PowerTech
your security expert

FEATURE

Interview with an Auditor

Sabino Marquez—Senior Information Assurance Analyst, InfoSight, Inc.

The PowerTech Group, Inc.
www.powertech.com

TEL USA: 253.872.7788
TOLL FREE: 800.915.7700

In December 2009, Jill Martin, PowerTech Product Support Manager, interviewed Sabino Marquez, Senior Information Assurance Analyst at InfoSight, Inc., a Florida-based company whose mission is to help their customers identify security risks and meet compliance regulations. Sabino holds multiple professional certifications including Certified Business Continuity Professional (CBCP) awarded by DRI International, Certified Information Systems Auditor (CISA) awarded by the Information Systems Audit and Control Association (ISACA), and Certified Information Systems Security Professional (CISSP), awarded by the International Information Systems Security Certification Consortium (ISC)2.

Jill Martin: In the context of the current regulatory environment, how would you define "Information Assurance"?

Sabino Marquez: I often speak with my clients in terms that they would care about—and that is from their point of view. A bank or a financial institution only really cares about two or three things:

- They want to make sure that their information assets remain secured from unauthorized access.
- They want to make sure that any changes that they make to their systems or their business processes don't break any existing information security and compliance processes that they have in place.
- They want to do everything as cheaply as possible.

So, whenever I speak with customers about information assurance and how it affects them with their regulators, we always start from the standpoint of how we can achieve security goals, securing assets in a way that examiners would have no question, but at the same time really provide security. There's a big difference between meeting regulatory compliance for information security, and actually being secure.

You find that when many organizations implement the FFIEC [Federal Financial Institutions Examination Council] program, or the ISO standards, or whatnot, they implement the letter of the framework in their environment without taking into account what it is they're securing, what their security goals are, and if they are, in fact, secure. From a hacker standpoint, we can go into a bank or into an insurance company that has implemented a COBIT or an ISO security framework and we can hack them to bits in a matter of fifteen minutes. That's because they configured and tweaked their processes just enough to get a check mark on their audit checklist without really thinking about how what they're doing at the process-level interfaces with the large security program that they're trying to have in place.

JM: *So the goal in those cases is to secure for regulation and not necessarily for the purpose of securing their data.*

SM: And that's fine, because some customers really don't care if they're secure or not, they just want to pass the audit. For those customers, we'll help them pass the audit because that's what they want, but we tell them that just because they're passing the audit, it doesn't mean that they'll be safe from—I don't know—a fourteen-year-old Russian hacker.

Sabino Marquez
Senior Information Assurance Analyst
InfoSight, Inc.

INFOSIGHT
www.infosightinc.com
305-828-1003

There's a big difference between complying and defending. From a regulatory standpoint, information assurance is about making that choice. If you comply, you may not be safe; but if you defend against real actual threats, you're probably going to comply with the framework that's required of you. One of the reasons why customers don't always choose to defend against the attack is because of the cost factor. It's a bit more expensive to make information security and information assurance a part of the everyday process.

At that point, it's cultural and more money has to go into training, and they start to realize (by they, I mean management) that you can't just buy a firewall and say "Boom, we're secure from hackers." There's a lot that needs to be taken into account when dealing with securing your assets while still complying with everything you comply with.

JM: How has current regulation of finance and banking affected the way those sectors approach the areas of information assurance?

> "There's a big difference between meeting regulatory compliance for information security, and actually being secure."

SM: This question actually gets to the heart of what we were talking about earlier. You're familiar with Sarbanes-Oxley and GLBA and this myriad of other information-oriented legislation that's been passed that everyone has to comply with…

JM: *And more that's coming, right?*

SM: …coming down the pike, yes, because you've got high-tech coming from HIPAA and you've got the tweaks coming up in the spring of 2010 with the new financial revision coming in—so what you're getting is these huge, vague laws which the regulatory agencies then use to create guidelines, which are then pushed down to the customers that they're regulating. The problem with it is that legislatures and regulators are not, for the most part, criminals, so they can't really think of all the hundreds of thousands of ways to attack a company so you can steal their assets. So they create these large laws that are meant to be used by the regulators to cover everything that needs to be covered within existing regulatory frameworks, which then are expanded to meet the goals of the new regulations. So, if you have HIPAA, for example, and they implement all of the high-tech improvements to the law (which they have), now you have a larger set of guidelines under which you can expand your existing information security policies and procedures. What happens then is that it creates more work for auditors and examiners without necessarily increasing security of the customers.

JM: *Not necessarily creating that defense against the assets.*

SM: Exactly, the laws and the frameworks which resulted from them were more about accountability than defense, and that may be lost on a lot of non-technical or non-audit people. We see these big regulatory frameworks that come out that have the words "assurance," "security," or "compliance" in them. If you're not really knee-deep in this stuff every day, you might not really be aware that by implementing these frameworks, it doesn't necessarily secure you, it doesn't defend you. It'll make you comply with whatever check marks that the auditor has when they audit you, but it won't necessarily keep you what we call safe—as safe as possible.

