CYBERSECURITY

Understanding & Mitigating the Growing Threats to Legal Departments

Written For

SPECIAL COUNSEL

By

Gregory Peterson
(ARCHETYPE COMMUNICATIONS, INC.)

WORK SAMPLE

FOR PROFESSIONAL PROMOTION ONLY

Cybersecurity issues were explicitly recognized in the 2012 revisions to the American Bar Association's Model Rules of Professional Conduct. In drafting those changes, the ABA formally recognized that all lawyers have a clear duty to keep abreast of the benefits and risks associated with information technology [Model Rule 1.1 (Comment 6)].

Consequently, cybersecurity issues will constitute an increasing share of your bandwidth in the years ahead — whatever your position in the legal universe. In corporate law departments, in law firms, in government entities and nonprofits, and in the home offices of solo practitioners, competence with computer security issues has become an essential capability. If cybersecurity issues somehow have not yet found a place on your list of professional priorities, now is the time to begin.

What is cybersecurity?

Cybersecurity (also known as "computer security" or "IT security") is the protection of computer hardware, software, information networks, digital services and data. These digital resources can be damaged or compromised in many ways— both accidentally and intentionally — and a robust cybersecurity program addresses them all.

In general, cybersecurity threats arise from three major sources: Human Error; Natural Disasters; and Intentional Breaches. It is this third category — characterized by the rampant rise in unauthorized access to digital information that has spurred the legal profession (and the nation) to make cybersecurity measures a pressing priority for concerted attention.

> "Law firms are…
> 'one-stop shops' for attackers."
>
> *Shane M. McGee, general counsel and vice president of legal affairs at Mandiant Corp., a leading cybersecurity firm.*

More data means more threats.

As digital information technologies became the common standard for businesses, government and third-sector organizations, so grew the numbers of digital devices. With this dispersion of devices, data collection expanded and decentralized, then grew substantially as data-storage costs steadily decreased. Consequently, the sheer volume of resources available to cybercriminals has grown exponentially.

Every Internet-connected office and home now promises cybercriminals a potential windfall of valuable information. At the same time, the value of these digital resources has soared. In today's globally competitive marketplace, cyberthieves are discovering new ways to extract and process the data assets they steal, and there appears to be no shortage of "underground" customers willing to pay handsomely.

Cyberattackers are getting smarter

During the 1990s and into the early 21st Century, computer security conversations typically revolved around "hackers" — individuals or small groups who broke into the websites of highly visible targets and caused mischief. Oftentimes, it seemed that the hackers just wanted to make a public demonstration of their hacking skills.

However, today's cyberattackers and criminals are not so benign; they belong to a highly sophisticated ecosystem dominated by foreign governments, activists and criminal organizations. With systematic efficiency, these criminals and espionage agents transfer vast amounts of wealth, steal information that is vital to economic competitiveness, disrupt social systems and threaten the security of nations.

The legal industry is under attack

Simply put, law firms are being attacked as a matter of "criminal efficiency." Consider a scheme to steal data from a large corporation: Even when a cybercriminal succeeds in the resource-intensive work of breaching that well-defended corporate target, the attacker often has to wade through massive amounts of data in order to find actionable information that will bring a high price in the underground economy.

A similar attack against legal professionals, in contrast, is likely to be faster and easier while offering cybercriminals possible treasure troves of financial data, intellectual property, competitive business strategies, state secrets and sensitive personal identity data. A recent Wall Street Journal article put it this way, describing lawyers as "soft targets in the hunt for insider scoops on mergers, patents, and other deals."

Making law firms even more vulnerable and attractive to cybercriminals, the databases and digital devices they maintain have already been culled and sorted. Thus, they contain only "pre-screened" information that is relevant, timely and valuable.

By targeting lawyers and law firms, then, cybercriminals often "net" a higher ratio of marketable data — and typically without having to overcome the time-consuming and technologically challenging work of breaching better-protected corporate targets.

What's at stake for legal professionals?

For legal professionals, numerous potential dangers arise from failing to adequately address cybersecurity issues. The key elements of this risk are professional, financial, governance and reputational.

