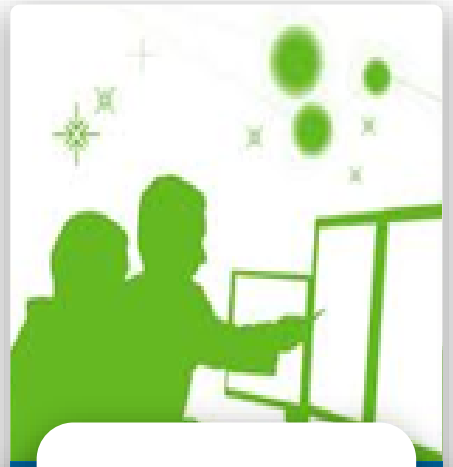
The Only Opportunity Our Industry has Against Cyber Criminals is to Work Together

Spencer Mott
Chief Information Security Officer and VP Information Security, Amgen

The world is around us is changing rapidly…

Passive Capture of HC Data Via Sensors

Technologies Enabling HC Decentralization



Collection and Integration of All HC Data

Shift From Art to Science of Diagnosis and Therapy Selection

The story of Robin Sage

facebook

Robin Sage requests friend

Confirm

LinkedIn

Connect with Robin Sage

Continue

Twitter

Follow Robin Sage

Today

- **Cybercriminals are increasingly interested in our business**

  And I'll explain why!

- **Collaboration across our ecosystem requires "collaborative" cyber-risk management initiatives**

- **Industry Chief Information Security Officers (CISOs) came up with a plan to set six "horizons"**

- **Next steps**

AMGEN®

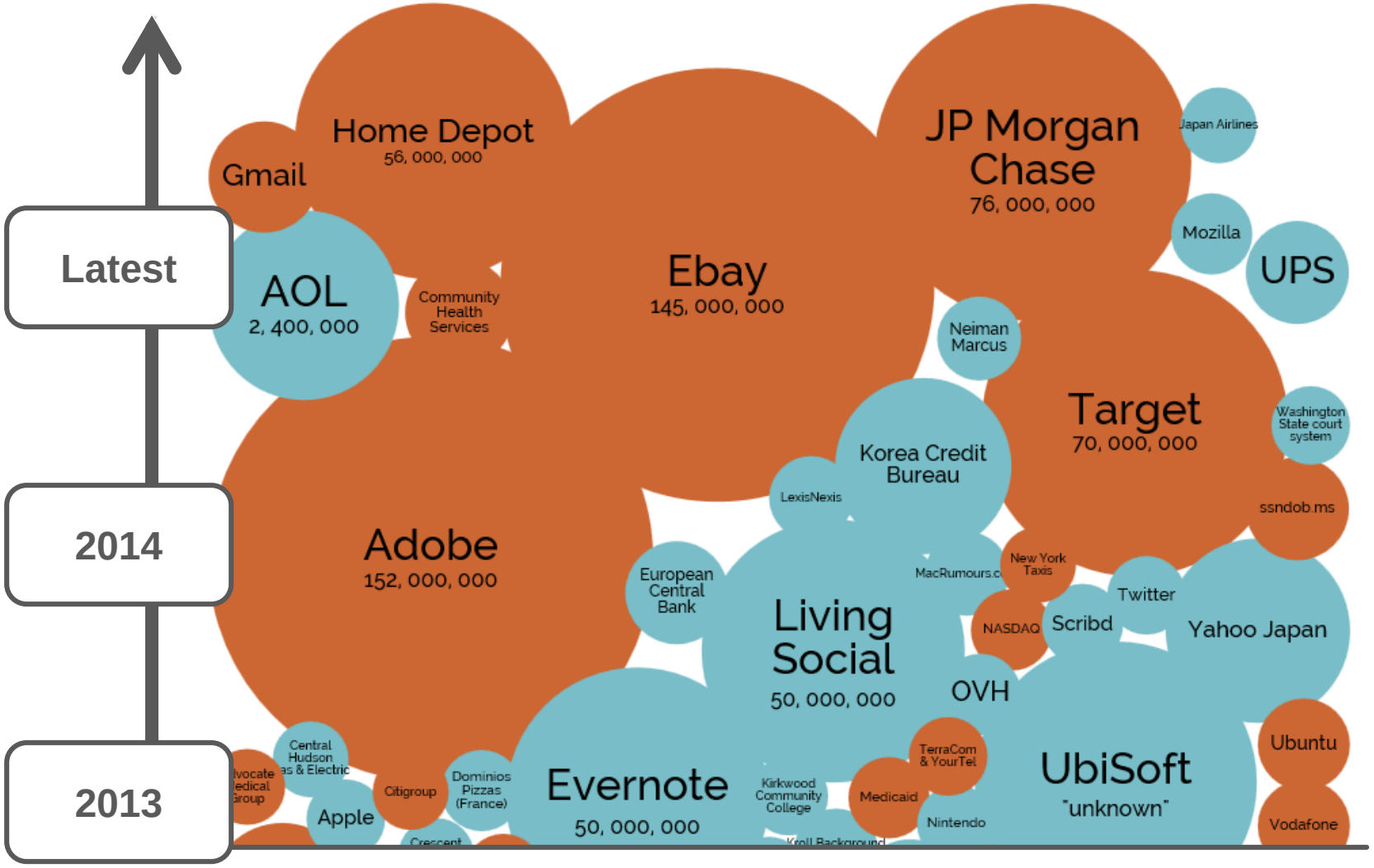
Cyber threats: A matter of *when* not *if*

