



## WHARTON AEROSPACE & DEFENSE REPORT

Your Knowledge Source on the Aerospace & Defense Industry

# The New Consensus Security Audit Guidelines: Expert Matt Brown on How Implementation Will Work

## Consensus Audit Guidelines for Security Take Shape

May 15, 2009

The *Wharton Aerospace & Defense Report* recently published an [article about the growing number of attacks](#) against Defense Department and defense contractor computer networks, and the feeble response over the past decade to defend against such attacks. The attackers' goal is not to debilitate military networks, security experts say, but rather to steal classified design and engineering data about the United States' most advanced weapons systems, the article noted.

As if on cue, *The Wall Street Journal* reported just after the *Wharton Aerospace & Defense Report* article appeared that digital spies had infiltrated and stolen several terabytes of data related to the Pentagon's \$300 billion Joint Strike Fighter project. The spies, however, did not gain access to some of the most sensitive data, which was stored on systems not connected to the Internet.

The response to such attacks has been scatter-shot at best, but that might be changing as the new administration is instilling a greater sense of urgency. The Obama administration now plans to

create a new military command that would spearhead an effort to protect key computer networks from intrusion. Defense Secretary Robert Gates is "planning to make changes to our command structure to better reflect the increasing threat posed by cyber warfare," a Pentagon spokesman told the *Journal*. Gates plans to make cybersecurity a priority and the 2010 budget will include funds to hire hundreds more cybersecurity experts.

But critical systems could be left vulnerable while these new offices are established. In the meantime, a consortium of federal and defense agencies and private companies have compiled guidelines -- known as Consensus Audit Guidelines (CAG) -- that define the most critical security controls required to protect federal and defense industry systems. The CAG initiative is part of a larger effort led by the Center for Strategic and International Studies in Washington, D.C., to set up best practices for cybersecurity.

The 20 CAG-recommended guidelines include terminating dormant accounts, controlling who has access to systems (and at what level), and setting up boundary defenses. The guidelines can be found [here](#).

How exactly they will be implemented remains a critical issue, with companies worried about the complexity of working with new criteria. To answer this question, the *Wharton Aerospace and Defense Report* spoke with Matt Brown, the vice president for Information Assurance Services at Knowledge Consulting Group, who also spoke on this subject at the recent Cyber Security Conference & Expo in Washington, D.C.

*The Wharton Aerospace & Defense Report* asked Brown how agencies, defense contractors and other private companies should approach and implement the CAG guidelines.

**Wharton Aerospace & Defense Report:** How likely are defense contractors, or government agencies that deal with them, to really implement all 20 recommended guidelines? And if they don't implement all 20, how effective will the cybersecurity be?

**Matt Brown:** Companies are taking a look at the guidelines and using them as a way to kind of prioritize some of the areas of security they need to shore up. Whereas the Federal Information Security Management Act (FISMA) Implementation Project process provides the overall framework for certifying and accrediting the system, and identifying security controls, CAG is more targeted towards the controls needed to mitigate some of the most known and I guess the most highly effective exploitation techniques. So the way I see these guidelines being used, at least initially, is to help prioritize some of the things that CIOs look at as far as "where do I prioritize, what are my problems, where do I spend money and where do I reduce risks the most?" CAG provides the first set of, attack-based metrics that really reduce the technical security risk of the infrastructure, as opposed to the FISMA process which kind of goes through a very exhaustive approach at what data is on the system and what security controls are needed.

**Wharton Aerospace & Defense Report:** So these 20 guidelines all have varying importance based on the security various companies have set up already?

**Brown:** Correct. I think these 20 are great initial stab at the most important areas of focus. But they are very broad and an organization can look at where they have holes against these 20 and

focus some of their efforts where they have the most significant risk, as opposed to say the FISMA process, which has over 150 controls. The FISMA process doesn't really give you a tremendous amount of weighting of what controls and what threats produce the most risk to the infrastructure.

**Wharton Aerospace & Defense Report:** In terms of the order of the guidelines, is No. 1 the most important and No. 20 the least important? Is there a hierarchy to the list?

**Brown:** I don't read them that way. I don't read No. 1 is the most important and No. 15 or No. 16 is less important.

**Wharton Aerospace & Defense Report:** But when you do look at them, do you see some that are more important than others or would it just depend on a particular company's take on it?

**Brown:** I think it depends on the actual information that you are trying to protect and where your weaknesses may lie. I don't think you can broadly say that No. 3 is more important than No. 13 in every infrastructure. I think it really depends on the information that you are processing, the threat to that information, the business use of that information and what you currently have in place to protect that information and where you have holes.

