The Good, The Bad and the Ugly of Complying with the HIPAA Security Rule

Hint: Compliance ≠ Security

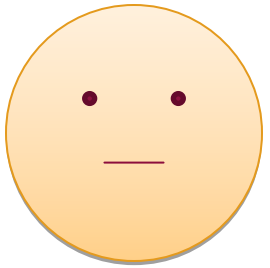
March 17, 2015

IDT911 Consulting

Unofficial Poll

Physicians who lead provider organizations believe:

- Patients will not change doctors because of a breach
- They believe OCR won't bother them if they are small
- They believe compliance is prohibitively expensive
- They believe this is not a patient care issue and that time and money is better spent on improving patient care



Myth #2 – Small Providers Are Not a Target

THE NATIONAL LAW REVIEW

March 16, 2015

PUBLISH / ADVERTISE WITH US TRENDING LEGAL NEWS ABOUT US CONTACT US QUICK LINKS SEARCH

8 NEW ARTICLES

View PDF

1) Click the download button
2) This will take you to our web page
3) Download the FREE product

Another Small Healthcare Provider Settles Potential HIPAA Violations Following Data Breach, Office For Civil Rights Announces

posted on: Sunday, December 29, 2013

A familiar story – *small health care provider suffers a d affecting patient data, reports incident to the federal Offi (OCR) and winds up becoming subject to an OCR investig beyond the breach itself, resulting in a significant settlen corrective action plan.*

In this case, a relatively small adult and pediatric der in Concord, Massachusetts has agreed to settle pote the Health Insurance Portability and Accountability A Privacy, Security, and Breach Notification Rules, agre payment and a comprehensive corrective action pla OCR review.

ARTICLE BY

Joseph J. Lazzarotti

Jackson Lewis P.C.

HIPAA: HHS Keys in on Security Rule for Small Hospice Organization

by Peter Notarstefano

Published On: Jan 15, 2013

Hospice of North Idaho, has agreed to pay $50,000 to the U.S. Department of Health and Human Services (HHS) to settle allegations of federal data security rule violations over the loss of a laptop containing the personal health information of 441 patients.

The organization has entered into a 2-year corrective action plan with HHS as part of the settlement.

Myth #3 - Compliance is prohibitively expensive

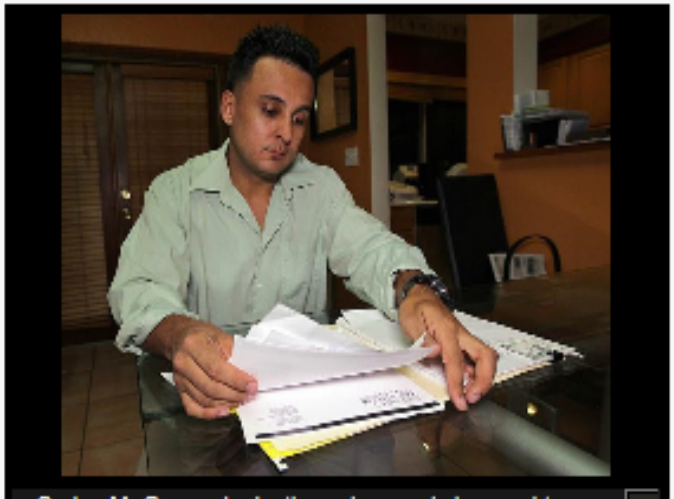
- Year after year the Verizon Data Breach report shows
  - 75% of victims were targets of opportunity
  - 78% of attacks were considered in the low to very low ‘difficulty level’
  - 76% of network intrusions exploited weak or stolen credentials

- Free or Inexpensive Resources
  - HHS Website tools
  - Open source software
  - Security as a service

Myth #4 – This is Not a Patient Care Issue

Banking bad: One man's ID-theft nightmare

Like 319



Carlos M. Gomez looks through records he used to help clear his name in a 2011 money-laundering case. A Wachovia bank employee stole his identity to open a fake accounted used to launder money also stolen from other bank customers. PEDRO PORTAL / EL

Fullsize Buy Photo ◀ previous | next ▶
Image 1 of 3

BY JAY WEAVER
JWEAVER@MIAMIHERALD.COM

Fighting a bad cold, Carlos Gomez had decided to sleep by himself that night so he wouldn't expose his wife.

