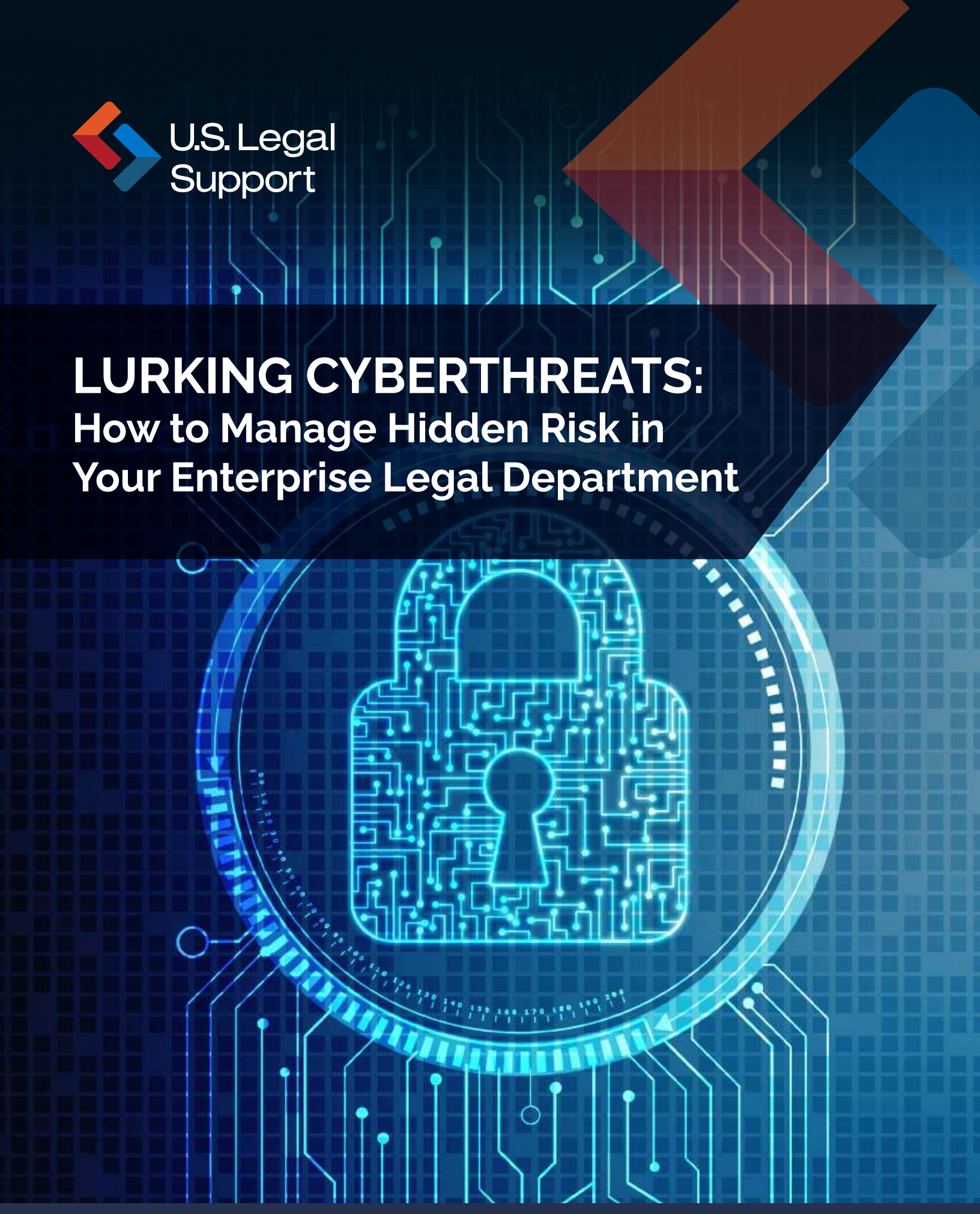
U.S. Legal Support

LURKING CYBERTHREATS:
How to Manage Hidden Risk in Your Enterprise Legal Department



U.S. Legal Support

INTRODUCTION

The quote that a chain is only as strong as its weakest link may have been coined centuries ago, but it aptly describes contemporary cybersecurity strategy.

While the vast majority of large organizations have put robust policies, procedures, and technologies in place to shore up enterprise-wide defenses against malware, phishing attacks, ransomware, SQL injections, and a host of constantly evolving cyberthreats, they also recognize that risk exposure doesn't begin and end within internal business units. To further protect against data breaches, most also routinely and thoroughly vet external vendors up and down the supply chain to ensure each provider deploys appropriate safeguards as well.

