2008-01
Accidental Security

Introduction:

While most security education and training surrounds defeating intentional malicious attackers, many of the losses and much of the liability for those losses surrounds errors and omissions rather than malicious acts. Security against unintentional acts is quite different, and well worth considering.

Doesn't good security cover that?

The question of what constitutes good security aside, any security program that protects against malicious acts of insiders and outsiders is likely to be effective at dealing with accidents. But that doesn't mean that accidents won't happen, and perhaps, just perhaps, it is a bit overboard and unnecessarily expensive to try to protect everything on the assumption of intentional malicious threats.

At a minimum, due diligence would seem to suggest that accidents should be understood and protected against, and at the end of the day, there is never a way to provide perfect protection against all malicious acts or accidents anyway. A sound approach should protect against most common accidents, and liability laws suggest that we should spend as much protecting against them as the harm we can identify from them.

Insurance against errors and omissions and the resulting accidents is often attainable. That means that we can transfer accidental risks in most cases, and that provides a basis for identifying annualized loss expectancy and mitigation alternatives that are financially justified.

So I guess the answer is that even though “good” security likely covers unintentional acts, “great” security should be able to identify what those are and provide for different standards of care from identifiable accidents as opposed to malicious acts.

How do we identify all of the accidents

Of course there is no hope of identifying all of the possible accidents. But unlike malicious acts, unintentional acts are relatively easy to characterize because they follow normal human and natural behavioral patterns.

In malicious acts we need to worry about all of the event sequences that can be planned by groups of actors with intent do do harm. But for accidental acts, we can reasonably use probability and analysis of coincidence and historical events to limit the number of events and the lengths of event sequences at issue. This means that instead of exponential growth in the number of event sequences with the depth of consideration, the total number of concerns is finite and not all that hard to find.

How hard is it to protect from accidents?

It is not in any way trivial to identify all of the accidents that can happen involving information protection. But it is also nowhere near as hard as it is when we add in malice.

Consider, for example, loss of integrity of content. For malicious acts, we need to worry about a wide range of things that can be done, from intentional subversion of software to computer viruses to frauds, and so forth. But for accidents, almost all of the common errors are largely eliminated by redundancy in data entry, reasonable care and testing in the development of software, the hardware mechanisms that assure that computers work in the first place, and some fairly easy to implement output checks and overall processes checks and you are most of the way there.

Add in backups and facility and people redundancy, and you can get some pretty good availability protection as well. Use control and confidentiality are also quite easy to attain with a bit of training, some screen covers, marking, and training. Accountability simply means keeping audit trails and embedding them throughout processes.

All of this is well understood and fairly standard to get done. And while this is not an exhaustive list, if you start with a set of standards like ISO 27001 and 27002, you can eliminate the things that deal exclusively with intent and get a pretty good set of things to do that will work against almost any accident you can come up with.

What's my point here?

My purpose in pointing this out is to identify something that should be obvious, but apparently is not. In the effort to attain “security”, we often get caught up in the obscure and complex world of malicious actors working in the dark for years to defeat complex protective systems designed for the rarest of cases. Yet all you have to do i read the papers and you can see that we still manage to have accidental failures that make us look like fools and cause substantial harm.

Part of the reason for these rather spectacular failures is a lack of attention to the basics of sound system design with attention to history, statistics, and basic principles. As we rush toward security products that do enormous numbers of things for huge and increasingly complex internal infrastructures, we seem to be losing track of the basics.

Conclusions:

If we focussed on the accidents instead of the malicious acts, we might find that we could get a lot more done with a lot less resistance and, along the way, make some real progress in balancing protection and gaining support for defense against malicious acts.

Accident of the month

Every month, we take an example from "*Frauds Spies and Lies and How to Defeat Them*" and describe a recent example. But this month, since we are looking at accidents, we'll look at an accident as the example:

"Over consolidation: should have known better!

> One of our clients came to near disaster when a mainframe outage put them 80% out of business for two days. As they stated to lose critical customers they managed to get back online.

At some point later, we did an assessment and identified that they had over consolidated their data centers. The consequence we identified was near total business collapse resulting in loss of most shareholder value. The evidence we had to support it was their recent buy-out of a major competitor who suffered business collapse due to a similar computer outage, not involving a mainframe.

Once we understood about the previous incident, it became clear that the CIO who had failed to consider the consequences of excessive consolidation had accepted far more risk than would normally be allowed. Since that same CIO had not informed top management of this acceptance of risk, of the need to mitigate the situation within a short time frame, or of the cost of the mitigation, which exceeded the 5-year savings of the consolidation and was therefore not done, top management felt an obligation to correct the situation permanently.

The accepted solutions we identified included paying the cost of adding back the necessary redundancy, doing analysis in the future so as to identify other similar circumstances and prevent them from recurring, and the movement of the CISO position out from under the CIO so that clarity could reach top management without being blocked by the CIO. Top management augmented out suggested solution what a cast change, which is likely one of many reasons we won't be working for that CIO at their next job, assuming they ever get one.

This is something we have seen a lot of lately. Accidents happen, and when they are not considered in advance, they can sometimes result in extreme consequences. Perhaps it would be wise to have your exposures to accidents reviewed as well?

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 is our back-end services.

> *We have largely abandoned sales as a way to generate business, in favor of servicing folks who ask us for help based on references or reputation, and providing our services through others under their names. When others resell our service, we call it "back end" service.*

For some time we have been reselling services through others, and recently, we have moved almost entirely to this approach. As a result, we help out clients by helping their clients.

> *In one recent case, a company we have had a relationship with for many years ended up in need of a short turn-around highly confidential review of a very sensitive situation at one of their clients' sites.*

We obviously can't go into any details, but by the nature of the work we had to do in this matter, we ended up doing a write-up specifically designed so that anyone reading it without the context of the situation could not understand what it was about, while anyone who was aware of the circumstance could clearly understand it and apply it immediately.

It was one of our finest pieces of work. You could publish it on the front page of the New York Times, and it would be viewed as a dire situation handled in a complex but clearly workable way, and yet the nature of the situation would remain unfathomable.

Our client's client was happy with the result, and our client was able to serve their client well, so they were happy too. And that's what a good back-end service should set as its goal.

Mollie gets the last word in

I'm back from vacation now, and I cannot tell you how happy it makes me feel to visit my family – for a short time – and then get back to my place.

Speaking of accidental losses, when my mom drove me back (I was not fully recovered from a recent operation and could not yet drive), she accidentally left her cell phone in my car. Before I mailed it back to her... but that's a story for another day... when there's more space available. Cell phones – they are accidents waiting to happen.