White Paper

The Legal Imperative: Why Law Firms Must Invest in Information Security & Compliance

...and why Cloud Security may be the Best Solution

Table of Contents

- Hacking and Malware breaches ranked 2nd and 3rd in 2009, responsible for more than 95% of all data comprised. Breaches using social tactics more than doubled, to 28% in 2009 from 12% in 2008.

VerizonBusiness, 2010 Data Breach Investigations Report

Law firms have moved to the front lines of information security and compliance. Historically under-investors in information security technologies and solutions, law firms have been discovered by information criminals who have them directly in their crosshairs.

Hackers have discovered a treasure trove of valuable business information, intellectual property and even national secrets stored by the legal community. Criminal gangs have developed highly specialized and focused attacks, some using the latest social networking gimmicks, in targeting both law firms and individual attorneys. They constantly seek to steal confidential and sensitive legal information to sell in online forums, or to ransom back to victims.

Firms practicing in international law, trade disputes, intellectual property and privacy have experienced attacks by state-sponsored information criminals. Foreign agents use information attacks to intimidate law firms while seeking to advance restrictive national policies, ease entry into competitive markets, or to steal trade secrets and legal strategies to weaken bargaining positions.

Meeting these new challenges, and to comply with existing privacy and security levies, requires law firms to invest in new and stronger countermeasures. Their courtroom battles and legal actions, and the integrity of the judiciary, begin with maintaining the privacy and confidentiality of sensitive legal and client information used in legal arguments.

This white paper reviews the latest attacks targeting law firms with trends in information security impacting legal professionals. It explores the benefits of cloud-based security defenses with the synergies created in hybrid combinations of cloud-based and licensed security solutions installed in trusted networks. An overview of the McAfee security software-as-a-service (SaaS) solution suite also is provided.

Why Law Firms Must Invest in Information Security and Compliance

The legal community understands better than anybody the importance of confidentiality. Confidentiality for legal firms is driven by two requirements – security and compliance.

Security is critical to the attorney-client privileged communications needed to confidentially develop strategies and arguments. This applies to confidential information used across the legal process, from the pre-trial phase, to information revealed in the discovery process, and to courtroom arguments. A loss of confidentiality would expose key legal arguments allowing pre-trial motions to target key facts and critical evidence. Attorneys without confidential legal positions would face point-by-point rebuttals of key evidence and arguments throughout the trial process.

Law firms historically have not kept pace with industry averages for investment in information security defenses. Fortune 500 firms have established a 3%-5% threshold of security spending as a percentage of the total IT budget.[1] Some segments, such as financial services and banks, traditionally spend more. Few law firms have invested this level of revenues in information security. Recent surveys of legal professionals show that law firms have plans to boost investments in security in 2010 and beyond to position themselves for growth and new business.[2]

[1] http://www.networkworld.com/news/2010/061010-gartner-security-identity-management.html?fsrc=netflash-rss

[2] http://www.tmcnet.com/usubmit/2010/06/25/4869567.htm

Legal firms are not directly covered by compliance regulations but many of their client firms are. Law firms therefore are custodians of their client's sensitive information and have a legal obligation to maintain confidentiality until it becomes public in, or protected by, a court proceeding. Additionally, all types of personally identifiable information in consumer finance, healthcare, education, some Web browsing and other private acts must remain confidential. Privacy regulations increasingly are extending protection requirements, and potential penalties, to business associates acting as information custodians for their clients.

Phishing and Spear-Phishing

Law firms must be aware of the new universe of threats targeting them on the Internet, and specifically the warning signs for phishing and spear-phishing attacks already targeting attorneys. Spear-phishing[3] is a specific tailored email message designed to entice the targeted individual to do something that will compromise defenses. It is a more precise variation of the general phishing attack with the same result – giving information criminals access to sensitive information. Garden variety phishing attacks broadcast messages containing malware designed to bypass defenses of recipients responding to the lure of what appears to be an attractive offer.

The FBI has issued several warnings for spear-phishing attacks, including specific warnings to law firms in Nov. 2009 and July 2010.[4] The FBI warnings advise of threats to confidential information from email messages containing "subject lines spoofed, or crafted, in such a way to uniquely engage attorneys with content appropriate to their specific business interests."

