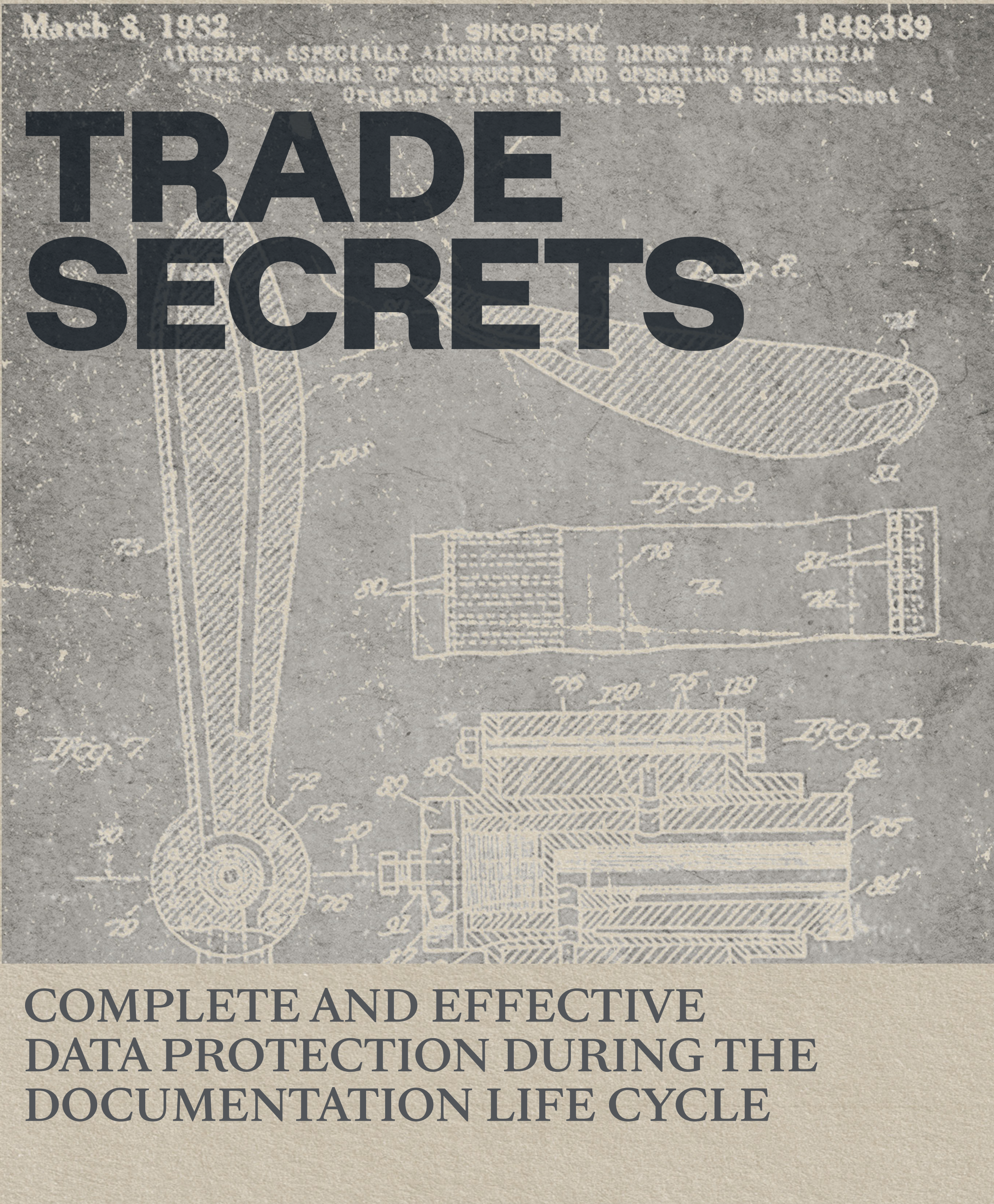
perimetrix


March 8, 1932.
I. SIKORSKY
1,848,389
AIRCRAFT, ESPECIALLY AIRCRAFT OF THE DIRECT LIFT AMPHIBIAN
TYPE AND MEANS OF CONSTRUCTING AND OPERATING THE SAME
Original Filed Feb. 14, 1929
8 Sheets-Sheet 4
Fig. 7.
Fig. 8.
Fig. 9.
Fig. 10.

