Health IT Security Journal

Volume 2, No. 2

A publication of the HITSF

Data classification made simple

Embedding supply chain Information risk management into vendor management processes

Health IT Security Journal

Volume 2, No. 2

HITSF

This journal is a publication of the Health Information Technology Security Forum.

The Health IT Security Forum is an International Security Organization that dedicated to help healthcare organization in securing their privacy data, confidential information, medical devices and will be recognized for the passion of its members in conducting multidisciplinary research and development in the area of Healthcare IT Security and e-Health.

Letter from the editor

Dear readers,

This is the second year of the Journal and we are proud to present another issue. This issue of the HITSF journal offers insight into information security for healthcare practitioners. We hope you will enjoy it and we welcome your feedback. Please send questions and feedback to editor@healthitsecurity.org

- Hadi Syahrial

Disclaimer

The author(s) of each article appearing in this Journal is/are solely responsible for the content thereof; the publication of an article shall not constitute or be deemed to constitute any representation by the Editors that the data presented therein are correct or sufficient to support the conclusions reached or that the experiment design or methodology is adequate.

IN THIS ISSUE

www.healthitsecurity.org

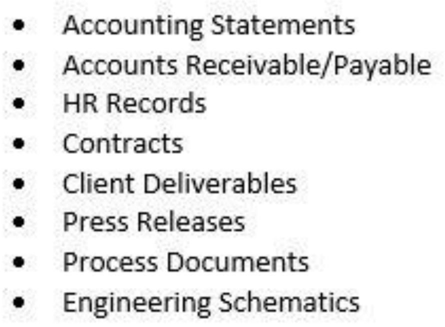
Data Classification Made Simple

by Eric Vanderburg

Few people are probably unfamiliar with the concept of classified data, yet what likely springs to mind for many is a government office deep within the confines of The Pentagon where a stack of top secret documents rests. There it is. Clearly stamped in red, bold-faced type. **CLASSIFIED.** While classification is imperative for government documents containing secret, top-secret, or other sensitive information, determined – for reasons of national security – to be in need of protection, data classification should not be misunderstood to be only for governments or for reasons of national security. Rather, data classification is a key measure critical to the everyday success and longevity of all organizations.

While many companies already classify their data, the classification system has been set up to be somewhat basic. For instance, some information is determined to be public and, accordingly, is published on company websites or in promotional materials; and other information is kept within the organization, guarded from outsiders. Some further classification may even exist based on the internal structuring of departments so that not all employees have access to all information. Classifications that are limited to particular areas within the organization can range from salaries and other personal employee information to research and development ideas or even advanced technologies and business strategies.

Unfortunately, many organizations either stop at this fairly straightforward level of data classification or they fail to organize and communicate the criteria for classification. Further, even with such elementary measures of classification, implementation is neither consistent nor actionable. This is often due to the perception of the high costs of implementing such programs, which would necessarily involve individual pieces of data being categorized, the purchase of equipment, and maybe even the hiring of outside experts.

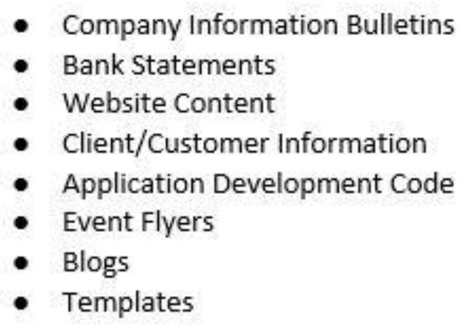


- Accounting Statements
- Accounts Receivable/Payable
- HR Records
- Contracts
- Client Deliverables
- Press Releases
- Process Documents
- Engineering Schematics

In order for organizations to move beyond a simpler classification structure and achieve the significant benefits of data classification without the associative high costs that could go with it, there are some easy steps that can be performed by teams easily created within any company. The steps include identifying the data that exists within the organization, grouping the data into areas of similar sensitivity and availability needs and defining classifications for each. The team then determines how the data will be handled for each of the classifications. Here is how it works:

