

RE: CISSP-ISSMP

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2006-05/msg00099.html>

- *From:* "Craig Wright" <cwright@xxxxxxxxxxxxxx>
 - *Date:* Wed, 10 May 2006 08:56:56 +1000
-

Hi,

Although I agree with much of what you have said, it needs to be taken into context. Unless there is some focus on the question, there will be no correlation to the answers.

First as to not wanting ""generalists". They want "specialists". This is wholly dependant on the organisation, the size and the focus. Whilst true in many larger organisations, it is generally not so in SME's where a limit to staffing precludes having a specialised IT function for each IT discipline.

If you want to get more money this is another issue. I have never received a job or a pay rise for industry certs. Any rise that I have received would have occurred either way. Having completed a MMgt (Master of Management, similar to a specialist MBA) I have found that this has aided my career more than any of the certs.

From a point of view of risk and security, the LLM I am currently completing has added far more value to clients than any of the certs, and thus helps my career more. It is amazing how much more you can get done arguing legal and contract requirements with an outsource vendor than trying to enforce firewall rules etc on a purely technical basis. For those out there wanting to get into the Digital forensic sciences, a law degree or two will do more for your career than a whole bag of industry certs.

A PhD will get 5-10% (averaged) income greater than a standard Masters of the same discipline. As far as cost effectiveness, the time to undertake the degree and the costs associated with completing it make it unlikely that you will earn more over your life. Why do it? There are a number of reasons. Myself, I am involved in both industry and academia, and for the most part I enjoy a mix of business and academic life.

Statistics training should be a requirement PRIOR to allowing people to spurt off on their interpretation of statistical data and it should be mandated before people are allowed to start one of the generally flawed

RE: CISSP-ISSMP

studies that abound.

So why do "I" pay the extra for an ISSMP (which incidentally I do not use on my card etc). Because I wanted it. Because I can deduct half on tax and have the other half paid for anyway.

Regards,
Craig

PS As for research masters and esp. doctoral degrees, I have had 1 employer (ever) read any of my dissertations (and he only read the first 3 chapters). No client that I know of ever has. Even then, like most people in the industry with doctorates, my doctorate is not in IT, so all it shows is "advanced research" training.

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

From: Bob Radvanovsky [<mailto:rsradvan@xxxxxxxxxxxxxx>]

Sent: Tuesday, 9 May 2006 11:30 PM

To: Nathaniel Hirsch

Cc: pen-test@xxxxxxxxxxxxxx

Subject: Re: CISSP-ISSMP

This doesn't surprise me. Nor does it surprise me that now, many people are finding out that their certifications are either meaningless, or have significantly less value than what they were lead to believe. It is almost like 'snake oil salesmen', promising a cure to an ailment that sassafrass oil doesn't have any medical correlation with. Certification companies stipulate that certified people have a better chance at getting jobs -- not true anymore. A recent survey concluded that people *are not* getting those jobs based upon their certifications. Some companies stipulate that certifications may get you more money in places you are already employed. Again, not true. I have known folks who have passed their CISSP -- or whathaveyou -- certification, only to have IT management say "that's nice", and move on. They're still doing the same job, with no pay increase, and no job structure realignment.

Can't say that I've told many of you that "I told you so" -- but -- "I told you so". ;P

What companies want are well-rounded people (not literally; if we did, we'd have a seriously huge problem here) with a balance between education, certification, experience, know-how, abilities, and willingness to 'do the right thing'.

