The Classification of Valuable Data in an Assumption of Breach Paradigm

Jeffrey Carr

When a company or a government acknowledges that they cannot keep a dedicated adversary out of their network then the applicable security strategy changes from perimeter-based to an assumption of breach; a new security paradigm that was raised by Debora Plunkett (head of NSA's Information Assurance Directorate) on 16 December 2010: "We have to build our systems on the assumption that adversaries will get in."[1] Once that major hurdle is crossed, the next security hurdle is to acknowledge that an organization cannot protect everything all of the time. Therefore, the responsible organization must identify which data is worth protecting and which is not.

Dr. Daniel Geer, who is presently the CISO of In-Q-Tel, called this the "shrinking perimeter" in a 2004 white paper that he wrote while he was the Chief Scientist and Vice President at VerdaSys.[2] Dr. Geer concisely composed the problem statement in two sentences: "To protect individual objects of value individually. More precisely: Contract the protection perimeter to individual data objects."

This protection focus presumes that there is high value attached to a company's data. After all, a target that has no value either to its owner or to an adversary is not worth

Jeffrey Carr is the author of "Inside Cyber Warfare: Mapping the Cyber Underworld" and is an adjunct professor at George Washington University. He is the founder of the cyber security consultancy Taia Global, Inc. as well as the Suits and Spooks security conference.

protecting. When a large corporation has literally millions of data files on its global network, some are going to be more valuable than others. A few will be worth extraordinary protection while others could be let go without any possibility of harm coming to the company. Since protection is not free, it is vital that a company assign relative value to its disparate information. One way to do that is to evaluate how much harm would be caused by the release of that data (i.e., what would the monetary losses be):

"Almost any company has some bit of information that is both privately held and crucial, some bit of information that if prematurely revealed or revealed at all would cause irreversible harm. An equity pricing strategy, expansion plans not yet board-approved, the contents of a protein database, corporate succession plans and associated compensation, next generation chip masks, incomplete responses to subpoenas, patent filings in process, customer details acquired under the promise of safe handling, the negotiating position in merger talks, and so forth."[3]

Another way to measure the value of a company's intellectual property and gauge how much a breach would cost the company is to determine their research and development investment. If a new technology cost x and is projected to generate y, then xy would be the value of documents related to that technology. If one just examines x as total research and development (R&D) costs on a national level without including projected revenue, the numbers are in the hundreds of billions.

For example, according to a VentureBeat article from 12 October 12012, 50,000 scientists at 100 U.S. labs are creating technologies fueling 100 startups a year thanks to a $100 billion program funded by the U.S. Department of Defense.[4] This represents about 25 percent of the total R&D expenditure of the United States (estimated at $400.5 billion in 2009).[5] Yet, the loss of intellectual property through IP theft has been estimated by the IP Commission report to be $300 billion in 2012.[6]

The U.S. government has a well-known system of classification for its valuable data: FOUO (For Official Use Only), Confidential, Secret, and Top Secret. Private industry has developed a similar process. This paper examines ways that the U.S. government as well as some private sector organizations classify their valuable data as well as what controls are applied with those classifications.

Executive Order 13526. Kevin Kosar of the Congressional Research Service wrote a CRS report entitled "Classified Information Policy and Executive Order 13526" on 10 December 2010. Much of the information in this paper related to government classification policy comes from that report.

EO 13526 came about as a result of the unauthorized release of several hundred thousand classified documents from the State Department and the Department of Defense allegedly accessed by Private Bradley Manning who provided them to Julian Assange's Wikileaks organization. Wikileaks quickly posted them on the Web. These documents, which included 250,000 classified State Department cables, were accessed via the U.S. government's clas-

sified network known as SIPRNet. It is perhaps the clearest and most dramatic example of what's known as the "Insider Threat" (i.e., the malicious act of a person with trusted credentials on their corporate or government network). The release of those cables had worldwide implications that were serious enough for the U.S. Secretary of State Hilary Clinton to make personal phone calls to various governments around the world in an attempt to mitigate the damage that their release may cause.

