

Convergence of Risk and Security – an Interview with Andreas Wuchner

Listen to Podcast [here](#).

Brian Contos: Welcome to the Imperva Security podcast. I'm Brian Contos, chief security strategist for Imperva. If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.

Joining me today is Andreas Wuchner. Andreas is an experienced IT manager, risk, compliance, and security professional who is globally acknowledged and a well-known thought leader who is a highly respected deliverer within the risk and security industry.

Andreas sits on advisory boards of the leading technology companies, including Microsoft, Oracle, Symantec, and Cisco. In addition to his role at a multinational pharmaceutical company Andreas operates the risk management blog ITRiskSpace.

Well, welcome to the show Andreas!

Andreas Wuchner: Thank you.

Brian Contos: So Andreas, today's topic, the convergence of risk management security, or more specifically, perhaps taking security beyond the technology and the bits and bytes, it's something that I think a lot of our listeners and just a lot of people in general have been trying to deal with as sort of security and risk have merged and evolved over the years.

From your point of view, what's the role that risk management security plays in a modern IT organization?

Andreas Wuchner: You know, I think the question is, "what are the people really used to?" Because most of the security and risk groups are coming out of this traditional IT point of view, so they are normally at home around technology and they have quite a hard time getting to the right tables to have a voice, to be a trusted partner.

If you think about a typical IT shop, what it needs, what kind of strategy elements and IT shop has then you very easily see; OK, you need talented people to run an IT shop. OK, you need some kind of governance to deal with what the customers want to have.

But at the end the primary building blocks of an IT organization are price leadership. "OK, how much money do I spend if it's worth, or is the hands and feet shop in India are cheaper, are they delivering the same service that I do?"

Yet the other side of the operation is integrity, that's where normally security is located, and risk management is in. Just keep the lights on and say availability of services are there and everything is fine. But you have also the whole innovation piece, that's really where value creation for the business happens.

Convergence of Risk and Security with Andreas Wuchner

And as most of the organizations around us are still focusing just on operation integrity, they very early on struggle already with cost leadership. "Yeah, OK, always fighting for budget." "Yeah, but this is best practice; we need to do that."

And very, very few of IT organizations and security organizations or risk groups are focusing on value creation. "What can we do to support the business, to do things which they normally cannot?"

I normally use a picture for it. I take a very nice sports car, sunset, beautiful looking. I ask the people, "Hey, guys, why are we putting big brakes in such a sports car?" And then you normally get the answer, "To be able to stop, not to kill people."

I turn it around normally saying, "hey look, that's alright, but the real reason is we want to allow the driver to go fast. We really want to go faster. And without big brakes they just cannot be going faster."

And that's the idea of risk management, allowing the business to do things which they cannot without knowing what they do.

Brian Contos: Let's try to get a concrete example in here. For example, let's take a technology like web application firewalls and the use for the business.

Can you give us some background on how you think that really plays out? Maybe talk about a business case and the various aspects about time to market, around usage of WAF and their possible role within-as you mention-the value of innovation?

Andreas Wuchner: Sure. Web application firewall. When this topic came up, the first reaction of most of the people was, "who needs another firewall? That's another kind of flavor. A little bit more yellow, or a little more spicy, more sexy, whatever it is." And most of the people just turned away from it without really having a closer look at it.

If you take a closer look at the business case on web application firewall and you go just beyond the pure technology stuff you'll say, "OK, look, if I am comparing a traditional firewall setup with all the testing of every system that you want to place in the traditional firewall setup you need to have the testing site somewhere, the production and all the effort which was needed to get the application up and running..." It's huge.

I'm not saying web application firewalls are the solution for everything, for every scenario, but the majority or a huge amount of systems could be placed behind a web application firewall, which would then fall into a direction to say, "You know what? Time to market this, maybe."

Forty percent of the original time, the cost if you say, "OK, I want to do this as a cost leadership initiative. I want to reduce costs." It's much cheaper because we don't need to have a double system in place somewhere which allows internal people to work on the internal data, the external people on the external data, and you need to figure out...

So, if you run, create and design for web application firewall from a pure IT technology point of view then it's "OK, good. It's another firewall."

If you put the business glasses on and you say, "OK, what is the value for me as a business shop for a data marketing organization, for example?" If you tell them, instead of, let's say, two months to get the application up and running we can do it now in 15 days? That's value for them.

Convergence of Risk and Security with Andreas Wuchner

And then the decision-"OK, it costs even less"-then becomes already a secondary topic because time to market is absolutely key for most of the marketing people.

