
# Third-Party Security Management

## December 2018

*The Los Angeles Cyber Lab Presents*


# A SecureTheVillage Webinar

# Third-Party Security Management

LOS ANGELES

311 City Services LA City Directory

Eric Garcetti @MayorOfLA

LA CYBER LAB

About Us | Cyber Education | STOP Cyber Crime | Tools for L.A. Businesses


## About Us

Who we are and how we are helping L.A. businesses with cyber threats

## Cyber Education

Resources to educate L.A. businesses about cyber security and cyber threats

## Cyber Tools for L.A. Businesses

Digital tools for L.A. businesses to stop cyber threats

# Third-Party Security Management

- Guide: Stan Stahl, PhD
  - Founder, SecureTheVillage
  - President, Citadel Information Group
- Guest
  - John Coleman, EVP Information Technology, Pacific Premier Bank
  - SecureTheVillage Board of Directors

# Discussion Topics



- The 3rd-Party Information Security Management Challenge
- Third-Party Security Management Basic Requirements
  - Legal / Compliance
  - Security Management
- Information Security Manager (ISM) Responsibilities
  - Identify high-impact vendors
  - Assess security risk
  - Establish Cybersecurity SLAs
  - Document information security expectations
  - Integrate incident response

# The Scope of the 3rd-Party Information Security Challenge



3rd Party Risk Management , Breach Response , Data Breach

## Attack on Billing Vendor Results in Massive Breach

Atrium Health Says Attack on AccuDoc Affected 2.65 Million Individuals

Marianne Kolbasuk McGee (HealthInfoSec) · November 28, 2018 0 Comments

Twitter Facebook LinkedIn Credit Eligible Get Permission


SEARS

DELTA

THE HOME DEPOT

BEST BUY

UNIVERSAL

UNIVERSAL MUSIC GROUP

goodwill

myfitnesspal

HYATT

# Key Objective: Avoid Disastrous Consequences



You as customer are accountable for vendor IS incidents

- Financial losses
- Complaints and loss of customers
- Regulatory sanctions, fines, legal judgments
- Damage to brand and reputation
- Loss of market share
- Business failure

# Third-Party Information Security Management Challenges



Examples of major IS challenges related to 3rd parties:

- Information security may be given lower priority in vendor selection and outsourcing initiatives
- Lack of visibility into the vendor's IS risks and controls
- Difficulty obtaining IS-specific reporting (e.g. incidents)
- Reliance on independent audits which can be flawed
  - Pen tests vary greatly in scope and quality (lack of standards)
  - Regulatory exams of 3rd parties can be too infrequent (i.e. every 3 years)
  - SOC reports usually fail to adequately address information security
- Effective IS oversight and accountability for 3rd parties is a continual process that requires effort/tenacity

# Third-Party Security Management Basic Requirements



Effective management of 3rd party information security is one aspect of a sound **Vendor Management program** that includes the following requirements:

- Procedures for assessing vendor risks
- Documented policy and procedures
- Adequate staffing and clearly defined responsibilities
- Initial due diligence and ongoing monitoring
- Clearly defined contracting requirements (required T&Cs)
  - Confidentiality and privacy (safeguarding customer/confidential data)
  - Scope of services and SLAs
- Ongoing oversight by the Board of Directors and management (i.e. IT Steering Comm)
- Regular reporting (daily, monthly, annual)

Authoritative sources of information for managing 3rd party risk are readily available!!

- NIST (SP 800-161 - Supply Chain Risk Mgt Practices for Federal Info Systems & Organizations)
- FFIEC/FDIC (e.g. FIL 44-2008 - Guidance for Managing Third-Party Risk)
- HHS/CMS (e.g. HIPAA Security Series - Interpretation of 45 CFR 160 and 164)

# Information Security Manager (ISM) Responsibilities



- Collaborate with and enroll business owners in 3rd party information security oversight
- Conduct risk assessments (both initial and ongoing)
- Perform due diligence and evaluate integrity of IS controls for both existing and prospective vendors
- Establish Cybersecurity SLAs for inclusion in contract and statement of work/services
- Document information security expectations
- Review information security reports from 3rd parties
- Insure adequacy of staffing/coverage related to 3rd party information security
- Integrate 3rd parties into incident response program (joint simulations)
- Provide reports on 3rd parties to executive management and the Board of Directors

