SANS Ask The Expert User 2004 Series

What Works In Information Security: Automated Security Audits and Remediation

Volume 1. No. 3

April 15, 2004

The Expert

Paul Simmonds is Global Information Security Director at the ICI Group. Paul joined ICI in 2001 when he was recruited to head up Information Security for ICI, headquartered in the U.K. Prior to joining ICI he spent a short time with a high security European web hosting company as Head of Information Security, and before that seven years with Motorola, again in a global information security role. Paul has a degree in Electronic Engineering and qualifications in Radio Communication. He came to the Information Security field in 1993 from a background in IT Systems Implementation and consultancy.

The Enterprise

ICI is an $11 billion global company with 35,000 employees producing specialty products and paints with 50,000 products and ingredients developed for a wide range of consumer and industrial markets.

The Business Problem

As a giant distributed global business, ICI needed to ensure security of its mostly outsourced network infrastructure. Regular security audits would fuel this effort but manual vulnerability assessments were too slow, incomplete and not up to securing more than 400 web sites operated by suppliers. ICI solved its problem by using an automated 3rd party Web service to audit suppliers and enforce remediation. In one 22 week period last year, ICI eliminated the most severe vulnerabilities and cut two-thirds of the minor vulnerabilities in its global outsourced network.

The Interview

SANS: What was the principal concern that led you to look for a vulnerability remediation program?

PS: We have a lot of web sites and many of them are outsourced or hosted by third parties. We simply did not know how much risk we were facing because we did not know how well those sites were being protected.

SANS: Did you do anything to test their security?

PS: We hired a penetration testing firm to test our five prime business sites — the ones that hosted our most visible domain names. They were able to deface three of the five sites. The defacements were very subtle and beautifully done; no visitor would have noticed the changes.

SANS: Three out of five is a big number and those are your prime sites. What did the folks running the sites say about the successful tests?

PS: I remember on one of the sites, we were also paying for site change monitoring. We waited two weeks after the defacement to tell them, and when we did, the sales folks said, “That’s impossible.” But they sent their technical people in and we showed them how the penetration had been accomplished and they said, “You’ve got us. You are right.”

SANS: Did you use the penetration testing data to help justify your investment in your perimeter vulnerability remediation program?

PS: Yes. In fact, we scheduled the tests to be completed just before the budgeting period for 2003, so that if we found problems we would have recent information to explain to our management why vulnerability remediation should be implemented. We looked at doing it ourselves using free software like Nmap and Nessus, and put out a request for quotes with a big wish list knowing we were not going to get everything we needed. We asked five vendors to propose solutions.

Seven Critical Security Technologies For 2004

1. Vulnerability Monitoring and Remediation
2. Automated Patch Management
3. Identity Management and Tokens
4. Deep Packet Inspection Firewalls
5. Intrusion Prevention
6. Email Security
7. Security Compliance (Quarantine) Gateways

Seven new key defenses are being used by security-savvy organizations. The SANS “Ask the Expert User” series will help you plan for these improvements by taking you inside organizations that have implemented the new defenses and posing the questions you might have asked. We complement each of these interviews with an online “Ask the Expert User” webcast in which you may ask follow-up questions. To get weekly updates in security news and an invitation to the “Ask the Expert Webcast Series,” email info@sans.org with the subject “Ask The Expert Users.”

SANS: Did you find the least expensive one was also the least effective?

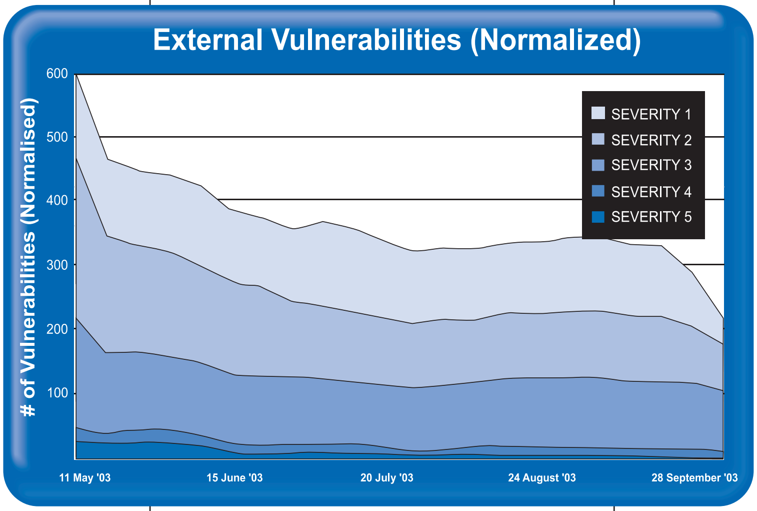
PS: Actually we did not. One of the lower bids actually offered more than any of the others.

SANS: Wasn't the free software approach less expensive than any of the commercial solutions?

PS: The free software approach was far more expensive in an organization our size — hiring people, building hardware and software facilities, keeping all the vulnerability signatures up to date, defining how to resolve each problem, setting up systems that monitor progress in correcting each important vulnerability, and most important of all, distributing the data automatically to each of the people who need it. Add up the costs of all that and you'll find the free software is a tiny part of the total equation.

