

Firewall-Wizards: Going meta (was RE: [fw-wiz] Ok, so now we have a firewall...)

Going meta (was RE: [fw-wiz] Ok, so now we have a firewall...)

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2005-06/0032.html>

From: Marcus J. Ranum (*mjr_at_ranum.com*)

Date: 06/02/05

To: "Bill McGee (bam)" <bam@cisco.com>, "Mark Tinberg" <mtinberg@securepipe.com>

Date: Thu, 02 Jun 2005 13:36:20 -0400

Bill McGee (bam) wrote:

>This is a classic "perfect world" versus "real world" scenario. I think
>Chris Blask nailed it on the head earlier when he said we have to
>acknowledge (and live with) the limitations of what we have while
>working to build something better. That's a challenge to be taken
>individually AND as a collective.

I must disagree.

As I read your posting, I had to take a couple of deep breaths because it triggered a really strong emotional response in me, and I wasn't sure why. My initial urge was to just hit the afterburner but I realized that you're actually being quite reasonable. But I think your position is reasonable in the context of current security practices – and therein lies the problem. In "Marcus Land" the way 99.999% of the world does computer security is so utterly silly that I simply reject what most practitioners see as the "real world" and "practical security." Perhaps you can imagine how weird it feels; I sometimes wonder if I'm the lone nutcase who still believes that the world is a flat tray that is carried on the back of a giant turtle. Or, perhaps I am the lone nutcase who thinks it's round and all the folks who preach "real world" still think it's flat.

The simple answer is "time will tell" but, like with the flat-versus-round earth controversy, it's important to get people thinking in terms of observable phenomena that might bear out the accuracy or inaccuracy of a particular view. So let's look at some assumptions, shall we??

For the last 15 years we've seen security practitioners trying hard to "be practical" and "facilitate business needs" etc. You've all seen how that plays itself out in the real world – business needs bump up against

Firewall-Wizards: Going meta (was RE: [fw-wiz] Ok, so now we have a firewall...)

security concerns and some kind of compromise occurs. Sometimes the compromise is small, other times it's large – but it's virtually always someplace on the continuum between "less than guaranteed security" and "no security at all." So now's where I point out the paw of the turtle: LOOK AT WHAT IS HAPPENING.

In the last 15 years, the rate at which systems are compromised has consistently increased year after year. Granted, the measurements are not very scientific, but I think we can probably agree on the broad trend:
Security is getting worse.

Now, let's look at another data point: we're spending more money on security all the time. Again, the numbers aren't very scientific but the various research analysts estimate that security expenditures have been outperforming the rest of technology expenditures year after year. Estimates vary between 5% and 9% compounded annual growth in security budget (adjusted for inflation) compared to 2% to 5% overall for information technology. If you don't buy those numbers, do your own research – it wouldn't help for me to post links because if you want to believe I am manipulating numbers then you'd also believe I'd manipulate the choice of links I offered. I hope we can agree on the broad trend:
We have been accelerating security spending.

OK, now, we're spending more and the problem is getting worse. Can we agree that expenditure on security is a measure of "quantity of technology"? I.e.: how much stuff we are throwing at the problem? If so, there are different conclusions we can draw from that:

Option A) There is a relationship between the effectiveness of security technology and its quantity

Option B) There is no relationship between the effectiveness of security technology and its quantity

If 'A' is true, and we're spending more on security and security is getting worse, then we should immediately stop spending money on security and hope it gets better. Right? I don't believe that. Which leads us to option 'B' – what are the implications of option B?

If 'B' is true, then there is some other reason why our security gets worse no matter how much we spend on it. I can't haul us all past this point with pure logic, but maybe if you look closely you can see the shadow of the entire turtle.

Going meta (was RE: [fw-wiz] Ok, so now we have a firewall...)

Firewall–Wizards: Going meta (was RE: [fw–wiz] Ok, so now we have a firewall...)

Some possibilities:

- Some of the products we're buying simply don't work
- Some of the products we're buying aren't being used properly
- There is no correlation between cost and effectiveness of security products
- (some of the above)
- (all of the above)

A few years ago I tried to point out that the same logic applies to security education. We're spending more money and time teaching people about computer security than ever before. The situation is getting worse. Ergo; it's not helping, let's stop wasting the money and search for an alternative. As you can imagine (especially since I made that observation during the keynote of a conference that makes its \$\$ doing security education) that view was not popular.

Anyhow, I've tried to keep this clear and unemotional, and I hope that if you've stuck with me this far you'll see where I'm coming from. I think that the security practitioners who are preaching "real world" are really advertising their willingness to compromise in an area where the results of those compromises are all blindingly clear.

To me, the stellar example remains the whole firewall "debate" of the early 1990's. Let's not beat around the bush: convenience kicked security's ass in 1994 and has been kicking it ever since. Yes, there are lots of perfectly good–sounding "business justifications" for doing it, but today's firewalls let too much stuff back and forth. To me, the fact that organizations with firewalls continue to get brutally hacked is empirical proof of that view. I know a handful of organizations that have very strict firewalls with draconian and unpopular rulesets – and they simply don't get hacked. To me, that's a good argument supporting my view. I can't prove any of this, and there are no studies I can think of that attempt to tie practices to getting hacked, but I bet if there was, there'd be a lot of red faces in the security community.

Basically, what's going on is that a lot of security practitioners are in the position of being asked to make something safe that is fundamentally dangerous. So we hide behind the notion of "risk management" – basically the illusion that "if we try hard to cover our butts it's less dangerous than otherwise." What that has accomplished is to create an environment in

Going meta (was RE: [fw–wiz] Ok, so now we have a firewall...)

Firewall-Wizards: Going meta (was RE: [fw-wiz] Ok, so now we have a firewall...)

which security has NO CHOICE but to compromise because senior execs know that if they don't get the answer they want out of one security practitioner, they can keep asking until they get the answer they want out of another that has been better trained in the art of "security by bending over and gripping your ankles tightly" (the "tight" part of the ankle-gripping is known as "risk management.")

My feeling is that during the 90's we, as an industry, dug ourselves into a hole we're not going to be able to spend or risk manage our way out of. We did that by trying to deal with the "real world" instead of demanding excellence, good design, and wise leadership.

I am totally sympathetic to the plight of the security practitioner who isn't willing to put his job on the line by telling the CTO he's a moron. I completely understand why people feel they need to compromise. But I still think compromise is for sissies.

mjr.

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>