9th January 2009

So you think you want a job in Computer Security

This is my blatant attempt to re-direct any aspiring, up-and-coming security professionals into another line of work, for the sake of their own physical and mental health.

...

So, you think you want a job in Computer Security, eh? Are you sure? Have you been properly informed what the work and conditions are really like? Do you have visions of Hollywood movies where Cheetos-eating one-handed-typists are madly furying away any would-be "hackers" and think you "want a job like that"? Or have you just heard about large salaries and want to make some extra do-re-mi for another coat of white paint on your picket fence? Or maybe still, you're one of those who think the "enlightened" few computer professionals rise above to the pinnacle of computer security research or applications, and you want a piece of that intellectual satisfaction?

Regardless of *why* you have been considering a job in computer security (or maybe you landed into one and you're wondering *"How did I get here?"* and *"Now what?"*), it is extremely likely you're missing a bit of a reality check you could have used prior to now. Now for a dose in reality ...

1. **Perfect Security is not possible.** It's not. It's depressing, I realize, but it's not. You may be surprised to find so many people working {Computer, Information, Network, System, Application, Software, Data, IT} {Security, Assurance, whatever} jobs who don't get that. I must admit that a former, more naiive version of myself once thought computer security was just getting some complicated recipe of hardware and software components just right. There's still a surprising number of "security professionals" out there who think that way. It's very depressing, but there's a very large "surface" to protect and it only takes a microscopic "chink" in your armor to lose everything. As a result, perfect security being not possible is the foundation to all other reasons why you should seriously re-consider your career aspirations.

2. **Most security work is really about making sure everyone else does their job *"correctly"*.** *Correctness* of systems is the real task at hand in a security job. Is it correct that a website of known sex offenders allows the general public to inject records of anyone they want labeled as such? Is it correct for a web server to execute arbitrary code if it is passed 1024 letter "A" characters? Is it correct that a user can click on a link and divulge intimate secrets to a total stranger because the page looks "normal" ? None of these are "correct" assuming even a smidge of common sense looking on afterwards. Yet they all have happened, and it was some security professional's job to deal with them. To put it simply, if everyone figured out how to design and implement systems "correctly" (assuming they know what is "correct" and what is "incorrect"), then security professionals would be out of a job, but thanks to #1 (perfect security is impossible), we're guaranteed to be picking up the poo poo flung by others from now until retirement, which means the following ...

3. **Security Response jobs suck.** It may seem like CSI or something, but jobs that deal with responding to incidents suck. Except in high profile cases, computer forensics and true chain of custody techniques are not followed-- and if you want a computer forensics job, you'll probably have to work for a large government/public sector bureaucracy (and all the fun that goes with spending tax payers' dollars), which means you'll be primarily working on child pornography or drug trafficking cases and riding daily the fine line between public good and privacy infringements (warrantless wiretaps come to mind). My anecdotal observation is that very, very seldom do drug dealers and child porn traffickers actually employ decent computer security tactics; therefore, the job is lot less "CSI" and lot more mind-numbing "lather, rinse, repeat". From the words of someone I know who does this work: "I pretty much just push the big 'Go' button on EnCase [forensics software] and then show up at court

explaining what it found." Not exactly the most intellectually stimulating work. The coolness factor wears off in the first 90 days, plus there's the joy of having convicted felons know who you are and that your work put them behind bars-- but not quite long enough, as they might still have a grudge against you when they get out. Even if you're lucky enough to not have a begrudging felon on your hands, there's the deep psychological torment that will slowly boil you alive if you are constantly exposed to the content of criminal minds. Your mileage may vary, but it probably won't be what you expect.

For those who hope to work responding to computer intrusions, you should realize that very few organizations can afford to keep people on staff who perform only computer intrusion investigations. Most orgs just want to know what it will take to get things back to normal, because to do a full root cause analysis on a computer system that generates revenue, well, that likely means the org will have to forego revenue, at least long enough to take a forensic snapshot of all of the data. Very rarely (mainly just high profile cases), will an org be able to afford that. So the competition is tough. Not to mention that in many publicly traded companies, there is indemnification from not knowing exactly how an intrusion occurred. And there's even more stigma if the details are made public. So there's just no incentive for them to really find out all of the details. The 20,000 foot view is good enough (e.g. "vulnerability in a web server").

