



# Unlocking the Mysteries of Cyber Liability: What Every Lawyer Needs to Know

NOVEMBER 3, 2015 - CONCORD

NOVEMBER 4, 2015 - GREENSBORO

NOVEMBER 5, 2015 - CARY

# Unlocking the Mysteries of Cyber Liability: What Every Lawyer Needs to Know

## TABLE OF CONTENTS

pg. 3	Agendas
pg. 6	List of Presenters
pg. 9	Cyber Security for Trust Accounting
pg. 10	Checklist for Protecting Your System and Client Data
pg. 11	Common Types of Malware
pg. 12	Cyber Resources
pg. 17	Email Encryption: How Secure is Your Email?
pg. 18	Email Encryption Resources
pg. 20	Cyber Risk Presentation: Breach Responses & Coverages
pg. 28	Sample Form: Incident Response Plan
pg. 41	Protecting Yourself From Cybercrime Dangers: The Steps You Need to Take

# Unlocking the Mysteries of Cyber Liability: What Every Lawyer Needs to Know

## CONCORD AGENDA

8:30 a.m. -  
9:00 a.m.

Registration

9:00 a.m. -  
10:00 a.m.

Cyber Breaches: What Are the Threats?

***Ric Messier, Professor from Champlain College in VT;***

***Clark Walton, lawyer and owner of Reliance Forensics in Charlotte; Jim Granozio, FBI agent***

What is cyber liability?

- A. How do hackers and others get into our systems?
- B. The dangers of e-mail.
- C. What do they want (money, data, ransom)?
- D. Examples of law firm breaches

10:00 a.m. -  
10:15 a.m.

Break

10:15 a.m. -  
11:15 a.m.

Cyber Safeguards and Procedures

***Ric Messier, Professor from Champlain College in VT and***

***Clark Walton, lawyer and owner of Reliance Forensics in Charlotte***

- A. Best practices for protecting data and confidential information.
- B. Internal threats.
- C. Mobile devices.
- D. Encryption: What is it and do you need it?
- E. Protecting your trust account.

11:15 a.m. -  
11:30 a.m.

Break

11:30 a.m. -  
12:30 p.m.

Responding to a Data Breach

***Thomas A. Widman, CPCU, AMIM, President & CEO of Identity Fraud, Inc.;***

***Charles Marshall, Brooks Pierce; Jim Granozio, FBI agent***

- A. North Carolina law and notification requirements.
- B. Preparing a breach response plan.
- C. Notifying law enforcement, regulatory authorities and insurers.
- D. Costs associated with a response.
- E. Insurance coverage and exclusions.
- F. Ethical Obligations

12:30 p.m. -  
2:00 p.m.

Networking Lunch

# Unlocking the Mysteries of Cyber Liability: What Every Lawyer Needs to Know

GREENSBORO AGENDA

8:30 a.m. -  
9:00 a.m.

Registration

9:00 a.m. -  
10:00 a.m.

Cyber Breaches: What Are the Threats?

***Ric Messier, Professor from Champlain College in VT;***

***Clark Walton, lawyer and owner of Reliance Forensics in Charlotte; John Maser, FBI agent***

What is cyber liability?

- A. How do hackers and others get into our systems?
- B. The dangers of e-mail.
- C. What do they want (money, data, ransom)?
- D. Examples of law firm breaches

10:00 a.m. -  
10:15 a.m.

Break

10:15 a.m. -  
11:15 a.m.

Cyber Safeguards and Procedures

***Ric Messier, Professor from Champlain College in VT and***

***Clark Walton, lawyer and owner of Reliance Forensics in Charlotte***

- A. Best practices for protecting data and confidential information.
- B. Internal threats.
- C. Mobile devices.
- D. Encryption: What is it and do you need it?
- E. Protecting your trust account.

11:15 a.m. -  
11:30 a.m.

Break

11:30 a.m. -  
12:30 p.m.

Responding to a Data Breach

***Thomas A. Widman, CPCU, AMIM, President & CEO of Identity Fraud, Inc.;***

***Clark Walton, lawyer and owner of Reliance Forensics in Charlotte; John Maser, FBI agent***

- A. North Carolina law and notification requirements.
- B. Preparing a breach response plan.
- C. Notifying law enforcement, regulatory authorities and insurers.
- D. Costs associated with a response.
- E. Insurance coverage and exclusions.
- F. Ethical Obligations

12:30 p.m. -  
2:00 p.m.

Networking Lunch

# Unlocking the Mysteries of Cyber Liability: What Every Lawyer Needs to Know

## CARY AGENDA

8:30 a.m. -  
9:00 a.m.

■ Registration

9:00 a.m. -  
10:00 a.m.

■ Cyber Breaches: What Are the Threats?

***Ric Messier, Professor from Champlain College in VT; Jessica Nye, FBI agent***

What is cyber liability?

- A. How do hackers and others get into our systems?
- B. The dangers of e-mail.
- C. What do they want (money, data, ransom)?
- D. Examples of law firm breaches

10:00 a.m. -  
10:15 a.m.

■ Break

10:15 a.m. -  
11:15 a.m.

■ Cyber Safeguards and Procedures

***Ric Messier, Professor from Champlain College in VT and Brian Love, attorney, Teague Campbell***

- A. Best practices for protecting data and confidential information.
- B. Internal threats.
- C. Mobile devices.
- D. Encryption: What is it and do you need it?
- E. Protecting your trust account.

11:15 a.m. -  
11:30 a.m.

■ Break

11:30 a.m. -  
12:30 p.m.

■ Responding to a Data Breach

***Thomas A. Widman, CPCU, AMIM, President & CEO of Identity Fraud, Inc.;***

***Bill Bulfer, attorney, Teague Campbell; Jessica Nye, FBI agent***

- A. North Carolina law and notification requirements.
- B. Preparing a breach response plan.
- C. Notifying law enforcement, regulatory authorities and insurers.
- D. Costs associated with a response.
- E. Insurance coverage and exclusions.
- F. Ethical Obligations

12:30 p.m. -  
2:00 p.m.

■ Networking Lunch

**Unlocking the Mysteries of Cyber Liability:  
What Every Lawyer Needs to Know  
November 3 – 5, 2015**

**List of Presenters**

**Bill Bulfer** – Partner – Teague Campbell Dennis & Gorham, LLP

Email: [wbulfer@teaguecampbell.com](mailto:wbulfer@teaguecampbell.com)

P: 828-254-4515

Bill's practice is focused mainly on liability and coverage issues. Bill has defended numerous wrongful death claims, professional liability claims, and general liability claims. He has provided coverage opinions, prosecuted and defended declaratory judgment actions, and has provided legal advice on the creation and modification of coverage documents on behalf of insurers. Bill assists his clients with drafting cutting edge policies, including cyber-liability coverage and drone coverage forms. He dedicates a significant portion of his coverage practice to local governments and trucking & commercial transportation clients.

**Jim Granozio** – Special Agent – Federal Bureau of Investigation

Email: [james.granozio@ic.fbi.gov](mailto:james.granozio@ic.fbi.gov)

P: 704-672-6351

Special Agent James Granozio joined the FBI in July 2003 and was assigned to the Newark Field Office where he investigated organized crime, public corruption and cyber crime matters. While on the cyber squad, Agent Granozio spent two years working as an undercover Agent targeting online child sexual predators leading him to become the Acting Supervisor. In 2009, Agent Granozio was deployed to Afghanistan where he operated as a hostage negotiator before being selected for a supervisory position in the FBI's Cyber Division in Washington, D.C. In 2012, Agent Granozio was transferred to the Charlotte Field Office where he now investigates cyber national security matters and serves as FBI Coordinator for the Charlotte and Eastern Carolina InfraGard Chapters.

**Brian Love** – Associate – Teague Campbell Dennis & Gorham, LLP

Email: [BLove@teaguecampbell.com](mailto:BLove@teaguecampbell.com)

Phone: 919-873-0166

Brian is an Associate at Teague Campbell Dennis & Gorham, LLP. His practice involves civil litigation and insurance coverage issues. He has appeared on behalf of clients in North Carolina's state and federal courts, the North Carolina Industrial Commission and has appeared before the North Carolina Court of Appeals, the North Carolina Supreme Court, and the United States Court of Appeals for the Fourth Circuit. Brian's civil litigation practice is primarily concentrated in the areas of complex construction defect claims, products liability and general tort liability. Brian has also provided coverage opinions, prosecuted and defended declaratory judgment actions and has provided legal advice on the creation and modification of coverage documents for insurers.

**Unlocking the Mysteries of Cyber Liability:  
What Every Lawyer Needs to Know  
November 3 – 5, 2015**

**List of Presenters**

**Charles F. Marshall – Partner – Brooks Pierce**

**Email:** [CMARSHALL@brookspierce.com](mailto:CMARSHALL@brookspierce.com)

**Phone:** 919-573-6247

Charles has counseled companies responding to data breaches, including notifications to consumers, state regulators, insurers and vendors in various states. He also helps companies identify data privacy issues on the “front-end” and implement policies to reduce the risk of a future data breach. Charles also helps digital media and e-commerce companies draft privacy policies for online services and mobile applications and to avoid risks. Charles draws on his media law experience to help clients identify and address digital and social media content, including copyright, trademark, right of publicity, and online marketing issues. He has worked with “start-up” online services, large media companies and even a national presidential campaign.

**John Maser - Special Agent – Federal Bureau of Investigation**

**Email:** [John.Maser@ic.fbi.gov](mailto:John.Maser@ic.fbi.gov)

**Phone:** 919-380-4500

John is a Special Agent for the Federal Bureau of Investigation in the Charlotte Division, Raleigh Resident Agent, currently assigned to investigate Cyber Intrusion matters, both criminal and national security. Special Agent Maser began his career as a FBI Special Agent in 2004 in the Cincinnati Division, investigating White Collar Crime and Violent Crime. Special Agent Maser has also been assigned to the Philadelphia Division, investigating Public Corruption, and to FBI Headquarters in Washington, DC, where he was a Supervisory Special Agent at the National Cyber Investigative Joint Task Force.

**Ric Messier – Assistant Professor, Program Director, Cyber Security & Digital Forensics Division of Continuing Professional Studies – Champlain College**

**Email:** [rmessier@champlain.edu](mailto:rmessier@champlain.edu)

**Phone:** 802-865-6477

Ric is currently the Program Director for Cybersecurity and Digital Forensics programs online at Champlain College. He has been involved in the information security space over the past three decades including time at small software companies all the way up to the largest Internet service providers. He has published four books in the last two years on security or forensics-related topics and recorded a number of video training titles.

**Jessica Nye – Supervisory Special Agent – Federal Bureau of Investigation**

**Email:** [Jessica.Nye@ic.fbi.gov](mailto:Jessica.Nye@ic.fbi.gov)

**Phone:** 919-380-4500

Supervisory Special Agent Jessica Nye is the current Supervisor of the FBI Cyber Squad in Raleigh. SSA Nye spent eight years working in the Baltimore Field Office on their Cyber Squad and most recently two years at FBI Cyber Division Headquarters in Washington D.C. SSA Nye has a long experience working cyber related matters to include computer intrusion investigations, intellectual property rights violations, theft of trade secrets, economic espionage and other investigations.

**Unlocking the Mysteries of Cyber Liability:  
What Every Lawyer Needs to Know  
November 3 – 5, 2015**

**List of Presenters**

**Clark Walton** – JD, EnCE, CCME, Managing Director– Reliance Forensics, LLC

Email: [clark@relianceforensics.com](mailto:clark@relianceforensics.com)

Phone: 980-335-0710

Clark Walton, Managing Director of Reliance Forensics, LLC has practiced law in Charlotte for over 10 years and has been involved in cybersecurity and digital evidence issues for over 15 years. He has personally led over 150 digital forensic investigations since co-founding Reliance. A former assistant district attorney and special federal prosecutor, he holds a Computer Science degree from the University of North Carolina at Chapel Hill and a law degree from Georgetown University Law Center.

A former CIA cyber threat analyst, Clark is a former member of the American Bar Association Advisory Committee on National Security and was a contributing author to the ABA Cybersecurity Handbook published in 2013. An adjunct law professor in the area of cybercrime, Clark was named the ABA National Outstanding Young Lawyer for 2012. He has also taught numerous CLE's and undergraduate courses, and has trained US military assets in computer forensics and digital security. He is an EnCase Certified Examiner and a Cellebrite Certified Mobile Examiner.

**Thomas A. Widman** – President & CEO – Identity Fraud, Inc.

Email: [twidman@identityfraud.com](mailto:twidman@identityfraud.com)

Phone: 925-296-2601

Tom helped pioneer identity and data theft insurance and risk management products that originated in 1997. As founder, president and CEO of Identity Fraud, Inc., he developed and is responsible for all aspects of IFI operations including product and business development for both the consumer and small business divisions. Most recently, Tom is credited with designing the nation's first Business Identity Fraud insurance product, which has been integrated into IFI's comprehensive small business "SB" data theft risk management offerings. Over the past 25 years, Tom has worked at leading US insurance brokerages and earned the CPCU and AMIM insurance designations while working in the Lloyd's insurance market in London, England. He holds his BA in Economics from the University of California at Berkeley.



## **Cyber Security for Trust Accounting**

1. Monitor your trust account daily and report suspicious activity immediately.
2. Change your banking password frequently.
3. Use updated anti-virus and anti-spyware products.
4. Log off when you have finished conducting banking business.
5. Do not click on links or open attachments to e-mails unless you are certain they are from someone you trust.
6. Do not respond to any e-mail that requests account information, account verification or banking access credentials.
7. Avoid accessing your bank accounts through unsecured networks such as hotels, internet cafes or public libraries.
8. Designate a stand-alone computer in your office that is used only for banking transactions and is limited to one or two trusted users.
9. Establish dual control of ACH and wire transactions.

