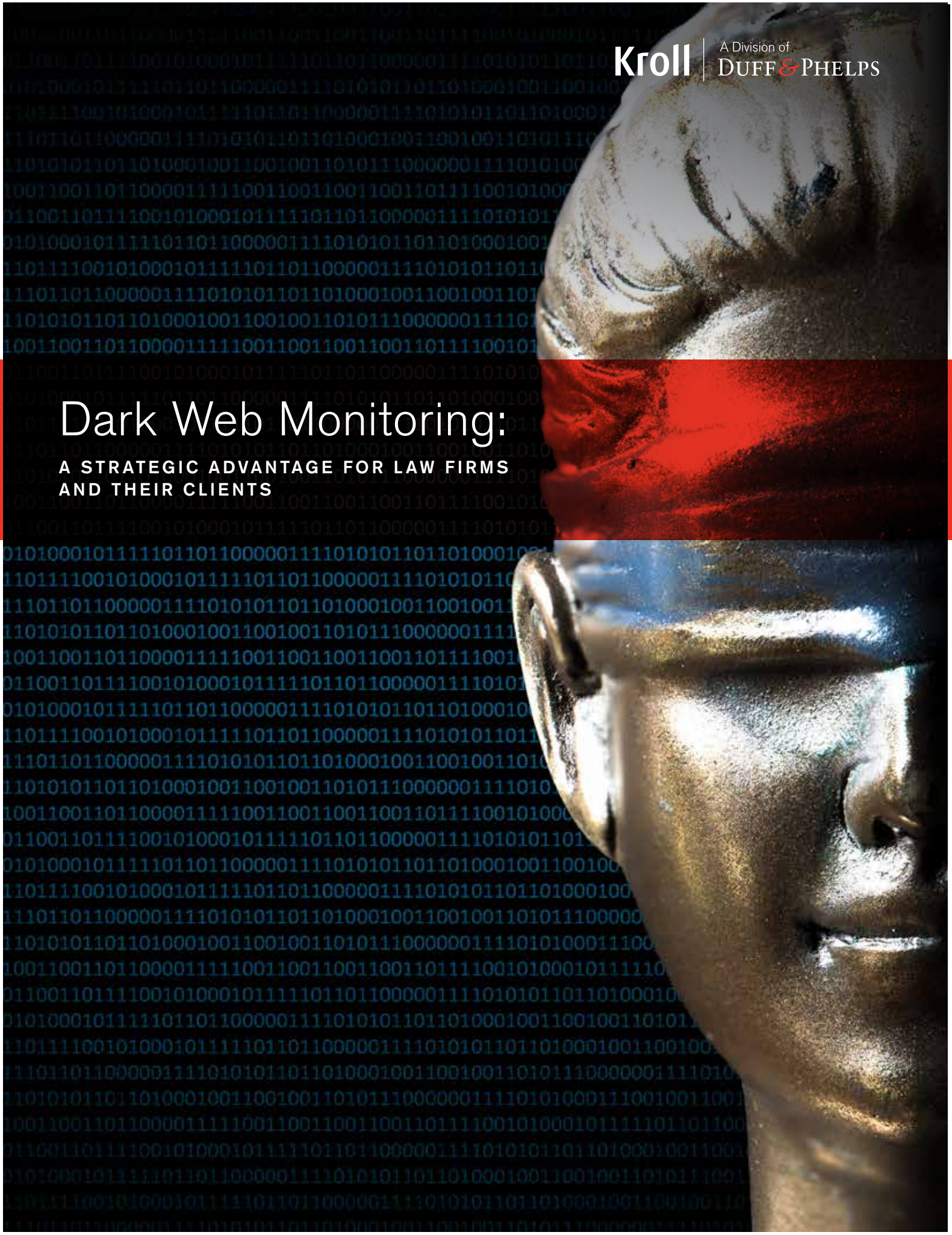
Kroll | A Division of DUFF & PHELPS

Dark Web Monitoring:

A STRATEGIC ADVANTAGE FOR LAW FIRMS AND THEIR CLIENTS



In a law firm's role as strategic advisor to its clients, the ability to gather, analyze and protect information is critical. Firms that can excel in their handling of information are thus likely to enjoy an advantage at a time when even the top of the legal marketplace is experiencing sustained competition and commoditization pressures.

One way that firms can raise the sophistication of their approach to information is by including *dark web monitoring* in their research and due diligence arsenal. Dark web monitoring allows firms to see what sensitive information may have made its way onto the thriving global underground marketplace where cybercriminals buy and sell exposed data. But while dark web monitoring offers an important measure of the quality of a law firm's cybersecurity, it is an even more powerful *strategic* tool that can help lawyers advise clients on a wide range of legal and business matters.

Consider the amount of sensitive information that exists across the myriad relationships formed by the firm, its clients and the parties those clients interact with—adversaries in legal matters, potential joint venture partners, acquisition targets and so on (see Figure 1). Some of this information, like employee login credentials and board minutes, is internal to each party, and some, like terms sheets and strategic plans, may be confidentially shared between parties. In either case, the inadvertent exposure of that sensitive information can have significant negative effects on the party or parties involved, including decreasing the value of assets or potential strategic moves, reputational damage and signaling out the entities for further cyberattacks.

