South Carolina Bar
Continuing Legal Education Division

2019 SC BAR CONVENTION

Technology Committee

"People, Processes, and Technology: Practical Information Security For Lawyers"

Thursday, January 17

SC Supreme Court Commission on CLE Course No. 190132

South Carolina Bar
Continuing Legal Education Division

2019 SC BAR CONVENTION

Technology Committee

Thursday, January 17

We Have Met the Enemy, and He is Us: The Role of the "Human Factor" in Protecting Information

Jack Pringle, Jr., Esq., CIPP-US

We Have Met the Enemy, and He is Us:
The Role of the "Human Factor" in Protecting Information

Jack Pringle
Adams & Reese, LLP
jack.pringle@arlaw.com

Contents

How Is Confidential/Sensitive Information Managed In Your Organization?

Note: Where reasonably possible, all of the actions below should be documented by written policies that are communicated to all relevant employees, followed, enforced, and updated as necessary.

I. Defining Confidential and Sensitive Information- make sure you know what you are touching and how you will protect it.

A. Do you collect confidential information? (presume your entire client file is confidential for this exercise).

B. Do you collect sensitive information? (all sensitive information is confidential, but additional requirements may exist if information is sensitive).

1. Do you collect, receive, and/or store personal information? Personal Information means any information relating to an identified or identifiable person (employees, clients, and any other individual) and includes, for example a person's name in connection with:

a. physical address, phone number, e-mail address;

b. social security number (SSN);

c. credit card numbers:

d. driver's license number:

e. passport numbers:

f. date of birth:

g. savings account, checking account, insurance policy or other health account or financial account number or information;

h. health or disability information;

i. employee background checks, including credit reports, and any records that are derived from this information;

j. consumer credit reports and any records that are derived from this information that relate to an identified or identifiable individual, whether an employee of the Firm, a client or otherwise.

2. Do you receive other sensitive information, such as personal health information, personal financial information, or other information from various third parties (for example, in discovery)?

    a. Does that information need to be subject to a Confidentiality Agreement or a Protective Order?

    b. Does your storage and use of that sensitive information (such as personal health information) need to be covered in a Business Associate Agreement (BAA) under HIPAA?

B. What document(s) memorialize how your firm will handle confidential/sensitive information?

    1. Do you have a client engagement letter? Does that engagement letter specify how you will:

        a. store confidential/sensitive information (e.g. using encryption),

        b. share confidential/sensitive information (via secure portal, an email encryption standard, etc.);,

        c. retain confidential/sensitive information (for how long and in what format); and

        d. dispose of or destroy confidential/sensitive information (return to client or other party, secure destruction)?

    2. If a Confidentiality Agreement or a Protective Order applies, what does that document require with respect to the sensitive information or documents protected thereby?

    3. If a BAA applies, what does that Agreement require you to do in order to protect information?

II. <u>How You Collect Information</u>

A. Do you collect more than you need to collect?
B. How do you collect or receive information? What's your procedure?
    1. In Person
    2. Phone
    3. File Transfer (from Client. Opposing Counsel, Other Third Party)
        a. Paper
        b. Electronic- is file transfer secure?
            1. email encryption

2. other secure file transfer

4. Website Form

C. Who collects it or receives information? (paralegal, attorney, legal assistant, someone else).

D. Does the person collecting information do so according to a procedure that recognizes confidential and sensitive information?

III. How You Protect Information in Storage

A. Do you need to store it at all?

B. Who is responsible for getting the information into your system?

C. Where do you store it?

1. Network

2. Hard Drive

3. Portable Device

D. Do you add additional protections to confidential/sensitive information?

1. Do you truncate or redact it?

2. Do you password-protect or encrypt it?

3. Do you limit access to it?

4. Who decides who can have access to what?

5. Do you back that information up?

IV. How You Share and Transfer Information- Does confidential/sensitive information leave your office?

A. How do you protect information when it leaves your office?

1. Do you password protect attachments (and send the password in a separate email message)?

2. Do you use email encryption or secure file transfer?

3. Do you encrypt portable media (e.g. thumb drives)

4. Do laptops that leave the office have encrypted hard drives?

B. Do you have a process for managing information you receive and share pursuant to a confidentiality order, protective order, or other agreement (e.g. BAA)?

V. How You Retain and Destroy Information- what do you do with the client file when the representation ends?

A. Do you have a documented file closing process?

B. Does Your Client Engagement Letter reference that file closing process and provide for what happens to the client file after the matter comes to an end?

C. Do you return documents to the client (esp. original documents) or to another party (for example, pursuant to a Confidentiality Order or a Protective Order)?

D. When and how do you destroy documents and electronic information? Do you memorialize that destruction?

E. Before you close a file, do you "harvest" or save what you might use again (without any confidential or sensitive information contained therein of course)?

General Security Concepts for Businesses and Individuals

Business Must-Dos

- **Control** access to your offices, computers, and computer networks, and prevent or limit unauthorized access.
- **Protect and secure** your computer networks (including any wireless network) with firewalls and antivirus protection that is updated regularly, and appropriate encryption. Periodically test the security of your network.
- **Install** security patches and software upgrades on all operating systems and applications as soon as they become available.
- **Identify and backup** the information that is important to you.
- **Manage, encrypt and password-protect** all devices (desktops, laptops, smartphones, usb/flash drives) used for business.
- **Train** all employees in basic security awareness, with policies, reminders, testing, videos, and seminars.

Individual Must-Dos

- Use strong, unique passwords for your online accounts. Consider a password manager.
- Set your devices, (including your smartphone), to lock after a short time, and require a passcode to unlock them.
- Patch and update all your software, applications, and operating systems.
- Employ dual-factor (2-step) authentication wherever possible (Google, Twitter, Facebook, LinkedIn).
- Avoid public computers and Wi-Fi, or work through a virtual private network (VPN) when accessing public Wi-Fi.
- Never click links in emails or texts that appear to come from your bank or any other institution. Always login to your account directly, and never send your financial information via email.
- Verify your privacy settings on mobile devices and social media.
- Be skeptical (on the Internet and with emails and attachments).
- Backup all of your devices.
- You are a line of defense against hackers (a security layer).

Electronic Funds Transfer Best Practices

1. **It Takes Two**. Have procedures in place that require two authorized people to send a wire or payment — one to initiate and one to approve.
2. **Validate** all electronic payment instruction requests you receive, even if the request is internal. **Be wary of "urgent" and "confidential" requests, or any other request that attempts to circumvent the Firm's procedures.**
3. **Make and Confirm Changes to Payment Methods or Instructions *By Phone*.**
    a. **Do not** use the contact information provided on the request to change payment method or payment instructions;
    b. **Do** use contact information known to be genuine such as the contact information in your file or information collected from the original engagement.
    c. **Have** the contact confirm existing payment instructions on file prior to making changes to those instructions (i.e. current bank account and routing number provided in original instructions).
4. **Document** the verification process you follow to validate payment instructions. The person responsible for entering/updating wire instructions **and** the person approving new/updated instructions must approve the record of verification. Maintain a record of the verification.
5. **Guard Your Account Number and Routing Number**.
6. **Monitor** bank accounts and transactions vigilantly. Check electronic payments and bank balances daily. Reconcile banking activity to the Firm's general ledger in a timely fashion.
7. **Use a Clean Computer for Banking Transactions**. Consider using one computer exclusively for electronic fund transfers. If you cannot dedicate a computer solely to wire transfers you should ban access to certain websites (e.g. social media website), as these are a significant source of malware used to hijack accounts.
8. **Download, Install, *and Update* Malware Protection Software** for all workstations.
9. **Consider Encrypted Email Communications**. Utilize encrypted emails for delivery of personal or financial information if possible.