Despite strengthening security across and beyond the enterprise, many companies overlook a critical vulnerability with surprising frequency – the risk presented by the third and fourth parties engaged by enterprise legal departments.

WHY IS THE LEGAL DEPARTMENT A CYBERSECURITY RISK?

Responsibility for vetting outside vendors used by internal business units generally falls within the purview of corporate IT teams and procurement departments. Most often, when onboarding a new vendor, the IT team typically completes Standardized Information Gathering (SIG), confirms compliance with data security certifications, and reviews the vendor technology for security vulnerabilities; then the procurement team conducts a vendor risk analysis.

However, in nearly all organizations, legal departments are the exception to the rule. Typically, the decision of which outside counsel to partner with is outside the scope of corporate procurement departments, instead relying on the same relationship-based approach the legal department has used for decades. That is not to say that legal departments assume the law firms they outsource have their own cybersecurity controls in place. Most often, there are rigorous Data Protection Agreements in place; but these do not effectively manage the risk of a fourth-party data breach.

Unfortunately, this approach no longer works in 2022, as cybercriminals have increasingly set their sights on the legal industry. Considered tantalizingly lucrative due to the sensitive nature of the work they handle, law firms have become prime targets for cybercriminals ready to move beyond the Fortune 500 to hack mid-size businesses and professional services providers. Fully 100% of the law firms in a global sample analyzed by BlueVoyant Cyber Security Firm had been targeted in attacks, and of those surveyed, 15% experienced compromised networks.[1]

1. https://www.bluevoyant.com/news/bluevoyant-sector-17-press-release/

Simply put, businesses can no longer afford to overlook the security risks posed by this all-too-common practice. Here's why:

The "fingers-crossed" approach doesn't work.

A Ponemon Institute survey found that reliance on reputation is the most common reason organizations do not evaluate the privacy and security practices of third parties. Yet more than half of organizations surveyed experienced a data breach caused by a third party.[2]

Without the oversight and involvement of the enterprise procurement and IT teams in legal department outsourcing, intensive cybersecurity risk assessment of outside counsel is rare, exposing the entire enterprise to potential compromise.

To make matters worse, law firms often lack comprehensive cybersecurity preparedness. The 2021 ABA Cybersecurity Tech Report found that only half of law firms encrypt files and only 53% reported using intrusion detection and prevention systems.[3]

Fourth-party partners exacerbate data breach risk.

Cybersecurity risk is further heightened when outside counsel engages multiple partners to support their business – vendors for court reporting, record retrieval, transcription, and other litigation support services. Enterprise legal departments have zero visibility into the data protection policies of these fourth-party vendors, assuming they even know who they are.

For example, a recent audit of outside counsel by a large national insurance company revealed the law firm it retained used over one thousand different court reporting services. When one thousand companies – and multiple employees at each – have access to confidential deposition data residing on unsecured, unmanaged, un-inventoried devices or cloud services, it's probably an understatement to say that the risk of a data breach skyrockets.

The consequences can be dire.

By nature, outside counsel deals with highly-sensitive, confidential, contentious litigation. Often, it seems, the prevailing attitude of enterprise legal departments is that the law firms they retain are responsible for protecting all information shared by or relating to the enterprise. But if a data breach exposes information intended or required to stay private, this presumption of responsibility does absolutely nothing to negate the devastating reputational damage to the enterprise that can result.

Data breaches seriously erode customer trust and loyalty as well as brand value, despite consumer skepticism about data safeguards. Nearly 70% of consumers surveyed by PwC believe that the companies they use are vulnerable to hacking and cybercriminal attacks, with 87% willing to walk away and take their business with them in the case of a data breach.[4]

The financial costs of data breaches can also be enormous – and sustained. In 2021, the average ransomware payment was close to $221,000[5], and the average cost of a data breach per incident skyrocketed to a record high $4.24 million.[6]

In addition, stock prices can plummet both in the short term and over the long run when a breach occurs. As an example, CapitalOne share prices dropped 6% following a data breach in 2019, and other companies have experienced a market value decline of 25% during the year after an attack.[7]

2. https://www.securitymagazine.com/articles/95143-of-organizations-have-experienced-a-data-breach-caused-by-a-third-party
3. https://www.americanbar.org/groups/law_practice/publications/techreport/2021/cybersecurity/
4. https://www.securelink.com/blog/reputation-risks-how-cyberattacks-affect-consumer-perception/#:~:text=PricewaterhouseCoopers%20(PwC)%2C%20an%20audit,and%20attacked%20by%20cyber%20criminals
5. https://www.ohiobar.org/member-tools-benefits/practice-resources/practice-library-search/practice-library/section-newsletters/2021/small-and-midsized-law-firms-slammed-by-ransomware/
6. https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic
7. https://www.aon.com/unitedkingdom/insights/reputational-damage-and-cyber-risk.jsp

HOW CAN YOU REIN IN THIRD- AND FOURTH-PARTY RISK?

