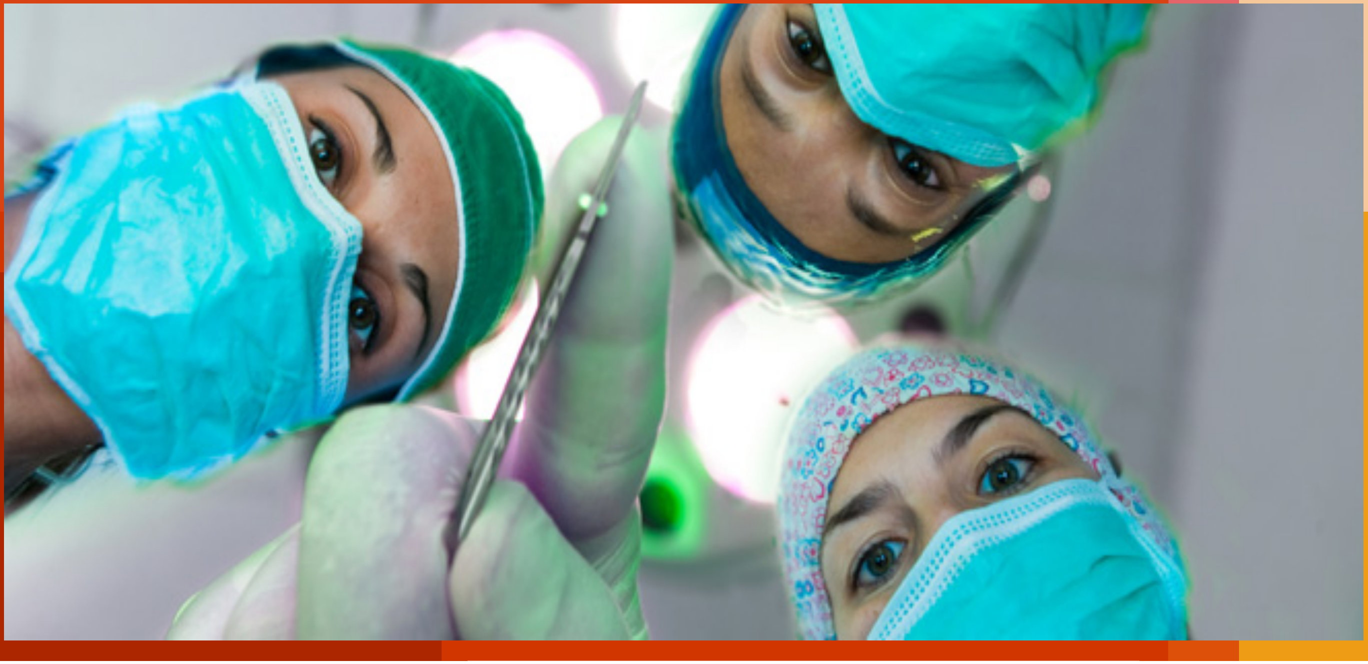
pwc

Today's Agenda

- Welcome & Introductions
  - Rebecca Jones, Program Manager, eHealth Initiative
- Creating a Culture that Values Privacy & Security
  - Nalneesh Gaur, Director, PwC
- Enterprise and Third Party Risk Management
  - Mark Lantzy, Chief Information Officer, WellCare Health Plans
  - Ted Webster, Senior Director, Information Security, WellCare Health Plans
- Panel Discussion
- Q&A from Audience

Creating a Culture that Values Privacy & Security

Healthcare Privacy and Security Landscape
Dec 17th 2013



Nalneesh Gaur, Director
PwC
Nalneesh.Gaur@us.pwc.com

Healthcare marred with rising Incidents and inadequate countermeasures

21.7 Million Patients impacted[1]

~875K records exposed in Q1 2013[2]

94% of hospitals exposed in past two years[3]

54% suffered multiple breaches by 3rd parties[4]

69% of medical devices are vulnerable[4]

85% breaches due to negligence , lost or stolen devices[4]

Less than one-third encrypt sensitive data[5]

only 41% require third parties to comply with their privacy policies [6]

Only 39% have an incident response process [6]

1 US. Department of Health and Human Services, 2013

2. Identity Theft Resource Center, 2013

3 Third Annual Benchmark Study an Patient Privacy and Data Security, Ponemon Institute, December 2012

4 Securing Outsourced Consumer Data, Ponemon Institute, February 2013

5. Is Your Company Ready for a Big Data Breach?, Ponemon Institute, March 2013

6. PwC 2013 GISS Survey

HHS is increasingly vocal in sharing its Security and Privacy Concerns

Privacy

1. Impermissible uses and disclosures of protected health information;
2. Lack of safeguards of protected health information;
3. Lack of patient access to their protected health information;
4. Uses or disclosures of more than the minimum necessary protected health information; and
5. Lack of administrative safeguards of electronic protected health information.