And then there is an entirely different breed of "computer security professional": those who work on disaster recovery and business continuity planning and response. As you get engrossed in this sort of work, it tends to be less about "security" (critics: I realize "availability" is a tenet of the CIA Triad [http://en.wikipedia.org/wiki/CIA_triad]) and more about the daily employ of scare tactics to get organizations to fund remote data centers that are ready for the next apocalypse. The work is surprisingly more akin to "facilities" planning work: buildings, electric, plumbing. There is a "cyber" aspect to it, but it's mainly about funding the necessary equipment and then getting sysadmins to build it and test it out. That's project manager work; tedious, nanny-like, often political. It's not for people with short attention spans or high expectations.

4. **Security Operations jobs suck more.** Security Ops is at the bottom of the security professionals' totem pole. Most of these jobs are just sysadmins or network admins who have been promoted an extra notch, maybe because of that shiny new industry cert that some trade rag said was "hot" and would result in a 15% salary increase. But all of the usual sysadmin/network admin griefs apply here and then some. It's an operations job, so you inherit all of the problematic decisions that the project planning and implementation people lopped over the fence at you. Very rarely do Security Ops people in an org get to influence the architecture of future deployments. And besides lightweight tweaks like patches or an occasional config change, very rarely do Security Ops folks get to do much to systems "in production", especially for "legacy systems" *(what part of "legacy" isn't a euphemism?)*. For the most part, it's sit back and watch to see if a security failure occurs. I use the word "failure" with specific intention, because Security Operations folks have to constantly keep delicate China plates spinning atop poles, because each plate represents a certain security failure. As it is with spinning plates, it's often about deciding which failure is *more* acceptable, not about preventing all failures (see #1, again).

   In fact, there's an interesting twist: Security Ops managers or directors who experience a breach may find themselves losing their jobs on incompetence grounds. Going back to #1, this seems counter-intuitive. If we know perfect security is not possible, then we know security operations will experience a breach at some point (if we give them enough time). How, therefore, can you ever expect to be successful at a security operations job? When the shareholders want to know who was responsible for the unauthorized disclosure of thousands of company-crippling account records, the first person with the cross-hairs on their back is the person in charge of security operations. So, to survive at this game requires either company hopping before the inevitable breach

occurs, OR, it requires politics (or black mail on somebody high up).

Outsourced security operations is just a variation of this. If the contract includes full accountability, it's one and the same as what is described above. If it's a "we monitor your systems that you are accountable for" scenario, then you as an individual security operations employee of the contract firm may not get fired, per se, but your company may lose the contract renewal, which means if you allow #1 (above) to be true too many times, then you might find yourself out of a job there, too.

The worst part about SecOps is that you'll either realize you've hit your Peter Principle [http://en.wikipedia.org/wiki/Peter_Principle] with that job, in which case it's time to spend all of your free time on backyard barbecues and retirement planning *(nothing necessarily wrong with that -- ignorance is bliss)*, OR, you'll want out immediately because everyone around you has hit their Peter Principle highest job and you want more.

5. **Security Planning jobs are set up to fail.** Think about it: perfect security is not possible. So, even the most cerebral of security planners is going to deliver a work product that has flaws and holes. If you can convince yourself that's not depressing and continue on, maybe you can also be lucky enough to get into an organization whose culture thinks it is acceptable for people to deliver faulty products to a Security Operations group (#4 above)-- and that it is entirely the Operations' people's faults when it capsizes. Not to worry, though, you probably won't work for an organization that can afford a true security response group (#3 above -- it's probably just the Security Operations' people who get to handle the full response process to break up their mundane day), so nobody may know it was your fault. Besides, if you're dealing with a bunch of vendors' COTS (Commercial Off The Shelf) wares, there's not a whole lot of control for you to have, which begs the question why your organization even has a position for you in the first place. They probably could have just paid some consultant for a couple weeks, rather than have you permanently on staff.

