
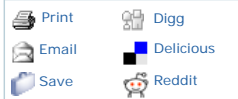


Government Information Security Articles

The State of Information Assurance Education 2009: Prof. Eugene Spafford, Purdue University

 [Credit Eligible](#) **Interview with Prof. Eugene Spafford, Purdue University**
October 20, 2009 - Tom Field, Editorial Director



Information assurance is a topic atop many agendas these days, starting with the president's own cybersecurity initiative. But what is the state of information assurance education?

Dr. Eugene Spafford of Purdue University is one of the icons of security education, and in this exclusive interview he discusses:

- The state of information assurance education;
- How schools, businesses and government agencies must collaborate better to improved education;
- What it will take to truly raise the bar on information assurance.

Spafford is a professor with an appointment in Computer Science at Purdue University, where he has served on the faculty since 1987. He is also a professor of Philosophy, a professor of Communication and a professor of Electrical and Computer Engineering. He serves on a number of advisory and editorial boards. Spafford's current research interests are primarily in the areas of information security,

computer crime investigation and information ethics. He is generally recognized as one of the senior leaders in the field of computing.

Spaf (as he is known to his friends, colleagues and students) is Executive Director of the Purdue Center for Education and Research in Information Assurance and Security, and was the founder and director of the (superseded) COAST Laboratory.

TOM FIELD: Hi, this is Tom Field, Editorial Director with Information Security Media Group. We are talking today about information assurance education, and we are talking with one of the most stellar in the field, Professor Eugene Spafford with Purdue. Gene, thanks so much for joining me today.

PROFESSOR EUGENE SPAFFORD: Happy to be talking to you.

FIELD: Gene, it has been nearly a year since the last time we spoke, and I guess I would like to start out by asking you: What have you seen as the biggest changes in information assurance education in this past year?

SPAFFORD: I would say that the biggest changes have been more schools getting involved in teaching curricula in this area, probably more towards the community colleges and smaller four-year colleges.

FIELD: Now as you know, we have got a new emphasis on information assurance in the country that really starts right up at the top with the president. Given that sort of as a context, what would you say the state of information assurance education is today?

SPAFFORD: Well, it is still rather chaotic. There are a range of issues and priorities within the field where education can be directed; some of the education is directed towards people who are practitioners, who are going to be on the front lines running systems. Some are oriented towards management-type positions that are setting policies and ensuring compliance. And there still is a community focused on the research aspects, more how to solve problems that are just emerging.

We don't really have a common curriculum that runs across these, although there are a couple efforts that are underway to try define parts of it, and it is isn't really certain what the best practices are, what the background expertise should be for these positions. So it is still an area that is evolving quite rapidly.

FIELD: Do you have hope, Gene, that those chaotic elements can sort of come together and there will be some cohesion?

SPAFFORD: I think it will happen. I wouldn't count on it happening anytime very soon. Part of the problem is that as a field we are very young, and we don't understand all of the foundations and principles on which security is based. We have a few concepts that we applied, but we don't have sound understanding of how they merge or how they are threatened. We don't fully understand any

"Too often, we have agencies who manage what we call paper compliance, rather than really addressing the security of their networks."

- Sen. Tom Carper | [Read Article](#)

Recent Content	Most Popular
1 Navy CIO Sees Key Role for Social Media	
2 Combat Biometrics for the Home Front	
3 Tokenization Vs. End-to-End Encryption	
4 Lessons from Spies	
5 Fed Regulation of Private Data Mullied	
6 NASA IT Vulnerable After 1,120 Incidents	
7 NIST Set to Create Real-Time IT Metrics	
8 Tom Carper, U.S. Senator	
9 Napolitano, Bank Heads Confer on InfoSec	
10 NIST Scientist: FISMA Rules Constructive	
View More	

Privileged Access Control Support for NISPOM Compliance

How to address the threat of insider attacks





DOWNLOAD WHITE PAPER

GovInfoSecurity.com Research

- Podcast:** [Getting a Consensus on Regulating Data](#)
- Webinar:** [Creating a Culture of Security - Top 10 Elements of an Information Security Program](#)
- Handbook:** [Identity and Access Management: Because You Need to Know Who is in Your Systems](#)
- White Paper:** [Five Ways to Reduce Your IT Audit Tax](#)
- Regulation:** [NIST Guide to Security for WiMAX Technologies \(Draft\)](#)

[More from the Content Library](#)

Recent Blog Entries

Can Obama Define the Word 'Soon' Soon?

