

White Paper

---

# The Shrinking Perimeter: Making the Case for Data-Level Risk Management

**VERDASYS™**

Daniel E. Geer, Jr., ScD  
Vice President, Chief Scientist  
Verdasys, Inc.  
January 2004

Some day, on the corporate balance sheet,  
there will be an entry which reads, "Information";  
for in most cases, the information is more valuable  
than the hardware which processes it.

*Grace Murray Hopper, USN (Ret)*

The future is already here, it's just not evenly distributed.

*William Gibson, Neuromancer*

*When the threat increases, perimeters must contract. When perimeters are porous, insiders and outsiders are little different. The perimeter is contracting to the data-level as we speak, and data-level risk management is where it's at going forward. Know your data? Confirm it. Unsure? Explore it. Already in trouble? Take action.*

## WHY READ THIS

The time has come to value information in the books-and-records sense. No, it is past time. And what are the implications of the idea that information is a bookable asset?

The first is the issue of how to value it, and the second is how to arrange the protection of it in proportion to its value. Until we know more about your business, we will leave the first to you. We know about the second and hope you invest the time to read on.

## WHY INFORMATION SECURITY MATTERS

- Information security is central to trust, but it is a means, not an end.
- It will soon form the language of liability because while winners will certainly be those with the most information in play, losers will have too much.
- Information security is what distinguishes information that has economic value from information that does not.

## The Economics of Threat and Value

Security is an economic issue just as quality and reliability are economic issues. While the means to accomplish any of them are technical, the goals are economic. This is rarely said about security, and almost never believed. So much the worse.

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. For privately held companies, nearly everything about them is not ordinarily made available to just anyone. For publicly traded companies, premature disclosure can be nearly as bad as improper disclosure.

The point is this: We, all of us, already have information that in and of itself represents a corporate asset. The implication is just as clear: The loss of such information assets is a negative impact on the corporate balance sheet, whether we "realize" that loss on the balance sheet or not. As Gibson would have said, Hopper's prediction of the future is already here — just unevenly distributed.

This is not about scaring you or giving anyone else an I-told-you-so opportunity down the road. It is about a trenchant look at what is just now real and what it will mean to be an early adopter versus a laggard.

## SOLUTION SPACES

There is little doubt that the electronic exchange of information is a permanent feature in business. But just the same, extending the electronic franchise to all comers ensures that, on the Internet, every sociopath is your next door neighbor. This is not news, and it certainly never was good news, but a fact is a fact. The wonderful advantages of information technology and universal connectivity are tempered with some disadvantages.

*The problem statement from this time forward is this: To protect individual objects of value individually. More precisely: Contract the protection perimeter to individual data objects.*

## The Problem Statement

To get a good result the engineer, the financial planner, and the corporate visionary all have the same core focus: To get the problem statement right. The wrong problem statement gets us “solutions in search of a problem” or “we solved the wrong problem” or “these sunk investments did not yield value.” In every case, it is getting the problem statement right that makes the difference.

The problem statement from this time forward is this: To protect individual objects of value individually. More precisely: Contract the protection perimeter to individual data objects.

In a perfect world, such a statement would be obvious when well said. We don't believe we are yet masterful enough to have one sentence say it all. So to make sure that we are being clear, here is how we've come to that problem statement and why we think it has steering power.

## Limits to Technology

The best security technology has exactly two characteristics: **Inescapable** and **Invisible**. This is simply to say that it cannot be evaded and that it is never significantly underfoot. These are real limits – never perfectly achieved – but they are the objective, the goal state, just the same.

In the political marketplace of regulation and liability, security technology is mostly called upon to prove a negative, to prove that such-and-such cannot happen (“No one can get a weapon on any flight ever”.) Students of science know that proving a negative is impossible. Students of economics know that proving a negative is wildly diseconomic.

Why do scientists and economists know this? Because to prove a negative you must be able to enumerate all of the alternatives and eliminate them. Why does that matter here? Because this is almost never doable. But, for once, we are in a position to prove a negative because we are in a position to do the enumeration that matters. Read on.

## Re-Focusing on Object-Level Protections

In computing, information tends to be organized into individual files. Perhaps that will change, but not soon – the file system abstraction is pervasive and already reduced to hardware. Accept it as a given for the moment.

If we can get protections to the level of an individual file, then we will have something of real value to the corporation. But before you say, “Sold!,” consider for a moment how hard that is.

A file containing a document is downloaded from a corporate server to a desktop, emailed as an attachment to a different computer where it is then copied to a removable device, carried to yet another computer where the document is opened and a portion of it is transferred via cut & paste to a new document that is then written onto a CD-ROM that is subsequently carried out of the building inside a book jacket.