   The other downsides are, of course, that you (like the Disaster Recovery & Business Continuity Planners) will also have to use scare tactics to implement draconian policies which probably won't actually amount to any real benefit, but some "power user" or Joe Software Developer will figure out he can circumvent them if he has two laptops and a flash drive *(long personal anecdote story)*. If that doesn't work (or if you just want to cut to the chase), enter regulatory compliance into the equation: *"Your project must do that stupid, expensive thing that results in no real added value because PCI says so! [http://securology.blogspot.com/2008/12/stupidest-pci-requirement-ever.html]"* It won't be a policy for something that 100% makes sense 100% of the time. Instead it will be something that makes life difficult for everyone (and everyone will love you for that), but is generally accepted by 3 out of 5 security professionals who also have no clue and are stuck in the dark ages (hence there are a lot self-perpetuating bad ideas out there, like firewalls and anti-virus). If you're an enlightened security strategist, you'll realize the futility of your job and want out, or you'll revert to also longing for weekend barbecues, vacations, and eventually retirement, all the while wondering if this is your Peter Principle job.

6. **Security vendors have to sell out.** They sell out because they thrive on the perpetuation of problems, selling subscription services to deal with them. Scare tactics are used so frequently the vendors are numb-- finding themselves unaware they're even using them. Not to mention, there are so many security vendors out there for startups and small boutiques alike that most security professionals on the potentially-receiving side of their goods and services haven't even heard of them. Or maybe they have? The names all sound so familiar, like: Securify, Securification, EnGuardiam, Bastillification ... they all seem to make sense if you're still in that state of mind after having woken up from an afternoon nap's dream, otherwise they reek of a society with too many marketing departments and far too many copyrighted words and phrases. If the company is any good, they'll

eventually be swallowed up by one of the bigger fish, like Big Yellow (Symantec), Big Red (McAfee), Big Blue (IBM), or one of the other blander colors (HP, Microsoft, Google, etc.). Only a few stand strong as boutiques, and if they do, they almost certainly have a large bank or government contract as a customer.

Once you get a job at a security vendor, you'll probably be working as a developer who maintains a security product. And, as Gary McGraw has often pointed out, that's not about writing *secure* software, that's about writing security *features* into software. If you're not maintaining it, you'll be *supporting* it, which is the exact same as Security Operations (#4 above). You'll be the low level person who is stuck taking tickets, interpreting manuals (RTFM!), and talking to the Security Ops people at your customers' orgs. Fun times. Don't think for a second you'll go get a job at one of those big companies and fundamentally shake up their product lines and come out with cool new security-features-software that the Security Ops folks could really benefit from. These big companies get new ideas by buying the startups that create them; rarely does a lightbulb idea make its way into fruition. In fact, if you have such an epiphany and develop it as your brainchild into a security startup, rest assured that the bigger fish that swallows you up will succeed in turning your baby into yet-another-amalgamated product in their "enterprise suite" of products and services. It will lose its luster. They'll make the UI match the "portal" their customers already love to hate, but by then, you will have sold out and you can take your new nest egg with you into early retirement (*weekend barbecues, here you come!*).

If you're not one of those, then you will really be a sellout-- either a sales rep or a sales engineer. If you are somebody who like repeating what you say and do, this is the job for you, because you'll repeat the same lowly power point slide deck that marketing (you remember-- the people who came up with that killer company name!) for every customer-- that is, all of the customers that let you in past the cold call. If you're the sales rep, remember to drag along your sales engineer to get you out of a sticky situation where you promise some security perpetual motion where it's just not possible. And if you're the sales engineer, try to remember the security perpetual motion is just not possible. It'll be hard to tell the customer that, though, since it will say otherwise in the power point slide deck that marketing provided. It's be right there in big red letters: "Secure", "Unbreakable", "Keeps all hackers out", etc., etc., etc.