Spear-phishing is a rapidly growing plague for visible public figures and business executives, although nobody knows the exact numbers. The impact of phishing attacks are better understood, although still disputed. In May 2005, approximately 1.2 million consumer computer users in the U.S. suffered phishing losses amounting to $929 million. Two years later damages for an estimated 3.6 million phishing victims were said to have rocketed to $3.2 billion. Businesses in the U.S. have been estimated to lose an additional $2 billion yearly, mostly as their customers become victims.[5]

Three underlying trends are prime contributors to the ballooning growth in phishing and spear phishing attacks on law firms. First is the realization by hackers, many based off-shore, that law firms are a new and lucrative market, as witnessed by the FBI's warnings of the rapid growth in spear-phishing attacks on attorneys. Second is the exploding growth in smart phones and mobile computing, a trend including attorneys among its enthusiastic adopters. Mobile wireless devices are less secure than wired computers, requiring more investment in countermeasures and procedures to prevent eavesdropping. A third driver of phishing and spear-phishing growth is the huge social networking community, best illustrated by the 500 million global Facebook members[6] and double-digit growth in the millions of Twitter users. Both Facebook and Twitter are commonly used to launch phishing and spear-phishing attacks.

The vulnerability of law firms to spear-phishing attacks arises from busy principals making big use of smart phones and mobile devices to increase their productivity, coupled with high-profile legal actions. Lawyers frequently are involved in issues that "go viral" on the Internet, spreading rapidly through social networks and the blogosphere.

The poster child for spear-phishing attacks on law firms was a sophisticated Jan. 2010 attack launched against Gipson Hoffman & Pancione in Los Angeles by hackers thought to be in China.[7] Gipson recently had filed a $2.2 billion patent infringement lawsuit against several Chinese software companies. Because of the high risk posed by the lawsuit, Gipson attorneys had been briefed on spear-phishing and did not respond to the bogus email messages, ostensibly from trusted legal associates and containing an attack for bypassing defenses.

[3] http://en.wikipedia.org/wiki/Spear_phishing#Phishing_techniques

[4] http://www.fbi.gov/cyberinvest/escams.htm

[5] http://en.wikipedia.org/wiki/Spear_phishing#Phishing_techniques

[6] http://www.govtech.com/dc/articles/141457

[7] http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=222301001

The attack against Gipson is believed to have been unsuccessful. Other attacks against other targets, both in the legal community and elsewhere in the public and private sectors, are known to have succeeded. One of the most prominent examples is the spear-phishing attacks against Google in early 2010, believed to have originated in China. These attacks included very sophisticated advanced persistent threat (APT) attacks that use multiple methods to breach defenses and sustain themselves, and resulted in the theft of sensitive Google intellectual property.

Web Attacks

Hackers and information criminals use a multitude of gimmicks, lures and tricks to entice Internet users to visit websites where they can be infected by malware. In addition to phishing and spear-phishing lures in email messages, hackers today often use social media, such as malevolent Facebook pages and Twitter "tweets", to trick unsuspecting visitors or recipients.

A typical Web attack today sends an unsuspecting user a message. The user receiving the message could be targeted from addresses stolen from the contacts of a compromised legitimate social media user. The message offers something to entice the recipient into visiting the bogus website, or social media page, resulting in malware being injected into their browser. A successful Web attack invariably involves clicking on a link or icon that injects the malware that spreads throughout the system.

- Unsuspecting Facebook users get a message from a friend urging them to "check this out" and including a link to a Web page that appears to be a Facebook log-in page, but it is a fake site that steals their information when they type in their username and password. The worm also sends a copy of the message to the infected Facebook member's contacts.

www.cnet.com, April 30, 2009

Some Web attacks use general enticements such as pornography or get-rich-quick schemes. Others are specifically targeted at dating, free software downloads, or goods and services. Some Web attacks have infected legitimate websites with malware. Infected websites can redirect the user to a hidden malicious website masquerading as the legitimate site, ready to inject malware. Another attack by infected websites is to offer malware hidden in a popup window to a site visitor's browser. The popup window has some enticement to lure the visitor into clicking on the offer and infecting themselves.