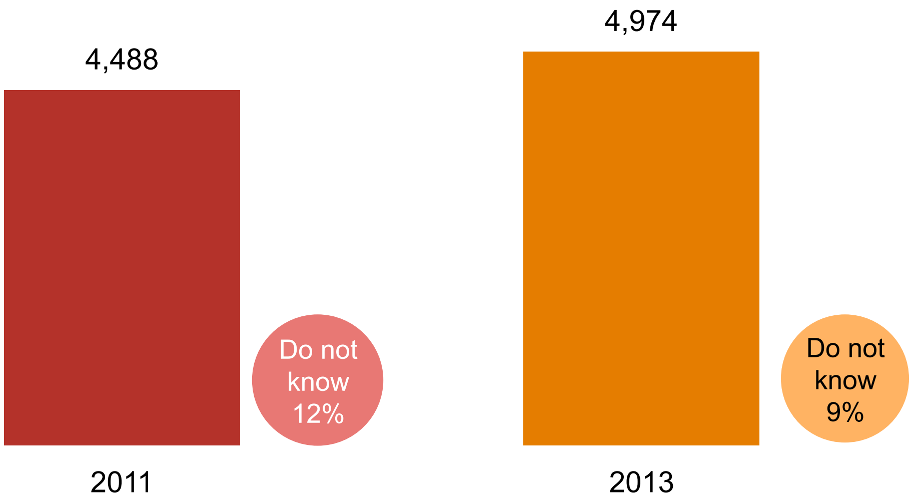
Security

1. Lack of risk analysis
2. Lack of security incident response and reporting
3. Lack of security awareness and training
4. Lack of access controls
5. Failure to address encryption and decryption (data in storage)

*Healthcare detecting more security incidents.**

The average number of incidents detected in the past 12 months increased by 11% compared with two years ago. This increase is evidence of today's elevated threat environment and perhaps respondents' improved ability to identify incidents.

