Ballard Spahr LLP

Overview of the Association of Corporate Counsel Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information

By David M. Stauss, Edward J. McAndrew, Gregory P. Szewczyk, and J. Matthew Thornton

INTRODUCTION

The Association of Corporate Counsel (ACC) has published its *Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information (Model Controls)*. The Model Controls are intended to "serve as a benchmark for law firm cybersecurity practices" and "to help in-house counsel as they set expectations with their outside vendors, including outside counsel, regarding the types of data security controls these vendors should employ to protect their company's confidential information." This memorandum summarizes some of the primary controls.

OVERVIEW

The Model Controls cover thirteen areas:

- data security policies and procedures
- retention and return/destruction of client confidential information
- data handling
- physical security measures
- logical access controls
- monitoring
- vulnerability controls and risk assessments
- system administration and network security
- security review rights
- industry certification/additional security requirements
- background screening
- cyber liability insurance
- subcontractors

Although described as a "baseline," the Model Controls are fairly comprehensive. Therefore, each organization should consider which individual controls are relevant to protecting the confidential information it shares with outside counsel. For example, your organization may decide that counsel working on intellectual property matters should comply with all of the controls, whereas counsel working on a routine breach of contract case may only need to implement certain ones. Some of the factors that organizations may wish to consider in deciding whether and which controls to adopt include: organizational size, scope of operations, types of data shared with outside counsel, types of legal services performed, legal budget, cyber threat risk landscape, and cybersecurity maturity.

Organizations also may wish to consider certain implications of adopting the Model Controls. Compliance costs are a good example. Although law firms may already comply with some of the controls, the cost to implement others could run into the tens of thousands of dollars. That high compliance cost may impact the number and types of firms that are available to provide legal services to your organization. Another important consideration is whether the organization meets or exceeds

any information security standard to which it will hold its outside counsel. The standard you set for your outside counsel should be consistent with your own policies and procedures. If your organization suffers a cyber incident and is sued, you do not want to find yourself in a position of not meeting the standard of care you selected for your outside counsel.

DISCUSSION OF SPECIFIC PROVISIONS

Definition of "Company Confidential Information"

The Model Controls adopt a very broad definition of "Company Confidential Information" (CCI). It includes not only information that your company may already consider confidential, such as protected health information, Social Security numbers, and account numbers, but also a person's name, IP address, email address, postal address, telephone number, information that is attorney-client privileged, and information that could damage the interests of the company, among other types of information. Although not expressly listed, intellectual property would be subsumed within other categories. It also has a catchall provision for "information that is legally required to be protected under the laws applicable to the company data."

Policies and Procedures

The Policies and Procedures section of the Model Controls requires outside counsel to implement "appropriate organizational and technical measures to protect Company Confidential Information." It identifies a number of policies that must be implemented, including a security policy, organization of information security, human resources security, access control, personnel training, and business continuity management, among others. Although the terminology for these policies may differ from company to company, these policies are directed at ensuring that outside counsel have basic information security policies in place. The Model Controls also require that outside counsel have an incident response plan that is reviewed at least annually.

Finally, this provision requires outside counsel to have resource and management oversight to ensure information security and specifically requires that counsel train its employees on information security.

Retention and Return/Destruction

The Retention and Return/Destruction section requires outside counsel to: (1) retain CCI only for as long as dictated by the client; (2) return, delete, or destroy the information unless it falls into an exception (*e.g.*, day-to-day exchange of emails); and (3) certify that the information has been returned, deleted, or destroyed within 30 days of the company's request.

These provisions are consistent with recommendations such as those in the FTC's *Start with Security, A Guide for Business*, which advises companies to "hold onto information only as long as you have a legitimate business need." The underlying rationale for such provisions is that a company cannot lose something it does not have.

Data Handling

The first four provisions of the Data Handling section deal with encrypting CCI. Encryption is the process whereby information is rendered unreadable and only can be accessed with an encryption key. For data security purposes, encryption is a silver bullet that, under many laws, may exempt a company from certain notification requirements should the company lose protected information. In this context, the Model Controls seek to address how CCI should be securely transmitted to and from the company and its outside counsel, and how outside counsel should securely store that information on counsel's network, computers, and portable storage devices.

