



# Risk Assessment Models for Healthcare Organizations

# Webinar Contributors

## **Rebecca Herold**

CEO and Founder of The Privacy Professor  
Email: [rebeccaherold@rebeccaherold.com](mailto:rebeccaherold@rebeccaherold.com)  
TwitterID: @PrivacyProf

## **Dr. James L. Angle**

Regional Information Security Manager  
Trinity Health

## **Grant Johnson, CISSP, CISM**

Principal and IT Security Consultant  
Array Information Technologies, Inc.

## **Gary Long, CISA, CISSP**

Chief Technology Officer  
GT Global Network, Inc.  
[glong@gtglobalnet.com](mailto:glong@gtglobalnet.com)  
[www.gtglobalnet.com](http://www.gtglobalnet.com)

## **Matthew Sharp**

CISO  
Logicworks

# Our Presenter






Rebecca Herold is CEO and Founder of The Privacy Professor® consultancy she established in 2004, and is Co-Founder and President of SIMBUS, LLC, an information security, privacy, technology & compliance management cloud service for organizations of all sizes, in all industries, in all locations founded in 2014. Rebecca is an entrepreneur with over 25 years of systems engineering, information security, privacy and compliance experience. Rebecca created the information security and privacy department functions at a large multi-national financial and health care organization throughout the 1990s. Rebecca has authored 19 books to date, dozens of book chapters, and hundreds of published articles.








Rebecca led the NIST SGIP Smart Grid Privacy Subgroup for seven years, was a founding member and officer for the IEEE P1912 Privacy and Security Architecture for Consumer Wireless Devices Working Group, and serves on the Advisory Boards of numerous organizations. Rebecca also serves as an expert witness for information security, privacy, and compliance issues. Rebecca was an Adjunct Professor for the Norwich University MSISA program for many years. Rebecca has provided invited keynotes on five continents, and has spoken at over 100 conferences, seminars and other events. Rebecca has received numerous awards for her work, is frequently interviewed, including regularly on the CW Iowa Live morning television show, and quoted in diverse broadcasts and publications. Rebecca holds the following certifications: FIP, CISSP, CISA, CISM, CIPT, CIPM, CIPP/US, FLMI. Rebecca is based in Des Moines, Iowa.

[www.SIMBUS360.com](http://www.SIMBUS360.com), [www.privacyprofessor.org](http://www.privacyprofessor.org), [www.privacyguidance.com](http://www.privacyguidance.com), [rebeccaherold@rebeccaherold.com](mailto:rebeccaherold@rebeccaherold.com)

# 10 Security Risk Analysis Myths

1. The security risk analysis is optional for small providers.  FALSE
2. Simply installing a certified EHR fulfills the security risk analysis MU requirement.  FALSE
3. My EHR vendor took care of everything I need to do about privacy and security.  FALSE
4. I have to outsource the security risk analysis.  FALSE
5. A checklist will suffice for the risk analysis requirement.  FALSE

# 10 Security Risk Analysis Myths

6. There is a specific risk analysis method that I must follow.  FALSE
7. My security risk analysis only needs to look at my EHR.  FALSE
8. I only need to do a risk analysis once.  FALSE
9. Before I attest for an EHR incentive program, I must fully mitigate all risks.  FALSE
10. Each year, I'll have to completely redo my security risk analysis.  FALSE

# What is a Risk Analysis?

OCR's guidance is not prescriptive...

*The following questions adapted from NIST Special Publication (SP) 800-66 are examples organizations could consider as part of a risk analysis. These sample questions are not prescriptive and merely identify issues an organization may wish to consider in implementing*

*the Security Rule:*

- *Have you identified the e-PHI within your organization? This includes e-PHI that you create, receive, maintain or transmit.*
- *What are the external sources of e-PHI? For example, do vendors or consultants create, receive, maintain or transmit e-PHI?*
- *What are the human, natural, and environmental threats to information systems that contain e-PHI?*

## What is Risk Assessment?

The [Health Insurance Portability and Accountability Act \(HIPAA\) Security Rule](#) requires that [covered entities](#) conduct a risk assessment of their healthcare organization. A risk assessment helps your organization ensure it is compliant with HIPAA's [administrative, physical, and technical safeguards](#). A risk assessment also helps reveal areas where your organization's protected health information (PHI) could be at risk. Watch the [Security Risk Analysis video](#) to learn more about the assessment process and how it benefits your organization or visit the [Office for Civil Rights' official guidance](#).