7. **Pen Testers and Consultants have Commitment Issues.** If you can get over the fact that penetration testing doesn't actually prove anything [http://securology.blogspot.com/2007/09/penetration-testing-tom-sawyers.html] , then it might not be a bad way to go. That is, if you can sell out, work for just a paycheck, and position yourself in one of the jobs with the least amount of accountability and responsibility in the entire InfoSec space. The same is true for third party consultants, too. Any job where you are hired to come along and tell the hiring org where to put more bandaids falls into this category. Sure, there's a broad body of knowledge to comprehend ... but there are plenty of security vendors (see #6 above) who think they have a tool they can sell you so that you can point and click through your brief engagement with the hiring org, which begs the question: *Why should they even hire you if an automated tool can give them their results?* That's not true of all independent consultants and pen testers, though. Some of them do provide usefulness beyond that of a canned COTS tool. But they all suffer from the same problems as Security Planners (#5 above), only they probably had a prior job working directly for the org and saw how painful it was to stick around through the accountability phase after an incident. So now, they've learned their lesson: get in, get out, cash the check. They say: *"Hey, it's a living."* Are they the smartest security professionals around? Probably not. Do they have what it takes to do the other security jobs like Planning, Ops, and Incident Response? Definitely not.

8. **Exploit writers perpetuate the problem.** They're either criminals and this is their day job in which they hope to get paid for the same work they do it after hours for organized crime syndicates, OR, they really wanted to be

that one-handed Hollywood typist with Cheetos all over his fingers and they have even more commitment, communication, and wherewithall problems than do the Pen Testers (#7 above). All they do is sit on a chair all day in front of multiple computer screens (no doubt [http://www.flickr.com/photos/dobrien/1598629374/]), and attempt to prove over and over again what academics have been saying since the 1970s. Yet there seems to be some economic sustainability [http://securology.blogspot.com/2007/09/economics-of-security-researchers.html] , because otherwise the security vendors (#6 above) would have no way to sell you subscription services to access today's latest hack that a criminal otherwise might find on their own. But thanks to the vendor (and their handy, dandy *exploit writer* they have locked up somewhere with unlimited access to Cheetos and caffeine), we can all rest safely that the exploit code they just wrote won't be weaponized to prove #1 again (that happens all the time, actually), causing some poor Security Ops person (#4) to get sacked, while some Security Planner (#5) thinks *"glad I'm on this side of the fence"*, and some Pen Tester (#7) thinks *"I gotta download that into my pen testing tool for tomorrow's gig-- that way I know I'll find a hole and they'll hire me back next year"*.

9. **Security Educators either are paranoid or should be.** If you're just contemplating a career in information or computer security for the first time, you probably aren't acquainted with any of the lovely people in this category, mainly because the good ones are expensive. Typically, it's only existing security professionals that get to experience security educators, because their employers realize that it's important to keep them up to date with information-- primarily thanks to exploit writers (#8) who keep the litany coming. The principles of security rarely change; only the scenery changes (and the exploit writers change scenery like the masters paint in oil).

   Educators fall into one of two categories: 1) they suck because they've been out of the game for so long (if they were ever in it at all), or 2) they're spot on, but they don't want you to know what you're reading now because you may consider a career change and that's one less pupil, one less paycheck for them. If they're on top of their game, they're paranoid. They have trust issues with everything and everyone. They can't stay away from the topic, so they're very well-versed in what has happened as well as the current goings-on in the field of security, but they have worse commitment issues than Pen Testers and Consultants (#7). They have the ability to scare you, but not in the same way as the security vendors (#6) and security planners (#5); you'll be able to tell that they don't want anything in return-- it's almost a *relief* for them to share the information they know with someone. Sometimes a vendor sneaks in and pretends to be an educator. Beware of that; though the way to spot them is their horror stories will result in an emotion to buy a product or service. You won't come out having learned anything other than their products solve a niche need.

