

These are dangerous times. Each week, we are confronted with the reality that another organization has had their security breached. This is the good news. The bad news is that in matters involving intellectual property breaches quite often go undetected; the damage has been done and the victim is unaware.

For legal and intellectual property professionals, senior executives, researchers, developers and others involved in handling intellectual property, Evizone provides a secure online service for the exchange of files and view-only messages and documents.

Identifying the threats

Corporate Espionage

There was a time when a computer virus was an isolated incident. However, over time, this moved from being simply an isolated incident to being a certainty. IT organizations now routinely take preventive measures to ensure this threat is countered.

Over the last few years, the increase in leaks, hacking attacks and corporate espionage has followed the same path. It has moved from being an isolated incident to being a distinct possibility and is now on the way to becoming certainty. Many companies and individuals have been hacked and had their confidential and secret information stolen; often without being aware that this has occurred.

An article from [Bloomberg](#) in December 2011 provides some insight into how prevalent this has become. iBahn, a service provider whose customers include Marriott and other hotel chains, was hacked. Customers and companies staying at hotels or using hotel meetings rooms had their computers and communications compromised. The article puts the low estimate of at least 760 organizations known to be compromised through this attack.

Another article from January 2012 highlights the awareness problem in full. Symantec, a company known for its security software, publicly revealed that source code to key products had been stolen during a [breach in 2006](#). The breach was discovered at the end of 2011, more than five years later. Since they have now asked their customers to stop using their product, [pcAnywhere](#), it begs the question as to what has been occurring to their customers over the last five years.

Based on what is known of attacks from China, Russia and other countries, a declassified estimate of the value of the blueprints, chemical formulas and other material stolen from U.S. corporate computers in the last year reached almost \$500 billion, said Rogers, a former agent for the Federal Bureau of Investigation.

Bloomberg – Dec 14, 2011.

China-Based Hacking of 760 Companies Shows Cyber Cold War

Employee theft

Not all threats originate outside the organization. Another key issue is how to prevent employees and soon to be ex-employees from stealing confidential corporate information and intellectual property. While many organizations have Data Loss Prevention solutions, these existing solutions are usually focused on detection rather than prevention. In many cases, an employee copying files to a USB thumb drive will go undetected.

In 2008, a low-level Intel engineer, Biswamohan Pani, was able to steal information valued by Intel at more than \$1 billion. This theft is well documented in a [Businessweek article](#). There are a few interesting takeaways from this theft:

- First, a low-level engineer had access to valuable design documents.
- Second, it was luck that this theft was detected. Pani's boss "heard a rumor" that Pani was headed to AMD. This prompted the investigation into what he had been up to.
- Pani's new employer, AMD, was unaware that the theft had taken place. So, Pani could possibly have applied this information for his personal benefit while at AMD. This could have potentially created problems for AMD if and when this was detected in the future.

It is only by chance, according to the government, that Intel learned of Pani's plans to work for a competitor and decided to check if he had made off with confidential files.

Businessweek – Nov 18, 2008.

Lessons from Intel's Trade-Secret Case

As with external corporate espionage, employee theft of confidential information, trade secrets and intellectual property often goes undetected. It is in the interests of the thief and any beneficiaries that this be the case. This is an important distinction. Neither the thief nor the beneficiary will care if a stolen document says "Confidential" or carries a watermark; a rudimentary approach that many organizations take. `

Hacks

Unlike corporate espionage infiltrators, hackers who attack corporate information infrastructure strongly prefer that these attacks be known. Currently, the most public of these groups is Anonymous. However, Anonymous isn't a specific group of people; rather it is a collective of like-minded individuals who attach the moniker, Anonymous, to their activities. While much of the discussion surrounding Anonymous speaks to the characteristics or culture of the group, from an Intellectual Property viewpoint, the key issue is each attack could result in a highly public release of confidential information.

A recent exploit of Anonymous was the [attack on Stratfor](#), a subscription-based provider of geopolitical analysis. In this attack, Anonymous stole subscriber information including credit card details, passwords and home address data. In this case, the public release of information was the

subscriber data. Another attack was the release of an [18 minute discussion](#) from a conference call between the FBI and the British police. The subject of the call was actions being taken against hackers.

It is characteristic of these hacks that two things will come out. One, anything of value that can be made public will become public. Two, the name Anonymous will be attached to this now public information which serves as proof that, once again, Anonymous has been successful.

Leaks

Finally, internal leaks occur. The most public forum for these leaks is, of course, WikiLeaks. As with externals hacks above, the threat is that confidential information, trade secrets and intellectual property are given wide public distribution by an employee.