The first provision leaves it to the company to decide whether to encrypt CCI when transferring the information between the company and outside counsel and in communications between the company and outside counsel.

The second provision requires outside counsel to encrypt all CCI while it is "at rest." This provision envisions outside counsel (or its subcontractors) saving confidential information to a network or server in an encrypted format that can only be accessed with an encryption key. Notably, a comment to this provision states that encryption at rest is only "highly recommended" and that law firms may use other procedures to secure the information properly.

What the comment is alluding to is that encrypting all CCI at rest is likely to be very difficult to implement. Prior to requiring outside counsel to implement this control, you should consider whether the control is necessary as to all shared data or just certain types of more sensitive information. You also might consider whether its security objective can be accomplished by network and device segmentation or compartmentalization of more sensitive data. A useful benchmark to consider is whether your company encrypts the information while it is at rest or whether it relies on the same security provisions used by outside counsel.

The third and fourth provisions deal with outside counsel encrypting CCI when it is stored on portable devices (*e.g.*, thumb drives or CDs) or when it is being transmitted electronically. For example, services such as FileShare or Proof Point transfer information securely through email. Importantly, the fourth provision recommends multi-factor authentication for remote connections to networks via mobile device, tablet or laptop.

Although not specifically stated in these sections, the organization may consider what measures outside counsel should take if and when counsel produces CCI to third parties, such as opposing counsel in litigation. For example, you may wish to consider requiring outside counsel to produce confidential information to opposing counsel only if it is encrypted. You also should consider whether the protective orders that your outside counsel are using contain data security provisions that obligate opposing counsel to protect your confidential information in the same manner as the Model Controls.

The data handling provisions also require outside counsel to notify your company within 24 hours of discovering an actual or suspected "Data Security Breach," which is expressly defined as "any suspected or actual unauthorized disclosure, loss, or theft of Company Confidential Information." Outside counsel also must designate a single point of contact who "shall be accessible on a 24/7 basis," and must cooperate fully with the company's investigation, including making any required notifications and "identify[ing] a root cause and remediat[ing] any Data Security Breach at their sole cost." The Model Controls do not specify what costs are covered by the language "at their sole cost." However, given that the Model Controls later state that the company should be an additional insured on outside counsel's cyber insurance policy, a reasonable conclusion is that outside counsel is responsible for covering all costs associated with the investigation and remediation.

Physical Security Measures

The Physical Security Measures section identifies 12 physical security measures for law firms to implement if they "host Company Confidential Information on [their] systems and servers." For example, outside counsel should disable access of separating personnel and should use picture badges, 24/7 security guards at the facility, CCTV surveillance, enhanced restrictions for computer rooms, and visitor logs.

The basic purpose of these controls is to ensure that someone does not walk into counsel's office and steal your company's CCI. However, as with some of the other provisions, prior to wholesale adoption of these controls, it would be useful to review them in light of your company's policies to protect that same information and consider whether the information being provided to outside counsel is of such sensitivity that the controls are reasonable or necessary.

Logical Access Controls

The Logical Access Controls section sets forth a number of provisions for controlling electronic access to CCI, such as defined authority levels (*i.e.*, restrictions on who can access the information on outside counsel's network), unique IDs and passwords, and two-factor or stronger authentication for remote access to counsel's system. Two-factor or stronger authentication means requiring at least two out of three credentials to gain access. These can include something you know (*e.g.*, a password); something you have (such as a randomly generated code delivered to a fob or mobile device); or something you are (such as a biometric measure).

Among other things, this section also states that outside counsel will disable an account after, at most, 10 consecutive invalid log-in attempts. The purpose of that provision is to prohibit "brute force" attacks whereby attackers use programs that crack passwords through repetitive guessing.

Monitoring

The Monitoring section provides that, "unless prohibited by applicable law," outside counsel must "continuously monitor its networks and employees, subcontractors, and contingent workers for malicious activity and activity that may cause damage or vulnerability to Company Confidential Information." Although important to cybersecurity programs, continuous monitoring also implicates user privacy interests and must be undertaken with these competing concerns in mind.