The solution to this scenario is now available and, as you may already guess, that solution tracks individual file-level objects through their lifecycle. That solution is very nearly inescapable and it is as invisible as you need it to be.

*You can get a lot of security out of just paying attention to what you can see and measure.*

## Why Now is the Time for Object-Level Protections

The general solution to security design problems has always had two parts: (1) Trust the people you have to trust, but (2) make sure that they are who they say they are. Until now that was good enough. It is not good enough any more.

Proving who you are is technically called “authentication.” You have used authentication every time you have given a username and a password or plugged in a smartcard. Authentication proves who you are, and in most systems there follows some sort of one-for-one match between who you are and what you are allowed to do. The combination of authentication (who you are) and authorization (what you can do) is generally referred to as “access control” and it underlies nearly every security design widely in place today.

But it is time to face facts: For a lot of reasons access control can no longer meet either the security challenge or the economic challenge. Unless, of course, you have nothing of value (in which case we apologize for wasting your reading time).

Access control does not scale up indefinitely. When you consider the access control model, you have what amounts to a matrix: One row for each person (or thing) that can ask for access to a system resource; one column for each system resource that these people can ask for. The number of boxes in this matrix is the product of the number of people and the number of resources. If you double the size of the company, then you double the number of people and the number of resources. This quadruples the number of boxes. If there is a fixed minimum cost to maintaining a check in each box, then the cost of maintaining the matrix grows faster than linear with company growth. Any cost that scales faster than linear is in and of itself a barrier to growth. Security cannot be a barrier to growth, or people will inevitably work around it.

A similar argument applies if you are busy making your company more secure by subdividing rows and columns into “finer grained access control,” and that is without growing the corporation at all. Pushing access control too far ensures that the result is diseconomic, the only question is when.

The alternative to pushing access control farther than it should be pushed is to turn your security problem statements towards accountability. Like in a free society, there is huge efficiency in not having to ask permission for every niggling little thing – but if and only if there is a high probability that if you misuse your freedom you will then lose your freedom. That is what accountability is. Accountability at the object level is where security goes next, and it goes there whether you come along or not.

## DELIVERING OBJECT-LEVEL PROTECTIONS

The 1990s were a decade in which the commercial sector caught up with the military sector in cryptography. Crypto is now everywhere, cheap, and unremarkable. In this decade, the same thing will happen to what military folks call “traffic analysis” which is just to say that you can get a lot of security out of just paying attention to what you can see and measure.

A user downloads a file containing a document from a corporate server to a desktop. Record that. The user then emails that document as an attachment to a different computer. Record that. At that different computer, it is copied to a removable device. Record that.

The removable device is removed and carried to yet another computer. Record that. The document is then opened and a portion of it is transferred via cut & paste to a new document. Record that. The new document is then written onto a CD-ROM. Record that.

How, you may ask, can you do that? Simple. And if it weren't simple it wouldn't work. With less footprint than antivirus, such transactions with the file system are intercepted and recorded. The records are periodically compressed, made tamperproof, and shipped to a central archive. Analysis software can run right away, if you are protecting actively, or the records can just be saved against a rainy day. The point is: Get the data. If you don't get it while it's fresh, you won't get it. "The dog ate my homework" works at most once.

### ALL ABOARD

Because file-level tracking is now possible, many other things are now possible, too. This is a technology that has legs. It is valuable now, and it is valuable later. It won't be long before "Why are you doing this?" is replaced with "Why aren't you doing this?"

First, because this is possible, persons with fiduciary responsibilities in companies with sensitive and/or proprietary file-level data assets will soon be asked not just "What did you know, and when did you know it?" but rather "What didn't you know, and why didn't you know it?"

Accountability flows uphill. This is not to frighten anyone, but it is a fact. The future is already here, just unevenly distributed.

Second, because you know when a file is being manipulated, you can supervise it: "John, you are welcome to mail that proposal to that other address, but note that we will know you did. Click here to proceed." Keeping honest people honest is often about nothing more than delivering them from temptation.

You can even interfere: "It is against corporate policy to mail modifiable documents to non-internal addresses." As always, some people will try to get around this. Perhaps they actually do have the evil genius to succeed, but it won't be automatic and they will leave tracks.

### Trust, But Verify

"Trust, but verify," Ronald Reagan's famous words, take on new meaning, a deeper meaning. Risk is a growing component of all electronic business interactions, and not just the counterparties in some transaction or other. You want to entrust your data to, say, an outsourced call center? Perhaps you'd like to know that no one can take a copy of any of those files. Perhaps you'd like to contractually require this file-level monitoring. Perhaps your outsourced call center will self-impose such a requirement because people like you will prefer to buy from call centers where files can't go for a walk on their own.