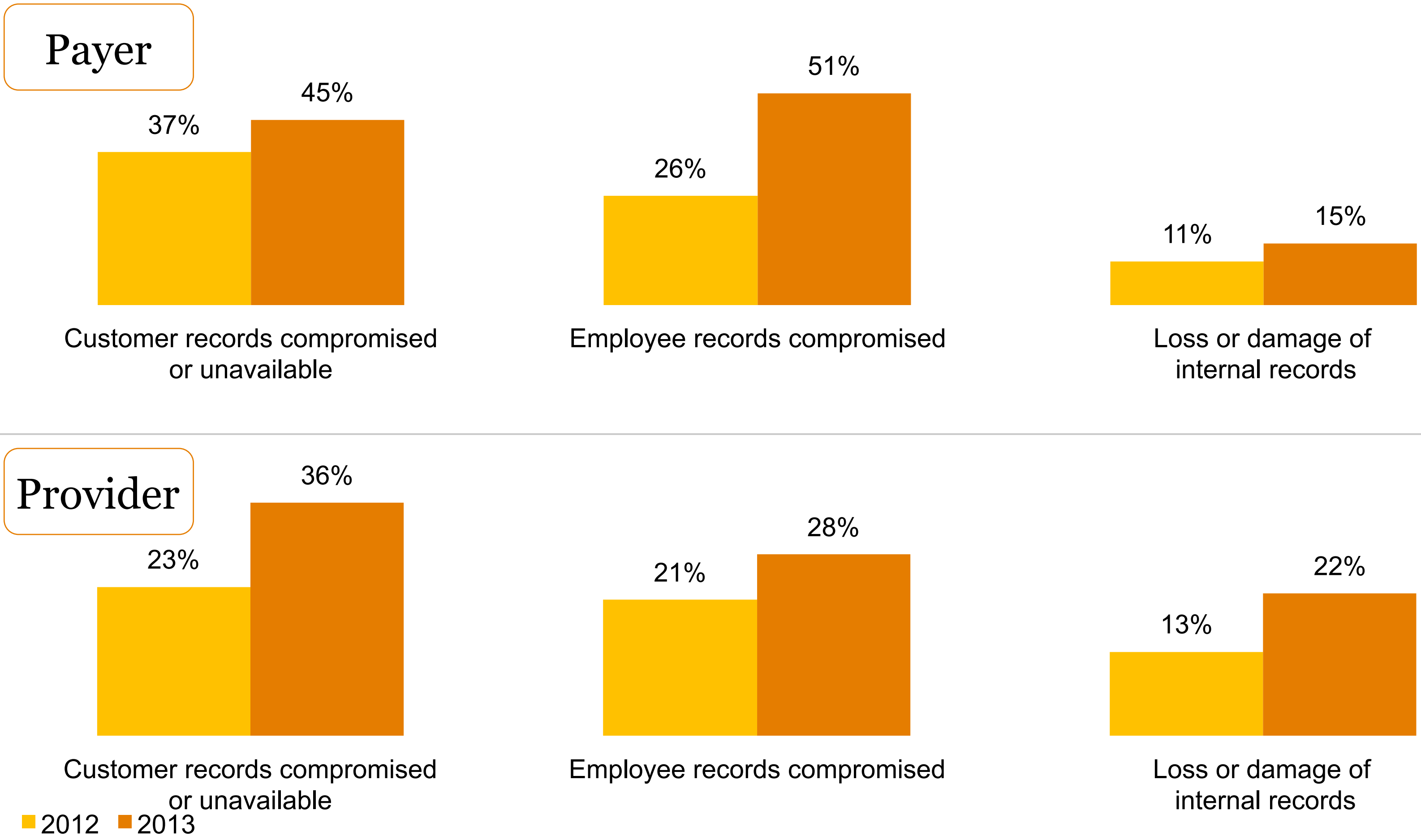
Average number of security incidents in past 12 months



* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: "What is the number of security incidents detected in the past 12 months?"

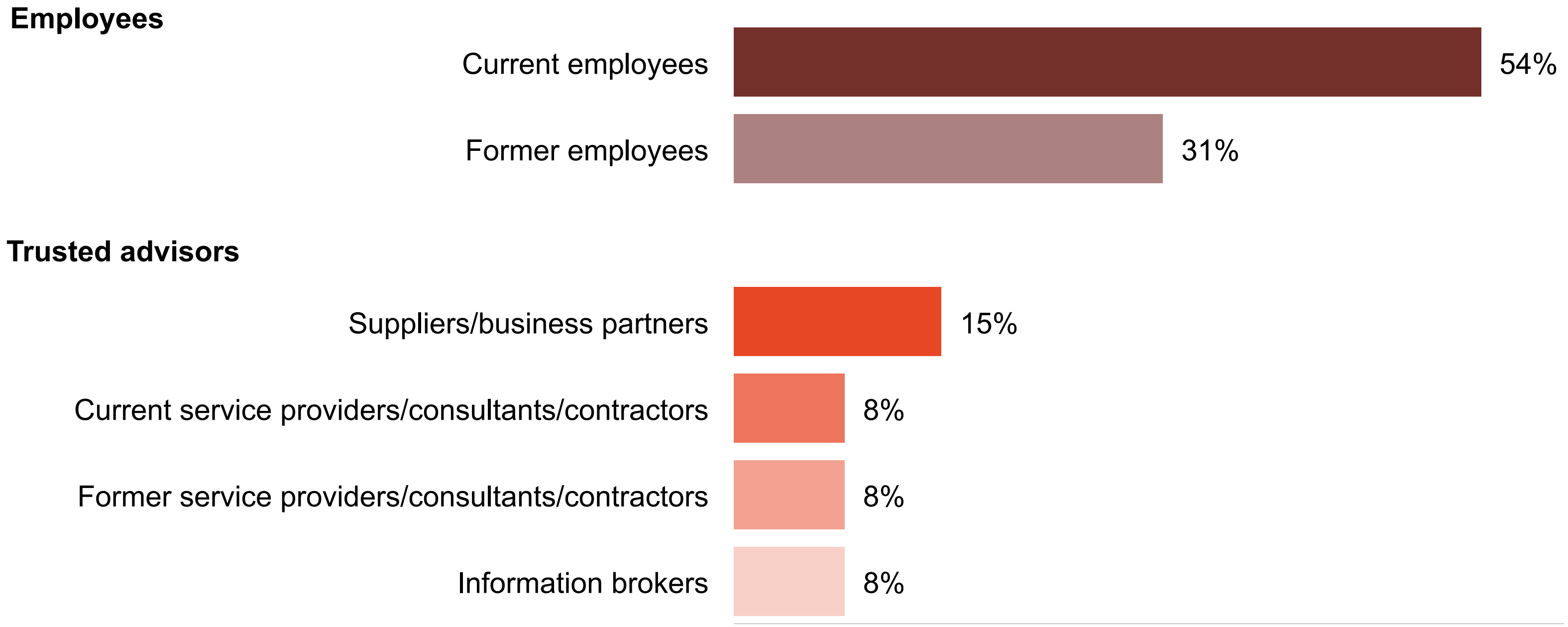
Healthcare respondents report an increase in loss of employee and customer data as a result of incidents.



