SPRING/SUMMER 2020 $25

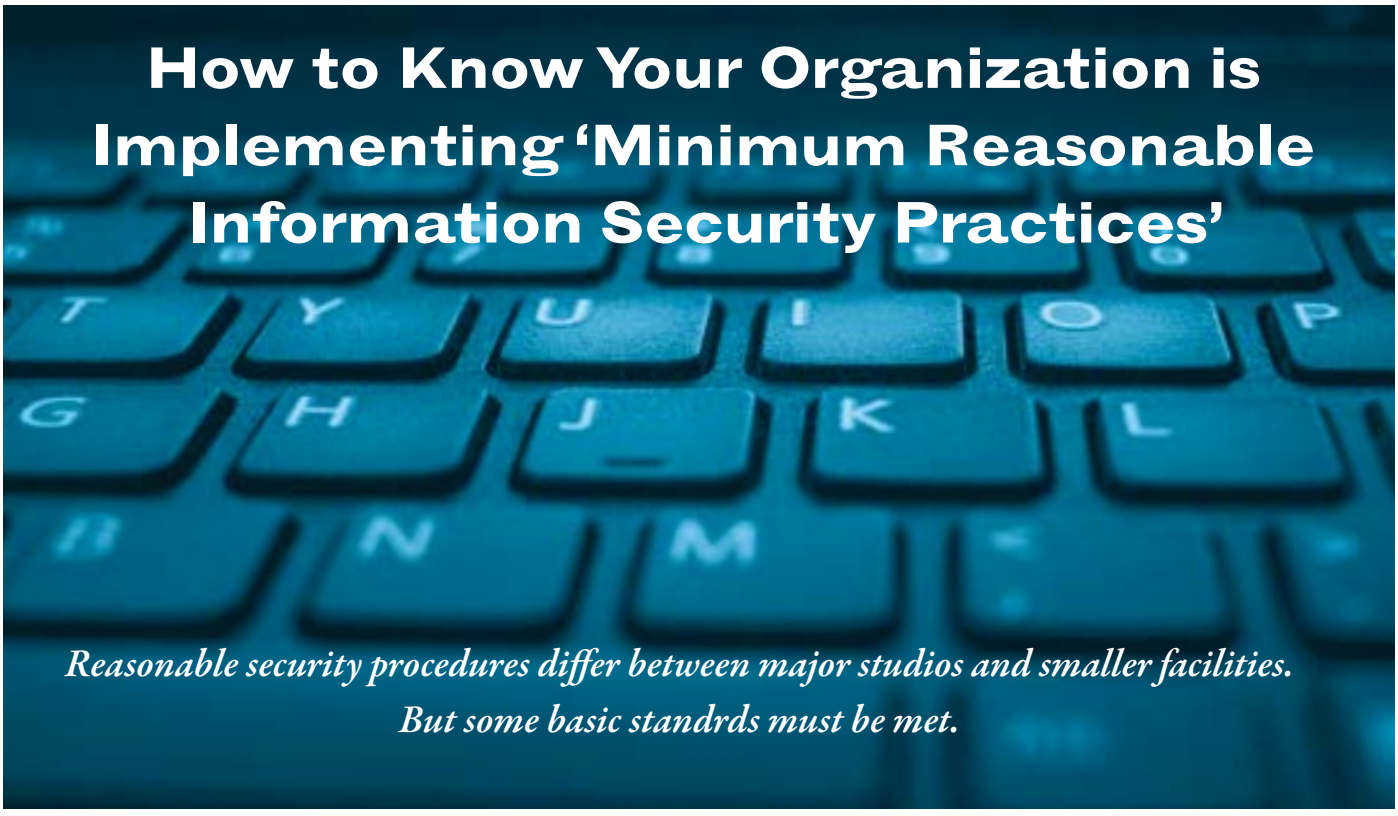
The NOW WHAT? *Issue*

A new remote-work reality will mean long-term changes for how M&E gets business done. Welcome to Hollywood's new normal. *P. 15*

M AND E JOURNAL
Media & Entertainment
Strategies. Solutions.

published by
MESA
Media & Entertainment Services Alliance

How to Know Your Organization is Implementing 'Minimum Reasonable Information Security Practices'



Reasonable security procedures differ between major studios and smaller facilities. But some basic standrds must be met.

Photo by Ingvio Studio from Pexels

By Dr. Stan Stahl, President, SecureTheVillage; Ilanna Bavli, President, Eleven/11 Counsel and Strategy; George Usi, Founder, Co-CEO, Omnistruct; and John Coleman, CISM, Senior Associate, AuditOne

Abstract: Are your information security practices reasonable? Shortcomings may result in content leaks or poor Trusted Partner Network (TPN) assessment results, and now may also increase the risk of financial losses due to the California Consumer Privacy Act (CCPA). We describe cybersecurity nonprofit SecureTheVillage's Minimum Reasonable Information Security Practices and how it provides a foundation for efforts to reduce business information risk.

