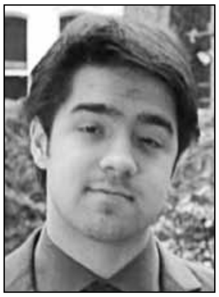
Protecting and Tracking Confidential Materials

BY NIKOLAUS BAER AND JASHAN AHUJA

Nikolaus Baer



Jashan Ahuja

Nikolaus Baer is a project manager / research engineer at Zeidman Consulting, a contract R&D firm. He has utilized the CodeSuite® software as an expert witness in litigation involving copyright infringement and trade secret theft, and designed the internal asset tracking system used at Zeidman Consulting. He can be reached via email at Nik@ZeidmanConsulting.com.

Jashan Ahuja was an engineering intern at SAFE Corporation during the summer of 2011. He implemented many features of the internal asset tracking system used at Zeidman Consulting. Currently he is a student studying Mechanical Engineering, Computer Science, and Business at Cornell University. He can be reached via email at jna33@cornell.edu.

INTRODUCTION

When you send your confidential material to an outside expert, do you know how it is handled and what steps are taken to protect it? Through our years of working on numerous high tech intellectual property disputes, we have developed several policies that we follow to protect our client's valuable confidential materials. There are greater efficiencies when we are able to perform an analysis at our own location with our own systems and tools, but this privilege has required the establishment of a strict security protocols. Our clients entrust us with some of their most valuable property, in the form of source code and confidential documentation, so we take the necessary steps to safeguard their property while it is in our possession. Unfortunately, it has been our observation that not everyone assumes the same level of responsibility for protecting confidential material, so we would like to help promote best practices in the industry by sharing how we handle and protect confidential materials. Our system is based upon careful personnel management, multitier physical and electronic security, and an asset tracking system that reinforces the proper handling of confidential material.

PERSONNEL AND POLICIES

A security policy is highly dependent on the proper implementation by a firm's employees, so we are careful to screen each job applicant and all employment offers are subject to reference and background checks. Our security policies are well documented, approved by the president of the company, and reviewed by the current employees. Furthermore, all new employees are required to review the security policy documents and all employees are required to implement the security policies of the company.

PHYSICAL PROTECTION

The first elements of protection are the physical barriers that we utilize to prevent unauthorized access to electronic media.

Security System

Our facility itself is equipped with motion detectors throughout the offices and alarms at every entrance, which are monitored at all times. Intrusions result in immediate notification of local law enforcement.

Safe

Even inside our secure facility, we store all confidential material in a locked safe that is only accessible to the employees. This is further protection against theft, as it adds another layer of protection against any intruder. It also prevents accidental disclosure of confidential information to facility visitors, since the materials are always stored in our locked safe and not available for inadvertent or casual observation by unauthorized persons.

Removable Drives

One aspect of our protocol that facilitates the physical protection as well as electronic protection of materials is our use of encrypted removable drives to store confidential electronic data. We have observed that many organizations often store confidential digital materials directly on individuals' computers, which are difficult to secure both physically and electronically. To circumvent this issue, we store all confidential electronic data on removable drives. When the data needs to be examined we connect a drive to a secure non-networked computer and when not in use, we store the drive in our locked safe, so that it is both physically and electronically secure.

ELECTRONIC PROTECTION

We are as cautious about the electronic protection of our client's confidential materials as the physical protection, so we are also careful about when and how material may be exposed to networks as well as how we dispose of confidential material.

Email

There are several steps that we follow to secure our email. We have a company-wide policy of never sending confidential material through email, unless specifically allowed by a client. Even when emailing a document is approved, we still encrypt client documents unless specifically instructed not to do so. We also have a detailed policy for creating rules in our email clients to segregate emails from different clients into specific folders, so that materials from our various clients are not intermixed.

Networks

Another aspect of our security policy is our network security protocol. Our network has the usual protection of a firewall and every single computer on the network must have anti-virus software installed and running. Regardless of these common security features, we only examine client material on computers that have been disconnected from the network. Not only is this a typical requirement of many protective orders, but it protects against network security issues. For instance, security vulnerabilities that can be created by practices such as remote access are absolutely prevented, because the confidential material is never exposed to any network.

Encryption

We further protect all confidential material by storing it in encrypted volumes with a program called TrueCrypt, the free open-source encryption tool from the TrueCrypt

Foundation. We have found this to provide excellent security with the minimum amount of workflow interruption. TrueCrypt automatically encrypts data right before it is saved and decrypts data right after it is loaded. We create a large TrueCrypt volume on each removable drive, and use it to store all confidential material, so that even if the removable drive were to become compromised, all of the data would be inaccessible without the correct password.

Furthermore, we maintain separate passwords for each client, and the employees are only provided with the passwords for the particular material they should examine. This ensures that employees only have access to the confidential material that they are entitled to examine. Also, if one password is discovered, it limits the potential vulnerability to a single client.

