INTERVIEW WITH DAVID GRANT

Lindsey Green: Hello and welcome to the Biztech Report's Internet Radio. Hi, I'm Lindsey Green and today we present the next installment in our IT Solutions Series, Doing More With Less, sponsored by IBM. In today's report, we once again discuss the challenges IT managers are facing and explore the latest trends and approaches being used by leading edge organizations around the world to accomplish organizational objectives. Here to bring us another discussion on how organizations in today's economy are doing more with less is Biztech Report's editorial director, Lane Cooper.

Lane Cooper: Thank you, Lindsey. Application security, compliance scrutiny, along with the growing sophistication of the barrage of new threats that are facing IT managers today represent the major areas of concern for both the global 2000 in general and corporate America in particular. Here to help us understand the role the application security in particular and how it can be best managed is David Grant, who is Director of Security Solutions for IBM Rational and he brings over 12 years of experience in the software industry, organizing the strategy and developing ways to respond to these sorts of new issues. David, thanks for joining us today.

David Grant: Great, thanks for having me.

Lane Cooper: David, why don't we start by sort of breaking down what you think are some of the biggest misconceptions as well as sort of the things that people need to address and prioritize as they deal with new threats, especially to the applications.

David Grant: I think definitely by far and away is that I already have application security addressed. I have it covered. IT security's been around for a long time. People have been implementing firewalls, post security, network security, but unfortunately many times they fall under false security in feeling that they have the application level covered. Please step back for a second and define what we mean by application security, I think it will become apparent that today's traditional security measures are not covering the application layer.

So application security in a nutshell is essentially when an application is built and delivered via the web or some other mechanism, it has unintended functionality. And by unintended, I mean there's ways in the application that a malicious individual or a hacker, for better words, could actually exploit that application to get at the data in the back end. So to get the database, to get the

employee data or the sensitive customer data, and perform identity theft, which we're seeing in the news every day.

The problem is that the heavy side of the budgeting lately on IT security has been on the host or the network side. But we see the proliferation of applications in the world, social networking. We're all putting more on the web to drive more business via the web, self-service. Because we've been putting more to the web, we're seeing a lot more threats coming in via the web layer. Unfortunately, most applications are vulnerable. Developers themselves have not been trained on security, so they're delivering applications that they feel are on budget and on time and up to spec when it comes to requirements but they're not delivering secure applications.

They're also very easy to access. It's over the web. Hackers can get access to applications simply over the web. And according to IBM's X Force's most recent research from the end of 2008, over 50% of all vulnerabilities disclosed last year were related to the application layer. So I don't think there's any doubt that application security is one of the top threats, if not the top threat out there right now, and unfortunately, the biggest misconception is, most people think they have it covered with today's protection that they have in place, which unfortunately is not the case in most situations.

Lane Cooper: Well it sounds that there's sort of a legacy mentality still. As we move full speed ahead, I just read in a recent – I think there were two reports, one from Gardner and one from IBC, that suggest exactly what you were talking about. That software, the service, and these new web-delivered enterprise applications are one of the few growth areas as people tighten up the rest of their budgets. Are there particularly unique threats associated with that sector that people should be more aware of, and how should IT managers respond to that?

David Grant: Absolutely. So regardless of the reason why you're building web-based applications, whether it's for a cloud-based service or for enterprise applications as you mentioned, just by the nature of the applications being delivered via the web, they're more open to more individuals out in the world. So more people can get access to those applications, first and foremost. Secondly, because they're based on newer technologies, they typically haven't had the same amount of diligence put through them in terms of security best practices. For example, Noware, malicious software, has

become issue in the market where hackers will insert malicious code into an application. Unfortunately, the application owner doesn't even know that it's there.

A customer comes and visits that application, the piece of malicious software that's embedded in the application collects information about that customer, steals the information, and that company that owns that application and has deployed that application may never even have known that that was there and may never find out in the end either. So that's an example of one that we're seeing a lot more focus on and somewhere the customer should start looking at.

