



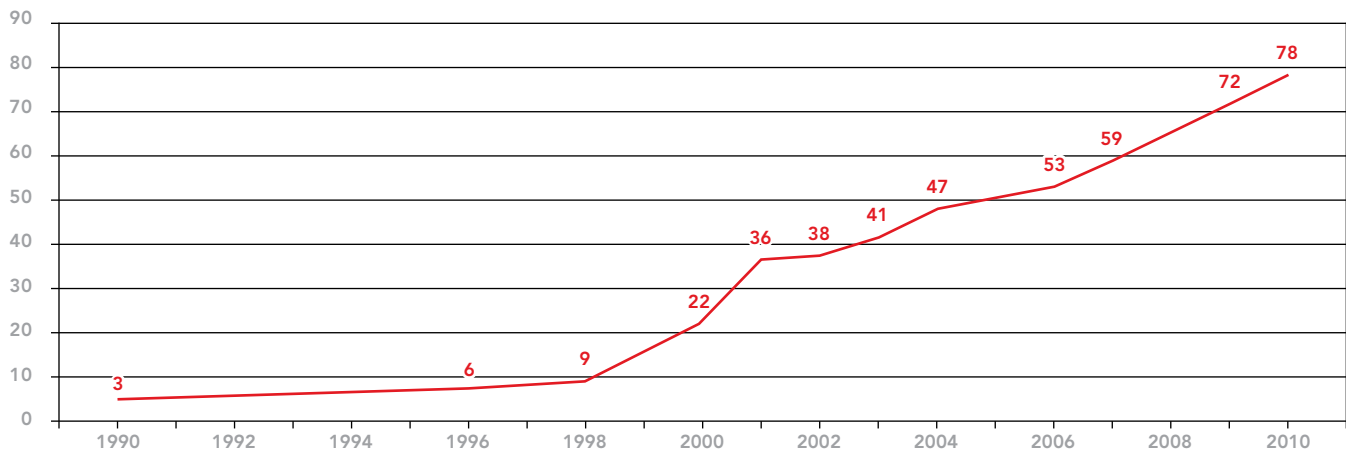
LAW FIRMS AND RISK CONTROL:

Information Security and Confidentiality Survey Results

CNA's Large Law Firm team is focused on providing high quality Risk Control advice to our clients. As part of our efforts to help law firms identify, understand and manage the risks relating to data security, privacy and the use of technology, CNA conducted a survey of our law firm professional liability policyholders.

The survey information was gathered to determine what law firms are currently doing to manage and identify technological risks. The results were then analyzed and used to identify and share the most effective and innovative risk control techniques and to provide our clients with insight into Risk Control best practices and what their peer law firms are doing to manage and identify the risks related to data security, privacy and the use of technology.

QUESTION 1: WE HAVE HAD A WRITTEN POLICY REGARDING IT SECURITY AND/OR DATA PRIVACY SINCE:



IT SECURITY/PRIVACY POLICIES IN PLACE (% total respondents)

As of 2010, 78% of the responding firms have a policy in place.

Over 50% of the firms indicate having written policies in place as of 2005.

In approximately 2005, the rise in identity theft-related crime, the widening adoption of state breach notification laws and several high profile privacy breaches converged, creating a spike in breach activity and public awareness.¹

QUESTION 1A: PLEASE IDENTIFY ANY THIRD PARTY VENDORS OR SPECIALISTS THAT YOU USED TO ASSIST IN DEVELOPING YOUR POLICY:

The responses included a variety of resources, including:

- Privacy and security consulting firms – gap analysis related to standards such as ISO/IEC 27002 and ISF Standard of Good Practice for Information Security.
- Information technology companies and vendors.
- The firm's own attorneys.
- Templates provided by the Association of Legal Administrators.

¹ DataLossDB, Open Security Foundation, 1/1/00 through 12/31/10. Data accessed February 8, 2011, <http://datalossdb.org/>

Any organization handling sensitive or nonpublic personal information should institute and monitor compliance with privacy policies. In general, a privacy policy details what information is gathered from the persons or entities that the law firm does business with, how it is protected, and the circumstances under which this information may be shared with a third party. Specific regulatory guidelines may apply to a law firm's privacy policy.