Read the [HHS Press Release](#).



<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf>  
<https://www.healthit.gov/providers-professionals/security-risk-assessment>

# Risk Management vs. Risk Analysis

- **Risk Management:** The ongoing, continuous process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.
- **Risk Analysis:** The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact.
- **Per NIST SP 800-30:**
  - Risk analysis is a necessary risk management activity.
  - “Risk Analysis” is synonymous with “Risk Assessment.”



# HIPAA Requirements

## § 164.308 Administrative safeguards.

(a) A covered entity or business associate must, in accordance with § 164.306:

(1) (ii) Implementation specifications:

(A) Risk analysis (Required).

Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

(B) Risk management (Required).

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

**“Addressable” versus “Required”**



# HHS OCR Guidance

Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a risk analysis is foundational, and must be understood in detail before OCR can issue meaningful guidance that specifically addresses safeguards and technologies that will best protect electronic health information.

The guidance is not intended to provide a one-size-fits-all blueprint for compliance with the risk analysis requirement. Rather, it clarifies the expectations of the Department for organizations working to meet these requirements.<sup>3</sup> An organization should determine the most appropriate way to achieve compliance, taking into account the characteristics of the organization and its environment.

We understand that the Security Rule does not prescribe a specific risk analysis methodology, recognizing that methods will vary dependent on the size, complexity, and capabilities of the organization. Instead, the Rule identifies risk analysis as the foundational element in the process of achieving compliance, and it establishes several objectives that any methodology adopted must achieve.

See full statement at:

<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf>

# HIPAA Violations & Penalties

HIPAA Violation	Minimum Penalty	Maximum Penalty
Unknowing	\$100 per violation, with an annual maximum of \$25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)	\$50,000 per violation, with an annual maximum of \$1.5 million
Reasonable Cause	\$1,000 per violation, with an annual maximum of \$100,000 for repeat violations	\$50,000 per violation, with an annual maximum of \$1.5 million
Willful neglect but violation is corrected within the required time period	\$10,000 per violation, with an annual maximum of \$250,000 for repeat violations	\$50,000 per violation, with an annual maximum of \$1.5 million
Willful neglect and is not corrected within required time period	\$50,000 per violation, with an annual maximum of \$1.5 million	\$50,000 per violation, with an annual maximum of \$1.5 million

# 2016 Breaches & Penalties

Entity	Date	Penalty Amount	PHI Breach	Individuals Impacted
University of Massachusetts Amherst (UMass)	November, 2016	\$650,000	Malware infection	1,670
St. Joseph Health	October, 2016	\$2,140,500	PHI made available through search engines	31,800
Care New England Health System	September, 2016	\$400,000	Loss of two unencrypted backup tapes	14,000
Advocate Health Care Network	August, 2016	\$5,550,000	Theft of desktop computers, loss of laptop, improper access of data at business associate	3,994,175 (combined total of three separate breaches)
University of Mississippi Medical Center	July, 2016	\$2,750,000	Unprotected network drive	10,000
Oregon Health & Science University	July, 2016	\$2,700,000	Loss of unencrypted laptop / Storage on cloud server without BAA	4,361 (combined total of two breaches)
Catholic Health Care Services of the Archdiocese of Philadelphia	June, 2016	\$650,000	Theft of mobile device	412
New York Presbyterian Hospital	April, 2016	\$2,200,000	Filming of patients by TV crew	Unconfirmed
Raleigh Orthopaedic Clinic, P.A. of North Carolina	April, 2016	\$750,000	Improper disclosure to business associate	17,300
Feinstein Institute for Medical Research	March, 2016	\$3,900,000	Improper disclosure of research participants' PHI	13,000
North Memorial Health Care of Minnesota	March, 2016	\$1,550,000	Theft of laptop computer / Improper disclosure to business associate (discovered during investigation)	299,401
Complete P.T., Pool & Land Physical Therapy, Inc.	February, 2016	\$25,000	Improper disclosure of PHI (website testimonials)	Unconfirmed
Lincare, Inc.	February, 2016	\$239,800	Improper disclosure (unprotected documents)	278

# HIPAA Violations & Penalties

Expect penalties related to risk assessments to increase...