Almost all Web attacks are designed to do two things. First, like a worm or virus, they attempt to use the newly infected system to spread the infection. Spreading the infection can be by sending email spam to contacts stolen from the newly infected system, or by attempting to inject malware into other websites visited by the infected system. Secondly, web attack software seeks to steal login and password credentials for identity theft and fraudulent financial transactions that drain money from online financial accounts. Malware injected into an attorney's system could seek to steal login credentials for sensitive internal legal or case information, or client systems.

Hactivism

Hacktivism is a relatively new type of cyber attack to promote political causes.[8] Most of the early forms of hacktivism were less harmful website defacements by private individuals or groups seeking to promote a point of view. Hactivisim evolved into more malevolent nationalistic forms in 2008. Hackers, believed to be sponsored by the Russian government, launched denial of service attacks against the Republic of Georgia during a war, and Estonia and Lithuania during political disputes.

The spear-phishing attack on Gipson Hoffman & Pancione would be classified as hactivism if the Chinese Communist Party were involved. Law firms involved in highly visible lawsuits, especially those involving social, environmental or political issues, are exposed to heightened risk for a range of hactivist attacks from private activists or national governments.

Compliance

Compliance today requires the confidentiality and integrity of unreported financial information in all public companies, as mandated by the Sarbanes Oxley Act (SOX). This includes related information that is material to finances, such as intellectual property, and mergers and acquistions. SOX levies

[8] http://en.wikipedia.org/wiki/Hacktivism

requirements for quarterly attestations of the integrity of financial information, as well as a system of controls to enforce confidentiality. All information covered by SOX, and the controls to enforce confidentiality, integrity, access and availability, must be protected.

The confidentiality requirement also extends to operational information and processes in clients engaged in critical infrastructure and processes such as communications, networking, transportation, food, energy and many others. Law firms have a legal obligation to maintain the confidentiality of this critical business data, including the defenses of the systems and processes, unless it becomes public in a court proceeding.

Federal privacy laws require confidentiality for all types of personally identifiable information in consumer finance, healthcare, education, some Web browsing and other types of private acts. Privacy regulations in the U.S., such as HIPAA and GLBA, are specific in extending coverage in what generally is an « opt out » culture in the U.S. Law firms practicing internationally must be knowledgeable of the more restrictive privacy requirements of many foreign jurisdictions following « opt in » guidelines requiring even more protections.

Bankruptcy keeps many lawyers busy and places law firms into custodianship of much sensitive business information. Federal bankruptcy laws require the confidentiality of this information until it has been made public in a court proceeding or by a court order.

In addition to Federal and state privacy regulations, law firms must comply with mandates to produce timely financial or legal documents for discovery orders. Discovery applies to client communications and therefore can include topical email messages. Self-interest compels law firms to maintain the confidentiality of the firm's financial information, and the personal information of the law firm staff. Similarly, successful law firms must have business continuity plans in place to sustain operations in the event of a business disruption.

- The unique defensive perspective offered by cloud-based services helps to meet several critical privacy requirements

Effective Security and Compliance for Law Firms

Security and compliance management

Effectively managing security and compliance in a law firm is no different than in any other company. It begins with designating somebody to manage the security program, with responsibilities to identify the location and degree of sensitivity of all confidential information. This is closely followed by prescriptive steps to secure the information, and developing an ongoing program to maintain and increase security.

For law firms, training staff on security requirements and compliance responsibilities is a critical task. Law firms are operated and managed by people to serve other people. The human element is central to maintaining security and compliance, and requires the diligence of all. This is exactly how Gipson defeated the spear-phishing attack launched against it.

Documents are critical to law firms so each document, and document repository owned, must be assessed for document retention and disposal. This includes the key requirement for e-discovery of electronic documents and email messages. Legal documents are covered by multitudes of regulations forming complex layers of retention, discovery and disposal requirements. Management diligence and the proper tools can prevent this critical function from becoming a time-consuming headache.

An excellent management strategy for efficient and effective law firm security is using a lifecycle model to evaluate the risk and cost. Information usually poses more risk early in its lifecycle. Retention costs are higher earlier in the information lifecycle because documents typically are filed in more costly disk storage and require stronger protections. As documents age, they can be migrated to less costly, and more secure, secondary or tertiary storage. All can be indexed by a cost-effective e-discovery retrieval system.