An information security policy should be designed to address how information handled by the firm should be protected. The policy should take the form of a written statement designed to protect the firm's information assets against accidental or malicious disclosure, modification or destruction. The policy should:

- Include the security objectives of preserving the confidentiality, integrity and availability of the organization's information assets.
- Address network access by employees, contractors or any other person with access to the company's network.
- Require a signed acknowledgement by all parties to which the policy applies.

QUESTION 2: WE HAVE A WRITTEN SECURITY INCIDENT RESPONSE PLAN THAT ADDRESSES THE FOLLOWING: (CHECK ALL THAT APPLY)

- | | |
|--|---|
| <input type="checkbox"/> Network intrusion | <input type="checkbox"/> Network disruption |
| <input type="checkbox"/> Regular review of compliance with policy | <input type="checkbox"/> Denial of services attacks |
| <input type="checkbox"/> Compliance with breach notification laws | <input type="checkbox"/> Privacy/confidentiality breaches |
| <input type="checkbox"/> Audit and testing of responses to incidents of breaches | <input type="checkbox"/> Data loss |

56% of responding firms indicated having written incident response plans in place.

33% of those firms with a written plan indicated that they conduct auditing and testing of responses to incidents of breaches.

Of the firms with response plans the following was indicated of the specific elements that are included in these plans:



A security incident response plan should address both direct attacks, such as hacking and privacy breaches, and indirect attacks, such as virus and malicious code attacks. Plans should be tested at least annually to ensure that all individuals responsible for implementing recovery operations are proficient in their respective roles. Basic elements of a response plan should include:

- A designated senior member of law firm staff to coordinate and implement the response plan.
- Provisions for immediate investigation of the incident.
- Steps which should be taken to contain the breach and close off existing vulnerabilities or threats to sensitive information.
- A list of entities to be notified in the event of a breach or attack.
 - This may include law enforcement, insurance carriers, customers, credit bureaus and other businesses that may be affected by the incident.

QUESTION 3: WE HAVE A SPECIFIC POLICY TO ADDRESS INTERNATIONAL TRANSFER OF PERSONALLY IDENTIFIABLE INFORMATION. (YES OR NO)

69% of responding firms do not have a specific policy.

Privacy regulations vary by country and local laws may have a significant impact on allowable safeguards.

QUESTION 4: WE DO NOT PERMIT ACCESS TO OUR NETWORK VIA UNSECURE PUBLIC WIRELESS NETWORKS. (YES OR NO)

53% of responding firms do not allow such access.

Lack of effective encryption and authentication protocols on public networks may allow attackers to access the firm's networks. If it is necessary for mobile users to access the firm's networks via public wireless networks or hotspots, access should only be allowed by secure means, such as the use of a virtual private network or VPN connection. Users should be educated about the risks presented by "rogue hotspots." Rogue hotspots are temporary access points that are set up by attackers and may look like authentic hotspots.

QUESTION 5: WE DO NOT ALLOW NON-FIRM ISSUED EQUIPMENT TO ACCESS OUR NETWORKS. (YES OR NO)

53% of responding firms do not allow such access.

Systems of other parties such as vendors, contractors, and employee home computers may be less secure than the firm's and provide intruder access and the potential to spread malicious code to the firm's network. If direct network access is allowed from non-firm issued and controlled equipment, the firm should set and enforce minimum standards for this equipment, specifically addressing:

- Maintenance of application and operating system security updates.
- Use of a properly configured personal firewall.
- Use of up-to-date anti-virus software.

QUESTION 6: WE REQUIRE THE FOLLOWING SECURITY METHODS FOR REMOTE ACCESS TO FIRM NETWORKS: (CHECK ALL THAT APPLY)

- | | |
|--|--|
| <input type="checkbox"/> VPN | <input type="checkbox"/> Password |
| <input type="checkbox"/> Encryption | <input type="checkbox"/> Content filtering |
| <input type="checkbox"/> Two factor authentication | |

34% of responding firms indicated encryption, passwords and two factor authentication are utilized.

50% of responding firms indicated use of encryption and passwords.

The remaining responses did not indicate combined use of passwords and encryption to secure remote access.

QUESTION 6 (cont'd):

Remote user systems often present the weakest link in otherwise secure networks. Data is vulnerable during transport over public networks through eavesdropping by unauthorized individuals. The devices may be less secure, and there is likely less physical security in the environments in which these devices are used.

