

Security

- [Home](#)
- [Business](#)
- [Hardware](#)
- [Software](#)
- [Security](#)
- [Internet](#)
- [Networking](#)
- [Gadgets](#)
- [Gaming](#)
- [Entertainment](#)
- [Science](#)
- [Misc](#)
- [Free Games](#)

[Science News](#)

[Internet Security](#)

[Password Manac](#)

[Virus Protection](#)

[Research Papers](#)

[Solar Energy](#)

GO

Q&A: Gwyn Fisher of Klocwork

by Steve Ragan - Aug 15 2008, 17:28

The Klocwork logo is displayed in a bold, blue, sans-serif font.

Gwyn Fisher of Klocwork sits down with The Tech Herald for a chat.

- [Email](#)
- [RSS](#)
- [Comment](#)
- [Facebook](#)
- [Twitter](#)
- [Digg](#)
- [FARK](#)
- [Slashdot](#)

The Tech Herald recently got a chance to talk to Gwyn Fisher of Klocwork. Fisher has over twenty years of technology experience under his belt, and is currently the CTO of Klocwork. As with all of our recent Q&A articles, The Tech Herald allows vendors to add commentary, as well as allowing them a chance to speak out. Last month, The Tech Herald held a one-on-one with Barmak Meftah of Fortify [Software](#). After that article was posted, Gwyn took the time to cover some of the same questions and topics.

[Note: Klocwork is a competitor of Fortify Software, both have been in business for a long time, and both are known for their compliance and auditing tools. This Q&A is not a direct mirror of the Fortify Q&A, but covers the same general topic; that is, it covers compliance, auditing and PCI-related information and opinions. Klocwork has had no coverage or contact by The Tech Herald prior to this interview. The interview took place after Klocwork read the Fortify Q&A and asked if it too could comment. Because of the open nature of the Q&A format on The Tech Herald Klocwork was naturally allowed to respond.]

The Tech Herald (TTH): PCI Compliance saw a lot of news coverage around the June 30 6.6 deadline. What's your take on PCI? Why is PCI compliance so hard, and if it is not that hard, why are there so many companies that fail to comply?

Gwyn Fisher (GF): PCI in general, and 6.6 in particular, are good steps forward in terms of recommending some best practices, but as with many of the various standards related to software development and validation – whether security, safety or other types of standards – the recommendations tend to be pretty high-level. So, from that perspective, 6.6 isn't hard – it's actually quite straightforward in that it provides an over-arching best-practices framework to follow, but the challenge for organizations is taking that guidance and translating it into a set of concrete changes that involve new processes or tools. This takes time.

Even 6.6 provides three complementary, but very different approaches to address application security. Many organizations are trying to figure out not only what technology mix to deploy, but how they need to change their approach to application development in order to address the compliance requirements outlined in PCI 6.6. As with any standards or regulatory compliance effort, new tools are the least of the problem, of course. New processes and new oversight, however, take time and significant effort, not just once but on an ongoing and rigorous basis.

TTH: Are there things in the PCI compliance rules that you would want changed or think need more attention?

GF: From a regulatory standpoint, I think PCI probably serves its purpose. These regulations are really just designed to provide a basic framework and high level guidance. Each individual organization is left to figure out how best to address software security, privacy or even safety concerns within that framework though. It's a fine line between telling a company exactly what they have to do, and advising them of what's acceptable on a broad industry basis. PCI DSS is obviously much more aimed at the latter intent, and as such has the short-comings of any such advisory regulation.

Leaving intent up to the individual invites compromise, and while it's obvious that nobody ever wants their name to land up on a document that not only states "thou shalt..." but then turns out to be either short-sighted or just flat-out wrong, it's perhaps disappointing that PCI DSS is so hand-waving in regard to what financially exposed institutions must actually do. I would personally like to see more detailed instruction and less "do something like..." guidance.

TTH: You launched Klocwork Insight in January 2008. As a product, it helps with compliance on section 6.6. Why do you think this section went from a suggested step to a required step?

GF: You can't create secure applications if you don't build security in, right from the source code on up. The industry is recognizing this, which is why various approaches to software security are now being mandated – it's that simple.

TTH: Briefly, tell our readers about Klocwork Insight.

