Essential How-To Guide

Protect Your **Law Firm** or **Legal Department** from Accidental Emailing

VIPRE®

TABLE OF CONTENTS

VIPRE®

Did You Just Send an Email to the Wrong Person?

For the average person, mistakenly sending an email to an unintended recipient is certainly embarrassing...and surprisingly common. It's easy to glance up at an autocomplete email address, see that it looks correct, and just hit send...only to realize it was the wrong "Mike." Most of us have done this at least once, and experienced the uncomfortable sinking feeling that results.

But the stakes are much higher for legal professionals. By their very nature, law firms routinely deal with highly-sensitive information (e.g., financial data, medical records, insurance claims, personal details of clients, etc.) that is subject to strict compliance and regulatory requirements. Emails containing such info are vital to conducting legal business—and a veritable treasure trove for would-be hackers.

NO BUSINESS IS IMMUNE TO HUMAN ERROR

Think your law firm or legal department isn't at risk? Think again—one of your employees may actually have sent dozens of messages to the same wrong recipient without even knowing it. Accidentally emailing privileged attorney-client communications isn't just a theoretical hazard, it is a very real risk. Your legal team could inadvertently breach the confidentiality of such messages in any of the dozens of emails that are typically sent by each of your employees every day.

In some cases such email data breaches are the result of targeted attacks (e.g., hacking, malware, phishing & spoofing) by cybercriminals. That's no surprise, according to ABA Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack:" "Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms and legal departments are inviting targets for hackers.

In this e-book you'll get a closer look at data breaches and misdeliveries via email, and learn how law firms can implement security measures to prevent accidental emailing by using an email data loss prevention (DLP) solution.

TOP EMAIL SECURITY THREATS

Email is the backbone of modern business communications, and the most popular digital medium in the world. 3.7 billion users send 269 billion emails every day—representing three times the global daily messaging traffic of Facebook, WhatsApp, and SMS combined. Running a legal team without email is unthinkable, especially as employees become more mobile and work remotely from home or at clients' sites, often in different time zones.

Fortunately, today's legal professionals benefit from some level of security when using email. For example, authentication and encryption protocols are commonplace. In addition, communications can be centrally governed by the firm's information security policies. Furthermore, the IT administrator controls the allocation of company email addresses, and thus can remotely wipe any device that is lost, stolen, or retained by an employee leaving the firm or department.

Regardless of these security capabilities, legal entities still remain vulnerable to a variety of cyber threats and data breaches that can plague email, including hacking, malware, phishing, spoofing, and misdeliveries.

NOTABLE STATISTICS ON EMAIL SECURITY THREATS[1]

#1

Email phishing is the #1 type of threat action in breaches

94%

Detected malware was delivered via malicious email attachments

84%

Social media attacks featured phishing emails

60%

Misdeliveries represent approximately 60% of security errors

1 Source: Verizon's 2019 Data Breach Investigations Report; https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

TOP EMAIL SECURITY THREATS

HACKING

Email hacking consists of the unauthorized access and manipulation of a user's email account and messages, and is a common organizational threat according to the Verizon 2019 Data Breach Investigations Report. The report states that for the top hacking action vectors in breaches, 60% of the time the compromised web application vector was the front-end to cloud-based email servers; such hacking is usually linked to stolen or weak passwords.

MALWARE

Malware can be broken down into different categories, often infecting computers or networks via attachments in malicious emails. With ransomware hackers can lock their victim's computer, demanding money in exchange for a decryption key. But the damage malware can inflict goes far beyond ransoms. Spyware, for example, can collect key personal information—passwords, usernames, social security numbers—and reveal it to a variety of third parties (possibly including opposing counsel) for months without you knowing you've been compromised.

PHISHING & SPOOFING

Hackers may also try to trick your employees by presenting themselves as someone trustworthy. Wouldn't they be tempted to execute a request coming from a managing partner, asking for an urgent wire transfer to purchase business plane tickets or complete a time-critical project? Demands like that certainly appear legitimate and thus are often complied with, which is why business e-mail compromise (BEC) scams continue to be popular with cybercriminals.

MISDELIVERIES

The threats discussed so far all have the intent to harm your law firm or legal department deliberately—and they all originate externally. The media love to report these types of attacks, and prudent firms invest a sizeable portion of their IT security budget to fight them. By contrast, unintentional security incidents don't receive the same attention—but that doesn't make them any less dangerous. In fact, human errors (including misdeliveries via email) are almost twice as likely to result in a confirmed data disclosure.

CAUSES OF ACCIDENTAL EMAILING

DID YOU KNOW THAT 52% OF COMPANIES CHARACTERIZE INSIDER THREATS AS UNINTENTIONAL?[2]

Such errors can be attributed to busy employees, constantly on the move or juggling deadlines and deliverables. They strive to work better and faster, but sometimes they don't spend enough time verifying whether each recipient's email address is correct. In their defense, today's employees function in a business landscape that fundamentally makes mistakes more likely.