At this stage in the evolution of America's digital culture, we expect individuals and organizations to behave responsibly in their online conduct and data-management practices. Where these expectations are not met, stakeholders have proven themselves unforgiving, resulting in customer defections, plummeting stock prices and significant damage to reputations and brands.

Where a cybersecurity breach damages customer relations, competitive position or public reputation, the long-term costs of these incidents can be substantial, indeed.

Professional liability

In its 2012 revisions to the Model Rules of Professional Conduct, the ABA's House of Delegates addressed this issue head-on.

Comment (6) of ABA Model Ethics Rule 1.1 now states:

"To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."

In the ABA Cybersecurity Handbook, the consequences of failing to exercise appropriate care are outlined clearly enough:

"…lawyers and their practices can now be held liable for breaches. Ignorance of the risk is no longer an option or an excuse."

Personal information (PII)

Specific standards apply where legal professionals have possession of Personal Identifiable Information (More commonly now referred to as "Personal Information" (PII) such as Social Security numbers, birth dates and credit card information.) Public policy recognizes privacy rights and the sanctity of inherently sensitive personal information.

Given the increasing incidence of identity theft, some states require that sensitive personal information be encrypted in transmission, and most states have enacted security breach laws.

What are your responsibilities as a legal professional?

Sensitive client information may exist in a lawyer's memory, in his or her briefcase, in a file cabinet or in a number of digital formats and devices. Regardless of where the data is stored, its security is safeguarded by an overriding ethical imperative: confidentiality.

ABA Model Rule 1.6(a) states [a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent." (Note: The Rule does allow for limited exceptions.)

And in subpart (c) the Rule states "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

A key question, then, revolves around what constitutes "reasonable efforts." Whether these efforts are physical (e.g., locking files in a safety deposit box, for example), technical (e.g., maintaining up-to-date antivirus software), or administrative (e.g., enacting strict limitations to data access by non-essential staff), any-and-all such safeguards may be considered as part of a lawyer's responsibilities.

In the Rule's revised comments, guidelines are offered regarding these factors which include (but are not limited to):

"… the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)…"
(Excerpts from Comment 17 of Rule 1.6(c))

The ABA Model Rule 1.1 specifies a lawyer's obligations to provide competent representation. And in the newly amended Comment [6] of this Rule, the ABA offers a clear statement on how "competent representation" encompasses the management of technology:

"To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."
(Comment [6] to ABA Model Rule 1.1)

How can you develop an effective cybersecurity program?

Comprehensive planning

Before you can adequately protect your data, you need a thorough understanding of what kind of data you possess, where it is stored and who has access to it. So auditing is a good first step. Then, determine what digital information requires the highest degree of protection and make it a priority to secure the data immediately.

Once you're confident that your information is securely protected, you can undertake a thorough process to produce a comprehensive plan, from implementation to monitoring to ongoing education.

Risk assessment

Once you've catalogued the data that's in your possession, conduct an assessment of the attendant risks. (Information that is available to many people — or transported via many portable devices — is inherently more vulnerable than data that is held in a central location and accessed by few.) In all likelihood, your assessment also will uncover personal information and corporate data that you neither need nor want but that does puts you at risk of disclosure. By sanitizing your files you can eliminate these unnecessary risks.

Cybersecurity policies & procedures

A key "deliverable" from your security audits and plans will be a framework of policies and procedures to guide your organization's cybersecurity efforts. Make this a "living" document, one that guides your organization towards a unified approach that adapts to meet changes in the threat environment.

Common cybersecurity scenarios

Since the types of data, devices and security risks vary so widely for each organization, any attempt to impose a "one size fits all" plan is destined to disappoint. A more useful exercise is to develop cybersecurity scenarios that are customized to address the needs of your organization and its stakeholders or clients.

