2006-10
Physical / Logical Convergence?

Introduction:

Many have asserted that a convergence between physical and information security is underway, and clearly there is a case to be made for some level of convergence. But how closely will they converge and how closely should they converge?

What is this convergence thing all about?

A few simple examples serve to point out the potential for convergence of physical and information security:

> **Scenario 1:** At a remote facility an attacker enters, logs in as a legitimate user, and gains access to the internal network.
> **Scenario 2:** At a warehouse, a stranger walks in, loads a palate of valuable goods onto the back of a truck, and drives away with it.

We have done both of these in protection assessments, and they were relatively easy to accomplish. But if convergence between physical and information security are used, both can be blocked:

> **Scenario 1:** When the attacker tries to log in, the fact that no physical entry was detected for the user logging in brings a guard and the attacker is caught..
> **Scenario 2:** When the stranger tries to load the palate, the RFID tags are detected and since no authorized shipment was allotted to them a guard shows up to catch the driver.

If this sounds good to you, there are two things I should note. The first is that neither of these things should happen in the first place. A good security program would prevent either from occurring - and yet they happen all of the time today. The second thing is that since these things do happen today, a technology solution like this may be inexpensive and effective, so why not take it?

Why take it?

That was a pretty big if there – inexpensive and effective. Let's take a deeper look. The inexpensive part comes if and when the systems that provide for inventory control, personnel authorizations, and integration between those systems are on-line on the same network, able to communicate, and integrated. The effective part comes when they provide as good or better protection than what can be similarly achieved with other means at a lower price. If:

- You already have a strong inventory control system in place and RFID tagging AND
- You have RFID sensors at key locations, AND
- Your workers are required to badge in at all locations AND
- This is already integrated into the personnel systems, AND
- The order entry and processing system and inventory control systems are integrated AND
- You have a guard system in place that can adequately respond to incidents

Then the integration effort is achievable in a few months of project effort. At that point, you only have to eliminate the many false positives associated with gaps between IT and physical systems and the many false negatives associated with the RFID technology and other detection mechanisms, and you have a workable system. But this is not the end of the issues you will face.

All your eggs in one basket

Risk aggregation is one of the key things that has to be considered in any security program, and when physical and information security are merged in this way, once independent systems may become closely integrated and therefore highly interdependent. Here are some scenarios to consider:

> **Network outage:** A network outage that disables the link back to central databases results in failsafe behaviors that either stop business or allow undetected attacks.
> **Corruption of a database:** A corrupted database in any of the systems prevents work from being done on all of the intertwined systems and produces large volumes of false alarms and missed alarms.
> **An insider is involved:** Insiders historically cause the largest losses. An insider that can attack this system can legitimize physical and logical access all at once, producing still larger single losses.

Conclusions:

As these examples show, there remain serious concerns, and we have not even started to exhaust the possibilities. The complexity of the converged system, its costs, and its limitations, along with the aggregation of risks may make it not yet ready for prime time today. But convergence is not to be ignored or put down. It's just not quite there yet.

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 51, section 2.6.2.3 we present:

"Phony job interviews (employer)"

> *"In places where jobs are hard to find, fake job listings are created to generate interviews where the interviewer collects information on the potential employee like name, social security number, date of birth, and so forth - all of the information required for identity theft."*

Most of these forgers don't even have to go to the interview phase. A simple on-line resume collection service will get a lot of information on a lot of folks. Physical mail follow-up or even email follow-up is often adequate to get the rest of the information you need. They might try something like this:

> *Bank references are required for new employees these days – it's part of the government's anti-terror efforts in select industries like ours.*

Worker awareness programs are all find and good to defeat these frauds, but most of those being defrauded are looking for jobs and may not be amenable to the awareness messages of their current or former employer.

Chet's Corner

When election time grows near, we all shudder at the extent to which politicians of all sides are willing to lie or pander to our fears to get votes. They lie, cheat, steal, give jobs to friends, create pork, redistrict to make elections easier, and spend money like there is no tomorrow. Maybe they know something we don't know about the future...

But the good part is that we don't need revolutions and civil wars in order to change things. All we need to do is vote. Just do it in November!

"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 risk management:

Risk management is one of the least well understood issues for decision makers in most enterprises. It is hard for most folks to translate from the lofty notion of risk into day-to-day decisions. Not all risk is to be avoided. Risks must be taken to make gains, mitigated to limit consequences, and transferred when costs are not too high for the benefits. Our risk management practice helps clients make better decisions by:

- Modeling business processes,
- Relating business process failures to their consequences,
- Relating technology and human failures to process failures,
- Analyzing options for risk acceptance, transfer, avoidance and mitigation, and
- Presenting understandable decisions to the decision-makers

The basis for understanding risk in a business context are presented to the enterprise's authorized risk managers along with options, costs, and effects, so they can make informed decisions about risks.

> One of our clients needed help building a risk management program from scratch, so we were brought in. We did an initial workshop and review and helped them create a risk management office that was independent of operational groups. We helped them do initial risk assessments while building a framework and training risk assessment teams. Then we transitioned the function over to their teams.

Most enterprises want help doing risk management in a structure that makes better business sense, and we help them achieve it.

Mollie gets the last word in

Most students and recent graduates don't vote where they live. Help make the world a better place. Get your absentee ballot in now, before time runs out.

Specializing in Information Protection Since 1977