The author was speaking before the National Security Council of India on the morning that a New York Times story broke about this breach and the first question that he received from the attendees had to do with how the U.S. government could have let something like this happen. There was no other answer than current access policies at the time allowed a person with the appropriate clearance level access without establishing a "need-to-know" or other controls such as establishing a set number of allowable downloads in a given time period. It was clear to everyone in the room that the system was broken.

Private companies can learn a lot from the federal government's system of classification, both positive and negative. For one thing, a good classification program is a necessity for every company that has information that needs protecting. In some cases, like financial data (PCI) and personal identifying information (PII), those controls are regulated. However, the safeguarding of source code, trading strategies, patent data, and other "crown jewels" of a company is sorely in need of a standardized classification system.

The standard in federal law that is applied to the question of classification is:

"Information or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security (50U.S.C. 426(1)).[7]

So the key definitional standard is - will the release of this information harm national security? If the answer is yes, it gets classified. Corporations can ask that same question by simply replacing "national security" with "profitability." And in fact, corporate boards of directors should demand that their executive team ask that question and take action to identify, classify, and protect with special handling the intellectual property whose loss will negatively affect the ability of the corporation to maximize profits. That is rarely being done today.

Part of the reason is probably related to cost. Kosar writes that, "The

Private companies can learn a lot from the federal government's system of classification, both positive and negative.

total government classified information policy costs were $8.8 billion in FY2009."[8] That figure doesn't include the classified information policy costs of the following intelligence agencies, whose budgets are themselves classified: CIA, DIA, ODNI, NGIA, NRO, and the NSA.

Kosar writes that about "55 percent ($4.8 billion) of the FY2009 estimated costs are attributed by agencies to "information security;" 15 percent ($1.3 billion) to "security management, oversight, and planning;" and 30 percent ($2.7 billion) for background checks and other personnel related costs like training in the handling of classified documents.

Corporations have the opposite problem from the government — they do not classify enough documents.

Unlike corporations, the U.S. government has three primary classification categories: Top Secret – for documents whose release could be expected to cause "exceptionally grave damage to national security;" Secret – for documents whose release could be expected to cause "grave damage;" and Confidential – for documents whose release could be expected to cause "damage."

The types of information that are available for official classification in the interests of national security are not all-inclusive, but are limited to the following per E.O. 13526:

·Military plans, weapons systems, or operations

·Foreign government information

·Intelligence activities (including covert action), intelligence sources or methods, or cryptology

·Foreign relations or foreign activities of the United States, including confidential sources

·Scientific, technological, or economic matters relating to the national security

·United States Government programs for safeguarding nuclear materials or facilities

·Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans or protection services relating to the national security

·The development production or use of weapons of mass destruction

While the system that the U.S. government uses to classify its critical information is robust and well documented, it is facing a new problem of classified information overload.[9] In FY2010, officials classified 77 million documents – a scenario that's been criticized by everyone from Donald Rumsfeld to President Barack Obama.

Corporations have the opposite problem from the government – they do not classify enough documents. Once a company correctly assumes that its network could be penetrated at any time or has already been breached, it must acknowledge that it is impossible to protect all of its information. It can, however, protect its most critical information – its crown jewels. To do that, it must have a system of classification with

special handling protocols assigned.

California Independent System Operator (Cal ISO). California Independent System Operator is the organization responsible for distributing electrical power throughout the State of California. They don't have the best track record when it comes to keeping hackers out of their system, nor in implementing best practices in network defense; however, they have recently done a fine job in producing a document classification standard. Cal ISO produced a public document in 2010 entitled "Information Classification Standards and Protection Procedures," which standardizes sensitive document handling in accordance with the company's Enterprise Information Security Policy.[10,11]

"The objective of information security is to reduce the risk to the California ISO and Market Participants by protecting information, information systems and communications that deliver the information, from failures of integrity, confidentiality, and availability, whether information is in storage, processing, or transmission. Information security is seen as an enabler to achieve California ISO business strategy and objectives and to avoid or reduce relevant risks."[12]

The document starts out by categorizing information for which enhanced protection is mandated by law:

-Protected Health Information

oPer the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

-Personnel Records

-Personal Identification

oPer the California Database Protection Act (CDPA), this act protects an individual's first and last name in combination with their SSN, Driver's license number or CA I.D. card, account number, credit card number, and account passcodes.