Common scenarios include events such as:

- Lost or stolen electronic devices or storage media
- Unauthorized access to sensitive data by disgruntled employees
- Hackers compromise data belonging to customers and clients
- Loss of Personally Identifiable Information (PII) assets

Security factors to consider

To provide guidance to practitioners deciding which security measures to implement, the ABA Cybersecurity Handbook recommends evaluating these factors:

- The probability and criticality of potential risks
- The size, complexity and capabilities of the business
- The nature and scope of the business activities
- The nature and sensitivity of the information to be protected
- The company's technical infrastructure, hardware, and software security capabilities
- The state of the art of technology and security
- The cost of the security measures (cost was the factor mentioned most often, which suggests that businesses are not required to do everything theoretically possible)

THE ABA CYBERSECURITY HANDBOOK

In recognition of the growing challenges that digital information poses for legal professionals, The American Bar Association (ABA) created a Cybersecurity Legal Task Force in 2012.

The resulting ["ABA Cybersecurity Handbook"] was published in July, 2013 — and should be a cornerstone reference for every legal professional information to guide his/her decisions in this arena.

Recommended practices for legal professionals

Conduct annual cybersecurity audits

Annual cybersecurity audits should be required. A robust cybersecurity program is "always on," continuously monitoring the developments of an entity's IT environment. In addition to these constant "blips" on the cybersecurity radar screen, however, there also are "Big Picture" changes that emerge from the information ecosystem. Assessing these new technologies, threat patterns and security needs requires a structured session for analysis, review, planning and budgeting.

Develop backup plans & procedures

Even when a practitioner (or an entire organization) has basic cybersecurity measures (strong passwords, data segregation, encryption, etc.) in place, bad things still can — and will — occur to digital data assets.

Fires start, floodwaters surge and lightning strikes. But even more prevalent than these natural disasters are the disasters caused by humans. These include theft, data corruption and other cybercrimes, as well as the unintentional problems (such as losing a device or accidentally deleting files) that occur in every workforce. In the face of these commonplace problems, even the best-prepared organizations suffer from the loss of digital data.

When sensitive digital data has made its way into criminal hands, you're facing a serious problem. There is no "quick fix" for a cyberattack, and sometimes there is no fix whatsoever — reason enough to invest heavily in protective measures.

But with natural disasters and man-made errors, "data loss" does not always have to translate into "data disaster." In these situations, a comprehensive data-backup program truly is a lifesaver.

Best practices for backing up will vary according to individual and institutional data usage, so there are few simple rules that apply universally. Many individual computer users, however, follow this mandate: One doesn't have a secure backup program unless key data are simultaneously stored in three separate places. (For example: A laptop's hard drive, a database stored "in the cloud," and an external hard-drive stored at a remote location.)

Implement bring your own device (BYOD) controls

In a cost-conscious environment, the prospect of employees bringing their own computer hardware or mobile devices can be a tantalizing way to stretch a limited budget. There's also the "familiarity" factor: When an employee already has invested the necessary time to become familiar with his/her particular device, both productivity and employee satisfaction often rise.

These attractive benefits, however, are dwarfed by the potential cybersecurity risks, including:

- Exposure from mixing personal and business data
- Increased opportunity for losing sensitive data
- Loss of IT "policing standards"
- Introduction of potentially dangerous apps

New products are emerging that create firewall protections that insulate corporate networks from malware on employee phones and prevent the loss of company data. If you are considering allowing employees to use their own digital devices, you'll want to get smart about these Mobile Device Management (MDM) options.

Apply internal document-access practices

Not every data breach is a result of foreign agents or organized criminals. An increasing number of computer security leaks originate from unauthorized access of employees (current or former), vendors and partners.

Curbing these attacks requires well-designed administrative procedures that limit an individual's ability to access data resources outside of their scope of responsibility.

Best practices in this area also include careful management of password credentials and prompt termination of access when an individual no longer is actively involved in a matter or doesn't have a compelling need-to-know.

Keep your anti-virus protection up to date

Once you (or your firm) are aware of cybersecurity risks — and are unwilling to accept the potential consequences of a data breach — you become engaged in an effort that requires commitment and ongoing attention. At a minimum, this program involves the installation of a high-quality anti-virus program — one that is scrupulously kept up-to-date. Consider newer, cloud-based solutions in addition to traditional programs from Norton, Symantec, etc. (It's not an "either-or" situation; security experts recommend using both.)