Compliance and Security for the Cloud

Privacy and security best practices for cloud computing require effective information defenses, including anti-malware for email and Web sessions, perimeter defenses and encrypted communications to secure confidential legal information. Security vendors deliver such solutions in various forms, including locally deployed software and appliances,and increasingly as cloud-based security services.

Security-as-a-Service protecting confidential information transmitted through the cloud brings economic advantages in lifecycle cost savings. When compared to the costs of licensed security software solutions, cloud-based SaaS security services often are easier to deploy and simpler to use. They are paid as a monthly expense, avoiding entirely capital acquisitions and depreciation, and minimizing expensive support and training costs.

Preventing malware threats

Cloud-based security is designed to work with existing IT or network infrastructure, requiring no additional hardware or software. Message defenses in the cloud protect confidential legal information by blocking or removing messages containing malware, including phishing and spear-phishing attacks. Spear-phishing messages, along with viruses, spam, and unwanted content, never reach your firewall. The risk to internal systems is drastically reduced.

Most email defenses redirect the customer's MX record to the address of the filtering servers. MX records are DNS entries that identify the server receiving a domain's email traffic. Once redirected, the MX record sends all email to the service provider's servers for filtering according to set policies. The same technique can be used to filter outbound email, ensuring that messages sent from the corporate network are free of viruses and worms, and are policy-compliant.

Internet session security

Message defenses today also are required to protect sensitive information communicated in Internet sessions, defending both the user's browsers and servers hosting websites. Legitimate websites may be compromised by malware that seeks to infect a user's system in a "drive-by" attack. Drive-by attacks inject malware into the user's Web browser during a visit to the infected website. The malware burrows from the browser deep into the infected system where it steals sensitive information. Malware seeks to propagate by infecting other machines, or injecting a copy of itself into a server through a browser session.

Confidentiality and integrity attacks from direct malware injections are a serious and sophisticated threat. Drive-by injections target the growing use of social networking sites with phishing and spear-phishing lures in bogus email messages, and with bogus social network members. Compliance regulations and benchmarks include numerous requirements to protect against malware injections and help secure cloud computing by combating browser injection attacks.

Ensure confidentiality with encryption

Regulations such as the HIPAA HITECH Act and the Payment Card Industry Data Security Standard (PCI DSS) elevate encryption to a preferred technology for securing confidential storage. Encryption is an effective security and privacy control because most breaches of encrypted information are exempted from costly notification requirements.

Additionally, confidential legal information transmitted across a public network must be secured from the message originator to the recipient, especially when using mobile devices. The industry-standard Transport Layer Security (TLS) encrypted tunnel[9] is the most cost-effective way to secure end-to-end delivery of sensitive messages across all public and private clouds.

[9] http://tools.ietf.org/html/rfc5246

The most efficient TLS deployments include policy settings that automatically identify, encrypt, and decrypt messages containing confidential information. Encryption keys transparently set up the secure message connections from the source to the destination, across all network hops configured to support the TLS standard. Users are spared the pain of managing encryption keys and the cost of operating complex configurations.

Availability of critical legal information

Owners of confidential information must provide access during business disruptions and disasters to sustain business operations. Cloud-based message security services effortlessly meet this requirement by queuing messages until destination servers signal their restoration. Users are freed of business worries for email. Messages can be accessed in a Web mail browser application freeing users to focus on other critical priorities knowing messaging will automatically be delivered once systems are recovered.

Message archiving

Legal firms, like their clients, frequently must respond to court-ordered discovery requests from plaintiff's law firms and others. Discovery extends to messages containing evidence to support legal proceedings. Automatic email archival in the cloud is an efficient way to manage this legal requirement.

Cloud-based message archiving offers law firms the ability to search and retrieve historical email messages based on any number of variables, such as originator, contents, or destination. Archival and retrieval options for storage volume, retention and search parameters are best managed by users as self-service options in the network. Those closest to the information can most efficiently retrieve it, freeing your IT staff from costly and time-consuming searchings and allowing them to focus on more strategic and critical tasks.

