RSA CONFERENCE 2013

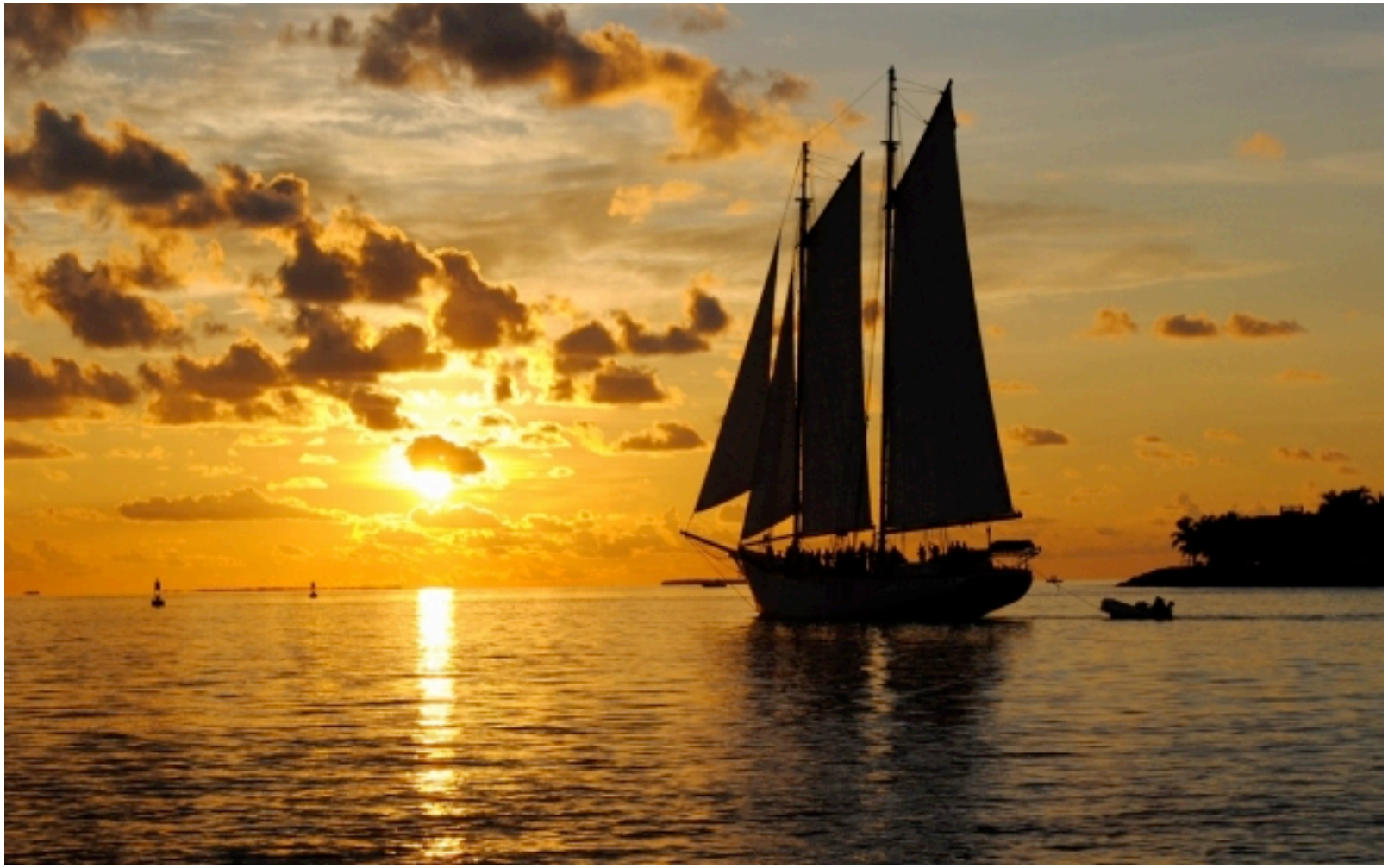
WHY COMPANIES FAIL WITH COMPLIANCE INITIATIVES

Seth R Wilson

Session ID: GRC-W25A

Session Classification: General Interest

WHY THIS TOPIC?