Question 22: “How was your organization impacted by the security incidents?” (Not all factors shown.)

Insiders, particularly employees, are cited as a source of security incidents by most healthcare respondents.

It's the people you know—current or former employees, as well as other insiders—who are most likely to perpetrate security incidents.



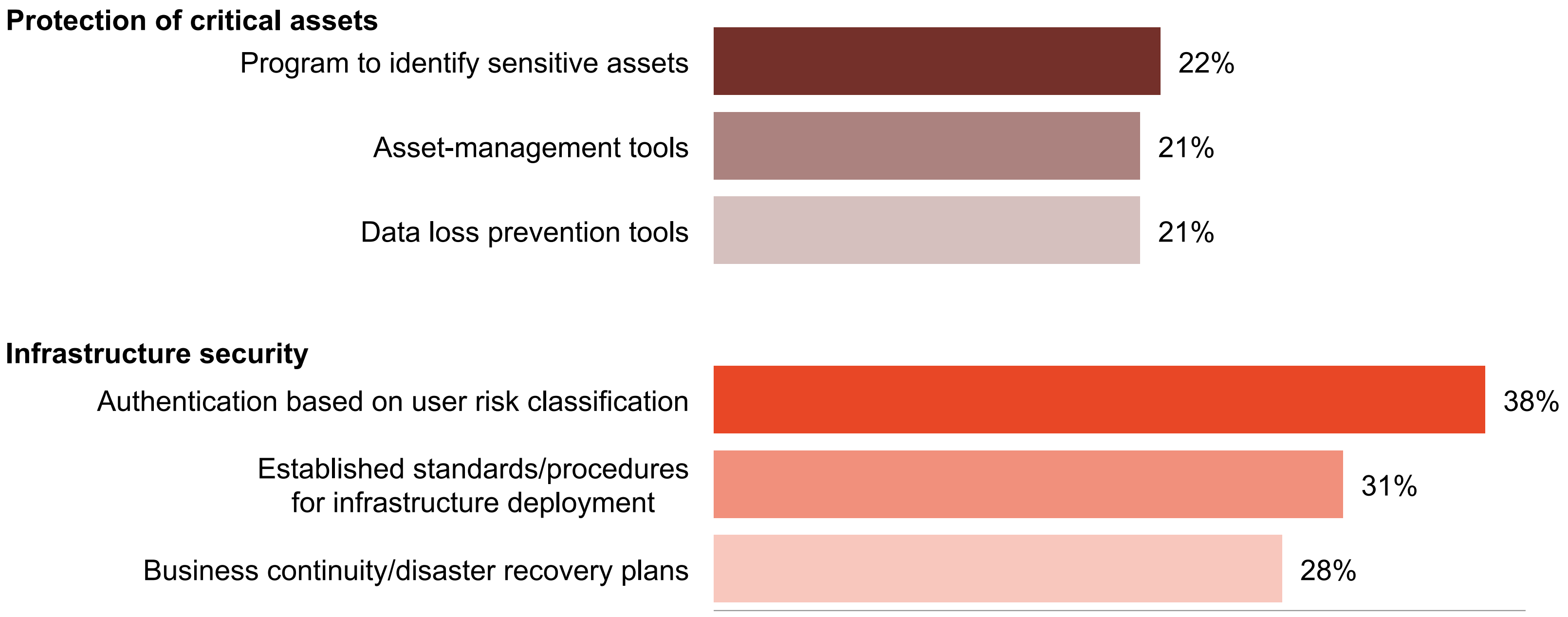
Estimated likely source of incidents

Question 21: "Estimated likely source of incidents" (Not all factors shown.)