## **Checklist for Protecting Your System and Client Data**

1. Adopt procedures and protocol and ensure staff is properly trained on both.
2. Email:
  - a. Use spam filters.
  - b. Be wary of attachments to and links contained in emails. These are some of the most common delivery methods for malware.
  - c. Do not update information from a link in an email message. Only update via a secure connection (“https”) and inspect website address in the address bar.
3. Internet browser:
  - a. Disable pop-ups.
  - b. Don’t accept third-party cookies.
  - c. Disable ActiveX controls.
  - d. Enable automatic updates.
4. Install malware and update it, and make sure operating systems, programs and applications are updated.
5. Use strong passwords and protect and change them frequently.
6. Encrypt, encrypt, encrypt.
7. Use a firewall. More recent versions of Windows and Mac operating systems have built-in firewall protection. Enable it.
8. Avoid using public Wi-Fi when viewing or sending client data and information.
9. Restrict access to sensitive data, both physically and electronically.
10. Do an Information Security Assessment periodically.

# Common types of malware

Malware is classified by how it propagates itself or what it does. The names and a brief description of the common types of malware appear below:



## Viruses:

Viruses are one of the most common types of malware and will do one or more of the tasks and damaging things listed in the adjacent text. Like their biological namesakes, computer viruses propagate by making copies of themselves. When an infected program runs, the virus will attempt to replicate itself by copying itself into other programs, usually while completing the malicious actions it is designed to do. Viruses often arrive in infected email attachments or via a download triggered by a click on a link in an email or on a website. Even just visiting a website can start an automatic download of a virus. Some viruses will send themselves to everyone in your contact list; others will use your computer to infect strangers as they come with their own address lists.



## Worms:

After viruses, worms are one of the next most common types of malware. Unlike a virus, a worm goes to work on its own without attaching itself to programs or files. Worms live in a computer's memory and can propagate by sending themselves to other computers in a network or across the Internet itself. As they spread on their own, they can very quickly infect large numbers of computers and may cause a firm's network – or even parts of the Internet – to be overwhelmed with traffic and slow down or stop working all together.



## Trojans:

Trojans are named after the wooden horse the Greeks used to infiltrate Troy. A Trojan is a malicious program that is disguised as, or embedded within, otherwise legitimate-looking software. Computer users often unwittingly infect themselves with Trojans when they download games, screensavers, utilities, rogue security software or other enticing and usually “free” software from the Internet. Once installed on a computer, Trojans will automatically run in the background. Trojans are used for a variety of purposes, but most frequently they will open a backdoor to a computer or capture keystrokes so that sensitive information can be collected and sent to cyber criminals. See the sidebar on page 7 for details of a large fraud involving a Trojan infection.



## Spyware:

Like Trojans, spyware also often comes in the form of a “free” download, but can also be installed automatically when you click on a link or open an attachment. Spyware will do many different things, but usually it will collect keystrokes or other information about you that will be shared with third parties without your consent. This can include usernames, passwords and surfing habits.

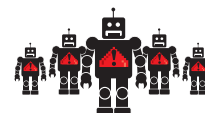
## Adware:

Adware works like spyware, but will focus on your surfing habits and will slow down or stop your browsing by taking you to unwanted sites and/or inundating you with uncontrollable pop-up ads while you are browsing the web.



## Botnets:

A botnet is a collection of software robots (“bots”) that together create an army of infected computers (known as “zombies”) that are remotely controlled by the originator. Your computer may be part of a botnet and you may not even know it. On an individual level, bots will do most of the typical malware tasks and damaging activities. When working together, botnets are used to execute denial-of-service attacks (DoS attack) or distributed denial-of-service attacks (DDoS attack). A DoS attack is accomplished when thousands of computers are told to visit a particular website or server at the same time, thereby crashing it and/or making it impossible for regular users to access it.



## Rootkits:

Once malware is installed on a system, it is helpful if it stays concealed to avoid detection. Rootkits accomplish this by hiding inside the host computer's operating system. They can be very hard to detect and will do most of the typical malware tasks and damaging activities.



## Scareware:

Scareware is plain devious. While visiting a website, a pop-up advertisement will appear with a “Your computer may be infected with harmful spyware programs. Immediate removal may be required. To scan, click ‘Yes’ below.” If you click “yes,” you download malware onto your computer.



## Ransomware:

Ransomware infections are becoming much more common recently and are usually spread by infected email attachments or website links that trigger a download. The most common type, Cryptolocker, will scramble all the data files on your computer with virtually unbreakable encryption. You learn you are infected when a pop-up window tells you that your data has been scrambled and will be deleted unless you pay a ransom within a very short period of time, typically 48 hours or so. The ransom is typically in the range of \$100 to \$300 and payable only in Bitcoins, a type of virtual currency that makes payments untraceable. It is a relatively low amount so you have an incentive to pay it as a nuisance; but as you are dealing with criminals, paying it does not guarantee that you will get your data back.



## Cyber Resources

### Cloud Computing:

- The Ethics of Cloud Computing and Software as a Service <http://www.lawyersmutualnc.com/risk-management-resources/articles/the-ethics-of-cloud-computing-and-software-as-a-service-saas>
- Keys to Selecting a Cloud Storage Provider <http://www.lawyersmutualnc.com/risk-management-resources/articles/keys-to-selecting-a-cloud-storage-provider>
- Legal Implications Regarding Data Security <http://www.lawyersmutualnc.com/risk-management-resources/articles/legal-implications-regarding-data-security>
- Practice Management Options <http://www.lawyersmutualnc.com/risk-management-resources/articles/practice-management-options>

### Cyber Insurance:

- Cyber Insurance: I don't know what it is, but am pretty sure I need it! <http://www.lawyersmutualnc.com/blog/cyber-insurance-i-dont-know-what-it-is-but-am-pretty-sure-i-need-it>
- How Much Risk in Cyber Liability? <http://www.lawyersmutualnc.com/risk-management-resources/articles/how-much-risk-in-cyber-liability>
- Lawyers Beware: A Single Data Breach Can Bring Down a Practice <http://www.lawyersmutualnc.com/risk-management-resources/articles/lawyers-beware-a-single-data-breach-can-bring-down-a-practice>
- Real Estate Attorneys Take Note: Funds Transfer Fraud or Social Engineering Fraud? <http://www.lawyersmutualnc.com/risk-management-resources/articles/funds-transfer-fraud-or-social-engineering-fraud>
- Cyber-Policies Soar on Insurance Market <http://www.lawyersmutualnc.com/blog/cyber-policies-soar-on-insurance-market>

### Mobile Security:

- Mobile Security for the Family Lawyer <http://www.lawyersmutualnc.com/risk-management-resources/articles/mobile-security-for-the-family-lawyer>
- Mobile Device Security: Has Your Client's Smartphone Been Hacked? <http://www.lawyersmutualnc.com/risk-management-resources/articles/mobile-device-security-has-your-clients-smartphone-been-hacked>
- Protecting Data on your iDevice <http://www.lawyersmutualnc.com/risk-management-resources/articles/protecting-data-on-your-idevice>
- Scamming Goes Mobile <http://www.lawyersmutualnc.com/risk-management-resources/articles/scamming-goes-mobile>

### **Email Security:**

- How Secure Is Your Email? <http://www.lawyersmutualnc.com/risk-management-resources/articles/how-secure-is-your-email>
- 7 Ways to Protect Your Email from Hackers <http://www.lawyersmutualnc.com/blog/7-ways-to-protect-your-email-from-hackers>
- 9 Things To Do If Your Email is Hacked <http://www.lawyersmutualnc.com/blog/9-things-to-do-if-your-email-is-hacked>
- 7 Steps to Avoid Email Malware <http://www.lawyersmutualnc.com/risk-management-resources/articles/7-steps-to-avoid-email-malware>
- Lawyer Clicks on Email Attachment, Loses Nearly \$300,000 <http://www.lawyersmutualnc.com/blog/lawyer-clicks-on-email-attachment-loses-nearly-300000>
- State Bar Adopts Ethics Opinion Impacting Email Communications <http://www.lawyersmutualnc.com/risk-management-resources/articles/state-bar-adopts-ethics-opinion-impacting-email-communications>

### **Office Policies:**

- Office Equipment Disposal Policy [http://files.lm2014.gethifi.com/risk-management-resources/risk-management-handouts/Equipment\\_Disposal.pdf](http://files.lm2014.gethifi.com/risk-management-resources/risk-management-handouts/Equipment_Disposal.pdf)
- Data Security Policy [http://files.lm2014.gethifi.com/risk-management-resources/risk-management-handouts/Data\\_Security\\_Policy.pdf](http://files.lm2014.gethifi.com/risk-management-resources/risk-management-handouts/Data_Security_Policy.pdf)
- Disaster Planning and Recovery [http://files.lm2014.gethifi.com/risk-management-resources/risk-management-handouts/Disaster\\_Planning.pdf](http://files.lm2014.gethifi.com/risk-management-resources/risk-management-handouts/Disaster_Planning.pdf)
- Social Media and Crisis Communications Policy [http://files.lm2014.gethifi.com/risk-management-resources/risk-management-handouts/social-media-and-crisis-communications-policy/MediaCrisis\\_Policy.pdf](http://files.lm2014.gethifi.com/risk-management-resources/risk-management-handouts/social-media-and-crisis-communications-policy/MediaCrisis_Policy.pdf)
- A 5 Item List to Check Twice- Getting Your Firm's Security Plan Off the Naughty List <http://www.lawyersmutualnc.com/risk-management-resources/articles/a-5-item-list-to-check-twice-getting-your-firms-security-plan-off-the-naughty-list>
- Electronic Records Retention and Destruction <http://www.lawyersmutualnc.com/risk-management-resources/articles/electronic-records-retention-and-destruction>
- Be ready with an Incident Response Plan <http://www.lawyersmutualnc.com/risk-management-resources/articles/be-ready-with-an-incident-response-plan>
- 5 Tips for Handling Office Equipment Disposal <http://www.lawyersmutualnc.com/risk-management-resources/articles/5-tips-for-handling-office-equipment-disposal>
- Cyber-Threats Open New Law Doors <http://www.lawyersmutualnc.com/blog/cyber-threats-open-new-law-doors>

## **Fraud/Hacking:**

- Frauds and Scams that Target Lawyer Trust Accounts [http://www.lawyersmutualnc.com/risk-management-resources/articles/frauds-and-scams-that-target-lawyer-trust-accounts?utm\\_source=Social+Engineering+Alert&utm\\_campaign=WiringInstructionsAlert&utm\\_medium=email](http://www.lawyersmutualnc.com/risk-management-resources/articles/frauds-and-scams-that-target-lawyer-trust-accounts?utm_source=Social+Engineering+Alert&utm_campaign=WiringInstructionsAlert&utm_medium=email)
- 5 Things You Should Know About Your Exposure to Computer Hacking <http://www.lawyersmutualnc.com/blog/5-things-you-should-know-about-your-exposure-to-computer-hacking>
- Do You Have a Hacker on Your Payroll? <http://www.lawyersmutualnc.com/blog/do-you-have-a-hacker-on-your-payroll-2>
- Ransomware: Has Your Computer Been Taken Hostage? <http://www.lawyersmutualnc.com/blog/ransomware-has-your-computer-been-taken-hostage>
- Profile of a Fraudster <http://www.lawyersmutualnc.com/blog/profile-of-a-fraudster>
- If you are holding funds in trust for disbursement and receive a change in payment instructions, STOP. <http://www.lawyersmutualnc.com/risk-management-resources/articles/frauds-and-scams-that-target-lawyer-trust-accounts>
- A New Twist on an Old Internet Scam [http://files.lawyersmutualnc.com/risk-management-resources/malpractice-alerts/a-new-twist-on-an-old-internet-scam/ALERT\\_newtwist\\_feb2012.pdf](http://files.lawyersmutualnc.com/risk-management-resources/malpractice-alerts/a-new-twist-on-an-old-internet-scam/ALERT_newtwist_feb2012.pdf)
- Beware Email Scam [http://files.lawyersmutualnc.com/risk-management-resources/malpractice-alerts/a-new-twist-on-an-old-internet-scam/ALERT\\_emailscam.pdf](http://files.lawyersmutualnc.com/risk-management-resources/malpractice-alerts/a-new-twist-on-an-old-internet-scam/ALERT_emailscam.pdf)
- How Can I Spot An Email Scam? <http://www.lawyersmutualnc.com/risk-management-resources/videos/risk-management-minute-clips-beware-email-scams>
- How Can I Protect Myself Against Email Scams? <http://www.lawyersmutualnc.com/risk-management-resources/videos/risk-management-minute-clips-beware-email-scams-long-version>
- Email Scams Continue to Plague Lawyers <http://www.lawyersmutualnc.com/risk-management-resources/articles/email-scams-continue-to-plague-lawyers>
- Email Scams Target North Carolina Attorney <http://www.lawyersmutualnc.com/risk-management-resources/articles/email-scams-target-north-carolina-attorney>
- Is This For Real? – Email Scams and Client Confidentiality <http://www.lawyersmutualnc.com/risk-management-resources/articles/is-this-for-real-email-scams-and-client-confidentiality>
- Canada is the New Nigeria <http://www.lawyersmutualnc.com/risk-management-resources/articles-2/canada-is-the-new-nigeria>
- There is a Deposited Prince on the Line and He Wants to Scam You <http://www.lawyersmutualnc.com/risk-management-resources/articles-2/theres-a-deposed-prince-on-line-1-and-he-wants-to-scam-you>
- Nigerian Prince Keeps on Scamming <http://www.lawyersmutualnc.com/blog/hacker-nigerian-prince-keeps-on-scamming>