- All remote access should require user identification and authentication, utilizing strong passwords.
- Due to the potential accessibility of remotely connected devices by those with malicious intent, utilization of two-factor authentication techniques is recommended. These techniques require that in addition to a personal password, authentication requires the use of a device (security token, smart card, etc.) or provides a biometric identifier (fingerprint, voice pattern, etc).
- Encryption should be used to provide secure communication between the remote users and the firm's networks. A Virtual Private Network is the most common method to provide this protection. When properly implemented, e-mail and other traffic will be encrypted, reducing the risk of a privacy breach.

**QUESTION 7: WE RESTRICT ACCESS TO BLOGS OR SOCIAL NETWORKING SITES IN THE FOLLOWING WAYS:
(CHECK ALL THAT APPLY)**

- | | |
|--|---|
| <input type="checkbox"/> No attorney access at work to any such sites | <input type="checkbox"/> No staff access at work to any such sites |
| <input type="checkbox"/> Allow access to some sites, but not others
(please specify restricted sites) | <input type="checkbox"/> No attorney or staff identification of connection
with firm on such sites |
| <input type="checkbox"/> Allow access, but monitor participation | <input type="checkbox"/> Allow access and posts with prior approval |
| <input type="checkbox"/> No restrictions | |

50% of the responding firms indicated no restrictions regarding the access of firm employees to blogs or social networking sites.

Where firms restricted access to social media at work:

- 19% indicated no attorney access to any such sites at work.
- 16% indicated no staff access to any such sites at work.
- 13% indicated access is allowed to some sites, but not others.

Where access is allowed, the firm responses indicated the formal restrictions that are in place:

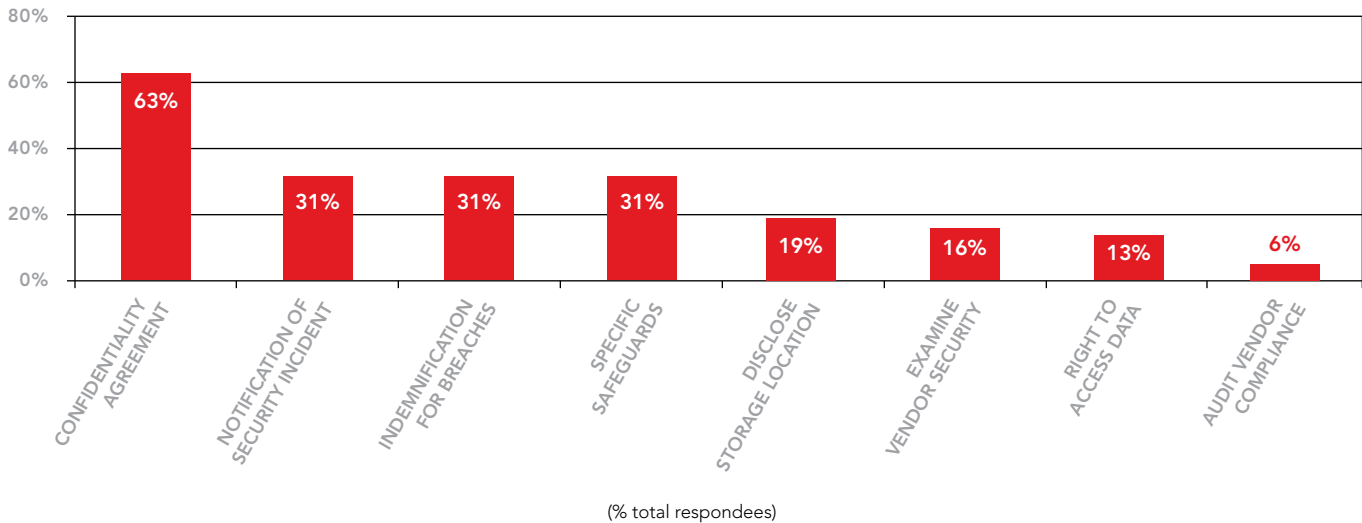
- 13% indicated that no attorney or staff identification of their connection with the firm is allowed on such sites.
- 13% indicated that access is allowed, but participation is monitored.
- 16% indicated that access and posts are allowed with prior approval.

Social media applications which firms restricted from use included Facebook, LinkedIn, Twitter and an instant messaging program.

At a minimum, law firms should develop and enforce written guidelines regarding the use of social media by firm employees. The goal of these guidelines should be to protect client privacy, prohibit misleading and harassing statements, and designate individuals who are authorized to speak on behalf of the firm.