He awoke to a nightmare. Just before dawn, insistent pounding on the front door jolted the ex-Marine and young father out of bed. Federal agents poured into his Kendall home, pushing his wife aside and rushing to his bedroom. They held guns to his face before slapping him in handcuffs.

"I kept asking, 'What is going on?' " recalled Gomez, who works as a UPS driver. "I was scared for my life."

Gomez, busted in a money laundering scheme, would spend nearly two weeks in a federal detention center and another seven months under house arrest.

It took 222 days before federal prosecutors realized it was all a terrible mistake: A rogue bank worker had stolen his identity.

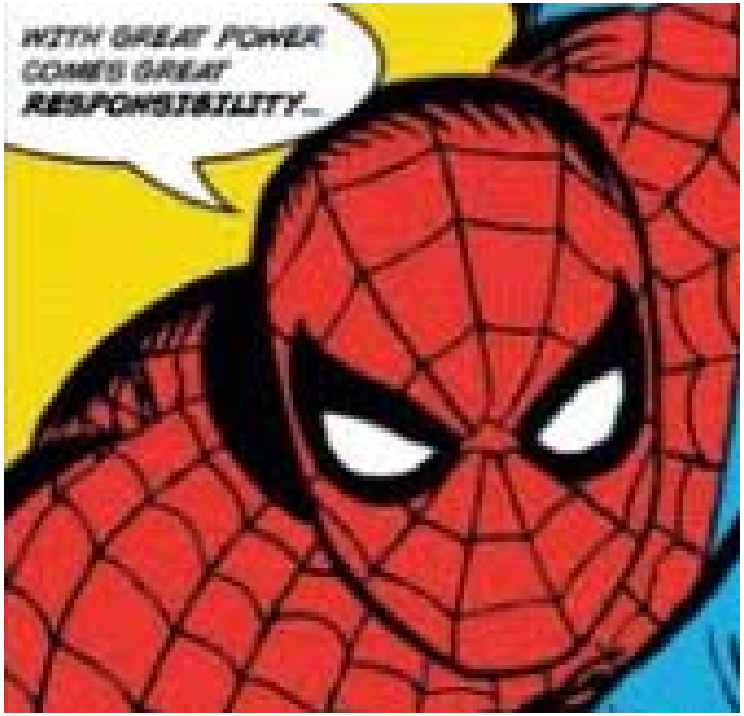
The Good

Technology is a powerful tool to potentially reduce administrative costs and improve patient care.

But…..

“With great power comes great responsibility.”

-Spiderman



The Bad

Identity Theft Tops FTC's Consumer Complaint Categories Again in 2014

Agency Also Notes a Large Increase in Complaints About "Imposter" Scams

FOR RELEASE

February 27, 2015

TAGS: Consumer Sentinel Network | Bureau of Consumer Protection | Consumer Protection

Identity theft topped the Federal Trade Commission's national ranking of consumer complaints for the 15th consecutive year, "imposter" scams

	Number	Percent
Identity Theft	332,646	13 percent
Debt Collection	280,998	11 percent
Imposter Scams	276,662	11 percent
Telephone and Mobile Services	171,809	7 percent
Banks and Lenders	128,107	5 percent
Prizes, Sweepstakes and Lotteries	103,579	4 percent

By the Numbers

- 1.8 million people were victims of medical identity theft in 2013 (Ponemon Institute)
- Medical records are particularly lucrative as it often contains:
  - Name and address
  - Family members
  - DOB
  - SSN
  - Payment
  - Insurance information
- Which is able to be used for:
  - Billing Fraud
  - Medical treatment
  - Credit
  - Arrests
  - Legal proceedings
  - Tax refund fraud

