

## [Full-Disclosure] Security Industry Under Scrutiny: Part 3

**Source:** <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2002-12/0117.html>

---

**From:** sockz loves you ([sockz@email.com](mailto:sockz@email.com))

**Date:** 12/06/02

From: [sockz@email.com](mailto:sockz@email.com) (sockz loves you)

Date: Thu, 05 Dec 2002 23:18:58 -0500

----- Original Message -----

From: "Steve W. Manzuik" <[steve@entrenchtech.com](mailto:steve@entrenchtech.com)>

Date: Fri, 6 Dec 2002 10:47:47 +0900

To: <[full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)>

Subject: RE: [Full-Disclosure] Security Industry Under Scrutiny: Part 3

> *This was a really good post, I think you touched on some good points that I  
> would like to comment on.*

woot, thankz steve.

> > *In light of who will access this vuln information we can now  
> > pinpoint a few areas in need of critical improvement. First  
> > of all is the proof of concept code being released into the  
> > wild via the whitehats website. Removing tools from the net  
> > means that you remove the threat of socially inapt morons  
>  
> *The problem with this is that there will always be someone who feels it is  
> their right (free speech and all that jazz) to post what they want on their  
> website and there will always be those who write/post exploit code. How do  
> you propose that this is prevented?**

well mechanisms like this are already in place when it comes to things like national security. freedom of information is limited where that information could pose a threat to international relations, military strategy, secret operations and investigations, etc. i think that if the internet is grown up enough to have laws that make it more capitalist-friendly it should be old enough to be subjected to State-based legislation that prevents the trading of information that could pose a threat to internet security.

of course there will always be those few anarchists out there who do go against this idea, and continue to produce exploit code etc. But if you have controls on the medium for transferring this information, you can at least cut down on the number of toolz sites and stuff. ie, having moderators remove proof of concept code from list postings, national laws that prohibit websites from hosting

hacking content. i mean, its going to be expensive and time consuming for sure, but its gotta be cheaper than creating a second internet right?

- > *Unfortunately history has proven that even your trusted sys-admin could be a script kiddie or malicious.*

tru, but in the cases where it has been proven these ppl are normally put through the courts right?

- > *How to you prevent the code from being distributed? Time bombed binaries?*

i was thinking legislation and heavier moderation would be easier... but its prolly a case of "whatever works, goes"

- > *What about the inept software vendors who \*require\* proof of concept code before they even consider looking at a problem? What about organizations like CERT who has had proof of concept code mysteriously leak?*

the internet has suffered enough at the hands of dodgy businesses. if companies that write software cant get their acts together then by rights they deserve to fall apart. i can speak only for myself, but i'm sure i cant be alone, i think that if i found out the manufacturer of my software was engaging in practices that increased MY security risk of using the product, i would simply cease to pay for it.

- > *What about vendors who will only give patches to companies who "donate" or pay for them? What about the poor one or two man open source project that while they are creating a great free product don't have the first idea on how to fix a specific issue?*

hmm. good questions. i think open source projects still have a chance if their communities focus more on development than bug-finding. ie, if you find a bug you should also work your hardest to find a solution. the reason why i think open-source has a chance here is because community participants are made to feel like they're the developers of the product, and with that ppl start to feel responsibly, loyal, proud of their work. why would you want to see something you worked hard on destroyed? freelance security professionals dont have that same kind of diligence. they seek to find ways to destroy software for profit, and often fame. they feel no responsibility for the products they write toolz for, instead defining themselves as authors of the toolz that destroy the product, as opposed to any kind of open-source developer.

the other reason why i think open-source still has a chance is because it is constantly changing to reflect new additions, ideas, holes, etc. closed source is limited to time-release that is further inhibited by a need to return profit.

- > *I don't think that any system is foolproof. A persistant person could get himself access to the members only stuff and convince people to share code. I don't see how you can effectively police this other than killing full disclosure completely which I don't think is a good option. Yes, full disclosure is flawed but I think it is less flawed than the alternatives.*

i realise this.

what we need is some kind of revolutionary concept.

i'm out of them at the moment.

- > *So you expect mailing list moderators to be the judge of who deserves what?*
- > *How do you ensure that the moderator of the mailing list is acting ethically*
- > *and in good faith? Are you willing to put that trust into the hands of*
- > *mailing list moderators?*

i guess you just have to pick someone with a good track record and have a bit of faith.

- > *So, as a moderator of a mailing list if I receive an advisory that contains*
- > *specific exploit information I should edit that post or retype it without*
- > *explicit information before letting it through? I have a feeling many of*
- > *the contributors to mailing lists would have a big problem with that. What*
- > *makes any moderator qualified to decide what is right and what is wrong?*
- > *Sure, common sense can kick in and play a role but in some cases just a*
- > *general description of a problem is enough to make others look at it and*
- > *find the hole.*

hmm, good point.