QUESTION 8: IN DEALING WITH THIRD PARTY PROVIDERS/BUSINESS PARTNERS/VENDORS, WE: (CHECK ALL THAT APPLY)

- Require examination of their written internal security policies and procedures
- Require that they sign confidentiality agreements
- Audit their compliance with these policies and agreements
- Require they notify you of all security incidents or breaches potentially affecting their data
- Require that they indemnify you for breaches of information entrusted to them
- Specify minimum required practices for protecting sensitive and confidential information in their care
- Require that they notify you of the geographic locations where your data is stored
- Require the right to access data at the vendor's locations



63% of responding firms indicated that a confidentiality agreement is in place with providers and vendors to whom sensitive information is entrusted.

31% required indemnification or notification in the event that the provider experienced a breach.

31% of the firms specified minimum required practices for protecting sensitive and confidential information in the provider's care, but only 2% of the firms required examination of the provider's written internal security procedures.

Security breaches caused by 3rd party custodians of sensitive information account for between 30 – 40% of all privacy breaches.² Some examples of third parties to whom businesses typically entrust sensitive information include:

- Network and application hosting vendors.
- Financial, payment and billing service providers.
- Data backup and recovery services.
- Document shredding and data destruction services.
- Records management services (paper and electronic) – archival storage, document scanning services, etc.
- Business process outsourcing operations.

Since 2005, the Federal Trade Commission (FTC) has settled numerous cases against companies for privacy issues ranging from failure to safeguard private information to failure to comply with their own privacy policies. One of the common requirements of FTC consent orders is for the law firm to develop and take reasonable measures to retain service providers that appropriately safeguard personal information, and to be able to monitor their safeguarding of personal information.³

² 2007 Annual Study: US Cost of Data Breach, Understanding Financial Impact, Customer Turnover, and Preventative Solutions, conducted by Ponemon Institute, LLC, November 2007.

³ Federal Trade Commission Business Center, Legal Resources, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html

QUESTION 8 (cont'd):

These reasonable measures can include:

- Selecting service providers that have previously demonstrated the capability to maintain safeguards over personally identifiable information.
- Including contract provisions requiring providers to maintain such safeguards during the course of the contract.
- Requiring written certification that the provider maintains a written, comprehensive information security program compliant with applicable privacy laws.

QUESTION 9: WE HAVE DEVELOPED SPECIAL POLICIES OR PROCEDURES REGARDING IT AND DATA SECURITY IN RESPONSE TO A SPECIFIC CLIENT REQUEST. (YES OR NO)

59% of responding firms indicated that they had developed special IT/data security policies or procedures in response to a client's request.

Maintaining effective information technology and data security policies and procedures are concerns shared by corporations, clients and the general public as well as law firms. It is a good business practice to develop and implement proper policies and procedures before a client requests it.

QUESTION 10: WE HAVE A CURRENT NETWORK TOPOLOGY MAP. (YES OR NO)

91% of responding firms indicated having a current network topology map.

Maintaining a current map of network topology is a basic step in managing network security configuration. *Configuration Management* is a process that includes procedures to track changes and evaluate changes to hardware, software and network configurations to ensure that changes to the system do not unintentionally or unknowingly diminish security. Seemingly insignificant changes to information systems can have a significant impact on the security of those systems.

Systems are constantly scanned and probed by potential intruders searching for exploitable weaknesses that may be introduced by these changes. Locking down system configuration makes it much more difficult for unauthorized executable files or malicious code to be surreptitiously installed.

QUESTION 11: WE TRACK THE WHEREABOUTS OF ALL PORTABLE MEDIA AND STORAGE DEVICES. (YES OR NO)

34% of responding firms track the whereabouts of portable media and storage devices.

Portable media storage devices may contain unprotected confidential firm or client data. Tracking the location of these devices can help prevent privacy breaches and the misappropriation of data.

QUESTION 12: WE PLACE LIMITS AND SECURITY ON THE USE OF PORTABLE MEDIA IN THE FOLLOWING WAYS: (CHECK ALL THAT APPLY)

- | | |
|--|---|
| <input type="checkbox"/> Require full encryption of all data | <input type="checkbox"/> Require encryption of certain data |
| <input type="checkbox"/> Restrict use of USB and other portable storage devices (but not laptop computers) | <input type="checkbox"/> Limit storage to data immediately necessary and require deletion after use |
| <input type="checkbox"/> Other | |

Almost 60% of responding firms encrypt all or some of the data stored on portable devices and media.