Avoiding and Managing Ransomware

Defend Yourself- Technical

- Back up data and verify backups
- Secure backups (not connected to the computers and networks being backed up).
- Patches up-to-date.
- Automatic updates of anti-virus and anti-malware

Defend Yourself From Yourself

- Be Skeptical of Links
- Don't Open Attachments in Unsolicited Emails
- Download Software from Trusted Sites
- Implement Least Access Privilege
- Train and Create Awareness
- Segment and Separate Your Network Based on Value

What to Report if Infected:

- Date of Infection
- Ransomware Variant
- Victim Company Information
- How the Infection Occurred
- Requested Ransom Amount
- Actor's Bitcoin Wallet Address (General Recommendation is **Not** to Pay Ransom)
- Ransom Amount Paid
- Overall Losses
- Victim Impact Statement

From Ransomware Victims Urged to Report Infections to Federal Law Enforcement
https://www.ic3.gov/media/2016/160915.aspx

Every Lawyer is A Technologist: Take a Step Back to Take the First Step Forward
March 24, 2013

Quit Pointing Out What I Don't Know, and Tell Me Where to Start Learning

The legal community is all atwitter (pun intended) about the current and future effect of computer technologies (and other forces) on the way law is practiced. You hear the use of terms like "revolution," "sea change," and "paradigm shift." Some observers suggest that emerging technologies are throwing out not only the bathwater of the legal practice, but also the baby, the bathtub, and the plumbing.

For those attorneys not riding this wave, all the discussion of algorithms, ESI, Big Data, TAR, and the "urgent" need for change is disconcerting at best, and downright terrifying at worst. Fear may be an effective motivator, but only if you know where you are going and what you are going to do. Fear that creates only doubt (including the Fear of Missing Out or FOMO)[1] results in paralysis (head in the sand), denial (it doesn't affect what I do), anonymous Internet comments (no explanation necessary), and/or substance abuse (likewise). You have to know the way forward. As W. Edwards Deming remarked:

> *"**Drive out fear. No one can put in his best performance unless he feels secure.**"*

And lawyers often respond to fear in that quintessential American way: by reflexively buying (and subsequently, constantly, and continually checking) something (smartphone, tablet, software) in the hope it will address our anxieties and solve our problems. We buy without a thought to how the product or service will become a part of our existing practice, (or part of an existing network). As a result, when we don't know what we want (or how we intend to use it), we end up with a lot we don't want (and don't use).

Another Point of View

Let me suggest a different approach. Forget computers for the time being, or at least step back from their thrall. Computers and devices are a distraction (and not just for the usual reasons), and make us lose sight of several crucial facts:

- Technology is not limited to computers and computer systems;
- Technology is the application of knowledge for practical purposes (look it up)[2];
- Technology is the collection of *all* the tools we use to solve problems for clients;
- ***Lawyers use technology every day even if they never turn on a computer***.

And no decision to buy shiny new tools (especially expensive ones) can take place without evaluating your current technology- nothing more than what you do and how you do it- and then considering if there are other ways to do it better.

In other words,

1. take stock of what you know, have and do;
2. consider how you might do those things more effectively, and then (and only then)
3. adopt the tools that will accomplish your goals.

We are talking about how to *evolve* and *adapt* by building on our current approaches to problem-solving, not by letting HAL[3] ("File the motion, HAL"; "I'm sorry, Jack. I can't do that.") take over our practices.

What Do Lawyers Do?

Lawyers solve problems. The reason clients hire attorneys is because they need assistance getting something or somewhere. That "destination" may be the consummation of a business deal, creation of an entity, a favorable resolution to litigation, an estate plan, or a variety of other outcomes.

What Do Lawyers Use to Solve Problems?

Lawyers Solve Problems Using What They Know: Information and Knowledge (Legal and Other Varieties).

In tackling our client's problems, in the most fundamental sense we use and apply what we know.

Information. One part of what attorneys use is the information we learn over the course of a particular matter:

- We process, store, and present information in service of our clients;
- We identify, seek, and exchange information in discovery;
- We take the facts we learn, discern how best to use them, and present them in an appropriate forum or context.

Knowledge. Lawyers also combine information with legal knowledge.

- We receive facts in one form and repackage them in the context of their legal significance;
- We cite and argue relevant law gleaned from cases, treatises, and other sources. Pleadings, motions, and briefs are nothing but collections of information and legal knowledge;
- We present information and legal knowledge to a jury, judge, or appellate court;
- Information and legal knowledge shape transactions, wills, trusts, and tax returns;
- We also store our legal knowledge somewhere (hopefully not just in our heads)[4].

Lawyers Use Knowledge (Both Legal and Practical) To Manage Information. In our representation and advocacy, lawyers already utilize various tools (all of which are forms of technology) to organize and and present information and convey legal knowledge:

Processes/Procedures. How we practice law is in large part a collection of processes. A process is just a series of steps involved in preparing and presenting what we know. The creation and preparation of any document is merely a process that applies knowledge to information. Pleadings are drafted, reviewed, edited, filed, and served according to the requirements of various rules, standards, and practices. Each attorney or firm performs many processes in the course of a day: calendaring, conflict checks, file creation and maintenance, etc. Getting a document into evidence is just a process, as is qualifying an expert. Processes are accumulated knowledge performed over and over again.

And, evoking W. Edwards Deming again:

"If you can't describe what you are doing as a process, you don't know what you are doing"

Policies. Policies are (hopefully) written documents expressing your purposes and goals, and containing guidance about the means of implementing same. Policies may protect the confidentiality of information as required by the Rules of Professional Responsibility, or ensure other applicable standards of conduct. Effective policies include specific procedures and consider how the people in your organization will comply with (and ensure compliance with) same.

People. Clearly the creation, adoption, and implementation of procedures and policies require people. A policy or procedure that is not communicated, understood, and implemented where appropriate throughout an organization is more commonly known as a "missed opportunity" (bad) or a "problem" (worse).

How Do You Currently Solve Problems and Manage Information and Knowledge?
In order to determine whether you need "new" tools to manage what you know (information and knowledge), you have to identify what information and knowledge you have, and how you currently manage these resources (processes, procedures, people).