As a consequence of the 2018 California Consumer Privacy Act (CCPA), chief information security officers in and out of the entertainment industry are being called upon to assure their management and boards that their organization's information security practices are "reasonable," i.e., that security procedures and practices are reasonable to protect the information being secured.

The concept of "reasonableness" goes to the heart of the Trusted Partner Network (TPN) program as well. A vendor having a TPN assessment should reassure a studio that security procedures and practices are reasonable to protect the content being secured.

But just what are "reasonable information security procedures and practices?" What is reasonable for a major studio whose server contains the full 137 minutes of its highly-anticipated franchise release is different from what is reasonable for a small VFX house whose servers contain three minutes of a low-budget indie movie. It's clear that there's no one-size-fits-all.

Recognizing that reasonableness can vary for different organizations and looking at the reasonableness question through the lens of the CCPA, cybersecurity nonprofit SecureTheVillage asks: Are there a minimum set of information security practices that a company must implement and maintain for it to claim that it has reasonable information security procedures and practices?

We believe the security practices summarized here are a minimum set of information

security practices that a company (subject to CCPA) must implement and maintain for it to claim that it has reasonable information security procedures and practices.

The security practices described here are designed to be a floor: If you are not doing these things, then you are unlikely to have reasonable information security procedures and practices¸ regardless of your size or the type of content or data you are attempting to secure.

Most definitively, SecureTheVillage is not claiming that a company that implements these minimum practices has reasonable information security practices. We're simply saying that a company's failure to implement these practices is highly likely to be prima facie evidence that the company's information security procedures and practices are not reasonable.

Objectives of SecureTheVillage

SecureTheVillage brings together the information security community as a force multiplier to help it better understand and manage the cybercrime and privacy challenge. We organize the community in order to mobilize what we call Cyber Guardians. These are people and organizations with the knowledge, skills and commitment needed to meet the ongoing challenges of cybercrime, cyber privacy and information security.

Recognizing that it takes a village to secure us all, SecureTheVillage leadership council members are aligned professionals with a commitment to assist in improving security capabilities, a desire to grow and expand the cybersecurity community, a passion for giving back, and a make-it-happen, results-driven attitude. We intend to scale and cascade the village concept throughout California and beyond.

SecureTheVillage developed its Minimum Reasonable Information Security Practices for the community in order to significantly improve the information security capability of everyone involved, to encourage all of our organizations to meet — at the very least — minimum reasonable practices.

Our primary motivation has been to provide meaningful operational guidance to those organizations needing to meet a standard of reasonableness. More generally, we see Minimum Reasonable Information Security Practices serving as:

- *A straw man in community dialog over what might constitute reasonable information security practices and what might not.*
- *A baseline for companies to use in designing their own information security procedures and practices.*
- *A guide for attorneys to use in advising their clients on managing the legal risks of CCPA, other laws and regulations, and contractual agreements (like the payment card industry).*
- *A guide for insurance providers needing to assess the information security reasonableness of policy holders.*
- *A guide to financial institutions in evaluating their exposure to an information security incident of a customer.*

Pointing the way

SecureTheVillage relies extensively on several frameworks and standards as pointing the way toward what might constitute reasonable information security procedures and practices:

- *The National Institute of Standards and Technology (NIST) cybersecurity framework is a logical contender for what constitutes reasonable information security, one that provides a top-down perspective of information security management based on five core functions: identify, protect, detect, respond and recover.*
- *The Center for Internet Security's (CIS) Critical Security Controls (CIS-20), another logical contender for what constitutes reasonable information security. In California's 2016 "Data Breach Report," then-attorney general*

***Stan Stahl**, co-founder of information security management company Citadel Information Group, co-founded SecureTheVillage as a nonprofit community-based response to the cybercrime and privacy crisis.*
stan@securethevillage.org @stanstahl

***George Usi** co-chairs the California IPv6 Task Force, a nonprofit IPv6 scientific advocacy group, and is a board member of SecureTheVillage.*
gusi@omnistruct.com

***John Coleman** provides audit and consulting services to financial institutions in the western U.S. He has 30-plus years' experience in various roles including CIO, CISO, IT director, and audit manager for Los Angeles-area companies.*
john.coleman@auditonellc.com

***Ilanna Bavli** represents entertainment content providers and vendors on content security, investigations, data privacy, vendor agreements, and production/development work. She serves on the board of SecureTheVillage.*
ibavli@eleven11counsel.com

The concept of **'reasonableness'** goes to the heart of the **Trusted Partner Network (TPN)** program. A vendor having a TPN assessment should **reassure a studio** that **security procedures** and **practices** are reasonable to **protect the content being secured.**

Kamala Harris wrote: "The 20 controls in the Center for Internet Security's Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the controls that apply to an organization's environment constitutes a lack of reasonable security."