You also talk about other you know, web technologies like Web 2.0, whether it's Ajax Technologies or other Web 2.0 based application development environments. By their nature, they are meant to be more interactive. They want customers to be able to upload documents. They want them to be able to share ideas and social networks. And by that nature, you're actually allowing people to exercise an application like they've never been able to do before, therefore introducing new places where that application could be attacked as well. So definitely all of those things that you stated are leading to an increase in the amount of vulnerabilities that could potentially be out there for customers.

Lane Cooper: So, the next logical question would be what can we do about it? What are things that rank and file IT managers as well as the security teams, how can they coordinate, or what do you see as sort of an appropriate response that can address these threats rationally?

David Grant: Well first of all, when I talk about this problem, and especially if a customer is new to this problem, you first have got to understand the extent of the issue for your particular organization. So what is the risk? You know, security is all about balancing risk versus you know, investment, and this is not different. So understand the extent of the issue. How many applications do you have, what's the exposure of those applications, how sensitive is the data that you're collecting? How bad are those applications? Are they terribly vulnerable right now or are they actually pretty good? Are you doing the development of those applications in house, or are you actually outsourcing this? It leads to a whole other of scrutiny that you're going to need if you have an outsourced provider. You know, are you trusting them that they're going through the right security diligence. Make sure you get management, and more

importantly, application development management, involved in this process.

Don't try and go about it yourself in IT or security and not think that you're going to have to get development involved at some point. Train those developers, give them best practices, make sure those are captured. Equip those developers and people in the application development life cycle with products that can test those applications for security issues. Automate as much as you can. You want to move this back earlier in the process with automation so that you can make sure you're catching these problems before they go live. And then have metrics on improvement so that you can show people – we're seeing a lot of improvement from this investment that we're making here. We've gone from X percentage of our applications being vulnerable to a much better percentage.

And the biggest mistake I think people make, not only in this category but just in IT security in general, is they think that they can put a strategy reason for doing this in place with management. Well there's definitely in this case a lot of reasons why this makes a lot of sense to an organization outside of just the risk reduction piece of it. Of course you want to protect your customers and your organization from risks, but their return investment for doing what we've been discussing here is pretty significant.

First of all, highly quantifiable. You're probably already today already either using consultants to come in and do an ethical – what they call an ethical hack of your applications periodically, to test to make sure that they're not able to be penetrated. Well, if you automate some of that, you can save a lot of those consulting fees. If you catch these problems earlier, so in development or in the quality assurance stage of the application's life cycle, it's a lot cheaper to catch them earlier than to wait until they're already out in production, and then try and go back and retrofit those issues. It depends on the study you're looking at, but it's anywhere from $25 to catch a problem in development to $15,000 to catch one in production. So that's an obvious return on your investment.

More non-quantifiable, but I think it's pretty apparent that these are definite risks to an organization from a cost perspective, is the actual fines that are associated with compliance. For example, the payment card industry standard, or PCI, mandates that all organizations that collect credit card information follow strict guidelines for application security. If they find out that you're not

doing that, they can implement fines, they can implement restrictions. And the latest stats that I've seen is if you have a data breech, it's going to cost you somewhere around $200 per record that's in your database, and the average breech cost last year to an organization was 6.6 million dollars. That's the average cost if you have a breech in your organization.

So I think those are some of the things that IT managers need to make sure they're equipped with when they're going to make a decision around investing in this area. These are hard dollar savings, and there's also a lot of not as quantifiable but definitely hard hitting fines and other things that they have into consideration as well.

Lane Cooper: So there's sort of – there's a little bit of offense and lots of defense to take into account here as you make these investments. I'm curious though, David, it sounds like, especially when you when you talk about bringing IT security issues into the application development process, I know that it took a long time to do that with Quality Assurance. Do you think that people are embracing the idea of doing security checks at each stage in the development process? Is that something – is that an investment or is that a culture shift that you are seeing being embraced by large enterprises?

David Grant: Well you brought up a good point, and the good news for us in security, application security in particular, is that the path has been laid a little bit for us with quality testing. So you're right, it took a while before organizations got sophisticated for quality testing. Now what we're saying is, because of this proliferation of applications, because we're seeing a lot more for-profit hacking going on in the world, not just recreational hacking, I guess for lack of a better word, that we're starting to see a lot more pressure for security.