A great deal of this evaluation doesn't involve your computer system at all, but instead a review of work flow and office practices. Put it this way, (and borrowing from Dennis Kennedy)[5], you only need a sheet of paper to map out how you communicate and collaborate with your staff and other attorneys. I guarantee that even such a seemingly basic analysis will show you ways to improve upon the way you share information and perform tasks. Try it.

What Can You Do Better, and What Tools Can Help You Do That?
Then, once you know what you have and how you currently use it, you can consider how you might collect, store, organize, search, share, and protect that information and knowledge (and perhaps other information and knowledge) more effectively. The storage, search, and communication capabilities of computer systems undoubtedly offer advantages to lawyers.

However, only after analyzing your current information and knowledge processes and policies can you determine what you want and how you will use it. Knowing your current processes, policies, and people will put you in a better position to integrate those tools with appropriate computer technology.

Keep in mind also that computer technology is always the most useful information or knowledge solution (i.e. the best tool) in every situation. If taking notes on a legal pad continues to be the only way you will gather information, then that tool should not be removed from your toolbox. But consider whether information collected and/or stored electronically might benefit you.

Likewise, a practitioner is not well-served using a computer presentation at trial (especially a slideshow or Powerpoint) unless she has evaluated its effectiveness in communicating information to a judge and/or a jury. And surely a review of the way you use email might spark some discussion about whether other methods of collaboration [6](and appropriate communication) exist and ought to be employed.

The point is to be aware of how you do it and how you might do it better.

Conclusion: Build On What You Already Know and What You Currently Are Doing

Competence as a lawyer requires using the tools available to you. You are already using many of those tools. Identifying and understanding the way you use information and knowledge to solve problems will help show the way toward effective computer technology use to improve upon those skills.

The algorithms can wait. (Maybe).

Also available at https://medium.com/@jjpringlesc/every-lawyer-is-a-technologist-take-a-step-back-to-take-the-first-step-forward-ffa5aa34fd6a

The Humanity of Computer Security
August 17, 2011

Last week I posted [7] about attempts to develop Robots to perform "human" tasks, and the challenges inherent in creating a machine capable of mimicking and co-existing with people.

A recent Economist article [8] describes another effort to make computers exhibit a fundamental tenet of humanity- error. Cybersecurity experts at the University of Southern California (known as USC in some other parts of the country) are testing the security of computer networks by creating software programs to recreate the human errors that open up these networks to attack.

Human mistakes, as opposed to software or hardware failures or inadequacies, account for the majority of computer security breaches. Users fail to follow rules involving downloads, pop-ups and untrusted sites, and often intentionally disable security features on their computers. Fatigue and hunger can also make mistakes more likely to occur.

These scientists have created "cognitive agents," computer programs that simulate the behavior of users, managers, and IT staff, and particularly the ways in which these individuals compromise a computer network.

As mentioned in the piece, this project's focus on isolating and addressing the human aspect of security recognizes the fallacy of the old saying that "To err is human, but to foul things up completely requires a computer," and underscores the truth in the statement that "behind every error blamed on computers there are at least two human errors, including the error of blaming it on the computer." As Bruce Schneier [9] observed many years ago, "security is a process, not a product," and process is ultimately fundamentally human.

So when assigning responsibility for the success or failure of your network, consider the timeless observation by Walt Kelly's Pogo (brought to my attention by my father many years ago): "We Have Met The Enemy and He Is Us."

Also available at https://pringlepracticeblog.blogspot.com/2011/08/humanity-of-computer-security.html

Manage Your People to Manage Your Information
April 21, 2016

Introduction

I recently purchased and read "Cybersecurity's Human Factor: Lessons from the Pentagon,"[10] published in the September 2015 issue of the Harvard Business Review. I recommend it to anyone grappling with the challenges of implementing and maintaining information security in an organization.

The U.S. Cyber Command has recognized that an effective security program focuses as much on managing the risks associated with human error as it does in adapting to new technologies. As in the private sector (and in other governmental areas), human mistakes have played a significant role in most, if not all, military security incidents. Both the Armed Forces and the private sector have experienced many of the same egregious human security failures (clicking on phishing emails, navigating to unsafe sites, failing to create unique and strong passwords, failing to update and patch, etc.) that lead to disastrous consequences. Accordingly, preventing and minimizing security compromises necessarily requires substantial attention to the "human factor" in cybersecurity.

Combating Human Error

The military, mindful that advanced technology can create a false sense of security, has emphasized six principles in its quest to identify, eliminate, and minimize the risks of human error:

- *Integrity.* This is certainly a loaded term, but in practice this means that employees are held accountable for intentional acts of dishonesty and repeat offenses, but given leeway to make honest mistakes, (presuming these errors are reported quickly and lessons learned). This tracks nicely with the concept of a Growth Mindset[11], in which the freedom to make some mistakes is a crucial part of autonomy and growth.
- *Depth of Knowledge.* This is the best example of why continuous and continual training is crucial and necessary. In order to practice effective security, all employees must understand technology tools, the risks associated with using these tools, and how to manage those risks.
- *Procedural Compliance*. Those information security policies, procedures, and requirements your company adopts must be followed by all employees. If discipline or other penalties are warranted, will your company follow through in enforcement after security procedures are bypassed or careless acts taken?
- *Forceful backup.* This is another way to advocate for "dual control": the idea that very risky things (like a wire transfer) are done by two people. Effective security is prioritized and communicated from the top. In addition, your organization must provide appropriate monitoring of employee practices in order to ensure that employees do not run afoul of important security practices (e.g. transferring sensitive information outside the company's network).
- *A Questioning Attitude.* This principle seems a little counter-intuitive. If an employee is being "procedurally compliant," then there would appear to be little room to "question" those rules. However, "questioning" is more about thinking critically, investigating thoroughly, and being empowered to make sure the job is done right. And a pure "rule follower" will lack the

flexibility to grow and adapt when the playing field changes (with the introduction of new technologies, new threats, etc.).

- *Formality in Communication.* I would probably call this "clarity in communication". The gulf in understanding between information technology professionals and others is often great. Within the organization, policies and directives must be communicated in plain language, and taught and trained (over and over again) in a way that is likely to stick.

A Critical View

Of course, it is natural to be more than a bit skeptical about applying the lessons of the military to civilian organizations. Even if the security challenges are similar, how many organizations (especially those with young employees and flexible organizational structures) could implement a command-and-control structure within which "procedural compliance," "forceful backup," and/or "formality in communication" could exist, much less thrive?

The answer is you probably can't be as structured as the Army. But that doesn't let you off the hook when your information is valuable (and what organization stores information of no value to anyone?), and managing information risk is a priority.

Takeaways

My two primary takeaways from the military's experience and emphasis on its six principles are that all organizations: 1) would benefit from a little more rigor and accountability in implementing (and enforcing) their security programs (even if it doesn't reach martial discipline); and 2) can take concrete, practical steps (policies, training, implementation of appropriate technology tools) to build a culture of individual accountability, knowledge, and skepticism.

