Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Risk aggregation – again and again and again...

As I look back on the last year of big-time information security challenges, it is hard to miss the failure of managers to deal with the issues of risk aggregation. From the Wikileaks case to the economic woes of the World, it seems like people in charge just don't get it and refuse to learn. Perhaps it's generational - a natural side effect of the information age. But we will see.

What is this risk aggregation thing all about?

A few years ago, when the DoD was announcing and touting its consolidation of all identity management infrastructure into a small set of redundant trusted servers, I asked the person in charge, in a public forum, about what analysis they had undertaken to deal with the risk aggregation from unification of all access to computers through a single centralized standard badge system. The direct response was essentially a non-sequitur indicating in essence that it had not been considered, at least at the top management level, and that the top manager didn't have a clue about what it even meant. The more spectacular response was during the subsequent break when some others in the room started questioning who I was, who I thought I was, why I was there, what I thought I knew, and so forth. They told me that since the centralized system was an EAL-4 trusted computer, it was perfectly safe, and (in essence) that I shouldn't screw up their gravy train by putting doubt into the minds of decision-makers.

A few years ago, I was working on a security review for a government entity, when we encountered a decision to consolidate all data centers government-wide into one data center so as to gain efficiency. Naturally, the data center was already being built and was put on the first floor of a facility in a flood plane just off the end of an airport runway with only one source of electrical power. In the assessment, the wisdom of this idea was questioned, and my team was told that there was a lot of business to be had with this government if we could just refrain from rocking the boat and go along to get along. Naturally, we quoted the exact words (not the ones I just gave) in our report, which did not enamor the folks who said them to us. I think the folks were eventually fined, and there was some $50M fraud also discovered in the process, but you can't make an omelet without breaking a few eggs.

A few years ago, I was doing a security review for a large enterprise, and we encountered a potentially serious negative consequence associated with an outage. It seems that the CIO had decided to save money by consolidation and, in the process, managed to get the multi-billion dollar enterprise into a situation where a single outage could, according to their own top-level assessments and historical data from competitors, put them immediately and permanently out of business within 48-72 hours. When I had the late night discussion with the CIO, I was told that the network director said they were using “best practice” and that this assessment would cause serious changes. I explained that the network director didn't know what he was talking about and that serious changes were necessary as indicated by the first bullet in the executive summary (spend $10M to fix it before you go out of business). The CIO resigned, the changes were made over the next 90 days, and they are still in business.

What do the stories have in common?

The Wikileaks matter, according to what I can understand from the media, involved a single member of the US military exploiting known weaknesses in a single computer that contained 250,000 or so classified memoranda, copying all of those memoranda to an external device, and sending them to an unauthorized person who posted them to what is claimed to be 100,000 places on the Internet. Assuming all of this is true, does it sound like the same story to you? It does to me. Only this one had the potentially serious negative consequences realized.

The story is a simple one:

- Proposed solution is identified
- Proposal and/or decision-makers ignore risk aggregation
- Solution is adopted and risk aggregated

Eventually, all of these stories are destined to end badly. Here are the possible outcomes:

- Nothing bad happens and the same mistakes get repeated elsewhere resulting in...
- Someone identifies the problem and instead of costing twice as much over the lifecycle to do it right in the first place, it costs 20 times as much but gets fixed... OR
- The potential for serious negative consequences are partially realized, and in addition to the factor of 20 lifecycle cost from fixing it, there are also substantial incident-related costs and consequences... OR
- The potentially serious negative consequences are fully realized, and really bad things happen, and if the entity continues to exist, it suffers even more incident-related costs, and the factor of 20 lifecycle costs from fixing it.

But we learn from our mistakes... don't we? It seems so simple now, but who could have possibly known?

What does history teach us?

If history teaches us anything, it is that, left on their own, people will (1) screw up the same way again and again, (2) remain ignorant of history, (3) forget about what history they do know, (4) rationalize that they know more, are better, or that times have changed, (5) ignore sound advice from others, (6) decide to take risks with other peoples' money, (7) claim that things are not as bad as they could have been, and (8) blame others for what happened.

Any serious solution to the risk aggregation problem will have to deal with these issues, and the only thing that I am aware of that has ever worked against such human forces has been the combination of professionalization and regulation.

> **Professionalization** means that those in information protection need to stop playing things by ear, stop giving into management foolishness and ignorance, and start doing their jobs seriously and fearlessly. Like the medical profession, standards of practice must be developed, and those standards must insist that risk aggregation be taken into account. Like the engineering profession, licensed professionals should not be willing to ignore standards or present designs absent appropriate standard calculations.

Regulation means that decision-makers responsible for systems that hold content of or about others or that has a substantial negative consequence of protection failure must be legally mandated to use qualified and licensed professionals and must follow that advice when the standards mandate it. Just as there are permits for buildings, there should be permits for databases, and those permits should be reviewed by trained professionals who follow standards.

Why are we over-aggregating risks?

Ignorance is not bliss, but it appears to be ever present in management when it comes to information protection. I don't believe that top executives want to create such problems, or that they would knowingly allow them to persist if they understood their implications. However, applying some personal implications such as those of Sarbanes Oxley do seem to force the issue and cause executive attention to be differently focussed.

I think that if the DoD top-level decision-maker would have had sound advice and a defined standard of care, he would have not allowed the level of aggregated risk that was allowed and still persists today. I think that the governor of the government described above would not have allowed the over consolidation is they knew what it meant. I think that the CIO who exchanged cost for availability would have made a different decision if they understood what was going on. And I think that the folks who apparently had 250,000 classified documents all accessible to a superuser who could remotely access the system and load the contents for export knew that was the case, they would have disaggregated that risk. But I am an optimist.

I am far more certain that if a standard of care was applied that required that risks not be aggregated beyond a certain level in a single system, method, location, facility, mechanism, or individual, regardless of what countermeasures or mitigation was thought to be in place, that it would have been far harder for these situations to ever have existed.

I also think that if that standard of care was such that no licensed professional would violate it without risk to their career, such that a zoning board had to define the standard and database inspector had to review for the standard and approve before the database could be built, used, or changed, and such that everybody working with those sorts of systems knew that this was mandated and violations were treated as criminal negligence, that these situations would occur far less frequently, and we would have case studies of 25 year jail terms and permanent debarment to help point out to decision-makers that they can't play fast and loose with these issues.

Conclusions

Why are we over-aggregating risks? There are lots of reasons. There is no way for competent professionals to wield leverage against management. There is no standard of care. There is no real legal mandate to deal with risk aggregation. Mitigation, regardless of how effective, is the ultimate excuse for sloppy architecture and design. Decision-makers can waive anything without apparent consequence. Nobody will stand up with the person who identifies a problem. We don't have a profession with properly defined standards of care. We don't have zoning boards or licensing or inspections according to database building codes. We don't even have assurance that auditors will find the problems, and if they do, there are no fines levied of requirements that the database not be used until fixed. And these are what we need.