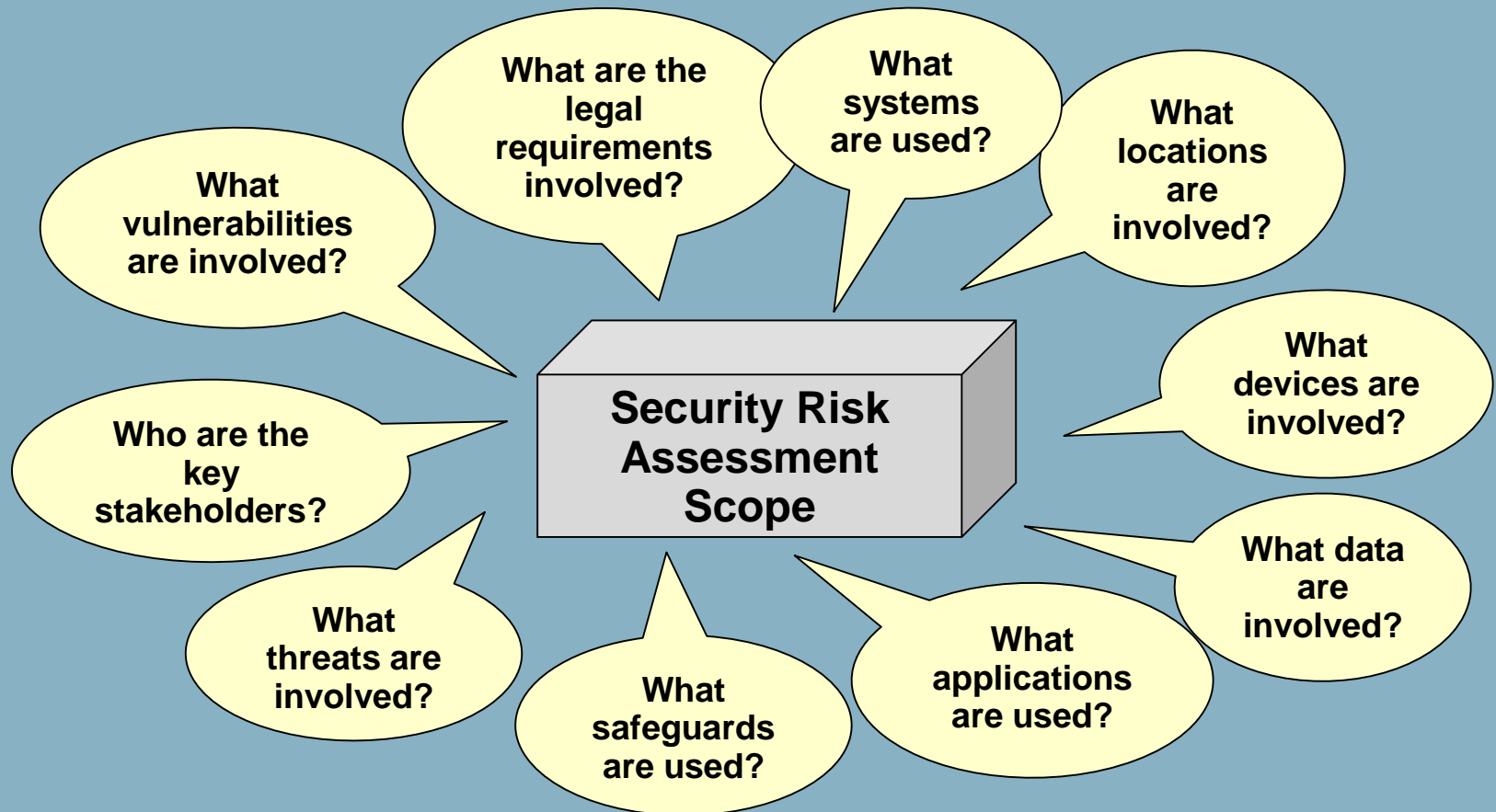
## Plans for Future Increased Enforcement

Based on the HITECH Act's 2009 mandate, OCR plans to continue prioritizing resolution agreements as a means of increasing awareness in the HIPAA-regulated community about continuing issues with noncompliance with the HIPAA Rules. Specific areas on which OCR intends to focus include business associate compliance, compliance with the risk analysis and risk management requirements in the HIPAA Security Rule, breaches due to cyber security incidents, and individual rights under the HIPAA Privacy Rule.