The pending appointment of a cyber coordinator...



metrics that we can use to do incremental improvements. And the variety of the threats that we are encountering are continuing to evolve and get more sophisticated over time.

FIELD: So, Gene, give us some historic perspective; you talked about the here and now, but how has information assurance education evolved in your time in the field?

SPAFFORD: Well, I would say that the biggest change that I have seen has been a split between the hands-on application of prepackaged security solutions versus the deeper understanding of how systems work.

When I really saw the start of this field in the late 80's and early 90's, most of the people who were involved had a deep understanding of issues of machine architecture, encoding, network protocols, and really understood the systems at a low level. What we see now for many educational institutions is they are focusing on high-level applications, web security, JAVA, running prepackaged firewalls and IDS systems, and many of the people going to that educational path are not exposed to those low-level details, even though some of the attackers are exploiting those low-level details. So we have seen a split off of that kind of expertise in two areas, both the research arena and also some in the forensics arena.

But of course the field has also grown; the level of threat has changed significantly. If we go from the late 80's/early 90's, there wasn't any commercial use of the Internet, and it didn't have the global reach it does now. So the issues of social engineering, fraud, phishing, many of the other kinds of false information presentation and mailed-around exploits didn't exist back then. So we have seen a huge evolution in the threat picture, in the target set, and in the overall understanding of what security in computing is all about.

FIELD: Now, Gene, one of the topics you and I talked about in the past is the need for schools, businesses and government agencies to collaborate for successful information assurance education. Where would you say these entities are collaborating well now?

SPAFFORD: Well, I am not sure that I would say that there is strong collaboration on any of those points. This has been an issue of discussion that keeps coming up in various places. We find that some commercial entities, primarily those that are associated with the defense contractors, are willing to do some collaborative research and provide funding for research in some cybersecurity areas on a limited basis.

A few of the large-scale vendors of networking or software are as involved, and then when we get into some government agencies and the financial community, our experience has been -- and that of many of my peers -- they are very, very reluctant to be involved because they are worried about information leakage, about who they are talking, to and they are very reluctant to be out there on the cutting edge when all too often they are judged on older standards.

So one of the biggest problems that many researchers complain about is the lack of good data and a lack of access to large-scale systems where we can actually run some experiments. But the data in particular -- too many organizations don't report problems, don't share the kind of malware that may be getting on their systems, they don't talk about where the failures in their systems occurred, so it gets very difficult for us to either teach how to prevent those or to do research in new mechanisms that could be used to combat them.

FIELD: Now I have got to think that a global recession has not helped to shake out any additional resources to assist you with these either.

SPAFFORD: No, we have seen problems with organizations not only reducing their commitment to engage in the academic arena, either to provide information for teaching or resources for research, but we have also seen many of them cutting back on their staff and their own internal resources, which is problematic given that many of them have a larger number of possibly disgruntled or desperate former employees, because they have done budget cutting across the board, and these are known to be possible agents of difficulties in the information security arena. And it has also heated up the competition internationally among both the thieves and competing organizations that may be seeking advantage by getting access to proprietary information. So there has been a heightened threat posture, and it really seems unusual, or at least ironic in a way, that the companies are cutting back in precisely the area they need to deal with these issues.

FIELD: Gene, I wanted to ask you about the government, specifically the NSA's Center's of Academic Excellence Program. The program is 10 years old now, and I know it has grown from a handful of schools to over 100. I want to get your perspective on where this program is doing well and where you think it needs some work.

SPAFFORD: Well, Purdue was one of the founding members of that organization, that collection of certified schools, and we stayed with it for some time until about a year and half ago we let our certification lapse. We decided that it wasn't really serving any of our needs anymore, and was in fact perhaps misleading. In particular, the idea that there are 100 Centers of Excellence is fundamentally misleading. Of the schools that are certified, and I am not going to take any out by name, there are

[Read The Public Eye by Eric Chabrow](#)

[More Blogs Posts](#)

Vendor Solutions

Intrusion Inc.



