IT Risk Assessments - major drag or worth every ounce of effort?

Eva Lorenz

Agenda

- The basics
- Which standard/framework to choose?
- Risk assessment under HIPAA / PCI
- Internal or outsource?
- Remediation
- Lessons learned from the past
  - Large environments
- Future developments
- Tips, Hints etc.
- Conclusion

The basics

- What is a risk assessment? From NIST 800-30
  - The purpose of risk assessments is to inform decisionmakers and support risk responses by identifying: (i) relevant **threats** to organizations or threats directed through organizations against other organizations; (ii) **vulnerabilities** both internal and external to organizations;(iii) **impact**(i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) **likelihood** that harm will occur. The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring).

The basics

- “Fact” gathering of threats and vulnerabilities
  - Interviews
  - Document review
  - Technical testing
  - Organizational threats
- Analysis
  - Impact
  - Likelihood
- Result
  - Corrective Action Plan with risk prioritization table

Which standard to choose?

- NIST
  - Part of a large collection of IT documents
  - Tie in with federal requirements
- ISO
  - Good for international organizations
- CSF
  - Becoming more widely used
  - Quite compact
  - Tie in with other standards

Risk assessment under HIPAA / PCI

- Is there a HIPAA or PCI-specific risk assessment?
  - NO!
- Requirement for risk assessment to be organization-specific
  - Can be and maybe should be done in-house
  - No generic risk assessment template, but include:
    - Industry-specific threats
    - Prior incidents within the organization
- Basis for identifying risks: IR log
- Risk prioritization/ranking: IR log
  - Recognize a pattern?
- If you do it well the first time, may only need minor modifications later on
  - Note: Ransomware, vendor management per industry guidance

Internal or outsource?

- Third party/outsource
  - Pros:
    - Unbiased view
    - More credibility
    - Industry trends for CAP
  - Cons:
    - Your organization = industry average
    - More expensive
    - All answers are true

Internal or outsource?

- Internal
  - Pros:
    - Cheaper
    - Understands the vertical and organization very well
    - May be able to better separate truth and wishful thinking
  - Cons:
    - Resource issues
    - Possible bias
    - Some units may not really participate (colleague = lack of authority)
    - Lack of management buy-in

Remediation

- Communicate remediation plan to staff
  - Splendid isolation may look like no action
- Involve SME (internal and external)
  - You spent $$ on risk assessment, ensure that remediation is effective
  - The auditor may be your best friend
- Prioritize
  - Often people vs money
- Multiple compliance requirements
  - Combine CAPs and see if PCI DSS or HIPAA can provide guidance on priority

Lessons learned from the past

- Large environments
  - No one size fits all – maybe expect for the standard chosen
  - Management buy-in a must
  - Do pre-assessments to prepare questions and allocate time needed
    - What type of information?
    - Reliance on central services?
    - Unique applications, processes?
    - Crown jewels?
  - Start off with central services, then move into unique departments procedures
  - Separate reports and combine CAP or do formal roll-up reports
    - Combined CAP will be used for remediation

Future developments

- Cybersecurity Framework
  - Fairly recent release, but broad adoption
  - Is widely adaptable and allows customization in a relatively painless way
  - Planned Privacy framework
  - Also planned Domestic Legal & Policy documentation for consumer privacy
    - Intent is to be consistent with international policy objectives as well
  - End-result = Possible coverage for Privacy – Security – Policies
- Privacy
  - GDPR / CCPA / ….. – Privacy risk assessments may become more frequent
- Usual suspects
  - Third party risk
  - Endpoint security (including users)

Source: https://www.nist.gov/news-events/news/2018/09/department-commerce-launches-collaborative-privacy-framework-effort

Tips, Hints etc.

- Roll-up reporting
- Prioritization
  - Low hanging fruit
  - Long-term investments
  - IT Roadmap 3 to 5 years
- Most bang for your buck
  - Reuse third party materials
  - CAP
- Document, document
  - Especially for PCI DSS

Questions?

- Risk assessments are often seen as a lot of checklists and a major effort with little to no apparent benefit or change to the IT operations. This presentation will show that a risk assessment can have significant payoff for an organization if the risk assessment is structured appropriately. Organizations exist in a variety of forms and so not one risk assessment template fits every organization. The presentation will cover risk assessments best practices and also present risk assessments as part of compliance requirements under HIPAA and PCI. Risk assessments can be a major effort even if outsourced to third parties, but they can also be done in a more manageable form internally and be beneficial. The speaker will cover risk assessment best practices, but also provide hints and tips from almost 10 years of experience in performing risk assessments for a variety of organizations.
  Whether you have to do a risk assessment due to a compliance requirement or not, this seminar will present various options for doing these assessments and also go into applying risk assessments to benefit the organization overall.