From the most recent annual report published: "Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance For Calendar Years 2013 and 2014" <https://www.hhs.gov/sites/default/files/rhc-compliance-20132014.pdf>

# Risk Assessment Elements (1/3)

1. Scope of the Analysis
2. Data Collection
3. Identify and Document Potential Threats and Vulnerabilities



# Risk Assessment Elements (2/3)

4. Assess Current Security Measures
5. Determine the Likelihood of Threat Occurrence
6. Determine the Potential Impact of Threat Occurrence



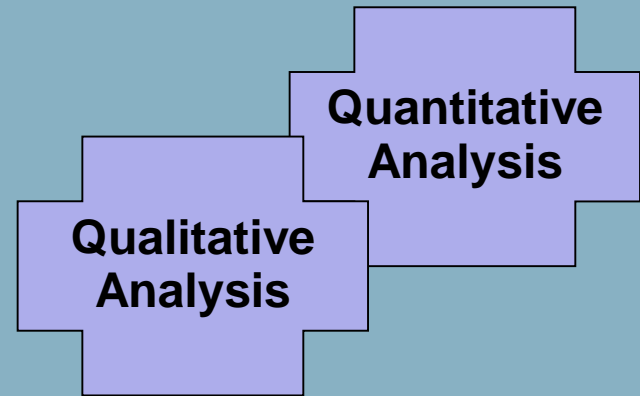
# Risk Assessment Elements (3/3)

7. Determine the Level of Risk
8. Finalize Documentation
9. Periodic Review and Updates to the Risk Assessment



# Risk Assessment Models

- Do-It-Yourself (DIY)
- Hybrid using Tools/Solutions
- Third Party



“We understand that the Security Rule does not prescribe a specific risk analysis methodology, recognizing that methods will vary dependent on the size, complexity, and capabilities of the organization. Instead, the Rule identifies risk analysis as the foundational element in the process of achieving compliance, and it establishes several objectives that any methodology adopted must achieve.”

*Source: HHS Final Guidance on Risk Analysis*

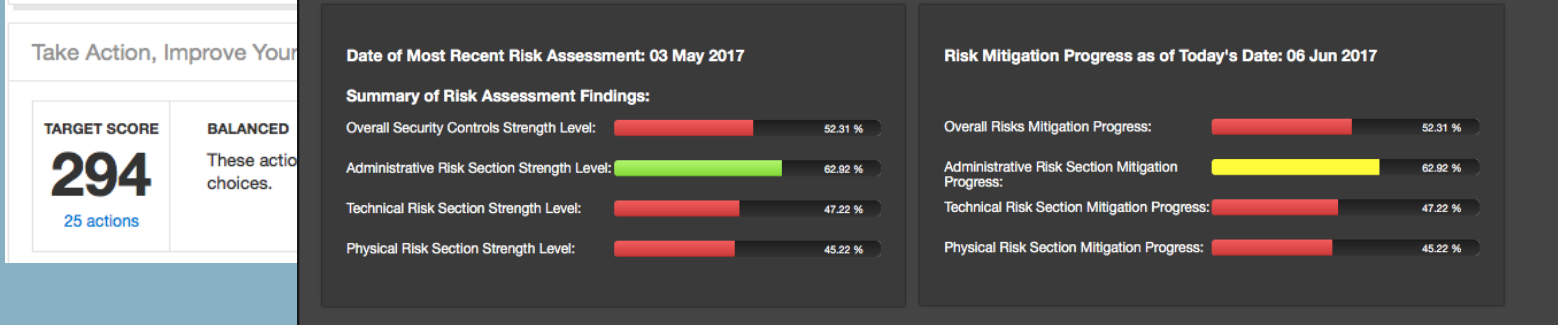


# Risk Assessment Frameworks

1. National Institute of Standards & Technology (NIST) Special Publication (SP) 800-30 Risk Management Guide
2. NIST SP 800-66 Implementing HIPAA Guide
3. Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)
4. Facilitated Risk Analysis Process (FRAP)
5. Forensic Analysis of Risks in Enterprise Systems (FARES)
6. Factor Analysis of Information Risk (FAIR)
7. Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)
8. Large assortment of others
9. Supported by a variety of security controls libraries
  - a. Cloud Security Alliance Cloud Controls Matrix (CCM)
  - b. HIPAA and other Generally Prescriptive Regulations
  - c. ISO/IEC 27002
  - d. NIST SP 800-53, etc.
  - e. US Cybersecurity Framework
  - f. Payment Card Industry Data Security Standard (PCI DSS)
  - g. Many others
10. Choose what is most effective and appropriate for your organization