TRADE SECRETS

COMPLETE AND EFFECTIVE DATA PROTECTION DURING THE DOCUMENTATION LIFE CYCLE

ALL FILMS ABOUT ROBBERIES begin with the perpetrators acquiring the floorplans or blueprints for the building that they are going to burgle. Moreover, the documents are usually sold to them by an employee of the company, who is well aware that the information will be used for nefarious purposes. Obviously, simple bribery is much easier and more effective than training spies or physically assaulting building. For us, however, it is important to understand that very often film plots are actually based on real–life events.

But there is another issue that design department managers do not want to talk about. Production sites are often full of dangerous materials and objects. And all of the information related to such hazards is usually concentrated in project archives. If people can learn how to properly design ammonia pipelines, chlorine or fuel storage facilities, then someone can learn how to properly destroy them, causing a maximum amount of material damage and human casualties. All that is needed is a blueprint to know exactly where to place the explosives.

Therefore, the project department head's policy of "security does not concern me, my business is to deliver the project documentation on time" is very *short-sighted*. And the subsequent "it wasn't my responsibility" never finds acceptance, neither from top management, nor from the prosecutor's office.

You can never be too prepared

Almost every design engineering or architectural firm, to one degree or another, faces the problem of preventing data leaks. Often in conversations with designers we hear sad stories about how their drawings or projects "pop up" in competing bids. Time and effort are spent, money is invested, and at the last moment it turns out that the proprietary knowledge of the company is not proprietary after all. The tender is lost and the company not only loses the long-awaited contract, but also propriety development methods and techniques as well as their competitive advantage. Locking everything down will not fix the situation. What is needed is to find the "gap" in security through which important data leaked.

Often in such situations, the head of the company flies into a rage and by using their authority, they prohibit everything that is possible to prohibit (flash drives, local printers, internet access, e—mail, Skype, etc.). As a result, the company's normal business processes and data processing procedures completely break down, productivity stops, and employee morale takes a huge hit. As a result, instead of solving one problem, the company winds up with lots of others.

What to do? How can you find a reasonable balance between "tightening the screws" and fighting leaks? Who should be involved in the search for security "gaps"?

Today's design documentation is a complex product created by a team using computer-aided design (CAD) tools. Naturally, the idea arises to seek help from the IT specialists who installed and who maintain the CAD solution. However, there is a catch to this approach, one which the head of the company likely does not even suspect.

Staff decide, "that's it!"

In order to understand why IT is not the best option for managing end-to-end information security, it is necessary to understand the main motivation of an IT employee.

From the point of view of information security, the three main properties of information are *confidentiality, integrity and availability* (CIA). At the same time, the main objective of IT, as a department that supports the main business of the company, is primarily to ensure the constant availability of IT services and to ensure their integrity (correctness). The task of ensuring confidentiality, however, requires thorough knowledge of the data, the content, the business value for the company, the permissions given to employees in terms of access, etc. These are "matters" that only the "owner" of the data can determine. The owner being the chief designer, head of the project management department, the financial director, etc. In other words, IT staff members simply do not have the required knowledge to make operational decisions that ensure the degree of data confidentiality required. In such a situation, the IT specialist either "ticks a box", introducing policies that restrict everyone, or they try to shift the decision-making responsibility for the classification of data to people who are able to really assess its importance. In addition, it is ideologically difficult for IT employees to implement security measures that restrict or make it difficult for users to access information. This is because the main task of IT is to ensure the availability of IT services. Information security is often understood by IT specialists as safeguarding the IT infrastructure, and not the actual content. By safeguarding the infrastructure, IT often focuses on things like antivirus protection, data backups, applying security patches to software, controlling internet access, etc.

