INTERVIEW WITH EWA HOYT AND PATRICK VANDENBERG

Eric Green: Hello and welcome to a new podcast series from IBM software that explores the challenges IT managers and business professionals are facing today. I'm Eric Green and I'll be talking with a range of experts to discover new perspectives, approaches and examples that can help meet these challenges and introduce you to the capabilities of smarter software from IBM. So let's get started.

Welcome back to the show. Today we're going to be talking about application security with Eva Hoyt who is Global Go to Market Marketing Manager for Rational Security and Compliance with IBM and Patrick Vandenberg, Manager of Rational Security and Compliance Marketing, also with IBM. Eva, Patrick, thanks so much for joining us today.

Eva Hoyt: Thank you too.

Patrick Vandenberg: Thanks so much, Eric. Pleased to be here.

Eric Green: So Eva if we could please start with you. Could you please talk about this growing awareness and risk around application security and give our audience an idea of how significant this is?

Eva Hoyt: Sure, thank you. A number of vulnerabilities are factoring into those applications today, it's one of today's fastest growing security problems. So public data breaches are frequent, so it's really critical to secure those applications that collect sensitive data from employees, clients, or even you know partners. However, as organizations move even more toward business services online and adopt ____ 2.0 technologies, probably securing these applications sometimes gets postponed or ignored, increasing security risks. This is why practice application security should be a top priority on everybody's agenda. Because failing properly protect and secure applications can expose your organization to really malicious attacks. And application security absolutely needs to be a key element in the application development process and be integrated early in the development life cycle.

Eric Green: Thanks Eva. Patrick, what do you have to add there?

Patrick Vandenberg: Well, as Eva pointed out, this area of security, specifically application security is really prevalent today. You know, the IBM X Force research team, their latest 2010 report points out that half of all cyber security vulnerabilities comes from web applications

and you know, if we want to look at another source of information, the Verizon data breach investigations report found that I think 143 million records were compromised that year. And somewhere in the range of 90% of those records were compromised through web application attack pathway. Now those two stats are calling out web applications, but that's only one aspect of application security as a whole, but it does certainly point out the prevalence of these vulnerabilities and the amount of risks that it brings to organizations. And if we step back from that just a little bit, I think it's pretty easy to understand that today, you know, innovation is such a key agenda for organizations. It's necessary to be able to excel, provide the needed capabilities or opportunities that organizations are looking for, it's the type of enabler that is required in our society, whether it's you know, our communications that we're looking for.

So really software is a common thread in a lot of our daily lives, and not just in the IT security. And really how can we expect to be confident in these technologies and elements in our society if it's not secure? And in part because of the increasing adoption of different types of software, I mean if we look at our vehicles today, they are complex pieces of software, as much or more so than mechanical devices today. And, you know, that's another example of something today that we really need to be prudent and proactive around software security. So there is from all angles in all industries growing need to be aware of the risk around software and application security and this is something that, you know, we are seeing increasing awareness on the part of organizations, but unfortunately there is a bit of a gap between the amount of investment of focus on enabling capability, speaking to the functionality, than actually addressing the security alongside with that. And it's that gap in focus and investment that is bringing more and more risk to organizations today.

Eric Green: Excellent. Well thanks for that. The message of build it in keeps on coming to mind as you guys are talking through this. But to that, what's really been changing over the past let's say 12 to 18 months that's really made this a challenge for organizations?

Patrick Vandenberg: So I think, you know, that's a great question that I can continue my discussion on. The types of vulnerabilities for the most part stay - are still there. We aren't seeing, for example, a loss as a list of type vulnerabilities. And we are seeing those same vulnerabilities present in the security issues that we're seeing in the software today. But I guess what you could say what is changing is that the

recognition of the prevalence, for example, mobile applications, right. The mobile device market has certainly exploded in the past couple of years and that's getting an additional focus around, you know, applications and application security. We've obviously continued to see the continued deployment of web applications for even things if we want to look at enterprise modernization. So the process where an organization would be transitioning their legacy systems from mainframes and green screen functionality and leveraging web applications and web services to deliver that functionality in a more efficient and cost effective manner, reaching potential broader audiences with that as well.

We're talking about shifting from one paradigm to another. And as that action happens, well, there's a whole set of considerations around the security of that information. So, you know, that's one example where in an IT perspective, we are exposing more and more critical information that the organization needs to secure to external audiences, and certainly that's very problematic. And if we want to expand that discussion a little further, then we can start looking at product capabilities in certain industries.