SANS: Before we look at the way you solved the problem, can you share with us any data that proves that the solution you chose actually worked?

PS: I'll give you a graph from last summer and then tell you where we are now:



As you can see from the graph, we systematically brought the vulnerabilities down - especially what we call the 4s and 5s which are the most critical vulnerabilities. In the last few months of 2003, we have completely eliminated all the 4s and 5s and we're very close to eliminating all the 3s as well. We had set a goal for 2003 to get our borders secure, and our 2003 penetration test has confirmed the progress we have made.

SANS: I notice a definite dip in vulnerabilities toward the end of the period covered by the graph. What happened?

PS: We moved some of our sites from a hosting company that was being unresponsive about security to another hosting company.

Remember, our target was our border, so testing it from outside the company was actually better than testing it from inside.

SANS: Your progress is very impressive, especially with 400 web sites managed by a lot of different people. What was it about the solution you chose that made it stand out from the others?

PS: There were two keys. First, it was really easy to implement and second, the risk of implementation was very low.

SANS: When you talk about ease of implementation, how easy was it?

PS: It took only two hours on a Thursday afternoon. That's all.

SANS: How did you do it?

PS: We used a Web services solution. Remember, our target was our border, so testing it from outside the company was actually better than testing it from inside. The Web service approach has several benefits for us: (1) the company keeps the signatures up to date and they cannot slack off because they are testing hundreds of thousands of systems every day, (2) we were able to get up and operating in just a few minutes — no hardware to buy, no software to install and debug, no training programs to attend.

SANS: What proved to you that it was the right decision?

PS: We invited the vendor to come to our conference room and we opened up a web browser on my computer and displayed it on the big screen for all our security people at headquarters. We projected the same picture to all our security officers around the world. The vendor started scanning our systems and showed the results on my browser — securely. Everyone could see the results, the format for delivery, and the information they provided on how to fix the problems. And best of all, we decided that if we tried it for a year and didn't like it, we'll still have learned more of what we want and don't want, and then we can get rid of it because there was no ICI investment in people or hardware. But based on our first year of experience we've just renewed for this year.

SANS: How often do you scan for vulnerabilities?

PS: We scan every single web site, firewall, business partner connection, and router that has ICI Intellectual Property behind it, and we do this every week. We run scans on Sundays.

SANS: Why on Sundays?

PS: Because the companies that supply our hosting services often make configuration changes on Saturday and Saturday night. We pick it up earliest if we scan on Sunday.

SANS: Has that schedule proven itself effective?

PS: Definitely. I remember one time when we called up a hosting organization on Monday morning and asked them what they changed. The sales people told us they had not changed anything. Then they went and checked with the techies and called back sheepishly saying that they had made changes and would be fixing the security problem immediately. One of the big benefits of the system we have is that we can share the data automatically with the people responsible for hosting our sites. Our goal is to ensure our systems are secure, not to catch them making security mistakes.

> One of the big benefits of the system we have is that we can share the data automatically with the people responsible for hosting our sites.

SANS: You seem to be scanning your borders effectively. What about your internal systems?

PS: Our goal for 2003 was to secure the border. Our goal for 2004 is to secure the internal systems. We'll be issuing an RFP for internal scanning in April.

SANS: Since the current vendor is using a web service approach, they wouldn't be eligible for selection as the vendor for internal scanning, so how will you choose?

PS: The current vendor has an internal solution with appliances that feed the data and distribute it. So they will be included with other vendors in the evaluation.

SANS: What new criteria comes up for internal systems?

PS: One of the keys will be information distribution effectiveness. We have overlapping groups responsible for machines, and they each need to get the data for systems they oversee but not the data about any other systems. We're going to be looking very closely at how well the competing vendors do that job.

SANS: How has the customer service been?

PS: It's quite remarkable. We have a cellphone company in the UK called Virgin Mobile run by a fellow named Branson, and he makes sure that every customer is given great customer service. Our vendor has done an amazing job of being just as good at customer service as Virgin. Calls are returned almost immediately, usually with a statement something like "it's done." And last fall I made a suggestion to one of their engineers for a new feature that highlights changes when it sends out emails. A few days ago I got an unsolicited call from customer service telling me that feature is in the version that is coming out in a couple weeks.

SANS: Any last thoughts for people evaluating vulnerability remediation systems?

PS: We have had good success starting by focusing the technical people on a small number of vulnerabilities and then expanding the number as they get better and better. I would suggest that asking people to fix all the high, medium, and low risk problems is counter productive.

SANS: Thank you very much, Paul. This has been illuminating and valuable. We are looking forward to hosting you on the "Ask The Experts" web broadcast so readers can follow up with their other questions.

Why ICI Chose A Web Service

- ***Low risk investment***
- ***Easy to use; no new infrastructure for deployment***
- ***Provides management and control of chaotic supplier situation***
- ***It works***

About the Web Service used by ICI

QualysGuard from Qualys, Inc.

- ***On demand, automated network security audits and vulnerability management***
- ***Distributed, scalable solution with no software to install, update, or maintain***
- ***Accurate vulnerability detection eliminates manual verification and consolidation of data***
- ***Award-winning solution used by 1,300+ enterprises worldwide***
- ***Free trial available at www.qualys.com***