Many 'security jobs' are nothing shy than that of an overly glorified 'security guard' job: you sit in front of a desk, and *wait* for a telephone call or alter to pop up on your monitor screen. It is purely RE-active, not PRO-active. People feel that if they get a certification, that they will get a chance at the glitz and glamour, see the sights, and most importantly, get paid...well. It's all a lie. You

RE: CISSP-ISSMP

RE: CISSP-ISSMP

are just another 'security monkey' to The System, and your role is one of thousands to fulfill a role for something else. Sure, they want you to get your CISSP (and if you read/listened to what you said, you might understand what I'm saying here, friend) so they can charge more for your efforts. The key words here are "charge more for *your* efforts". Does that mean that *you* will get paid more? Doubtful. If at all, all you've done is justified your existence in that organization for an <X> period of time, before they either don't need you any longer, don't want you any longer, or plan on selling your company. The fact is, you, like so many out there, believe that all of this will save your sorry butts, prevent you from getting laid off, and get you some more money. I'm sorry, but in the world today, that's just sooooo wrong.

Today's scale of economy doesn't work based on the hard work ethic principle any more. It's much, much different now: "How can I make as much money as possible, doing the least amount of work possible, while retaining the least amount of people possible?" Those kinds of questions are what's going through your manager's or their manager's minds. There are a few "pockets" out there that reward people for their hard work and efforts. But let's face it, Corporate America doesn't care, except for 'bottom line'. That's it. Nothing more.

If you get a certification, or an education somewhere, that's nice. Good for you! You got it because you *wanted* to get it, because you feel that it's something that will help you, both externally and (more importantly) internally. Not because you *think* you will get more money. If your *sole* purpose is to get money, you're doing it all for the wrong reasons. The certification companies *want* you to believe the money idealism at all costs, and, of course, *charge* both you and organization for getting there. Of course, if you don't get what you want, you can come back, and take another class, and another, and another...

Let me share a few insights with you...

I have several degrees, including a Masters of Science degree, with close to 28 certifications (not all are IT-related). I've been in this business for OVER 28 years, and have seen all sorts of flim-flam artists come and go, and people promising the sun, moon and stars. The certification folks provide *some* utility, but not for what you think it's for. It's a 'weeding mechanism'; that is, when you get tired at your currently lillypad, and decide to move to another lillypad, and there is a tie between you and another candidate, the recruiter or HR person will look at *both* of your qualifications and see if there is something that stands out between the two of you. If you have a certification, and they don't, and the job stipulates that a certification is "recommended", it's simple: you -- more than likely -- you might get the job. But then, I've seen other factors play into things, too. Some companies are cost-conscious, where 'bottom line' rules. If the other candidate is a senior-level technician, has 15 years experience, and wants \$80,000, versus someone else who has 5-7

RE: CISSP-ISSMP

RE: CISSP-ISSMP

years experience, and wants only \$55,000, then it's really a moot point. No matter what the person has done, or is capable of doing, companies will make a decision based *solely* upon the salary and NOT upon the job qualifications (which I have seen soooo many times in the past). Also, most recruiters are considered 'technical idiots'; that is, they know some of the lingo and terms, but cannot figure out if someone is performing a 'snow job' on them or not. In most cases, it comes down to the hiring manager to help filter through all the junk, to determine if someone is (truly) trying to pull a fast one on them. Sooner or later, the truth comes out if that individual is trying to pull a fast one, but lately, it doesn't seem to work any more. Also, recruiters and HR people have 'quotas' --- of course, they'll deny that they have quotas, but this is bunk. How many times have you applied for a job, only to find out that there are 6 other ones like the one you are applying for, different titles, all pointing to the EXACT SAME JOB? This phenomenon is becoming more and more prevalent these days, thanks for online job-boards such as Monster or Hotjobs. And, of course, recruiters want you to work with them because of the 'exclusivity' that they have to offer. Rrrrrrrright. The *best* jobs --- believe it not --- never make it to the recruiter's organization. What the recruiters get are the 'scum jobs' --- the hard-to-fill jobs that no one can, or will want, to fill. They are simply trying to find a person, who matches <X>% of the qualifications, to fill that role. Period. End of discussion. It's all a matter of economics.