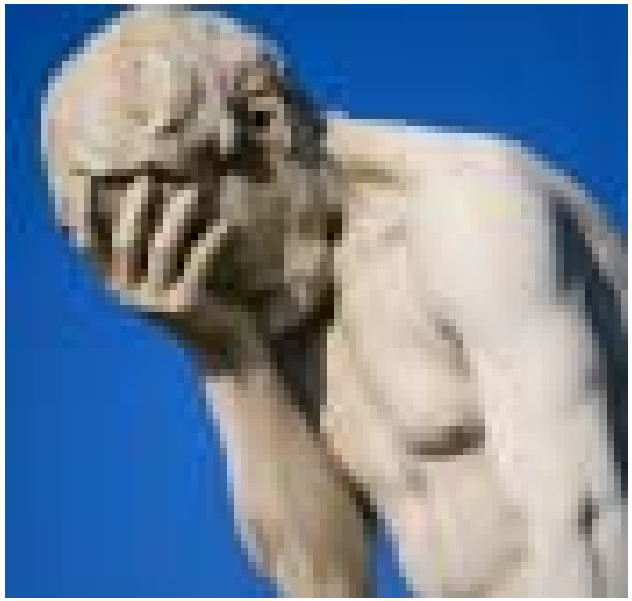
The Consumer's Compensation

DON'T SPEND IT ALL IN ONE PLACE

LinkedIn premium users to get $1 each in password-leak settlement

LinkedIn denies wrong-doing, but will salt and hash all passwords going forward.

by **Cyrus Farivar** - Feb 24, 2015 9:28am EST



The Ugly

Compliance Does Not Guarantee Security

IT

Compliance

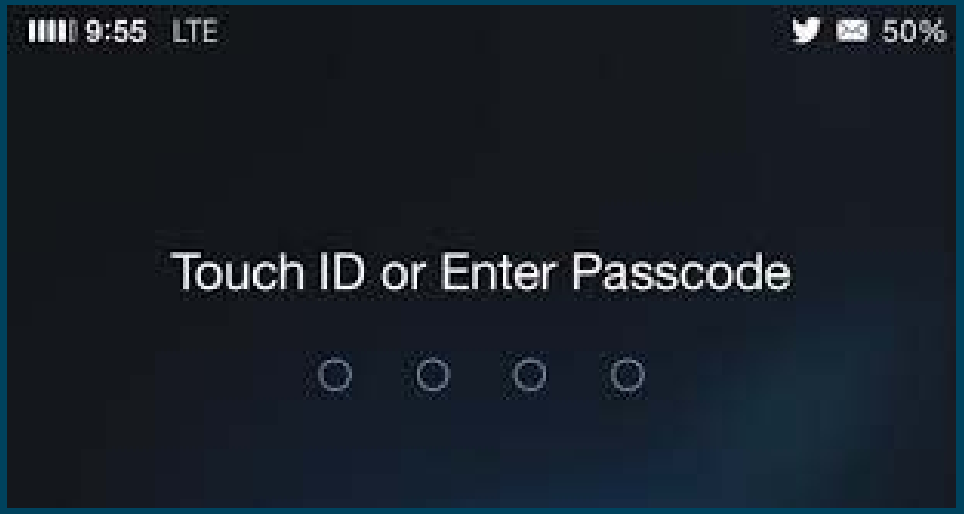
Security

Compliance	Security
Minimum Requirements	Effective
• Point in time • Static • Slow to adapt	• Continuous • Dynamic threats and defensive measures • Flexible and reasonable
• Silo	Integrated • Technical • Administrative • Physical
• “One size fits all” • Generic guidelines designed for bare minimums	• Bespoke • Best practices and industry norms are influential