What business imperatives and processes will healthcare prioritize this year?

Some of the highest priorities cited by respondents include technologies that can help the organization protect its most valuable assets and secure the infrastructure.

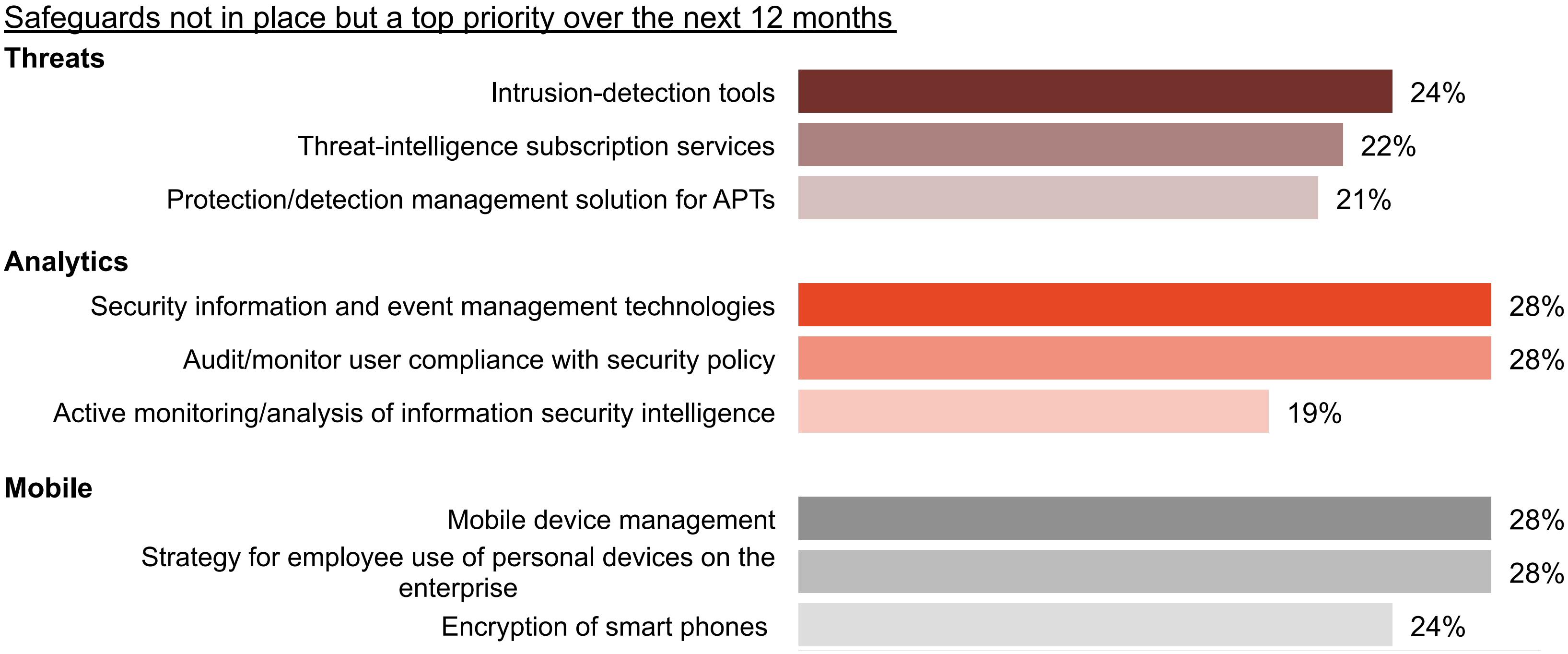
Safeguards not in place but a top priority over the next 12 months



Question 14: “What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?” Question 15: “What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?” (Not all factors shown.)

Other priorities focus on detecting and responding to threats.

Knowledge is power, and organizations are prioritizing technologies that can help gain a better understanding of threats as well as improve security for mobile devices.