This leads to two very important conclusions. First, the decision on how to protect the company's information assets (its know-how, product development, and product designs) should not be made by IT. It should be made by individuals who are responsible for security, with the involvement of specialists who have the necessary training in the field of information technology. Secondly, the classification of information assets should involve department line managers, who understand better than anyone else, the actual business value of the data. The value assigned should reflect the importance of the data both to the company itself as well as to any competitors who may want to use it to gain an advantage.

Anatomy of a leak

Now let's go back to the problem of leaks and try to understand how they occur. Let's begin by analyzing how information is created and transferred when creating complex data. Such items can include designs, architectural drawings, product documentation, etc.

Even though data is “insubstantial” and “intangible”, it is never—the—less, at any given moment stored in some form in some location. We call this a “data container”. Such a container can be a designer's brain, a file on a disk or a flash drive, an email, a printed drawing, a CAD application in which a designer works, etc. During processing, information is moved from one container to another: for example, an “explanatory note concerning a project” goes from the designer's head to an unsaved Microsoft Word document. The file is then saved to the computer's hard disk, from where it can be attached to an email, copied to a network folder, sent to a printer, etc. In each case, the data object moves from one container to another. At the same time, it is important to understand that there are many ways data can move between containers. Information in digital form has a “fluidity” that did not exist prior to the digital era. A leak, therefore, can be defined as a chain of successive "elementary" data movements, the result of which is having confidential data end up in the hands of those for whom it was not intended.

The first action that comes to mind when the need to safeguard confidential data arises is to place restrictions on every communication channel through which data can “leak” and to attempt to spend some time analyzing whether the information should be allowed to leave the security perimeter or not. Security software should be able to distinguish between “permitted” and “restricted” movements of data, blocking those that are unauthorized and not interfering with those that are allowed. In fact, such tools should monitor all data traffic, analyzing and classifying content on-the-fly. Since the main objective in this case is to identify “unauthorized” movement of data, a security system should contain a set of criteria by which it can identify and determine which activities are in fact permitted. To do this, the system analyzes the information’s context, patterns, digital fingerprints, file types, etc. The processes that determine if data movement is “prohibited” should analyze all possible methods (protocols) of transmitting data, catching any activities that appear “suspicious”. At the same time, when searching for intruders, it is important not to disrupt normal production processes with false positives. This is critical since the losses accrued from downtime can sometimes exceed the actual losses from a leak. As a consequence, companies often feel forced to use such tools in a “mirroring” or monitoring mode, saving the captured data in archives for subsequent analysis or “debriefing”. In fact, during monitoring the leak is still happening, and it is only discovered after a certain amount of time has passed. However, there is still a trace of the events in the system which can be used to investigate the incident and potentially identify the culprits.

We didn’t have a care in the world...

And then the company faces the next problem! An investigation of an information security incident should lead to some follow-up actions. Actions could include introducing new rules for detecting “unauthorized data movement” as well as more severe punishments of the perpetrators. However, in order to punish the culprits, it is necessary to prove their guilt and that they did indeed violate company policies. To this end, the company needs to prepare “on all fronts”. It needs to develop and implement security provisions concerning trade secrets. These include making appropriate changes to employment contracts, introducing procedures for familiarizing employees with materials that contain trade secrets, creating and formalizing internal groups that are responsible of analyzing security incidents, etc. The “user manual” eventually turns into a huge list of prohibitions that an employee, if they were to study the list in its entirety, would likely soon forget. The end result is that the employee is unable to fully comply with all of the policies.

At this point, management has usually already given up. They have realized that getting involved in the fight against leaks will require reworking existing policies and/or developing new ones. Moreover, they will probably have to recruit and pay for additional HR specialists and legal staff, train employees, and enforce compliance with the new rules. Therefore, the introduction of a trade secret security system often stops at simply declaring that trade secrets exist in the organization. Writing a policy "on trade secrets", however, does not actually translate into proper or effective working practices.