**Wharton Aerospace & Defense Report:** What is it about our systems has made them more vulnerable to attacks?

**Brown:** From my experience application security has become a big area of concern because there are so many different pieces of an application now. And the protection of the data that is actually being processed by that application depends on a number of different things. I think application security is an important one but from a global perspective, if you look back at incidents that have occurred, they have exploited a number of different weaknesses to get to the end game -- that could be gaining control of the computer or access to the information. For example, someone may have used a phishing attack with a link involved in an email that looks legitimate, but if you look at the underlying e-track on the email it goes to some criminal site and that downloads a piece of malware and puts it on the machine. And they use that malware to go out and explore other machines and inspect other machines. I think that is becoming the bigger problem for security professionals. You can't look at it as, "I have a solution in place to fix phishing" or "I have a solution in place to fix malware." The attacks are becoming sophisticated or are using multiple techniques to get at the information. You really have to have a number of defenses in place to either prevent these from occurring or detect them when they do occur. The CAG is the first time, to my knowledge, that we have looked at how incidents are actually occurring and what these bad guys are actually doing, and how they are getting into the information network. Now the people who put the CAG together published their findings to help CIOs prioritize protection mechanisms.

**Wharton Aerospace & Defense Report:** Will companies be able to implement CAG internally or will they have to hire consultants?

**Brown:** It depends on the skill set of the people they have internally. There are some agencies in

federal government that have very, very skilled information security professionals in-house. But there are others for which information security is not their mission or forte and they bring in people from the outside to help them with these types of controls. And that is not just limited to the CAG -- it also includes the FISMA process. So it depends on the organization. I think the field of information security is maturing and the professionals that are in it are becoming more and more aware, and have more and more experience in this area, especially when you compare it to a couple of years ago. The sorts of certifications that are out there are better. People are identifying the need to become certified and show off that proficiency in the information security field by being qualified for this type of work.

**Wharton Aerospace & Defense Report:** Cybersecurity has always been considered akin to a cat-and-mouse game where the security companies come up with a defense, the hackers find a way around it. Is CAG a new insurmountable paradigm, or is this just another step in that back-and-forth?

**Brown:** I think it's another step in the back-and-forth. I think that we will always have the cat-and-mouse game because the hackers are continually looking at ways to get at the information. And the money behind it has become so great that they will always kind of be a step ahead of the people trying to protect the information. But, again, going back to the goal behind the CAG and how they came up with the guidelines: People actually studied the security incidents themselves and how these incidents have occurred -- how people are gaining access to the system -- and trying to put some controls in place that would have protected against those incidents. So instead of doing a governance approach towards identifying what's on the system and performing a risk assessment associated with the system, CAG actually is more targeted to how are these systems being attacked and how do we protect against those attacks.

**Wharton Aerospace & Defense Report:** Are you working with SANS (a Bethesda, Maryland-based research and educational organization devoted to security issues) on testing how effective the CAG is?

**Brown:** We, like everyone else. We are providing comment to these controls.

**Wharton Aerospace & Defense Report:** How are you working with customers to implement CAG?

**Brown:** We have had a number of customers that are looking at these as a way to kind of prioritize some of their efforts today. So, for instance, we're taking a look at how the SANS Institute has mapped the CAG controls to the controls of the NIST process. An organization today could look at which controls they are testing as part of their annual assessment for FISMA to make sure that, at the very minimum, all the controls that they are testing, all of the controls that are outlined in the CAG, are controls that they are testing against as part of FISMA. They can also look at these controls and determine which technologies they currently have in place to help them measure against these controls, and what they need to either purchase or put on a kind of wish list. And then also, we look at testing against these controls, [they need] to look at how they are currently being tested by the organization, and whether or not they are being tested via agencies or a scan, or whether or not they are being tested by an interview of the person or

something similar.

**Wharton Aerospace & Defense Report:** Do you see anything that needs improvement in this in these guidelines?

**Brown:** I have been more focused on what we can do with these today. What we do in terms of feedback is that we are answering some of the questions for our customers about what are these guidelines are and what can they can do with them.

**Wharton Aerospace & Defense Report:** What are your final thoughts about CAG?

**Brown:** I will just go back to the comment that these guidelines were built by looking at attacks that have occurred and what could have been done to protect against these attacks or to reduce risk in a way that's a little bit more targeted than in the past. So do I think it's a great kind of panacea? No, not a panacea, but it's a great way for us to prioritize risks and priorities where limited funding can go to reduce risks in the infrastructure in a way that they probably haven't in the past. I know that CIOs struggle with making funding decisions. I think these controls provide at least one way to help prioritize some of the funding decisions they have to make to help reduce risks. We'll never get risk to zero, but you can reduce risk in a targeted way.