As with employee theft, WikiLeaks often reveals that the perpetrator had access to a surprising amount of information. The most public example of this would be Pfc. Bradley Manning who leaked the [Afghan](#) and Iraq war documents and the posting of [US diplomatic cables](#). From an Intellectual Property perspective, the key takeaway from these leaks should be:

- One person can cause a surprising amount of damage.
- Access to a network should not be the same thing as access to content. Manning had access to SIPRNet and the Joint Worldwide Intelligence Communications System. This network access should not have meant access to all content on the network.
- The means was reasonably unsophisticated. He brought a rewritable CD containing Lady Gaga to the office; rewrote the disc with downloaded documents and the rest, as they say, is history.

Threat Summary

The following grid summarizes these threats.

		Victim	
		Unaware of Breach	Aware of Breach
Threat	External	Corporate Espionage	Hack
	Internal	Employee theft	Leak

Identifying these threats is only the first step. It is the way people currently communicate, the *communications status quo*, which is the real threat. The communications status quo opens the organization to the above threats.

Protecting information which must be shared

Information is the life blood of today's enterprise. Value is created from the sharing of ideas and data between individuals and organizations. For those working with intellectual property, there is a challenge in protecting information which must be shared. The cost of a security breach can be substantial; affecting shareholder value and corporate and personal reputations. For these reasons, when it comes to intellectual property, the following security measures should be adhered to:

- ◆ Information can only be accessed by those with a need to know.
- ◆ All messages and documents must be stored and secured in as few locations as possible.
- ◆ Any files exchanged should leave no trace in the conventional email system or in the user's browser cache/history
- ◆ Users with access cannot save, copy, forward or print any message or document. The communications can only be viewed by permitted users.
- ◆ All message and document access should be automatically recorded; providing a full accounting of who read what, how many times and when.
- ◆ Corporate retention policies should be automatically enforced.

Evizone: the most secure solution

Evizone is a secure, online communications service for the exchange of files and view-only messages and documents.

Securing Workgroup Communications

In the time it takes to compose a short email, any Evizone subscriber can form a workgroup for the secure exchange of files and view-only messages and documents. Workgroup members can be other Evizone subscribers or non-paying guests.



Evizone provides the highest security

Evizone's secure internet client creates a locked-down high security zone for safe communication. Only Evizone combines a second layer of encryption with patent pending anti-screen capture technology. Evizone leaves no trace of view-only communications on the user's desktop or in the conventional email system.



Evizone covers all of your communications

A complete secure communications service provides for the secure exchange of files and the delivery of view-only messages and documents. With Evizone view-only messages and documents cannot be saved, copied, forwarded or printed. Files are exchanged without leaving a trace within the conventional email system or within the recipient's browser cache and history.



Evizone automatically enforces your retention policies

Conventional email creates multiple copies of documents and messages and then gives these communications an almost perpetual life.

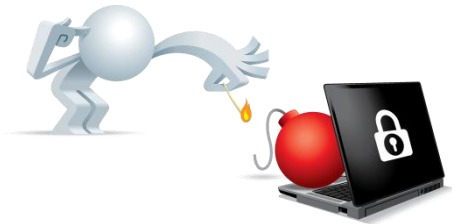
Evizone secures a single copy of your view-only messages and documents and will permanently dispose of these communications when your customer-defined retention period expires.

Access history is automatically recorded

Know whether or not recipients are keeping up with your communications.

Scheduling meetings and conversations is simpler when you know who has read your messages and documents, when they were read and how many times.





No trace left on the recipient's computer

Evizone only stores view-only documents and messages within the Evizone service.

If a notebook is lost, the user loses nothing while the potential hacker gains nothing at the same time.

A sender can withdraw a view-only message or document at any time; knowing that the withdrawn communication is not stored on the recipient's computer.

Evizone offers the Best Security and Control for your Intellectual Property



- ▶ Evizone copy and print protection puts you in control
- ▶ Messages and documents are only stored within Evizone servers
- ▶ Full life cycle management for all communications
- ▶ File transfer leave no trace in conventional email or browser cache/history
- ▶ Access history is automatically provided
- ▶ Withdraw messages and document from view at any time!

Secure | Controlled | Complete

It is easy to get started

Evizone's Software as a Service model* allows companies to be up and running in 20 minutes. Evizone's rich internet client software runs on both Windows and Apple OS X operating systems. The service is extremely cost-effective in that there are no setup costs and the service presents no capacity planning or upgrading issues. Contact enterprise@evizone.com for more information.

* other deployment options available upon request