### **General Security Issues:**

- Email, Internet, and the Wireless Age [http://files.lawyersmutualnc.com/risk-management-resources/risk-management-handouts/estate-planning-traps/Email\\_Internet\\_Wireless.pdf](http://files.lawyersmutualnc.com/risk-management-resources/risk-management-handouts/estate-planning-traps/Email_Internet_Wireless.pdf)
- The Cybercrime Dangers You Need to Address <http://www.lawyersmutualnc.com/blog/the-cybercrime-dangers-you-need-to-address>
- Understanding Important Cyber Security Issues <http://www.lawyersmutualnc.com/risk-management-resources/articles/understanding-important-cyber-security-issues>
- The Best Approach to Cybersecurity: Being Proactive <http://www.lawyersmutualnc.com/risk-management-resources/articles/the-best-approach-to-cybersecurity-being-proactive>
- Practice Cyber Safety or Lose Clients <http://www.lawyersmutualnc.com/blog/practice-cyber-safety-or-lose-clients>
- Top Ten Things You Can Do to Protect Your Data Today <http://www.lawyersmutualnc.com/risk-management-resources/articles/top-ten-things-you-can-do-to-protect-your-data-today>
- Lawyers Are Real-life Superheroes in Cyber-Wars <http://www.lawyersmutualnc.com/risk-management-resources/articles/lawyers-are-real-life-superheroes-in-cyber-wars>
- Malware – It Can Happen To You <http://www.lawyersmutualnc.com/risk-management-resources/articles/malware-it-can-happen-to-you>

### **Passwords:**

- Keeping Your Passwords Strong and Secure <http://www.lawyersmutualnc.com/risk-management-resources/articles/keeping-your-passwords-strong-and-secure>
- The 25 Worst Passwords Ever <http://www.lawyersmutualnc.com/blog/the-25-worst-passwords-ever>
- 8 Steps to a Perfect Password <http://www.lawyersmutualnc.com/blog/8-steps-to-a-perfect-password>
- Pssst ... What's the Password? <http://www.lawyersmutualnc.com/blog/whats-the-password>

**Specific Issues:**

- Internet Explorer Bug Squashes Browser Reliability <http://www.lawyersmutualnc.com/risk-management-resources/articles/internet-explorer-bug-squashes-browser-reliability>
- New “Google.docs” Email Phishing Scam Alert: Don’t Trust The Sender of “Important Documents” Link Even If You Know Him <http://www.lawyersmutualnc.com/risk-management-resources/articles/new-googledocs-email-phishing-scam-alert-dont-trust-the-sender-of-important-documents-link-even-if-you-know-him>
- Procrastinators: Read This! Upgrade Windows XP <http://www.lawyersmutualnc.com/articles/procrastinators-upgrade-windows-xp>
- LastPass Hacking Attempt and the State of Security <http://www.lawyersmutualnc.com/blog/lastpass-hacking-attempt-and-the-state-of-security>
- FREAKing Out about the Latest Cyber Security Issue <http://www.lawyersmutualnc.com/blog/freaking-out-about-the-latest-cyber-security-issue>
- Data of the Dead <http://www.lawyersmutualnc.com/blog/data-of-the-dead>
- Put Your Hands in the Air and Give Me Your Bitcoin <http://myemail.constantcontact.com/MALPRACTICE-ALERT--Beware-of-Ransomware.html?soid=1118263556714&aid=dDQFDjT06cI>
- Increasing Your Online Banking Safety <http://www.lawyersmutualnc.com/risk-management-resources/articles/increasing-your-online-banking-safety>
- Auto-Reply Can Mean Auto-Trouble <http://www.lawyersmutualnc.com/blog/auto-reply-can-mean-auto-trouble>
- “Reply to All” Is An Ethical Booby-Trap <http://www.lawyersmutualnc.com/blog/reply-to-all-is-an-ethical-booby-trap>

**Books Available from the Lawyers Mutual Lending Library (for Lawyers Mutual insureds only):**

- The ABA Cybersecurity Handbook
- Cloud Computing for Lawyers
- Encryption Made Simple for Lawyers
- Locked Down: Information Security for Lawyers
- The Lawyers Guide to Microsoft Outlook 2013

All book requests can be made online at: <http://www.lawyersmutualnc.com/risk-management-resources/book-lending-library>.



## **Email Encryption: How Secure is Your Email?**

Have you ever worried about the security of your email? If you have, you are probably not unlike many people who transmit sensitive data electronically.

Some of the most widely used types of email services use Transport Layer Security (“TLS”) to encrypt your message (Gmail, Yahoo!, Outlook.com, Exchange 2010, and Exchange 2007). This “automatic” encryption dates back to around early 2014.

But what does this mean for you?

By definition, “TLS is a protocol that ensures privacy between communicating applications and their users” and the successor to the Secure Sockets Layer (“SSL”). It means that your message is being sent using the latest version of end to end internet security as long as the TLS feature is activated for both the sender and the recipient.

If you are using TLS, your email server will always first try to make a secure connection to the recipient server before sending the message. If a secure connection is not possible, then your server will send the message without using this feature.

It is possible to set your server to only send messages if it is able to make a secure connection using TLS. It is also possible to specify the domains you want TLS communications enforced to.

TLS communications are already enabled if you use the “Big 3” email services (Gmail, Yahoo!, and Microsoft). If you or your company use Exchange 2010, TLS is enabled by default at installation. For Exchange 2007, you would need to turn on this feature manually, typically done at installation.

Firms that use Exchange can verify with your Network Administrator to see if TLS has been enabled. You can also verify end-to-end TLS communication with a recipient by looking at the properties or header information of an individual email.

Verifying this end-to-end TLS connection can help you feel good about having a basic level of secure communication for your sensitive emails.

For more information regarding additional encryption related topics (laptops, flash drives, smartphones, etc.) check out *Encryption Made Simple for Lawyers* written by Ries, Nelson, and Simek from [the Lawyers Mutual lending library](#).

*Linh Schladweiler has been with Lawyers Mutual since 1997 and currently fills the role of IT System Manager. You can contact Linh at [linh@lawyersmutualnc.com](mailto:linh@lawyersmutualnc.com) or 800-663-8843.*

## Email Encryption Resources

### General Encryption:

#### Articles:

- “How to Encrypt Attorney-Client Communications”, The Lawyerist, <https://lawyerist.com/78253/email-encryption-client-portals-can-help-secure-client-data/>
- “Easy Encryption for Email – Not an Oxymoron”, SLAW, <http://www.slw.ca/2013/08/12/easy-encryption-for-email-not-an-oxymoron/>
- “Why Lawyers Shouldn’t Email Their Clients”, Clio, <https://www.goclio.com/blog/why-lawyers-shouldnt-email-their-clients/>
- AvoidAClaim Blog, <http://avoidaclaim.com/?s=email+encryption>

#### Books:

- *Encryption Made Simple for Lawyers*, Lawyers Mutual Lending Library, <http://www.lawyersmutualnc.com/risk-management-resources/book-lending-library>


### Program Recommendations and Reviews:

- Virtru
  - “How to Use Virtru for Easy Email Encryption”, Lawyerist, <https://lawyerist.com/79706/use-virtru-easy-email-encryption/>
  - “Virtru Makes Email Encryption Easy, In Either Outlook or Webmail”, Lawsites Blog, <http://www.lawsitesblog.com/2015/01/virtru.html>
  - “Gmail Encryption with Virtru”, The Droid Lawyer, <http://thedroidlawyer.com/2014/09/gmail-encryption-virtru/>
- Dialawg
  - “Quick and Easy Email Security for Lawyers”, Divorce Discourse, <https://divorcediscourse.com/quick-easy-email-security/>
- AppRiver
  - “AppRiver Launches Next Generation Secure Email Delivery Services” Reuters, <http://www.reuters.com/article/2012/04/19/idUS162069+19-Apr-2012+BW20120419>
- Barracuda Networks
- Delivery Trust
  - “‘Delivery Trust’ Lets You Encrypt and Control Your Email”, Lawsites Blog, <http://www.lawsitesblog.com/2014/11/delivery-trust-lets-encrypt-control-email.html>

- Enlocked
  - “Email Encryption, Made Idiotically Easy”, Lawsites Blog, <http://www.lawsitesblog.com/2012/04/email-encryption-made-idiotically-easy.html>
  - “Update on Enlocked, the Easy Email Encryption Tool”, Lawsites Blog, <http://www.lawsitesblog.com/2012/12/update-on-enlocked-the-easy-email-encryption-tool.html>
  - “Encrypting Email with Enlocked”, Law Technology Today, <http://www.lawtechnologytoday.org/2013/02/encrypting-email-with-enlocked/>
- Gmail †
  - “Of Google’s Pending End-to-End Encryption Extension and Vintage Email Legal Ethics Opinion”, SLAW, <http://www.slaw.ca/2014/12/22/of-googles-pending-end-to-end-encryption-extension-and-vintage-email-legal-ethics-opinion/>
  - “Google Offers New Encryption Tool”, The New York Times, [http://bits.blogs.nytimes.com/2014/06/03/google-offers-new-encryption-tool/?\\_r=0](http://bits.blogs.nytimes.com/2014/06/03/google-offers-new-encryption-tool/?_r=0)
- Microsoft (Outlook, Office 365 and other Hosted Exchange products) †
  - “Encrypting Email with Office 365 Exchange Server”, Law Technology Today, <http://www.lawtechnologytoday.org/2014/10/encrypting-email-office-365-exchange-server/>

† Gmail and Microsoft (Outlook, Office 365 and other Hosted Exchange products) have encryption tool available, as a user you just have to turn on that option – for an extra cost.

Data theft is hard to stop.  
Identity Fraud, Inc. provides the optimal  
solutions that every organization needs.



# Cyber Risk Management

Breach Response & Coverages


Lawyers Mutual




## AGENDA

---

- **North Carolina Law and Notification**
  - ✓ ***Breach Response Plan***
  - ✓ ***Notifying Authorities / Insurers***
  - ✓ ***Breach Costs***
  - ✓ ***Key Insurance Coverage / Exclusions***
- **Ethical Obligations**







## PREPARING A BREACH PLAN - OVERVIEW

---

### Information Assets - Written Incident Response Plan

- **Legal Landscape / History**
  - **Obligation/Duty of Care**
    - **GLB, SEC, HIPAA, FCRA**
    - **Ethics / Rules of Professional Conduct**
    - **Contractual**
    - **Wyndham v FTC**
  - **Reasonable? NIST Guidelines, ISO, Size & Sophistication**
    - ✓ *Identify, Protect, Detect, Respond, Recover*
  - **Preparation helps ensure success**

## PREPARING A BREACH PLAN

---

### What type of information do you collect?


- PII – Personally Identifiable Information
- PHI – Protected Health Information
- PCI – Payment Card Industry Information
- Corporate Confidential Information

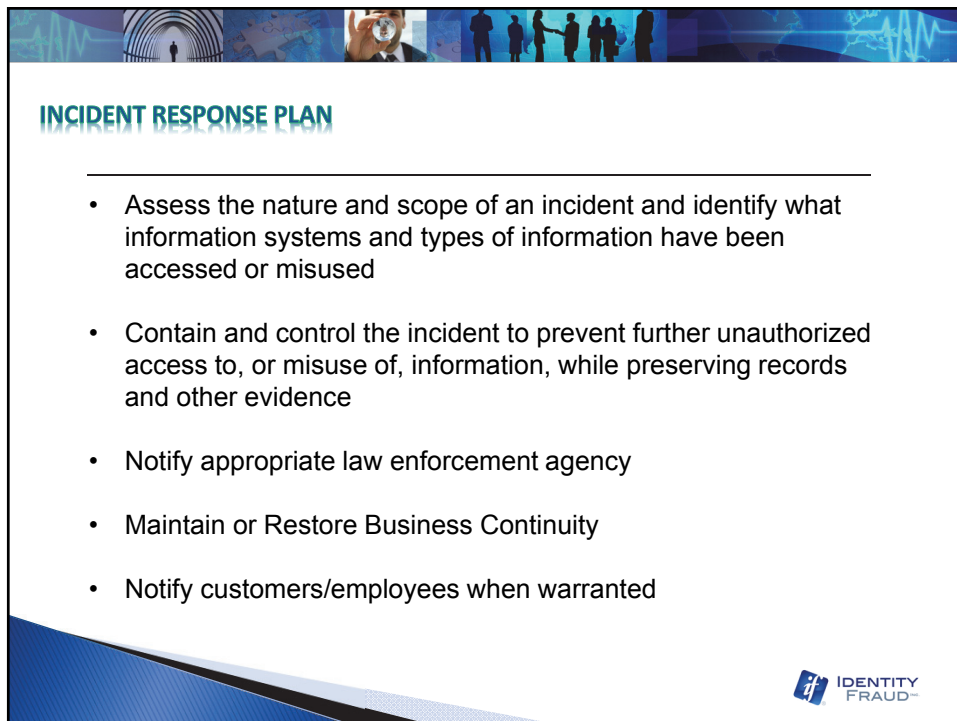
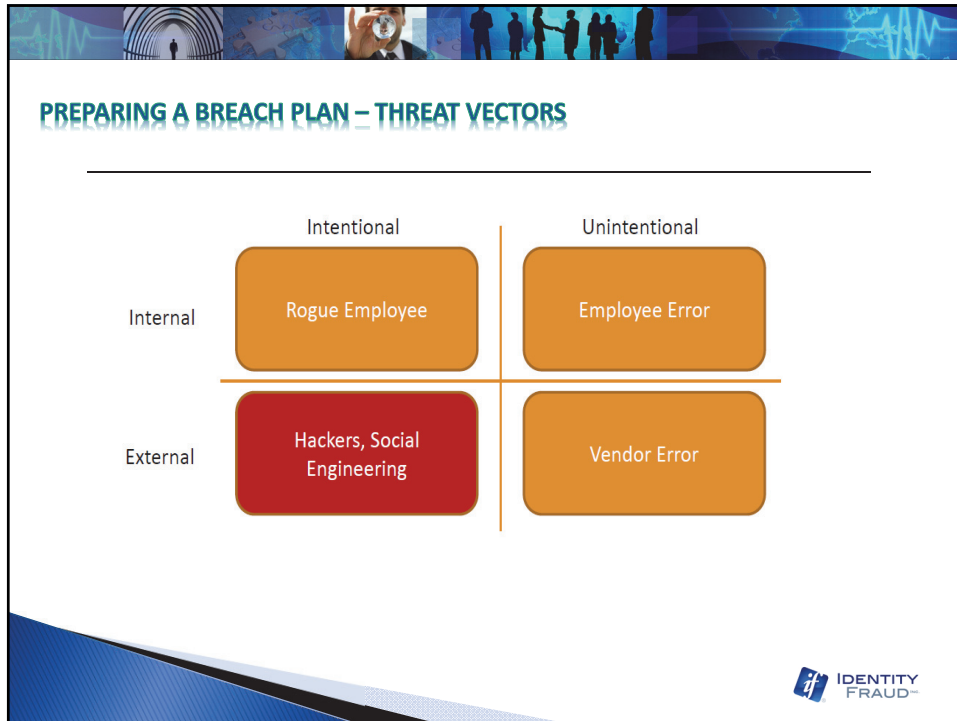
### Where is the information stored?