GF: Klocwork Insight is a source code analysis tool that uses static analysis technology to identify weaknesses in source code – these can include security vulnerabilities, programming bugs, along with a variety of architectural and maintainability issues. Uniquely, Insight gives software developers the ability to run accurate, effective analysis right at their desktop, before they check-in their code. This capability empowers developers to write more secure code early in the development process rather than receiving downstream audit reports that are costly and inefficient to act on in a timely manner.

TTH: As a vendor that helps businesses meet compliance regulations yourself, what are some of the more common problems you see with your customers when you first go in to help them?

GF: Most organizations we talk to are trying to figure out how to build more secure software without just wrapping some sort of downstream audit process around their current development lifecycle. They recognize that getting developers to begin writing more secure code involves some level of developer education but most of all giving them the capability to address these issues as part of their regular development routine rather than having to receive audit reports from somebody else.

Ultimately, Klocwork provides a solution that's a piece of the puzzle, and it's all about applying the right technology at the right stage in your development process – attempting to audit your source code later on in the development cycle just doesn't make sense if that's all you've got. Auditing as an adjunct to developer-facing analysis does make sense, and we're seeing more and more institutions taking advantage of Insight at both ends of the spectrum as a holistic solution.

TTH: Without naming the client, think of the one place you helped that needed the most work implementing a tool like Klocwork Insight. What issues was the client facing?

GF: Twenty-seven million lines of code that needed to be analyzed with our tool in one run, and a build system that nobody had touched in years - say no more.

TTH: This relates to the previous question somewhat. Tell us a battle story from the field. Has there been one company you worked with, or specific issue that you helped to resolve that at first left you wanting to scream or just laugh and walk away?

GF: There's a funny story with a customer that will remain nameless, but was trying to understand the capabilities of our tool and wasn't really familiar with static analysis, the kinds of analysis it does and doesn't perform.

After a bit of frustration, the customer stated, "Look, just give me a list of all the defects your tool cannot find!" Our response was, "Well, that could be a pretty big list - it might be easier if we just tell you what we look for, the depth of our analysis, and from that you can identify what's not on that list that might be important to you".

While this example is a bit comical, it is also instructive to our discussion – there is no silver bullet to any of these problems. Organizations need to find the right mix of tools and processes, used at different stages of the software lifecycle, to reduce their risk and exposure. No one tool will solve every aspect of software security... and no we don't keep a running list of everything "we don't do".

TTH: The concepts of software security and software quality have been getting more and more mainstream attention recently. What do you see happening to cause this change?

GF: It comes down to awareness. There have been some pretty high profile advocates to help educate the market on the importance of writing more secure code – everybody from Michael Howard at Microsoft to people like Gary McGraw. Beyond that sort of advocacy, however, it's probably just an observation on the obvious: if current approaches to security are completely effective, why are there still so many applications being deployed that are not secure?

TTH: Now, here's the hard question. Tell our readers about two companies they can check out and compare your solution to. Another way to phrase this would be to name your two biggest competitors in the field.

GF: Fortify Software and Ounce Labs are both strong players in this field with good solutions. They take a different approach to the problem since both of their solutions focus more on delivering an audit capability to security teams rather than a developer-enablement tool that allows developers to run accurate, effective analysis at their desktop.

We come from a software development tools background, so our focus from the outset has been enabling developers rather than delivering another audit tool to a security manager's already overflowing kit bag.

TTH: Let's talk about Klocwork as a company. Klocwork was recently named to the 'SD Times 100' list and also received an Editor's Choice Award from VME and Critical Systems. With so much competition in the source code analysis field, how do you stay cutting edge?

GF: Great customers and a smart research team. No matter how good your technology "smarts" are, without the ability to exercise your products against a huge volume of diverse code bases and capture feedback from people familiar with that code, the technology will struggle to meet its full potential. This is the kind of technology that you can't just sit back and engineer in a lab – it needs broad and deep exposure to a variety of code bases, software build systems, and development environments. That kind of technology maturity only comes from years of working with software development teams.

TTH: What vendors do you deal with on a day-to-day basis? What compliance regulations do you have to deal with, and how do you do this?

GF: Much like any software development organization, we live and die by the tools we use and processes we instill and adhere to. We use a pretty aggressive Agile development method within R&D, so we interact with the major tools, both open source and commercial, that you'd expect. Obviously, being the provider of our own tool set, we've done a thorough job of integrating Insight within frameworks like Cruise Control and within the many and varied IDEs that our developers use.