You're a law firm, and you're running a merger. You'd like to be sure that nothing leaves the merger room, but it is hard to even know what that means these days when cell phones automatically synchronize to laptops that coincidentally spray wireless everywhere, and so forth. Perhaps file-level interdiction of offboard copying operations would let your staff use the Internet, client-directed email, and so forth while in the merger room, but without the risk that you can't otherwise bear.

*Accountability flows uphill. This is not to frighten anyone, but it is a fact. The future is already here, just unevenly distributed.*

You are sick of buying storage, storage, and more storage for the G&A side of the house. Perhaps you'd like to know that you are storing no less than 4,238 copies of the same 37 page PDF. And it's obsolete. Or perhaps you'd just like to know something simple like how many files are written but never read.

You bought insurance, but is it worth anything? Your business insurance exempts acts of war, but governments are calling virus writers "terrorists." Does that not make their attacks on you a subset of acts of war? Worse, your D&O insurance has a clause that voids it if you "fail to maintain adequate insurance" and your property insurer won't sell you the terrorism rider except at a substantial premium. Are you failing to maintain adequate insurance if you don't buy the terrorism rider? Is a technical solution to the loss of corporate data a form of insurance? Do you want to be the test case once the availability of that technical solution is widely known to exist?

There's a last minute change to a corporate decision, say a succession plan in document form, and you discover that someone left Track Changes on in the most horribly embarrassing way. Perhaps you'd like to be able to say "Who has the last version; we have to replace them all now."

Conversely, you realize that you just deleted everything for Customer One. Sure, IT can get it back overnight, but perhaps you'd like to know that the same versions of the files you lost are sitting on Sally's desktop even though she's out sick and you can't reach her.

A subpoena arrives. Besides the groans, perhaps you'd like to be able to flip one switch and make it impossible for the Sales Department to delete any files until you say "All Clear", if ever.

You have a suspicion that someone in Engineering is using Instant Messenger to move drawings embedded in innocuous photos. Perhaps you'd like to be able to know when the contents of drawing files are moving to a clipboard and thence to Photoshop. Perhaps you'd like to know this silently, remotely, and with evidentiary rigor.

You've spent way too much money on the sum of firewalls, antivirus, intrusion detection, and patch management. You worry that each of them requires diligence, perfection, and even then there is always a chance that a laptop coming back from vacation brings a new worm right in the door. Perhaps you'd like to know that even if there is a takeover of this or that machine – even then there won't be any data leaving the premises. Perhaps you'd like to say that you've already spent your last dollar on those other technologies and/or that they won't get any more underfoot than they already are.

You're being acquired. Obviously, there will never be as high a percentage of angry staff as there are today. Perhaps you'd like to let the outplacement people set up shop on the company intranet, but with zero likelihood that, besides sending out resumes, your marketing plans are going with them.

You already lost a file. There is no denying that, but it could have been from here or it could be from your partner in that joint venture. Perhaps you'd like to have some forensic evidence that was already in the can, already collected as a matter of due care, that doesn't require ex-spooks at \$4,000/day to conjure up. Worse, perhaps your partner does have that sort of evidence because they are doing what you should already have been doing.

Describing this is a fun game, played here. None of it is fun, played there. Now that you can track files, keep honest people honest, and block file moves that would damage you, wouldn't you rather do so? Wouldn't you rather not have to explain why you didn't take the one precaution that complements every other precaution you already have? Wouldn't you rather prevent what you can't clean up?

### WHAT NEXT?

That's up to you. Perhaps the best advice is to just use this technology to take some notes for a while. Learn what "normal" is for your firm; be ready to notice an outlier, an anomaly, that something odd that excites the latent Sherlock Holmes in you. If something wrong is going on, the evidence will be here. Better still, if this technology is running everywhere, you will actually be able to do the thing you can almost never do: Prove a negative. Imagine the advantage in that.

**Bottom line: What you don't know is already hurting you.**

### ABOUT VERDASYS

Verdasys is dedicated to providing a new class of information security and management solutions focused on the largely uncountered threat from authorized internal users. Our founding was inspired by first hand experience with insider information theft and misuse and the severe lack of visibility and control available today to assist in the detection and prevention of such events.

#### Verdasys, Inc.

950 WINTER STREET  
SUITE 2600  
WALTHAM, MA 02451  
781-788-8180 TEL  
781-788-8188 FAX  
INFO@VERDASYS.COM  
WWW.VERDASYS.COM