Unfortunately, such inadvertent exposure can occur in a number of ways, including direct attacks by cybercriminals, infiltration through a trusted vendor whose system has been compromised or an employee working remotely over an insufficiently secure network. Once that information has been exposed, whether through human error, theft or misdirection, it is at risk of being bought and sold on the dark web. As organizations and individuals become more digitally interconnected at work and at home, the possibilities for these negative outcomes are growing and will continue to do so.

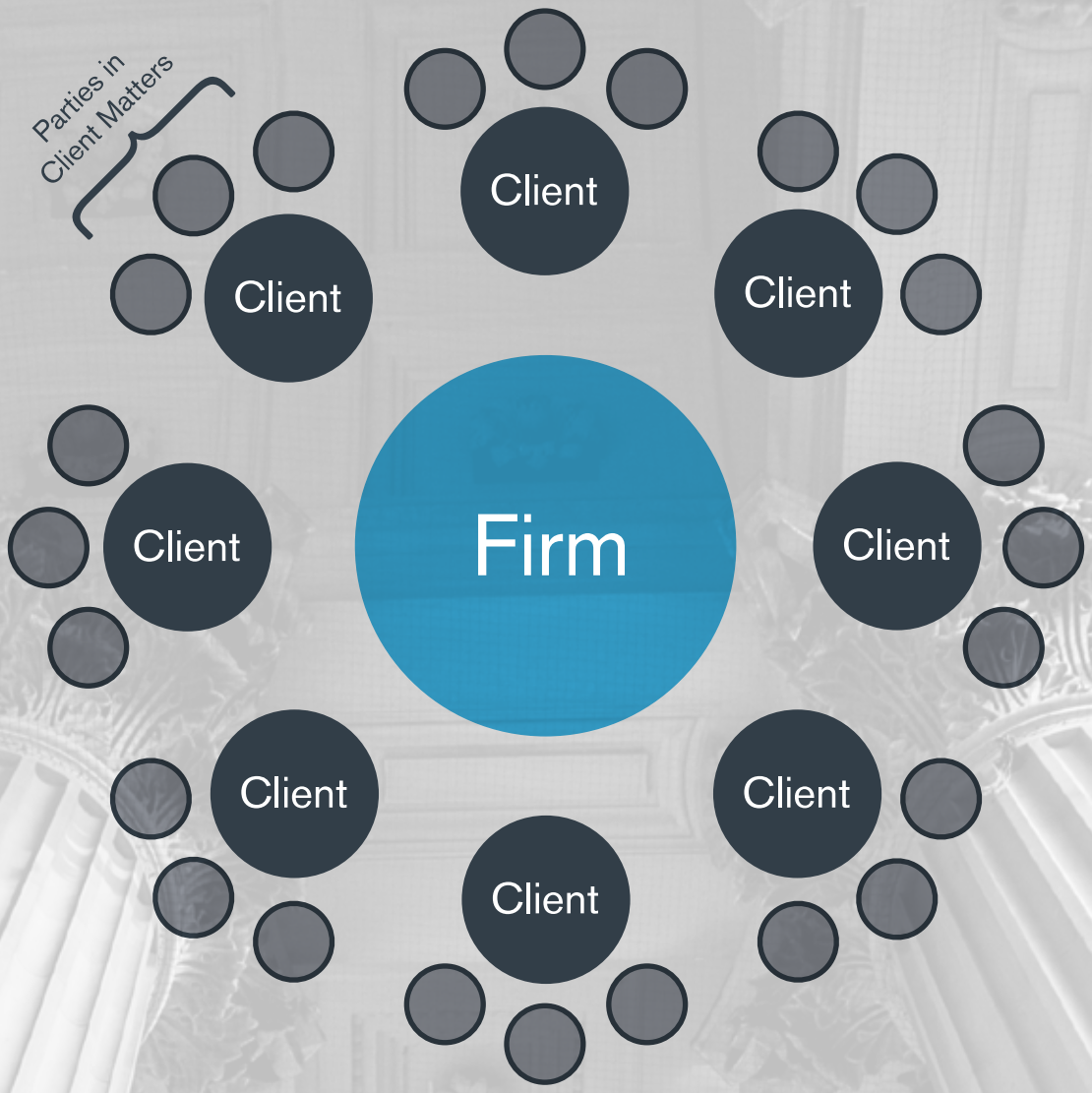


Figure 1: Information exists across the myriad relationships formed by law firms, their clients, and parties in client matters.

TAKING A MORE STRATEGIC VIEW OF INFORMATION AND ITS EXPOSURE

In this environment, *knowing the extent to which sensitive data has been exposed is itself valuable information*. To start at the center, for example, a law firm obviously needs to know if any of its information has made it outside its firewall and possibly into the wrong hands. This knowledge not only allows the firm to take whatever remediation is necessary, but it provides a more complete picture of the effectiveness of the firm's cybersecurity than can be had by penetration or vulnerability testing alone. (While those traditional assessments are important, they are focused more on the firm's *system* than on the data housed within that system.) It is also important to remember that in responding to a cyberattack, time is of the essence—and months can elapse between a breach's occurrence and its discovery. Because dark web monitoring directly tracks the information underground, the process provides a valuable early-warning system on cyber intrusions.