The only action type that is **consistently increasing** year-to-year in frequency is error.

Errors were casual events in **22%** of breaches

58% of victims had personal data compromised

3 Factors Underlying this Error-prone Landscape

- Interactions with External and Internal Stakeholders
- Large Contact Lists
- Emails to a Large Number of Recipients

2 Verizon's 2020 Data Breach Investigations Report https://enterprise.verizon.com/en-gb/resources/reports/dbir/

FACTOR #1: INTERACTIONS WITH EXTERNAL & INTERNAL STAKEHOLDERS

Do you outsource some of your legal organization's processes, whether to cut costs or to help you maintain focus on core business functions? Are you communicating with many potential candidates to hire the best attorneys? If so, your staff is likely sending a multitude of emails to external parties—often with attachments that potentially contain personally-identifiable information and intellectual property.

While that is obviously alarming, sending sensitive data to the wrong recipient(s) can be equally harmful. Imagine how risky it would be if all of your employees became aware of a confidential new technology that your patent team has been researching. What if a Human Resources officer inadvertently divulges detailed information on your attorney compensation plans?

Such risks can span a variety of departmental functions within a typical law firm or legal department. Activities prone to security breaches via accidental emailing include:

- Managing personal details of numerous clients every day
- Collecting, sending personally-identifiable information via forms
- Sending client-attorney privileged communications, re: ongoing litigation
- Different attorneys serving same client, sharing access to private files
- Managing documents containing trade secrets, commercial information
- Receiving blueprints, plans to obtain patent(s) for proprietary technologies

FACTOR #2: SIMILAR NAMES

As a natural part of their job duties, your team may come across different people with the same or confusingly similar names. Consider what could happen when employees deal with only two variants—James Smith and Jane Schmidt—in these hypothetical law firm scenarios.

Same Names in Different Companies

A partner at Law Firm A wants to add three attorneys to her team, and thus works with an HR officer named James Smith to discuss future job responsibilities, manage potential candidates and agree on salary packages. Coincidentally, there is another James Smith in the partner's contact list who works for another firm—Law Firm B.

An error could easily happen in this situation. For example, the partner might put the wrong James in CC and email him a list of shortlisted candidates—which he can then use to fill vacancies for the same or similar roles at Law Firm B! Or she might reveal valuable information about Law Firm A's strategy and compensation policies. Beyond looking unprofessional, this error could pose a serious threat to Law Firm A.

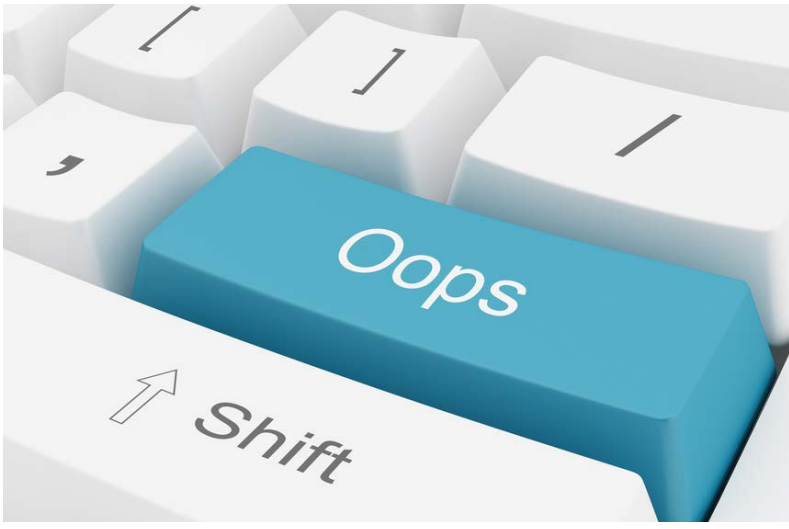
Same Names within the Same Company

Building on the example above, imagine there is an associate at Law Firm A who has been underperforming lately, and his name also happens to be James Smith. The partner is considering various ways to address this problem, including finding the ineffective associate a new job in another practice area. She sends several emails to James Smith—Law Firm A's HR officer—on that topic to discuss what to do.

That is obviously a very sensitive conversation, and the last thing the partner wants is to get the two recipients confused. If that happens she would inadvertently alert James—her direct report, who is not fully aware of his tenuous job status—about her concerns. Not only would this demoralize him, it could also potentially affect the performance of other associates in the firm.