- Who has access?
- How long is it kept?
- How is it protected?
- Is data backed-up?

### What Security and Controls are in place?

- How are criminals going to get the information?
- What about Encryption?
- Have there been prior breaches?





## INCIDENT RESPONSE PLAN

- Written
- Signed / Documented
- Functional / Useful
- Tested
- Updated

Don't Break Data Loss

### Incident Response Plan


Policies & Procedures  
For Incident Response


Organization: \_\_\_\_\_

Serial Number: \_\_\_\_\_

Date: \_\_\_\_\_


**CONFIDENTIAL**  
Not for Distribution  
Without Written  
Permission


 IDENTITY FRAUD™  
Prevent | Prepare | Respond

 IDENTITY FRAUD™

## INCIDENT ASSESSMENT

- Is the incident perceived or real?
- Is the incident arising internally? Or, externally at a vendor?
- Is the incident “live” and still in progress?
- What is the threat targeting?
- What type of incident is it?
- Is the incident singular or part of a multi-faceted attack?
- What evidence exists?
- Will evidence be preserved?
- What steps have already been taken to remedy the incident?
- What is the estimated severity?
  - Level 1 – Life Threatening?
  - Level 2 – Threat to Customer/Employee (Sensitive) Data?
  - Level 3 – Threat to Operating or Computer Systems?
  - Level 4 – Will Services be Disrupted?



 IDENTITY FRAUD™



## INCIDENT ASSESSMENT

---

- Can the incident be contained?
- Will containment efforts alert the attacker?
- How might the incident evolve?
- Can the incident reoccur?
- What are worst-case & reasonable scenarios?
- Is the incident an emergency?
- Is outside assistance to assess or remedy the incident justified?
- How will normal operations resume?
- What additional assessment criteria are needed?





## INCIDENT RESPONSE


---

### Communications / Notifications

- **#1 Law Firm – Privilege**
- **Team # 2 / Forensic #3 / Family #4**
- **(Do you own the data? If not, notify the owner)**
- **If Crime, then Law Enforcement**
- **If Insured, then Insurer/Broker**
- **Board / Employees**
- **Notifications as needed to Clients/Consumers**









## INCIDENT RESPONSE - COSTS

---

- Legal
- Forensics
- PR
- Consumer Notifications
- Remedies
- Other - Time, Disruption





## INCIDENT RESPONSE - COSTS

---

### Breach Response Remedies / Notifications

- The Law Requires Notification – Letter, email...
- Customer Service Hotline
- Identity Theft Victim Assistance
- Identity Insurance
- Credit Monitoring
- Identity Monitoring
- Cost v Benefit
- Insured or Self Insured






## CYBER INSURANCE

---


- **Cyber / Privacy / Data Breach**
- **New Age / New Exposures / Fill the Gaps**
- **First Party / Property Coverages**
  - **Network Interruption / Extra Expense / Loss of Income**
  - **Data Destruction / Reconstruction**
  - **Extortion**
  - **Incident Response**
    - **Forensics, Legal, PR, Notifications, Hotlines, Victim Resolution, Identity Insurance, Credit Monitoring**
  - **(Future – Bodily Injury / Property Damage)**





## CYBER INSURANCE

---

- **Third Party Liability**
  - **Got Data? Private information in your Care, Custody or Control or in the control of your Information Holder**
  - **Legal Liability / Lawsuits / Damages / Duty to Defend**
  - **Regulatory Fines and Penalties (FTC, CFPB, OCR...)**
  - **Payment Card Industry (PCI) Fines and Penalties**
- **Other –**
  - **Media Liability**
  - **Cloud, Mobile, (Un) Encrypted Data, PCI Compliance**







## CYBER INSURANCE

---

- **Other Key Terms / Exclusions**
  - **Yes or No - Crime / Theft of Funds**
  - **Computer Security Updates / Mistake Exclusion**
    - **Columbia Casualty Co v. Cottage Health (5/7/15)**
- **Primary v Excess / Erosion of Limits**
- **CFPB / Downstream Liability / Mandates**
- **Best Practices / Duty of Care**
- **Risk Management Tools**
- **Plain English Coverage – All Data, All Risks**





## DATA RISKS ARE REAL

---

### Sources / Contact

- **Free Vulnerability Scans / iScan:**
  - <http://events.iscanonline.com/legal-industry>
- **The Ponemon Institute:** [www.ponemon.org](http://www.ponemon.org)
- **Open Security Foundation:** [www.DataLossDB.org](http://www.DataLossDB.org)
- **United States Computer Emergency Readiness Team (US-CERT):**  
[www.us-cert.gov](http://www.us-cert.gov)
- <https://biz.identityfraud.com/lawyersmutualinc2>
- **Tom Widman (twidman@identityfraud.com)**



# Incident Response Plan

## Policies & Procedures For Incident Response

Organization: \_\_\_\_\_

Serial Number: \_\_\_\_\_

Date: \_\_\_\_\_

**Confidential**  
Not for Disclosure  
Without Written  
Permission



# Table of Contents

Approval Signature ..... 3

Introduction..... 3

Incident Response Team..... 4

Incident Response Contact Sheet..... 5

Suspecting or Detecting an Incident ..... 6

Incident Response Discovery Form ..... 7

Incident Assessment and Analysis..... 8

Data Breach Incident Response Flow Chart ..... 9

Notification ..... 10

Customer/Employee Notice Content ..... 10

Customer/Employee Notification Letter..... 11

Additional Policies and Procedures ..... 13

    Documentation..... 13

    Damage / Cost Assessment..... 13

    Insurance..... 13

    Review and Adjust..... 13

    Board of Directors Management and Reporting..... 13

End of Document ..... 13

## Approval Signature

I have approved this Incident Response Plan as reasonably designed to enable our Company to meet its compliance requirements as well as our continuing service commitments to our members in an incident.

Signed: \_\_\_\_\_

Title: (Chairman, President, etc....)

Date: \_\_\_\_\_

## Introduction

Our incident response plan has been developed to reduce the exposures to our organization, our customers/employees, and our partners that arise out of a data theft or data loss incident. We have an affirmative duty to protect our customer information and to properly respond to an incident that is both part of our Security Plan and that is required by law. (**Your State Law**)

In order to comply with (**Your State Law**) and following our Security Plan, our incident response plan specifically includes policies and procedures to:

- Assess the nature and scope of an incident, and identify what customer information systems and types of customer/employee information have been accessed or misused
- Contain and control the incident to prevent further unauthorized access to, or misuse of, customer information, while preserving records and other evidence
- Notify appropriate law enforcement agency
- Maintain or Restore Business Continuity
- Notify customers/employees when warranted

This plan further outlines procedures that we will implement and/or consider in the event an incident occurs. All staff is required to be familiar with this plan and supervisors have been instructed to share this plan with their staff.

It is important to note that our obligations under this plan extend to the information shared with and/or managed by our vendors. Therefore, it is our policy to monitor and review what third party vendors have our information and how we and/or they will respond to an incident occurring in their operations.

**Confidential**  
**Not for Disclosure Without**  
**Written Permission**

## Incident Response Team

Considering the size of our **Company**, we have set forth the following procedures in our Security Plan and at the direction of management responsible for overseeing its development, we have created an incident response team or have appointed a **Company** individual that is assigned with the duties to implement, review, test, and modify the incident response plan, as appropriate.

While developing our team, we have considered the size of our organization, available staff, staff expertise, budget resources and exposures to incidents. Where we have determined that we lack any specific expertise or other internal resources that are needed to carry out team assignments, we have considered the value of and made preparations for using third party experts. It is our policy and goal to be prepared for and competently respond to an incident.

The team's roles and responsibilities are communicated to all **Company** staff. Similar communication is provided if, and when, there are changes to the team, or its roles and responsibilities.

In order to measure the effectiveness of the team, it is our policy to evaluate the team's performance and preparedness, at least annually. While our evaluation may be conducted by management, staff, outside experts, and/or by the team's self assessment, the evaluation will consider the following:

- Benchmarking or comparing to other Incident Response Teams
- General discussions with management, team members and staff
- Surveys dispersed to management, team members and staff
- An audit by a third party knowledgeable in incident response plans, policies and procedures and actual incidents

Additional information that may be made available during the evaluation process may include:

- Number of reported incidents
- Response time
- Number of incidents successfully resolved
- Information or updates that have been supplied to the organization
- Whether or not security issues remain within the organization and what they are
- Preventive measures or practices in place, are being implemented, or pending further review

In an effort to maintain awareness of the incident response plan and its team, it is our policy to distribute the following team member contact sheet to all staff and to post the contact sheet in a convenient and conspicuous location.

## Incident Response Contact Sheet

Date:

Incident Response Manager: (name) \_\_\_\_\_

(telephone) \_\_\_\_\_

(mobile) \_\_\_\_\_

(email) \_\_\_\_\_

Responsibility: \_\_\_\_\_

\_\_\_\_\_

Incident Response Manager: (name) \_\_\_\_\_

(telephone) \_\_\_\_\_

(mobile) \_\_\_\_\_

(email) \_\_\_\_\_

Responsibility: \_\_\_\_\_

\_\_\_\_\_

Incident Response Manager: (name) \_\_\_\_\_

(telephone) \_\_\_\_\_

(mobile) \_\_\_\_\_

(email) \_\_\_\_\_

Responsibility: \_\_\_\_\_

\_\_\_\_\_

Incident Response Manager: (name) \_\_\_\_\_

(telephone) \_\_\_\_\_

(mobile) \_\_\_\_\_

(email) \_\_\_\_\_

Responsibility: \_\_\_\_\_

\_\_\_\_\_

**Confidential**  
**Not for Disclosure Without**  
**Written Permission**



## Suspecting or Detecting an Incident

In the event an incident is suspected, is actually occurring, or has actually occurred, it is our policy to have the staff member that becomes aware of the circumstance to report the event as an incident to their immediate supervisor. In the event a staff member is unable to communicate with their supervisor, contact is to be escalated to any one of the Incident Response Team Members, as identified in the Incident Response Contact Sheet.

The following definitions are adopted to interpret what constitutes an incident:

### Incident

Any perceived, actual, or successful attempt to gain unauthorized access to or use of customer/employee information that could result in substantial harm or serious inconvenience to a customer.

(Incidents may arise out of or include breach of data confidentiality, stolen computer, laptop, PDA, or storage device, data modification / destruction, unauthorized use of data, computers or changes to computers and any attempts of the above, a computer virus, computer spyware, burglary, pre-text calls, and more. Incidents may also be detected based on anomalies in information, unusual behavior by customers or staff, and notification by a customer, vendor, or law enforcement, etc.)

### Customer/Employee Information:

Any record containing nonpublic personal information about a customer/employee, whether in paper, electronic, or other form, maintained by or on behalf of the **Company**.

Employee/customer information that is considered sensitive in nature is as follows:

Name, address, or telephone number, social security number, financial institution account numbers, a personal identification number or password that would permit access to the customer's or employee's account. Sensitive customer's and employee's information also includes any combination of components of customer's and employee's information that would allow someone to log onto or access the customer's and employee's account, such as a user name and password or password and account number.

Following the detection of an actual or perceived incident, staff is instructed to complete the following Incident Response Discovery Form and forward it to their supervisor or an incident response team member, as appropriate.

## Incident Response Discovery Form

Date: \_\_\_\_\_

Time: \_\_\_\_\_

Your Name: \_\_\_\_\_

Dept: \_\_\_\_\_

Phone: \_\_\_\_\_

Location Where Occurred: \_\_\_\_\_

Date Discovered: \_\_\_\_\_

Time Discovered: \_\_\_\_\_

Who Discovered: \_\_\_\_\_

Please Provide A Description Of The Incident Below:

---

---

---

---

---

---

---

Name of Supervisor Contacted: \_\_\_\_\_

Contact Number of Supervisor: \_\_\_\_\_

Incident Response Manger Contacted: \_\_\_\_\_

Contact Number of Incident Manager: \_\_\_\_\_

**Confidential**  
**Not for Disclosure Without**  
**Written Permission**

## Incident Assessment and Analysis

The internal and external environment of our **Company** is subject to constant change. Therefore, it is our policy to assess each incident based on its own unique merits and characteristics.