Other controls indicated included:

- Client / server configuration with no local storage.
- Restricted access to and use of removable media.

Physical theft and loss of desktop PCs, laptops, PDAs, tapes, disks, USB drives or other devices and media create significant risks to the information stored on these devices.

The 2010 – 2011 *Global Fraud Survey* conducted by Kroll, an international risk consulting company, revealed that 27% of respondents experienced data theft between 2009 and 2010. 40% of those respondents were professional service firms. Almost half of all privacy breaches arise from physical loss or theft of devices or media containing sensitive information.⁴

Prevention of unauthorized access to sensitive information on end user devices requires the development of a multileveled strategy which addresses the following:

- Is the risk of storing sensitive information on end user devices or removable media worth the benefit obtained?
- With respect to end user devices, are the organization's information retention policies being followed? Are appropriate sanitization methods used to remove information from devices and media as soon as no longer needed?
- If storing sensitive information on end user devices or removable media is deemed necessary, are levels of physical and data security in place appropriate to the level of exposure?

In many cases, analysis will lead to the conclusion that the need for storing information on devices that are difficult to secure is not worth the benefit, given today's threat environment. It may be determined that either that no storage is necessary or that storage can be greatly restricted. Clear, enforceable information security policies detailing the type of data that can be stored and where is a first step, but technology-based solutions are also typically necessary to balance information access needs with security.

If storage of sensitive information on *removable media* (including but not limited to laptops, PDAs, USB drives, tapes, disks, hardcopy, etc.) is determined to be critical to business processes, encrypt the data and ensure that encryption keys are distributed securely and independently from the encrypted information.

QUESTION 13: WE MAINTAIN A COMPREHENSIVE INVENTORY OF ALL HARDWARE AND SOFTWARE CONNECTED TO OUR NETWORK. (YES OR NO)

91% of responding firms indicated that a comprehensive inventory of all hardware and software connected to their networks is maintained.

A wide variety of software solutions are available to maintain a perpetual inventory. Firm hardware that is no longer connected to a network is likely to contain confidential data and cannot be monitored. The installation of unauthorized software presents a security risk that can result in theft of data through access to the network. Additionally, a perpetual inventory allows firms to monitor compliance with software licensing agreements and prevent piracy.

⁴ DataLossDB, Open Security Foundation, 1/1/06 through 12/31/09. Accessed October 7, 2010, <http://datalossdb.org/>

QUESTION 14: PLEASE DESCRIBE THE STEPS YOU TAKE TO ENSURE THAT SOFTWARE SECURITY PATCHES, FIREWALLS, VIRUS DEFINITIONS, AND OTHER SECURITY SOFTWARE ARE REGULARLY UPDATED ON ALL FIRM EQUIPMENT:

A wide variety of responses to this question were received, reflecting varying approaches to managing software vulnerabilities.

A general summary of best practices in this area include:

- Subscribing to patch notification services from vendors for software utilized, reviewing and evaluating available patches at least weekly, and preferably daily.
- Where possible, enabling automatic update capabilities.
- Testing and installing critical security patches and upgrades within 24 hours of availability and installing all patches within 30 days of availability.

Formal patch management procedures should include the following:

- An inventory of IT resources — hardware equipment, operating systems and software applications used within the organization.
- Monitoring of security sources for vulnerability announcements, patch and non-patch remediations, and emerging threats that correspond to the software within the firm's system inventory.
- Establishment of a priority system for the order in which the organization remediates vulnerabilities.
- Testing of patches and non-patch remediations on IT devices that use standardized configurations.
 - Verify that the remediation will not disrupt operations or degrade security elsewhere on the network before implementing in the firm's production environment.
- Automated deployment of patches to IT devices, using enterprise patch management tools.
- Automatic update of applications whenever possible and appropriate.
- Verification of vulnerability remediation through network and host vulnerability scanning.

QUESTION 15: PLEASE DESCRIBE HOW YOU ENSURE CONFIDENTIALITY AND SECURITY WHEN DELETING DATA AND OR RETIRING EQUIPMENT:

Responses to this question indicated a high degree of awareness of appropriate data destruction techniques.

In general, most responses indicated compliance with the following recommended best practices:

- Destroy sensitive information using a technique that leaves no residual information as soon as it is no longer needed. For data on electronic media, including hardware which is scheduled for disposal:
 - Degauss (demagnetize) the media,
 - Physically pulverize the media, or
 - Irreversibly erase the media using a technique that leaves no residual information in accordance with DOD Standard 5220.22-M, NIST 800-88 or their equivalent.