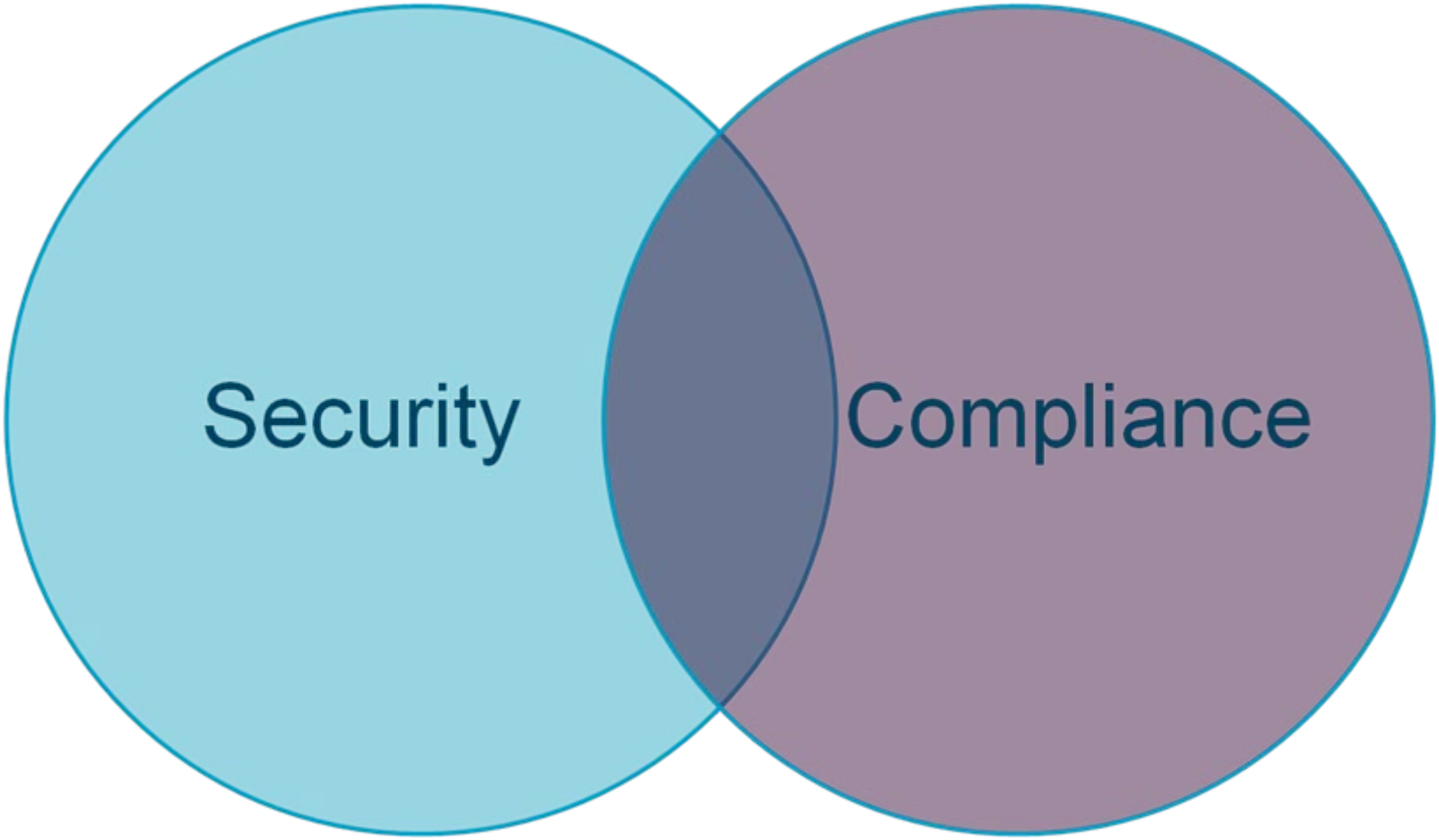
Checklists

Compliance = “what” to do, not “how”

“How” matters



Security & Compliance Are Friends, But Not Twins



Last Year’s Security Is Not This Year’s Security

Password Policies Have Short Shelf Lives

- Enforce strong passwords that are changed more frequently than the time it takes to crack them. This includes members of IT and system passwords.

  Advancements in inexpensive processing power and the availability of online password cracking services have rendered passwords essentially ineffective against a motivated attacker. Now, the attacker doesn't have to build an entire password cracking infrastructure, but she or he simply "rents" it from a cloud service makes it CHEAP and FAST to break short passwords. The table below is from **2012**.

Worst-Case Brute Force MD5 Cracking at One Trillion Hashes per Second			
Password Length	**Lowercase Letters**	**Letters & Numbers**	**All 95 Characters**
8	< 1 second	3.7 minutes	1.9 hours
9	5.5 seconds	3.8 hours	7.3 days
10	2.4 minutes	9.8 days	1.9 years
11	1.1 hours	1.7 years	180 years
12	1.2 days	102.4 years	17,135 years

May 2013

Think you have a strong password? Hackers crack 16-character passwords in less than an HOUR

- **During an experiment for Ars Technica hackers managed to crack 90% of 16,449 hashed passwords**
- **Six passwords were cracked each minute including 16-character versions such as 'qeadzcwrsfxv1331'**

By VICTORIA WOOLLASTON

PUBLISHED: 11:17 EST, 28 May 2013 | **UPDATED:** 12:15 EST, 28 May 2013

http://www.dailymail.co.uk/sciencetech/article-2331984/Think-strong-password-Hackers-crack-16-character-passwords-hour.html

