



TOP 10 TECH TIPS

for Corporate Lawyers

TOP

10

TECH

TIPS

for
Corporate
Lawyers

Data breaches and cyber attacks aren't just happening to other companies. They are real, constant threats to every company, brand, and bottom line. It's no longer "if," but "when" you'll get breached. With this heightened focus on security, one of the biggest challenges faced by many in-house counsel is understanding what all the technology means and how to ensure your company is taking the proper actions to protect your company.

Why should corporate lawyers care about technology?

According to the FBI, law firms and law departments are amongst the most vulnerable targets for cyber attacks because of the types of information lawyers manage and access¹—like information about mergers and acquisitions, new product launches, trademarks, patents, and domain names to be filed. *The American Bar Association (ABA) Cybersecurity Handbook*² reports that lawyers are targeted because they have limited resources to dedicate to computer security, lack a sophisticated appreciation of technology risks, and lack an instinct for **cyber security**. It's really worth doing everything possible to protect against cyber threats. The good news is, you can do some simple things that have big impact on your cyber security.

There may also be an ethical obligation for lawyers to know and care about technology. Most lawyers are familiar with the ABA's *Model Rules of Professional Conduct*. Model Rule 1.1 defines competent representation, in part, as requiring the legal knowledge and skill reasonably necessary for representation. In 2012, the ABA added comment 8 to this Model Rule, requiring lawyers to maintain the requisite knowledge and skill, and to keep abreast of changes, including the benefits and risks associated with relevant technology.

CSC® spoke with our associate general counsel and director of Corporate Markets and Privacy, Jennifer Mailander, and chief information security officer, Scott Plichta, to identify the top 10 technology tips for corporate lawyers. These tips can help you become familiar with technology and cyber security so you can provide the guidance needed to help protect your company's business. We've provided general definitions to assist your understanding. The **bolded and italicized** terms throughout the article lead to definitions in the Technology Terms Desk Reference at the end.

1

Understand your company's business and the technology your company uses

First, you need to understand your company's business, and the services or products you provide, so you can fully understand what it is your company does. Closely related to this is an understanding of the technology behind your business and what is done with data that's collected, stored, and shared. For example, does your company have a policy for data classification and storage? What does your policy say about storing data in the cloud? Learn and know the policies for implementing new technology and disposing of old technology. You may even want to become part of the process for buying and maintaining technology, so you can keep tabs on when *shadow IT* is being bought or used.

2

Know your vendors, and your vendor's vendors

Know the vendors your company is using and what services they provide, including who they contract with, to avoid potential liability. If a vendor stores your data, you need your vendor to be as secure as, or more secure than, your company. Determine what type of data they have from your company, how they manage it, and how secure their data management processes and systems are. Depending on the sensitivity of the data, you may want to require your vendor to agree to compliance training, and require they provide proof of security testing on a regular basis. Connect with your Security Team to put a process in place for vetting new vendors, and consider adopting standardized questionnaires like the *Standard Information Gathering (SIG)* or *SIG Lite assessment*.

3

Know your law firm's security practices

Many corporate attorneys forget that law firms are vendors as well. You should know and vet your law firm's security practices just as you do any other vendor's to make sure your information is secure. The Association of Corporate Counsel (ACC) has created a Cybersecurity Work Group in conjunction with the ACC Litigation Committee to help companies identify what questions to ask, and what information to request from firms. In addition, ensure you have a secure mechanism to exchange files. Increasingly, many large law firms either have, or are in the process of attaining, security certification, like *ISO 27001* by the International Organization for Standardization, or other certifications.