QUESTION 16: PLEASE LIST THE TITLES OF KEY PERSONNEL (ATTORNEYS AND OTHERS) RESPONSIBLE FOR MEETING YOUR IT SECURITY AND DATA PRIVACY OBLIGATIONS:

42% of responding firms indicated an officer or partner as one of the individuals responsible for meeting IT security and data privacy obligations.

QUESTION 16A: ARE THESE PERSONNEL REQUIRED TO HAVE ANY SPECIAL TRAINING OR CERTIFICATIONS?

25% of firm responses indicated that special training or certifications are required of personnel responsible for the firms' IT security and data privacy.

Many of the firm indicated a multi-disciplinary approach to IT security and data privacy, with involvement of firm management, IT, compliance, ethics, human resources, facilities and risk management personnel.

Due to the wide variety of threats and the increasing potential for high severity losses, it is important for firms to ensure that physical, technical and procedural controls are addressed by parties with appropriate expertise within the firm. As information security is a rapidly evolving area, ongoing education is necessary. Additionally, management of these risks should have the support of senior firm management.

QUESTION 17: HOW OFTEN DO YOU PROVIDE TRAINING AND EDUCATION TO ALL ATTORNEYS AND OTHER STAFF REGARDING IT SECURITY AND DATA PRIVACY?

Approximately 40% of the responding firms indicated that training is provided once per year, at hire only, or that no training is provided. The remaining responding firms indicated that a combination of initial training, annual updates and ongoing awareness or refresher training is provided throughout the year.

Most major indicators of the current causes of information security threats identify users, who are easily misled, as a leading, if not the leading, vulnerability for law firms. As technical network security controls have improved, attackers have increased their efforts toward sophisticated and effective social engineering techniques. Increasingly well known threats, such as phishing, have evolved into more complex attacks, such as spear phishing and whaling. The payloads of viruses and Trojan horses which are introduced as a result of user interaction have also become more damaging.

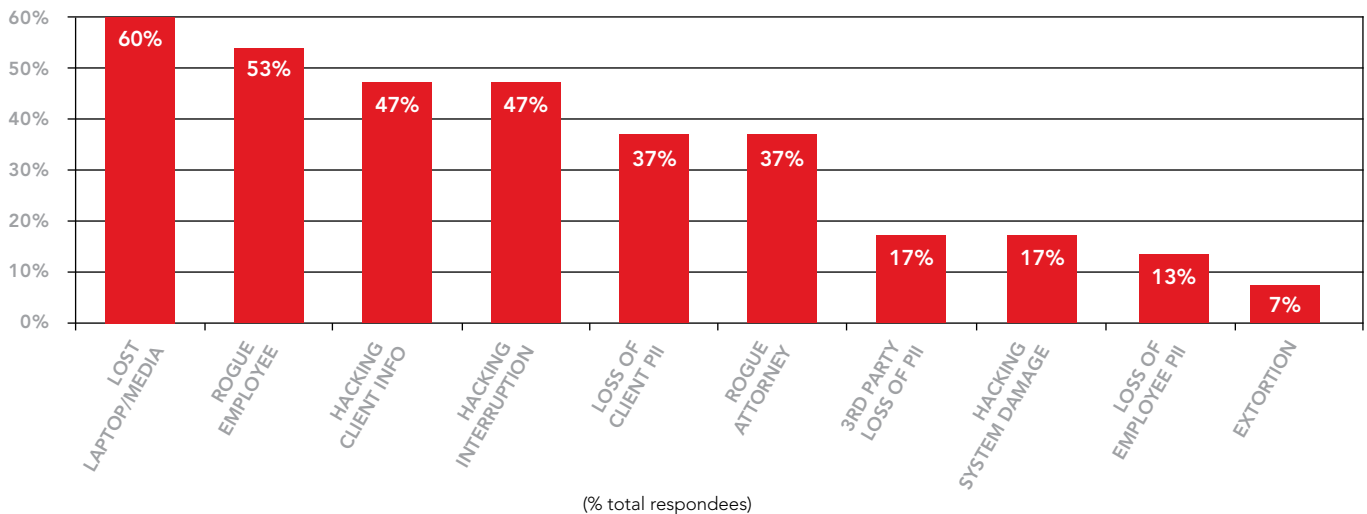
While law firms that provide initial training with annual updates are meeting a minimum standard of care, the dynamic nature of changing information security threats warrant more frequent awareness efforts, such as monthly updates addressing key concerns.