I currently work with a 'technical idiot', but this person is shrewd and cunning. They leave just minutes before an event happens, often times, leaving me to do all of the work. We are a 'team' --- so long as I do ALL of the technical grunt work, while he gets to attend meetings and drink coffee all day (yes, it's straight out of Dilbert, or the movie "Office Space", if you've ever watched it --- excellent movie). Doesn't sound fair, does it? Life isn't fair, and neither is working in a corporate environment. Get used to it, kiddo. You're going to see more and more people who have a 'technical IQ' of an ant, but the prowisness and cunning to that of a puma. Not all IT or IT security people actually *know* what they're doing. That's why they've got...you.

Many of them, are nothing more than 'paperpushers'; most of them rely on people like *you* to do the job that they *should* be doing, but fill other roles like 'customer relations'. Sometimes, it works for the better. Many (often times, most) times, it does not. Most people and organizations are lazy, and want to lay claim that it is someone else's fault for not getting the job done. This is why we have job segmentation/compartmentalization today. Or haven't you noticed? You do ONE thing in your job --- THAT'S IT. The Days of Generalized Specialization are almost dead. Companies don't want "generalists". They want "specialists". And why do you ask? So, when they have no further need of your services, they simply get rid of you, your job, or your position entirely. It's all "ala carte" nowadays. And the certifications are an almost *direct* correlation to that mindset.

RE: CISSP-ISSMP

Finally, it's not *what* you know, it's *who* you know that counts these days, what connections you have, how well-to-do you are, and if you have any *influence* that you can exert over your 'target' (that being a manager). And the security industry is no exception. In fact, it's far more political than standard IT-related work, because of the 'human factor' involved. You interact with humans more often than computers, and thus, the amount of politics increases accordingly. It is very proportional.

Know that you're not the only person who's going through this. Many other technicians and security folk alike, will probably agree with me that this is more commonplace today than ever before. Those of us who are "old farts" (been in 'da biz for more than 10 years), know that times are changing -- rapidly. I don't what other advise I can give you, except be flexible, and always keep looking. I've been doing the same darn thing now for over 15 years. Does it get tiring? You bet it does, esp. when you aren't appreciated nearly as much as the next person. But, be thankful that you even have a job in a time when our jobs are continually being threatened by outsourcing, or worse, offshoring. Unless you like curry chicken, you have to keep your options open...and your mouth shut. If you don't like what you have at your place, move on; otherwise, find ways to work with the psychodynamics of your workplace, of which there are plenty of books out there on the subject. ;))

Hope this helped...

-r

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

From: Nathaniel Hirsch [<mailto:nh2@xxxxxxxx>]

To: Mohamed Abdel Kader [<mailto:makster12@xxxxxxxxxxxx>]

Cc: pen-test@xxxxxxxxxxxxxxxxxxxxxx

Subject: Re: CISSP-ISSMP

I recently got my CISSP. The company that I work for paid for me to go to a class, and take the test assuming I passed. If I failed then the \$500 would be on my nickle. Thankfully I did not fail. The main reason they wanted me to get my CISSP is now they can charge more for the work they contract me out to, this and you need it or some other equivalent to do level 3 and 4 DITSCAP testing. As for an ROI after I passed a got a 15% raise which was nice, but I was also up for a raise, so I can not tell you how much that was due to the CISSP, and how much was due to my overall performance at the company. Personally I feel that the exam and certification process is a waste of time, and so does everyone else at the company, but they are needed, or so they say. However we have a guy who works here who is a CISSP and a CEH(certified ethical hacker), and to be truthful, he is quite possible the most worthless tester I have ever had to work with, and

RE: CISSP-ISSMP

everyone else in the office knows this. So having the cert doesn't make you good, and doesn't prove to anyone that you have experience or skill. It just proves that you can pick the correct answer out of a four possible answer on a 250 question multiple choice exam. As for giving an out of 10 scale for everything you mentioned I guess they would all be 5s because it all really depends on a lot of other things. As for what job its good for, I would have to say more managerial then anything else. The topics covered are really only puddle deep, not enough to know whats going on, just enough to know that it is going on though.

