



**INDORSE TECHNOLOGIES**

## **If there is more than one person in your organization – including you – then IT security is a necessity.**

In order to explore the importance of IT security, just look at the upcoming Presidential race. What do national presidential politics have to do with your enterprise IT Security? With illegal immigration; isolationism; global trade; and homeland security all looming as major issues, you face the same risks and challenges inside your organization when you consider the effectiveness of your IT assets.

Your organization is in the information service business. If it wasn't important information, then there would be no need to provide it as a service and even less concern over protecting the information. The very reason you exist makes the protection of your IT assets a genuine requirement. For a variety of reasons, there are people who want to access the information you have. There are only a few reasons they want access to this information – to know what you know; to delete what information you have; and/or to change the information in your charge (fraud).

You can, and most organizations do, scramble the information (encrypt) so that it requires a key (PKI) to unscramble the information and be able to read, use, store, change, print and share with someone else. Once done, the latest user encrypts the information again and sends it on its way. While encryption can be "unscrambled," few malcontents ever have to resign themselves to it – they simply inject themselves in places where the information is legitimately opened – in an application – in an e mail – at the printer – saved on a thumb drive. Organizations spend millions to establish sophisticated security procedures across their networks, electronic gatekeepers (firewalls) that apply a list or "rules" to the information that wants to get into your organization and information that wants out. The stronger and more effective the gatekeeper, the more difficult it is to have unwanted information coming in and flowing out. A good thing, right? Wrong.

Information in the hands of one person is much like a clay sculptor working in a dark closet. Real valuable information is the result of the input and collaboration of a number of people, each contributing a thought, an inspiration, a challenge, and an occasional epiphany. This is your organization's treasured "work product." It is your organization's "reason for being." That's when this valuable work product is most coveted by those outside your organization.

Now, the most valuable bit of information. The strongest and most impenetrable IT security is a security strategy designed for only a single user who never has to interact with anyone else. Said another way, the instant a user has to interact or connect with another user – security becomes an issue. Once you need to create a secure environment for two or more, the chance for your security to be compromised is increased exponentially. The stronger the firewall, the harder it is to collaborate. Your organization has built a tight security perimeter around your organization. Today, little is accomplished with full potential without having to reach outside a given department or enterprise, so, the security has to be made "lax" enough to facilitate relatively easy transport in and out of your secure enterprise.

The IT department is the war room serving as the front line against information attacks. In their arsenal are numerous encryption tools (we can encrypt the information, the network, the message and more); firewalls (gates)

can be set up between departments, organizations, and the general public ( the world wide web) with a variety of weapons, rules and challenges built in at different levels. Figurative system guards are armed with challenges to ensure you are who you say you are (authentication) by seeing if you have the right answers or the right thumb print. Once a guard (rule) is satisfied you are who you say you are, he looks in a series of policies, rules and procedures to discover where to send you – what doors you can open and what you are allowed to walk in with and, more importantly, what you can walk out with (authorization).

The most cautious have integrated digital rights management (DRM) into their infrastructure. DRM enables the creator to “lock down” the way certain work product will be dealt with while “in the system.” A set of electronic “dog tags” are hung on the work product that tell system “security guards” who is supposed to have this work product; who can print it; who can save it; who can edit it; and who can send it along to someone else.

Many have added e mail scanning and scrubbing tools. For example, it applies an algorithm to recognize patterns like social security numbers, or 26 consecutive digits that could likely be check information or the number of consecutive digits in a credit card.

The right mix of security is the product of IT alchemy in the domain of the IT wizards in any organization. Put the same rules and protection on everything in the organization and the system resources required to check, double check and recheck are overwhelming. One can expect that everything moving through the IT system will slow to a crawl. Things will be so slow it will make passing notes and sending interoffice mail in manila envelopes look speedy again. Organization have to “dial back” security to achieve an acceptable mix of secure protection and free flowing collaboration.

While not every piece of information in your IT system would be considered “sensitive” or mission critical, there are classes of work product that would be categorized as “not for everyone!” and “protect this with your....job!” Volumes of regulatory rules have been published from the medical community to define and defend certain kinds of information from being publicly consumed (HIPAA, JAHCO, ACCA). **Sarbannes-Oxley** has established rules and tests to ensure that financial information is protected from being intentionally modified and the source go unchecked.

