SecureTheVillage: Turning People and Organizations into Cyber Guardians

Information Classification and Control

August 2, 2018

This SecureTheVillage Webinar brought to you by …

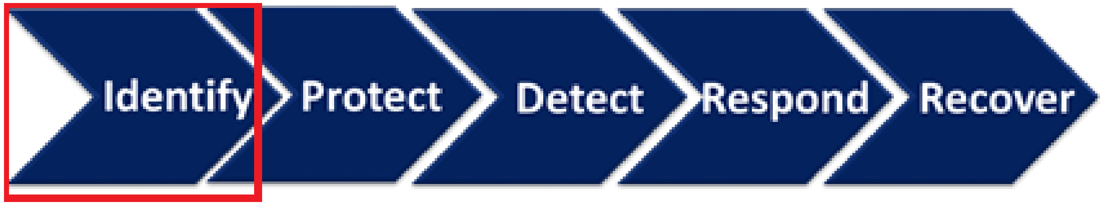
CITADEL
INFORMATION GROUP, INC.

JMBM
Jeffer Mangels
Butler & Mitchell LLP

Information Classification & Control

- Guide: Stan Stahl
  - Founder, SecureTheVillage
  - President, Citadel Information Group
- Guest
  - Michael A. Gold, Esq.
    Co-chair of Cybersecurity and Privacy Group
    Jeffer Mangels Butler & Mitchell, LLP

Classification & Control: The First Step in Securing Information



NIST Cybersecurity Framework

Identify: Three Imperatives for Securing Information

1. Know what it is
2. Know where it is
3. Know who has management oversight (Owner)
    - How sensitive the information is
    - Who is authorized access the information

Information Requiring Protection

- Information of others that must be protected
  - 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 systems; server configuration information, etc.
  - Websites
  - Backup and recovery systems
  - Physical inventory records

Example Classification and Control Policy

- Working in collaboration with the Information Security Manager, each Department is responsible for managing the security of the information it generates and uses.
- Department managers are expected to
  - Identify, classify and control their information in accordance with the harm that would result from a loss of confidentiality, integrity, or availability;
  - Identify those groups or individuals with authorized access to information, granting only the access needed to do one's job (“least privilege” and “need-to-know”) based upon the job duties and job requirements of each individual;
  - Manage the security of sensitive information in accordance with security documents established in collaboration with the *Information Security Manager.*

Information Classification

- Public
- Internal Use
- Restricted

- Commensurate with harm resulting from loss of confidentiality, integrity, or availability
  - Breach disclosure costs
  - Extortion
  - Business interruption
  - Cybertheft and fraud
  - Brand loss
  - Competitive loss
  - Loss of strategic focus

Information Classification: Public

- Unauthorized disclosure of this information is not expected to cause problems for the organization or its community.
- There are no restrictions on access to or dissemination of *Public* information.
- *Examples of Public information*
  - Websites
  - Newsletters
  - Brochures
  - Marketing materials

Information Classification: Internal Use

- There is no need or reason to disclose this information to those outside the organization - although the damage from such disclosure is seldom significant
- Examples:
  - The Employee Manual
  - Forms and templates
  - Training materials
  - Organizational policies
  - Personnel phone extension lists

Information Classification: Restricted

- Private or otherwise sensitive in nature
- Access is restricted to those with a legitimate need for access, a need-to-know.
- Unauthorized disclosure of this information to people without a need for access may be against laws and regulations, may cause significant problems for the organization, or may even cause grave damage to the organization.

- Client, customer, and staff personally identifiable information (PII)
- Electronic protected health information (ePHI)
- Client / customer credit card numbers
- Login credentials to network, bank accounts, admin accts
- Staff salary data
- Employee performance records
- Trade secrets
- Financial data
- Customer / vendor information
- Acquisition strategy
- Donor databases (Non-Profit)

Information Owners

- The Information Owner is responsible for the security of the information he/she "owns."
- An Information Owner is responsible for
  - Identifying the appropriate level of protection that is to be assigned to information (sensitivity)
  - Approving which personnel or job profiles are permitted access to information
  - Providing users with guidance on who they are authorized to share information with, where they can move or save information, and, more generally, explaining to users how the information is protected
  - Maintaining an up-to-date "Information Inventory"
    - What: Non-public information managed by the owner
    - Who: Personnel having access to the non-public information
    - Where: Systems on which information is stored and transmitted

Developing The Information Inventory: Phase 1: Collect & Organize

- Interview users; first-line managers
- Focus on Information, not Systems
  - What information do you use and process?
    - Not just ‘obvious’ big picture systems
    - Seek out shadow systems
  - Who’s the “owner”?
  - How sensitive is it?
  - With whom do you share it?
  - Where is it? ?
- Collect raw data in a consolidated spreadsheet
- Use this to Identify
  - Information people use
  - Extent people know security relevance
  - Organizational knowledge gaps
  - Apparent inconsistencies
- Initial raw inventory only intended as a necessary start point

Summary Observations from a Recent Phase 1 “Real-World” Example

- 14 Information Categories
    - 11 Information Categories contain restricted information with no identified owners
- 1352 Information Instances
    - 902 (66.72%) identified as Restricted
        - 598 (66%) of the 902 restricted instances have no identified owner
    - 361 (26.7%) Internal Use Only
    - 89 (6.58%) Public
- 777 (57%) of all 1352 identified data is located on the cloud
- 566 (42%) of all identified data is on-premise and almost 50% of that data is located on user machines (email included)
- 400 (44%) of the 902 restricted information instances is located on-premise
- At almost 55%, more than half of restricted information (495 of 902 instances) is reported to be in the cloud

Phases 2 and 3: Complete & Maintain the Information Inventory

- Phase 2: Complete
  - Review data
  - Identify information owners
  - Information Owner
    - Fill-in missing information
    - Resolve inconsistencies
    - Resolve specific findings of note
    - Complete inventory section
    - Establish configuration control

- Phase 3: Maintain
  - Individual owners maintain their information inventories
  - Information Security Manager and Leadership Team Review
    - At least semi-annually and as appropriate
      - Merge
      - Review
      - Update
      - Restructure

Wrap-Up: Information Classification & Control

- Identify: Core Security Function
  - What
  - Where
  - Who Manages (Owner)
    - Sensitivity
    - Who has access

- Policy
- Information Classification
  - Public
  - Internal Use
  - Restricted
- Information Owners
- Information Inventory
  - The hardest step is the first step

Next Webinar: Securing the Human

- Guide: Stan Stahl
  - Founder, SecureTheVillage
  - President, Citadel Information Group
- September 6, 10 AM 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

Michael Gold, Jeffer Mangels Butler & Mitchell, LLP
mag@jmbm.com
(310) 201-3529

For Sponsorship Opportunities

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

SecureTheVillage: Turning People and Organizations into Cyber Guardians