WHAT ARE YOU PROTECTING?

HIPAA

CONTROLS

- Companies want to drive down the cost of audits by **removing controls or making them non-key** to improve audit "efficiency"
- Controls are re-designed to **pass audits easier**

"Logical access is revoked within 24 hours of termination."

"Logical access is revoked within ~~24~~ **48** hours of termination."

"Logical access is revoked ~~within 24 48 hours~~ **timely upon notification from HR** of termination."

CONTROLS PASS!

USE YOUR AUDIT RESULTS

- Areas where Security / IA Audit must play a key role:
  - Identify root cause.
  - Identify areas for improvement.
  - Partner with affected business area(s) for a solution (advanced technique).

CONTROLS PASS AUDIT != SAFE

- Disprove the hypothesis
  - Use your breakers to attack and pen test.
  - Find weaknesses that audits will miss.
  - Use outside vendors to help.

THINK OUTSIDE THE COMPANY

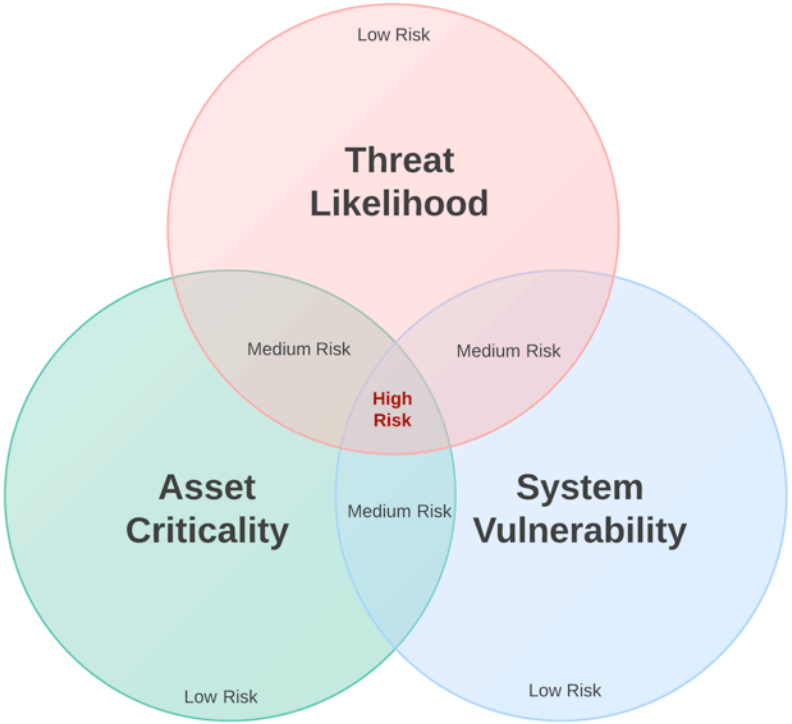
- 2011 Crowe Horwath LLP Survey:
  - **75%** reported that their organizations experienced harm from the action or inaction of a third party.
  - **Only 21%** reported that their companies are very effective at identifying and managing third-party risks.

3RD PARTY MANAGEMENT

- **Develop a rubric** to evaluate how critical the 3rd party is to the organization
  - Will they handle confidential information, PII, NPCI?
  - If they are breached or shut down, how screwed are we?
- **Work with your legal team** to include security elements in the SA
  - Include a right to audit.

Planning and Risk Assessments

- Identify assets, threats and analyze risks:



Planning and Risk Assessments

- Security should be involved in the **planning** phases for **any audit**:
  - Map risks to controls that affect information security.
  - You are likely doing something already that you can take credit for!

#RECAP

- Role of Security must be **strategic**:
  - Use your audit findings as a lever to improve information security.
  - Disprove the hypothesis.
- Do not forget about your **3rd parties**.
- **Risk assessment process** adopted across all audits.

Thank You.

srwilson777@gmail.com

Follow me: @SRW