Vulnerability Controls and Risk Assessments

The Vulnerability Controls and Risk Assessments section requires, among other things, that outside counsel perform vulnerability tests and assessments—including manual penetration testing and code reviews—at least annually on systems that contain CCI. The purpose of those measures is to ensure that outside counsel's network is secure from external threats and free of known vulnerabilities. Testing of this nature is typically performed by third-party vendors and can be a significant expense.

System Administration and Network Security

The System Administration and Network Security section requires outside counsel to have industry standard safeguards in place on its system. The purpose of these controls is to ensure that outside counsel's system is secure from external threats.

The section also requires implementation of protections such as using and regularly updating antivirus software, using firewalls (*i.e.*, restricting access to outside counsel's system or within counsel's system), and intrusion detection and prevention systems (*i.e.*, looking for and protecting against hacking). Many larger law firms will already have these protections in place, but smaller firms may not.

Security Review Rights

The Security Review Rights section allows the company and its vendors to access outside counsel's facilities, books, systems, data, practices, and procedures to ensure that counsel complies with their obligations.

Industry Certification/Additional Security Requirements

The Industry Certification/Additional Security Requirements section provides that the company can require counsel to become ISO 27001 certified and to implement additional requirements requested by the company. The comment to this section states that it is "recommended but optional."

ISO 27001 is a specification for an information security management system. It is a framework of policies and procedures that include all legal, physical, and technical controls in an organization's information risk management processes.

The specification includes details for documentation, management responsibility, internal audits, continual improvement, and corrective and preventive action. For a further discussion, *see* Philip Yannella, Partner, Ballard Spahr, *Law Firms are Seeking Data Security Certification* (Bloomberg Law), August 19, 2016. It is important to note that no certification provides a guarantee that an organization is not vulnerable to or currently experiencing a cyber incident. At most, it certifies that a robust cyber risk management program is in place.

Becoming ISO 27001 certified is a lengthy and expensive process for law firms to undertake. Because of that, requiring your outside counsel to be ISO 27001 certified may ultimately restrict your selection of outside counsel.

Background Screening of Outside Counsel Employees, Subcontractors, and Contingent Workers

This section requires outside counsel to conduct background screening on all individuals who come into contact with CCI. Outside counsel must certify, on an annual basis, that those individuals have passed the screening.

Cyber Liability Insurance

This Cyber Liability Insurance section requires outside counsel to maintain a minimum of $10 million in cyber liability insurance and to list the company as an additional insured on the policy. The Model Controls do not explain why $10 million was selected as the appropriate coverage amount.

In considering this provision, one issue to contemplate is how much cyber liability coverage your company has secured and how to value the risk to CCI that you provide to outside counsel. For example, consider whether the CCI outside counsel possesses includes personally identifiable information, personal health information, or intellectual property. The key question is whether requiring $10 million in coverage is commensurate with the risk associated with outside counsel's access to your company's confidential information. It is also worth considering whether a $10 million policy is appropriate given the security controls required under the Model Controls.

Subcontractors

The Subcontractors section requires outside counsel to be responsible for all subcontractors it uses and to ensure that any contractor receiving CCI is contractually obligated to follow the Model Controls.

Conclusion

The Model Controls are a significant step forward in providing in-house counsel with a "streamlined and consistent approach" to data security practices for outside counsel. Like everything else in cybersecurity, though, they are not a one-size-fits-all checklist to eliminating cyber threats. As they do in all other areas of practice, in-house counsel should engage in a deliberate process of identifying which controls are necessary for each different relationship and representation.

If you would like additional information on the Model Controls, please feel free to contact the authors at **David M. Stauss** (staussd@ballardspahr.com); **Edward J. McAndrew** (mcandrewe@ballardspahr.com); **Gregory P. Szewczyk** (szewczykg@ballardspahr.com); and **J. Matthew Thornton** (thorntonj@ballardspahr.com).