Step 1: Consider the Data

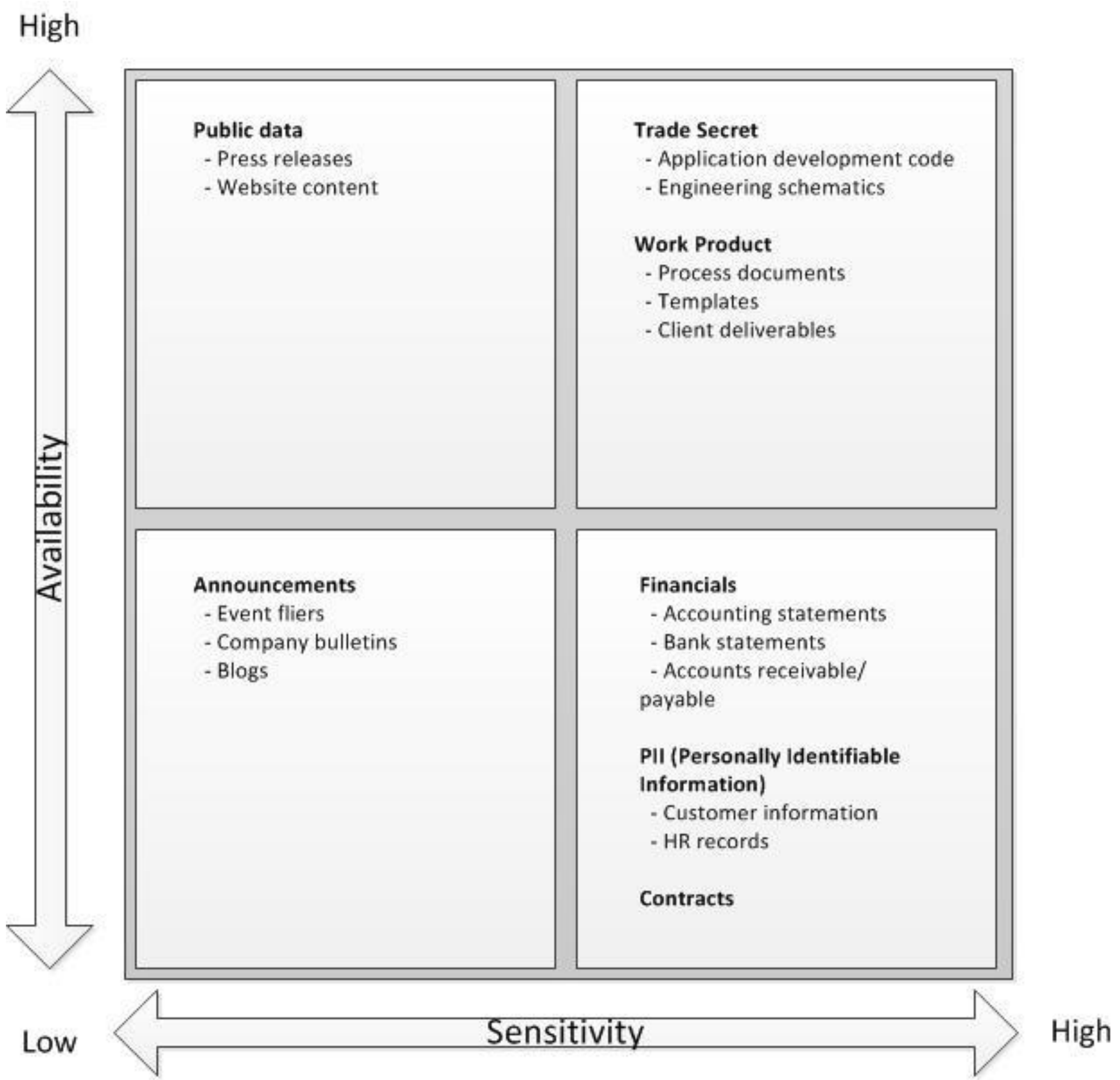
A data classification scheme ensures protection. Without knowing the types and location of data, it is not possible to be adequately protected. Unfortunately, if you were to ask most IT folks in small or mid-sized companies to provide a schematic of the data types going into and out of their network, they might not be able to do it.



- Company Information Bulletins
- Bank Statements
- Website Content
- Client/Customer Information
- Application Development Code
- Event Flyers
- Blogs
- Templates

Brainstorming sessions can help facilitate this step, and important component of the brainstorming is to include individuals from different areas within the company who understand the various data types and how losses of data or availability can impact the organization. At this stage, it is critical to obtain different inputs as to values as they are determined across different functions within the business.

The list of data types might look something like this:



Public data
- Press releases
- Website content

Trade Secret
- Application development code
- Engineering schematics

Work Product
- Process documents
- Templates
- Client deliverables

Announcements
- Event fliers
- Company bulletins
- Blogs

Financials
- Accounting statements
- Bank statements
- Accounts receivable/ payable

PII (Personally Identifiable Information)
- Customer information
- HR records

Contracts

Step 2: Group Data

Once the data types have been identified, they must be grouped into areas that have similar sensitivity and availability requirements. It is important that the organization adopt a common set of terms with which to group such data. This way, impacts and risks can be assessed for different data types and exposures. The example below only illustrates a low or high selection for availability and sensitivity. The matrix for a specific organization, however, could have three or more sections for each, as desired.

Step 3: Define Classifications

The diagram created in Step 2 highlights the data within the organization along with parameters for determining levels of sensitivity and availability. Once the data has been grouped, data classifications can be created to encapsulate that data. There should be at least as many classifications as there are filled cells in the matrix. In the example, the following classifications can be created:

SECRET: <u>High Sensitivity/High Availability.</u> Secret data includes trade secret and work product data that could cause serious damage if altered, disclosed, or made unavailable.

RESTRICTED: High Sensitivity/Low Availability. Restricted data includes such information as financials, Personally Identifiable Information (PII), and contracts that do not need to be as available as secret data but could still cause serious and long-term damage if disclosed.