There's an axiom in the hacker community that says "If it's plugged into a wall somewhere, we can get to it." That's not a joke; that works. If the customer was aware of how

many ways there are for an unauthorized party to access their information assets, they wouldn't sleep at night, like me. I spend most of my time at night, when I should be sleeping, studying tactics of what hackers are doing nowadays so that I can go back the next day to my customer and tell them what's going on: here's what the Chinese, the Russians, the Estonians, the Swiss—here's what the hacker community around the world is working on; here's what's succeeding in banks similar to yours; and here are the countermeasures we can use to defend. They ask if the countermeasures will help them to comply. Sometimes they will and sometimes they won't; sometimes the two are mutually exclusive, but most of the time they overlap pretty well.

JM: What impact do you think these statutory and regulatory compliance requirements have had on the manner in which companies operate?

SM: For the most part, the impact has been one of business culture. Now that you have all of these regulative verticals versed in the language of assurance, in the language of security, it makes it easier to walk into a bank and speak to them in a language they feel comfortable with. Before all these laws were passed and before these frameworks were taken seriously, it was difficult to walk into an organization and speak to them about how to secure their assets without sounding like you're talking ancient Greek.

"You start with seeing how you're doing the work: you model it on paper, you model it in Excel, and you train your people."

Now, everybody speaks the same language, everybody understands what a security process is, what an information assurance process is, what an internal information security policy is. They understand how important a policy is. They understand that you don't write a policy first and then hope your people follow it. You start with seeing how you're doing the work: you model it on paper, you model it in Excel, and you train your people. You have a culture of security and a culture of awareness, and it becomes easier to implement better security practices because everywhere the customer turns, they're bombarded with the same message: regulation, security, compliance, assurance. You can't turn your head any direction without being reminded how important it is to secure your information assets.

That's what I think is the biggest impact of the statutory and regulatory compliance requirement—customers are a lot more aware and they take it a lot more seriously, whereas before they were like, "we'll never get attacked" or "we have a firewall" or "that happens to the big banks and not us." So you get leadership to place dollar values on their information assets and make them see how disruptive not following the framework and not following the statute and not complying is. All of a sudden you're speaking their language. You're talking about dollars, impact of brands, loss of customers. You're talking about possible jail time for leadership for not doing their jobs or even having a modicum of shared responsibility. That's the biggest impact—the mind of the customer.

JM: What are some "best practices" for achieving and maintaining compliance with the myriad of regulations financial firms must now adhere to?

SM: Well, again the best practice begins in your head. First, you have to believe that you are threatened, that your assets are threatened. You have to believe that there is a risk that you will be compromised. Once you believe this, once you internalize the risk inherent to a potential attack, then you start to look at the frameworks and to pull the practices from there; because really, the frameworks are a collection of common sense, best practices, and goals to shoot for once you are where you want to be.

For example, I work with banks a lot, and they are required to follow the FFIEC work programs that are put out by the government. But the FFIEC is actually based on the ISO 27001 and the NIST standards, so when you look at those two standards, which is what the banks draw from, all you're finding is the collection of the best practices. Things like having a process in place to prevent unauthorized access to files that you're not supposed to have access to. If that's the best practice, at any given time, there's 7,000 people who want to show you solutions for that best practice.

So, start by looking at the framework and by recognizing that the information security frameworks—the ones that are independent of industries—all come from the same national standards, the same ISO standards, the same NIST standards. I have a spreadsheet that I use all the time, this little cheat sheet that shows you if the customer's attempting to follow a particular item from the ISO 27001, it also complies with this one from SOX, this one from GLBA, this one from PCI, this one from this and so on. And, you can show the customer that if they implement this particular best practice, they are now compliant with seven frameworks that any auditor will use to judge their security posture. So, for best practices, look toward the international standards and have a team—at least two people—compare the standards for yourselves so you can see that when you comply with one of the practices, you can actually comply with many.

> "For best practices, look toward the international standards... have a team compare the standards for yourselves."

JM: What are some of the most common missteps committed by firms as they prepare for compliance audits and reviews?

SM: The first misstep—and this happens so often I'm sorry to say it—is that compliance audits are not taken as the huge project that they really are. They'll push it off and push it off and wait until a month before the examiner comes, and then they'll do terrible because they've spent a sleepless month trying to come up with all the documentation and proof of compliance that the auditors are going to ask for. So the biggest one is waiting until the last minute. Successful companies that integrate information assurance programs into their daily corporate cultures do exactly that—it's part of their everyday work; the paperwork and compliance checks are part of their everyday work. When it's time for the auditors to come in, there's no work to do; they're just going to be observing your daily business process, of which security is a central part.

The second mistake is companies paying lip-service to compliance and assurance just for the purpose of passing the audit. This gets back to the original question of defending versus complying where you have a company with the correct mentality that says "we are at risk, we must defend." Companies that do not have that mindset are the ones that will fall into that particular trap—they don't take it seriously, they don't realize how big of a job it is, or they wait to the last minute. Then, the auditors and examiners will come into that particular business and "eat them for lunch," because they're not doing what they should be doing: defending information assets.

