

### INTERNET SECURITY

Today's cyber criminals are exploiting vulnerabilities faster than ever before. Assessing and managing these threats require continuous monitoring and comprehensive support to mitigate these risks.

### NETWORK PROTECTION

The devices and systems deployed to protect firms generate millions of events every day which are virtually impossible to analyze without automation. The integrity of client data, to meet serious regulatory requirements and fiduciary responsibilities, has to be protected 24/7.

### MOBILE COMPUTING

Protection for data on the move and remote access to the firm's network is vital to maintain ease of attorney services while away from the office.

## Legal Firm IT Security Case Study



### Situation

This unknowing victim is one of the top international law firms in the United States. With more than 1,000 attorneys in over 20 offices around the globe they provide legal services to their clients in business and government, both here nationally and on the international landscape.

They had a fully equipped IT and data management staff but with only one Security Professional in the whole organization. This Security Professional had no policy or plan to protect the information and assets of the firm. Additionally, appropriate levels of governance, risk management, audit and compliance were also overlooked. In a word, this lonely Security Professional was overwhelmed which left the firm defenseless to today's sophisticated cyber attacks.

### Challenges:

- A recent incident was discovered that compromised the firm's network from an inside laptop.
- This compromise allowed outside threats to enter the network undetected and with unhampered access to critical servers.
- The source of the data theft indicated foreign country sponsored cyber attack efforts is becoming more prevalent.
- The firm had only one security staff member without security governance, risk management, audit or compliance authority.

Could this firm throw more money at the problem, bring in a whole new IT discipline and hire several new personnel to maintain the new discipline of security? Yes but, it would have cost more in time and political struggle internally than wisdom would allow.

The IT Director learned overnight that the first generation of security (firewalls and anti-virus software) is not enough to protect a law firm in today's cyber attack battlefield. The principles of sound security engineering and governance were ignored for far too long but how could they change direction overnight? There had to be an answer that is cost effective and flexible enough to adopt quickly!

**Simplifying**  
IT Security

# Service Features and Benefits



There are significant threats to the information assets on a firm's network. These threats could originate from inside or outside a network—from hackers and internal users with malicious intent or from users who accidentally unleash viruses or worms; information security departments have to stay vigilant around the clock 24/7.

## Solution

A partnership with a 24/7 Managed Security Service Provider (MSSP) for your Computer Network Defense (CND) is so important and valuable to your firm\*. We partner with firm executives to assess Security Risks, develop a solid Security Program, stand in as a **Chief Security Officer (CSO) pro tem** and take the heat of vital IT resources so you can focus on your business services.

\* According to the Computer Security Institute (CSI) Computer Crime and Security Survey for 2007, the average annual loss due to computer security incidents were \$350,424 per firm. Respondents reported 18 percent suffered a "targeted attack" aimed exclusively at their organization. Fraud and data theft overtook virus attacks for the first time and insider threats were noted as the most perilous weakness in all networks.

## Security Solutions

- Security Management Experts that work with your management team to engineer a comprehensive IT Security program.
- Security Assessments and Vulnerability Scans performed by trained and certified security professionals with at least 3 years experience.
- 24/7 Managed Security Operations, Event Log Management and Incident Management Services
- Active Network Defense services to protect the confidentiality, integrity and availability of your data.
- Security Awareness of emerging threats to your network, the firm and the condition of your network health available 24/7.

## SERVICES AVAILABLE

Security Risk Assessments  
IT Vulnerability Scanning  
Security Program Development  
Security Log Management  
24/7 Security Operations  
Active Network Defense  
Security Intelligence

## PremiereTec

Security  
Division

220 E. Central Pkwy, Suite 1020  
Altamonte Springs, FL 32701  
Phone: 407-215-1737  
Email: [info@premieretec.com](mailto:info@premieretec.com)

### SECURITY ASSESSMENT

Security capabilities (focus, scope, approach, ownership, funding) assessment; baseline creation, role and security organization creation, IT architecture appropriateness.

### SECURITY POLICY

Security Policy development is the most crucial step in the security engineering process by identifying security controls to be implemented in the network environment and responsibilities assigned to users, administrators and management.

### 24/7 SECURITY MONITORING

Most IT departments cannot afford to hire and retain enough security analysts to monitor and defend your network on a 24/7 basis. That is what we do, so you don't have to.

For more information on any of our services please visit us on the Web at:

[www.PremiereTec.com/Security](http://www.PremiereTec.com/Security)