Safeguards not in place but a top priority over the next 12 months

Question 14: "What process information security safeguards does your organization not have in place, but is a priority over the next 12 months?" Question 15: "What technology information security safeguards does your organization not have in place, but is a top priority over the next 12 months?" (Not all factors shown.)

Recap: Dramatically evolved risks, security strategies are compliance-based and perimeter-oriented

1 Stolen Patient and Employee information used to launch targeted phishing attacks

2 Expanded attack surface—partners, 3rd parties, suppliers, customers, and others

3 Hot-button technologies like cloud computing, mobility, and BYOD are implemented before they are secured

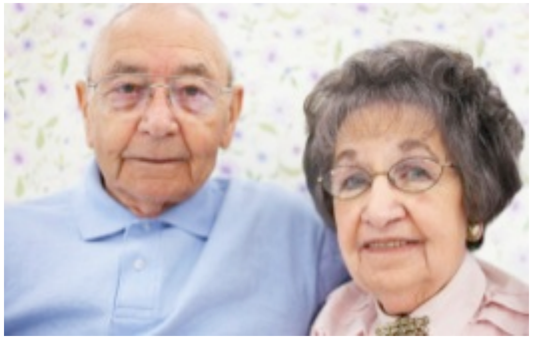
4 Unauthorized insiders and external threat perpetrators are gaining access to sensitive information

5 CISOs are unable to secure sensitive Information because they lack knowledge about its storage and flow

Thank you

Nalneesh Gaur, Director
PwC
Nalneesh.Gaur@us.pwc.com

WellCare



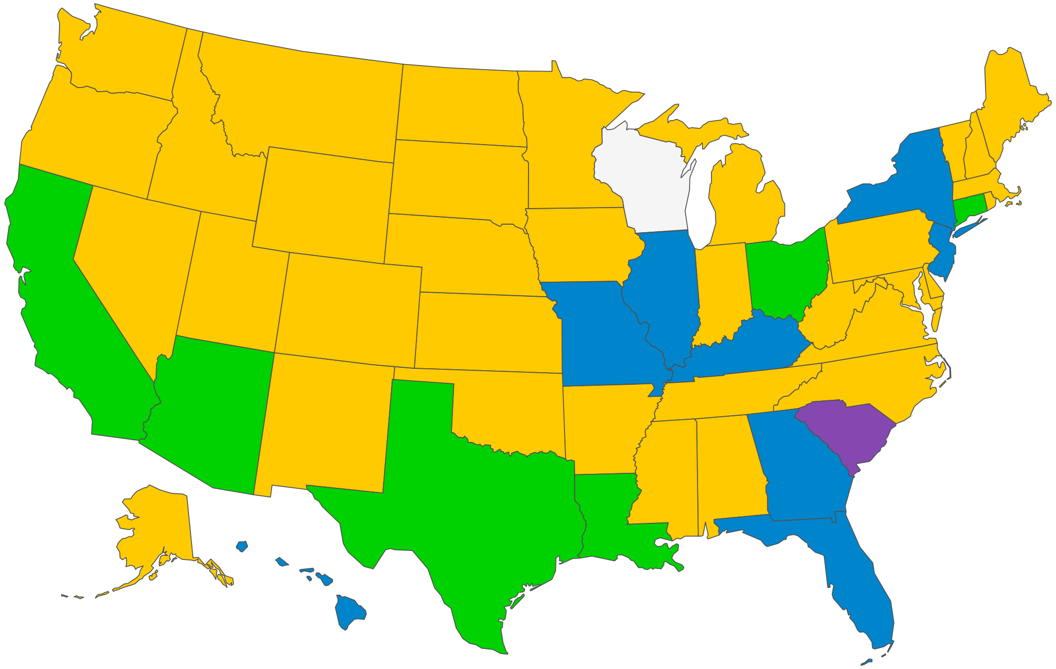
WellCare Health Plans, Inc.

Corporate Overview

December 17, 2013

WellCare Health Plans, Inc.

Company Snapshot



🟦 Medicaid, Medicare Advantage & Medicare Part D PDP
🟩 Medicare Advantage & Medicare Part D PDP
🟪 Medicaid & Medicare Part D PDP
🟨 Medicare Part D PDP (49 states & D.C.)

*Map as of Dec. 1, 2013

Founded in 1985 in Tampa, Fla.