Like the auto industry as an example. Right? So if we want to consider things today where, you know, we can insert a jump drive into a car to upload our music - to our moving software application if you will. Right? There's millions of lines of code in new cars today. So the very consideration of ensuring that that jump drive has no viruses that's going to be able to compromise the safety of the car. Or the remote connectivity, the wireless connectivity of these cars, if you will, from GPS, you know, or the proximity sensors that we have on these cars, ensuring that other devices cannot hijack and communicate to these vehicles, so that we can all be safe.

So we're starting to see the growing presence of software in our daily lives, and these activities, which are really all functionality demands by us the users, are demanding that the development community, whether it's in IT applications or products, you know, working on cars on the like, they continue to be pressed to provide this additional functionality. And if the security requirements and validation for delivering quality application software are not walking step for step with the functionality, this gap gets created. Essentially and security really in effect becomes deprioritized relative to the functionality. And this is where organizations run into problems where if there are vulnerabilities introduced into the applications or the products that they're providing, they're

introducing risk for their constituents as a result of that. So really, you know for the last 12 to 18 months, we're seeing a continued acceleration on the demands and the use of, as an example, web applications, where as I mentioned previously the BMX Force 2010 trend report, you know, we continue to see half of all cyber security vulnerabilities are from web applications alone. So the other half is from all the rest of the different types, you know, network, endpoint security, identity, data, all the different types of cyber security vulnerabilities that can exist are shared. so that is a tremendous, tremendous share of vulnerabilities in an area that still does not have enough attention to it And I mean attention from a mindset perspective, from a budget perspective.

Later last year, we were just starting to see application security being an IT budgeted line item to invest and protect the organization, whereas we know that IT security in general has been investing in network perimeter defense for quite some time now. And we're not here to say that that is a misuse of that spend, not by any stretch. There are a number of different ways where a rogue personality can try to attack an organization's assets. What we are saying, though, is that the biggest area of risk for the organizations is actually receiving the least amount of investment. And that problem is only going to create a bigger problem in the way of risk to the overall business, financially speaking, to the organizations that are, you know, not going to be adopting the right practices to try to close off those risks.

Eric Green: So you touched on some thoughts around the issues and functionality and added functionality when it comes to automotive and other places. I was hoping you could give us an example of how an organization is actually addressing this issue today.

Patrick Vandenberg: So how an organization is going about it really depends on their level of maturity or awareness in application security. And historically what we have seen is a progression. And we have referred to it as a customer maturity model. And it's not to disparage any customers that are earlier in the chain, it's more to point out that there is a progression of the amount of activity or the type of activity for this to happen. And it's unrealistic to expect an organization that is - such as a development shop - that is quite regimented and has some pretty stringent demands on it to overhaul itself, that's not a fair ask at all. So what is fair to ask is that there is a progression, there is a progression that will allow an organization to maintain and deliver against its existing mandate but also evolve to deliver, you know, secure, quality software. So

with that, what we see is an organization in an early state of awareness might be looking at a reactive approach to, for example, if we focus in on web applications. And they've identified some high risk applications, perhaps we're talking about financial services organization with online banking. That's a pretty widespread example that we can all relate to. They would want to have typically an outsource penetration testing firm who is going to do a security audit as well as applications to tell them where the risks are in that software and point out some steps to correct the code to remove those vulnerabilities from being exploited. And typically that's the right course because these organizations don't have the level of expertise and tooling in house to be able to deliver on that kind of a capability.

But as organizations realize this and they realize the widespread prevalence of vulnerabilities across their applications, they would undoubtedly look to dedicate a resource internally to be responsible for this and start investing in some tooling. What we typically see happen is, you know, there is one or two application security specialists that are designated. In large organizations, that number can grow, but typically you're looking at one or two. And for the organizations that start pushing through hundreds of applications that need to be validated by these one or two security auditors, there can be a bandwidth problem for sure. And while it's a significant positive step forward to actually bring that practice in house to have somebody validating it, the reality is that these vulnerabilities actually got introduced earlier in the process, typically by the development organization, and actually frequently inadvertently, because a lot of times, a vulnerability can manifest itself after all of the data is collected from the extended development team and put into a system. That's where we see edge case vulnerabilities appear.