How can we escape from this vicious circle? In fact, there is a relatively simple way out of this situation. We just need to look at the problem from top to bottom.

Defending the security system

Let's look at the task of protecting confidential data from the point of view of the head of the organization. Senior management doesn't think about network protocols, I/O ports, network storage addresses, valid file name extensions, etc. These are all “superfluous matters”. A senior manager will never define point-by-point what can or can’t be done with confidential information. The manager will simply say, “Let people who are authorized do what they are supposed to do. And stop anything else related to our information assets that is either harmful, not needed or not required.”

Therefore, the old democratic approach to protection based on the principle of “Everything is allowed except that which is prohibited” is now transforming into a radically different approach. The new approach is to state that “everything is prohibited except that which is explicitly allowed”. This maxim might seem extreme, but such an approach to protecting confidential information is, in fact, much more productive than its liberal counterpart.

First of all, when considering all of the possible activities that can be performed in a digital environment, the number that actually need be controlled for busines processes to work is extremely small. Workflows are generally known in advance and are usually very stable and not subject to major changes. Therefore, it is much easier to make a list of “permitted” activities rather than defining everything that is prohibited.

Secondly, by defining and reinforcing business processes and workflows that are allowed, we wind up standardizing and organizing them, which ultimately leads to an increase in both their efficiency and security.

Thirdly, safeguarding confidential data in this way does not interfere with permitted and legitimate user activities since the system is actually built around them.

In order to implement the “everything is forbidden except that which is explicitly allowed” approach at the information system level, we need to take the following four steps.

Master the path by walking it

Step one → *classifying* content. You need to determine what needs to be protected and what its value is to the company.
Step two → *defining* permissions (authorization) for users who are allowed to work with confidential data.
Step three → *defining* the rules (in the language of IT, “policies”) according to which users will work with confidential data.
Step four → *implementing* a system that will verify the user’s credentials based on the classification of the data object.

At each and every step the system will either allow or prohibit subsequent actions based on defined policies. Let's look at all of the above in relation to design and development activities. Let’s assume that the data to be protected is a drawing created in a CAD application. Included with the CAD file are text files, tables, images, etc., which were created in office applications and are stored all together on the PDM portal.

Each one of the documents above contains an integral “classification tag”, which accompanies the document and any documents derived from it throughout every stage of its life cycle. The classification tag specifies things such as user permissions, which applications can be used, authorized storage locations and formats, transmission methods, etc.

The classification of information can and should be carried out using categories that are clear to the business, and at an appropriate level of detail that will provide the necessary granularity when assigning user permissions.

For example, ❶ the following *specifications* can be defined:
— **CONFIDENTIALITY** (values: “unclassified”, “for internal use only”, “trade secret”).
— **FUNCTION** (values: “design data”, “design documentation”, “financial data”, “marketing information”).

❷ user *permissions* are defined using the same specification, for example:

- The **chief designer** has access to “design data” and “design documentation” with any level of confidentiality, and to other data only up to the level of “for internal use only”;
- A **finance specialist** has access only to “financial data” with “CONFIDENTIALITY” of “unclassified” and “for internal use only”;
- A **secretary** has access to all documents with any defined function but with no access to items whose CONFIDENTIALITY is “trade secret”;
- The **head of the company** has access to all data.

❸ when we define *policies* for working with data, we can formulate them at a fairly high level, for example:

- Design data can only be *stored* on the PLM/PDM system or on the hard drives of authorized computers.
- *Working* with design data is only possible using approved applications (e.g., AutoCAD, Compass, nanoCAD, etc.) as defined by policies.
- *Printing* of design documentation is allowed only on certain network printers which are physically located in the project delivery department.
- Design data can only be *copied* to registered removable drives and to authorized network locations.
- *Sending* design data via e-mail is restricted to an approved list of addresses.
- *Saving* design data to cloud storage is not defined as being allowed.

