2007-03
Sensible Security – You Wouldn't?

Introduction:

When someone who knows little about information protection interacts with a professional, the language and rational behind things is unclear. One of the tricks I use when discussing security issues with folks who tell me that they don't want gold-plated security, only something sensible is to put things to them backwards.

Which thing do you not want to do?

I use extensive lists and pictures with extensive numbers of elements to get at the security issues when I deal with clients. And as I go through the discussions about one issue or another, they sometimes start to think that some of the things I am asking about and the things I expect a sound program to have are excessive.

I am not dogmatic about security, I am a pragmatist. If a standard says you need to have change control and you explain why it is just not relevant or possible for a particular situation, I will be as quick as anyone you will find to say that you are making business sense, assuming you are. But in most cases, it's not that way. If you have a system in which protection-related failures can put you out of business, you need to have adequate protection, even though it may seem like the list is a bit long, you need to do what has to be done to make it safe or have someone who is authorized to do so decide to risk going out of business because they don't think the effort is worth the benefit.

All of this is another way of saying that someone in a position of authority needs to decide what not to do.

Where don't you want to go today?

Here's what the audit dance looks like:

- The auditor asks if you do each security-related thing that is part of some standard.
- You say or they asses that you only do three.
- They give you poor marks in that area.
- You complain that this is excessive and tell them to give you better marks because you don't need to do all these things to “be secure”.
- They go through each one and ask you to sign a document on behalf of the company that makes the determination that you understand the risk of not doing each thing, that you have decided to accept the risk for whatever time period.

You pass... sort of.

But who is authorized to accept the risk?

Of course it doesn't really work that way. That's just the formality of the dance. If you have any sense at all you will know that unless you are the CEO you are not authorized to accept all those risks and if you are the CEO there is no way you will sign that piece of paper. Still, you can't afford to fail the audit either.

If you read the words of the standard and think about it, you would look pretty silly signing a piece of paper that says you will accept the risk of enterprise failure by not using hard-to-guess passwords. But on the other hand, it may not be that easy to get your executives to memorize a new 12-symbol password for entering their office every week if they can't write it down. Not to worry, they will hire someone to open the door for them.

There is a trick to success. Or rather, there are a lot of tricks to success. The trick is to use a lot of tricks. Don't do something excessive if you can find something easier and as good. Instead of a 12-symbol password that changes weekly, try a key, a guard, a biometric, keyboard patterns, computer mantras, or any other option that meets the need without creating the burden.

Security is not for simpletons. It involves a lot of creative thought. And this is something that a lot of people don't get. To make good security decisions, you need common sense, which is not that common. Implementation has to be pretty simple to use or it won't work. Someone once said that the military is a system created by geniuses to be implemented by idiots. It's harder to make something complex seem simple than to make something simple seem complex. And that is the job of the security leader in an organization.

Conclusions:

Which brings me back to what you don't want to do about security:

1. You don't want to not do things that seem to make sense. You need to find sensible ways to do them.
2. You don't want to sign pieces of paper that indicate you won't secure important things, so find ways to secure them or get the pieces of paper signed by someone higher up the food chain.
3. If you are at the top of the food chain, see step 1. And if you don't have the time to be a creative, thoughtful, innovative security person, hire one and give them what they need to do the job.

Sound security is always sensible, but it only makes sense when you make sense of it. Think about it!

Fraud of the month

Every month, we take an example from "*Frauds Spies and Lies and How to Defeat Them*" and describe a recent example. From page 24, section 2.3.7.1 we present the age-old and oft-repeated:

"Paper firm"

> *"A fictitious company is created to defraud another company. These days you can create a company for a few hundred dollars from over the Internet and build up a Web site for next to nothing to make it all look legitimate."*

Section 6.1.4.7 (page 176), "Fake Companies" has several counters to paper firms. It starts by telling us:

> *"Any company that your business is doing business with should be checked out before you start working together. How long have they been in business? How does their credit check out? Who runs the company and what is their history?..."*

If they are offended by being checked out, be very concerned. I tell my clients and perspective clients to feel free to check me out. I have much of my history posted on my Web site including plenty of things they can independently verify.

Of course when you are looking for a security consultant, you probably have to be extra careful. After all, you are placing a lot of trust in them. But even when you are looking for a supplier for paper goods, there are plenty of ways to get scammed.

Chet's Corner

Cornered again!!! As we march forth toward tax day I am reminded of the ancient saying. Never put off till tomorrow what you can do today. Tomorrow may never come. Security usually makes sense when properly applied, checking the backgrounds of the people you deal is inexpensive and easy to do, and figuring out which business records to keep for how long and when and how to destroy them isn't that hard to do. The thing that's really hard to do is to get the people in middle management to tell the truth to the top executives.

"Always look on the bright side of life"!

Service Summary

Every month we feature one of our services and give an example of how it benefited one of our clients. This month it's a review of record retention and disposition.

Record retention and disposition sounds like the most boring topic of all time. It's close. It is all about following a huge array of laws and regulations, while simultaneously doing what makes sound business sense. It is not about getting rid of as much evidence as possible as soon as possible.

The challenges many of our clients face come from two distinct sources:

1. They are hard pressed to keep up with all laws in all relevant jurisdictions, and
2. They are unable to do the risk management activities required to make good decisions.

We can't make risk management decisions for clients because we don't suffer from their losses or gain from their wins in proportion. We can help create and operate risk assessment process to provide uniform and reasoned approaches to understanding business consequences and, when warranted, threats and vulnerabilities. We also customize automated data collection and analysis systems for their use and help sustain process while they build capabilities.

The legal challenge is simply a matter of experienced lawyers and experts spending enough time and effort chasing down the laws and changes all the time. It's complex, it's hard to manage, but what can you do? Break the law?

Mollie gets the last word in

Easter is coming and I can tell that the bunny in all of us is hopping out to find the chocolate. Rewards for making it through the winter. Last month I almost got scammed. Somebody asked me to help them with their broken down car and it wasn't long before the trail got too tricky to make sense. I brought few friends along on the short road trip and saved myself a lot of hassle. Friends don't let friends get scammed.