   Becoming a security educator isn't an easy task; it typically means you were an educator of some other specialty domain and then learned how to teach security (which usually doesn't work as well as someone who has lived it), or you lived it yourself through one of the other job types and have educated yourself beyond the level of ordinary practitioners. If you're already in a security career and find yourself disheartened by the lacking options around you (because you've realized that it isn't the glamorous field you once thought), but find that you have an amazing affinity towards learning all that you can, this might be a saving grace that will prevent you from leaving everything you've learned behind and taking up a job as a dairy farmer (or some other similar job that will not require you to touch a computer). There's also the potential for life as an academic, where you can ~~infiltrate~~ inspire open minds that have yet to be corrupted by corporate ways.

10. **Security Media don't really exist.** There are like 4 or 5 real "computer security reporters" in official media outlets. Anyone wanting to aspire to be them would have nearly as good of odds at becoming a professional athlete-- and that pays better. For all intents and purposes, they're either vanilla columnists whose writing glares

that they don't understand the technical underpinnings of the subject of their writing, OR, they're paid bloggers.

11. **And Security Bloggers are the worst above all.** (Present company included.) They know some or all of the above and chronicle it where they can, thinking that just collecting their thoughts in some digital pamphlet will change things. In order to be a security blogger of any real significance, you have to be known among the security community. For most, that means affiliation with a brand, product, or service. For a very elite few (the Schneiers out there), that means being one of the first to do so, calling everyone out for who they are, and taking as many opportunities to spout off in normal press/media as they'll allow (e.g. Schneier's a self-proclaimed "media slut"). For the rest of us, this may just be an attempt to alleviate the pressure of painful security information in our brains-- a pressure-release valve.

Do you still think you want a job in computer or information (IT) security? If your sole motivation is a paycheck, even if it means beating your head against the wall while trying to solve unsolveable problems, then this may be a career choice for you. If you can survive without gratitude for a job well done (because when these security professionals are actually successful, by dumb luck or otherwise, they largely go unrecognized and unthanked), then you may have a chance.

If you hope to change the world with your career, may I suggest a rewarding opportunity teaching high school math or science in a public school system? The pay is for shite, and there will be harder days than being a security professional, but your pupils will be grateful for your job well done later in life-- even if they don't manage to get around to tell you. Besides, everyone knows Americans spend what they make-- just learn to make ends meet on a teacher's salary.

...
[My general apologies for starting off 2009 with a lump that is hard to swallow.]

Posted 9th January 2009 by securology

Labels: complexity vs security, ethics, humor, Marketing FUD, penetration testing, politics, predictions, security advice, security economics, security education, security history, security metrics

9 View comments

Anonymous January 12, 2009 at 10:58 AM

Thanks for making me depressed.... Sooooo true though.

Reply

Anonymous January 30, 2009 at 9:17 PM

Wow. This is the most depressing thing I've read in a long time. Then I realized - maybe you're jaded? Or maybe not making the big $$ you'd hoped for? I'm not sure if I know you, I know a lot of damn people in this industry, but if I don't - please keep your incredibly depressing, wannabe-proselytizing opinions to yourself. Let me throw some rebuttals out, just for giggles.

1. Right - perfect security is not possible. Neither is "perfect profits", "perfect project management" or "perfect anything else" for that matter. Should that dissuade you from a career path? Hell no - don't feign such idealism, it's silly. Hackers like problems to solve, and good security people are fond of solving security issues. I am not yearning for perfect security, and I don't know anyone else that is either.

2. I'll give you this, to some extent. Trying to get other people to "do right" IS frustrating. But when that one person DOES the right thing, it's a fantastic moment of elation - "someone got it!". If you don't feel this when it

happens, you are way too depressed and cynical about the whole thing, and you are not likely to make friends at parties.

3. You've got some points here. I agree - most organizations can't pay full-time IR people. But some of us actually LIKE doing IR work. I've done some that sucks, sure, we all have, but some of it is incredibly stimulating and rewarding. You are just over-generalizing WAY too much here.