Update software regularly

Flaws in software code frequently provide opportunities for cybercriminals to gain unauthorized access of computer systems. As software vendors discover such flaws, they issue patches or upgrades to remedy the vulnerabilities.

Unfortunately, there often is a considerable gap between a vendor's release of a software patch and an end user's installation of the repair. During the ensuing days, weeks and months, any organization that has not upgraded its software is vulnerable to easy access by a determined outsider.

Enforce password policies

Law enforcement agencies and cybercrime studies routinely use the word "opportunistic" to describe the patterns of cybercriminals, who typically seek the easiest targets — those organizations that fail to observe basic cybersafety practices. Unfortunately, many legal professionals fail to implement one of the most basic practices of all – the rigorous and consistent use of robust passwords.

Be careful what you put in the cloud

Legal professionals have taken full advantage of cloud-based data storage that allows 24/7 access to case files. Working through the cloud allows mobile workers to synchronize data. As a result, a document that's edited on an iPad (for instance) is immediately available (in its newly revised state) for viewing/editing on an iPhone or personal computer.

All this convenience, however, does come at a price: Storing confidential client materials on servers controlled by someone else. And as the world has learned, some of these remote servers have been accessible to prying eyes.

Drawing on the ethics opinions emanating from state bar associations, lawyers have learned to exercise due diligence before placing sensitive client data in "the cloud." Conducting this "cybersecurity analysis" requires legal professionals to understand the mechanics of cloud-computing, the security practices of the vendor-in-question, the vendor's policies regarding data requests from third parties, and other factors that could impact access to (and protection of) confidential client data.

Educate about social media

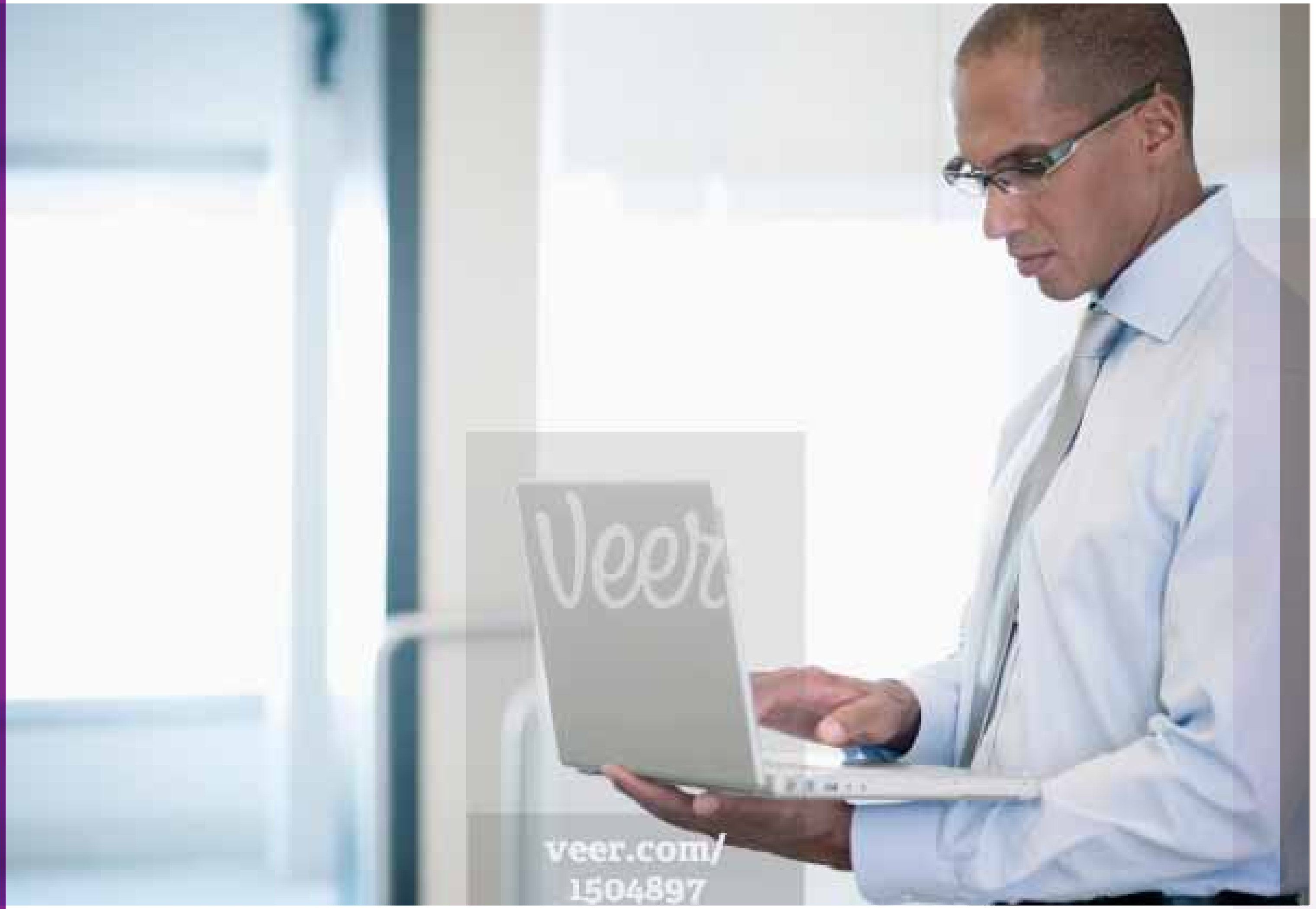
Legal professionals must be considerate about what they post on social media sites. According to security analysts, cybercriminals targeting your firm or department will patch together a mosaic of information that may allow them to craft a convincing "social engineering" attack. These attacks occur when you or one of your employees clicks on a spoofed email link, thinking it came from a legitimate partner. And with that simple "click," a cybercriminal now may have all he needs to begin unlocking your data assets or to make mischief with your operating system.