Also available at https://medium.com/@jjpringlesc/manage-your-people-to-manage-your-information-b39a6631e3a1

Effective Security Starts at the Top: The S.C. Supreme Court Mandates Strong Passwords

November 26, 2013

Earlier this month the South Carolina Supreme Court ordered[12] all members of the South Carolina Bar and all foreign legal consultants to log-in to the Attorney Information System (AIS)[13] and 1) adopt a stronger password; 2) choose and answer updated security questions; and 3) update and verify their contact information in AIS. Pursuant to the terms of the Order, those who fail to do so by December 15, 2013 may face suspension.

The Court's Order offers good lessons for all attorneys (and others) attempting to secure their firms and businesses.

Security is a Process, Not a Product

The Court recognizes that the security of the AIS relies in no small part on strong passwords created by attorneys, and mandates a process to attain that end. And *human* mistakes, as opposed to software or hardware inadequacies, account for most security breaches. Using a "weak" password (one that a computer can guess by means of generating many characters) or a "common" password (one that a person can guess or read) is like leaving a door open or a safe unlocked.

Although various technology products offer essential parts of an effective security program, (and as discussed in Locked Down: Information Security for Lawyers[14]) no product will save you from yourself if you decide to use "password" as your password, use the same password on multiple sites, click on bad links, or voluntarily share your bank account number in response to an email message.

Consider how to make security a priority in your firm, through the use of policies, training, and/or other methods. And understand that the combination of people, processes, and technology is necessary for appropriate security.

Any Effective Security Process Has Support from the Top and Appropriate Teeth

A Supreme Court mandate with Chief Justice Toal's signature and the threat of losing the ability to practice law is an effective way to get an attorney's attention and ensure compliance. Moreover, the fact that attorneys will not be allowed to pay their license fees until they have complied with the Order all but ensures 100% participation.

By contrast, how many attorneys would have updated their information in response to an email memo from a systems administrator for the AIS suggesting the use of stronger passwords? How many of you consider the recommendations of your IT staff, implement same, and follow through to make sure they are followed?

Protecting the client file as required by Rule 1.6 (“Confidentiality of Information”) and Rule 1.15 (“Safekeeping Property”) of the South Carolina Rules of Professional Conduct ("RPC") includes securing electronic information. A security breach caused by a weak password or

indiscriminate browsing may cause the same unauthorized disclosure of a client's confidential information as the theft of a paper file.

Conclusion

Although strong passwords may be a hassle and create yet another thing for attorneys to remember (and for some assistance with "password fatigue" click here),[15] clearly their use is one part of an effective information security program. Just as incentives and discipline are used in connection with other corporate purposes and obligations (e.g. to "encourage" lawyers to get their time in), so too should lawyers consider how to best encourage and enforce the development of a culture of security in their firms.

Also available at https://pringlepracticeblog.blogspot.com/2013/11/effective-security-starts-at-top-sc.html

Essential Computer Security Tips for All Businesses and Employees
April 26, 2016

In a connected world, sound information security practices are crucial for every employee of a business. Even a single simple lapse in judgment, like clicking on a link in a "phishing" email, can put all computer networks- and the sensitive information stored on them- at risk.

Every business must educate and train all of its employees on how to protect information and computer systems.

Below are a number of best practices (by no means a complete list) for securing personal and business devices and networks.

1. Use strong, unique passwords for your online accounts. Consider using a password manager.
2. Set your devices, including your smartphone, to lock after a short time, and require a passcode to unlock them.
3. Patch and update all your software, applications, and operating systems regularly.
4. Employ dual-factor (2-step) authentication as appropriate, both on corporate networks and for popular online sites (e.g. Google, Twitter, Facebook, LinkedIn).
5. Avoid public computers and Wi-Fi, or work through a virtual private network (VPN) when accessing public Wi-Fi.
6. Be skeptical on the Internet, and with emails, texts and other communications.
7. Never click links or open attachments in emails or texts that appear to come from your employer, bank or any other institution. Always login to your accounts directly.
8. Verify your privacy settings on mobile devices and in your social media accounts.
9. Backup all of your devices and storage systems.
10. Consider yourself a very important line of defense against hackers.

Employing these practices will not guarantee the security of your devices, networks, and information. However, creating security awareness and a culture of security will help eliminate or reduce the human error that so often compromises security and costs individuals and businesses dearly.

Also available at: https://medium.com/@jjpringlesc/essential-computer-security-tips-for-all-businesses-and-employees-b2d1c6af9c39

Amended Rule 1.15 RPC, and the Need for S.C. Law Firms to Implement File Retention Policies
May 17, 2012

On March 1, 2012, the South Carolina Supreme Court issued an Order[16] amending Rule 1.15, "Safekeeping Property," of the South Carolina Rules of Professional Conduct.

Minimum File Retention Requirement and Adoption of a File Retention Policy

Rule 1.15(i) establishes for the first time in South Carolina the requirement for an attorney or law firm to maintain client files after they are closed **for a minimum of 6 years** (unless the file is delivered to the client or the client has authorized destruction of the file and no pending or threatened legal proceedings are known to the lawyer). If the client does not request the file within 6 years following the end of the representation, the lawyer may destroy the file unless pending or threatened legal proceedings are known to the lawyer.

The last sentence of Comment 13 to Rule 1.15(i) will be of particular interest to the Bar:

"Attorneys and firms should create file retention policies and clearly communicate these policies to clients."

Benefits of a File Retention Policy for Law Firms

The development of a file retention and destruction policy, while daunting, is also a real opportunity for a firm.

First, a properly implemented policy will be more efficient, as fewer resources need be devoted to storage of closed files. (Other efficiencies may result from choosing electronic storage over paper storage for closed files. As the amended rule recognizes, electronic storage of documents is also an option, subject to the requirement that the client's file be "securely" stored and capable of being retrieved-- more on that in a future post).

Second, implementing a file retention policy allows an attorney or firm to "harvest" precedent, briefs and forms, to make those resources available for future use. (Thanks to Jim Calloway[17] for this observation). A consistent set of Knowledge Management[18] principles is crucial for a law firm, and should be woven into a firm's file retention policy.

Some Basic Elements of a File Retention Policy

Consistent with Rule 1.15(i) and the clear mandate in Rule 1.4 regarding communication with clients, the firm's written retention/destruction policy should be communicated and followed from the outset of the representation, considered continuously throughout that representation, and implemented upon file closing and after:

The Policy Should be Included in the Client Engagement Letter. Communicate with the client and obtain agreement at the outset regarding what will happen to the file upon the close of

the matter.

The Policy Should Be Implemented Throughout the Representation. Make sure that to the extent possible, no original documents provided by the client are contained in the file. If maintenance of original documents is necessary, label and segregate them accordingly.

The Policy Should Be Implemented at File Closing. All originals should be returned to the client. An attorney should determine whether an exception (e.g. pending or threatened legal proceedings) might prevent some or all of the file from being destroyed pursuant to the policy. As mentioned above, valuable drafts or cases that may have utility in other matters should be removed (and appropriately named[19] for easy retrieval. (As a substantive matter, attorneys should consider a File Autopsy[20] at the time the file is closed to figure out how to get better on the next one). Strip out unnecessary materials and duplicates. The client should be contacted with a closing letter containing a reminder of the file retention and destruction policy and asking the client to determine what should be done with the file. Once a thorough review and culling takes place, the file can closed and its future destruction date logged. The idea is to have the file closing process be the last time the file needs review.