# Risk Assessment Tools

- Basic Business Software
- HHS SRA Tool
- Risk Assessment Vendor Tools
- GRC Tools with RA Components



# Risk Assessment Results

- OCR expectations
- Mitigation progress monitoring
- If possible, include privacy ← My recommendation
- Consider Program Capability Maturity ← My recommendation

## Levels of Risks

There were:

- 14 **High** risk findings
- 39 **Medium** risk findings
- 5 **Low** risk findings

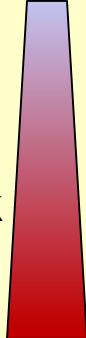


Source: <https://simbus360.com/ra/>

# Risk Actions

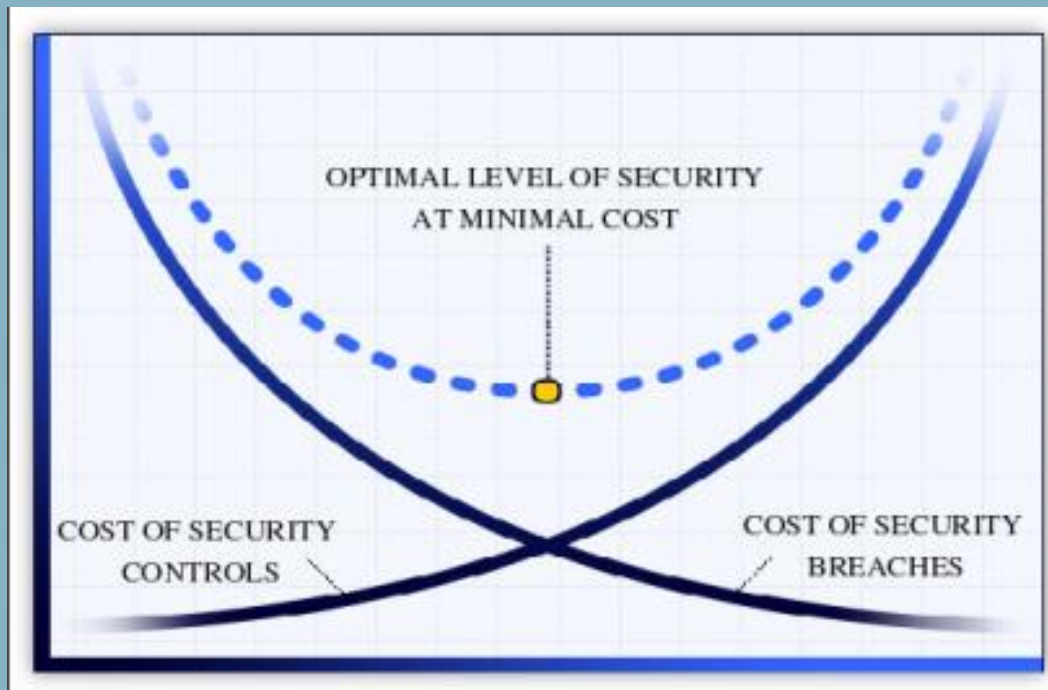
1. **Avoidance:** Eliminate the risk cause or consequence
2. **Mitigation:** Establish controls to lower the risks
3. **Transfer of Risk:** Pass the accountability and liability to someone else (e.g., purchase cyber security insurance that covers the risk)
4. **Acceptance:** Accept the risks and the associated potential consequences

## *What to do with risk?*

- |                  |  |                                       |
|------------------|--|---------------------------------------|
| 1. Avoidance     |  | Easiest but could be bad for business |
| 2. Mitigation    |  | Practical but requires resources      |
| 3. Transfer risk |  | Expensive and may not remove all risk |
| 4. Acceptance    |  | Huge gamble and scary consequences    |

