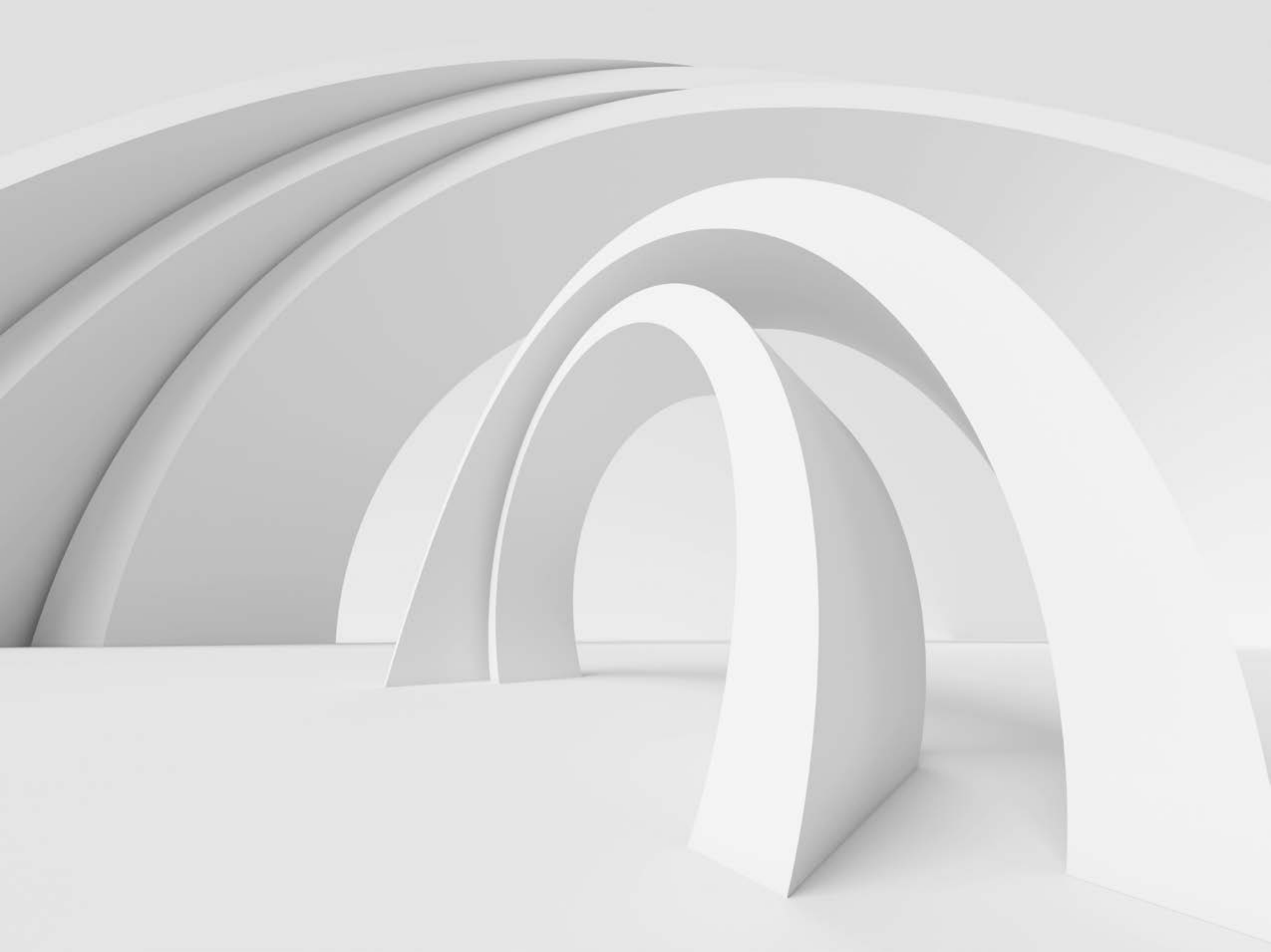
MANAGED TECHNOLOGY SERVICES

an HBR Consulting solution



A Six-Step Checklist for Building a Law Firm Data Security Plan

An Ethical Duty of Competence

The practice of law in America has always been rooted in a strong sense of ethical conduct. From the required curriculum in law school, to the oaths that lawyers take to join the Bar, and then on to continuing legal education requirements for all lawyers, ethics are the bedrock of the legal profession. When it comes to the collection and maintenance of client data, law firms have historically been bound by that same commitment to ethical conduct and have been able to assure clients that their files were safe in their offices. But the sobering truth is that it has never been harder for firms to secure their clients' data.