The Policy Should be Followed. Once the firm has established a policy, it should follow it, by communicating with clients over the life of a file, and undertaking to "destroy files in a way that protects client confidentiality" (that means shredding, not tossing).

As with many processes, there will be some time and effort on the front end, but law firms will experience long-term benefits, financial and otherwise, from effective use of a file retention and destruction policy.

Also available at https://pringlepracticeblog.blogspot.com/2012/05/amended-rule-115-rpc-and-need-for-sc.html

Because That's Where the Risks Are: Vendor Management in a Connected World
July 29, 2014

When the infamous bank robber Willie Sutton[21] (reputedly) was asked why he robbed banks, he answered "because that's where the money is." Thomas J. Curry, Comptroller of the Currency, cited Sutton's quote in a recent speech[22] explaining why financial institutions are such attractive targets for cybercriminals. Not surprisingly, the Office of the Comptroller of the Currency (OCC) and other bank regulators have recognized the critical importance of information security in protecting (among other things) "the money."

These days, banks aren't the only businesses grappling with the challenges of protecting valuable assets from criminals. As a report[23] on cybersecurity published in *The Economist* recently pointed out, the internet was built for connectivity, not security. Companies in many industries are discovering that the benefits of connecting and sharing information with others (including doing business in "the cloud") come with a price: their valuable information assets (and those of their customers) are increasingly at risk.

Information security risks extend beyond the (fire)walls of a business and frequently involve third-party vendors. The Target breach -- and an HVAC contractor's role in same -- underscored just some of the myriad risks associated with third-party vendors. One lesson is that although business partners may be at fault when information security or networks are compromised, the ultimate responsibility for those incidents -- the financial, legal, and reputation damages -- cannot easily be shifted from the business to the otherwise-responsible third parties.

The OCC understands the potential risks of doing business with third-party vendors. Its OCC Bulletin 2013-29[24] (the "Guidance") identifies a number of issues that banks must consider when assessing and managing risks associated with third-party relationships.

The Guidance's holistic approach to risk management is particularly instructive for any business connecting with vendors and entrusting third parties with valuable information (e.g. personal identifying information, intellectual property, competitively sensitive information).

Implement Effective Information Risk Management throughout the Life of the Vendor Relationship (A Work in Progress and Process)
Because information risk is dynamic (emerging technologies, the ever-changing threat landscape, an evolving legal and regulatory landscape), it cannot be "managed" at any given single point in time. For these reasons, the Guidance emphasizes that management of vendor information risk, like all information security and risk management, is an ongoing process or project, involving a combination of people, policies, and technology that is assessed and adjusted based upon particular circumstances.
The "lifecycle" of a vendor relationship includes the following milestones:

- *Planning*. Identify the potential information risks associated with a vendor before those risks arise;
- *Vendor Selection.* Evaluate and choose vendors with an eye towards addressing and minimizing those risks;

- *Contract Negotiation.* Insist upon written contracts that take into account the value of information assets and address information risk as appropriate; and
- *Ongoing Oversight*. Monitor vendor performance over the life of the relationship.

Planning (Identify Information Assets and Risks)

- Designate those individuals and groups with specific responsibility for vendor management that will continue during the life of the relationship;
- Identify those information assets (e.g. personal identifying information, intellectual property, confidential information, trade secrets) that will be shared with a vendor (or put at risk as a result of a vendor relationship);
- Consider the laws and regulations applicable to the business and the third-party vendor, plan for how the business will assess potential vendors, negotiate a contract with appropriate information privacy and security provisions, and oversee the vendor's performance of the parties' contract;
- Determine the potential negative consequences (e.g. financial risk, legal and regulatory risk, reputation risk) that a third-party data breach, system outage, or network intrusion might have on your business..

Vendor Selection (Make Sure the Vendor Can and Will Protect Information)

- Undertake a proper investigation before selecting a third party to manage information assets. Due diligence at a minimum requires an assessment of a vendor's *legal and regulatory compliance, financial condition*, and *business experience and reputation.*
- Consult reference information available on the Web and elsewhere (including background and reference checks through the Better Business Bureau, the Federal Trade Commission, state attorneys' general offices, state departments of consumer affairs, etc.) to learn about a prospective partner's business and history; customer complaints or litigation; Securities and Exchange Commission and other regulatory filings; and its website and other marketing materials.
- Review the vendor's *risk management and information security programs* (and any written documentation, including policies, processes, and internal controls, which may be associated with those programs), consider any certifications (ISO/IEC[25], NIST[26]) the vendor may hold, and review the results of any information security assessment or audit the vendor may have conducted.
- Evaluate the vendor's *resilience*, or ability to respond to various service disruptions or breach events. Does the company have a disaster recovery or business continuity plan? And what kind of *incident-reporting and management programs* does the vendor have in place, especially in the event of a data breach? *In other words, has the vendor considered information risk in creating its own processes and systems?*

Contract Negotiation (Define Rights and Responsibilities)

- Negotiate a written contract specifying the rights and responsibilities of the parties, particularly when a business has direct privacy and information security obligations. If a vendor will have access to personally identifiable information or other confidential or sensitive information, then the contract must define the specific information that will be provided to the vendor, as well as the vendor's obligations with respect to that information. If legal or regulatory requirements (e.g. GLB, HIPAA, various state statutes) govern information provided to the vendor, then the vendor's compliance with all such authority should be spelled out clearly in the contract.
- Spell out in sufficient detail the information security safeguards to be employed by the vendor, and the oversight rights to ensure vendor compliance with those safeguards. The business may require annual third-party assessments, audits and/or examinations of the vendor's security systems and practices, in order to ensure ongoing compliance with the terms of the agreement.
- Designate the requirements and procedures to be followed by the vendor in the event of a security breach, including timely notification, full cooperation, and assignment/allocation of responsibility for response, mitigation, and remediation activities.
- Include reimbursement, indemnification, and applicable insurance requirements (including, but not limited to, cyberliability insurance) as appropriate and necessary.
- Define the events that will bring about default and termination under the contract, and consider the transition from that vendor to another provider and the effect it may have on the business.

Ongoing Oversight (Assess, Adjust and Adapt)

- Maintain clear roles and responsibilities for monitoring the performance of the vendor over the life of the relationship.
- Examine and evaluate a vendor's performance and compliance periodically. In the same way a business must continually assess, adjust, and adapt to evolving information risk, so too must its business partners.
- Consider whether the information security standards, insurance requirements, and other obligations set out in the contract must be revised based upon the parties' experience, changes in the legal or technological landscape, or other factors.

Conclusion

Nassim Nicholas Taleb has written that "*It is preferable to take risks one understands than understand risks one is taking.*" Understanding the risks of connecting with and entrusting information to third parties, and taking steps to manage those risks is an essential requirement for doing business in the information age- and protecting your "money".