Clearly, there's good reason that Chief Legal Officers (CLO) rank cybersecurity and data privacy among the top three issues most important to their business.[8] Extending those security concerns to third and fourth parties is more important than ever as outsourcing volume continues to grow. 41% of CLOs surveyed anticipate sending more work to law firms this year, and 24% expect to increase the amount of work outsourced to other legal service providers.[9]

The good news is that there are highly effective ways to mitigate this risk for companies willing to make doing so a priority. Here's how:

#1.

DEVELOP A SET OF CYBERSECURITY AND DATA PRIVACY BEST PRACTICES FOR YOUR CLO TO SHARE WITH ALL OUTSIDE COUNSEL.

The 2021 ABA Cybersecurity Tech Report found that clients are focusing more on the cybersecurity programs and policies of the law firms representing them and are more frequently using security requirements documents, questionnaires, and guidelines to enforce standards. However, security preparedness may still fall short, considering that barely one-quarter of law firms reported they had undergone a full security assessment by an independent third party.[10]

In addition to assessing security preparedness, other best practices for law firms include implementing technology—and data—related security policies, training employees on security awareness, and developing an incident response plan. Law firms should also deploy a broad spectrum of security tools, including multi-factor authentication, encryption, firewalls, and intrusion detection and prevention systems.

#2.

SET REQUIREMENTS.

Enterprise legal departments with higher risk should begin requiring their outside counsel to use providers that have been vetted by the organization. A good start would be for legal organizations to begin using a modified version of the contract that requires outside counsel to engage only those vendors that meet enterprise security standards. Entrusting vetting to the outside counsel provides law firms greater flexibility but also forces your company to relinquish some control over security protocols.

#3.

CONDUCT A THOROUGH RISK ANALYSIS OF ALL VENDORS (BOTH THIRD AND FOURTH PARTY).

Partnering with a vulnerable legal services provider can quickly compromise a law firm's carefully executed cybersecurity strategy, putting sensitive client data at risk. If not using a provider pre-approved by the enterprise legal department, outside counsel should conduct their own risk analysis.

Key questions to ask as part of this process include:

- Do all transmitted files have end-to-end encryption to protect data from being read or modified by unauthorized parties?
- Do you follow an established cybersecurity framework such as National Institute of Standards and Technology (NIST), Center for Internet Security (CIS), or International Organization for Standardization (ISO)?
- Do you maintain redundant datacenters to support uninterrupted data availability?
- Do you have a 24/7 Network & Security Operations Center to prevent and detect malicious activity?
- Has an independent auditor verified SOC 2 Type 2 compliance with best-in-class procedures, safeguards, and technologies to safeguard data? What about HIPAA compliance to ensure the integrity of all protected health information?
- Do you conduct third-party penetration testing?
- Do you have an incident response plan? And a disaster recovery plan?

8. ACC-CLOreport22_Final2%20(1).pdf
9. ACC-CLOreport22_Final2%20(1).pdf
10. https://www.americanbar.org/groups/law_practice/publications/techreport/2021/cybersecurity

GOODBYE HIDDEN RISK, HELLO PEACE OF MIND

With cyberthreats growing more pervasive, you need to escalate cybersecurity vigilance to protect sensitive data within your enterprise and beyond. Ignoring weak links can imperil even the most robust defenses. This makes it imperative organizations ensure that every single external partner and provider – even those hired by your legal department – along with every single partner and provider engaged by outside counsel and other third parties, meets your rigorous security and data privacy requirements.

Act now to close the gaps in your cybersecurity strategy. Your reputation, customer loyalty, and bottom line could depend on it.

ABOUT U.S. LEGAL SUPPORT

U.S. Legal Support was founded in 1996 with the goal of becoming the first nationwide, all-inclusive litigation support company. Nearly three decades later, we're one of the leading providers of litigation support services and the only company to provide a full suite of court reporting solutions, record retrieval, interpreting & translations, trial services and transcription services to law firms, major corporations, and insurance companies nationwide. With on-demand access to 12,000+ offices in 2,700 cities across the country and a robust digital infrastructure, we can accommodate your litigation support needs quickly, comfortably, and safely from anywhere in the country. For more information about U.S. Legal Support, visit the company's website at: www.uslegalsupport.com.