Sources: [U.S. Department of Health & Human Services](#)

[Chronology of Data Breaches | Privacy Rights Clearinghouse](#)

AMGEN

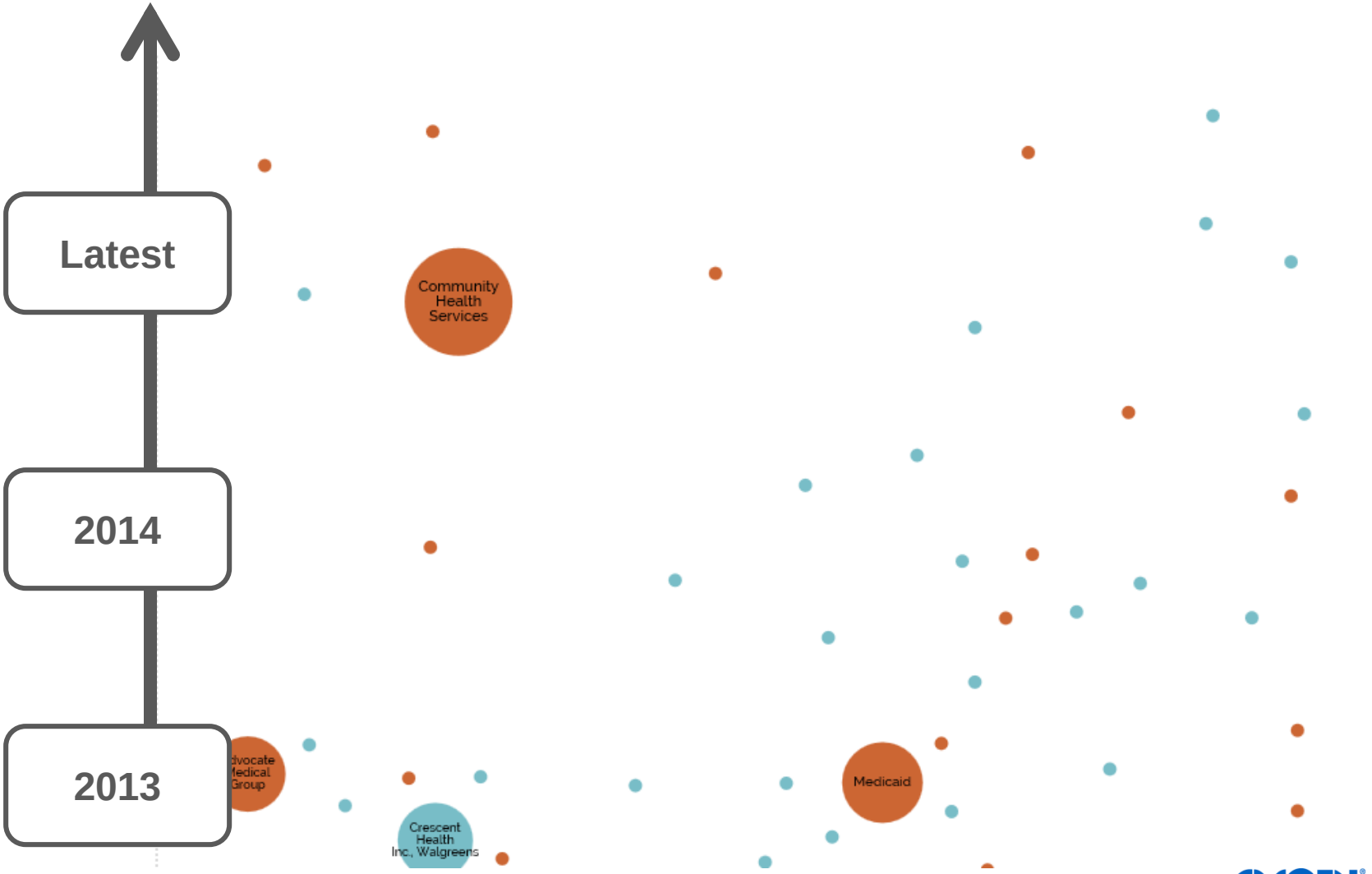
Attacks are impacting more people and at an increasing rate…