# The Information Risk Management Process



- A comprehensive inventory of all vendors should be maintained and kept current
- An annual risk assessment of all vendors should be performed to identify high-risk vendors, adequacy of controls, needed improvements, etc.
    - An initial comprehensive risk assessment should be performed before signing a contract with a new major vendor.
- Prioritize Vendors by Risk
    - High Risk: The vendor has access to sensitive / critical information or services, such as HIPAA data, PCI information, etc such that a security incident could cause grave harm
    - Medium Risk: The vendor has access to sensitive / critical information or services such that a security incident could cause harm
    - Low Risk: The vendor has no access to sensitive / critical information or services
- Manage Risk via Prioritization and Appropriate Due Diligence

# Due Diligence Considerations



- Due diligence is critical to identifying, avoiding, and/or mitigating risk
- Appropriate due diligence procedures should be performed for all high-risk vendors
  - Initial due diligence before signing a contract
  - Ongoing due diligence (annually or at contract renewal)
- Factors to consider when determining due diligence requirements
  - Materiality of relationship
  - Ease of replacing vendor
  - Criticality of services provided
  - Impact of an outage or business interruption
  - Processing or storage of confidential (customer) information
  - Performance of compliance-related services
  - Past performance

# A Matrix Approach to Managing Due Diligence Requirements



Vendor Due Diligence Requirements Matrix
(Example)

| Due Diligence Procedure | High Risk Vendors | | Medium Risk Vendors | |
|---|---|---|---|---|
| | Initial | Ongoing | Initial | Ongoing |
| Legal review of contract | Yes | At renewal | Yes | Discretionary |
| Send control questionnaire | Yes | Annually | Yes | At renewal |
| Obtain/review 3rd party audit reports (SOC reports, pen tests, etc.) * | Yes | Annually | Yes | Annually |
| Obtain/review financial statements * | Yes | At renewal | Yes | Discretionary |
| Review other info (public records, analyst opinions, media reports) | Yes | Monthly | Yes | At renewal |
| Conduct site visit(s) | Yes | Discretionary | Discretionary | Discretionary |
| Review compliance with SLAs, including information security | n/a | Monthly | n/a | Annually |
| Contact other customers (reference checks) | Yes | (1) | Discretionary | (2) |

(1) Business owner should be required to participate in user groups whenever possible.

(2) Business owner should be encouraged to participate in user groups whenever possible.

(*) May be part of an “Information Security and Privacy Compliance Package”

# Vendor Management Reporting: Considerations for Senior Management



Vendor Management reporting including information security management should be tailored to the business needs of the organization:

- Detailed reporting on individual vendors may be needed for specific business units
    - Third-party providing claims management for a health care provider
    - Web developer providing online financial transactions for a business
- Performance reports should be regularly reviewed by business owners that are responsible for SLAs
- General or summary-level reports presented annually are usually suitable for Board of Directors or management committee

Vendor reporting should be taken into account when selecting, designing, or modifying management reporting systems

Larger organizations typically require specialized applications for vendor management and reporting

Reporting should be designed to facilitate accountability of both vendors and internal constituents (e.g. business owners)

# Annual Report to Executive Management and the Board of Directors



Annual report to Board of Directors or management committee should include:

- Summary of vendors (risk classifications, types of service, numbers of vendors)
- Profile of each high-risk vendor and results of ongoing due diligence
- Important changes in policy, vendor relationships, etc.
- Major incidents or issues
  - Compliance violations
  - Breach of SLAs
  - Security incidents
  - Financial/legal problems
- Results of internal audits or compliance exams (findings and status of Corrective Action Plans (CAPs)
- Future planning considerations

