Three Keys to Preventing Misdirected Emails in Law Firms

Law firms offer a treasure trove of valuable data for cybercriminals. They can blackmail a business with the threat of exfiltration of client data, sell personally identifiable information on the dark web, and even offer IP to competitors. They can lock an entire system with ransomware and demand a huge sum to unlock it – knowing full well top law firms are insured and can pay the ransom. Cybercriminals can also use compromised accounts to launch attacks into a law firm's client base, damaging reputation and hitting the bottom line.

Email remains the primary and riskiest communication channel for law firms. The consequences of email data loss are severe, leading to regulatory fines, litigation from affected parties, significant reputational damage and client churn. Clients are also increasingly scrutinizing the email security and data loss prevention (DLP) safeguards their legal partners have in place, making robust security a competitive differentiator.

Read on to explore best practices for securing legal email communications against the persistent threat of insider risk, encompassing both accidental mistakes and intentional actions.

Understanding the Human Element in Email Data Breaches

To effectively mitigate risk, understanding the behaviors and environmental factors that lead to email data loss is crucial:

- **Human Error is Inevitable:** Simple mistakes like selecting the wrong recipient from an Outlook autocomplete suggestion, attaching the incorrect file or using "Cc" instead of "Bcc" are common. These errors are often made by diligent professionals who are rushing, stressed or distracted.
- **Modern Work Environments Increase Risk:** Remote and hybrid working models introduce new challenges. Many legal professionals work in shared communal spaces rather than dedicated home offices, increasing the risk of distraction. The use of mobile devices to access and send emails, often outside of standard working hours, further elevates the likelihood of mistakes.
- **"Productivity Workarounds" Create Vulnerabilities:** Employees may break security rules not out of malice, but to circumvent cumbersome security systems they feel hinder productivity. A common example is emailing sensitive documents to personal accounts to print them at home.
- **Malicious Intent is a Reality:** Not all data loss is accidental. Some employees intentionally leak data for personal gain, to exfiltrate IP to a competitor when changing jobs, or to retaliate against an employer.

Implement Intelligent, Context-Aware Email DLP

Static, rule-based DLP tools are insufficient for addressing the dynamic and human-centric nature of modern email threats. Legal firms must adopt an intelligent, proactive approach.

The most effective strategy is to deploy a system that understands normal user behavior to detect abnormal activity. Such a system should analyze historical email metadata—like common senders, recipients and groups—to build a network of trusted interactions.

The system should operate silently in the background and alert users to potential mistakes before they click send. This proactive engagement helps prevent data loss from misdirected emails, incorrect attachments or failure to use Bcc, without creating unnecessary friction for the user.

Here are the three most important elements an intelligent DLP platform should be able to handle:

1 Address Specific High-Risk Scenarios

An intelligent DLP tool should be capable of identifying and preventing the five most common types of sending mistakes:

- **Accidental Sends:** Flagging when an unusual recipient is added to a familiar group email thread (e.g., adding Bob2 instead of the usual Bob1)
- **Mistyped Recipients:** Detecting slight misspellings in email addresses or domains that could lead to a breach or be part of a phishing attempt
- **Forgotten Recipients:** Recommending the inclusion of a recipient who is typically part of a specific group communication but has been omitted
- **First-Time Sends:** Warning the user when they are emailing a recipient for the first time, prompting them to double-check the address
- **Misuse of To/Cc:** Analyzing recipient domains and suggesting the use of Bcc when an email is being sent to a large number of external contacts who may not know each other

2 Augment Your Defenses Against Sophisticated Phishing

- **Recognize the Limits of Native Security:** While essential, the native security tools in platforms like Microsoft 365 can be bypassed by sophisticated, text-based phishing attacks such as business email compromise (BEC) and executive impersonation. Cybercriminals constantly test these defenses to find ways through.
- **Employ Machine Learning and NLP for Inbound Threats:** Enhance your security stack with technology that uses machine learning and natural language processing (NLP) to analyze the context and content of inbound emails. This allows the system to detect subtle signs of social engineering and impersonation that traditional defenses miss.

3 Support Employees Across All Work Environments

- **Provide a Safety Net on All Devices:** With a significant number of legal professionals accessing email on mobile devices outside of office hours, your security solutions must provide real-time protection on these endpoints
- **Foster a Proactive Security Culture:** While technology is the most reliable defense, it should be used to support employees, not just blame them. Use technology that helps people avoid career-limiting mistakes and frames security as an enabler of safe, efficient work. Advanced analytics from your DLP tool can demonstrate its preventative value to the wider business, reinforcing the importance of security investments.