- **Health Insurance Portability and Accountability Act (HIPAA)** – Enacted in 1996, this broad law covering all aspects of health insurance contained among many provisions an entire portion concerning administrative simplification.
- **Federal Reserve Board Interim Final Rules on Electronic Disclosures** – These rules establish uniform standards for the electronic delivery of federally mandated disclosures under five consumer protection regulations: B (Equal Credit Opportunity), E (Electronic Fund Transfers), M (Consumer Leasing), Z (Truth in Lending), and DD (Truth in Savings).
- **Office of Management and Budget (OMB) Guidance on Implementing E-SIGN** – this guidance is for Federal agencies that may create regulations on how electronic records and signatures may be used in specific commercial processes that they regulate.
- **Government Paperwork Elimination Act (GPEA)** – federal law passed in 1998 allowing for the use of electronic signatures and records by all federal government agencies.
- **Office of Management and Budget (OMB) Guidance on Implementing GPEA** – as required by GPEA, OMB has developed and published procedures and guidance to Federal agencies on their use and acceptance of electronic signatures.

- **eAuthentication Guideline** - this guideline is published by the eGovernment eAuthentication Initiative team and addresses the principles and techniques to be used by government agencies in authenticating any user that will interact electronically with the government.
- **National Archives and Records Administration (NARA)** - publishes a number of guidance documents relating to electronic records management including guidance for agencies implementing electronic signatures and records.
- **Electronic Recording for County records** – There are many documents handled by county recorders. The most important are real estate documents that consume the majority of their time and could be streamlined with electronic recording.
- **FDA CFR 21 Part 11** – This regulation came into effect in 1997 to enable the use of electronic records and signatures in all companies regulated by the FDA.
- **Federal Aviation Administration (FAA)** – In 2002, the FAA issued guidance on the use of electronic signatures, record keeping systems and manuals.
- **Gramm-Leach-Bliley Act (GLB) and other privacy laws** – GLB was enacted at the federal level to address a number of privacy issues.
- **USA PATRIOT Act** – Enacted following 9/11, this law contains a wide variety of provisions. Section 326, Verification of Identification has implications of systems using electronic records and signatures.
- **US E-Government Act** – Enacted in 2002, E-Government uses improved internet-based technology to make it easy for citizens and businesses to interact with the government, save taxpayer dollars, and streamline citizen-to-government communications.
- **State Laws** – all US states and territories have enacted laws and regulations on the use and acceptance of electronic records and signatures by state and local governments.

The best approach is to create an exercise of **Discovery/Index/Classification** for areas where an organization perceives work product worth protecting is being kept. This enables an organization to establish a series of “common thread” rules to apply to these classes of work product. Priority levels will be set; a list of user authorization rules applied; policies and procedures will be challenged against this catalogue of sensitive work product to explore potential gaps in the protection scheme.

Conversely, new projects and new initiatives that would fall into a “secure classification” require an exercise to apply authentication, authorization, access and other applicable rules and policies to how this work product will be managed from a security perspective.

A sure way to ensure that all the investment in defining these rules, policies and procedures pays off is to actually embed or fuse the relevant security information directly to the work product itself. For example, an e mail carries with it a requirement to check back with the security server when this particular user wants to open – edit – print – send – save or fax a particular work product and then only allow this user to do what they are “authorized to be able to do.”

Newer solutions create a “chain of custody” as the work product moves through its collaborative life cycle. This captures and records that this person created the work product; who opened it; who edited it; who did something with the work product – time stamped and recorded. Additionally, the original of the work product is compressed, encrypted and fused to the work product in a bar code to provide any authorized user throughout the life cycle of the work product – even after it is printed, faxed and/or archived – to provide the “original” work product to warrant authenticity – provide content integrity – deliver the true original. This sort of “Follow-Me-Security”© delivers a unique level of security for work product in BOTH electronic and in PAPER FORM.

This technology also makes it possible to extend the same security rules, policies, procedures and protocols to be followed even with someone who has a hard copy (paper) of the work product and they are well outside your own secure enterprise – Asian port preparing to export a ship full of product receives a Letter of Credit – and needs to be certain it is **a)** it is authentic and **b)** it has not been tampered with. With this approach, “multiple originals”© can be delivered securely with all the protection intended for the work product as if it stayed within the secure enterprise.

Anyway you cut it – if your organization designs work flows to be “isolationists” over “free trade” proponents then while you can potentially achieve higher levels of security – the quality of your organization’s work product will suffer. Electronic “terrorists” go well beyond hackers and “mercenary geeks” and include disgruntled employees and even work-aholics who take secure work product home on thumb drives to “work on over the week end” and their personal computers now are open to attack.

So whether your personal politics is for or against open borders or expanded executive powers to thwart terrorism, your organization’s secure “economy” lives or dies by how well you manage and anticipate where your most valuable work product is – and , especially, where it’s going.

CONTACT DETAILS:

WEBSITE: [www.indorse-tech.com](http://www.indorse-tech.com)

Email: [Joe.orlando@indorse-tech.com](mailto:Joe.orlando@indorse-tech.com)

Telephone: 646-495-6128