August 2013

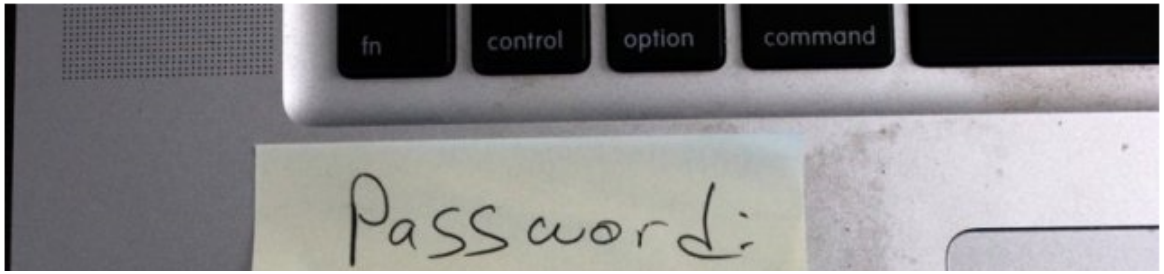
RISK ASSESSMENT / SECURITY & HACKTIVISM

"thereisnofatebutwhatwemake"—Turbo-charged cracking comes to long passwords

Cracking really long passwords just got a whole lot faster and easier.

by **Dan Goodin** - Aug 26, 2013 4:44pm EDT

Share Tweet 280



For the first time, the freely available password cracker ocl-Hashcat-plus is able to tackle passcodes with as many as 55 characters.

http://arstechnica.com/security/2013/08/thereisnofatebutwhatwemake-turbo-charged-cracking-comes-to-long-passwords/

Remember: “HOW” Matters

100 character password with all the complexity possible would easily be picked in clear text over FTP or telnet.

Or email

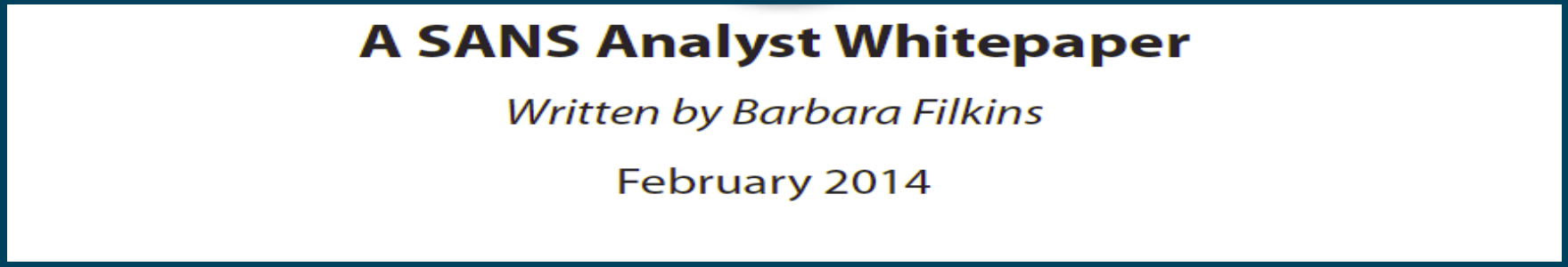
or WiFi.

Credit: flick/allaboutgeorge http://www.itworld.com/article/2832596/security/how-many-seconds-would-it-take-to-break-your-password-.html

The Good, The Bad and the Ugly

Good	Technology is cool
Bad	Compliance is required to get businesses to protect consumers in circumstances where the consumer lacks power, visibility or control.
Ugly	Compliance with the HIPAA Security Rule may not equate to effective security, but it will get you moving in the right direction.

The Really Ugly



Norse captured malicious Internet traffic from September, 2012, to October, 2013, in honeypots and sensors was analyzed and those that originated from public IP addresses associated with companies in the healthcare industry. They worked with SANS to analyze the findings.

375 healthcare organizations were identified in the collected data as compromised.

