The Quest For Cyber Security

Jeff Grady, HCISPP Senior Director

Three Pillars Technology Solutions LLC

Security and Compliance Solutions Advisor

Is Cyber Security Our Impossible Dream ?

And YOU thought Don Quixote had an impossible dream – as you follow this quest – to protect your sensitive data

As was succinctly observed by the title of an article that appeared online in conjunction with the Black Hat and Defcon conferences of Cyber Security Professionals held annually in Las Vegas

https://www.theguardian.com/technology/2016/aug/08/cyber-security-black-hat-defcon-hacking

"The State of Cyber Security: We're all Screwed"

Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020

Forbes - Cybersecurity Market Expected to Reach $170 Billion by 20202

The 'Wicked Crossroads' – where Data Security & Technology meet Privacy & Compliance

Today's Objectives

- **Goals of this Presentation – Very Limited – I can guarantee you will not leave this room a cyber security expert**
- **Make you more knowledgeable about the issues surrounding Cyber Security and hopefully a wiser consumer of the products and servces offered in that area**
- **A little bit about my background HCISPP – HealthCare Information Security & Privacy Practitioner**
- **An overview of HIPAA compliance and some observations on the current U.S. approach to Data Security and lessons we could learn from the EU Approach**
- **Some thoughts and observations regarding the practical challenges and limitations on any effort to protect Private Data that is stored or transmitted in the 'digital world'**

Your Key Take Home Question #1

Have we ever conducted an organization wide Security Risk Analysis?

Why label it the 'Wicked Crossroads' ?

- **Crossroads: An Intersection, where things meet in passage – but they can also 'collide'**
- **The** 'Wicked Crossroads' **is where you'll find a** Collision of Clashing Cultures and Characteristics
- **Technology - Data Security - Compliance - Privacy**

❑ **Technology**
- Lack of Standardization
- Ever Changing and Fast Evolving – Literally Impossible to Keep Up With
- Loose and Flowing Free – Open Source – Interoperability - Mobile

❑ **Data Security**
- (old school) Control – Build Walls to Protect – Restrict Flow and Access
- (new school) Transparency and Accountability – Ability to Monitor, Log and Track

❑ **Compliance**
- Typically built upon enforcement of a Defined Set of Standards that controls conduct and operation
- Preference for Conforming and Maintaining adherence to a relatively stable and established – uniformly accepted set of rules or standards

❑ **Privacy**
- Who's definition? Which Generation's Definition and Expectation?
- Changing societal expectations and transactional norms
- What's the true harm or potential for abuse when private information is shared or stolen?

Compliance ≠ Data Security

Data Security ≠ Compliance

The problem with Silos of Compliance and why Europe does 'data security' better

HIPAA

FISMA

PCI

FedRamp

DoD SRG

SOX

GLBA

CJIS

NERC

EFTA

According to the Wisconsin Historical Society, Wisconsin has more silos than any other state.

Label and Call The Sensitive Data whatever you wish…….but

- **To Technology – Data – Is all the same, just 'Bits and Bytes' -- the silos of compliance approach when it comes to 'data security' makes no sense and creates a burden upon organizations already overburdened by regulation**

The Wizard of (Oz)HIPAA

Why Does HIPAA Compliance Intimidate So Many?

HIPAA = An Example of our siloed Regulatory Approach that Overly Burdens and Punishes the Best Intentioned 'Do Gooders'

- **Didn't do a good job of recognizing differences in size or scale**
- **Was built with 'large enterprise' environments in upper most mind and failed to consider the impact on the SME world of healthcare**
- **Takes an unnecessarily harsh and overly punitive approach to achieving better data security protections and compliance – the harsh world of 'willful neglect' under HIPAA**
- **In Employment Relationships we promote 'Progressive Discipline Techniques – Why not Progressive Compliance Techniques?**
- **Much of the HIPAA process and methodology is 'out dated' and overbuilt for much of today's technology**

Let's Get Real About HIPAA

Once you 'pull back the curtain' and get to really understand HIPAA, and what's required for compliance – it's not so overwhelming and intimidating

Steps to HIPAA Compliance for the Small to Medium sized Practice and Organization

1. **Conduct a proper HIPAA Security Risk Analysis, including:**
   a. **Full ePHI inventory and data flow description along with an inventory of all IT that handles, stores or transmits your ePHI**
   b. **Identification of likely and potential risks and vulnerabilities to your ePHI**
   c. **Lists and identifies existing controls and protections and assesses their adequacy**
   d. **Includes an action plan to address any compliance gaps or data security vulnerabilities and insures that you have an ongoing risk management program in place**
2. **Review and Update as necessary Policies and Procedure Documentation for the Privacy, Security Rules and Breach Notification**
3. **Compile accurate list of all Business Associates and related BAAs and Documentation and conduct proper due diligence**
4. **Have in place and conduct proper user training on HIPAA compliance for both the Privacy and Security Rule – supplement with ongoing user awareness program**
5. **Insure that you have appropriate Cyber Liability coverage and that you fully understand both what it does and does not cover and the limitations on that coverage which exists**
6. **Make sure that you have adequate and complete back-ups for your stored data and that you have a business continuity – disaster recovery plan that has been reviewed and tested.**
7. **DOCUMENT – DOCUMENT – DOCUMENT all of the above**

Your Key Take Home Question #2

What Is Actually Covered Under Our Cyber Liability Insurance Policy?

