Law Firm Protects Confidential Client Information

WWR depends on its security solution to protect sensitive consumer data and maintain its sterling reputation.

EXECUTIVE SUMMARY

WELTMAN, WEINBERG & REIS CO., L.P.A.

- **Industry:** Legal Services
- **Location:** Cleveland, OH
- **Employees:** 1000+

BUSINESS CHALLENGE

- Protect confidential client records from hackers, viruses, malware, and other network threats

NETWORK SOLUTION

- Layered security solution safeguards the entire legal firm, from the network perimeter to the desktop level

BUSINESS RESULTS

- Comprehensive view of network data from 200 devices enables staff to identify and respond to network issues more quickly and proactively

Business Challenge

For more than 70 years, Weltman, Weinberg & Reis (WWR) has been a leader in providing collection services and legal representation to creditors. Headquartered in Cleveland, Ohio, WWR is the largest creditor's rights law firm in the United States. The company depends on its network to connect 1000 employees at nine offices, and to provide real-time status information on cases and files.

Protecting the sensitive client information that resides on its network is a top priority for WWR. Much of the firm's application data contains confidential or nonpublic information (NPI). Along with privacy concerns, maintaining data integrity is also important, because customer contact records and other business information is often used in legal proceedings. Records that have become corrupted or inaccurate because of a security or network issue can result in a total breakdown of the process and a significant loss to the firm.

"We act on behalf of many of the largest lending institutions in the country, and security is important because of the personal consumer information contained within our systems," says Robert Baird, director of IT at WWR. "A security breach would damage the reputation of our firm, along with that of the client whose information has been compromised."

WWR is a privately held institution and not subject to the same regulatory and corporate governance legislation as public companies. However, the company must meet the highest security standards to continue to do business with its large financial clients.

"Our regulators are in effect the very same clients we service, and we get audited by them on a regular basis," says Baird. "We need to give clients confidence that their data, while under our control, is well protected."

WWR needed a flexible, manageable security solution that could provide a defense-in-depth approach, safeguarding not only the network perimeter, but also the firm's internal network all the way to the desktop level.

> **"The Cisco Security MARS solution gives us the ability to condense a flood of information from multiple devices into a single source for faster, easier monitoring."**
> **—Robert Baird, Director of IT, Weltman, Weinberg & Reis**

Solution

WWR deployed a layered Cisco® security solution controlled and managed by Cisco Security Manager and the Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS). Cisco Security MARS is an appliance-based solution that lets the firm enjoy complete insight into its network security, and identify, manage, and counter security threats.

Cisco Security MARS monitors Simple Network Management Protocol (SNMP) traffic from all of WWR's routers, switches, servers, and firewalls. The solution also collects information from Symantic Antivirus, as well as Cisco IOS Netflow data. Netflow tracks network performance and provides detailed information about users and applications, as well as network routing and usage statistics. If a security event occurs, Cisco Security MARS identifies the issue and informs IT about incidents or anomalies that require attention.

"Cisco Security MARS produces event information that allows us to watch what is happening on the network," says Baird. "For example, if our antivirus software spots an incident, it communicates with Cisco Security MARS, which in turn brings it to our attention. We can check to be sure the antivirus server did its job and removed the virus."

WWR protects its primary Internet connection with two Cisco firewall appliances and Cisco Intrusion Prevention System (IPS) 4200 Series sensors, which report all of their activity to Cisco Security MARS. Cisco IPS 4200 Series Sensors let WWR identify and stop malicious activity like worms and denial of service attacks. The firm also uses Cisco Virtual Private Networking (VPN) to provide secure remote access for contractors and other remote employees.

To centrally manage the security device configurations and policies, WWR installed Cisco Security Manager. This easy-to-use software solution lets the firm manage and provision its network devices with a rich graphical user interface, from one location. WWR can define and assign new security policies to devices in a few simple steps, to respond more quickly to threats.

WWR wanted its network security to not only protect the firm from outside threats, but to deliver layered security down to the endpoint device level. The firm is deploying Cisco Security Agent software on both servers and desktops for protection against targeted attacks, spyware, rootkits, and zero-day attacks.

Cisco Security Agent also provides protection against threats that have not been seen before. Its proactive approach to security helps WWR reduce the need for emergency system patching, and helps reduce patch-related downtime and IT management expenses.

"One of our requirements for security certification is to maintain patch levels on all workstations and servers," says Baird. "Cisco Security Agent lets us schedule patches more easily and lets us keep our network devices secure between maintenance times."

Results

WWR is in the process of deploying Cisco Security Agent on more than 1000 desktops at all of its offices.

“Overall, I am very pleased with how the install is going, and we have not encountered any serious problems with our deployment,” says Baird.

Tracking more than 14 million events on an average day, Cisco Security MARS now provides WWR with a coordinated vision of exactly what is taking place within its network. The solution gathers information from more than 200 devices (not counting workstations), enabling the firm to see and investigate possible threats more rapidly than before.

“Prior to Cisco Security MARS, we had to individually manage each security device,” says Baird. “We had to hope that the device was doing its job, maintaining the signature updates, and effectively resolving issues. The Cisco Security MARS solution gives us the ability to condense a flood of information from multiple devices into a single source for faster, easier monitoring.”

If a security issue does emerge, the Cisco solution provides detailed information to enable WWR to mitigate the issue more effectively, stopping threats before they can spread throughout the network.

“The Cisco solution gives us the ability to track any anomalies from endpoint to endpoint,” says Baird. “If a security issue originates from outside our network, Cisco Security MARS also provides us with information about the access list or IPS intervention in order to address it. We can resolve an issue at whatever location is necessary to best mitigate it.”

Cisco Security Agent plays an active role in threat detection as well, providing detailed information to the Cisco Security Agent Management Console, which enables Baird and his staff to discover and react to events occurring at the workstation and server level. “Identifying threats and resolving issues more efficiently helps our overall throughput within our network, providing better response time to our end users,” says Baird.

Streamlining patch management and other administrative tasks has also enabled WWR to provide stronger network performance and protection. “In the past, we had difficulty staying current with our patches,” says Baird. “Now our systems remain 100 percent up-to-date.”

Next Steps

As it completes deployment of its Cisco security solution, WWR is planning to provide additional protection for its critical business network with a disaster recovery plan. “We have begun the analysis to determine what our strategy and recovery time objectives are, and are evaluating co-location sites,” says Baird.

The firm’s Cisco network is flexible and scalable to grow as business needs change, so WWR can continue to build on its success well into the future.

PRODUCT LIST

Security and VPN

- Cisco Secure MARS
- Cisco Security Manager
- Cisco Security Agent
- Cisco IPS 4200 Series sensors

For More Information

For more information, please visit http://www.cisco.com/go/security

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C36-473500-00 05/08