Compliance Requirement	McAfee SaaS Security Services Feature
SOX Confidentiality Requirements for Corporate Financial Information: A risk analysis for covered financial information must identify **confidentiality requirements for information transmitted electronically over open networks.** Is confidential information in danger of being intercepted by anyone other than the intended recipient?	McAfee® SaaS Email Encryption protects confidential information being transmitted, from the source to the destination.
HIPAA Security and Privacy Rules: Requires service providers to covered entities – the owners of personally identifiable healthcare information – to meet HIPAA requirements. Law firms working in healthcare must be able to demonstrate proper security, including documentation of all **network configuration settings** for network components. Audit evidence is required because components are complex, configurable, and always changing.	McAfee® SaaS Email Protection includes a Web -based management console with easy and intuitive configuration settings for all subscribed network security services.

Compliance Requirement	McAfee SaaS Security Services Feature
Gramm-Leach-Bliley Security and Privacy Rule: Law firms working with clients in consumer finance must have security equal to their clients. This includes a risk analysis to ensure that all reasonable precautions are taken to prevent the theft of confidential information by malware and spear-phishing attacks. Anti-malware controls must **protect confidential legal information from malicious attacks** including spear-phishing, Trojans and viruses.	McAfee SaaS Email & Web Protection protect against malware that is either email or web-borne, including malicious drive-by injections. SaaS Email Protection protects against phishing and spear phishing by disabling urls.
Homeland Security Act of 2002: **Critical Infrastructure Information Act** requires confidentially and the ability to recover business operations in economic segments defined as critical such as food, energy, financial markets, transportation, communications and public utilities.	McAfee SaaS Email Protection includes built-in disaster recovery. Email messages are automatically queued when the destination mail server fails. Users can easily access their email messages securely, with full encryption from source to destination, via Web mail in a standard browser.
The **U.S. Bankruptcy Code** (Title 11, Chapter 3) Law firms representing parties in bankruptcy proceedings must protect the privacy of financial information until decided by the court. An evolving area of law is information assets, such as customer files that include personal information, which must be protected until disposition is determined by a court-appointed ombudsman.	McAfee SaaS Email & Web Protection block email & web borne threats that can infiltrate your network. SaaS Email Encryption protects messages and attachments in transit.

The McAfee Advantage

Security leadership

McAfee has been a pioneer and leader in delivering a suite of award-winning security solutions. McAfee solutions extend from the information perimeters to all forms of content security to protect against hacker attacks in messages and websites – defenses against phishing and spear-phishing, Trojans, viruses, worms, and website injections.

All McAfee SaaS security services are simple to deploy, operate and use. Email is an excellent example of this. The McAfee cloud-based email discovery solution allows retrieval of messages by the users themselves. Similarly, business continuity and disaster recovery is built into cloud-based security solutions for cost-effective protection.

Introducing McAfee SaaS Security Services

McAfee® SaaS Security Services require no hardware or software, have no setup costs, operate on month-to-month agreements, and share a single integrated console.

McAfee SaaS email security services include:

McAfee® SaaS Email Protection—Analyzes inbound email flows to block spam, viruses, worms, and phishing threats before they enter your network, with over 99 percent accuracy. Scans outbound email to enforce corporate email policies and prevent sensitive data leaks. Includes policy enforcement to recognize outbound messages containing confidential information to launch encrypted TLS tunnels to the recipient.

McAfee® Web Protection – Analyzes web traffic to block viruses and spyware. Prevents spyware from phoning home, strips viruses from webmail, prevents users from entering known phishing sites, and blocks drive-by malware injections, Also provides control over sites visited, and visibility into employee Web usage.

McAfee® SaaS Email Encryption – Enables organizations with McAfee SaaS Email Protection service to enforce email encryption in order to safeguard information to meet data privacy and compliance regulations. The service eliminates the need to deploy and maintain expensive third-party PKI or certification authorities.

McAfee® SaaS Email Continuity—Provides email backup during a system outage, engaging automatically when a server failure is detected. Offers full email functionality via a secure web interface, allowing email access, use, and management until normal service can be restored.

McAfee®SaaS Email Archiving—Automatically, safely, and economically stores email for future review and e-discovery. It provides complete email backup for any organization with unlimited, in-the-cloud storage and quick, powerful search capabilities.