It then moves to categorizing information that is mandated by the company itself, which includes:

-Intellectual Property, which includes information protected by copyright, trademark, trade secret, patent or other intellectual property right under Federal law.

-Company Records, which may be any information required to be kept confidential by Cal ISO's Articles of Incorporation.

-Records pertaining to matters properly discussed in closed executive session.

-Records that refer to commercially sensitive matters, disclosure of which may affect the competitive positions of the Corporation's market participants, or otherwise compromise the efficiency of the market as a whole or of the efficient and nondiscriminatory access to the transmission grid.

-Critical Infrastructure Protection (CIP) Information, associated with Critical Cyber Assets regardless of media type, shall be treated as CAISO Confidential, and shall include:

oOperational procedures for Critical Cyber Assets

oThe Critical Asset List and Critical Cyber Asset List as required in CIP-002

oNetwork topology or similar diagrams for Critical Cyber Assets

oFloor plans of computing centers that contain Critical Cyber Assets

oEquipment layouts of Critical

Cyber Assets
- oDisaster Recovery plans for Critical Cyber Assets
- oIncident Response plans for Critical Cyber Assets
- oSecurity configuration information for Critical Cyber Assets

Cal ISO has created five classification levels along with handling protocols for each. The levels of classification and their definitions are:

Cal ISO Classification	**Definition**
CAISO Public	Public information is information that can be disclosed to the public without restriction in compliance with federal and state laws, and regulatory tariffs and protocols. Knowledge of this information does not violate an individual's right to privacy or expose the corporation to financial loss, embarrassment, or jeopardize the security of assets
CAISO Internal Use	Internal Use information is information that, due to technical or business sensitivity, is limited to sue by employees and contractors only. Unauthorized disclosure, compromise, or destruction would not have a significant impact on the corporation or its employees.
CAISO Confidential	Confidential information is information that the corporation and its employees have a legal, regulatory, or social obligation to protect. It is intended for use solely by employees who have a need-to-know. Unauthorized disclosure, compromise, or destruction would adversely impact the corporation or its employees.
CAISO Restricted	Restricted information, the highest level of classification, is information whose unauthorized disclosure, compromise, or destruction could result in severe damage, provide significant advantage to a competitor, or incur serious financial impact to the corporation or its employees. It is intended solely for restricted use within the corporation and is limited to those with an explicit, predetermined "need-to-know".

PCII or CEII	PCII or CEII classification was established by the Federal government (e.g., DHS and FERC) to protect information relating to the nation's Critical Infrastructure Information submitted to the government by the private sector from being released to the public sector. PCII is for information being submitted to DHS and CEII is for information being submitted to FERC.

Just as the U.S. government evaluates what the impact to national security might be if classified information is made public, Cal ISO has identified an impact disclosure for each of the above classifications.

Cal ISO Classification	**Impact Disclosure**
CAISO Public	If disclosed, no impact to the ISO business processes or damage to company's public image and trust.
CAISO Internal Use	If disclosed, low to medium impact to the ISO business processes or damage to company's public image and trust.
CAISO Confidential	If disclosed, medium to high impact to the SO business processes such as potential compromises or damage to the company's public image and trust. Loss of confidence by the company's shareholders.
CAISO Restricted	If disclosed, high to critical impact to the ISO business processes, computing and communications infrastructure, individual privacy, and compromises or damage to the company's public image and trust. Loss of confidence by the company's stakeholders.
PCII or CEII	If disclosed, critical impact to the reliability of the nation's Electric Grid.