4. Security Ops jobs are often people's first step into the industry. And they're also the ones where a) real work gets done, unlike many of the bullshit "architects" I've met, and b) can be incredibly rewarding for some people who LIKE working with gear. I have done a ton of this work, I am further along in my career, but I will NEVER say I'm too good for it. I'll crawl around in a data center and config a firewall any day. And I bet there's a lot more like me than you realize - being a geek is part of the fun of this profession, lose that sentiment and you're probably lost anyway.

5. Damn dude, where you have you worked? It's about doing the best job we can. I've worked in some horrible places where the environment sounded a little like this, my advice to people who relate to this point even a little bit - get the F*** out! Don't hold on to your job just because the economy sucks, unless you live in Bumblef*** where there ARE no jobs (and then you should move anyway), but come on! This is a little too "Office Space" for me, you can pretty much make your own attitude.

6. Yes, some security vendors are totally pushing FUD. But without them - what do we have? Open source? Bah. There's some good stuff in that, sure, but there's nothing wrong with people selling products, it's that whole economy thing. And there is NOTHING wrong with making money, so don't hate the sales people. Just doing their job - if you don't like their approach, fine. But what about the product? Does it solve a problem? Do you need it? Better questions. And I was a sales engineer, and they have something incredible going for them, in most cases - people skills! That's right, they can TALK to PEOPLE, and actually look you in the eye sometimes! Wow! And they probably make a lot more money than you do, too. Most SEs I know are very technical and simply do most of their tinkering in their spare time. Which they have some of, since their jobs are usually pretty kick-ass and they have more $$. So.....what sucks about repeating the slide deck? Oh, I forgot, your incessant idealism keeps getting in the way. Well, most of us will happily deal with a little repetitive action to make double the money.

7. Some pentesters suck. Others do not. Sometimes they provide value. Sometimes they do not. They also make a lot of $$ if they're good. So...what's the problem here?

8. Some exploit writers do perpetuate the problem. Some don't though - HD Moore has given more to the community in his time than you or most ever will. But what is really the argument here? People will always find flaws in things, these folks are just doing it more often. And MOST of the time, things get fixed as a result. Given that most of the real security issues come down to stupid simple issues like patching and access controls, we actually could prevent most of those exploits from being a reality, but that's a different issue.

9. I teach people at a few conferences a year. I do it because I enjoy it. Now, I agree with you, many times full-time teachers don't know what the f*** they are talking about since they only teach, but not always. I can back my shit up, EVERY TIME. And the folks I tend to teach with can too - we all consult and do a number of different things in the security community, so we actually have a clue. Are we paranoid? Sure, to an extent - any good security person is. But most of us have learned to chill a bit, too - we have families and lives away from the Internet. And we all make enough money to be pretty damn optimistic.

10-11: Yes, most security media people need to STFU. Especially those who think blogging is making them special. For God's sake, say something insightful instead of just whining about stuff. Or pointing out the obvious. Or regurgitating stories. Ugh. You're not getting paid for it, so why do you have so much damn time to do this? Blog readers != friends.

As for changing the world, the everyday security people of the world actually ARE. Sure, they're not getting public recognition for it, but who cares? Every time someone prevents some asshole from stealing my credit card number or health records, they're my hero.

So, anyone reading this post - it's bullshit! Security is a GREAT career for curious, technical people who need constant and ever-changing intellectual stimulation. Is it thankless sometimes? Sure. Do you put up with BS and vendors and idiot bloggers who spew drivel and actually say and solve nothing? Yep! But if you can get past all

that, welcome to the club. Most of us aren't this depressing.

Reply

securology January 31, 2009 at 10:41 AM

Dear anonymous (Jan 30),

I won't comment on everything you said (I welcome and appreciate your differing perspective, though), but I will say this: There will be people who will read my original post and say "Oh, no that's not the job for me." And that's good. Those people don't need to work like that. There will be others, like yourself, who will read this and say "Yeah, so what? I deal with it and am fine." That validates that you're willing to put up with it all. That's good, too.