The above policies are then translated into low—level security system policies. The verification of the legitimate use of confidential data is monitored and managed at an elementary level, that being the movement of data from one “information container” to another.

Automatic protection

The questions that immediately comes up are: how, when and who will assign the classification tags? Wouldn't the user have to keep track of all of these tags resulting in lots of extra work? What happens if the user unknowingly or, conversely, intentionally does not assign a classification tag? The answer is simple. The lion’s share of the work on assigning classification tags, as well as on controlling the movement of confidential data, is performed by the security system itself. As far as the system is concerned, a person is an “untrusted” user, because our ultimate objective is to protect confidential data from a user’s unauthorized actions.

A so—called **mandatory rights management model** is implemented. The data owner determines the value of the data and the basic requirements for ensuring its confidentiality. The user can only handle the data in strict accordance with the rules (*security policies*). Even when creating data, the user is not allowed to make the decision about which classification tag to assign. It is the system that makes the decision based on the requirements that were defined by the data owner.

Therefore, classification tags are assigned as follows: the initial classification of data that is stored on each user’s workstation is performed by a special agent of the security system. This agent scans the storage locations and, based on specified rules (e.g., file type, context, storage location, etc.), assigns a persistent classification tag to the file, which cannot be removed by the user. For example, you can define a rule that ensures any new file created in AutoCAD is automatically assigned a “trade secret, design data” classification tag. Any subsequent actions with the file will be subject to the defined security policies. Moreover, if a user makes a copy of the file, the classification tag will be inherited, and any subsequent files will automatically carry the same classification tag as the parent file. The classification tag also follows content. The tag persists not only when making a copy of the file, but also when transferring content to the clipboard, or to another application, etc. You can implement more complex procedures for assigning classification tags if needed. For example, if a designer receives data from the PDM portal, then you can define a rule by which the data will receive a classification tag on-the-fly.

What should be done in a situation where the workflow requires the transfer of confidential data outside of the security perimeter? For example, if there is a need to show the project to a customer in their offices. In this case, the confidential information can be placed in a "*cryptocontainer*", which is a kind of encrypted archive. A cryptocontainer can only be opened on a computer (e.g., laptop) with the security driver installed and which has access to the corporate policy server. The policy server issues the password for opening the cryptocontainer. Therefore, even when outside of the office, confidential data will continue to be managed according to corporate security policies.

No more illicit activities

One of the positive side-effects of using the described security system is in the fight against people who use company property for personal financial gain. It's no secret that some designers manage to do projects for "private" customers during paid working time using company resources. The company where the person works can sometimes lose significant amounts of money because of this, by essentially paying for illicit work that is sold by a designer to a third party. So, by assigning classification tags and defining appropriate permissions, it becomes impossible to transfer work created on company resources outside of the organization, except through formal corporate channels. Using company property for illicit activities no longer makes sense because the end product can no longer be taken out of the organization. At least not without admitting that the illicit activities were done during working hours.

Conclusion

To conclude, many modern computer-aided design and electronic document management systems have fairly well-developed tools and processes for managing user access to content that is stored and processed on them. However, when the data is transferred to a user's computer, it is no longer under the control of the CAD or EDM system. It is necessary, therefore, to control any subsequent actions involving confidential data using specialized security measures in order to prevent leaks.

The security system needs to protect confidential information while at the same time not blocking information that has no significant value to the company. Moreover, the system should not allow "false positives" to disrupt legitimate business activities, nor should it create additional bureaucratic overhead. ■

All of these features are catered for by **PERIMETRIX SAFESPACE** *classified information management system.*

ⓘ visit us on perimetrix.com for more details

perimetrix © 2021 Perimetrix LLC

A Russian company founded in 2007, whose products have been trusted for more than 10 years to protect the confidential data of organizations such as AvtoVAZ, Gazprom Energoholding, the Federation Council of the Federal Assembly of the Russian Federation, TVEL and others. The company has a network of partners in Russia and abroad. The company's headquarters are located in Moscow.

www