
# Conducting an Information Security Risk Assessment

## June 29, 2018

# This SecureTheVillage Webinar brought to you by …



Grandpoint.

GRANDPOINT BANK

# Conducting an Information Security Risk Assessment

- Guide: Stan Stahl
  - Founder, SecureTheVillage
  - President, Citadel Information Group
- Guest
  - John Coleman
    Chief Information Officer
    Grandpoint Bank

# Our Objective: We want you to …



- Understand Why …
  - Key role played by information security risk assessment in the overall information security management strategy
- Know What / How …
  - Key elements of an information security risk assessment

# To Get Started …



*The secret of success lies in managing risk, not avoiding it.*

*Merryle Rukeyser*
*Financial Journalist / Educator*

# Why an Information Security Risk Assessment?



- Information risk is business risk
  - Money
  - Time
  - Strategic Focus
  - Opportunity
  - Competitive Advantage
  - Reputation
  - Brand
- If you don't know your information security risk, then you can't manage it
- And you must manage it
  - Cybercrime
  - Business Disruption
  - Murphy's Law
  - Laws, regulations

# Risk Assessment Questions & Key Considerations



- When is a risk assessment needed (what are the drivers)?
  1. Major business changes
  2. Major system changes
  3. Legal/regulatory requirement
- Who should participate?
  1. Business owner(s)
  2. Subject matter experts (IT, InfoSec, Compliance, critical service providers
- How often should a risk assessment be performed?
  1. One-time, annually, every other year?
  2. Depends on factors such as regulations, legal/insurance requirements, business need, etc.
- Who will review and approve?

# Risk Assessment Contents

- Risk categories/areas of impact
  - Financial, reputation brand, legal, operations/services, etc.
- Types of risk exposures (threats)
  - Intentional vs accidental
  - human vs non-human
  - internal vs. external
- Likelihood that it could happen
- Severity of risk (assuming no controls)
- Mitigating controls
  - Technologies, systems, etc.
  - Policies and procedures
  - internal vs. external, etc.
- Residual risk rating (after controls)

# RA Example – New Product (Pay Day Loans)



## New Product Risk Assessment: Pay Day Lending (Small Dollar/Short-Term)

| Risk Category | Nature of Risk | Risk/ Impact Rating | Likelihood | Mitigating Control(s) | Residual Risk Rating |
|---|---|---|---|---|---|
| Financial/ Credit | Borrowers with poor or no credit histories will have high default rates leading to significant losses in the portfolio | High | High | • Underwriting policies<br>• Underwriting procedures and guidelines<br>• Begin with pilot test | Low |
| Reputation/ Brand | Perception of payday lending as a predatory business could harm reputation and lead to loss of existing customers | Low | Low | • Use social media, direct mail, and advertising to educate customers | Low |
| Compliance/ Legal | Abuse by other lenders and adverse media coverage could lead to onerous legislation and difficulty achieving compliance | Medium | Medium | Compliance and training departments work closely to monitor pending legislation and quickly adjust training and compliance programs as needed | Low |
| Operations/ HR | Economic downturn leading to high defaults overwhelms existing Collections Dept. staff | Medium | Medium | Large of number of 3rd party collection agencies available to augment staff | Low |
| Vendor | Major vendor used for processing payments suffers major financial losses resulting in bankruptcy and ceasing operations | High | Low | Vendor subject to initial and ongoing due diligence reviews to assess financial strength and stability of customer base | Low |
| IT/Information Security | Online account access tool could be hacked resulting in loss of customer information | High | High | • Application testing<br>• Pen testing<br>• Strong authentication controls | Low |
| Business Continuity | Earthquake in Southern California damages operations center and renders it unusable | High | Medium | BCP includes an alternate operations site in Oregon | Low |

# RA Example – Summary of Results



## Summary of Risk Assessment Results

| Risk Category | Overall (Composite) Risk Rating | Overall Strength of Mitigating Control(s) | Residual Risk Rating |
|---|---|---|---|
| Financial/ Credit | High | Strong | Low |
| Reputation/ Brand | Moderate | Moderate to Strong | Low |
| Compliance/ Legal | Moderate | Strong | Low |
| Operations/ HR | Low | Strong | Low |
| Vendor | High | Moderate to Strong | Low to Moderate |
| IT/Information Security | High | Strong | Low |
| Business Continuity | High | Strong | Low |
| **Overall** | **Moderate to High** | **Strong** | **Low** |

Control Improvements Identified

- A
- B
- C

# After the RA is Done – What's Next?

- Address gaps/control deficiencies
- Use as a checkpoint on the road to a go/no-go decision
- Use as input to audits, self assessments, training
- Identify improvements for future risk assessments

# General Overview: Key Steps in Assessing Information Risk



- Identify Information Assets
- Identify *Assessment Framework*
- Identify information threats – what can go wrong?
- Identify / characterize threat actors to defend against
- Identify how they are likely to attack you
- Identify major vulnerabilities
- For each information asset, each threat, and each threat actor
  - Analyze residual risk
  - Decide what to do about it