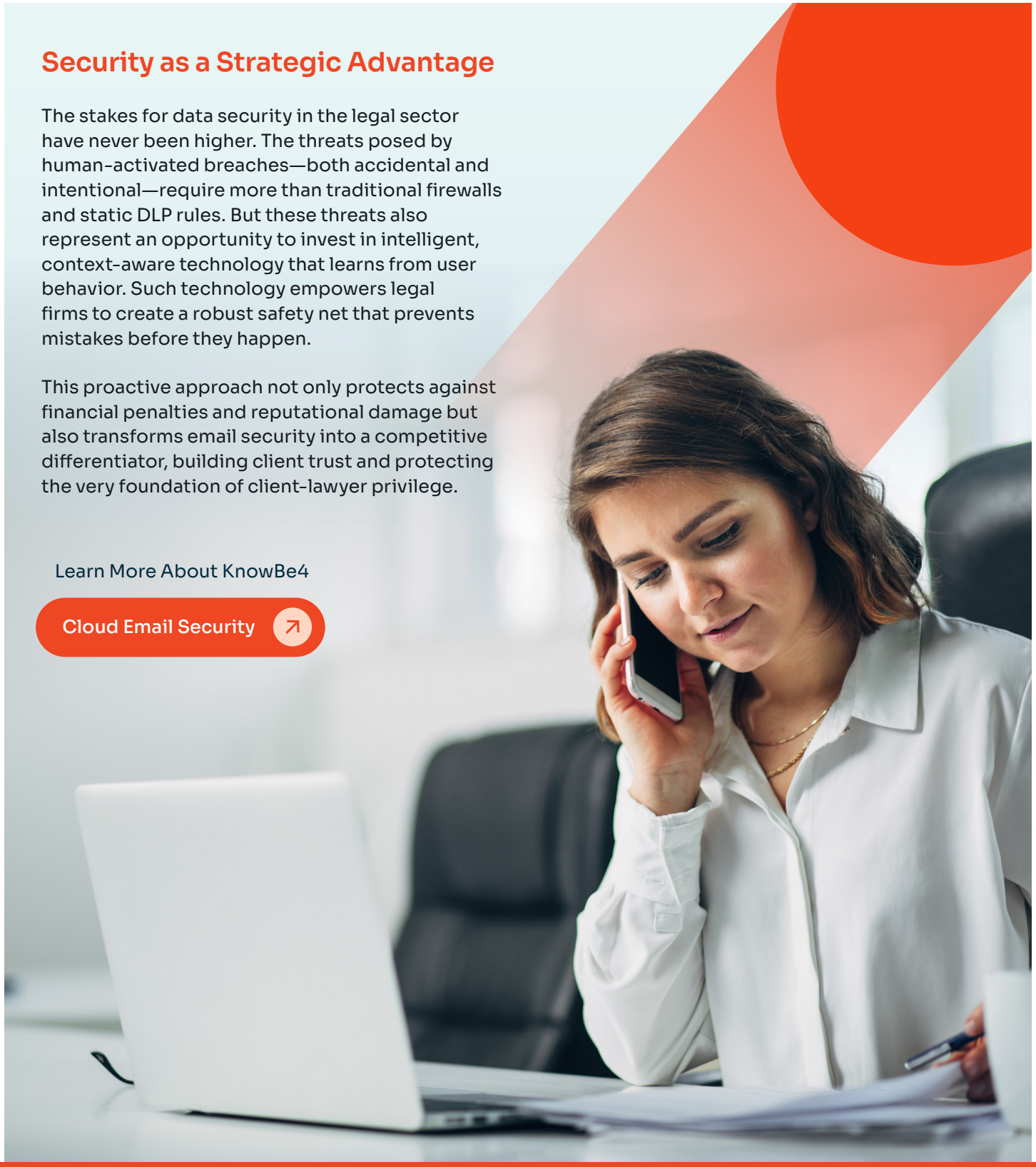
Security as a Strategic Advantage

The stakes for data security in the legal sector have never been higher. The threats posed by human-activated breaches—both accidental and intentional—require more than traditional firewalls and static DLP rules. But these threats also represent an opportunity to invest in intelligent, context-aware technology that learns from user behavior. Such technology empowers legal firms to create a robust safety net that prevents mistakes before they happen.

This proactive approach not only protects against financial penalties and reputational damage but also transforms email security into a competitive differentiator, building client trust and protecting the very foundation of client-lawyer privilege.

Learn More About KnowBe4

Cloud Email Security



KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com