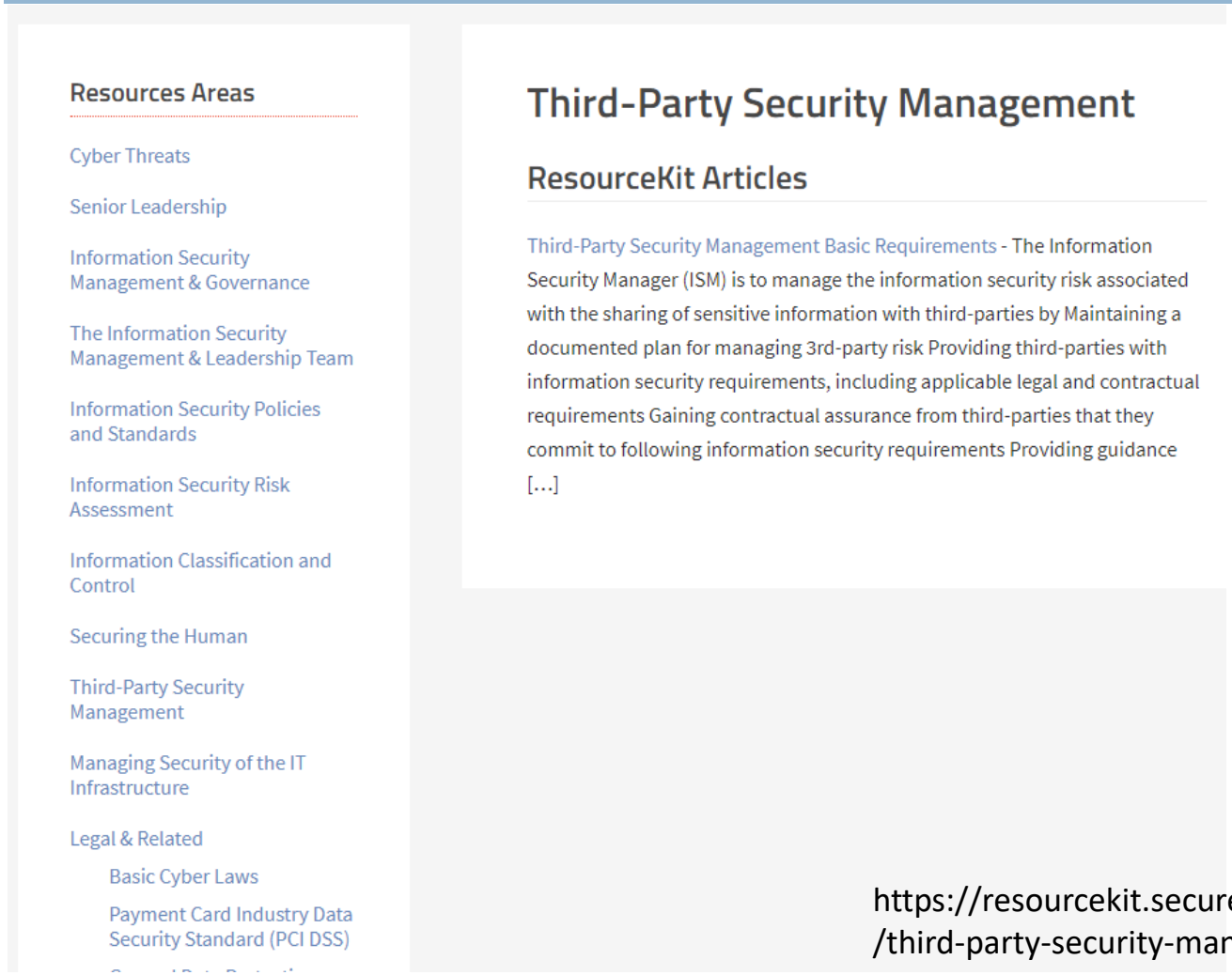
# Information Security Manager & Leadership Team — Getting Started



- Identify Third-Parties with Access to Sensitive Information or Critical Systems
- Prioritize by Cyber Risk
- Begin Conducting Risk Assessments
  - Webinar: *Conducting an Information Security Risk Assessment*
  - *ResourceKit: Information Security Risk Assessment*

# ResourceKit: Third-Party Security Management






https://resourcekit.securethevillage.org/resources/third-party-security-management/

# Next Webinar: Managing Cyber-Risk and Insurance

- Guide: Stan Stahl
  - Founder, SecureTheVillage
  - President, Citadel Information Group
- Guest: Howard Miller
  - Vice President, Director Technology Division LBW Insurance
  - SecureTheVillage Board of Directors
  - Pepperdine Graziadio CyRP Board of Advisors
- January 17, 10 AM Pacific
- Registration: SecureTheVillage.org

# SecureTheVillage Webinar Series



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

# Information Security Management Webinar Series: Basic Curriculum



| | |
|---|---|
| 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 8 | Getting Cyber-Prepared: Incident Response & Business Continuity |
| December 6 | Third-Party Security Management |
| January 17 | Managing Cyber-Risk and Insurance |

# Webinars: What to Expect in 2019



January 2019: Managing Cyber-Risk and Insurance

February 2019: The Cybersecurity Threat Landscape

March … December: Email us with suggestions. What would YOU like?

# 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**
banktechconsulting@gmail.com
(213) 910-4240

**FREE Citadel *Cybersecurity News of the Week & Weekend Vulnerability and Patch Report***
https://Citadel-Information.com

**For Marketing / Sponsorship Opportunities**
Email us at info@securethevillage.org. Put *Sponsor Opportunity* in Subject
Visit us at https://securethevillage.org/sponsorship-opportunities/

SecureTheVillage

About | Cybersecurity Guardian Program | Events | Resources | News & Views | Our Village | Contact


LA CYBER LAB