# Risk Impact & Prioritization

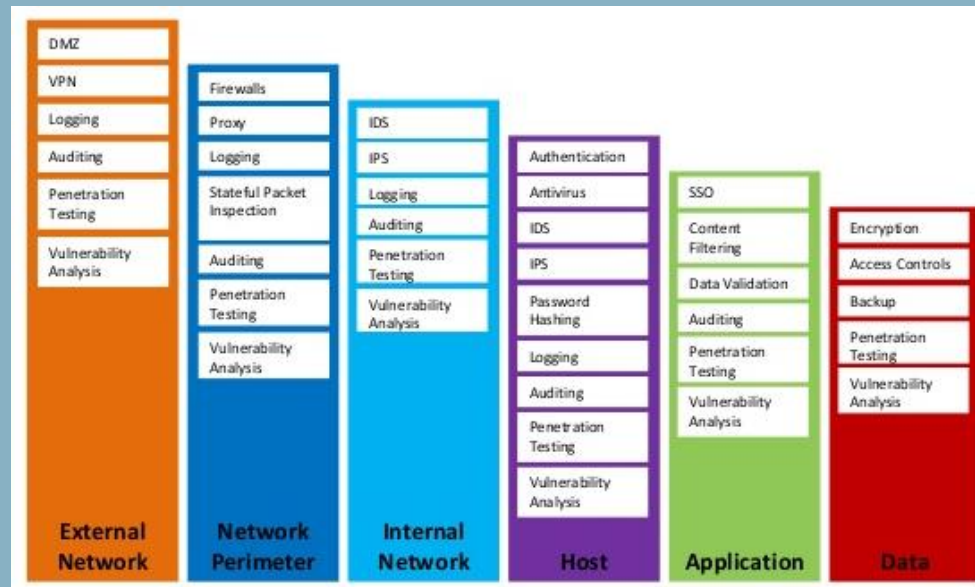
- Corrective Action Plans
- Mitigation Strategy
- Cost/Benefit Analysis



Source: <https://mainweb-v.musc.edu/security/guidelines/images/optimal-security.png>

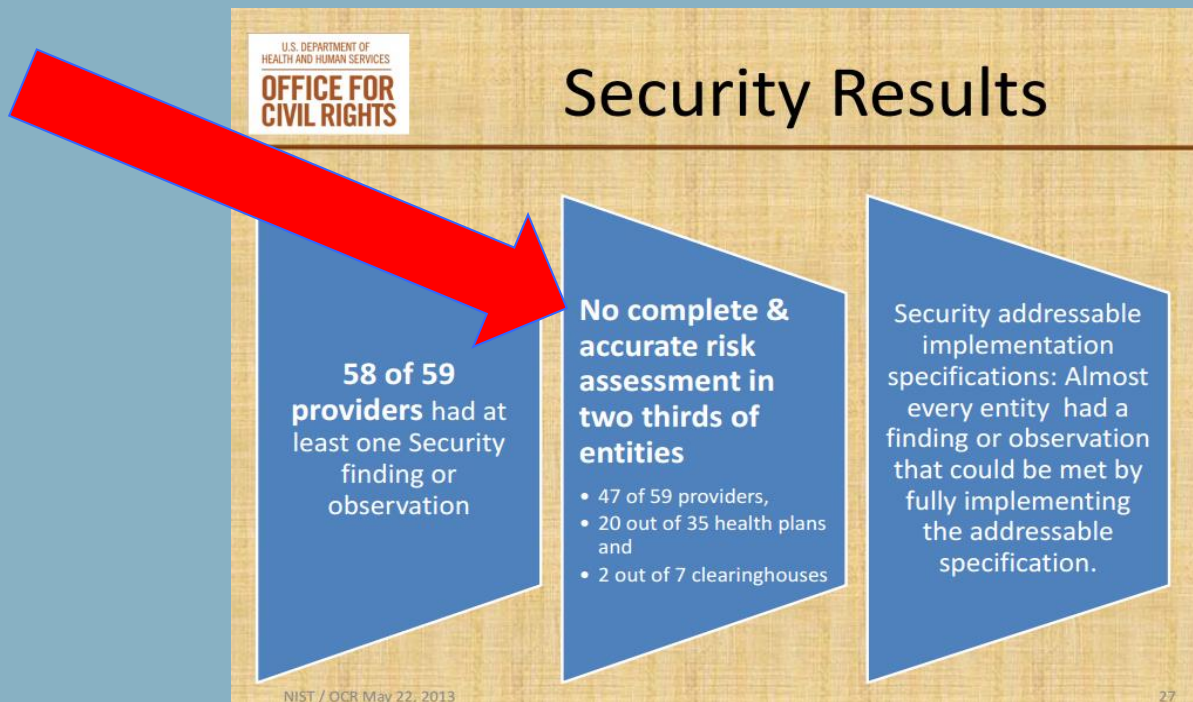
# Common Risk Findings

- Lack of Documented or Updated Policies
- Lack of Documented or Current Procedures & Processes
- Inadequate Security/Privacy Training and No Awareness Reminders
- No or Inadequate Vendor Management
- Insufficient or Lack of Technology Safeguards