Secure MX record

McAfee SaaS Email Protection requires only an MX record redirection to begin protecting confidential information. Redirecting the MX record to McAfee adds a new security layer. All message-borne threats are directed first in the cloud at McAfee as your visible email proxy. Hiding, or "delisting," your actual MX record exposes less information about your network and its employees, greatly reducing your risk of a breach.

Putting your business in complete control

With McAfee as your organization's sole MX record, unsolicited email cannot be sent directly to you or your employees. McAfee uses unique MX record-masking techniques that protect your network from denial of service attacks, directory and dictionary harvest attacks, mail bombs, and channel flooding.

Even with all the added email security, McAfee never controls your MX record. You can remove McAfee as the primary MX record at your discretion, at any time. McAfee has also engineered its email defense solutions to eliminate unauthorized email viewing or alteration—even by McAfee.

Around-the-clock protection

Most organizations can't afford a dedicated team of email threat specialists to monitor the global state of email around-the-clock, and provide real-time updates. McAfee services provide this level of expert protection, beyond what most organizations could provide for themselves.

Behind the services sits McAfee Global Threat Intelligence, a sophisticated streaming data environment which monitors the global state of the Internet for threats 24 hours a day, seven days a week. It continuously incorporates updates from a global network of million of sensors, dynamically rewriting and updating filtering rules to protect against the latest threats

McAfee customers can also integrate a disaster recovery feature to protect against message loss in the event of a customer network outage. This service level, combined with the early detection of McAfee and notification of destructive email, is unmatched by most on-premise email filtering solutions.

Processing and availability

As expected from an industry leader, McAfee's leading technology and redundant message processing centers give 99.99 percent service availability, with historic network availability of 100 percent. Our data centers provide immediate disaster recovery and high availability, and the McAfee Network Operations Center (NOC) provides 24x7x365 operational support and automated monitoring of all service components.

Internal passwords are changed frequently, with server access restricted to only authorized personnel. Firewalls restrict IP access and all message traffic is load-balanced for optimum message throughput. Production facilities provide carrier-grade infrastructure, with a low-cost and highly distributed "pod" architecture. Network and application monitoring provides visibility into suspect alerts and trouble alarms. Servers running McAfee SaaS services are inaccessible via the public Internet, ensuring a redundant, diverse, and secure service.

Summary

Law firms must invest in security and compliance equal to that provided by their clients in this era of elevated privacy, security and threats. Privacy and security requirements continue to evolve and, for law firms, are compounded by increasing reliance on smart phones and mobile platforms relying on wireless technologies. Well managed security programs can help to improve the quality and efficiency of legal services.

Law firms are joining the trend to increased use of cloud computing. SaaS security is the most cost-effective way to meet security and privacy requirements for cloud-based information systems, especially when they are combined with legacy systems behind a firewall.

McAfee SaaS Security Services put network cloud-based security into your organization's email & web traffic stream, adding security layers that protect your confidential information. Because it's easy for users to activate, configure, and control, McAfee SaaS Security Services quickly become an integral part of any security architecture and reduce the risks to your network.

Spear-phishing gets ever more clever, spamming continues unabated, new computer viruses are constantly released, social & mobile media bring entirely new threat vectors and each workday brings new waves of ever-more sophisticated threats. Successfully protecting the business requires constant diligence and extensive resources. McAfee SaaS Security Services provide affordable and effective security that is easy to administer, easy to use, and constantly updated against the latest threats. It lets you focus on providing high-quality law services, not on managing threats.

About McAfee

At McAfee, security is our only focus, which enables us to build products that anticipate threats and help you stay a step ahead of would-be attackers. With IT departments stretched thin, it makes sense to entrust to the experts those areas that are outside your expertise, so you can focus your talent and resources where they can add the most value to the business.

McAfee Security-as-a-Service solutions run in our data centers, relieving you of the responsibility for managing the entire infrastructure. And because we develop our software, we have the knowledge and capacity to run it more efficiently for you. That allows you to focus on securing your business, rather than managing security installations, patches, and upgrades—or developing security expertise in-house. The bottom line for you? Peace of mind with lower total cost of ownership and much less effort.

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com