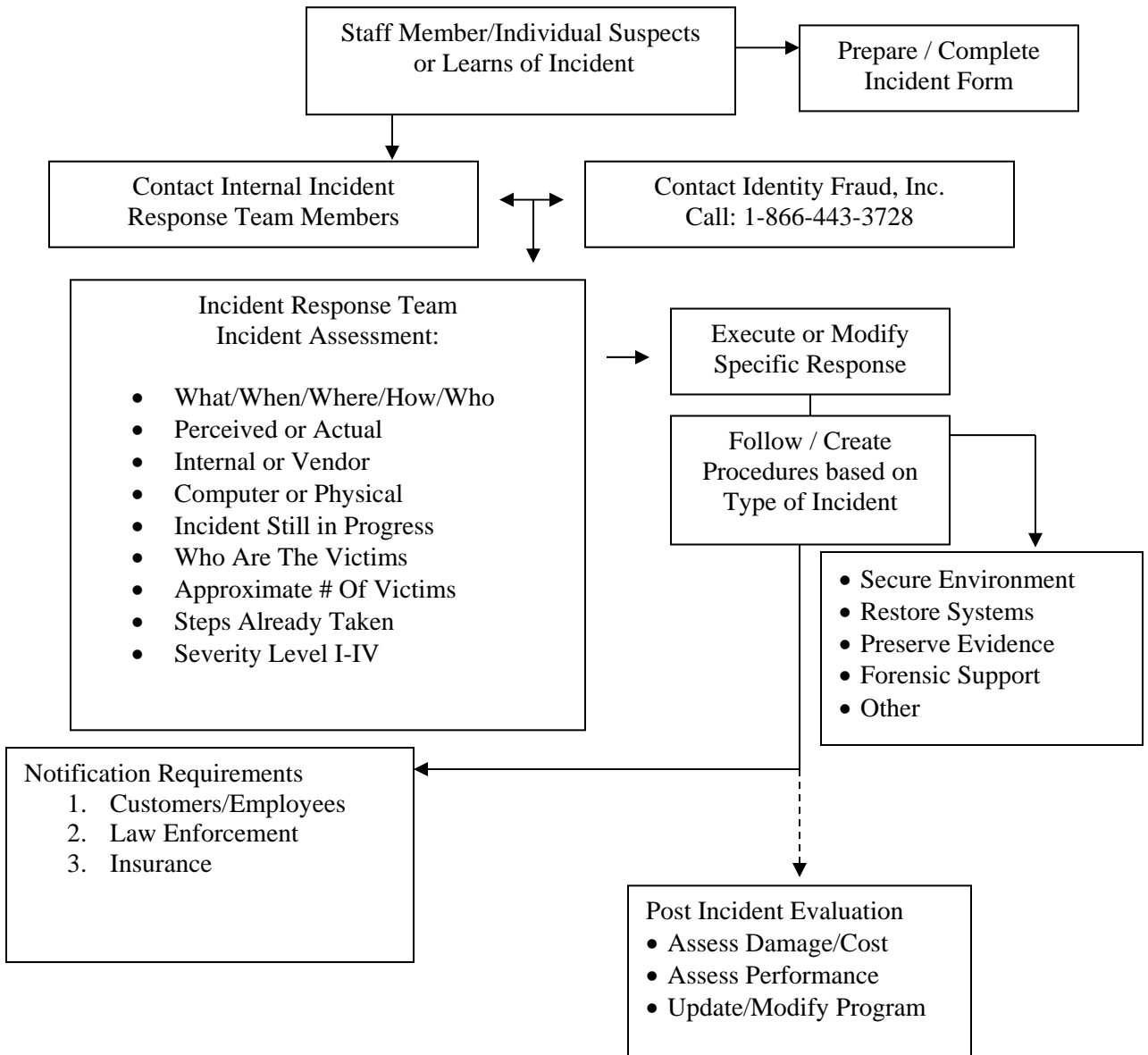
Upon assessing the incident, we shall consider the following:

1. Is the incident perceived or real?
2. Is the incident arising internally? Or, externally at a vendor?
3. Is the incident “live” and still in progress?
4. What is the threat targeting?
5. What type of incident is it?
6. Is the incident singular or part of a multi-faceted attack?
7. What evidence exists?
8. Will evidence be preserved?
9. What steps have already been taken to remedy the incident?
10. What is the estimated severity?
  - a. Level 1 – Life Threatening?
  - b. Level 2 – Threat to Customer/Employee (Sensitive) Data?
  - c. Level 3 – Threat to Operating or Computer Systems?
  - d. Level 4 – Will Services be Disrupted?
11. Can the incident be contained?
12. Will containment efforts alert the attacker?
13. How might the incident evolve?
14. Can the incident reoccur?
15. What are worst-case & reasonable scenarios?
16. Is the incident an emergency?
17. Is outside assistance to assess or remedy the incident justified?
18. How will normal operations resume?
19. What additional assessment criteria are needed?

Following the incident assessment, team members will create an incident response strategy and will carry out duties to execute the incident response strategy according to established and/or new policies and procedures. For illustration and reference purposes only, the following flow chart is provided.

## Data Breach Incident Response Flow Chart

Sample Only



## Notification

As a business subject to regulations and laws, and as a business that emphasizes the value of customer/employee trust and loyalty, it is our policy to notify the following parties in the event of an incident.

1. Our President, CEO, Board of Directors and our Security Division
2. Appropriate law enforcement authorities
3. Customers and employees, when warranted

We are given a reasonable time to investigate. A determination will need to be made regarding the likelihood that information has been or will be misused or is reasonably possible to be misused. While notice to customers/employees may also be delayed if law enforcement is involved in an investigation and if such notice will interfere with the investigation, it is our policy to provide notice to customers/employees as soon as notification will no longer interfere with such investigation.

During our investigation of an incident, we will need to determine which customer/employee information has been improperly accessed, if any. In the event we are able to determine that a group of files has been improperly accessed, but are unable to identify which specific customer/employee information has been accessed, notification will be made to all customers/employees in the group if we determine that misuse of the information is reasonably possible.

## Customer/Employee Notice Content

The content of the customer/employee notification will be given in a clear and conspicuous manner that provides a description of the incident, including the type of customer/employee information that is the subject of unauthorized access or use. Other content that we will consider includes:

- What the **Company** has done to protect the information from further unauthorized access or use
- A telephone number the customers/employees may call for further information and assistance
- A reminder that customers/employees should remain vigilant over the next twelve to twenty-four months and to promptly report incidents of suspected identity theft to their financial institution(s) and law enforcement
- Recommendations that the customer/employee review account statements and report suspicious activity
- A description of credit bureau fraud alerts and how they may be obtained
- Recommendations that the customer/employee periodically obtain credit reports and have information relating to fraudulent transactions deleted from their records
- An explanation of how to obtain credit reports free of charge

**Confidential**  
**Not for Disclosure Without**  
**Written Permission**

- Information about the Federal Trade Commission’s website, phone number, and online identity theft resources and guidance on preventing identity theft
- Other customer/employee remedies provided by the (Company) at no cost to the member

Customer/employee notice will be delivered in a manner designed to ensure that a customer/employee can reasonably be expected to receive it, either by phone, letter, email, or similar communication.

## Customer/Employee Notification Letter

### Sample Only

The following notification letter illustrates content that we may include in a response.

-----

Date

First Name Last Name

Address

City, State, Zip Code

RE: Incident Subject / Your Personal Information

Dear First Name Last Name:

We are writing to let you know that as a result of the recent **data breach** and attempt to misappropriate your personal information, **(Company’s Name)** is taking steps to help protect your identity.

The personal data that was potentially exposed includes **your name, address, telephone number, account number, social security number .....**

Although we have no indication that your personal information has been abused, we take the protection of your account information and your identity very seriously. Therefore, we are implementing the following precautionary measures to protect you.

- We have placed a warning flag on your customer/employee file.
- We will take additional steps to confirm your identity as the customer/employee of the file whenever you contact us.
- We have established a dedicated phone number at **(Company’s Name), (123) 456-7890 or toll-free (800) 456-7890**, to answer your questions and provide additional information. This number will be available **Monday through Friday from 8:00 am to 6:00 pm and Saturday from 9:00 am to 5:00 pm.**
- **(Company’s Name)** will pay the cost of enrollment for a one-year membership in the **Identity Fraud, Inc. Identity Protection Plan**, customized especially for our members. This service, at no cost to you, starts today and provides:

**Confidential**  
Not for Disclosure Without  
Written Permission

- Access to VRS Elite™ fraud resolution counselors (24/7) to answer questions you have and to help resolve any circumstances relating to identity theft, whether simple or complex. Simply call IFI toll-free at **1-866-4-IDFRAUD** (1-866-443-3728).
- \$25,000 of identity insurance (\$0 deductible) to cover certain expenses you may incur as a result of identity theft.
- Credit Report Monitoring, which will monitor your Experian credit file and send an email to you of any unusual activity on your credit file. *(Your enrollment is required)*
- One free copy of your credit report
- Access to the IFI Members Section for additional benefits, including educational materials, newsletters, discounts on additional products, and more

To enroll in the Credit Monitoring program, please call Identity Fraud, Inc. at 1-866-443-3728 between the hours of 8:00 am to 5:00 pm, Monday through Friday, Pacific Standard Time.

**As an additional precaution, you may want to consider taking the following step:**

- You may want to place a FREE 90-day initial **Security Alert** on your credit bureau file. The Security Alert, which can be requested only by you, provides another significant layer of protection by flagging your credit file for additional scrutiny by potential lenders. If you choose to activate a Security Alert, you need to successfully activate the alert with only ONE of the three main credit reporting agencies listed below. The agency you report to will automatically notify the other two agencies, as required by law. Their contact information is:

<b>Equifax</b> 1-888-766-0008	<b>Experian</b> 1-888-397-3742	<b>TransUnion</b> 1-800-680-7289
----------------------------------	-----------------------------------	-------------------------------------

**(Company's Name)** is committed to protecting the confidentiality of our customer/employee personal information. While we regret any concern or inconvenience the recent incident may cause you, both **Identity Fraud, Inc. and (Company's Name)** believe the above items will help protect you from potential identity theft, no matter what type or how it may occur.

Please do not hesitate to contact us if we can assist you in any way.

Sincerely,

First Name Last Name

President and CEO

**Confidential**  
**Not for Disclosure Without**  
**Written Permission**

## **Additional Policies and Procedures**

### ***Documentation***

Documentation of an actual or perceived incident will include but not be limited to information relating to the person(s) that discovered the incident, suspect(s), incident assessment, strategic response, hard copy evidence, electronic evidence (computer logs, emails, telephone recordings, etc.) meeting notes, damage, and costs.

### ***Damage / Cost Assessment***

Prior to an incident occurring and during and after an incident occurs, attempts will be made to quantify the potential damage to the **Company** and the associated costs to contain and remedy the incident.

### ***Insurance***

Insurance coverage may or may not apply to incidents. Therefore, we will conduct a review to better determine when insurance may or may not apply to various incidents and whether or not insurance applies to any specific incident that is occurring. We will consult our professional insurance advisor/broker and/or company, as necessary.

### ***Review and Adjust***

Following an incident, **Company** and incident response team will review its performance and take appropriate steps to improve its prevention and response efforts and to improve its policies and procedures to better avoid the recurrence of incidents.

### ***Board of Directors Management and Reporting***

It is our policy to provide a report, at least annually, to management and/or the Board of Directors regarding the status and condition of our incident response plan and team. Furthermore, following an actual incident or testing of an incident, a report will be prepared and distributed to the appropriate parties.

## **End of Document**

**Confidential**  
**Not for Disclosure Without**  
**Written Permission**



## **Protecting Yourself From Cybercrime Dangers: The Steps You Need To Take**

Lawyers' Professional Indemnity Company (LAWPRO) is a wholly Canadian owned insurance company that provides professional liability insurance to lawyers in Ontario. LAWPRO is headquartered in Toronto, Ontario, Canada. LAWPRO provides errors and omissions insurance to more than 24,000 members of the Law Society of Upper Canada

*This article first appeared in the December 2013 issue of LawPro magazine. Reprinted with permission.*

*Cybercrime dangers are many, complex and ever-changing. Hardly a day goes by without another news report of a data breach or other cyber-related scam or theft. Cyber criminals have considerable resources and expertise, and can cause significant damage to their targets. Cyber criminals specifically target law firms as law firms regularly have funds in their trust accounts and client data that is often very valuable. LAWPRO encourages all law firms to make dedicated and ongoing efforts to identify and understand their potential cybercrime vulnerabilities, and to take steps to reduce their exposure to cyber-related dangers. This article reviews the specific cybercrime dangers law firms need to be concerned about, and how they can mitigate their risks.*

### **It starts with support from senior management**

Any effort to tackle cybercrime must start at the top. Senior partners and firm management must be advocates of cyber security, support the implementation of appropriate practices and policies, and allocate sufficient resources to address cybercrime exposures. While there are some quick fixes that can help make your office and systems more **secure (to find them see "quick fixes" opposite)**, most firms will need to spend some time and money to better protect themselves from cybercrime. This may include upgrading or installing new technology, training staff, and changing how some tasks are done.

Firms should also put some thought into how a cyber breach – the loss of client data or hacking of a firm server – would be handled. Firms should have a formal incident response plan so they can avoid making bad decisions on an ad hoc basis in the middle of a crisis. See the [“Be Ready with an Incident Response Plan”](#) article on the Lawyers Mutual website.

### **You likely need expert help**

Beyond the very practical issue of wanting to avoid being the victim of cybercrime, remember that when using technology, lawyers and paralegals must meet their professional obligations as outlined by the lawyers' *Rules of Professional Conduct* and the *Paralegal Rules of Conduct*. These rules provide that you should have a reasonable understanding of the technology used in your practice, or access to someone who has such an understanding [Rule 2.01 of the lawyers' Rules, Rule 3.01 of the Paralegal Rules].

It is unlikely that sole practitioners and smaller firms will have someone on staff who has the technical expertise to properly address all relevant cyber security issues. With their larger and more complex technology infrastructures, even medium and larger firms may also need to seek outside help. One of the biggest dangers here is that people just don't realize what they don't know when it comes to cybercrime dangers and how to prevent them. LAWPRO encourages firms to seek appropriate help from

knowledgeable experts when required. To identify vulnerabilities, firms may want to consider engaging an outside expert to do a formal security assessment.

## **Staff education and technology use policies**

As you will learn in this article, despite being technology-based, many cybercrime dangers involve a human element. Cyber criminals create situations in which law firm staff and lawyers will unintentionally and unknowingly facilitate cybercrimes as they go about their common daily tasks. Educating staff to help them understand, recognize and avoid cybercrime dangers is a critical part of reducing cybercrime risk.

Written policies that clearly establish guidelines and requirements governing the acceptable use of all firm technology resources can also help reduce cyber exposures. Through technology use policies, law firm staff should be given clear direction on what they are permitted and not permitted to do with law firm technology resources. These policies should use simple and non-technical language that all employees can understand. They should be reviewed with new employees at the commencement of employment, and on an annual basis with *all* staff. It is also essential that these policies be consistently and strictly enforced.