As we have witnessed in the past few years – most recently in the "Paradise Papers" data security breach[1] – hackers are targeting law firms specifically to get their hands on their clients' confidential data. Malicious individuals, organizations and even nation-states have compromised law firm information networks. Extraordinary lengths will be taken to hack an firm's network, compromise their security systems and access the information the firm has worked hard to protect. A number of law firms have been so overwhelmed by this data security threat they have essentially been paralyzed by the sheer scope of the problem, a reaction that is understandable considering they are in the business of practicing law, not cybersecurity. However, law firms do not have the luxury of taking their time to map out the perfect plan for data security. They need to revisit their data security protocols[2] and make sure their plans include a few key ingredients, working under the assumption that hackers are plotting how to attack the firm's network.

Indeed, the importance of a smart data security plan extends beyond mere best practices for law firms. A growing number of states (currently 27) have adopted the "duty of technology competence" standard that requires firms to be on top of these matters. In addition, in May 2017, the American Bar Association (ABA) issued a new ethics opinion -- Formal Opinion 477[3] – that clarifies the need to take additional security precautions such as data encryption and due diligence on third-party vendors that are engaged by the firm.

Building a Data Security Program

The first thing your firm should do is take stock of the unique security challenges you face in your areas of practice and / or geographic location in order to better determine what data you are required to protect for regulatory reasons,[4] evaluate how much risk is too much for the firm to bear and establish which parts of your network are most exposed to that risk. Develop plans to mitigate if those risks are outside the tolerance you have identified for loss or operational impact. Information and compliance risks are part of the risks associated with running any business. Loss of sensitive data or a breach is not just a security risk – it has strategic, operational, financial and reputational implications.

Once the assessment is conducted, leverage this six-step checklist for building a law firm data security program:

1. Create written policies, based on standards like ISO 27002, and secure buy-in from your executive team so these policies are reinforced. Schedule regular training sessions for anyone in the firm who is involved with data management to maximize security awareness among your employees.

2. Inventory your information systems and maintain a detailed record of what the firm has in its purview and where all of the controls / permissions are located.

3. Implement access controls on a "need to know" basis so that employees only have credentials to get into the files that relate to their job functions. Then, segment your systems so that specific IT pieces that do not need to be connected to highly sensitive client data are not inadvertently connected.

4. Keep your systems up-to-date with the most recent software patches, including antivirus software. It is crucial to keep your firm's IT armor updated to reduce the attack surface available to criminal hackers.

5. Conduct annual third-party risk assessments to validate your vendors. Make sure to establish managed services agreements that cover security and privacy expectations and regularly assess your vendors' security protocols to determine what specific data you will allow them to process, access or host.

6. Have an incident response plan in place so the firm is "breach-ready" on a 24/7/365 basis in case of a cyberattack. Also, check your liability / cybersecurity insurance policies on an annual basis so that your policy coverages remain comprehensive and adequate for the firm's risk exposure.

Looking Forward

Successful law firms are committed to a strong sense of ethical conduct with how they treat client data, so it is essential to understand that you may have enemies prowling around your networks, looking for a way to get their hands on that valuable information. Take swift and decisive action now to review and, if necessary, rebuild your firm's data security plan so you have the best possible defense in place against cyberattacks.