Also available at https://www.linkedin.com/pulse/20140729115402-13052403-because-that-s-where-the-risks-are-vendor-management-in-a-connected-world/

Learning the Lessons of John Henry: The Importance for Attorneys of Embracing Automation
January 18, 2016

We've all heard stories of Human v. Machine. Perhaps the most memorable is that of John Henry, the "steel-driving man" who (legend has it) won a race with a steam-powered hammer, only to die from exhaustion soon after with his hammer in his hand.

The late great Johnny Cash memorialized Henry's feats in the "Legend of John Henry's Hammer":

John Henry said to his captain said "A man ain't nothin' but a man
But if you'll bring that steamdrill 'round I'll beat it fair and honest.
I'll die with that hammer in my hand but, I'll be laughin',
Cause you can't replace a steel-drivin' man.

In this age of ubiquitous computer technology, there is no shortage of opinions regarding the effects that automation may have on many occupations and professions, including the proposition that computers may replace certain jobs entirely. Once again the human is seemingly pitted against a machine.

A Time of Potential Transformation (and Perhaps not Extinction)

So I am relatively encouraged to read some recent views suggesting that attorneys and law firms (and other businesses) are not necessarily in a death match with high-powered computers. As the New York Times article "The End of Lawyers? Not So Fast"[27] suggested, citing a McKinsey & Company study[28], technology is "likely to *transform*, rather than *eliminate*, jobs." As the McKinsey study put it:

few occupations will be automated in their entirety in the near or medium term. Rather, certain activities *are more likely to be automated, requiring entire business processes to be transformed, and jobs performed by people to be redefined, much like the bank teller's job was redefined with the advent of ATMs.*

In other words, the existence of one set of tools (computer technology) requires an organization to figure out how to use those tools in concert with its other tools (people and business processes).

To put a finer point on the importance of effective computer technology use, the authors of the McKinsey study asked "How Many of Your Daily Tasks Could be Automated?"[29], and posited two principal benefits of automating tasks: 1) investments in automation generate benefits worth three to ten times the cost; and 2) businesses derive value from activities that employees do *instead of* the work that is now automated.

In other words, as tasks are automated, lawyers and law firm employees are freed up to do other work, and must determine how to use that time most productively. As the McKinsey Automation potential and wages for US jobs[30] interactive graphic shows (give it a try), 23% of a lawyer's time could be automated with the use of current technology, and *fully 69% of time currently spent by paralegals and legal assistants* could be automated. Of course, those statistics also suggest that if law firms do not automate those tasks, someone else will. In other words, the outlook is not so good for those attorneys continuing to swing a steel hammer when they should be operating a steam-powered hammer.

Make Sure You Are Using the Right Hammer

The good news for attorneys is that there are a great many "steam-powered hammers" sitting (quite literally) at our fingertips, in the form of available computer tools. Automation in the law office context doesn't necessarily mean "big data" algorithms and writing software code. Think of computer technology tools helping out with any task that you do over and over again (words, sentences, paragraphs, contacts, pleadings, briefs).

As described in this article[31] from the ABA's Law Technology Today, automation may involve using your current tools more effectively (email rules, automatic renumbering of sections, spellcheckers, QuickParts, templates), or exploring new automation tools (like voice recognition software or document creation software).

Render Unto the Lawyers . . .

Other studies cited in "The End of Lawyers: Not So Fast" show how automation *complements* labor in the workplace, especially in the law office. Significantly, lawyers do a great many tasks that are less structured and not subject to being automated:
As it turns out, being a lawyer involves performing a range of tasks, from reading and analyzing documents, to counseling, appearing in court and persuading juries. Indeed, reading documents accounts for a relatively modest portion of a lawyer's activities.

Additionally, software programs employed for e-discovery require a great deal of human involvement. The trick is figuring out those tasks that are better suited to automation, rethinking processes to incorporate appropriate automation, and then doing more of the things—like counseling and advocacy, and the client development to have more of that work to do—that the machines don't do so well.

You Are Smarter Than You Think

Attorneys have the opportunity to transform their practices by working with—and not against—computer technology. As author Clive Thompson wrote, in his book Smarter Than You Think: How Technology is Changing Our Brains for the Better[32]:

Which is smarter at chess—humans or computers?
Neither.
It's the two together, working side by side.

Unlike John Henry, attorneys are in the position to continue to be relevant, as long as we identify and utilize the strengths of both Human and Machine.

Also available at https://counselorchronicles.com/learning-the-lessons-of-john-henry-7de7f4c2b130

---

[1] http://sethgodin.typepad.com/seths_blog/2013/03/fomo-joy-jealousy-and-the-lizard.html
[2] http://www.merriam-webster.com/dictionary/technology
[3] http://en.wikipedia.org/wiki/HAL_9000
[4] http://pringlepracticeblog.blogspot.com/2011/09/building-will-power-feed-your-brain-and.html
[5] http://www.americanbar.org/publications/law_practice_magazine/2013/march-april/13-tech-tips-for-2013.html
[6] http://www.wsj.com/articles/how-i-tamed-the-email-beast-at-work-1457921533
[7] http://pringlepracticeblog.blogspot.com/2011/08/ready-for-robots.html
[8] http://www.economist.com/node/21525360
[9] http://www.schneier.com/
[10] https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon
[11] http://mindsetonline.com/whatisit/about/
[12] http://www.judicial.state.sc.us/courtOrders/displayOrder.cfm?orderNo=2013-11-04-01
[13] https://www.sccourts.org/AIS
[14] http://apps.americanbar.org/abastore/index.cfm?pid=5110741&section=main&fm=Product.AddToCart
[15] http://pringlepracticeblog.blogspot.com/2013/02/remember-and-protect-important-stuff_25.html
[16] http://www.sccourts.org/whatsnew/displaywhatsnew.cfm?indexID=796
[17] http://jimcalloway.typepad.com/lawpracticetips/2009/07/closing-the-client-file.html
[18] http://lawyerkm.com/
[19] http://apps.americanbar.org/lpm/lpt/articles/ftr09091.shtml
[20] http://www.nonbillablehour.com/2011/12/perform-file-autopsy.html
[21] https://en.wikipedia.org/wiki/Willie_Sutton
[22] http://www.occ.gov/news-issuances/speeches/2014/pub-speech-2014-59.pdf
[23] http://www.economist.com/blogs/babbage/2014/07/special-report-cyber-security
[24] http://occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html
[25] http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534
[26] http://www.nist.gov/
[27] http://bits.blogs.nytimes.com/2016/01/04/the-end-of-work-not-so-fast/?_r=0
[28] http://www.mckinsey.com/Insights/Business_Technology/Four_fundamentals_of_workplace_automation
[29] https://hbr.org/2015/12/how-many-of-your-daily-tasks-could-be-automated
[30] https://public.tableau.com/profile/mckinsey.analytics#!/vizhome/AutomationandUSjobs/Technicalpotentialforautomation
[31] http://www.lawtechnologytoday.org/2015/09/5-questions-on-automation/
[32] http://www.amazon.com/Smarter-Than-You-Think-Technology/dp/1594204454