Every technology use policy should cover some basics. They should clearly state that technology resources provided by the firm, including Internet and email access, are to be used for legitimate firm activities. Staff should understand that they have an obligation to use resources properly and appropriately. Technology use policies should also direct firm staff to ensure that the confidentiality of firm and client information is protected at all times, that there is compliance with network system security mechanisms, and that resources are not used in a manner that would negatively affect others on the system. Technology use policies should also indicate that the firm retains the right to monitor any and all electronic communications and use of the Internet to ensure the integrity of the firm's systems and compliance with the firm's technology use policy. As well, the policy should indicate that there may be sanctions for failure to comply.

You can find some sample technology use policies you can use and adapt for your firm on [practicePRO.ca](http://practicePRO.ca).

## **The cybercrime dangers you need to address**

The cybercrime dangers firms need to address are many and varied. This article reviews these dangers in more detail and will help you start on the work that is necessary to address them so you can reduce the likelihood that cyber criminals will breach your law firm's systems.

These topics covered in the sections to follow are:

- I.** Avoid the dangers of email
- II.** Lock down your browser and avoid surfing dangers
- III.** Avoid infections with antivirus and/or anti-malware software
- IV.** Lock things up by using passwords properly
- V.** Address security vulnerabilities by installing operating system and program updates

- VI.** Keep the bad guys out with a firewall on your Internet connection
- VII.** Stump hackers by changing key default settings
- VIII.** Lock down and protect your data wherever it is
- IX.** Scrub confidential client information on discarded equipment
- X.** Be safe when using remote access and public computers
- XI.** Secure your mobile devices to protect the data on them
- XII.** Harden your wireless and Bluetooth connections and use public Wi-Fi with extreme caution
- XIII.** Be careful about putting your firm's data in the cloud
- XIV.** Inside people can be the most dangerous
- XV.** Be careful of the dangers of BYOD and family computers
- XVI.** A backup could save your practice after a cybercrime incident

As they can be used as a point of access to your firm's systems, it is critical to address the above issues on your personal smartphones and tablets, as well as your home computers and networks.

## **You must address all the dangers**

Don't be tempted to ignore any of the dangers listed above, or to skip or skimp on the steps suggested to deal with them. Remember, your data and systems are only as safe as the weakest link in your security plan. When you leave on vacation, you lock every door and window in your house. Leaving just one door or window open gives a thief easy and instant access. To protect yourself from cybercrime, it is critical that you fully and properly address all cybercrime dangers. Cyber criminals will look for and exploit holes in your security plan.

Note that some of the configuration changes suggested in this article will require you to have "administrator" access to your device or systems. Operating your computer or device with the administrator account (or an account that has administrator status) will allow you to freely change your configuration or settings. A regular "user" account will not have the ability to change many device or software settings. To prevent regular staff from changing their settings and intentionally or unintentionally causing damage to your systems, everyone in your office should be using a "user" account, not an administrator account or accounts with administrator status. Doing your day-to-day work while logged into a "user" account can also reduce the damage that a malware infection will cause. Without administrator access, the malware will be restricted in its abilities to change settings on your computer.

As a final note, you may find yourself unable to change your configuration if your firm centrally administers and controls the settings for computers and other devices. Speak to your technology support person if you have questions or concerns.

## **I. Avoid the dangers of email**

Email has become a primary communications tool for the legal profession. It allows virtually instant sharing of information and documents between lawyers and their clients. Email is also one of the most

dangerous tools in a modern law office. Infected attachments, spam and phishing attacks delivered by email make it easy for cyber criminals to deliver malware and breach law firm security protections. It is essential that you educate your lawyers and staff about these dangers and the steps they should take to use email safely.

### **Be wary of attachments**

While email attachments are frequently used to share documents between lawyers, law firm staff, and clients, they are also one of the most common delivery mechanisms for malware. While most messages that have infected attachments will be stopped if your anti-malware software and/or spam filter are working properly and updated, some will make it through. **For this reason, everyone at a law firm should follow these two simple rules:**

1. No matter how interesting or enticing they appear to be (e.g., jokes, celebrity gossip or pictures), never open attachments from strangers.
2. No matter how interesting or enticing they appear to be, never open attachments unexpectedly sent to you by people you know.

The reason for Rule #1 should be obvious – enticing attachments from strangers usually have a malware payload. The reason for Rule #2 might be less obvious: to trick you into feeling comfortable about opening an attachment, some types of malware will send an email with an infected attachment to all the address book contacts it finds on a computer that it has just successfully infected. This is done intentionally with hope that people getting such a message will be comfortable opening the attachment as it came from someone they know – and bingo – the person opening the attachment will become infected and all *their* contacts will get a similar message.

### **Use spam filters to avoid annoying and dangerous spam**

On a daily basis you undoubtedly receive unsolicited commercial junk email, advertising or other offensive messages commonly known as spam. Spam is not only annoying – it is also very dangerous as it is commonly used to deliver malware (if you click on a link in the message) and phishing scams (see the next heading).

To combat spam, many firms use spam filters that are intended to detect unsolicited and unwanted email and prevent those messages from getting into a user's inbox. Spam filters use various criteria to identify spam messages, including watching for particular words or suspicious word patterns, messages that come from websites that are known to send spam, etc. Anti-spam products also use “blacklists” that intercept messages from recognized spammers, and “whitelists” that let messages through only if they come from your personal list of recognized email addresses or domains (the domain is the main part of an email address or website, for example, lawpro.ca or gmail.com).

**If your email program includes a spam or junk mail feature, you should turn it on.** For additional protection, consider installing a third party spam filter. They are often included in anti-malware suites. See Lawyers Mutual’s article “[Malware – It Can Happen To You](#)” for more information.

While spam filters can significantly reduce the amount of spam you receive, they are not perfect. They will sometimes let spam messages through. **Advise firm staff not to open or respond to spam messages, and to flag them as spam so that the spam filter can learn to recognize and prevent a similar message from getting through in the future.**

Links in spam messages will often cause malware to be downloaded to your computer. **For this reason, everyone at a law firm should be told to never click on links in spam messages, no matter how interesting or enticing they appear to be.**

### **Don’t be fooled by phishing**

Did you know that emails appearing to come from companies you trust may actually be from criminals trying to steal your money or identity? Because they are so successful at duping people, “phishing” emails have quickly become one of the most common and devastating scams on the Internet.

Phishing scams use spoofed (meaning faked or hoax) emails and websites to trick you into revealing your personal and financial information. By using the trusted brands and logos of online retailers, banks, or credit card companies, phishing scammers trick surprisingly large numbers of people. The phishing email directs users to visit a website where they are asked to confirm or update personal information such as: passwords; and credit card, social insurance and bank account numbers. In doing so, people are tricked into giving this information directly to cyber criminals, who, in turn, use it for identity theft, financial theft or other cybercrimes.

Legitimate companies will never ask you to update your personal information via an email message. Don’t get tricked by phishing scams.

## **II. Lock down your browser and avoid surfing dangers**

After email, your Internet browser is probably the second most dangerous technology tool in your office. Even casual surfing on the web can expose you to malware and other cyber security issues. You and your staff need to know how to safely surf the web and configure your browsers so that surfing is less dangerous.

### **Safely surf the web**

Teaching your staff the following surfing “don’ts” will help you reduce cyber-related surfing risks, and reduce the likelihood of a malware infection:

- Don't complete online transactions involving account information, passwords, credit card numbers or other personal information, unless you are on a secure connection as indicated by an "https" in the website address.
- Don't visit unknown websites, and especially music, video, or pornography sites because they are often loaded with malware.
- Don't use file sharing sites, or services unless you are familiar with them and know the people you are sharing files with.
- Don't download software, unless it's from a reputable and trusted site.
- Don't download new apps (wait until downloads hit the thousands and it is likely any malware in the app has been detected).
- Don't download browser add-ons, plug-ins or toolbars, especially from unknown or untrusted sites.
- Don't click on "OK," "Yes" or anything else in browser "pop-ups" (the small windows that sometimes open within a browser). These are sometimes made to look like "dialog boxes" (the windows you change settings or options in) to make you think you are clicking on options or settings you normally deal with. Quickly closing all browser windows and tabs can help, especially if you are being flooded with multiple pop-ups. On Windows-based browsers use Ctrl+W or Alt+F4 to repeatedly close the top-most tab or browser window. In Safari, ⌘+Shift+w will close all tabs in the current window and ⌘+q will close all Safari windows and tabs.

Run an antivirus or anti-malware program that runs in the background and scans for dangers (see below for more information on anti-malware software).

If you are doing online banking for your firm trust or general accounts, it is critical that you ensure all security risks are addressed. See the "[Increasing Your Online Banking Safety](#)" post for the extra steps you need to take.

### **Beware the dangers of social media**

Many people are comfortable sharing a great deal of personal information on Facebook, Twitter, Instagram and other similar social media tools. While family and friends may enjoy this information, people should keep in mind that cyber criminals could use the same information to assist them in personal identity theft or the hacking of online accounts. **Be cautious about the amount and type of information you share on social media.** Posting vacation pictures while you are away or using apps that broadcast your location (e.g. Foursquare) tells the world you are away from your home and office.

**Facebook, Twitter, LinkedIn and some other sites can be configured to only let you login on a secure connection.** This can prevent your account from being hacked since your login credentials and connection are encrypted, making it harder for someone to intercept them.

## Lock down your browser

Malware programs can automatically and secretly install themselves while you are browsing. These are called “drive-by downloads.” This occurs when websites run scripts (small bodies of code designed to perform a specific action) or ActiveX controls (a module of code that adds extended functionality to the browser).

All browsers allow you to change individual configuration settings, many of which can deal with these and other security issues. Some browsers let you easily change multiple security or privacy settings by choosing from different levels of security (Medium-high or high are best). While changing browser settings can provide greater protection, it may also prevent some websites from running properly. While the options and terminology will change slightly between the various browsers, these are some of the settings you should change to lock down your browser:

- prevent pop-ups from loading (or prompt you before loading a pop-up).
- disable JavaScript.
- don’t accept third party cookies.
- delete cookies on exit.
- clear history at close.
- disable ActiveX controls (or prompt to run ActiveX controls).
- enable automatic updates.

See the [“Browser Security Settings for Chrome, Firefox and Internet Explorer: Cybersecurity 101”](#) webpage for detailed instruction on how to lock down these three browsers. “iOS: Safari web settings” on the Apple Support site has information on Safari security settings.

There are also various browser plug-ins and add-ons that can increase browser security and warn you about suspicious activity. Widely used WOT (Web of Trust) will warn you about untrustworthy sites (available for all browsers).

## Pharming

“Pharming” is another common trick used to perpetrate scams. Pharming takes you to a malicious and illegitimate website by redirecting a legitimate website address. Even if the website address is entered correctly, it can still be redirected to a fake website. The fake site is intended to convince you that it is real and legitimate by spoofing or looking almost identical to the actual site. When you complete a transaction on the fake site, thinking you are on the legitimate site, you unknowingly give your personal information to someone with malicious intent.

**You can avoid pharming sites by carefully inspecting the website address in the address bar.** Make sure you are on the site you intended to visit and look for “https” (see sidebar on next page) before you enter any personal information, passwords, credit card numbers, etc.

### **III. Avoid infections with antivirus and/or anti-malware software**

Good behavior alone will not protect you from viruses or other malware infections. You must run software that will prevent and/or detect infections on your computers, and you may want to consider it for your tablets and smartphones too.

But what is the difference between antivirus and anti-malware software? As explained in the “Common types of malware” sidebar on page 9, viruses are a specific type of malware. Malware is a broad term used to describe many different types of malicious code, *including* viruses, but also Trojans, worms, spyware, and other threats.

Does this mean antivirus software will only protect you from viruses and anti-malware software will protect you from all kinds of malware, including viruses? The answer is, unfortunately, it depends. While most of the more popular tools will scan for many types of malware, you need to look at the specific functionality of each product to know for sure what it will protect you from. From this point forward this article will refer to the broader category of anti-malware software.

#### **The options**

Windows computers are prone to infections so you must run anti-malware software on them. Microsoft Security Essentials is a free product you can download to help protect computers running Windows XP, Windows Vista, and Windows 7. Windows 8 includes Windows Defender, also free. Both offer good real-time anti-malware protection.

There are a number of widely used commercial anti-malware programs, some that come in suites that include other functionality like anti-spam, firewalls, remote access, device location and scrubbing.

The two most widely used antivirus programs are Norton™ AntiVirus (symantec.com) and VirusScan (mcafee.com). Expect to pay \$40-\$60 per computer to buy the software, plus an additional annual fee for virus signature file updates (see opposite). Buying antivirus software that is bundled with other products, such as firewall and anti-spam software, will save you money.

Until recently, it was generally felt it was not necessary to run antimalware software on Apple computers as the Mac OS architecture prevented infections and there were no real malware threats targeting Macs. There are now potential malware threats, and consider ClamXav, an effective and free antivirus program for Mac OS X computers. Note: If you run a Windows emulator on a Mac computer you open yourself to the full gamut of Windows malware risks and you must use a Windows anti-malware tool.

Tablets and smartphones are, in general, much less likely to get malware infections, but you may want to run anti-malware apps on them for greater protection.



As no one tool will catch everything, you may want to consider using more than one anti-malware tool. To better protect yourself, install one security tool that scans for as much as possible and that runs all the time in the background with an on-access scanning engine. This will protect you from threats as you surf the web, install applications, open files and complete your other daily activities. Then, install another anti-malware tool that you can occasionally use on demand to make sure nothing got through or was overlooked. Scan your entire hard disk(s) at least weekly, either manually or automatically (automatic is better as you don't have to remember to do it).

Bitdefender QuickScan is a free online scan that is handy if you need a second opinion on a Windows computer.

But note, it is important to make sure you do not run two antivirus applications simultaneously. Anti-malware programs do not usually play well together, and running two at the same time can often lead to one identifying the other as a virus, or in some cases, file corruption. Running two at the same time will likely also slow your computer down.

