

Law Firm Technology Group

Security Guide

The Best Free Resource for Managing Your Law firm

Join our group for free at
<http://LawFirmTechnology.com>

The screenshot shows the VirtualLegalShow.com website. At the top, there is a navigation bar with links for HOME, VENDOR LIST, FIND A VENDOR, NEWS, and KEYNOTE. A search bar is located in the top right. The main content area features a large banner with a woman in a business suit. On the left, there is a 'Find a Vendor' section with a search box and dropdown menus for 'Select Category', 'Select State', and 'Enter City'. A central text box reads: 'Visit us on Friday November 18th, 2011 for our Virtual Show Get Free Training & Awesome Prizes'. Below the banner, there are sections for 'Featured' and 'Latest News'. The footer includes the text 'VirtualLegalShow.com' and 'VENDOR GUIDE'.

The screenshot shows the LawFirmTechnology.com website. The top navigation bar includes links for Home, Software, Hardware, Services, Litigation Support, NEWS, and Members Login. A search bar is in the top right. The main heading is 'Law Firm Technology' with social media icons for Twitter, Facebook, LinkedIn, and RSS. Below this is a sub-heading: 'General Technology, Marketing Technology, Litigation Technology for Law Firms'. A large orange banner promotes a 'Free Law Firm Technology Membership' and a 'Free Email Newsletter'. It includes a sign-up form with the text 'Enter your email here:' and a 'Click Here to Submit' button. Below the banner, there is a news article titled 'ADERANT Names Doug Geller Managing Director of ADERANT StarLaw' dated Monday, August 22nd, 2011. To the right of the article is a 'CATEGORIES' sidebar with links for Hardware and Billing Systems. The footer contains the text 'LawFirmTechnology.com'.

The screenshot shows the EDiscovery Universe website. The top navigation bar includes links for EDiscovery Home, About Us, Services, Software, News, LawFirmTechnology.com, and Members Login. A search bar is in the top right. The main heading is 'Electronic Discovery Universe' with the tagline 'For Law Firms'. A large orange banner promotes a 'Free E-Discovery Universe Membership' and a 'Free Email Newsletter'. It includes a sign-up form with the text 'Enter your email here:' and a 'Click Here to Submit' button. Below the banner, there is a news article titled 'EDiscovery Conference, Hollywood FL on March 23-25' dated Thursday, January 27th, 2011. The footer contains the text 'EDiscoveryUniverse.com'.

The screenshot shows an email newsletter interface. At the top, there is a header with a date 'September 26, 2011' and an 'Issue: 23' label. The main heading is 'Many Changes Affecting Law Firms This Month'. Below this is a 'Dear Chris,' salutation. The body of the email contains several paragraphs of text, including a section titled 'HP buys Autonomy/Interwoven/Imange for \$10 Billion' and another mentioning 'Aderant acquires Client Profiles, Compulaw & CRM4Legal'. On the right side, there is a sidebar with social media icons for Facebook, LinkedIn, and Twitter, and a 'Join Our Mailing List!' button. Below the sidebar, there are two small images: one of a woman with the text 'copitrak Enterprise Level Cost Recovery & Expense Management' and another of a woman with the text 'Legal Search Solutions, Inc. Florida's Premier Legal Temporary & Direct Hire Placement Partner'. The footer contains the text 'Monthly + E-Newsletter'.

Law Firm Security Guide

Our Definition of Security:

*Security is the art of identifying potential threats that may do harm to the law firm, and taking decisive action to plan for, eliminate or take measures against these threats.

*A thorough security analysis encompasses much more than technology systems. It involves every facet of the firm's operation, and as a result, all employees, directors, lawyers and upper management.

Resources:

***Compliance & Security Testing** -- (Certified Ethical Hacker)

Mark Akins, CISSP, CISA, PCI QSA

561.866.6887 /mark.akins@1stsecureit.com

***Forensic Analysis** – (eDiscovery)

Matthew J. Thomas Ph.D.

mthomas@usinfosec.com //1.941.951.6015

***Security Solutions** (Firewall Monitoring, Archive, Spam, More)

Tom Garcia

President & CEO | InfoSight, Inc.

p 305.828.1003 x101

tom.garcia@infosightinc.com

Prioritize the Biggest Threats:

*Economic Threats

*Ethical Threats , and Compliance Readiness Law Firms

*Management Threats

*Physical Threats

*Direct Scam Attacks

*Computer-Based Threats

*Disaster Situations & Recovery Planning

Biggest Threats that have actually Destroyed Law Firms

- Dot Com Crash killed core business
- Real Estate Recession
- Credit Constriction Issues
- Mass Departures triggering a clause in the Line of Credit to defund the firm — Forcing them to liquidate
- Compliance Issues/Dipping into client funds
- Bad Accounting/Fraud
- Single Client provided more than 50% of firm's revenue

Best Practices:

*Diversify your practice. Keep track of economic trends that may affect your firm's prospects.

*Pay Yourself First. Save 10% each year to create a cushion to protect against downturns.

*Make sure that one client, or one industry or practice area comprises no more than 25% of the company as a whole.

*Don't ever stop marketing. Market when you are busy and when times are slow. Marketing has a delay of effectiveness of 6-24 months or more.

*Law Firm Leadership is critical. Keep key personnel happy. Avoid mass defections at all costs.

*Diversify assets into other classes – multiple currencies and alternative currencies (Gold /Silver)

*Proper billing practices – Avoiding Overbilling (Good Billing software with good Conflicts of Interest System)

*Protect Credit Card (PCI – Payment Card Industry and DSS- Data Security Standard) and other sensitive Data – Sarbanes Oxley, HIPAA, FISMA, FERPA compliance

*Good Accounting Practices--Proper accounting audits, penetration tests, etc.