Solutions For:

Data Privacy, Identity Theft Prevention, Network Security

VeriSign



Solutions For:

Authentication, Identification and Authentication, Identity Management

[More Vendor Solutions](#)



small number that really are excellent, and the rest of them are adequate.

The Center program was originally designed to recognize a few places that were really leading the way and to perhaps provide them with more resources. But over time, everybody wanted that designation for one reason or another, and right now there are schools that are the equivalent of a low-grade community college that have gotten certified by meeting the checklist, but not necessarily by meeting any definition that we would consider to be excellent.

That isn't to say that the programs that they offer are not worthwhile. What the CAE program has effectively become is a kind of accreditation program particularly valuable to those schools without significant resources or name that would otherwise allow people to judge their quality. Generally, they are all offering some quality programs, but they are not really leading the field in any sense. What they are doing is, as I said, kind of meeting a lowest common denominator, and they are producing people who are needed by the government and industry to manage security tools, to adhere to commonly accepted standards. But as I said, that is not really leading; it is just basically supplying a commodity. So looking at the program, it is successful in a way; it hasn't really adapted well to the fact that the threat and need have grown tremendously.

There has been some change, though. They have created a separate category for research institutions. But, again, the way that they certify those is not so much leading as it is meeting a certain set of requirements. So it is accreditation really rather than a recognition program, and the government never really came through with any extra resources for any of the participants. This has been a complaint from many of the researchers: The government simply doesn't put money into long-term research here.

There is a lot that goes into near-term defense (tactical kinds of things) but very little that we actually see supporting the pushing of the field forward aspects of research, education and leadership that people like myself believe are really important to have.

FIELD: Gene, have you found over the past decade that the program has at all raised the bar on information assurance education?

SPAFFORD: I don't believe it has. The kinds of things that raise the bar would be educational materials, textbooks, lab studies, prepackaged modules that could be used at other schools that could then be innovated from. None of that has come out of the CAE program, or really much of any other organized program.

The national colloquium for information system security education has helped there some by bringing together educators, but the real need is more focused on providing materials from those with experience and with the necessary expertise to be easily deployed by institutions where you have people who don't have that experience. There hasn't been enough emphasis on that really through any of the organized programs by government or industry.

FIELD: Well, I guess the flipside of that is what will raise the bar on information assurance education?

SPAFFORD: That is an interesting question, and one that I have been looking at over time, and the same is true of really raising its level within government and within the research community, all of which have been somewhat neglected.

The problem is that we generally only respond to crisis. And the kinds of problems that we are seeing in the whole information security arena is not a spot crisis; it is a growing community problem. So when we are talking tens of billions of dollars of loss every year in intellectual property theft, fraud, unnecessary or over-expenditure on security goods and services, and various other kinds of problems, that cost is not borne by any single entity, but it is borne by everyone. This results in a huge friction on the economy. It is definitely a loss to society. But no one feels it enough that they are willing to make the investment and the sacrifices to move forward. The government might play a role in this, and one way would be to phase in some liability on operators and vendors for obviously making poor choices.

It is unlikely that we are going to see that because that is politically a very, very difficult subject, and in fact that I believe that is one reason why the presidential attention here in the U.S. on the cyber advisor position resulted in that position being created as reporting in part to the National Economic Counsel rather than being a presidential-level advisor, was because of the business push back on what it might cost businesses.

So no individual business is facing huge losses necessarily, but collectively we are facing just unimaginable losses, but nobody is willing to pay the cost up front for what is necessary to solve the problem in the longer term.

FIELD: Gene, a final question for you. As we have talked about this a lot of attention being paid to information security. There are people that are wanting to get into the field because they know that that's where the jobs are; there are people that have lost jobs elsewhere and are looking to sort of reinvent themselves and are getting into the field. What advice would you give to somebody that wants to get into the information assurance field today?

SPAFFORD: I think part of it is to understand what part of the field they want to get into. There are needs in several different areas that require different talent sets. For instance, there is a growing need for people with forensic and investigative abilities. Those individuals should know something about the low-level operation of computers, more in line with the traditional computer science/computer engineering degree. They can learn what else is needed at a variety of colleges, universities and otherwise, or many can actually start work with some law enforcement agencies or accounting firms, which will then pay to help them get through this additional training.