For the record (not that you're surprised, I'm sure), I fall in and out of several of those categories. I'm probably jaded-- I'll give you that, but the pay is fine (more than I ever expected). It's not about money for me, though. Yes, I am an idealist (the world needs more of those, in my opinion), which leaves me to cling to the options in #9. If I could sell out my ideals, I think I could be happy with the paycheck from #7. The truth is, I've done at least a little of all of these and am making fun of myself as much as the rest of you who have those jobs.

If you read the original post and take it as a challenge to improve the state of the state (or prove that the state is better than I claim because you see things the rest of us cannot), then I'll label this an accomplishment.

You said:
"So.....what sucks about repeating the slide deck? Oh, I forgot, your incessant idealism keeps getting in the way. Well, most of us will happily deal with a little repetitive action to make double the money."

You're absolutely right; I won't do it for the money. (Now, if somebody was learning as a result, that's a different story-- that's where us idealists get value-- actual overall improvement through knowledge.)

I don't know if we've met, but I certainly have no hard feelings from your comments. Thanks for your time.

Reply

securology January 31, 2009 at 11:04 AM

@anonymous,

And I think my last two paragraphs sum up nicely-- even validating your remarks.

1) If you can work on an unsolvable problem without being depressed-- go for it.

2) If you cannot (because of your idealism), go seek a job that may be more rewarding (like teaching high school math).

It's interesting that you saw only the negative aspects in my original post. I had to re-read what I wrote (forgot it already) to confirm I really did look at both sides.

Reply

Aaron February 22, 2009 at 1:35 PM

Haha, good read. I am an aspiring student hoping to get into this line of work. So thanks for blowing my aspirations!

Na just kidding, but I will definitely show this to our schools system admin. Hopefully he will get as much of a kick out of it as I did.

Reply

securology February 22, 2009 at 4:33 PM

Aaron,

Woo-hoo! I succeeded! (That is, of course, if you really do change your mind. :)

On a (slightly) serious note, like some of the other commenters said, it is possible to enjoy this work, provided you understand all of these negative aspects first and are still okay with it. Or, provided that you get your satisfaction out of something outside of work (like my references to backyard barbecues and retirement). If you can make it "just a job" then it could be a rewarding one. It tends to pay better than average IT pay.

Reply

James February 25, 2009 at 9:16 AM

Looks like someone has a bad case of "sour grapes". Awwwwwww.....

Reply

Anonymous February 27, 2009 at 2:16 PM

What this really boils down to is the organization that an in"duh"vidual works for in any security related role.

It is the company in how effectively they have laid down their security strategy, requirements, policies, procedures, directive, guidelines, planning, etc..that will influence your experience as a security employee. All of these will affect whether your role is taken seriously, whether or not you will get lynched at the end of the day, if you get sold out or not, frowned upon or appreciated, and ultimately whether you hit the peter principle.

For all those security folks out there, I am sure many of you have landed a role in an organization where "functionality" "ease of use" and "product delivery" occupy a substantially higher priority than security ever will. In places like this you will constantly be thrown into oncoming traffic, you will be ignored, hated, shunned, frowned upon and disrespected. Why? Because the company has no desire whatsoever to implement security into their application development process. If you find yourself in a role like this without any executive level sponsorship, GTFO and don't go back.

So my advice, don't bitch about it and don't try and talk other people out of it, educate them so they know what to look for, how to identify warning signs, what sort of questions to ask, and above all, how to make sure they do not end up like you!

Reply

D4741us7 March 1, 2009 at 12:25 PM

Take the post for what it is: The far end of the spectrum of opinions on Security jobs. I enjoyed the article, and I believe it has great merit and deserves to be read, whether or not it is 100% true for everyone. It's targeted towards aspiring security professionals, and if you fall into that category, you should be interested in hearing BOTH sides of the story, not just the fluff fed to you by schools and certification vendors. It's his experiences, we should all be interested in listening to them. It's that mark of an educated mind to entertain a thought without accepting it.

Reply