*Good Stewardship of Client Funds

Law Firm Security Guide

Internal Threats — Users:

- *Illegal Download Protection—Tools to disable USB Access or CD Burners. PolicyPac.com, Kioware.com
- *Lock down pc's. Limit access to Administrator user, use Citrix to deploy Thin clients or VMware to deploy virtual desktops which auto-wipe user changes upon next log-in.
- *Use software alerts to inform you if a user is extracting, emailing, large amounts of data or accessing sensitive data.

Wireless Security:

- *Wireless guest visitor's network (Partition off from main network. Throttle speeds to limit use)
- *Wireless telephony (PBX)
- *Laptops – Unsecured network
- *Turning off security
- *Training of users in security is important
- *Mobile smartphones (Rogue Apps)
- *Jailbroken phones—less secure

Website Security:

- *Wordpress, Mysql, linux are common platforms and routinely get hacked.
- *Plug-ins can contain insecure code.
- *Web- App security is a big issue today.
- *Increasing amount of collaboration with sharepoint, FTP servers, Large filetransfer programs such as YouSendIt
- *Ediscovery platform security – Relativity, Lextranet, Catalyst, Clearwell, IConnect

Social Network Threats:

- *Big source for Identity Theft
- *Chat systems offer a way for viruses to enter the enterprise.
- *Hidden links using shortener sites such as Bit.ly can camouflage .exe payloads
- *Socially engineered attacks. Email from social network is 99% chance of being read.
- *Social network accounts are routinely hacked creating potentially embarrassing or worse security issues.

Law Firm Security Guide

Protect Against Physical Attacks:

- *Create a secure physical environment – secure paper check books, sensitive data, and make sure building and floor access are limited to authorized personnel.
- *Keep close tabs on temporary and laborer staff
- *Train the staff in security awareness. Know who are truly authenticated visitors, not thieves, hackers roaming the hall.

Mobility Security:

- *iPhones, iPad, Android can be less secure when connecting to the main email system.
- *SSL Secure Sockets Layer Encrypted packets rather than interceptable communication at key data intersections.
- *Remote Data Wipe options (Blackberry Enterprise server (MobileMe?))
- *Third Party solutions – NotifyLink

Virus, Malware, Botnet Attacks:

- *Malware – Malicious Software targets end-users via web browsers, e-mail attachments, mobile devices and other vectors.
- *Bots, Trojans, Worms – special programs written to bypass perimeter defenses, evade detection, and resist efforts to disable it. Often targets payment data, healthcare records, trade secrets.
- *Use Anti-Virus programs that update daily (Trend Micro, AVG, Kapersky, Norton)
- *After infection Remove pc from network and run – Hijack This/Crap Cleaner, Rkill (kills processes), ComboFix, Malware Bytes, Spyware Doctor. Or Reimage pc with Ghost or Acronis.

Protect Against Direct Scam Attacks:

- *Know that there are tons of scams being created every day. Madoff, Rothstein, Stanford Fiduciary are just the big-time examples.
- *Direct Scams – Phony phone calls asking for credit card info, fake clients, fake invoice letters. (Fake Department of Corporations, Fake domain registration letters, Fake Magazine Subscription Renewals)
- *Indirect Scams –Phishing Attacks geared to trick users into entering password information, or private information. Emails may come from friends or trustworthy sources such as banks or social media (Facebook). May be bribes, or offers of great wealth.
- *Inside Information—Undercover Thieves. Background checks, financial well-being important. 45% of IT Directors identify unauthorized access of data by insiders.

Law Firm Security Guide

Securing the Edge from Hackers:

- *Firewall
- *Log files
- *Firewall Monitoring
- *Firewall add-ons (Botnet, antivirus, content filtering, packet inspection)
- *Close unnecessary ports
- *Juniper, Checkpoint, cisco, Fortinet, Sonicwall, Watchguard, Palo Alto, Astero
- *Spam Filtering

Disposal of Equipment:

- *Copiers contain hard drives that should be erased forensically before they are given back to the leasing company.
- *Computers, laptops, Cell phones and more may contain vital data which should be wiped clean before they are discarded or repurposed.

Preparing for Disaster Scenarios:

- *Threats: Fire, Water Damage, Hurricane, Tornados, Terrorism, Theft, Sabotage, Hardware Failure, Hardware or Software Mistakes, Massive Power Outages, \$50/gallon Gas
- *Put servers in Datacenter. Create Remote access capability (Terminal Server or Citrix)
- *Put phone switch in Datacenter. IP connectivity, work from home.
- *Create replication or off-site backup plan
- *Scan all important paper documents
- *Keep copies of valuable software/documentation in other locations
- *Recovery plan, Action plan, Updated contact list, Emergency Hotline

New Attacks that may appear as time goes on:

- *Mailing of sensitive data used in Electronic Discovery may need to be encrypted before mailing and sent out in encrypted hardware. Send the encryption key separately.
- * Consider email tracking, rights protected mail solutions. Rather than sending text-based mail, send a link to the mail item which can be accessed on a secure website. This allows you to lock down mail, give view-only rights, eliminate printing (other than screen print), give a user limited time access to email communications, and be able to track # of reads and more. This is also very useful if you accidentally send an email that should not have been sent. In most cases you cannot retract an email sent. However with a Rights Protected Email solution you can revoke rights to an email message before a recipient reads the message. It also protects your communication from blind forwarding, and eliminates threats that may exist on the recipient's email system.