■ *Like the CIS-20, the New York State Department of Financial Services' Cybersecurity Requirements for Financial Services Companies covers operational requirements that provides reasonable information security procedures and practices.*

■ *Companies certified compliant with the International Standards Organization (ISO) family of standards likely meet the threshold of reasonable information security procedures and practices.*

Key elements for reasonable security

The following summarizes nine key elements constituting Minimum Reasonable Information Security Practices, as we see it:

■ *Information security management: The organization manages its information security by means of a formal documented Information Security Management program. The information security manager is an executive or reports to an executive. The program is designed to protect the confidentiality, integrity and availability of information in accordance with commercially reasonable information security management standards appropriate for a company with its security-risk profile and the security-risk profiles of others whose information it manages.*

■ *Information security subject matter expertise: The organization utilizes appropriate information security subject matter expertise, with either a Certified Information Systems Security Professional (CISSP) on staff, or is utilizing one through an ongoing consulting relationship.*

■ *Security management of sensitive and private information: The organization formally identifies, documents and controls access to sensitive and private information — including content — in accordance with laws, regulations, contractual obligations, and in accordance with its own fiduciary responsibilities.*

■ *SecureTheHuman: The organization has an active awareness training and education program to turn personnel into Cyber Guardians.*

■ *Security management of the IT interface: All access to the organization's network is protected in accordance with documented procedures, based upon the CIS-20. This includes user identification and authentication, account creation and removal, email, access to cloud servers, etc.*

■ *Security management of the IT infrastructure: The organization formally manages the security of its IT infrastructure in accordance with documented standards based upon the CIS-20. This includes security architecture, vulnerability and patch management, endpoint and network security, documentation, logging and review, encryption, etc.*

■ *Third-party security assurance: The organization follows a formal documented process to manage the risk associated with sharing information — including content — with third parties. This includes following documented standards based upon the CIS-20 to ensure the security of third parties having access to information or information systems, including vendors, distribution and promotional partners, solution providers, cloud service providers, backup/recovery systems, etc.*

■ *Information resilience: The organization develops, maintains, and tests incident response plans and business continuity plans. This includes training staff to meet their incident response or business continuity responsibilities and maintaining relationships with law enforcement and other professionals likely to be crucial should an incident or disaster occur.*

■ *Information security governance: The organization meets at least quarterly with executive management to review the organization's information security profile.*

Future plans

SecureTheVillage's Minimum Reasonable Information Security Practices is a work-in-progress, and our approach considers a community-wide effort to get our collective arms around reasonable information security practices.

Being "reasonable" with our industry's security procedures and practices begins with looking at the standards already out there, and anticipating what's going to be needed in the future. ■

SECURE THE VILLAGE
Creating CyberGuardians

A Community-Based Response to the Cybercrime and Privacy Crisis

It Takes a Village to Secure the Village. ™

Managing our security and privacy is a community-wide effort.

Collaboration and education are key.

From the Boardroom to the Family … Everyone's a CyberGuardian.

Join Our Village!!!

Media & Entertainment Product / Service Companies

- Attend Our Online Community and Educational Events
- Stay In-the-Know with FREE Cybersecurity News of the Week with Weekend Vulnerability and Patch Report
- Learn from Our Educational Resources
- Get Expertise from Our Leadership Council
- Connect: Follow us on LinkedIn

TPN Qualified Assessors & Other CyberProfessionals

- Join Our Leadership Council
- Add Your Leadership and Expertise
- Contribute to our Resource Library
- Be Part of a Community-Wide Solution
- Be a Speaker on Our Educational Events
- Showcase Your Expertise

SecureTheVillage Resources

- Information Security Management ResourceKit, including 20+ Webinars
- Minimum Reasonable Information Security Practices
- CyberGuardian: A SecureTheVillage ™ Guide for Residents
- Cybersecurity News of the Week with Weekend Vulnerability and Patch Report
- Cyber Town Halls … Cyber Roundtables … Cyber Happy Hours

SecureTheVillage is Supported by Our Platinum Sponsor, Miller Kaplan MILLER KAPLAN

SecureTheVillage is a 501(c)3 Public Benefit Corporation
Turning People and Organizations into CyberGuardians
https://securethevillage.org/