Source: http://www.informationisbeautiful.net/

AMGEN

… and the healthcare industry is gaining more attention from cyber criminals



Source: http://www.informationisbeautiful.net/

The payoff from stolen data makes our industry a very attractive target

Credit Card Data

vs

Health Data

10 - 20x greater value

$20,000 Average payout for medical identity theft

Source: 2014 Cyber Security White Paper, follow-on to Healthcare Innovation CIO Roundtable held in January 2014

AMGEN

And increasing risks make our industry an easier target

New technologies introduce new risks…

70%

of security executives have **cloud and mobile concerns**

2013 IBM CISO Survey

614%

Mobile malware growth in just one year

2012-2013 Juniper Mobile Threat Report

Source: IBM Corporation, 2014

… as well as human error and misuse.

OF INCIDENTS WERE

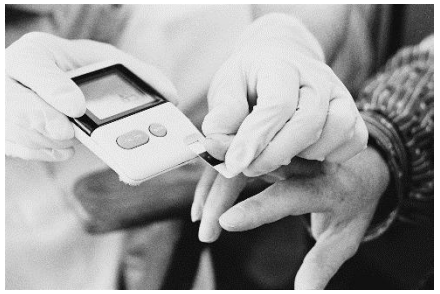
OF INCIDENTS WERE ATTRIBUTABLE TO INSIDER AND PRIVILEGE MISUSE.

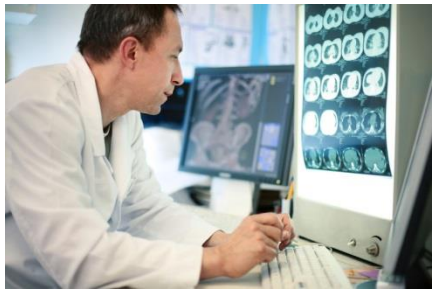
Source: Verizon 2014 Data Breach Investigations Report **HEALTHCARE**

AMGEN

Rapid digitization is outpacing traditional approaches and legal requirements for cyber security