# Common Risk Findings

- Training & Awareness Reminders
- Lack of Assessments
- Continuous Security Management Activities
- Missed Data Locations

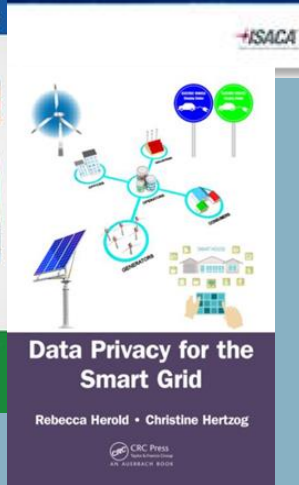
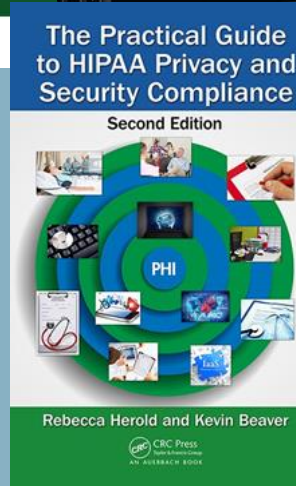
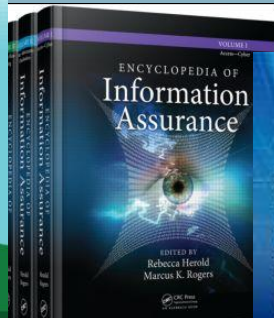
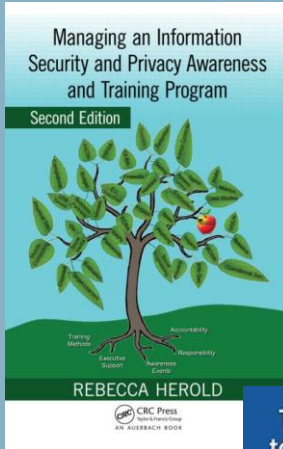


# Risk Assessment Success Factors

1. Documented Roles and Responsibilities
  - a. Required
  - b. Recommended
2. Executive Sponsorship & Visible Support
3. Adequate Budget & Related Resources
4. Documented Policies, Procedures
5. Consistently Performed Processes
6. Risk Management Activities
7. Security Safeguards
  - a. Administrative
  - b. Physical
  - c. Technical
8. Training and awareness reminders
9. On-going security & privacy management program maintenance & improvement







## Contact Information

**SIMBUS, LLC**  
**The Privacy Professor<sup>®</sup>**  
**625 42<sup>nd</sup> Street**  
**Des Moines, Iowa 50312**  
**Phone 515-491-1564**

[www.SIMBUS360.com](http://www.SIMBUS360.com)  
[www.privacyguidance.com](http://www.privacyguidance.com)  
[www.privacyprofessor.org](http://www.privacyprofessor.org)

**Questions?**

Blog: <http://www.privacyguidance.com/blog.html>

Email: [rebeccaherold@rebeccaherold.com](mailto:rebeccaherold@rebeccaherold.com)

TwitterID: <http://twitter.com/PrivacyProf>

# Join Us at our Next Event!

## 3<sup>rd</sup> Quarter Healthcare SIG Webinar

### Medical Device Security Including Patient Implants

09/14/2017 Noon – 1 PM Eastern

# Support Our SIGs!



**Financial SIG**



**Healthcare SIG**



**Security Awareness SIG**



**Women in Security SIG**

<https://www.issa.org/sigs>

# CPE Survey

A follow up email will be sent to you within 24 hours that includes:

- A link to the webinar recording

- A link to a copy of the presentation slides

- A link to the CPE survey/quiz

You can access all SIG webinars and CPE links via the ISSA website at

<https://www.issa.org/page/SIGOnDemandWebinars>