

SC

MAGAZINE

FOR IT SECURITY PROFESSIONALS

ALSO REVIEWED IN THIS ISSUE

Mobile data P67
DESlock+ does very well in our mobile data protection group test



Patching help P62
ManageSoft makes play for complex patch needs



Email filtering P54
Esoft's Threatwall 300 boxes above its weight in our mail filtering test



FEATURES:

Confidentiality is our business

Cigna's Craig Shumard on guarding intellectual property **P22**

SC's new Threat Report

We launch the most comprehensive security dashboard in the business **P6**

Rogues in the building

Can you be sure that no one has installed wireless networks? **P26**

GROUP TESTS

➤ Email content filtering

Keep spam at bay without all that effort. A round-up of the best of the best **P46**

➤ Mobile data protection

Five products that will keep your digital information safe and sound **P66**



Keep a grip on your assets

Intellectual property is a company's best friend, so Cigna's CISO takes a holistic approach to guarding it. **Marcia Savage** reports

For Cigna, one of the largest health insurers in the U.S., protecting intellectual property means protecting its lifeblood – customer data.

“It’s critical because what we do as a business is information,” says Craig Shumard, vice-president for data security at Cigna. “Being in the employee benefits industry, we are handling very sensitive health and disability information about our customers.”

Keeping customers’ data confidential involves using tools that ensure against data leakage but, just as importantly, it calls for employee awareness and other non-technical measures, he says.

“It’s really not just about the technology. It’s about an end-to-end perspective. It’s about risk, being a business enabler, and engaging everyone in the process,” explains Shumard.

Companies that do not take such a holistic approach run the risk of “fatal flaws” that could put them in the news for all the wrong reasons, he warns.

Protecting intellectual property (IP) and other proprietary information – whether trade secrets, customer lists or source code – has become a hot topic. Companies are increasingly concerned not only about keeping intruders and malicious code out of their networks, but

also that sensitive data is not leaving the enterprise. Such leaks can harm a business’s reputation and bottom line, as well as leading to lawsuits and fines.

The issue, while not at all new, is getting more attention these days in the wake of high-profile breaches involving source code belonging to Cisco Systems and Microsoft. Regulatory pressures have also put the spotlight on protecting proprietary data.

“Companies have always understood the value of IP. It’s one of those things that people used to maintain some

control over, but not complete discipline over,” says Paul Hooper, chief information officer at Extreme Networks.

“The events of the past few years – from Microsoft’s source code appearing on websites to *Sarbanes-Oxley* and its associated controls – have heightened the need to solve this problem.”

Companies are realizing they are losing money to IP leakage and are taking action, says Dr Larry Ponemon, chairman and founder of the Ponemon Institute, a research firm specializing in privacy issues. While corporate espionage does exist, the problem of IP leakage has more to do with unwitting or intentional actions by employees, he says.

For example, a sales manager leaves the company and takes their contact list to their new job, or an engineer takes a project to their new company.

“Most of these issues wouldn’t bring down a company, but they have the ability to siphon off dollars and wear away the assets of that company,” continues Ponemon.

“If a company can spend a little more effort, money and time... it’s good business, not just good security.”

At the same time, regulatory requirements such as *HIPAA*, *Gramm-Leach-Bliley* and *Sarbanes-Oxley* are driving



To a certain extent, the perimeters are starting to resemble Swiss cheese”

—Craig Shumard, vice-president for data security, Cigna



companies to protect their sensitive data, says Trent Henry, analyst at the Burton Group. As custodians of customer data, businesses may risk more than just harm to their reputation in the event of a breach – they could face lawsuits or even jail time “for not serving as proper custodians of that data,” he says.

Protecting IP and other proprietary data requires protecting the content itself versus the corporate infrastructure, says Henry. And although companies have done a good job in securing their infrastructures with firewalls and intrusion protection systems, they are not as far along in protecting the content.

“We’ve built moats around the infrastructure with firewalls,” says Henry. “Now we need to make sure we understand who is doing what in the infrastructure, identify people and make sense of what they should be allowed to do.”

A host of solutions are evolving to do that, including the array of identity management systems that provide access and authorization management, explains Henry. Another type of solution is enterprise rights management technology that protects the core valuable information in a corporation, such as documents, spreadsheets and emails.

The enterprise rights management technology uses local software, an agent, to protect documents and other data all the time no matter where the data goes, allowing what Henry calls “persistent protection of information.” This is achieved “through local software that understands the policies and can enforce and make use of the cryptography that is protecting those documents,” he says.

Some companies are turning to another type of solution, one that essentially keeps watch on the perimeter in an effort to prevent sensitive information from leaving the organization.

That type of technology might have a heuristic understanding of what sensitive data may look like, such as the format for a patient identifier or social security number, says Henry. Or it may sift

Cover Story **Intellectual property**

through a company's data system for sensitive types of data and create information fingerprints to detect data leaks.

In protecting its intellectual capital, Cigna takes a multi-faceted approach that starts with a risk assessment, explains Shumard.

"Our entire program is a risk-based approach, because we know no company, including ours, has the time, money, or resources to do everything," he explains. "So we have to make some intelligent choices on how we do it, where we do it and how creatively we do it."

The company makes sure it has business accountability in its process, that the business managers are engaged, and that everyone who works at and with the firm understands the importance of protecting information.

"Information protection is everyone's responsibility," says Shumard. "We really make an effort for people to understand why we are doing it, what the business impact is, and what the people impact is."

Having tools that enforce Cigna's policies is critical. "We focus on things like trusted-user validations, application monitoring – this is where we look to make sure we're monitoring high-privilege users, ones that have administrative rights, or certain outsourcers or off-shore people," he adds.



Don't get totally hung up on the technology. Although it is important, look at how they integrate"

—Craig Shumard

For that, Cigna uses host-based technology from Verdasys. The vendor's Digital Guardian agent monitors user activity related to the use of files, applications and storage devices, and can warn users before they transfer a file outside the company or block the transfer. It can prevent someone copying files into an email, or to a USB flash drive.

"It's really about protecting us from data leakage," says Shumard, adding that the technology also provides an audit trail, which helps with compliance.

Roles-based access control is another key element in Cigna's program. In protecting IP, it is critical that users only have access to the things they need to perform their jobs, he says.

Technology to enforce security policies at the endpoint is another essential component for Cigna. More focus needs to be on the individual endpoints and the data itself, because "to a certain extent, the perimeters are starting to resemble Swiss cheese," says Shumard.

"Don't get totally hung up on the technology. Even though it's important, look at how those things integrate. Look where your risks and vulnerabilities are and make sure that you are coming up with solutions that address those. Many times it will be technology, other times it will be awareness."

In conclusion, he urges enterprises to view security as a business enabler: "Don't just say no when protecting your intellectual property. There is never just one way of doing something. Usually, you can come up with options without compromising your intellectual protection objectives." ■

VERDASYS™

Data Security at the Point of Use

950 Winter Street., Ste. 2600
Waltham, MA 02451
(781) 788-8180
www.verdasys.com
info@verdasys.com