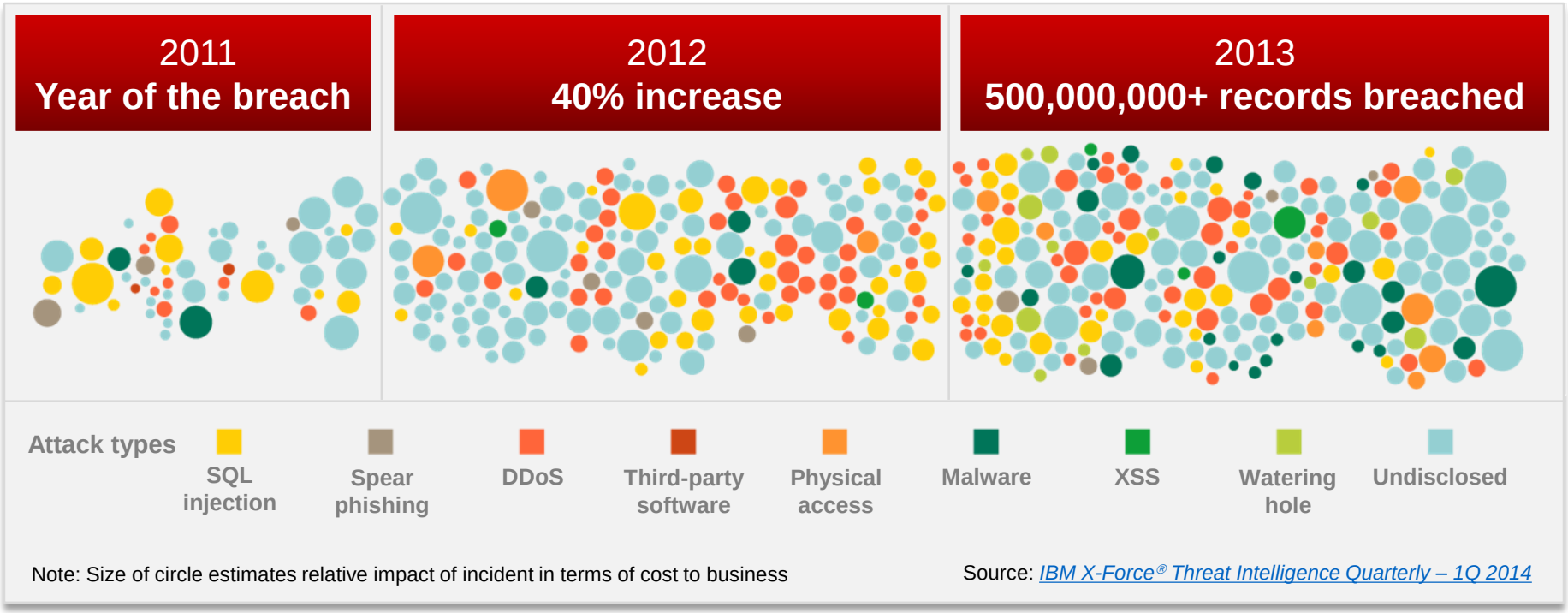
- Vastly extended technology surface that touches every aspect of the health management system
- Expanded interconnectivity between vendors and other 3rd parties
- Emerging technologies becoming embedded in “every-day” operations and devices
- Traditional views of security and privacy with a lens towards compliance vs risk management
- Reactive with cyber security and lagging more mature industries





Collectively these digitization trends are introducing new security risks to already susceptible IT ecosystems

Even with the better protection, sophisticated attackers break through safeguards every day



Note: Size of circle estimates relative impact of incident in terms of cost to business

Source: *IBM X-Force® Threat Intelligence Quarterly – 1Q 2014*

61% of organizations say **data theft and cybercrime** are their greatest threats

2012 IBM Global Reputational Risk & IT Study

$3.5M+ average cost of a **data breach**

2014 Cost of Data Breach, Ponemon Institute

Source: IBM Corporation, 2014

AMGEN

The Bottom Line:

Traditional security practices are unsustainable and a new approach is needed

85 security tools from **45** vendors

IBM client example

83% of enterprises have difficulty finding the **security skills** they need

2012 ESG Research

Source: IBM Corporation, 2014

As our companies come together in new ways to meet patient needs, we have an opportunity to work together to effectively combat cyber attacks against our industry.

