

## **Information and Physical Security: Issues in Working Together**

The field of Information Security (by the current definition) is a relatively new one, at most 25-30 years old. Thus, it is not surprising that we are still looking for solutions and doing a lot of “trial and error” in looking for ways to better defend our ever growing stores of electronic data. A look back at any industry – chemical, automotive, banking, retail, etc. would all show that it took many years to develop fine tuned policies and “Best Practices” to finally make the industry efficient.

Yet, there is little question that our current growth of dependence on, and utilization of electronic resources, has little or no previous peer. We now have more information on a laptop computer than all of the stored data and processing power to run the City of New York or State of California only 30 years ago. So, do we have another 10-20 years to “Get it Right”? Even that would be a good record if you look at how long it took for banking, retail, or the automotive industry to “work out the bugs” and become an efficient operating sector.

We might have a shortcut – if we choose to use it. And up to now we are not even close to doing so. That shortcut would be the historical lessons of Physical Security. While there are several variations on this theme, for comparison purposes let’s use the history of warfare and securing the physical assets of the forces and facilities. And with this example we get a long track record to look at.

Centuries ago all warfare was dispersed – think Genghis Khan and the Romans. All assets were unprotected, and very vulnerable to attack and raiding. Armies moved and were flexible, with no central forts or logistics facilities. A lot of armies (and data stores) were destroyed by a simple mistake – they were highly vulnerable. Move forward a few centuries, and supplies and assets were now being stored in Castles (databases?) where protection could be better deployed. This solved many issues, but after time, with catapults and other attack methods this strategy became vulnerable. Then move forward a few hundred more years to the US Civil War (or War between States depending on where you’re from) and we had distributed forces and stores again, but with multiple force types (Army, Navy) to either attack or defend (defense in depth?). And there was more than one way to acquire or resupply arms and supplies (factories, shipping, rail, etc.) Does this sound like the early 1900’s where paper was stored locally in file cabinet’s, then the 1950’s-70’s with centralization in Mainframes, and then the 80-90’s with networks? It should.

Now think of today with physical security. In our armed forces we have C4/I (Command, Control, Communications and Intelligence) all in one spot, under one authority. Or think of the building you might work in – is there a security room? That would probably have video screens to view cameras around the perimeter and inside, panels to see the real time status of doors and gates, radio’s to keep in real time communication with patrols or security check points. Basically the

**Government Technology Solutions, Inc.**

4110 Business Drive, Suite A • Shingle Springs, CA 95682-7230

530.677.1333 • 800.326.5683 • Fax 530.677.1416

[www.gvTechSolutions.com](http://www.gvTechSolutions.com)

same thing and concept as our modern military strategy of C4/I. Why? It works, and we have many centuries of trial and error to see why. If there is an attack or breach is it is seen at one spot, and the resources to defend against the threat are deployed from a central location. And progress and status is monitored from that very same location – no matter what defensive resource is being used.

Now think of how your organization develops and deploys Information Assurance/Information Security. Do you use contractors? Do you have a mandate for outsourcing? Do you break up every segment such as Firewalls, IDS, Web Servers, E-Mail, etc. and then put the products and services out to bid, possibly changing suppliers every few years or so? In other words are your security tools being treated like furniture and PC hardware? What would the logical outcome of that be? Even if you are using the same Firewall but the supplier is different, any past problems, compatibility issues, configuration tricks unique to your organization, etc. leave with that technology supplier. Your backup is the contractor – he or she knows what you did. But you outsource that, so every few years you have a new contractor. The new one and old one are competitors – do you really believe they are going to share all your “inside information” in order to keep a continuity of defense? And, do you also have multiple contractors for various segments of your network? One contractor for the firewall, a different one for the help desk, another one for the e-mail system, etc.? Are they the same company or competitors? If they are competitors do you really believe they are sharing all of their tricks and well earned secrets for securing your network? Sure, your RFP may have stated they would need to. And, you have agency or company representatives overseeing them all. But they are different companies, they are not going to work as one cohesive unit. Is that where your Information Security program is today? Don't worry, you have a lot of company! It is the way we purchase, deploy, and manage computing (and defensive) resources today, with little exception.

Since Y2K the number of outbreaks and serious loss of data has sky rocketed – take any guideline you want to add up the numbers (SANS, CERT, FBI, etc.). And in the same time outsourcing and contracting has also sky rocketed. Is that a coincidence?

I suggest we look at history, and learn from it. If we handled Information Security today the same way we handle physical security I believe the number of serious breaches would plummet. And I believe we could do it with less people, and at a lower cost. There are technologies today like Security Information Management (SIM), Extrusion Detection/Data Loss Prevention, NAC, etc. that do what people did only 3 or 4 years ago. And they do it faster and better. But we are not using them widely. Why? Because the contractors we put in place 3 or 4 years ago need to justify their positions. So the evaluation and decision making authority is not where it needs to be to take into consideration the best interest of the organization or agency. It is self preservation; to expect anything different would be foolish. Throw in unions and local government practices for providing jobs on a local level, and the factors to keep things the way they are become overwhelming.

How-ever – does the current “status quo” work? Did you have more intrusions and network breaches in the last 5 years than the previous 5 years - when you may have deployed or used Mini or Mainframe computers (or more centralized data storage).

If the above makes sense, you have a lot of work to do! Consider categorizing Information Security as a “Core Competency or Resource”. Thus, it is only handled by your company or agency. You have a single team that works as one, and meets regularly to discuss security – not Firewalls or Anti-Virus issues. And you have a single or as close to it as possible partner. They work with your team to provide the tools and solutions to defend you against today's – and

**Government Technology Solutions, Inc.**

4110 Business Drive, Suite A • Shingle Springs, CA 95682-7230

530.677.1333 • 800.326.5683 • Fax 530.677.1416

[www.gvTechSolutions.com](http://www.gvTechSolutions.com)

tomorrows attacks. You are doing this now with Physical Security. Brinks has their own trucks, drivers, radio operators, investigators, etc. And it works. Decentralized security does not – or we would still have an army like the Romans did. Make security an in house issue, and use as few contractors as possible so you can build a cohesive team. And think about whom you choose – does the partner make their money on as many people as they can place, or do they specialize in technology that allows you to scale up the number of human resources you need to make your goals effective? It might mean some drastic changes now – but I suspect if history has it's way, it's where you will be in 20 years anyway. The difference is how much you will loose or save in that time.

**Government Technology Solutions, Inc.**

4110 Business Drive, Suite A • Shingle Springs, CA 95682-7230

530.677.1333 • 800.326.5683 • Fax 530.677.1416

[www.gvTechSolutions.com](http://www.gvTechSolutions.com)