4

Be a partner to the business

Learning about technology and how your company uses it, including who it contracts with to provide services, will make you a valuable partner to the business. This knowledge gives you the ability to help the business understand how to identify potential risk, mitigate it, and achieve success. Hold regular "lunch and learns" with Technology, Marketing, Operations, and Sales counterparts to learn how your company works, and stay abreast of potential projects on the horizon. Share information with this cross-functional team about how Contracts and Licensing, Technology, Sales, and Operations intertwine. Technologists often don't understand the legal and privacy implications of using third-party vendors with sensitive data. Educating technology partners about how to mitigate vendor risk through contracts can go a long way. Having a reciprocal meeting to learn what technology the company is implementing can help you to be a better partner to the business—those connections can be key to an ongoing partnership with technology.

5

Conduct a data audit

Again with your cross-functional team, identify your data practices. Generally speaking, who has control of your company's data, what is the nature of the data, where is it stored, who has access to the data, how long is it stored, and where does it go when you are done with it? Depending on the size of your company or the resources at your disposal, you may want to start with reviewing the data practices of one department at a time. For your initial audit, it's okay to keep your analysis at a high level to help you begin to understand the processes you use and determine whether or not you need policies to help ensure better data management. With the decreasing cost of storage, there is little financial incentive to delete or remove data from systems. Explaining the legal, compliance, and breach risk to business counterparts can help the business understand the need for retention policies and aid your compliance efforts.

6

Assess your own individual data practices

Assessing your own individual data practices should be an ongoing security measure that you personally undertake. Where do you store your personal and professional data? Is your home computer secure? Are you secure across desktops, laptops, and mobile devices so that if a personal device was ever lost or stolen, it's **encrypted** and you're sure no confidential data can be extracted? Do you use complex passwords and a **two-factor authentication** system to protect yourself from phishing attacks? Do you keep paper copies of your bills and dispose of them in a secure manner? Do you access your personal bank account from your cell phone and is it secure? How do you manage all of your passwords?

For any data that you truly want to keep secure, you should implement two-factor authentication and not just rely on username/password. Complex and unique passwords are one of the most important things that you can do to protect your data. Consider a reputable password management system protected by two-factor authentication to store your passwords. While you should not reuse passwords between systems, your email password should be unique and the most secure of all passwords—as email is the gateway for most password reset mechanisms on all other accounts.

7

Conduct employee training on technology, security, and privacy

Do it. Ponemon Institute^{®3}, a leading cyber security research firm, has reported that a significant number of data breaches are caused by corporate employees or contractors—whether intentionally or through careless actions. It's paramount that employees are trained routinely on how to recognize cyber attacks like **phishing** or **spear phishing**, and are tested by IT through real-life drills. Phishing attacks work by exploiting a lack of awareness. With the amount of data available on social media, it is possible for cyber criminals to create an authentic-sounding email. We have seen a rise in well-crafted spear phishing attempts. Without appropriate controls, a single click on a malicious link can compromise an entire organization. Responding to this risk goes hand-in-hand with making sure employees know the privacy practices of your company, and regularly educating the workforce on any changes to those policies.

8

Know your company's breach and incident response plan and practice it

Change your corporate mindset around breach: It's not "if" but "when." Know your company's breach/incident response plan. If there is none, consult the cross-functional team and create one together. Having the perspective of Legal, Compliance, IT, Marketing, Human Resources, Operations, and Sales will ensure you cover all the bases. Then practice, practice, and practice that plan, assigning roles and responsibilities to everyone on the team. Conduct incident response drills that draw on real-life examples of how your company's data can be breached. Practice this annually so that you can tweak areas as technology and your business change, allowing you to quickly and efficiently respond to any real crisis. It will never be just as you planned it, but practice helps you prepare for the real event.

9

Get comfortable with technology

Getting comfortable with technology is essential, because technology is everywhere and it continues to evolve. Invest in continued education. Meet regularly with your IT department to share knowledge and ask questions. Get involved in professional associations focused on cyber security, get clarification on things you don't understand, and read up on the latest technologies—through blogs or otherwise—to be aware of how new technology works, and where the potential risks and benefits lie.