A Few Quick Thoughts on the EU Approach – and the EU – US Privacy Shield Framework

- **'Think Small First' Principle - thanks to the 'Think Small First' Principle, SMEs' interests are taken into account at a very early stage of policy making. This helps the EU develop SMEs-friendly legislation.**
- **Data Protection Impact Assessment (DPIA): SMEs will have no obligation to carry out an impact assessment unless there is a high risk.**
- **But, the Magnitude of Risk does not equate to Size of Entity with Access Technology is all about 'ACCESS'…..once you have access – you have the ability and freedom to roam**

Is attempting to secure privacy in the digital age – as we enter Industrial Revolution 4.0 - the coming IoE – possibly a 'Fool's Errand' ?

- **Look ahead to where we're heading to the IoT - "the Internet of Everything is the intelligent connection of people, process, data and things."**
- **Since beginning to track data breaches in 2005, ITRC (Identity Theft Resource Center) had counted 5,810 breaches through December 2015, involving more than 847 million records. (and those are just the breaches that have been discovered and reported)**
- **The challenge of Third Party Vendor and Business Associates Cyber Security Risks and Control**

The Challenge with a legalistic and regulatory approach to attempting to control technology

- Analogous to a Kia trying to keep up with a Jaguar on the Autobahn
- IoT & IoE – Literally impossible to control – contain or restrain
- Huge Investments taking place in Big Data – Data Analytics
- With Technology – It's all about ACCESS – All you need is a single point of access (entry)
- What about other technologies that impact **PRIVACY** – Drone Technology – Proliferation of Security and Monitoring Cameras - GIS (Geographic Information Systems) and GPS asset tracking technologies

Retrofitting a solution Attempting to repair a jet airplane as it's taking off ……..or already left the ground

It's a bit late to try and close the Barn Door now…….the horse has already bolted

The belief and consensus of most is that our private data has already been compromised to one degree or another -- If it's not a major 'private sector' breach – TARGET – HOME DEPOT – Anthem, etc. – It's a Government agency that has been breached - IRS --- OPM (the OPM government data breach impacted 21.5 million)

Perhaps we should focus more on the unauthorized use and abuse of an individual's private data - Where is the added value and benefit of placing most of the burden upon the legal holder in possession of the data?

Your Key Take Home Question #3

Do we have an adequate Data Back-up Solution and Disaster Recovery Plan?

The #1 vulnerability to any data security solution……

Who's Privacy Are We Really Working to Protect?

- What is the real danger? – the Possession and Knowledge of the private data OR the Misuse and Abuse of that Information
- Is it truly the ordinary citizen's – or are we establishing rules to protect the powerful and political elite?
- Balancing of often competing interests
- **Keep in mind the Law and Principle of Diminishing Return on the Effort and Investment**
- The key is being realistic with what you can accomplish by laws and legislation
- **Are we simply creating another industry? – the Privacy/Data Security Compliance Industry**

Are You contributing something which is ultimately a 'Value Add' or are you layering on an additional 'Cost' and 'Burden'……or worse, something that produces a misallocation of resources from what should be the primary mission or goal of the organization that must bear that added cost of 'good intentions' ?

Are we approaching the protection of Privacy and Sensitive Data from the wrong direction -- with a proper balance?

I see most of the effort – as well as most of 'the burden' being placed on those in came into legal possession of data – but what are we doing to more effectively go after – prosecute and put a stop to those who steal the data and use it without permission?

Your Key Take Home Question #4

Do we have a Data Breach Response and Notification Plan in place?

Links to Data Security Resources

- **Guide to Privacy and Security of Electronic Health Information**
  http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
- **Homeland Security – Cybersecurity Page**
  https://www.dhs.gov/topic/cybersecurity
- **Cybersecurity for Small Business**
  - https://www.fcc.gov/general/cybersecurity-small-business
- **NIST Cybersecurity Framework** http://www.nist.gov/cyberframework/index.cfm
- **NIST Special Publication 800-30** Guide for Conducting Risk Assessments
  http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
- **SANS** https://www.sans.org/critical-security-controls/
- **2016 State of California Data Breach Report**
  https://oag.ca.gov/breachreport2016