JM: What are some areas that auditors, examiners, and regulators are focusing on right now?

SM: It depends on the industry, and even substrata within the industry. I can tell you that within banking, the small cap banks right now are getting drilled a lot on whether or not they're complying with the letter of their policy. So, examiners will come in and ask for the information systems security policy, flip to random pages, and say "okay, section 10.5.7, show me evidence of how you're complying with this particular policy in your

handbook." This is causing some problems because a lot of customers will buy a pre-made security policy from some web site that says it will give the bank that check mark they're looking for. So, then the examiner comes in and asks if you have a policy and if you're doing what the policy says. That's when you don't pass because the policy isn't reflecting what you do; it's reflecting what you should do. Examiners are having a field day with that right now.

As for credit unions, which are a separately regulated entity than banks, I'm seeing a lot of focus on BCP [Business Continuity Planning] and DR [disaster recovery] from examiners and the credit unions that I've spoken to. In the last few months or so, I've heard about credit unions where the examiners have come in and they want to see the written disaster recovery plan, they want to see evidence of testing of the plan, and they want to see the board's involvement in revising the plan. They're really interested in making sure that the credit unions are disaster-ready and testing as such, so that it's part of their everyday business process. It's causing some challenges, really, because disaster testing is not part of the core business of banking, but again, keeping your customer's money safe is.

"The best thing to do to avoid complications... is to have knowledgeable, competent, proven people, accountable directly to leadership."

JM: *So, either in the case of a security policy, or in the case of a disaster recovery, the auditors are making sure that you're following those practices.*

SM: Yeah, they really want to see that you're doing what you say you're doing. As an aside, when an auditor or an examiner from FDIC or OGS or whatever your agency is, wants to go and audit a bank, they'll send out a notice two or three months ahead of time, so you have all this time to prepare for what's coming. They spend so much time preparing for the financial and the access side of the audit, that they forget to demonstrate how they're keeping access secure on systems and through processes, so that's where they really nail you.

JM: What are some issues that are most likely to complicate an audit or review of a firm's information assurance processes?

SM: This is going to sound harsh, but having unqualified or unprepared representatives for the institution to the examiner. The best thing to do to avoid complications—and this sounds like common sense—is to have knowledgeable, competent, proven people, accountable directly to leadership, in charge of assurance and all that that entails, as a full-time job.

The other big complication is that organizations become lax in their documentation procedures. When an examiner comes to an organization, they want to see proof in your work that things are being done the way that you're saying they're being done. The only way that you prove anything is if you have it in writing. If you make a change to the system, you have to document the change and you have to document the security testing you've done against that system to make sure that the change doesn't break the existing information security policy that you have. Then, you have to make sure that the board signs off on that change. It becomes this big chain of paperwork that oftentimes gets ignored because you make a change or an addition and business moves fast. You should have somebody whose explicit job responsibility is to document what's going on. When the examiner comes and asks for proof of 'X'—if you don't have written proof, they get annoyed.

JM: What are some resources firms can use to better implement an effective information assurance regime?

SM: They can hire me! I'll yell at them and tell them to do it right!

As I alluded to earlier, they can begin by looking at the accepted international information security and assurance frameworks. They can start looking at the ISO standards, the COBIT standards, and they can start to self-assess their existing information assurance environment against the best practices. Also, they can bring in outside firms who do nothing but assurance and security assessments. They'll go in and sit with a customer for as long as the customer will have them, and document their processes and compare them to best practices. They'll be able to find procedural security holes, as well as technical ones that they may not be aware of. It's always good to bring in the experts, especially if your line of business is not security.

I learned something from a very wise man about 10 years ago, who was a sort of outsource king. He believed in outsourcing everything. He had a certain logic that said if you have to do something for your company that is not part of your core competency and it's not going to make you money, then find someone to do that job for you and just focus your resources on making money for the company. So, if creating and maintaining disaster recovery plans does not increase a bank's bottom line, why are you going to have two or three guys on staff to do that for you? Bring in the experts; we do that all the time.

Same thing with the information security policy, audit, and awareness training. If you have somebody on staff who's an expert, use them; if you don't, find somebody and hire them; if you don't want to hire them, bring in the experts to help you. Those are some of the resources they can use.

Also, the biggest resource, now that I think about it, is training. Security is a people problem; it's a people problem and a people process. Assurance is only as good as your people's awareness of their role in the larger security program. Face it, workers want to make their bosses happy, they want to make their company successful, and the way to do that is by letting all workers know what is expected of them. When you expect them to be involved in a security information assurance program, they will rise to meet that challenge. Train your own people; if you don't want to train them, hire people who are experts at what they do. Confidence may not be enough to have that rich assurance culture that you're seeking.

"Security is a people problem; it's a people problem and a people process. Assurance is only as good as your people's awareness of their role in the larger security program."

JM: Any last comments before we finish?

SM: The world is full of bad guys, and if you were to spend an hour listening to how they talk, how they sell information that they've stolen from firms, and how they go about doing this, you would take this as seriously as I do. I'm surprised more people don't keep their money under their bed in a shoebox, knowing what we know.