Cybersecurity should not be a competitive advantage

A group of healthcare ~30 CISOs identified six collaboration opportunities

The following are being considered under the auspices of the NH-ISAC organization:

1. **Ensuring third parties have a compelling interest in protecting our companies**
2. **Managing information risk in high risk markets/situations**
3. **Common methodology and assessment to manage vendor risk**
4. **Common cyber risk communications with boards, regulators and employees**
5. **Sharing threat cybersecurity intelligence and best practices**
6. **Launching a shared security operations utility (SOC)**

The National Health Information Sharing & Analysis Center (NH-ISAC)

The tactical and operational arm of the private sector-led ISAC for ***advancing national healthcare and public health critical infrastructure resilience***.

ISACs are entrusted with advancing physical and cyber security protection by establishing and maintaining collaborative frameworks for operational interaction between and among members and external partners.

AMGEN

There are already several effective examples of collaboration in the healthcare industry

Collective security-related efforts include:

SAFE-BioPharma.

NH-ISAC

McKinsey Healthcare Information Risk forum

McKinsey&Company

Other industries have effective models of working collectively to address cyber security risk:

FINANCIAL SERVICES Information Sharing and Analysis Center

FS-ISAC is a not-for-profit member owned entity that serves as the industry's go-to resource for cyber and physical threat intelligence analysis and sharing

Processes up to 100,000 threat indicators per month for its 4,000+ members

AMGEN

There are compelling benefits to work together, which has been proven in other industries

- Lower labor and technology costs
- More effective ability to respond to threats
- Better access to talent
- Increased ability for smaller players (e.g., community hospitals) to reduce cyber risk
- Developed and scaled expertise
- Synergy of coordinated operational efforts
- Common information security data and metrics
- Joint resilience

What *Really* Matters

At the end of the day, protecting our information means we can all fulfill our collective mission of serving patients

**Whether we are discovering, developing, manufacturing or delivering innovative human therapeutics,
information is at the heart of helping patients**

AMGEN

AMGEN®

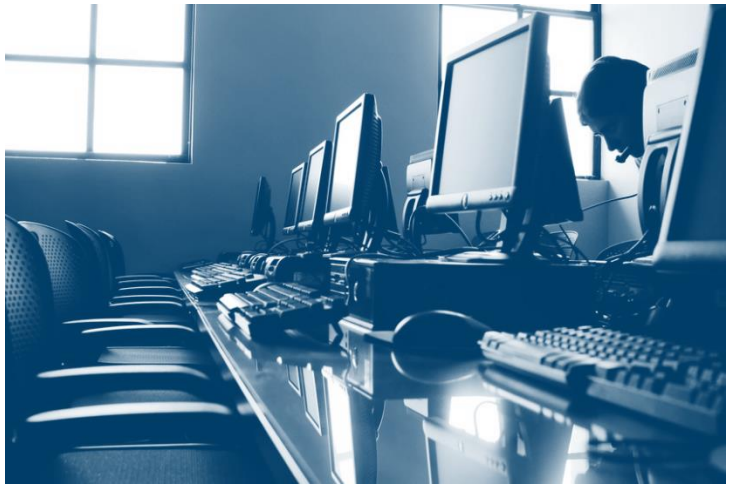
Pioneering science delivers vital medicines™

Thank you

Example:

Option 6

What a shared security operations center (SOC) would look like



- Offer shared services
  Such as first line triaging of alerts and incidents, vulnerability management, penetration testing, research, risk assessment
- Facilitate standards and knowledge/best practice sharing
- Complement existing in-house efforts

***Added benefit*: Companies can have the shared SOC perform more basic activities and redeploy information security resources to more challenging and rewarding next-level roles**

AMGEN®