Protect your employees on the go

The work of legal professionals increasingly is performed away from a headquarters office. And when on-the-go lawyers and paralegals need remote access, they make use of public WiFi access points, which are easy prey to lurking cybercriminals. Make sure that you (and your colleagues) always use an encrypted private network or "hot spot" when working away from the office. Alternatively, protect your transmissions via a Virtual Private Network (VPN).

Encrypt emails

When a legal professional transmits unencrypted data regarding sensitive client information in the body of (or as an attachment to) a standard email, the data enters the stream of public transmission. Since unprotected email is highly susceptible to interception and exposure, a "reasonable expectation of privacy" is not present. (Properly encrypted email, on the other hand, does retain the privacy expectation.) Fortunately, encryption capabilities are readily available. Note that using encryption requires that security is in place on both ends of a transmission, so you may need to educate your clients.



Limit the impact of lost or stolen electronic devices

The loss and theft of mobile computing devices are increasingly prevalent problems for legal professionals. The problem of a lost device escalates exponentially, however, when two factors are present:

1. The device contained sensitive data about a company, client and/or individual.
2. The device's hard drive and data were not encrypted.

The presence of these two compromising elements turns a loss of hardware into a far more serious data breach. Whenever possible, prohibit employees from keeping sensitive data on their portable devices and always insist that portable drives are protected by encryption.

Supervise vendors closely

In 2013 a major retailer, Target Stores, learned the hard way that a business's security can be compromised by the outside vendors it employs. Exercising due diligence in the choice and supervision of IT vendors is a critically important aspect of any comprehensive data-security process — and lawyers are responsible for this essential duty.

While legal professionals cannot single-handedly prevent cybercrime, there is much that can be achieved by understanding the threat of cyberattacks and adopting the cybersecurity best practices discussed in this white paper.

For more information about cybersecurity, or for help implementing best practices in your firm or company, contact your local Special Counsel office or visit specialcounsel.com.