Ideally, firms should:

- Train users annually on the firm's privacy and acceptable use policies. Require employees to sign an agreement that they understand and will abide by these policies.
- Provide annual security awareness training for all users. The training should provide information on how to recognize and report security threats. Periodic alerts and reminders should be provided to alert employees to new threats as they emerge, and to maintain vigilance in following appropriate procedures to avoid known vulnerabilities.

FINAL THOUGHTS: WHEN YOU THINK ABOUT CONFIDENTIALITY, IT SECURITY AND DATA PRIVACY RISKS, WHAT ARE THE THREE AREAS THAT CONCERN YOU THE MOST? (CHECK ALL THAT APPLY)

- Rogue attorney
- Rogue employee
- Extortion threat relating to your clients' sensitive data
- Hacking/network breach causing damage to your systems
- Hacking/network breach causing business interruption
- Hacking/network breach causing damage to, loss of, or release of client information
- Lost laptop or other portable media or storage device containing confidential information
- Loss of employee personally identifiable information (PII)
- Loss of client personally identifiable information (PII)
- Loss of third party personally identifiable information (PII)



Key concerns of the responding firms align with current high frequency and severity breach activity.

ADDITIONAL RESOURCES:

Are Your Company's Wireless Networks Putting Your Sensitive Data at Risk?

http://www.cna.com/vcm_content/CNA/internet/Static%20File%20for%20Download/Risk%20Control/Network%20Security/CNA%20-%20Wireless%20Technology.pdf

Security for Telecommuting and Broadband Communications, National Institute of Standards and Technology

http://www.nist.gov/customcf/get_pdf.cfm?pub_id=151263

SURVEY SOURCE INFORMATION:

Survey results compiled from November 2010 survey of 33 law firms in the U.S. and U.K., ranging in size as follows:

- Less than 100 attorneys: 10%
- 100 – 499 attorneys: 37%
- 500 – 999 attorneys: 15%
- 1000+ attorneys: 18%

CONTACT INFORMATION FOR AUTHORS OF SURVEY RESULTS AND ANALYSIS:

Stephen F. Douglas, CSP, ARM, Risk Control Director, CNA Technology, San Diego;

Stephen.Douglas@CNA.com; (760) 613-8417

Stephen F. Douglas, CSP, ARM, is Risk Control Director of CNA Technology, which provides insurance and risk control solutions to businesses in information technology and Internet services, telecommunications, and electronic component and hardware manufacturing.

Gawain Charlton-Perrin Esq., Risk Control Consulting Director, Lawyers Professional Liability, Chicago;

Gawain.Charlton-Perrin@CNA.com; (312) 822-2033

Gawain Charlton-Perrin is a Risk Control Consulting Director for CNA's Lawyers Professional Liability Insurance Program, which provides risk control training and consulting services to practicing lawyers and their firms, regularly addressing them throughout the country on ethics and practice management related topics.

ADDITIONAL CONTACTS FOR MORE INFORMATION:

Stuart Pattison, Vice President, Underwriting, Lawyers Professional Liability, New York;

Stuart.Pattison@CNA.com; (212) 440-7447

Graham Delf, Underwriting Consultant, Underwriting, Lawyers Professional Liability, New York;

Graham.Delf@CNA.com; (212) 440-7054

The purpose of this article is to provide information, rather than advice or opinion. It is accurate to the best of the author's knowledge as of the date of the article. Accordingly, this article should not be viewed as a substitute for the guidance and recommendations of a retained professional. In addition, CNA does not endorse any coverages, systems, processes or protocols addressed herein unless they are produced or created by CNA.

Any references to non-CNA Web sites are provided solely for convenience, and CNA disclaims any responsibility with respect to such Web sites.

To the extent this article contains any examples, please note that they are for illustrative purposes only and any similarity to actual individuals, entities, places or situations is unintentional and purely coincidental. In addition, any examples are not intended to establish any standards of care, to serve as legal advice appropriate for any particular factual situations, or to provide an acknowledgement that any given factual situation is covered under any CNA insurance policy. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All CNA products and services may not be available in all states and may be subject to change without notice.

CNA is a registered trademark of CNA Financial Corporation. Copyright © 2011 CNA. All rights reserved.