Again, if you're maybe a financial institution and you're talking about top-notch critical data, maybe privacy values, you need to look at it, if your risk scenario, risk assessment still allows you to use it. But a lot of pages could be placed, or systems could be placed behind such a system. And then the business case for them be absolutely positive, and then it's no longer a pure technology discussion.

This is the kind of "yes, but" attitude, instead of saying: "No, no, no...It just doesn't fit to our technology or it's not on our standard list."

Brian Contos: You know, when we talk risk management, ultimately the conversation gets to making better more informed decisions more quickly. Maybe we could go through an example, dive into maybe, some of the recent activity of the Conficker worm.

What is some of the value that having transparency and visibility into these types of events? What is some of the real value that they can add to an organization by being able to monitor and detect and respond to these types of events?

Andreas Wuchner: I think in a lot of old style IT shops where security and risk management is more or less a cost element only. They haven't really recognized the values you just described. Because take the Conficker worm, for example; there was a huge hype in the Internet that, "OK, now, 1st of May... oh, everything will get dangerous; the return to hell..." and whatever.

But most of the organizations which sort of did their homework before and focused on the risks. And let's take a very precise example here; vulnerability management.

Very simple. Everyone says, "Yeah, I know what it is." But Microsoft deployed this patch for the Conficker worm already in October.

Every company which did their homework and looked at their situation before and checked their network, they had a clue and an understanding which amount of systems are patched; which are unpatched, and which of the unpatched are critical, and if there are ways to patch them.

Because there is a threat out there called Conficker worm, and there is a known vulnerability which was this Microsoft security hole in the operating system.

So, if there are real risks and if an organization had this mapped and could say, "look, out of my 6000 servers, I have 300 still unpatched." Out of these 300 are, three for example which are critical but they cannot be patched because they are legacy systems.

The provider of the application on top has not given me the green light to update, or the application just does not work with this patch anymore."

So for any good reasons they could have done preventive controls or built preventive controls around it. Or they could have said, "you know what? We may take the risk on patching it even if the application..." things like that. But with all these activities and risks and vulnerability management systems solution in place, they would have the possibility to take informed decisions.

Convergence of Risk and Security with Andreas Wuchner

Even going further, "you know what? First of May, that's too dangerous for me." I will just switch it off or I will just disconnect them from the network until I know something happens or not. But they would have known exactly what they do.

If you don't do this, if you just have the feeling, "my stomach tells me one-third of my organization is unpatched," how can you really take informed decisions and go back to the management and tell them, "You know what? Our status is amber, yellow, green, or red."

How can you do that if you don't have the knowledge about the details about the basic information of what your threat level really is? Vulnerability was clear.

The risk was completely unclear, because if you don't know the threat or if you don't know the amount of vulnerabilities around on your systems landscape, you cannot really give good answers and say: "OK, this is the risk for our organization."

Brian Contos: You know you raise some interesting points there and one of them is... or a question that adds on that is, rather: How important is the usage of tools within risk management in addition to or, instead of, specific processes or specific individuals that are trained? Where does that mix of people processes and technology really play into a risk management strategy?

Andreas Wuchner: If you look at risk management within IT, that is a very, very, very young discipline.

There are not a lot of experienced people in this space. If you compare, for example, with operation risk management, you know, where we have 100 of years of experienced people who are really, really well trained in doing things and to judge if this is high risk, medium risk, or what the financial impact may be; the likelihood.

These are all trained things for them.

But in IT, that is a very, very young discipline. And a lot of the things go wrong in IT because a lot of things are manual. So people are judging on around their feeling and saying, "Ah! Hmm...hmm...hmm!" And a lot of things are... you know, if two or three people looking at the same solution or the same designing scenarios, they may come up to a different report and say: "Yeah, this is high risk, or what it is all about."

I think there is huge possibility to gain profits, to gain also trust into risk management by using tools.

So if you look at the tools market for risk management, there are only a couple of tools out there right now.

I think there are four or five which you can say they are somehow mature. And if you look at for example at RSA Conference, there is always this innovation council: "What are the tops developments this year? What are the products? And what are the scenarios the companies are playing around to it which may get become a blockbuster," or whatever "later on."

This year there is also a company in there which is developing a tool for automated risk assessment or risk management. I looked at it, and I think it's a quite interesting approach, because they come now from a technology point of view but also from a business process point of view.

Convergence of Risk and Security with Andreas Wuchner

So they start with the business process and say, "OK, this is my sales process," and then they map to the sales process the systems, and to the system the data elements. So you get a clear mapping from, you know, which data elements supports which business process.