PUBLIC: Low Sensitivity/High Availability. Public data such as website content or press releases needs to be available for use, but causes little to no damage when disclosed. In fact, the very purpose of the data in this classification level is to disclose it to others via website content or marketing materials.

UNRESTRICTED: Low Sensitivity/Low Availability. Unrestricted data such as the annual company picnic flyer, or the industry news bulletin, would have little impact if disclosed. Likewise, these types of data would have little impact if they were unavailable.

Step 4: Define Classification Handling Procedures

Once data has been identified, grouped and classified, handling procedures are ready to be defined. An outline can be created on the data protection for each classification level. Secret and restricted data naturally will require more security controls, including multi-factor authentication, encryption, and physical separation from other data types. Such controls are not necessary for public and unrestricted categories of data. However, while it is not a requirement, public and secret data might reside on redundant servers with more extensive backup and recovery options than those for unrestricted and restricted data.

By using this type of a data and classification structure, organizations can save significant costs by assigning only the necessary security protections to those areas that require it and, thus, direct important resources and the assignment of information security controls to those vital areas. The structure can be as elaborate as necessary and include automation and complex classifications. Ultimately, the classification structure is such that is it always created by the organization as a custom fit for the organization. Moreover, using the steps outlined provides a net of security without the costly expenses associated with additional software, hiring new employees, or utilizing large amounts of employee time. The end result is that such a structure offers up for the organization what is considered to be the most basic of needs required for any entity to maintain a healthy, vibrant existence: safety and security.

About the Author:

Eric Vanderburg

Director, Information Systems and Security, JurInnov Ltd.

Eric Vanderburg understands the intricacies inherent in today's technology and specializes in harnessing its potential and securing its weaknesses. He directs the efforts of multiple business units including Cyber Security, eDiscovery, Computer Forensics, Software Development, IT and Litigation Support at JurInnov, an eDiscovery and eSecurity consulting firm. Vanderburg holds over thirty vendor certifications and is completing a doctorate in information assurance. He has dedicated much of his career to designing and implementing systems, policies and procedures to enhance security, increase productivity, improve communications and provide information assurance. He has been invited to speak at conferences and events on technology and information security and he is active in promoting security and technology awareness through various publications. Look for his latest book, "Storage+ Quick Review Guide", due for publication with McGraw Hill in December of 2013.

Embedding Supply Chain Information Risk Management into Vendor Management Process

by Hadi Syahrial

Supply chain is the linked set of resources and processes that begins with the sourcing of raw material and extends through the delivery of products or services to the end user across the modes of transport. The supply chain may include vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers and other entities that lead to the end user.

Sharing information with suppliers is an essential part of daily operations, however doing so increases information risk: the risk that the confidentiality, integrity and availability of that shared information could be compromised.

The key to managing information risk in the supply chain is an information-led, risk-based approach to determine what information is being shared and assess the probability and impact of a compromise.

Information shared in the supply chain can be broadly grouped into six categories:

- commercial information
- intellectual property
- legal, regulatory and privileged information
- logistical information
- management information
- personally identifiable information.

Supply chain information risk management should be embedded within existing procurement and vendor management processes, so supply chain information risk management becomes part of regular business operations.

The following are the steps to embed information risk management into the procurement or vendor management lifecycle:

1. Define requirements
2. Search for potential suppliers
3. Conduct procurement tender
4. Evaluate tenders and select supplier
5. Negotiate and agree contract
6. Monitor performance, remediate
7. Exit, terminate, renew or renegotiate

Define requirements examines what information categories will be shared and the information security arrangements required, based on the information category risk assessment score.

Search for potential suppliers, the information security function supports the search for the potential suppliers Stage of the vendor management lifecycle by providing information security arrangements, questionnaires and analysis of supplier responses as input into the Request for Information (RFI) process.

Conduct procurement tender the information security function supports the conduct procurement tender Stage of the vendor management lifecycle by reviewing the RFI responses from potential suppliers and, based on the results of that review, providing new, revised or more detailed information security arrangements and questionnaires for inclusion in the tender documentation.

Evaluate tenders and select supplier, is where the information security function supports the evaluate tenders and select supplier Stage of the vendor management lifecycle by analyzing the tender responses from potential suppliers and, based on the results of that analysis, providing recommendations to assist the selection process. After the supplier has been selected, the requirement for due diligence and information security due diligence is examined and performed as required.

Negotiate and agree contract the information security function supports the negotiate and agree contract Stage of the vendor management lifecycle by proposing the information security related terms and conditions for inclusion in the contract.

Monitor performance, remediate information security function supports the monitor performance, remediate Stage of the vendor management lifecycle, by monitoring and evaluating the information security performance of the supplier. Frequency and type of evaluations are typically included in the contract.

Exit, terminate, renew or renegotiate, information security function supports the exit, terminate, renew or renegotiate Stage of the vendor management lifecycle by working alongside the business to determine whether to terminate, renew or renegotiate the contract.

Reference:
ISF, *Securing the Supply Chain Implementation Guide*, February 2013

About the Author:

Hadi Syahrial

Hadi Syahrial is a Lecturer and Researcher at Budi Luhur University, Jakarta, Indonesia.