South Carolina Bar
Continuing Legal Education Division

2019 SC BAR CONVENTION

Technology Committee

Thursday, January 17

Training Your Organization (and Yourself): The Ongoing Process of Maintaining an Aware Security Posture

Mary E.A. Lucas, Esq., CIPP-US, CCSK

TRAINING YOUR ORGANIZATION (AND YOURSELF):

THE ONGOING PROCESS OF MAINTAINING AN AWARE SECURITY POSTURE

WHY TRAIN

- In 2018, 70% of chief information security officers listed “lack of competent in-house staff” as their number one security concern, followed by data breaches, cyber attacks, and ransomware[1]
- CPO Magazine recently noted in regards to cyber security training, “Additional training and education is needed at every level – from mailroom to boardroom – to address the growing concern of vulnerabilities . . . .”[2]
- “90% of all cyber claims stemmed from some type of human error or behavior.”[3]

[1]HTTPS://WWW.HEALTHCARE-INFORMATICS.COM/NEWS-ITEM/CYBERSECURITY/WHAT-ARE-CISOS-WORRIED-ABOUT-2018-DATA-BREACHES-AND-HUMAN-FACTOR-SURVEY

[2]HTTPS://WWW.CPOMAGAZINE.COM/2018/08/27/THE-HUMAN-FACTOR-IN-CYBERSECURITY-TRAINING-WHY-ADOPTING-A-HOLISTIC-APPROACH-IS-MOST-VALUABLE/

[3]HTTPS://CHIEFEXECUTIVE.NET/ALMOST-90-CYBER-ATTACKS-CAUSED-HUMAN-ERROR-BEHAVIOR/

According to the 2017 ABA Legal Technology Survey, 22% of the 4000 respondents said they had experienced a data breach

WHO TO TRAIN

- Everyone: from the mailroom to the boardroom
- Appoint a security liaison
- Ensure IT representative attends
- Ensure information security representative attends
- Temporary employees—interns, runners, summer help

SECURITY LIAISON

- Someone not on the IT team
- Works well with IT and/or IS team
- Good communicator and natural teacher
- Interested in IT or information security
- Committed to staying abreast of information security trends
- Willing to lead by example

WHAT TO TRAIN

- IT terminology
- Basic principles of cyber-hygiene
- Password best practices
- Threat spotting
- Physical security
- Privacy
- Laws, regulations, rules
- Internal policies, directives, and/or guidelines
- Reporting of incidents or concerns
- Expectations of staff and consequences for failure to comply

WHEN TO TRAIN

- Onboarding
- All employees at least annually
- Bi-weekly/monthly email updates or newsletters
- As needed

TESTING

- Cyber-security industry recommends testing staff to ensure comprehension
- Test after train
- Test real-life scenarios
- Remedial training

WHERE TO TRAIN

- In person
- At workstation

H0W TO TRAIN

- Make it required
- Make it interesting
- Make it understandable
- Make it doable
- Make it meaningful

CONTACT INFORMATION:

Mary E. A. Lucas
Chief Information Security Officer
Assistant Chief Counsel
S.C. Department of Natural Resources
P.O. Box 167
Columbia, SC 29202
803.734.0997 (office)
803.722.3926 (cell)
803.734.3911 (fax)
LucasM@dnr.sc.gov

1.17.2019

TRAINING YOUR ORGANIZATION (AND YOURSELF): THE ONGOING PROCESS OF MAINTAINING AN AWARE SECURITY POSTURE

MARY E. A. LUCAS, ESQ., CIPP-US, CCSK

DESIGNATE AN IN-OFFICE SECURITY LIASION

Someone in your office, not on the IT team, needs to be responsible for ongoing security awareness and training.

Establish a schedule

i. The security liaison should establish a schedule for training and routine disbursement of information security considerations or concerns.
    (a) For example: training is done in person or through a purchased online training module every six months, while a weekly or monthly email details common information security tips or news stories, e.g., current phishing trends, effective password strategies, IOT considerations, practicing good cyber-hygiene, etc. The security liaison may choose to set Google alerts or subscribe to a reputable online information security newsletter to stay abreast of current information security trends: see, e.g., https://www.sans.org/security-awareness-training/ouch-newsletter, https://www.infosecurity-magazine.com/, https://iapp.org/news/united-states-dashboard-digest/.

Content

i. While formal security documentation has its place, security advice and tips delivered in manageable, bite-sized chunks are more likely to be effective at both training and reinforcing good security habits. Hence, weekly or monthly emails containing one piece of important information are effective.
ii. The security liaison should communicate with the IT team prior to the presentation of materials or information to ensure their concerns and/or desires are represented as well.

Communication

i. The security liaison should regularly meet with the IT and/or information security team to establish an open line of communication.
ii. The security liaison should be contemplated in the incident response plan for information security events, and should clearly understand their role and protocol should an event occur or be reported to the security liaison.
iii. In the event of an incident, the security liaison should follow established protocol and ensure proper communication with counterparts on the IT and/or information security team.

ESTABLISH A REPOSITORY FOR REPORTING INFORMATION SECURITY CONCERNS

It may be your in-office security liaison, someone from your in-office or outsourced IT team, or a specific inbox with its own email address, e.g., SecurityConcerns@LawFirm.com. There also should be a phone number to report urgent matters.

Encourage reporting

i. Staff members should feel comfortable and encouraged reporting incidents. Occasionally, malicious emails contain embarrassing content, like accusations the recipient has been watching pornography. See https://www.eff.org/deeplinks/2018/07/sextortion-scam-what-do-if-you-get-latest-phishing-spam-demanding-bitcoin. It is critical staff feel their reports will be handled with professionality, the appropriate level of confidentiality, and impunity (assuming he/she has not violated office policy).

Repetition is key

i. The security liaison should provide the appropriate email address and phone number for reporting incidents—e.g., phishing emails, social engineering attempts, etc.,—in all communications, including their regularly scheduled emails.
    (a) Either the security liaison or a designated IT team member (or both!) should be monitoring the email inbox.
    (b) Whoever monitors the inbox should be communicating trends and concerns with the rest of the information security team.
ii. All communications to office staff should encourage questions and reporting of concerns.

ESTABLISH, ENFORCE, AND ROUTINELY REVIEW SECURITY POLICIES

An information security policy is the cornerstone of an information security program.