Destruction

The multiple security barriers would not be complete without a policy regarding the proper disposal of confidential materials once they are no longer needed. This can take one of two forms, either we will return all confidential materials directly to the client in a manner directed by the client or we will destroy them. Confidential paper materials are shredded on-site, as are some electronic media such as CD-ROMS and DVD-ROMS.

All confidential material is completely erased from removable drives and computer systems through the use of Eraser©, a free open-source tool from The Eraser Project, which overwrites selected electronic data with carefully selected patterns. Normally, when one deletes a file, it is moved to the systems trash/recycle bin and can be easily restored. Even if the recycle bin is emptied (a file is "doubly deleted"), much if not all of the data is left as remnants on the computer's storage device, and forensic tools could be used to recreate the files and extract the data. To completely remove confidential data, the section of the storage device that contains the data must be overwritten with new data. This technique is also known as electronic shredding.

TRACKING

We have developed an internal material tracking system that enforces our security protocols by providing a convenient and secure method for recording who has possession of confidential materials.

Concept

Tracking the location of all materials is a key aspect of our system. Materials are either secure in a safe at the office or are in the possession of an employee, and our system allows for easy updating and real-time tracking of material locations.

Implementation

We use an internally designed system that is built around a SQL database of client material. The database system was first built by our engineers and recently updated to handle increased capacity and improve user functionality. The updated database has an entry for every single transaction, defined as a document or item transfer, and each entry contains various pieces of useful information including a "Client ID," "Material ID," "Item Description," "Bates Number," and the current "Possessor" or material location information. There is also a field showing which user last updated an entry, which is necessary for security and accountability in the system.

The Item Description and Bates Number are entered when a material is initially received and added to our system and are not changed as materials are transferred. The Client ID and Material ID are unique to a material's record and together define a material in the system. The most up-to-date entry for a material is displayed to the user, however together the Client ID and Material ID allow us to observe the material's transfer history. The material location status fields, Possessor, Transfer Date, Received Date, and Returned Date, are used for the actual tracking of materials. They are initialized when a material is received and updated accordingly as the option to transfer materials is exercised by the user.

The system also allows users to review a single material's transfer history, what material a user currently possesses, and what materials are being tracked for each client. These additional views of the material location history provide additional insight into how specific materials are being used and help to ensure that our other security protocols are being followed.

User Interface – Security and Functionality

Employees have access to the tracking system through a secure website. Only employees can access the system and must use their unique login credentials to access the tracking system. All users must login before they can see any information in the tracking system or make any modifications or transfers. When accessing the system, users can enter new materials, transfer materials, search materials, and edit materials. Whenever a user performs any action in the system, the user's unique User ID is recorded in connection to that action. This ensures accountability for all system users and allows the administrators and managers to track behavior if necessary.

When entering new materials the user must fill out all required database fields. The transfer function allows a user to transfer materials to a new location and only modify the Possessor and Transfer Date fields. The tracking system updates the most current entry in the displayed table, but maintains the previous entry as part of the material's possession history. The search functions allow users to search for all the materials in a certain location, or access the history of a material's possession. The edit function allows users to modify all entries for a material, including the material's Description and Bates Number. It is mainly used to correct any errors made when initially entering a material, and the user cannot modify any identifying ID numbers, such as the Client ID and Material ID, ensuring a correct document tracking history.

Anonymous labels.

The Client ID that is used with each material entry record is an anonymous numeric ID, as opposed to the actual client's name. Although the client's names are stored in the system, this use of an anonymous label for the actual material records insulates the specific materials and utilization of the materials from the client's other information.

Secure System Administration

Administrator access to the tracking system's underlying database is restricted to two employees of the company. This ensures that the core database and any low-level modifications to the system cannot be made by all user's of the system.

Furthermore, a user name is recorded for every user action. This cannot be modified by the user, so the proper use of the system can be ensured by monitoring whether users are correctly tracking materials.

CONCLUSION

The security protocols that we follow and enforce give us and our clients the confidence that confidential material will be secure when entrusted to our company. In an industry where so much valuable information is exchanged and protective orders must be adhered to, we hope that our security protocols can be used as a guide for other consulting firms that may not yet have created similar security protocols and for attorneys evaluating outside experts.

We have created multiple layers of both physical and electronic protection for our clients' materials through a combination of strict company policies and exact methods for storing and accessing materials. The material tracking system that we utilize helps manage and enforce these protocols by ensuring that we are able to locate any material at any time as well as determine a history of which employees have had access to any particular confidential material. Providing clear security protocols that outline proper material storage, usage, and accountability can help even the most conscientious people keep confidential materials safe.

We would like to thank Jim Zamiska and Bob Zeidman for their insight and valuable feedback in drafting this article.