QUALYS
SECURITY ON-DEMAND

CASE STUDY: Imperial Chemical Industries PLC — Enforcing Security SLAs of Outsourcers

Company
Imperial Chemical Industries (ICI)
20 Manchester Square
London W1U 3AN

Company Profile
Specialty products and paints with over 50,000 products and ingredients developed for a wide range of consumer and industrial markets. ICI employs over 35,000 people worldwide and had £5.8 billion in 2003 revenue (US $11 billion).

Business Objective
Centralized view of network security with focus on ensuring safety of both internal and outsourced infrastructure.

ICI Group was founded in 1926 and grew into a giant international chemicals firm based in the UK. The company recently finished a six-year business transformation, divesting more than 50 subsidiaries largely focused on commodity industrial chemicals. The “new” ICI has a strong consumer twist: it creates, develops and markets products that make the world look brighter, taste fresher, smell sweeter and feel smoother. While invisible to most consumers, ICI is a powerhouse global player for customers that sell paints and make foods, fragrances and personal care products used by people every day.

The new ICI Group is comprised of four international businesses—National Starch and Chemical Company, Quest International, Uniqema, and ICI Paints—plus the Regional & Industrial Group of businesses serving India, Pakistan and Argentina.

Its business transformation created two major challenges for ICI Group’s information security. Consultants advising ICI on transformation strategy noted the company’s heightened reliance of multiple businesses on one shared network. The company’s 400 web addresses were targets for Internet-born attacks on data, applications and the corporate identity. Another elusive issue was diversified responsibility because ICI outsources most of its IT operations.

To address these issues and augment information security, ICI Group hired Paul Simmonds to fill the new role of Global Information Security Director.

Technology Hurdles

Simmonds says the first priority was getting a clear, accurate picture of what ICI devices were exposed to attacks. “Your inventory system will say there are 25,000 PCs, 6,000 servers, and various control equipment in place, but broad images like these are not enough for ensuring strong security,” he says. “Intelligent decisions for security management require precise details for every attached system. If you can’t measure security, you can’t manage it.”

At the time, precise security information was hard to come by for ICI, which followed common strategies: do an annual penetration test, check security settings upon implementation of new hosts, and rely on service level agreements with third-party IT providers to find and fix vulnerabilities.

Those static measures did not provide enough useful information because ICI’s infrastructure was fluid, changing even on an hourly basis. “You’ll never catch it all in a huge organization,” says Simmonds, “but you must get close.” The mandate for better security was urgent, for ICI was able to subtly deface some of its own web sites during a routine penetration test.

The ICI Story

Business Problem

Giant distributed global business needed to ensure security of its mostly outsourced network infrastructure.

Technology Hurdle

Auditing the security of network and hosts on demand when most of IT was outsourced globally to 3rd party suppliers.

Solution

Used a 3rd party web service from Qualys to automatically find vulnerabilities in outsourced IT and provide remediation management to each supplier.

Simmonds' group issued a request for quote and did a two-month evaluation of five network mapping, vulnerability analysis and remediation management solutions. To reflect real needs, tests probed the security of ICI's own external-facing hosts. "We short listed Qualys as the winner based on best value for the money combined with overall performance," Simmonds says.

Fast Implementation With QualysGuard Web Service

ICI was surprised by the speed of implementing the QualysGuard Enterprise web service. "We sat down on a Thursday afternoon at 2:00 p.m. and finished by 4:00 p.m.," says Simmonds. The two-hour setup enabled ICI to immediately scan security on all outsourced network infrastructure, including all of ICI's 3rd party global suppliers. "The Qualys web service worked right away," Simmonds reports.

The nearly instant installation was a byproduct of Qualys' web services architecture. The only thing customers need to use the web service is a standard web browser. "This is a rare thing when products or services work this well out of the box," says Simmonds. "Not many security or IT products do this."

Scanning the infrastructure used in 3rd party networking services was a crucial step in ICI's new security strategy. To compliment scanning capabilities provided by QualysGuard, ICI now includes the "right of audit" in all supplier service contracts. With Qualys, ICI now scans all global infrastructure for vulnerabilities at least once a week and automatically sends copies of results to each supplier.

"There isn't much to argue about with vulnerability documentation provided by Qualys," Simmonds says. "We're serious about remediation and expect suppliers to fix security holes in a timely manner. If suppliers don't correct the problems, we are liable to terminate their services." Simmonds says ICI has replaced several suppliers due to their faulty security. One supplier, a large hosting company, was repeatedly informed of a serious vulnerability that the supplier insisted did not exist. "We gave this to our manual penetration testers and they hacked them in 30 minutes—placing a small defacement on our hosted web pages to prove the point," Simmonds says. "So far, everyone who has disputed a Qualys vulnerability finding has been proven wrong."