# What are Organization's Information Assets?



- Information of others it must legally protect
  - Personally identifiable information
  - HIPAA protected information
  - Information of minors
  - GDPR-protected information
  - Credit card information
  - Information protected by NDA or other agreements
- Internal information assets
  - Intellectual property
  - Trade secrets
  - Operational reports
  - Spreadsheets
  - Word files
  - Emails
  - eCommerce systems
  - Online banking systems
  - Passwords to critical system; server configuration information, etc
  - Websites
  - Backup and recovery systems
  - Physical inventory

# Identify Assessment Frameworks



- NIST Cybersecurity Framework
- ISO 27001, 02
- CIS-20
- SecureTheVillage *Code of Basic IT Security Management Practice*
- Regulatory & Compliance
  - GLB
  - HIPAA HITECH
  - NIST 800 – 171
  - FTC
  - GDPR
  - NY State Cybersecurity Requirements for Financial Services Companies
  - Payment Card Industry Data Security Standard
- Client audit requirements

# What are the Threats?



- Copied, stolen—Confidentiality
  - Credit card theft
  - Medical records theft
  - Intellectual property theft
- Changed without authorization — Integrity
  - Invoice fraud
  - Sabotage
- Made unavailable — Availability
  - Ransomware
  - DDos attack on a web site
  - Earthquake
- Used without authorization — fraud and misuse
  - Business email compromise
  - Theft of computing resources

# Who are the Threat Actors We Must Defend Against? How Sophisticated?



- Non-targeted Attacks
- Targeted Attacks
- Lone wolf cybercriminals
- Organized crime
- Malicious employees, vendors, etc
- Employees, vendors, etc making inadvertent mistakes
- Competitors
- Terrorists, political enemies, etc
- Nation states
- Natural disasters

# How Are They Likely to Attack Us?



- Social engineering
- Vendor attack
- Exploit a technology vulnerability
- Install a Trojan Horse or Key Logger
- Attack us via a Botnet
- Come in through a backdoor
- Install an Advanced Persistent Threat (APT)
- Launch a Distributed Denial of Service Attack (DDoS)

# Where are Our Major Vulnerabilities?



- People
- Processes
- Technology
- Management & Leadership

# For Each Information Asset, Each Threat, and Each Threat Actor …



- How likely is the risk to manifest?
- How important is managing risk?
  - What are the consequences of failure?
  - How significant would the damage be if something goes wrong?
- What controls do we have to keep this from happening?
- How confident are we that they work correctly?
- Given these controls, what is the *residual risk*, the remaining risk after applying these controls?
- Given the level of residual risk, what are we going to do about it?
  - Live with this level of residual risk
  - Strengthen controls to lower residual risk to acceptable levels

# Wrap Up: The Information Security Risk Assessment



- Understand Why …
  - Key role played by information security risk assessment in the overall information security management strategy
- Know What / How …
  - Key elements of an information security risk assessment

# Next Webinar: Information Classification and Control

- Guide: Stan Stahl
  - Founder, SecureTheVillage
  - President, Citadel Information Group
- August 2, 10AM Pacific
- Registration: SecureTheVillage.org

# SecureTheVillage Webinar Series



- Information Security Management Guidance
  - Practical
  - Real-World
  - How-To
  - Actionable
- SecureTheVillage ResourceKit
- First Thursday of month, 10AM Pacific

# Information Security Management Webinar Schedule — 2018



| | |
|---|---|
| February 1 | Information Security Management Overview; The Role of Leadership |
| March 1 | The Information Security Management & Leadership Team |
| *April 5* | *Online Bank Fraud — How To Avoid Being a Victim* |
| *May 3* | *Basics of Cyber-Law* |
| June 7 | Information Security Policies and Standards |
| ***June 29*** | ***Conducting an Information Security Risk Assessment*** |
| August 2 | Information Classification and Control |
| September 6 | Securing the Human |
| October 4 | Managing Security of the IT Infrastructure |
| November 1 | Getting Cyber-Prepared : Incident Response & Business Continuity |
| December 6 | Third-Party Security Management |
| January 2019 | Managing Cyber-Risk and Insurance |

# SecureTheVillage: Turning People and Organizations into Cyber Guardians



***Monthly Webinar Series:*** Provides Practical  Real-World Actionable How-To Information Security Management Guidance.

***Executive Focus Groups:*** Designed to assist Chief Executives understand how to turn their organization into Cyber-Guardians and create a cyber resilient culture.

***Information Security Management and Leadership ResourceKit***: A practical guide for implementing an information security management and leadership program in your organization.

***Code of Basic IT Security Management Practices:*** A set of basic IT security management practices that are so basic that a failure to implement them puts the organization at a dangerous and unnecessary risk of a costly information incident.

***Community-Based Programs*** to train the broader community in basic cybersecurity defense practices for themselves and their families, helping them become cyber-aware citizens.

Visit us at: *SecureTheVillage.org*

# For More Information …



**Stan Stahl, SecureTheVillage & Citadel Information Group**
Stan@SecureTheVillage.org
323-428-0441

**John Coleman, Grandpoint Bank**
jcoleman@grandpointbank.com
(213) 542-2741