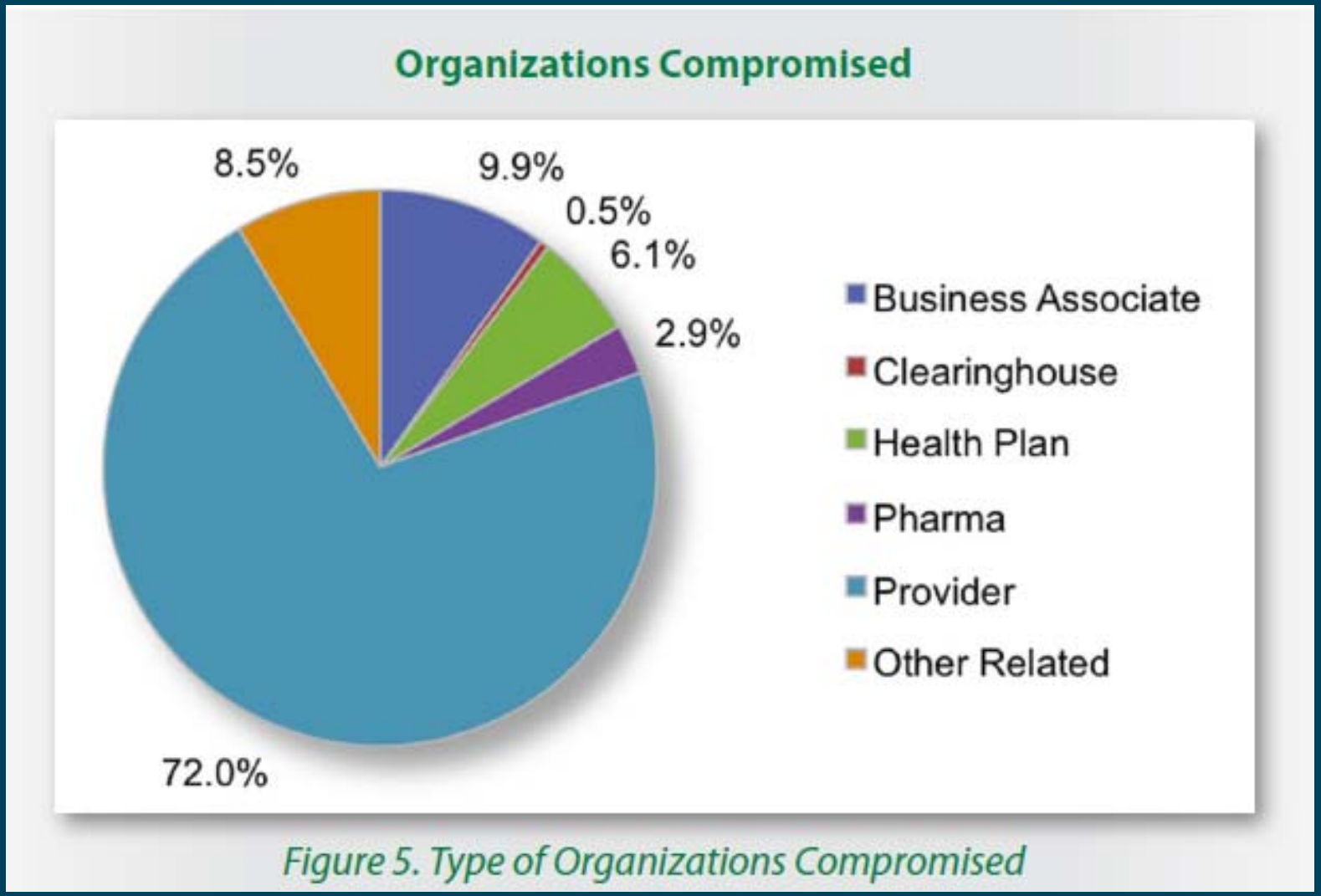


Figure 5. Type of Organizations Compromised

SANS Norse Healthcare Cyberthreat Report 2014

More Good:

The HIPAA Security Rule is not so prescriptive as to be “one-size-fits-all. It permits businesses of all sizes to tailor a security program to business needs and budget and focus on effectiveness.

To comply with HIPAA *and* effectively secure your business and patient information within the confines of reasonableness:

1. Start with an assessment of where and how sensitive information is received, is used, is transmitted, is stored and is disposed.
2. Protect those areas.
3. Stay in touch with technology advancements and the associated changes in your risk.
4. Use free/open source tools

Thank You

We're Hiring!

Deena Coffman | Chief Executive Officer, IDT911 Consulting

Information Security Officer, IDT911

Phone: 917.891.1845

Email: DCoffman@IDT911Consulting.com

Website: www.IDT911Consulting.com