- Approximately 2.8 million members nationwide.
- Approximately 222,000 contracted health care providers.
- Approximately 67,000 contracted pharmacies.

Serves approximately 1.8 million Medicaid members, including:

- Aged, Blind and Disabled (ABD).
- Children's Health Insurance Program (CHIP).
- Family Health Plus (FHP).
- Supplemental Security Income (SSI).
- Temporary Assistance for Needy Families (TANF).

Serves approximately 1 million Medicare members, including:

- Approximately 283,000 Medicare Advantage members.
- Approximately 784,000 Prescription Drug Plan members.

Serving the full spectrum of member needs

- Dual-eligible populations (Medicare and Medicaid).
- Managed Long Term Care.

Spearheading efforts to sustain the social safety net

- The WellCare Community Foundation.
- Advocacy Programs.
- Creation of Public-Private Partnerships.

Significant contributor to the national economy

- A FORTUNE 500 company.
- Ranked #16 in the nation on the Barron's 500.
- More than 5,100 associates nationwide.
- Offices in all states where the company provides managed care.

*Statistics as of Sept. 30, 2013

Information Security and Information Technology at WellCare

- Information Security and Information Technology report to separate Sr. VP’s
- Information Security reports through Corporate Compliance
- Gartner classifies this organizational structure as Medium/High maturity
- This structure creates a designed friction and accountability
- Security is funded as a business unit, not just an IT function
- Security must present valid business justifications and not just fear, uncertainty, and doubt
- Results in some dual ownership
- Potential for conflicting efforts and projects
- Emphasis on improved compliance
- Collaboration is key and supported by Information Security Council
- Leveraging HITRUST standard

Information Security and Information Technology at WellCare

Information Security Council

Chief Privacy Officer
Chief Financial Officer
Chief Compliance Officer
Chief Information Officer
Information Security Officer

Compliance

- Governance and Policy
- Platform and Network Security Requirements
- Application and Database Security Requirements
- Technical Vulnerability Management
- Third Party Security Assessments
- Security Deliverables within Software Development Lifecycle

Information Technology

- Technology Architecture
- Application and Database Design
- Identity and Access Management
- Software Development Life Cycle
- Access Reporting

Risk Assessment

Enterprise Risk Management

Information Security Risk Assessment and Management

- IT Assessments
- Information Security Program Assessments
- Business Managed Application Assessments
- Third Party Service Providers
- Business Associates
- HIPAA and PCI Compliance
- Information Security Maturity

Information Technology Risk Assessment and Risk Management

- Strategic Alignment
- Operational Effectiveness
- Compliance
- Data Classification
- Information Security (Availability, Integrity, and Confidentiality)
- Financial Integrity

Example: Vendor Management

HITECH forced a more active approach to vendor management.

Policy

- HIPAA requires BA’s to adhere to Security Rule

Objective

- Need assurances that can be quantified without assuming agency
- BAA renewals provided best opportunity to re-engage with BA’s on Security Rule assurances

Management

- Tracking with business area during initial acquisition or renewal
- Integrate Risk Assessment with Vendor Analysis
- Provide Assessment results to business area owner for ultimate risk awareness and acceptance

Risk Assessment

- Preliminary 14 question basic questionnaire provides enough information to allow for deeper dive if needed
- Additional follow-ups based upon vendor exposure and data being handled

Example: Business Managed Applications

As the cost of technology decreases and availability increases, business managed applications will continue to play a role in large enterprises.

Policy

- Business Managed Applications must apply the same controls as IT managed applications.

Objective

- Business Managed Applications pose an equal amount of risk as IT applications, yet traditionally haven't followed the same rules as IT or faced the same scrutiny.
- Shadow IT operates under the guise of being cheap and fast, similar to cloud technologies, but generally without the same controls as IT.

Management

- Registration of Applications
- Source code repository for in-house coded applications
- Education on base controls (ITGC's)
- Annual review of applications

Risk Assessment

- Basic Risk Self Assessment when applications are registered
- Leads to a larger self-assessment for medium and high risk applications
- A full assessment is then performed by Information Security with the remediation generally pointing higher risk apps to be migrated to IT

QUESTIONS / COMMENTS?

- Please submit questions and comments through the chat feature on Readytalk.

Thank You to Our Sponsor

pwc