Malware can be extremely difficult to remove from a computer, so it is best to prevent infections. **However, if you do get an infection, Malwarebytes Anti-Malware is a good free tool for removing malware from a Windows computer.**

### **Installing anti-malware software updates is a must**

Installing anti-malware software is only the start. You also need to regularly update your virus definition or signature files. Anti-malware programs use the information in these files to recognize virus infections when they are occurring. As there are new viruses being created every day, you need to have the most recently released virus signature file to be protected against all known infections. These updates are available on your anti-malware vendor's website. Expect to pay about \$30-\$40 per year for these updates. Most anti-malware programs can be configured to download these updates automatically, without user intervention. **Make sure the automatic update feature is enabled as this helps ensure that your protection is always up-to-date.**

### **Staff can help you spot malware infections**

Sometimes anti-malware software will not detect that an infection has occurred. While malware can be on a computer and never give any hint of its presence, in many cases there are clues that a computer is infected with malware. See the "How to recognize your computer is infected with malware" sidebar for a list of these symptoms. Teaching your staff to recognize these symptoms could aid in the earlier detection of an infection.

## **IV. Lock things up by using passwords properly**

Like the keys that start your car or open the front door of your home or office, computer passwords are the keys that "unlock" your computer, your mobile devices and access to all the data on your network systems. We all have more passwords than we can remember. This tends to make us a bit lazy. We use

obvious and easy to remember passwords – even the word “password” itself. Or worse: We don’t use them at all.

Cyber criminals know and exploit bad password habits as they are often one of the weakest links in data security schemes. For this reason, it is critical that all lawyers and staff in a law office use passwords properly. The article regarding the creation of strong passwords, “[Keeping your passwords strong and secure](#),” reviews the steps you can take to properly use and protect the confidentiality of your passwords, and how you can create passwords that are harder to guess or determine.

## **V. Address security vulnerabilities by installing operating system and program updates**

There are millions of lines of computer code in the operating systems and programs that run on your computers, tablets and smartphones. These operating systems and programs will have hundreds or even thousands of settings and features. These settings and features are intended to allow you to do all the things you want to on these different devices.

Amongst all these settings and features, cyber criminals look for “exploits.” An exploit is a particular setting, feature or sequence of commands that will cause an unintended or unanticipated behavior to occur on a computer or other device. Exploits create security vulnerabilities because cyber criminals can use them to open a backdoor to your network, allow malware to run, or do other damaging things. New exploits are discovered on a weekly or even daily basis.

### **Updates**

When an exploit is discovered, software companies quickly rewrite their code and release updates or patches to stop the exploit from working. To protect against newly discovered exploits, devices must be updated with the latest versions of operating systems and programs.

To keep your computers and other devices safe, you should be checking for and installing updates regularly, ideally on a weekly basis. This is particularly the case for Microsoft products, which are prone to security vulnerabilities. While not as prone to vulnerabilities as Microsoft products, Apple products should be updated regularly as well. Don’t forget to update the other non-Microsoft or non-Apple software running on your devices. Sometimes direct links to an updates webpage can be found on the Help menu. Otherwise, you should be able to find the software product’s site with a search on Google.

If you are using Windows XP or Office 2003, note that Microsoft will no longer be supporting these products as of April 8, 2014. Using these products after this date will expose you to greater security dangers.

## **Automatic updates**

**Enabling automatic updates can help keep your computers and other devices up-to-date.** Both Windows and Apple operating systems have an “automatic update” feature that automatically notifies you when updates are available for your devices. Once activated, the device will periodically check for updates. Available updates will be downloaded, and depending how you configure things, installed with or without your knowledge. Some people prefer to set the automatic updates feature to ask for permission to install updates to avoid problems that might arise due to an update installation. Others prefer to have updates installed without intervention from the computer user (this can help make sure updates get installed).

**The Ninite.com site can help Windows computer users check for and install updates (for free).** Note, in some firms individual users will have no control over updates as the installation of updates will be centrally controlled and managed. The paid version of Ninite can be used for this purpose for Windows computers.

## **Back up before you install updates**

It is very important to remember that installing updates can unintentionally interfere with the way your computer/device or individual programs/apps operate. It is possible that a program/app may not operate properly or at all, that data could be lost, or that a device will fail to restart after an update is installed. **Creating a restore point (a temporary backup of your configuration and data) and/or making a proper backup of all the programs and data on a device before you install updates can help you recover if there are unanticipated problems.**

## **VI. Keep the bad guys out with a firewall on your Internet connection**

When you are connected to the Internet, the Internet is connected to you. For computers to transmit data back and forth over the Internet, lines of communication must be established. These communications work through “ports” that are opened on each computer. The problem is that all the computers on the Internet can see one another, and these ports can allow unauthorized people to access the data on a computer and even take control of it.

Regardless of how your office connects to the Internet, your computer systems must be protected by a firewall – a type of electronic gatekeeper that ensures all incoming and outgoing communications are legitimate. A firewall watches these ports and will warn you about or prevent unauthorized communications.

Firewalls come in two varieties: software and hardware. Software firewalls are easier to set up, usually protect a single computer, and are adequate for personal or small firm use. Hardware firewalls are usually used to protect an entire network of computers. **The more recent versions of both the Windows and Mac operating systems have a built-in firewall that you should enable.** High-speed modems generally

include a basic firewall. If you are using remote access software, you should consider using a hardware firewall to better protect the ports that must be opened for the remote access software to work.

## **VII. Stump hackers by changing key default settings**

Changing the default settings for the hardware and software used in your office is another critical step in safeguarding the security of your data and protecting yourself from cybercrime. This is probably the most technical of the steps outlined in this article and you may need expert help.

Every computer operating system, program, and app, and every piece of hardware has certain preset or default settings. These are necessary to make them operate out of the box in a consistent manner that the vendor and user will expect.

However, these default settings are common knowledge (and if you don't know them, you can find them with Google in about five seconds), and hackers can use them to compromise a network, computer or other device. For example, if the administrator account on a computer is named "Administrator" (it frequently is), a cybercriminal only has to work on figuring out the password to hack into a system or device. If you change the name of the Administrator account to something different, your computer is much safer as the hacker has to work much harder to figure out both the name of the administrator account and its password.

You can make your systems much safer by changing the following key default settings:

- administrator account names
- server names
- network or workgroup names
- ports (change to non-standard ports and close standard ports that you don't use)
- standard share names

## **VIII. Lock down and protect your data wherever it is**

Long gone are the days when you had to worry about a single file folder that held all the documents for a particular matter, which you could easily secure by keeping it locked in a file cabinet. Today, client data can exist in electronic form in many different places inside and outside your office. You need to know where that data exists, who can access it, and what steps should be taken to secure and protect it from cyber criminals.

### **Physical access to servers, routers and phone switches**

Protecting your server(s) and other key telecommunications equipment such as phone switches and routers starts with physical security. Intruders who have physical access to a server can get direct access to files and data on the server's hard drives, enabling them to extract the usernames and passwords of every user on the system, destroy data, or give themselves a backdoor for accessing the server remotely. Even curious employees who want to change settings can unintentionally cause serious problems. Put

your servers and other key telecommunications equipment in a locked room to protect them from unauthorized access. Be cautious about any wall jacks for your network in unsecured areas of your office.

### **Access to devices on startup**

To protect the information on them, and the information on any network they connect to, every computer, tablet and smartphone should be configured to require a password at startup. Devices without a startup password allow free and unfettered access to anyone that turns them on.

Better yet, in addition to a startup password, consider encrypting the data on devices. Passwords will prevent the average person from accessing your device, but can be bypassed by people with greater expertise. Encryption will make information on devices far more secure. The operating systems on some devices have built-in encryption capabilities or you can install third party encryption programs or apps.

### **Put a password on your screensaver**

Activating a password-protected screensaver is a simple and very effective way to prevent an unauthorized person from rifling through the data on a computer or other device that's been inadvertently left on. All versions of Windows and Apple operating systems allow you to add a password to a screensaver. Remember to log out of any applications containing sensitive data and lock your screen when you leave your desk, or set a fairly short wait time on your screensaver so that it locks automatically if you step away. BlackBerry, Android, iOS and Windows mobile devices also have an automatic screenlocking feature.

### **Access across a network**

Almost every law office has a computer network with one or more central servers. Client and firm information can be stored on these servers, making it accessible to everyone in the office. To better protect information from unauthorized access, take time to understand what information is stored on your network servers, and who has access to that information.

“Network shares” make folders available and visible across a network. “Permissions” control what people can do with the data in a folder. Someone with “full access” can create, change or delete a file, whereas someone with “read only” access can open and copy a file, but not delete it. Segment your data and set appropriate access levels (e.g., public, sensitive, very private) so that access to sensitive information is limited or prevented. Remember that privacy legislation requires that you limit access to some types of personal information (e.g., financial and health-related data) on a need-to-know basis.

Restricting access to more sensitive data can help protect it in the event your network is hacked or an unhappy employee with bad intentions goes looking for data.

Your desktop or laptop computer can act like a server in some cases, and content on your hard drive could be shared and accessible to someone across a network or through the Internet. To prevent this from happening, you need to make sure that file and printer sharing is turned off on your computer.

## **IX. Scrub confidential client information on discarded equipment**

Many of the technology devices used today are essentially disposable. When they get old or break down, they are simply discarded as it is too expensive to upgrade or repair them. As a result, law offices will frequently find themselves discarding older computers and other devices. This is problematic as these devices often have confidential client information on them.

There are risks in donating your old computers to charity or a local school where a classroom of technology-savvy students will be itching to recover your data. Be sure to remove the hard drive from any computer you donate, or make sure the data on the drive has been thoroughly removed.

Third party access to confidential client or firm information can also be an issue if you are sending your electronic equipment outside the office for repair or maintenance. Client information can be in unexpected places. Most modern photocopiers and printers actually have hard drives on board that store copies of the images that go through them. This data can easily be found on, or recovered from, the hard drives on these devices.

### **Deleted doesn't mean deleted**

It's a common misconception that deleted files are gone for good. In fact, the deleted files on most devices (e.g., computers, tablets, smartphones, etc.) are easy to recover using widely available forensic recovery tools. Even reformatting or repartitioning a hard drive will not completely destroy all the data on it.

Keep in mind that forensic technology can also be used to restore deleted files on portable media (e.g., CDs, DVDs, USB sticks, SD cards), so you should always use new media when sending data outside your firm.

Physically destroying a hard drive or other device with a hammer is the free and low-tech option. You can also use specialized software that will “scrub” all data from a hard drive so that it is not recoverable. Widely used free tools for this task include [CCleaner](#), [Darik's Boot And Nuke \(DBAN\)](#), and [File Shredder](#).

[For more information regarding the removal of data from discarded equipment, read the risk management practice guide, “[Office Equipment Disposal Policy](#).”]

## **X. Being safer when using remote access and public computers**

Being able to access your work network while you are out of the office can provide increased productivity and flexibility. However, opening your systems to remote access creates a number of security risks as

external network connections are a ripe target for cyber criminals. And you should think twice about using public computers for firm work.

### **Setting up safe remote access**

There are many tools that allow you to easily set up remote access (e.g., PCAnywhere, GoToMyPC, LogMeIn, TeamViewer, SplashTop). If properly configured, these are suitable for a smaller law office or home setting. Virtual private networks or VPNs may make remote access more secure. A VPN is a network connection constructed by connecting computers together over the Internet on an encrypted communications channel. VPNs are secure and fast, but may be expensive and harder to configure. Securing remote access may require a degree of technical knowledge and advice from a computer expert. To make your remote access safe, you must secure your network and your remote access devices.

Do the following to secure your network:

- Use a firewall and security software to keep out unwanted connections.
- Only give remote access to people who really need it.
- In order to protect sensitive information, restrict the type of data that can be accessed remotely.
- Make sure all computers connecting to your network, including personal home computers, have up-to-date security software installed.
- Review firewall and other server logs to monitor remote access and watch for unusual activity.

Do the following to secure remote access:

- Ensure installation of remote access clients is done properly.
- Restrict access to the minimum services and functions necessary for staff to carry out their roles.
- Ensure that all staff use strong passwords on devices accessing your network remotely.
- Change remote access passwords regularly.
- Make sure that staff do not set their devices to login automatically and that they never store their passwords on them.
- Use strong authentication that requires both a password and token-based authentication.
- Have a formal remote access policy that clearly describes what staff are to do or not do with remote access.
- Delete staff remote access privileges if they are no longer needed, and immediately when a person leaves or is terminated.

### **The extreme dangers of using public computers**

Public computers in libraries, Internet cafes, airports, and copy shops are an extreme security risk. While you can take steps to reduce these risks, it is still very dangerous to access sensitive client information on them. Start with the assumption that most public computers will have malware on them and let this govern your activities accordingly.

The following steps can reduce some of the risks associated with public computers:

- Try to turn on the “private browsing” feature.

- Watch for over-the-shoulder thieves who may be peeking as you enter sensitive passwords to collect your information.
- Uncheck or disable the “remember me” or “log in automatically next time” option.
- Always log out of websites clicking “log out” on the site. It’s not enough to simply close the browser window or type in another address.
- Delete your temporary Internet files, cookies and your history.
- Never leave the computer unattended with sensitive information on the screen, even for a moment.
- Never save documents on a public computer.

These measures will provide some protection against a casual hacker who searches a public computer you have used for any information that may remain on it. But keep in mind, a more sophisticated hacker may have installed a keylogger to capture passwords and other personal information entered on a public computer. In this scenario the above steps won’t prevent your information from falling into the hands of the hacker. This is why it is not a good idea to access sensitive client information or enter credit card numbers or other banking information on a public computer.

## **XI. Secure Your mobile devices to protect the data on them**

Lost or stolen laptops, smartphones and USB sticks are frequently involved in major data breaches. This is because they often contain large amounts of confidential or sensitive information (e.g., client data, firm and personal information, usernames and passwords, etc.) and they are also easily lost or stolen as they are small and very portable. You can significantly reduce your exposure to breach involving a mobile device by doing the following things:

- Take steps to prevent mobile device theft or loss;
- Make it harder to access information on the device; and
- Configure remote “find and wipe.”