Eurofound's Rules for Classification of Documents. Eurofound is the European Foundation for the Improvement of Living and Working Conditions. Their "Rules for Classification of Documents" is much less robust than Cal ISO's, but it is included here for comparison reasons. Eurofound's document, like Cal ISO's, is public information and it was last updated in 2007. The following tables represent a summary of Eurofound's classification policies:

Eurofound Classification	**Definition**
Confidential	Documents are confidential when their unauthorized disclosure could harm the essential interests of an individual, the Foundation or the EU.
Restricted	Documents are restricted when their unauthorized disclosure would be disadvantageous to the Foundation, the EU or a third party. Documents with this classification are usually restricted for a period of time. Examples of restricted documents may include: • Documents of internal management meetings • Documents of groups involved in the preparation of the work programme • Documents that have not been finalized or adopted • Documents containing sensitive details supplied by third parties in confidence • Management reports prepared by external consultants.
Eurofound Classification	**Impact Disclosure**
Confidential	Commonly accepted criteria for confidentiality are where the release of a document would: • Harm the privacy and integrity of an individual • Breach undertakings to respect the confidential nature of information provided by third parties • Breach statutory restrictions on disclosure of information • Cause financial loss or facilitate improper gain or advantage for individuals or companies • Impede or undermine the effective management or operations of the Foundation
Restricted	Documents are restricted when their unauthorized disclosure would be disadvantageous to the Foundation, the EU or a third party.

Conclusion. While the standard approach to document classification by both governments and corporations is to evaluate the impact of disclosure upon the organization, there is another way to classify documents – by adversary interest. This is the process developed by the author for Taia Global's Chimera™ product.

The concept of classification by adversary interest is a simple one. If a company or government knows what information a potential adversary needs and is spending money on to develop, and if that company or government owns intellectual property (IP) that corresponds with those needs, then all documents related to that IP should be classified with appropriate handling controls.

The adoption of an assumption of breach security paradigm includes accepting that no organization can protect all of its data. Hence, it must decide which data is worth protecting and which is not. That should be done as part of the classification process (assuming that an organization has a classification plan that is operational), but it can be further refined by adding an additional layer: does this document contain IP that would appear on an adversary's shopping list?

While this paper examined different classification schemes, a simple three-option process is recommended: Public, Company Confidential, and Restricted. Examples of Restricted data would include everything that the company is legally compelled to protect along with trade secrets and intellectual property.

Restricted data should be stored and accessed on a separate internal, highly monitored network that has no Internet or email access, similar to the way that control systems at power generating stations have no Internet connectivity or connection to the front office or business network. In fact, if companies think of their Restricted data as radioactive, then the security procedures and protocols should be equally stringent for that limited data set; however, describing defensive protocols for radioactive data is a topic for another day.

NOTES

1 Brian Prince, "NSA: Assume Attackers Will Compromise Networks," eWeek.com (17 December 2010).

2 Daniel E. Geer, Jr., "The Shrinking Perimeter: Making the Case for Data-Level Risk Management," Verdasys, Inc. (January 2004).

3 Geer, ibid. p.1

4 John Koetsier, "Allied Minds and the DOD," VentureBeat.com (12 October 2012).

5 Science and Engineering Indicators 2012: http://www.nsf.gov/statistics/seind12/c4/c4s1.htm

6 Please see: http://www.ipcommission.org/

7 According to Kosar (Classified Info Policy and EO 13526, CRS), "this definition only applies to the Intelligence Identities Protection Act (50 U.S.C. 421-426). Similar definitions also may be found at 18 U.S.C. 798(b) and 50 U.S.C. 438(2)."

8 Kevin Kosar, "Classified Information Policy and Executive Order 13526," Congressional Research Service (10 December 2010).

9 Elizabeth Goitein and J. William Leonard, "America's Unnecessary Secrets" The New York Times (7 November 2011).

10 Power outages impacted 400,000 California households during May 7-8, 2001. Cal ISO had two Solaris web servers hacked and the hackers were active in their network from April 25 – May 11, 2001. According to the company, the breach wasn't responsible for the power outage but the timing can't be ignored. See: http://www.greenspun.com/bboard/q-and-a-fetch-msg.tcl?msg_id=005RHL

11 "California ISO Information Classification Standards and Protection Procedures," 2010.

12 Cal ISO, Ibid