So why not just add into the current quality assurance process that you have, an ability to test those same applications you're testing for quality, let's now test them for security and compliance issues. It makes it a much easier process to just embed it in the current process that you have in place. Don't try and recreate the wheel here. You already had something in place you're working on with development and with QA, let's just add security and compliance as another leg of that stool. It makes it a lot easier to do it that way than just a bolt on process, that as you say, we're really going to have to do a culture change.

Now like anything, we're going to have to change some behaviors here, but in my experience, most application developers who are building these applications do not want to build applications that are insecure, it's just they haven't been trained or they haven't been told that it's a significant requirement to make sure this is part of the application development and delivery cycle. So it just takes a little bit of education there, but the payoff in the long run – hopefully I've been able to state just what those returns are, should easily pay for the investment you have to make in that area.

Lane Cooper: Outstanding. Are there any tools, are there any technologies that can be leveraged to sort of make this particular process easier to execute?

David Grant: Absolutely. So of course, I couldn't finish a podcast here without stating the product that I'm responsible for, and that is marketed and sold by IBM, market-leading product called Apscan, Rational Apscan, that actually embeds itself into the software development life cycle and tests for security and compliance issues automatically. So it can test for all the issues that we talked about earlier. It can be embedded in developer tools, quality assurance tools, or it can be used as a standalone IT or security product that can be used to analyze the application before it goes into production, or once its in production, depending on how the organization wants to use it, to test – to automatically test for the presence of these vulnerabilities that hackers could exploit. So that's, you know, one example of how IBM helps, but IBM has a very comprehensive end to end solution in this area of application security and Rational Apscan is just one of a complete solution set here.

We also have IBM ISS. For those that don't know, ISS is a leader in managed services and security and they have lots of service offerings around, coming in to help you understand how bad your applications could be in this area, help guide you on practices. They also have real time protection of applications so that once the applications have embedded through the system and are put out into the wild, they can actually impose some real time protection in place for those applications.

And then lastly we have access management and policy enforcement of those applications by our Tivoli family with the Tivoli Access Management product as well as a policy management product that lets you understand who's accessing

your applications, what they're doing with those applications, and whether or not they should be allowed to access certain pieces of those applications. So we feel like we are the only end-to-end provider of application security solutions in the marketplace today. We cover everything from embedding testing throughout the software development life cycle through to protection in production, and then of course, providing products to let you then manage who is accessing those applications and auditing with what they're doing with those applications.

Lane Cooper: Interesting. Now bottom line, David, it is possible to move into this you know, sort of brave new world of fast computing and fast delivery and developing sort of web-based relationships with so many consumers globally, it is possible to move forward in that direction with confidence from a security standpoint?

David Grant: Absolutely. Just make sure that we're embedded security and compliance into the culture of that shift, into the development process of that shift. You know, it's like any other change that we see in computing and IT, there's always going to be some security issues, but we've overcome them before, and there's no reason why this will be any different. It's just – it's happening a lot faster than some other shifts, so that's why we're seeing, you know, it be a little bit of an issue right now. But I have full confidence that we're going to get to a point where embedding this is part of the application delivery and development process, and that it becomes as seamless, as we mentioned earlier, as other practices that we've embedded into software development over the years. So I'm very confident that we'll be able to move ahead without issue.

Lane Cooper: Excellent. David, thanks so much for joining us today. It was an excellent conversation.

David Grant: Great, thanks for having me.

Lane Cooper: This issue, security, you can just see how it's sort of blending in with governance and risk management and all these other important issues about making business processes in general more accountable, more secure, more reliable. These issues and other related topics will continue to be discussed here at www.ibm.com/itsolutions. So come back to this page. We'll be having more podcasts to explore these and other issues, and David, hopefully we'll bring you back to take the next level look at this issue. This is Lane Cooper for Biztech Reports. Lindsey, back to you.

Lindsey Green: Thanks Lane. Today's Biztech Report podcast is sponsored by IBM, where the big blue team is working with clients to develop new business designs and technical architectures that enable the flexibility required to compete in today's economy and global landscape. For Biztech Reports, this is Lindsey Green.