You know, this isn't necessarily a case of where we're pointing at what a developer is or isn't doing, it's just the complex nature of the software that's being built today. So, with the development team inadvertently or not being able to address these vulnerabilities and we have these volumes of applications coming down this development process to frequently a single person whose got to test this, well we can see this bottleneck occur that can start to delay the deployment of these software projects, and that just isn't good for anybody. There's a lost opportunity for the organization so however long that software is now not in market there's an opportunity cost there. Additionally, there's the added cost of having the security auditor to say hey, this software is

presenting too much risk for the organization and according to my mandate, I cannot allow it to proceed. Mr. or Mrs. Developer, here are the issues that have identified here, can you please address these. Well, that piece of software now has to touch a lot of different hands, and there's an inherent cost in doing that. So how can we get past this? This is where the more proactive and strategic organizations can realize some tremendous cost efficiencies. They implement a practice, and this can be done again in a staged approach, to minimize the disruption and allow the development organization still to maintain a commitment to their existing mandates. But over time what we can do is push some of the security testing process earlier in the development cycle.

So let's say for example we can implement this at the build stage, right? So as that software is being checked in compiled, we're also doing an automated security scan of that software that is going to catch vulnerabilities and have those logged into the bug tracking system. And our developers can actually see this, remediate and have more secure code, and this alleviates the pipeline of vulnerabilities that will get to our security auditor downstream and allows that security auditor's expertise to come out. So instead of all of this time taking to find the same vulnerabilities over and over again, we can use this person's expertise to truly test the integrity of the system. So here's an example of where we can engage more resources in the system, be more cost effective at doing it, and in the end, provide quality software that meets the integrity standards we're looking for, that protects our constituents be it from a product, software product or an application.

Eva Hoyt: And I wanted just to add and maybe just kind of as a summary of Patrick what you said. In all detail, definitely the organization can reduce costs and mitigate the risk of internal and external threats by driving either security early in the application life cycle, you know, the design and development and then deliver the secure application from inception when it's cheaper to fix. But then also a lot of the organizations within different industries rely on secure data, if it's, you know, customer data, patient data, different kinds of data. And they are scanning all of those and those scans, you know, they analyze and this helps them to ensure compliance and accessibility and also they comply to industry regulations. And I think from looking at the whole life cycle from the start to the end when the organizations look at this as a whole they absolutely need to understand that it's not just a one stop fix and you have to apply

it in the whole life cycle so they can really see the benefits from a solution like that.

Eric Green: Excellent, excellent. So I guess turning back to you, Patrick, can you talk a little bit about where IBM is innovating with regards to app security?

Patrick Vandenberg: Sure absolutely. IBM has made some tremendous investments over the past few years in bringing in some quality technology from the Watchfire and Ounce acquisitions and really it's been much more than technology. The knowledge from the people in those two organizations has come together to form the Rational Application Security Business Unit. And what we've done here with these capabilities is been able to build our portfolio under the banner of Rational App Scan to provide several flavors of application security testing and remediation to support the different stakeholders as I mentioned earlier, the different stakeholders in the software development process.

So when an organization is ready to engage the QA organization, or build or development or even requirements, there are solutions in place that are designed to support that specific use case and environment as opposed to just push a technology or a tool there. So, you know, we can, for example, integration into Rational Application Developer development environment or an Eclipse environment or a .net environment, tying to the build process or integrating with Rational Quality Manager.

And supporting these capabilities within the existing user's environment is very, very important. Application security is, you know, it's a specialty area and we can't expect our development organizations to get up to speed here, but what we can do is enable a set of capabilities that tie to their existing environments that can be supported by a security admin working in the background that can provide the governance across and collaboration across it so that, you know, we can have confidence in the organization identifying these vulnerabilities and over time, improving the security posture of the applications or software that's being developed.

And across all of that, what we've been able to do if I dive into some of the buzzwords in technologies in this space is we have the capabilities of dynamic security analysis or testing as well as static analysis, those being looking at deployed applications that are functioning and/or looking at the source code. In concert, we have

several hybrid technologies that are merging, being able to merge dynamic and static analysis. And this way, we are able to provide greater efficiency, coverage and accuracy of the testing beyond what else can be found in the market. So whether it's supporting the use cases that are going to allow organizations to successfully adopt this or innovating on the technologies that are going to allow for improved efficiencies and accuracy in it, you know, I feel very fortunate to be in a business unit where IBM is investing to help our customers be quite successful.

Eric Green: Thank you very much for that, and thank you both so much for joining us today.

Eva Hoyt: Thank you.

Patrick Vandenberg: Thank you, happy to do this.

Eric Green: Thanks for listening. Please do visit IBM.com/software to connect with our experts, continue the conversation, and to learn more about smarter software from IBM. Let's build a smarter planet.