10

Network inside and outside your organization

Network inside and outside your company to stay current on best practices regarding technology. Develop a core team of company contacts to assist you when it comes to technology issues. Join your local bar association and talk about technology with your peers outside of your company. Technology, and the laws and regulations governing it, changes very quickly, and you need to stay current on this ever-evolving area of the law.

With cyber attacks on the rise, understanding technology and how to protect your company is an essential part of your job. And we can help you. CSC is the top legal source for global compliance solutions with our Global Subsidiary Management service and Entity Management and Matter Management solutions. CSC is also a trusted partner of the top three—and more than half—of the 100 Best Global Brands as ranked by Interbrand[®], serving an international clientele with our domain management, brand protection, and Internet security services. Visit us at cscglobal.com to learn more about how we can help you.



Getting comfortable with technology is essential, because *technology is everywhere* and it continues to evolve.

To assist with your understanding of technology, here are some essential technology terms with basic definitions, compiled from many sources⁴ and edited by us to make them simple and easy to understand for a non-expert.

Big data: High-volume, high-velocity, and high-variety information that demands cost-effective, innovative forms of information processing for enhanced insight and decision making. These data sets can be so large and complex that traditional data processing applications are inadequate. Challenges include analysis, capture, search, sharing, storage, transfer, visualization, and privacy. Much of the value of big data is finding use in large amounts of data that might not be the purpose for which it was collected. Big data projects should be carefully evaluated against your company's stated privacy policy.

Cyber security: Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.

Cloud hosting and computing: A type of Internet-based computing in which different services such as servers, storage, and applications are delivered to an organization's computers and devices through the Internet. Examples of cloud computing include:

- » **Infrastructure as a Service (IaaS):** A service model that delivers computer infrastructure on an outsourced basis to support enterprise operations. Typically, IaaS provides hardware, storage, servers, and data center space or network components, and the customer will run their own software and services.
- » **Platform as a Service (PaaS):** A category of cloud computing services that provides a platform allowing customers to develop, run, and manage web applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an application.
- » **Software as a Service (SaaS):** A software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

Encryption: The conversion of electronic data into another form called ciphertext, so that it cannot be easily understood by anyone except authorized parties with the key to decipher. Types of encrypted data include:

- » **Data in Use:** Active data under constant change stored physically in the computer's memory while being changed by a program such as a word processor or spreadsheet.
- » **Data at Rest:** Inactive data physically stored in databases, data warehouses, spreadsheets, archives, tapes, or off-site backups.
- » **Data in Motion:** Data that is traversing a network or temporarily residing in computer memory to be read or updated.

Hosting (website hosting or web hosting): The business of housing, serving, and maintaining files for one or more websites.

Information security: Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide:

- » **Integrity:** Guarding against improper information modification or destruction; includes ensuring information nonrepudiation and authenticity.
- » **Confidentiality:** Preserving authorized restrictions on access and disclosure.
- » **Availability:** Ensuring timely and reliable access to and use of information.

Information security program: The program to identify threats, vulnerabilities, and requirements to implement security controls, and monitor.



For more than a century, successful law firms have relied on **CSC** to support their clients' many corporate filing, formation, and transactional needs. Whether you manage one or a thousand entities on your clients' behalf, we have the tools and expertise to keep them on track. Our services include:

- Annual reports
- Apostille, authentication, and legalization
- Articles of amendment
- Certificates of good standing
- Corporate domain name management
- Cyber security
- Dissolutions or withdrawals
- Document retrieval
- Doing business as (DBA) filings
- Foreign qualification
- Formations
- Global trademark services
- Mergers
- New gTLDs
- Online brand protection
- Registered Agent
- SSL certificates
- UCC searches, filings, and portfolio management

cscglobal.com/concierge

Copyright ©2017 Corporation Service Company. All Rights Reserved.

CSC is a service company and does not provide legal or financial advice. The materials here are presented for informational purposes only. Consult with your legal or financial advisor to determine how this information applies to you.