Collaborate, create, then communicate

i. Where applicable, members of the IT, human resources, leadership, and management teams all should be involved in drafting and reviewing information security policies.
    1) The first step is defining how management and leadership view security. Starting with a philosophical approach can help build consensus as to the types of information security mandates the organization is interested in implementing.
    2) Trust your professionals. Your IT team should be able to provide guidance on how technical solutions may be implemented, e.g., email encryption, VPN, removal media storage devices such as USBs, etc. Your HR team should be able to provide guidance on how to draft disciplinary provisions for failure to comply. If additional guidance is needed, consider consulting with an outside information security firm. A seasoned information security professional will have advice on how to build a consensus and implement a comprehensive information security policy.

ii. Avoid off-the-shelf products. There are information security policy frameworks available for free and for purchase. However, an effective information security policy takes a comprehensive approach by looking at the organizations existing infrastructure, policies, personnel, and values in crafting a narrowly targeted approach at protecting your information resources.
    1) However, there are existing information security industry standards that may serve as a baseline for implementing a more specific information security policy. See, e.g.: https://www.securityforum.org/, https://www.iso.org/isoiec-27001-information-security.html, https://www.isaca.org/COBIT/Pages/default.aspx. For South Carolina government agency recommended policies and procedures, see: https://www.admin.sc.gov/technology/information-security/policies-and-procedures. For a somewhat dated but nonetheless information ABA article on essential law firm technology policies and plans, see: https://www.americanbar.org/publications/law_practice_magazine/2012/march_april/hot-buttons/.

Keep it practical

i. Critical security functions must be included. Beyond that, it is better to have a policy to which there is agreement and compliance is achievable, than to have overly time-consuming or challenging mandates few in the organization are willing to observe.

ii. No exceptions. When people understand there are no exceptions to the policy, they are generally more willing to getting it right up front, and continuing efforts to remain compliant.
iii. Consider using sub-policies for very large organizations or specific subject matters.
    1) It may be necessary to have a broad, overall organization policy with mandates that apply to all, as well as sub-policy documents segregated by intended audience.
    2) Consider sub-policies that deal with subject matters, e.g., social media, data retention, etc.

Review, review, review

i. Once your policy is finalized, communicate the policy to office staff and require a signature acknowledging receipt and understanding of the policy.
ii. Your information security policy(s) should contain a provision for regular review of the policy document(s). Laws, regulations, rules, personnel, protocols, assets, and technology all change over time, and it is critical your information security policy stays up-to-date and relevant
    1) Require a signature of receipt and understanding by staff members with each new iteration of the information security policy(s).

LEAD BY EXAMPLE

Good security practices start with the leadership team.

Leadership should learn basic security practices and utilize them!

i. Follow security protocol and policy(s) to the letter; otherwise, others cannot be admonished in good faith for failing to do so.
ii. Staff members who observe other team members embracing and executing good security habits will likely feel a sense of responsibility to do the same.
    1) Examples of simple habits that translate to greater security: not displaying passwords openly, locking your computer every time you walk away, securing organization devices with dual authentication, etc.

PUT STAFF TO THE TEST

Continuing training and security updates are important, but testing staff members on retention of important principles as well as real-world simulations are priceless.

Test following instruction

iii. Ensure staff are engaged and retaining the information they are provided in their information security training by testing the material after each training session.

1) Testing not only incentives awareness during training, it also allows the security liaison or other instructor as to who may benefit from remedial measures.
2) Tests may be as simple or complex as desired, and generally should be generated based on the material presented or information staff is widely expected to know.

Provide real-world simulations

i. You may train on a topic like social engineering a dozen times, but you will not know if your staff is going to follow organization guidelines and training for such a scenario unless they are tested.
    1) Hire a "hacker" or do the job internally.
        (a) There are professional organizations that can work with you on real-world testing. If you contract with a third-party information security firm already, that may be a service they provide. One valuable third-party testing apparatus is to engage simulated phishing email attacks.
        (b) Or you can do the testing yourself. For example: have a member of your organization (preferably an unrecognizable voice) call a staff member(s) and feign that they are a member of your IT team. The caller will inform the staff member that they need his/her network username and password. The staff member(s) who provides their credentials fail the test, as staff should be trained to never provide credentials over the phone, as the caller is never truly verifiable. Staff members who fail the test should be provided appropriate remedial training.
    2) Test your security liaison.
        (a) The person responsible for training staff on information security may suffer from the common affliction of over-confidence in their ability to discern threats and/or properly follow organization guidelines. Have someone from your IT team or a third-party test the security liaison to keep them on their toes.

TRAIN STAFF ON PROPER SECURITY MEASURES BOTH INSIDE AND OUTSIDE THE OFFICE

We live in an increasingly mobile digital society. Access and availability of sensitive information is at an all-time high, and staff need to know how to be secure based on their environment.

Increasingly mobile

i. It is increasingly important that mobile devices accessing sensitive information— including cell phones, laptops, tablets, and iPads—are

appropriately safeguarding that data. Work with your IT and/or information security team to ensure staff mobile devices are secure.

ii. Ensure staff is trained as to the risks associated with mobile access of sensitive data and how to secure their devices. Important topics may include: regularly backing up mobile devices, educating on data loss prevention, and how to prevent against theft and accidental disclosure.

iii. Consider a mobile use policy or sub-policy that fits your organization's needs when it comes to the utilization of mobile devices. Consider measures that could better protect your information assets such as requiring staff to utilize user identification and strong authentication for logging into their mobile device, run current anti-malware software, and/or use virtual private networking (VPN) links to access the corporate network.

Public (unsecure) vs. private (secure) wi-fi

i. It is critical that staff understand that not all internet environments are created equal, and that some, like public wi-fi, are simply not acceptable means of connecting to the internet when accessing sensitive information. Work with your IT team to establish options around staff using public wi-fi, like providing secure mobile hotspots or VPN for staff that may need to work from the occasional Starbucks or hotel lobby.

MAKE SECURITY TOOLS WIDELY AVAILABLE

Staff will not engage security tools that are too cumbersome or inconvenient to access and utilize.

Train staff on how to secure it all

ii. Your information security toolbox should be comprehensive, and should reduce the risk of exposure of not only digital assets but also conventional ones.

1) Train your staff to lock their file cabinets, to have a clean desk practice, to close and lock their doors every time they exit their offices, to use paper shredders.

(a) If you notice staff not following guidance on the physical securing of assets, consider measures to incentivize or alleviate burdens to voluntary participation, e.g., invest in large, locked shred bins that make shredding easier and more efficient; use signage around the office to remind employees to close and lock their doors each time they exit their office, etc.

2) Train staff to utilize digital tools, and make those tools easily available. Your IT team may assist in determining how to make tools such as VPN, data encryption, malware scanners, etc. widely available. Staff should then be trained on how, when, and why they should utilize each tool.

South Carolina Bar

Continuing Legal Education Division

2019 SC BAR CONVENTION

Technology Committee

Thursday, January 17

When, Not If: A Simulated Law Firm Data Security Incident with Its Ethical Implications for Lawyers

Jacqueline "Jax" M. Pavlicek, Esq., CIPP-US

No Materials Available

South Carolina Bar
Continuing Legal Education Division

2019 SC BAR CONVENTION

Technology Committee

Thursday, January 17

Panel Discussion Q&A

Mary E.A. Lucas, Esq., CIPP-US, CCSK
Jacqueline "Jax" M. Pavlicek, Esq., CIPP-US
Jack Pringle, Jr., Esq., CIPP-US

No Materials Available