So suddenly you can go back to telling him, "You know what? Yeah, there this and this problem out there. You are phase process number one, two and five are affected by that, and the possible impact is X, Y, Z."

But this transparency in most of the organizations lacking today, if somebody had started and invested risk management, most of it is really on technology, but the link to the business process is not there. I'm really hoping that this company gets some momentum at the RSA conference. Let the people see, "hey look, what is it?"

You see that it's important for all the others, because if you look at the top security brand out there, which we all know, they have all bundled already with one of the other product which is out there. Because they have records that they cannot develop it by themselves, so they just buy it in from somewhere to integrate it in their own product suite.

I'm pretty sure, given another 12 months, maybe 18 months, this market will be much, much bigger than it is today and there is a big gain for organizations. So OK, If I have this much process already in the organization, let you a tool to automate many aspects of it and you get to reevaluate and get away from the feelings of people; really make it with people and make it based on facts and not on feelings.

Brian Contos: Andreas, you mentioned a 12 to 18 month outlook there. I'm wondering, with the new complexity that's being added to organizations. When I say complexity, I mean things like outsourcing challenges, cloud computing, trust-based models and things that we're not even considering right now. What do you see for the future right now? What kind of challenges are out there and what is going to require special attention?

Andreas Wuchner: Everyone who worked with me during the last 18 months knows that I'm absolutely an advocate for this whole trust model.

If we don't get into a position where we can separate good guys and bad guys, so we can say, "OK, Andreas Wuchner, at this point in the world, based on working on the system the trust and isn't this the kind of trust level compared to Andreas Wuchner sitting in Mumbai sitting in an Internet cafe, on a un-trusted system, get this kind of trust level, I think we'll never be able to win this race."

If you look at what cloud computing is all about. Now we're moving our services into whatever kind of cloud, my own cloud, an Internet cloud, or a cloud of another company. The collaboration is key and will be even more key in the future. The companies need to work together and collaborate; we have people from universities. Maybe even competitors working together to heed of the word on a specific thing.

We will need to start this trust idea. The other thing if it has trust around people and around location, we need to enlarge the trust offered to the data domain servers, the state of centricity, information centricity, from my point of view, will be absolutely key for success.

If I cannot prevent an specific data element which is important for me to flow somewhere, we will not be able to succeed either, because if you look at what digital rights management offers today, as long as I tell them this is critical and give them some passwords, the tools are able to prevent certain things.

Convergence of Risk and Security with Andreas Wuchner

But just to play around a little and to change it a little or just change some form words and suddenly the tools don't work anymore. So we are not there yet. It's still in its infancy. So there is another area of the state of centricity, together with the trust model, which we need to flow from a technology point of view.

From a management point of view, the whole outsourcing stuff gets more and more important all the time.

Especially if you take again, cloud computing into consideration. If I don't know where my provider of choice is hosting the data, if I don't know which change management processes they use. If I don't have security service level agreements with them, how can it ever get through an audit from the FDA or a financial tool auditor?

They will always come back to this government's pieces, they will need clarity on which processes I use. There, we don't have so much today, the maturity is not there and this is from a government point of view. This is the third big element for me which will need further attention and which will need focus and also some development from the organization.

The first two technology topics are somehow taken care of by the bigger and smaller IT shops, the whole government thing, I have the feeling that most of the companies are developing and reinventing the wheel once again, whenever it's needed. I would really love to see some more guidance and governance from the organizations out there; I don't want to mention any names yet at this point in time.

There are companies out there which help the industry to govern certain aspects of the outsourcing field. I think the development of practices in this space would help enormously. Every time I'm asking a provider, "do you have any kind of service level agreement around security?" You get all kinds of fancy answers, but nothing that you can really enforce and use.

Most of the time, you don't even get a clear understanding, "do you have to deal with processes?" Just face it, if you are in a company which has just two or three countries around the world, you already need global processes. If you do everywhere a local process, you just add complexity and complexity and complexity and resist the cost, then the price will go up.

Global processes are key for success, but if there are no global processes the whole thing will not really fly. Even the big outsourcing companies, the really big ones, most of the time don't have global processes. That's just a nightmare and pin point.

Brian Contos: Andreas, that was just fascinating information. Thanks so much for sharing some of your experiences and your perspectives on the industry.

Andreas Wuchner: You're welcome. My pleasure.

Brian Contos: If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.



North America Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

International Headquarters
125 Menachem Begin Street
Tel Aviv 67010
Israel
Tel: +972-3-684-0100
Fax: +972-3-684-0200