Connect With An Expert

Nate Evans, Senior Pre-Sales Architect
919.924.0554 | Nate.Evans@hbrmts.com

References

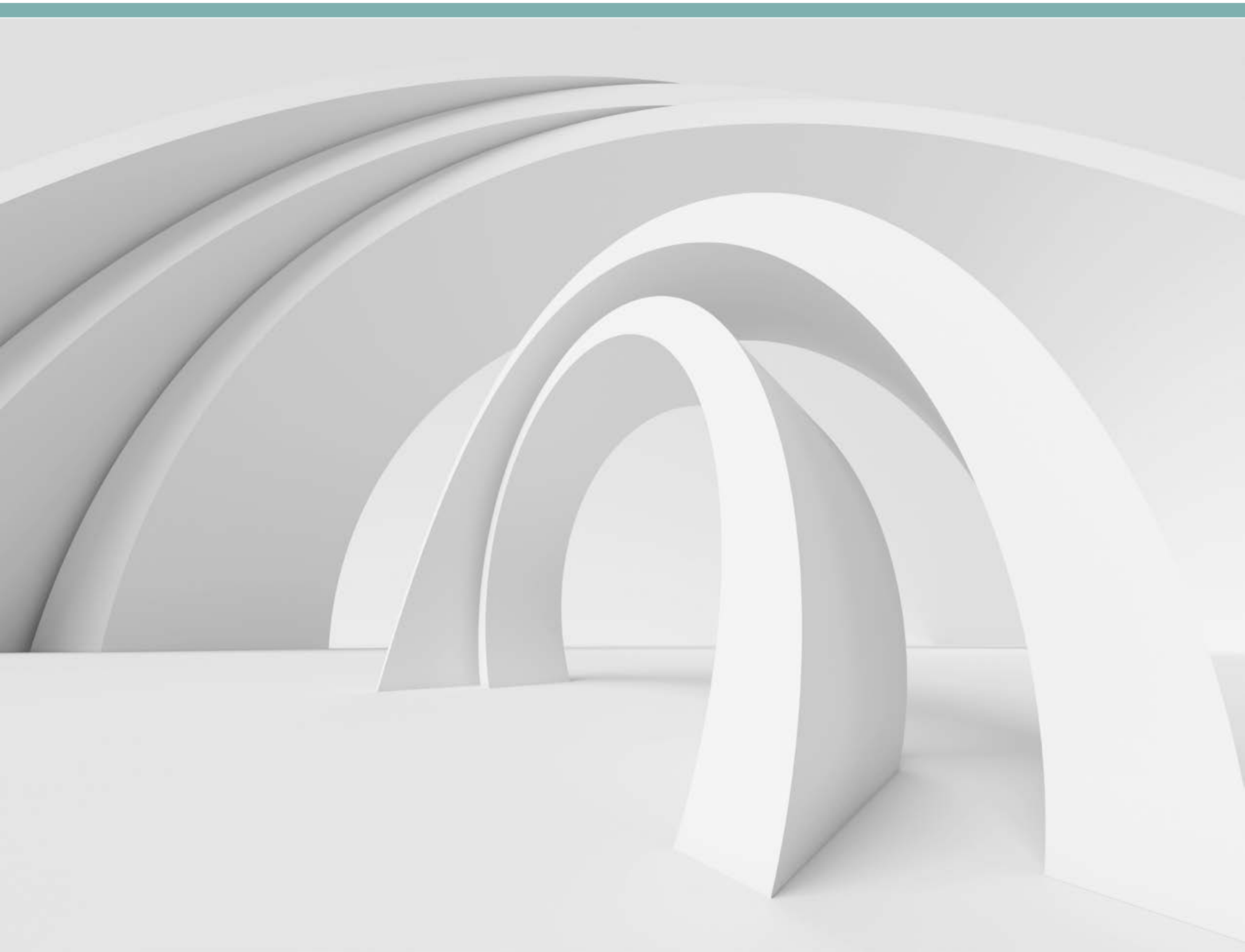
[1] “How Law Firms Are Failing To Keep Clients' Data Safe,” Coe, Aebra. Law360. October 25, 2017. https://www.law360.com/articles/978111/how-law-firms-are-failing-to-keep-clients-data-safe

[2] “Security,” Managed Technology Services LLC. http://www.hbrlegalmts.com/service/security/

[3] “Formal Opinion 477,” American Bar Association. May 4, 2017. https://www.americanbar.org/content/dam/aba/images/abanews/FormalOpinion477.pdf

[4] “When And How Cos. Should Address Cyber Legal Compliance,” Lexology. October 24, 2017. https://www.lexology.com/library/detail.aspx?g=fac660c9-815b-431f-aa62-a35cf4dfa7ee

MANAGED TECHNOLOGY SERVICES
an HBR Consulting solution



Managed Technology Services LLC (MTS) is a trusted data-hosting service provider to the legal industry. A leader in infrastructure and cloud hosting services, we maintain data and applications with the highest level of security standards. For over a decade, our team of MTS experts have collaborated with clients – including 25 percent of the Am Law 100 – to manage infrastructure, systems performance, cost and risk.