### **Preventing theft or loss**

Here are some very easy ways to prevent the loss or theft of your mobile devices:

- Never leave your portable devices unattended in a public place.
- In particular, don’t leave them in your vehicle – even locked in the trunk is not safe;
- To be a less obvious target, use a briefcase or bag that does not look like a standard laptop bag;
- Inexpensive cable locks from Targus ([targus.com](http://targus.com)) and others can help deter a casual thief, but are no obstacle for a determined thief with cable cutters; and
- If you are staying at a hotel, put the device in a safe in your room or at the front desk.

### **Making it harder to access data on the device**

If a device is lost or stolen, you want to make it as difficult as possible for someone to access the information on it. This is very easy to do. As a first line of defense, you can enable the startup password. After enabling this feature, anyone turning the device on will be challenged for a password and they won’t



be able to see any information on the device. Most laptops and smartphones have this feature. However, while this should protect the data on the device from the average thief or person that might find a lost device, someone with specialized knowledge can bypass these built-in password-protection features.

For an extra level of security you can use encryption, which scrambles the data on a device making it very difficult for someone to access it. Some devices have an encryption feature in the device operating system, and, if not, you can use a third party encryption program or app.

One other option to consider: if you allow remote access, have people travel with a device that has no client data or other sensitive information on it. They can use it to access client data in the office via remote access and if the device is lost or stolen there is no lost information to be concerned about.

You may want to keep in mind that current case law provides that law enforcement does not need the permission of a device owner to access information on a device that is not password protected.

### **Device locators and remote wipe**

To prepare for the eventuality that one of your smartphones, tablets or laptops gets lost or stolen, you should enable or install device locator and remote wipe functionalities. These features are built in on some devices, and there are many third party programs and apps that do the same things. Using GPS technology or the tracing of IP addresses, you can potentially view the location of your device on a web-based map, sometimes along with where and when it was last used. Just in case the device is lost in your residence, you can also trigger a high volume ring to help you locate it, even if the device is on silent or vibrate. If the worst has happened and it appears that the device is permanently lost or was stolen, you can usually lock the device so no one can use it or access the data, and you can also remotely tell the device to do a factory reset, which will delete all data on it.

### **Beware of data theft with USB sticks**

Tiny, high-capacity USB sticks are commonly used for moving data around. A combination of three things makes them a major security concern: (1) they are very easy to use, (2) they are compact, lightweight and ultra-portable, and (3) they can store huge amounts of information. They are, in other words, the perfect tool for a disgruntled or soon-to-be ex-employee who plans to easily and quickly steal firm data.

How do you protect yourself? Make sure you have appropriate security and access rights to confidential client and firm information on your firm's computers and servers. Auditing file access may help you spot someone who is accessing information they should not. Consider disabling USB ports on firm computers used by people that have no reason to use USB sticks.

## **XII. Harden your wireless and Bluetooth connections and use public Wi-Fi with extreme caution**

At home, coffee shops, restaurants, hotels, conference centers, airport terminals and many other locations, many of us use wireless and Bluetooth for our smartphones, tablets and even our computers without a second thought. While very convenient, anyone using wireless and Bluetooth should know that they are fraught with serious security issues. Unless you lock down your wireless network and devices, someone sitting in a car across from your office or home could easily find and connect to them. Hackers known as “wardrivers” actually cruise around looking for networks they can hack into. There are even websites that list “open” networks by street address.

### **Hardening your wireless networks**

Use wireless with caution, and only after you enable all possible security features on your wireless routers and devices. The hub of your wireless network is a router. It connects to your Internet service provider through a telephone line or other wired connection. Anyone connecting to your wireless network through your router can likely connect to the web and quite possibly access other devices on your network.

Completing these steps will make it much harder for strangers to connect to your wireless network:

- Use WPA or WPA2 (WPA2 is better) or 802.1x wireless encryption. WEP encryption is found on older devices and it is recommended that you not use it as it can easily be cracked;
- Turn off SSID broadcasting;
- Disable guest networks;
- Turn on MAC filtering;
- Change default router name and password; and
- Disable remote administration.

More detailed directions for completing these steps can be found on the practicePRO website in the [“How to enable the security settings on a wireless router”](#) checklist.

### **Bluetooth vulnerabilities**

Bluetooth technology makes it easy for keyboards, headsets and other peripherals to connect to smartphones, tablets and computers wirelessly. Although security is available for Bluetooth, many vendors ship Bluetooth devices in Mode 1 (discovery/visible-to-all mode) to make it much easier for people using the devices to connect to them. In this mode they will respond to all connection requests. This introduces a number of vulnerabilities, including making information on the device more accessible to hackers and making the device more vulnerable to malware installation.

To make your Bluetooth devices more secure, you should do the following:

- Configure devices so that the user has to approve any connection request;
- Turn off Bluetooth when not in use;

- Do not operate Bluetooth devices in Mode 1 and ensure discovery mode is enabled only when necessary to pair trusted devices;
- Pair trusted devices in safe environments out of the reach of potentially malicious people;
- Minimize the range of devices to the shortest reasonable distance;
- Educate your staff about how to safely use Bluetooth devices; and
- Consider installing antivirus and personal firewall software on each Bluetooth device.

### **Be extremely cautious with public Wi-Fi**

Public Wi-Fi has become ubiquitous and a lot of people use it without a second thought. Unfortunately, there are major security issues with it. If you connect to a Wi-Fi network without giving a password, you are on an unsecured and unencrypted connection. On an unencrypted or “open” wireless network, anyone in your proximity can intercept your data and see where you are surfing (except if you are on an https website). Using an unencrypted connection to check the news or a flight status might be acceptable, but keep in mind that performing other activities is akin to using your speakerphone in the middle of a crowd.

Even worse, hackers will create fake Wi-Fi hotspots in public places to trick unwitting Wi-Fi users. “Free Starbucks Wi-Fi” may not be the legitimate Starbucks network. Connecting to a fake network puts your data in the hands of a hacker.

And don’t equate subscription (paid-for) Wi-Fi Internet with secure browsing. It may be no more secure than open Wi-Fi.

To be avoid these dangers, it is best avoid using public Wi-Fi hotspots altogether. Get a device that has mobile cellular capability, tether to your smartphone, or use a mobile Wi-Fi hotspot. This is a small Wi-Fi router you carry around that has mobile cellular functionality. It gives you a personal and private Wi-Fi cloud you can configure to securely connect your other devices to.

If you are going to use public Wi-Fi, here are some steps you can take to connect your device as securely as possible:

- If your firm has a Virtual Private Network or VPN, use it. This will encrypt your data and make it harder for it to be intercepted.
- Never connect without using a password (this means you are on an unencrypted network) and avoid using Wi-Fi that uses WEP encryption as it can easily be cracked. Use networks that have WPA, WPA2 (WPA2 is better) or 802.1x wireless encryption.

Enable the firewall and run updated antivirus software on your device.

- Turn file, printer and other device sharing off.
- Disable auto-connecting so network connections always happen with your express permission.
- Confirm the network name in your location before you connect (i.e., avoid the Starbucks imposter).
- Use sites that have “https” in the address bar as they will encrypt data traffic. “http” sites transfer data in plain text and should be avoided as a hacker can easily read the data transmissions. You

could use browser extensions or plugins to create https connections on http sites.

- Follow the best practices for safe and secure passwords

By taking these steps you can reduce your Wi-Fi risks, but you should save sensitive tasks like online banking for when you are on a network you know is safe and secure.

### **XIII. Be careful about putting your firm data in the cloud**

Almost everyone has data in the cloud, although many people may not realize it. If you are using Gmail or another free email service, iTunes, Facebook, LinkedIn or other social media tools, Dropbox, or doing online banking, your data is in the cloud. The “cloud” is the very large number of computers that are all connected and sharing information with each other across the Internet. If you create or post information that ends up outside your office, you are most likely in the cloud.

Cloud computing offers many benefits to lawyers. There is a vast selection of services, software and applications that can assist with just about every task in a modern law office, in many cases allowing those tasks to be accomplished more efficiently and quickly. Many of these services permit remote access, thereby allowing lawyers and staff to work from anywhere with full access to all documents and information for a matter. Using these services is usually economical as they can significantly reduce hardware and software maintenance costs and capital outlays. Storing data with suitable cloud service providers will likely mean that it is more secure and better backed up than it might be in a typical law office.

However, placing your client or firm data in the hands of third parties raises issues of security, privacy, regulatory compliance, and risk management, among others. Firms should have a process in place to ensure due diligence is performed and all risks and benefits are considered before any firm data is moved to the cloud. The evolving standard from U.S. ethics rules and opinions seems to be that lawyers must make reasonable efforts to ensure any data they place in the cloud is reasonably secure. Contracts with any third party that is in possession of confidential client information should deal with relevant security and ethical issues, including having specific provisions that require all information is properly stored and secured to prevent inappropriate access.

The Law Society of British Columbia has a [“Cloud Computing Checklist”](#) that will assist firms in identifying the issues that should be considered when performing the due diligence on a cloud provider. When considering your options, keep in mind that a cloud product or service designed for lawyers may have been developed with the professional, ethical and privacy requirements of lawyers in mind.

### **XIV. Inside people can be the most dangerous**

People inside your office have the greatest knowledge of your systems and where the important data is located. Many of the largest and most damaging cyber breaches have been caused by rogue or soon-to-be-

departing employees. You should take steps to reduce the likelihood that a cyber breach will be caused by someone inside your office.

When hiring a new employee, make sure you are diligent. Carefully check their background and speak to references. Look for any red flags on an application letter or résumé, and watch for issues during the interview process. Watch for someone who is withholding relevant information, or who has falsified information on the application. Assess the overall integrity and trustworthiness of the candidate. Consider doing police and credit checks (after obtaining consent) as persons in financial difficulty may be under pressure and become tempted to steal your firm’s financial or information resources. Doing all these things can help you avoid hiring an employee who could be a problem.

When any employee leaves your firm, regardless of whether they are leaving of their own accord or are being terminated, ensure that your systems are protected. Keep a log of any mobile devices held by your staff (e.g., laptops, smartphones, USB drives, etc.) and ensure that they are recovered immediately upon termination. Immediately close all points of access to your office and computer systems, including keys and access cards, login accounts and passwords, email accounts, and – in particular – remote access facilities. If you discharge an employee who has access to critical company data, let them go without warning (you may have to give them a payment in lieu of notice), and don’t allow them any access to a computer after termination.

There are literally dozens of steps you should complete systematically to make sure all points of access for departed employees are closed down. See the practicePRO website for a detailed “[Employee departure checklist](#)”.

## **XV. Be careful of the dangers of BYOD and family computers**

In many firms, it is common for lawyers to use personal smartphones or tablets for work purposes. This is often referred to as “Bring Your Own Device” or “BYOD.” Lawyers or staff may also work at home and even access the office network from a personal home computer. Both of these practices raise significant cyber risks.

### **BYOD**

Permitting staff to use their own smartphones or tablets makes great practical sense. They already own and are comfortable with the devices so the firm does not have to incur the cost of buying them or paying for wireless plans. However, if these devices connect to the office Wi-Fi or network, or if they are used to create documents that will be sent to the office, they can potentially deliver a malware infection to the office network.

### **Family computers**

Young people have a very high exposure to malware as they are more likely to engage in many of the most dangerous online activities, including using social media, downloading programs, and file sharing.

As a result, it is far more likely that any device children or teenagers are using is infected with malware. This is a concern because using a compromised computer for remote access to your office can bypass the firewall and other security mechanisms, potentially delivering a malware infection to the heart of your network.

To be absolutely safe, avoid using a home computer or other device for work purposes if it is used by others. Where a home computer is being used for work purposes, the steps outlined in this article must be followed to protect the office network and systems from cyber risks. Creating separate user accounts will make things more secure, but a better alternative is to have two partitions on your home computer. This essentially means there are two complete sets of software on the computer: one that only you would use, and one that others in the house would use.

Where a home computer or other BYOD device is being used for work purposes, the steps outlined in this article must be followed to protect the office network and systems from cyber risks. Staff education is key for reducing the risks associated with the use of personal equipment. Technology use policies should be in place to ensure all necessary steps are taken to address relevant cyber risks. See the practicePRO [Technology Use Policies Resources](#) for sample BYOD and remote access policies.

## **XVI. A backup could save your practice after a cybercrime incident**

Every law firm has huge amounts of irreplaceable data on its servers, desktop computers, laptops, tablets and smartphones. A cybercrime incident such as a malware infection or the hacking of firm systems could result in the destruction or loss of firm data. Having a current and full backup of all firm data will be essential for recovering from such an incident with the least possible interruption to a firm's operations. And beyond any concern about a cybercrime incident, every law firm should have a current full backup of firm data as part of its disaster recovery plan.

When keeping past copies of backups, consider that firm systems could have an undetected malware infection for a considerable period. If you have an undetected infection, you may have to go back in time to get a backup that is clean or has uncorrupted data. For this reason, you may want to keep a series of past backups (e.g., daily for last week, end of week for last month, end of month for last 3 months, quarterly, etc.) so that you can do a complete and clean restoration of your data.

There are many options for doing data backups, including using a dedicated backup system, external hard drives or other portable media, or the cloud. Apple users can easily set up an automatic backup with Time Machine.

Our "[Data backup options and best practices](#)" article, available on the practicePRO website, can help ensure you have a current and full backup of all the data in your office.

## **Conclusion**

Cybercrime is a real and present danger to you and your firm. LAWPRO strongly encourages Ontario lawyers to take this danger seriously and to take appropriate steps to reduce exposures to all relevant cyber risks. The “quick fixes” highlighted in the feature articles in this issue of *LAWPRO Magazine* will get you off to a good start with minimal cost and effort. At many firms, further time and work will be necessary. This extra effort is worth the investment as, at the very least, a cybercrime incident will be a costly and significant interruption to your firm’s business. And in a worst-case scenario, the financial and business interruption associated with a cyber breach could destroy your firm.