As for our compliance regulations, we tend to impose stronger rules on ourselves than any compliance mandate out there. All of our code and finished products undergo rigorous and continuous security analysis as part of the regular development process.

TTH: What is the security policy like at Klocwork? Do you use Klocwork Insight internally on your own software?

GF: We use our own software, of course, as a matter of rigorous practice. Each developer in our distributed organization is responsible for checking in code that is clean, that is functional and that is free of vulnerabilities. We use a variety of tools to help the developers achieve this aim, of course, but Insight provides the cornerstone. In terms of downstream audit and oversight, we then use Insight from a management level to keep track of code stream activity and the aggregate security and quality of the churn that occurs each day. Needless to say, there are good days and bad days, but as a trend line, we can now trace our overall improvement in time and show how our code has not only achieved its current level of security and quality, but also that it maintains that level day by day.

TTH: Final thoughts. Name five things companies must know about a secure coding policy and why?

GF:

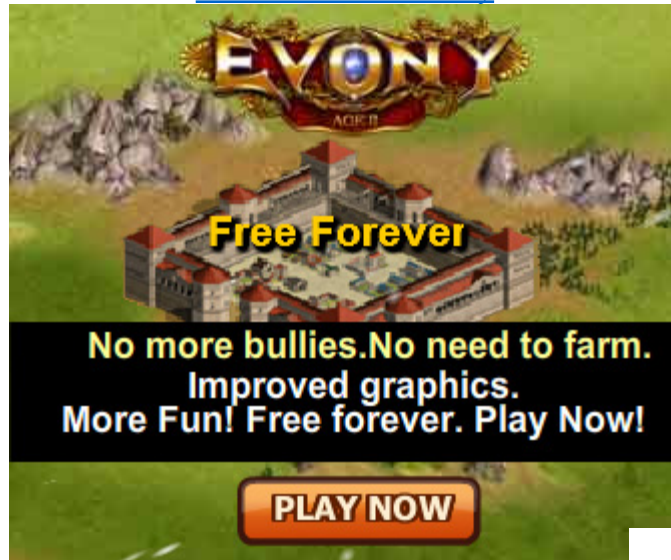
Get the developers on board.

Don't just audit.

Build security in.

Measure your progress.
...oh, and get developers on board

[Comment on this Story](#)




- [Email](#)
- [RSS](#)
- [Comment](#)
- [Facebook](#)
- [Twitter](#)
- [Digg](#)
- [FARK](#)
- [Slashdot](#)

Interested in a more interactive TTH? Join our [Facebook Group](#)
Want regular updates from The Tech Herald? [Follow us on Twitter](#)

Comment on this Story

Echo 0 Items

[Admin](#)

	Login	Your name here...
	Share	This Page
What's on your mind... <div style="border: 1px solid #ccc; height: 80px; margin-top: 5px;"></div>		
Follow	<input type="button" value="Cancel"/>	<input type="button" value="Post"/>

[Leaked: Dell's new Thunder, Flash and Smoke](#)
[Dell's leaked Lightning is truly electric](#)

Latest Articles on Monsters&Critics

[Clinton backs engagement with Syria despite weapons concerns](#)
[Aqaba blast caused by Grad missile, says Jordan \(3rd Roundup\)](#)
[New Sex and the City book reveals Carrie Bradshaw's teen years](#)
[Eccentric send-off for Malcolm McLaren](#)
[Zoellick pushes for changes as emerging powers fuel growth \(Roundup\)](#)

In The Tech Herald

[Home](#)
[Hardware](#)
[Software](#)
[Security](#)
[Internet](#)
[Networking](#)
[Gadgets](#)
[Entertainment](#)
[Science](#)
[Current Affairs](#)

Other Languages and Sites

[Monsters and Critics](#)
[Deutschland \(Monsters and Critics\)](#)
[Free Games Herald](#)

Site

[About Us](#)
[Contact Us](#)
[The Team](#)
[RSS Feeds](#)
[Privacy](#)

The Fine Print

© 2008 - 2009 The Tech Herald.com, WOTR Limited. All photos are copyright their respective owners and are used under license or with permission. The Tech Herald cannot be held responsible for the content on other Web Sites.

Servers supplied by [Servint](#)

BRASH Publisher Network