Nathaniel Hirsch, CISSP
Xacta Corporation
656 Shrewsbury Ave.
Shrewsbury, NJ 07702

On 5/8/06, Mohamed Abdel Kader <makster12@xxxxxxxxxxxx> wrote:

Hi all,
I was wondering if anyone out there did the CISSP-ISSMP

concentration.

I want to know the value added in the areas listed below, in an out of 10

scale for example:

Total ROI
Career Advancement
Industry Demand
Raise Potential

Suitable for what job/position (not an out of 10 answer of course :))

I also want to know the material to study from.

Thanks a million.
MAK

RE: CISSP-ISSMP

This List Sponsored by: Cenzic

Concerned about Web Application Security?

Why not go with the #1 solution – Cenzic, the only one to win the

Analyst's

Choice Award from eWeek. As attacks through web applications

continue to

rise,

you need to proactively protect your applications from hackers.

Cenzic has

the

most comprehensive solutions to meet your application security

penetration

testing and vulnerability management needs. You have an option to go

with

a

managed service (Cenzic ClickToSecure) or an enterprise software
(Cenzic Hailstorm). Download FREE whitepaper on how a managed

service can

help you: http://www.cenzic.com/news_events/wpappsec.php

And, now for a limited time we can do a FREE audit for you to

confirm your

results from other product. Contact us at request@xxxxxxxxxx for

details.

RE: CISSP-ISSMP

This List Sponsored by: Cenzic

Concerned about Web Application Security?
Why not go with the #1 solution – Cenzic, the only one to win the

Analyst's

Choice Award from eWeek. As attacks through web applications continue

to

rise,
you need to proactively protect your applications from hackers. Cenzic

has

the
most comprehensive solutions to meet your application security

penetration

testing and vulnerability management needs. You have an option to go

with a

managed service (Cenzic ClickToSecure) or an enterprise software
(Cenzic Hailstorm). Download FREE whitepaper on how a managed service

can

help you: http://www.cenzic.com/news_events/wpappsec.php
And, now for a limited time we can do a FREE audit for you to confirm

your

results from other product. Contact us at request@xxxxxxxxxx for

details.

This List Sponsored by: Cenzip

Concerned about Web Application Security?

Why not go with the #1 solution – Cenzip, the only one to win the Analyst's

Choice Award from eWeek. As attacks through web applications continue to rise,

you need to proactively protect your applications from hackers. Cenzip has the

most comprehensive solutions to meet your application security penetration

testing and vulnerability management needs. You have an option to go with a

managed service (Cenzip ClickToSecure) or an enterprise software (Cenzip Hailstorm). Download FREE whitepaper on how a managed service can

help you: http://www.cenzip.com/news_events/wpappsec.php

And, now for a limited time we can do a FREE audit for you to confirm your

results from other product. Contact us at request@xxxxxxxxxx for details.

Liability limited by a scheme approved under Professional Standards Legislation in respect of matters arising within those States and Territories of Australia where such legislation exists.

DISCLAIMER

The information contained in this email and any attachments is confidential. If you are not the intended recipient, you must not use or disclose the information. If you have received this email in error, please inform us promptly by reply email or by telephoning +61 2 9286 5555. Please delete the email and destroy any printed copy.

Any views expressed in this message are those of the individual sender. You may not rely on this message as advice unless it has been electronically signed by a Partner of BDO or it is subsequently confirmed by letter or fax signed by a Partner of BDO.

BDO accepts no liability for any damage caused by this email or its attachments due to viruses, interference, interception, corruption or unauthorised access.

This List Sponsored by: Cenzic

Concerned about Web Application Security?

Why not go with the #1 solution – Cenzic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you: http://www.cenzic.com/news_events/wpappsec.php

And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at request@xxxxxxxxxx for details.