- > *As someone who came from an IT background, I liked getting the full details*
- > *so that I could test ways to mitigate the risk, especially if a patch wasn't*
- > *available. My mistrust of vendors at the time also made me test patches. I*
- > *realize that this isn't the norm in the IT world but it was for mine.*

heh, i almost always test patches if i think they could have a critically bad effect. but unfortunately because the internet isn't just for ppl like us who know stuff about computers, some might be but they dont have the same kind of time needed to do all that stuff. i think its the job of responsible netizens (yes i just used that word :P) to cater for these ppl as well. because, whether we like to face up to it or not, they account for the majority here.

- > > *2. We need to place better control measures in the following areas:*
- > > *a) What moderators consider to be "acceptable" advisories*
- > > *b) On whitehat websites that provide proof of concept code*
- > > *c) Lists in general, because they are read by evil*
- > > *ppl and not just good*
- >
- > *I would love to hear some ideas on how we control this. We already do a.) to*
- > *a point at Vulnwatch but I really don't think it is my place to tell a*
- > *contributor how much detail to post or to deny a post just because the person*
- > *did not work with the vendor. Yes, I try to talk to that person and see why*
- > *they choose to do what they do but in the end I still let the advisory*
- > *through. If someone was to post "Here are directions on how to own XYZ*
- > *company" of course that should not make it to the list.*

what would be really interesting would be a roundtable discussion between moderators of major mailing lists, or any smaller ones that work really well.

i think that until we understand the jobs of moderators better this part of the solution will continue to be a problem.

> *So are you saying that all security consultants are bad? While I agree that*

in my bias opinion, yes :P rationally though, maybe not? but i think a 'good' security consultant would be the exception to the kind we see as the majority.

> *there is a large number of them out there that have no business collecting*

> *paychecks for what they do I don't think that they are all bad. Again, it*

> *only takes a few bad apples.*

or in this case a few bad apples who have created bad industry standards.

> *Is it a bad thing as a consultant to help a*

> *client setup a firewall properly, or install and teach them how to use Snort?*

no i dont think so. but thats a bit different from telling people how to hack others. what we're focussing on is the 'disclosure element' of the person's job description.

> *No, I don't think it is as long as you leave your customer in a more secure*

> *state than before and as long as you leave the customer with knowledge I don't*

> *see the problem. You are educating those who need to be educated to protect*

> *their business.*

yeah i agree whole-heartedly that this is good. i think this method is faaaar more effective than just slamming lists full of information and expecting everyone who \*could\* be affected (both now and in the \_future\_) to read it all and understand it all.

> > *A new industry standard for operating business?*

> > *Yes.*

>

> *Great, but this will simply create work for the security consultants out there*

> *to "help clients get to and maintain the new standard." Shit we have already*

> *seen this in the USA with HIPAA and more recently in Canada with Bill C-6.*

> *This will feed the beasts.*

its what the whitehat does that makes them so much of a problem. if we recreate industry standards based on non-disclosure mechanisms surely this would help curb the current destructive activities of the whitehat we know today? right?

> > *Tighter cyber-laws for websites that seem to tell ppl "how to*

> > *hack"? Yes.*

>

> *So how about we license pen-testers and consultants too? Of course I am being*

> *sarcastic here, what would this do to someone or a group of researchers who*

> *create code but keep it for themselves? What happens when that person or*

> *group gets owned and the code is leaked? So the USA passes a law preventing*

> *this kind of information -- we already know the rest of the world won't*

> *follow. There will always be somewhere to put your website of how-to*

## Full-Disclosure: [Full-Disclosure] Security Industry Under Scrutiny: Part 3

- > *information and tools. So what do we do? Own the sites and wipe their*
- > *drives? What gives anyone the right to do this or to judge?*

damn good questions. surely you'd have to have some ideas? i mean we've already seen how little authority internet-based law enforcement agencies have had so far. maybe the question should be "why hasn't it worked so far?" but i dont think i'm the person with enough knowledge to answer that so far.

- > > *Let's start being more responsible with our work. Let's stop*
- > > *rewarding malicious people with ready-to-go exploits. Let's*
- > > *stop educating our enemies.*
- >
- > *But, (and I think you are asking the same question in this post) how do we*
- > *educate those who need to be educated and prevent the enemies from getting*
- > *the information? There will always be bad people with knowledge and power.*

well maybe government initiatives to educate e-businesses in the areas of security (eg rebates or grants, etc). maybe software vendors could extend their user manuals to cover assessment and maintenance. or maybe we might even see this improve over the long-term as the kids in our schools who are already technologically aware (well, in the general sense) eventually start up businesses of their own.

--

---

Sign-up for your own FREE Personalized E-mail at Mail.com  
<http://www.mail.com/?sr=signup>  
One click access to the Top Search Engines  
<http://www.exactsearchbar.com/mailcom>