
Technology traps

Nothinz purfick

JOHN GLENN, MBCI
Certified Business Continuity Planner

The other day a fellow wrote from an island in the Atlantic that he needed an alternative to a US\$22,000-a-year/per person license for a biometric security product. What, he asked, was available for a little more reasonable cost?

Seems that when the then-bleeding edge security package was bought and implemented, someone forgot to involve our correspondent, the Business Continuity planner.

Had the enthusiastic purchasers of the product asked our Business Continuity guy, they would have learned - as the Business Continuity planner learned - that if someone was unable to access their assigned machine, the machine was useless. The security provided by the biometric shield prevented access by an alternate responder, the Business Continuity "guarantee" that someone will man the pumps (or whatever the task at hand).

My first reaction was pretty much what I just wrote - a "got'cha" caused by someone's failure to thoroughly do their homework.

Biometric security - it looks good on paper (especially on glossy magazine pages), but there may be some concerns that are "overlooked" by the advertiser.

Candy and pcb breach barrier



Turns out planner on the island doesn't need a US\$20,000-per-year/per person license for a "work around" to the biometric problem.

All he needs is some gummy worms - or bears or Swedish fish or any other similar sweet - a little time and talent, and with one or two other inexpensive ingredients, volia! - the biometric barrier is breached.

All is documented in an article titled "*Gummi bears defeat fingerprint sensors*" at

http://www.theregister.co.uk/2002/05/16/gummi_bears_defeat_fingerprint_sensors/

Biometric security is more than just the ridges and furrows on the surface of the finger, so the total biometric option is not lost with the someone's ability to accurately copy a finger's unique whorl, right loop, left loop, arch, and tented arch patterns.

Voice recognition also falls under the biometric umbrella. Like fingerprinting, voice printing has been around for decades . . . even before Leonard Nemoy signed on as Starship Enterprise's Science Officer, and has been sufficiently proven to be used as evidence in some court cases.

But, like those "unique" fingerprints, it turns out our "uniqueness" also can be accurately copied, at least close enough to fool a machine.

Do the eyes have it then?

In a word, "No." Biometric devices looking for the matching eye have been fooled by a high resolution color laser print of an iris with a hole cut in the center.



Not only is all this information available to "the world," much of it is available in PC World (<http://www.pcworld.com/article/id,103535-page,1/article.html>).

But, as the PC World article - "*Biometric Security Barely Skin-Deep*" - makes clear, there is a flip side to the security snafu - sometimes the technology which allows a miscreant into a classified area keeps authorized users out!

Fast forward to the past

We've all heard of the movie "Back to the Future."

In order to shore up the holes in the biometric sieve a step back to "the old days" may be in order.

The first thing to realize is that there is no single technology or methodology which can protect our environment.

Take a lesson from US embassies and consulates around the world.

For many embassies around the world, the facility is surrounded by a fence. Outside US buildings stand local police. At or near the entrance you'll find an armed US Marine. Behind the Marine you likely will find a two-way voice communications portal (microphone/speaker combination) which connects to a similar setup inside the building. Sitting by that portal is a person who controls the lock on the door behind the Marine behind the local police. Somewhere along the way inside there are other armed Marines and metal detectors and "other stuff."

Is the interior of the embassy absolutely, positively safe from invasion. No.

Is the interior of the embassy sufficiently safe for all day-to-day operations? Yes.

Note that the US embassies use a combination of technology (communications, detectors, etc.) and "manual" means - the armed Marines and clerk at the door release switch - to secure the building's interior.

Business Continuity planners should follow this example and mix technology - biometric security - and old fashioned strong passwords regularly changed.

They also need to assure there is a "backdoor" which allows authorized alternate personnel access to facilities and resources when necessary. Granted, at first blush this may seem to be mutually exclusive.

In most organizations someone is keeper of critical passwords. The keeper, and the keeper's alternate - if there's no alternate, there is a problem - need to be the only people privy to the passwords which are secured in two locations - one on-site and one off-site. Both locations must be secured within a secure facility, preferably at a location requiring another person to provide access.

On-site: The passwords, or master passwords, could be housed in the CFO's safe, the combination of which is known only to the CFO and the CFO's alternate. Off-site, the information needs to be at a secure site similar to the data vault. Such sites typically require a vendor representative to open the facility.

Still, as the headline of this exercise states: "Nothing is perfect." There is no absolute unbreakable seal; the best we can hope to accomplish is to make access so difficult that breaking the combination barrier takes too long and too many resources to make the effort worthwhile.



You don't have to be a certified geek or physical security expert to understand that technology, by itself, is not enough. Technology can provide some excellent tools, but they must be combined with "technology-free" (or "technology-limited") options to bring physical and data security to a level in which we can have confidence.

← Ringdale Access Keypad with Fingerprint and Swipe Card Reader

John Glenn, MBCI, has been helping organizations of all types avoid or mitigate risks to their operations since 1994. Comments about this article, or others at <http://JohnGlennMBCI.com/> may be sent to Planner @ JohnGlennMBCI. com.

© 2006, John Glenn, MBCI