Another area that people go into is more operation security. There are several different places where they could go here, that is more an on the job training or taking a few seminar-type classes for someone who understands computer operations. There are several training organizations that offer hands on training with tools.

Somebody who is really interested more in the higher levels of policy and design, however, they are probably going to need to go back to get graduate level education; maybe not a whole degree, but something at that level to pick up some of the deeper aspects and understanding what is being done in the area.

Each of those paths is different. Each of those is recognized in part by different kinds of certifications, whether they be something like a professional CISSP, CISM certifications, or a graduate degree like a Masters or a Ph.D. But the real key is for someone to find out what it is they like they do, what their background is and which area of cybersecurity they are really interested in being involved with and then there are a number of different paths.

I realize that is not the kind of direct advice that would tell somebody to go to Place X and take Course Y, but this reflects some of the chaotic nature and the growing nature of the field itself that I mentioned in the very first response.

FIELD: You are right; there is not one answer; there are several different directions somebody could choose.

SPAFFORD: Yes, and in part it is also driven by employers. What I have seen is that positions that have the exact same title at different organizations have an incredibly different skill set and requirements underneath. So there are people who are considered to be a security engineer or a forensic analyst ,and the job requirements for that position in a military agency versus a defense contractor compared to someone operating at a bank, compared to somebody who is working for local government, are all very, very different in what they require.

The biggest thing I could recommend, however, is that anybody who is interested in this shouldn't explore by going out and trying to break things. Increasingly, I am seeing organizations who are stressing no criminal record, no dark-side record for hiring people. Now they will hire some firms that have these people as consultants, although reluctantly in some cases, or not at all in others, and that this I think a key issue all along. There are people who are really fresh in the area who think this is the way to gain experience, and it is not. It is a way to actually shut yourself out of a number of jobs. Businesses are catching on that if they are going to hire someone, they want someone who knows the difference between right and wrong and isn't likely to turn on them at a later point.

FIELD: That is a good point. Gene, as always it is a pleasure to talk with you.

SPAFFORD: Very nice to talk to you, and I look forward to doing it another time.

FIELD: We have been talking with Gene Spafford. For Information Security Media Group, I'm Tom Field. Thank you very much.

Next Related Article:

[From Theory to Practice: The Value of an Online Education](#)

Tell us what you think of GovInfoSecurity.com

We Appreciate Your Feedback

We would love your opinion on our new web site.



Browse Topics Cloud Computing in a Military Context - Beyond the Hype.. Next Topic

1) Which topics would you like to see covered most on GovInfoSecurity.com?

2) Where do you usually get your government-related education and news?

3) What do you think of GovInfoSecurity.com - will you be coming back?

Please leave your email address if you'd like to contribute to our editorial content, or would like to be contacted by our Editorial Director to have a more in-depth discussion:

Submit



Topics of Interest

Congress

- Feds Seen Regulating IT Industry
Getting a Consensus on Regulating Data

Fraud

- Algorithm Sought to Analyze Insider Behavior
Online Fraud: An Insider's View of Today's Top Threats

Incident Response

- Incident Response for Data Breaches - Shane Sims, PricewaterhouseCoopers
Incident Response Essentials - Peter Allor, FIRST.org

Budgeting & Funding

- Creating InfoSec Occupational Categories - Interview with California CISO Mark Weatherford
City Defends IT System from Social Network Threats

Vendor Management

- Ten Questions You Should Be Asking Your Vendors About Hosted Phone Systems
Federal IT Agenda: 4 Top Priorities of 2009

Laws, Regulations & Directives

- Safeguarding a Massive, Decentralized IT System - Interview with California CISO Mark Weatherford
Cooperate, Not Regulate, on Cybersecurity

Information Security Media Group - Family of Websites

Banking

- BankInfoSecurity.com
BankInfoSecurity.com Careers
BankInfoSecurity.com Blog

Credit Unions

- CUInfoSecurity.com
CUInfoSecurity.com Careers
CUInfoSecurity.com Blog

Government

- GovInfoSecurity.com
GovInfoSecurity.com Careers
GovInfoSecurity.com Blog

Subscribe



GovInfoSecurity News

Get the RSS Feed

Agency Releases

Get the RSS Feed

Latest Articles

Get the RSS Feed

Webinars

Get the RSS Feed

GovInfoSecurity.com Blog

Get the RSS Feed