ICI's Mandates

- Protect ICI network's "public face" from exposure
- Find all vulnerabilities on 3rd party systems before compromise by new worms and other attack technology
- Automate remediation management process with suppliers

Why ICI Chose Qualys

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

Managing Global Security Remediation

ICI Group's outsourced information technology strategy relies on successful execution by two major suppliers and dozens of smaller ones. The company operates about 330 sites in 55 countries. About two fifths of its employees are in Europe, two fifths in America, and the remainder in the Asia/Pacific region. None of the sites are massive, but Simmonds notes many smaller sites are a bigger challenge to support.

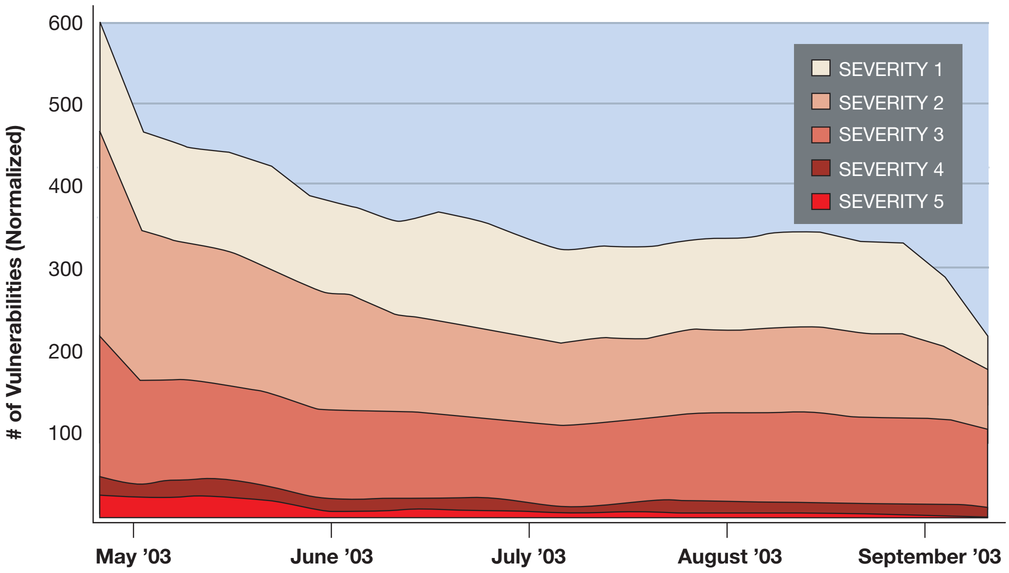
"Quite often our people are wearing many hats and frequently outsource IT support to all kinds of suppliers, so the whole trick is to get a consistent measurement of security," Simmonds says. With Qualys, ICI Group scans its network each week and automatically sends encrypted security audit reports to authorized people managing designated systems. "If remediation is required, that person will be expecting our call," says Simmonds.

Automated security audits and remediation workflow enable ICI Group to measure security performance and enforce policy throughout its outsourced IT infrastructure. "Before Qualys, we could not enforce policy with suppliers," says Simmonds. "Now we have a dashboard to measure on demand the vulnerability status of 3rd party services anywhere in the world."

Documenting Results for Management, Auditors and Government Regulators

ICI uses QualysGuard security audit reports in many ways. Internally, security operations mangers and staff use results from the weekly audits to remediate vulnerabilities on an ongoing basis. A monthly summary report goes to chief information officers in each of ICI Group's subsidiary companies. A quarterly summary report documents the general state of security for ICI's senior executives.

Trend of External Vulnerabilities (Normalized)



ICI's ongoing global use of QualysGuard has resulted in a dramatic reduction in network security risks.

Since it began using QualysGuard Enterprise, ICI has significantly reduced vulnerabilities in its network and improved the state of enterprise network security. The previous chart documents vulnerability reduction for a 22-week period in mid-2003. Using the QualysGuard scale of ranking vulnerabilities from 1 (least severe) to 5 (most severe), ICI has virtually eliminated the most severe vulnerabilities and cut two-thirds of the minor vulnerabilities in its global outsourced network.

> "If you can't measure security, you can't manage it...Qualys lets me measure and manage my network security...Their reports demonstrate ongoing security improvement in working with IT suppliers."
>
> Paul Simmonds ICI Group

Security audit reports also document ICI Group's compliance with a growing body of government-mandated laws and regulations. For example, Simmonds says ICI Group can use the reports to document compliance with six sections in ISO 17799. These security controls published by the International Standard Organization are now used by the "critical infrastructure" chemical and petrochemical sector as a common security framework for the U.S. Department of Homeland Security. ICI Group's external financial auditors will be able to incorporate its security audit reports to document compliance with the Sarbanes-Oxley Act of 2002. This law was passed to improve and safeguard the reliability and transparency of a public company's accounting statements and regulatory filings.

For ICI Group, the use of QualysGuard plays a key role in safeguarding its outsourced digital infrastructure. "Enforcing security with suppliers is vital," says Simmonds. "Qualys reports demonstrate ongoing security improvement in working with suppliers. Bottom line, Qualys works. End of story."