As one moves out from the center, however, the insights a law firm can glean go beyond the state of its cyber hygiene to take on powerful strategic overtones. The extent to which a client's intellectual property has been exposed and may be available to other parties, for example, can have direct bearing on negotiations or disputes in which the client is involved.

Tracking exposed information can also play a key role in the due diligence that needs to be conducted into other parties in client matters. For example, the exposure of an acquisition target's trade secrets may affect the valuation of that target—both because trade secrets are exposed and because that exposure may indicate further problems or cybersecurity deficiencies that an acquirer may have to address. (Consider that the acquirer may be liable for remedying the damage caused by a target's exposed confidential customer financial or health records.) Similarly, a client may need assurances from a potential joint venture partner with exposed information so that the client is not placing sensitive information that it shares with that partner at risk.

Mapping exposed information can also be important in litigation. If, for example, a client is a defendant in a suit claiming damages because the client allegedly exposed sensitive customer information, being able to show that the information had been previously exposed elsewhere may offer a potent defense.

Figure 2: Dark web monitoring gathers and filters hard-to-access information using both technology and insight from experienced threat intelligence analysts.

PIERCING THE "INFORMATION UNDERGROUND"

Dark web monitoring enables law firms to assess the exposure of sensitive information across the firm's relationship universe by penetrating the unindexed websites, chat rooms and networks, often accessible only with private credentials and the use of a special browser, that cybercriminals use to communicate and conduct business with one another. Comprehensive dark web monitoring platforms employ advanced tools to gather, review and analyze dark web data in a methodical and organized way (see Figure 2). First, computer programs use IP addresses, email addresses, keywords and other markers provided by the law firm and its IT department to scour the dark web and identify information of potential interest. Artificial intelligence programs then employ disambiguation, contextual analysis and other tools to analyze that data to extract signal from noise.

The intelligence gathered through these automated methods is then reviewed and further refined by an experienced analyst, who adds additional information that may be gathered from private chat rooms where cybercrimes and the data generated from those crimes are discussed. The end result is a map of the relevant entity's exposed information, ultimately providing actionable intelligence and meaningful insights for better decision-making.

A POWERFUL—AND EASY TO IMPLEMENT—TOOL

Two aspects of dark web monitoring make it particularly attractive for law firms from an operational perspective. First, unlike some types of cyber monitoring, it is non-invasive. Dark web monitoring requires no integration with the computer network of the law firm, its clients or anyone else. Second, the insights and context afforded by the specialists analyzing the data provide a sophisticated look into emerging threats from the perspective of the cybercriminals who design and implement those intrusions. This intelligence can help law firm IT managers better tailor their cybersecurity strategies and resources—an important advantage given that the information held by law firms makes them perpetually high-value targets for cyberattack.

More than ever, information—and particularly sensitive information—is a key currency fueling opportunity, valuation and transactions. Dark web monitoring gives law firms critical insight into this asset, helping them to provide informed, nuanced advice to their clients in strategic matters while keeping a close eye on their own cybersecurity performance.

Kroll | A Division of DUFF & PHELPS

CONTACTS

Anju S. Chopra is Senior Vice President, Technology with the Identity Theft and Breach Notification (ITBN) practice, based in Pittsburgh. In a career spanning over 20 years, Anju has been a leader in delivering innovative, often ground-breaking advances in complex technology systems, cybersecurity, artificial intelligence and enterprise architecture. She has particular expertise in developing cybersecurity and identity theft remediation products that integrate artificial intelligence technology. Anju's strong business acumen and entrepreneurial vision have resulted in strategic solutions that have transformed client services and the internal operations that support them.

anju.chopra@kroll.com | +1 412.400.6120

Brian Lapidus is the Identity Theft and Breach Notification (ITBN) Global Practice Leader, based in Nashville. Brian provides the strategic vision and direction for a globally recognized organization that helps clients and their advisors, including boards of directors, legal counsel and insurance providers, resolve the myriad complex issues resulting from a data breach. In addition to facilitating the response for some of the largest, most high-profile breaches on record, the team regularly delivers comprehensive notification and remediation services for organizations across the public, private and government sectors. With more than two decades of diverse corporate experience, Brian has particular knowledge in the challenges faced by clients in highly regulated industries, such as healthcare, financial services and higher education, as well as evolving regulatory regimes.

blapidus@kroll.com | +1 615.891.8540

About Kroll

Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security and data and information management services. For more information, visit www.kroll.com.

About Duff & Phelps

Kroll is a division of Duff & Phelps, a global advisor with nearly 3,500 professionals in 28 countries around the world. Our clients include publicly traded and privately held companies, law firms, government entities and investment organizations such as private equity firms and hedge funds. We also advise the world's leading standard-setting bodies on valuation and governance best practices. For more information, visit www.duffandphelps.com.