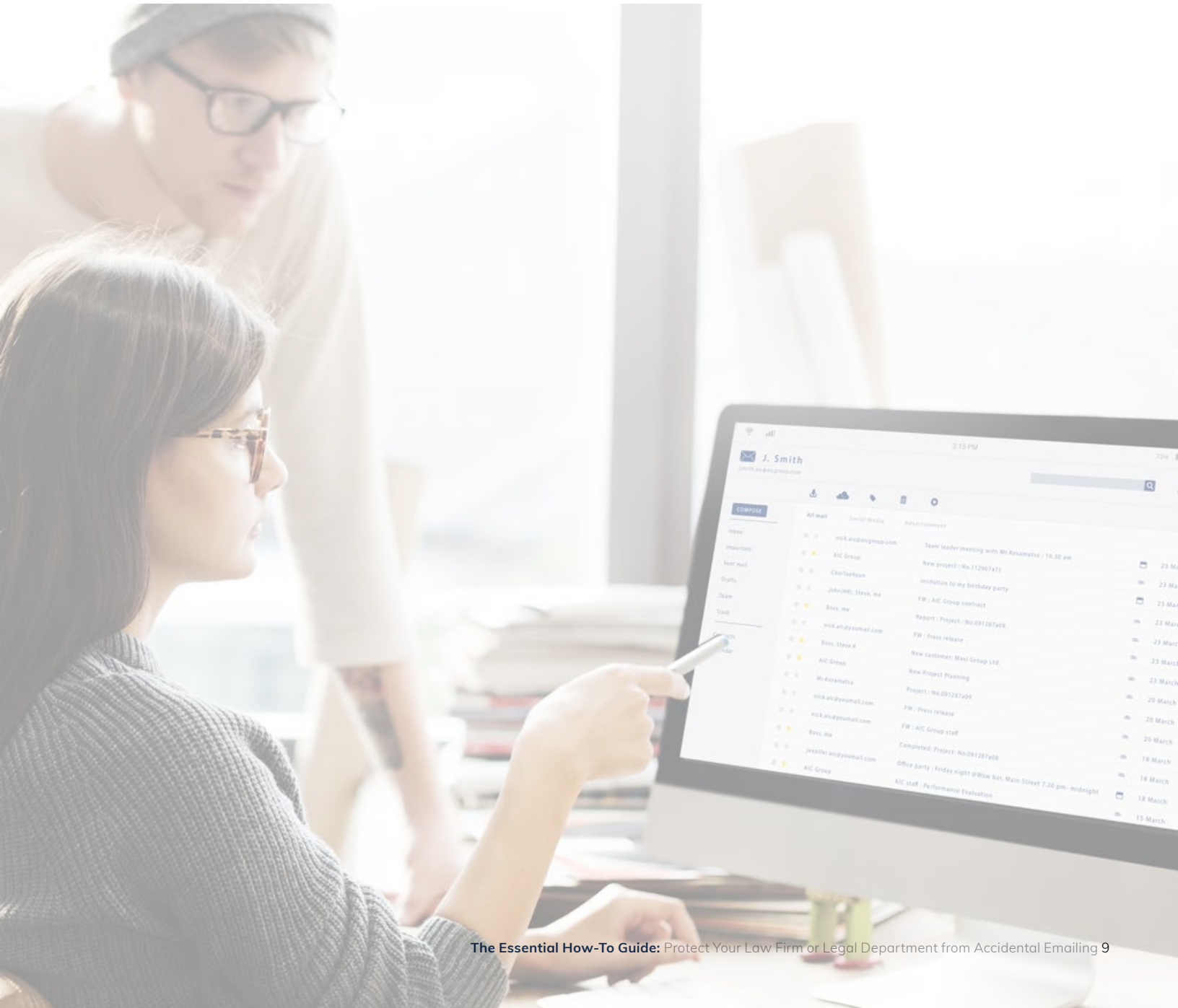
Similar Names within the Same Company

Law Firm A hires a new Office Manager named Jane Schmidt; the partner has not yet met Jane personally, but would like to make a positive first impression on her when she has the chance. If the partner tries to send an email with personally-identifiable information to James Smith (the HR officer) but mistakenly sends it to Jane Schmidt instead, it's a safe bet Jane will never trust the partner's judgment—potentially slowing her career advancement.



FACTOR #3: EMAIL IN GENERAL

Some employees in your law firm or legal department may need to send strategic and confidential communications via email. This might include data surrounding a current trial case or sharing a client's personal files and background. One big danger here is the potential of disclosing the confidential details of the case or client by mistakenly emailing the work person, thus disclosing either your strategy or other private data.



CONSEQUENCES OF DATA BREACHES

It is difficult to predict what the exact consequences of a given breach could be. Deloitte published a report[3] that takes an in-depth look at the various business impacts that may occur when confidential records are lost or stolen. The study makes an important distinction between direct costs (which companies incur shortly after an incident) and hidden costs (which have long-lasting effects). **The repercussions from these latter costs may account for 90% of the total business impact**—including financial and reputational damages

SHORT-TERM FINANCIAL COSTS

If your firm or department is responsible for a breach, you'll need to allocate the resources and time needed to remediate the situation. This begins with a thorough technical investigation to find out what happened, identify security holes, and manage any external communications. You then must take immediate actions to notify and protect individuals at risk, as well as secure faulty systems and processes.

LONG-TERM FINANCIAL COSTS

The real financial costs only surface later on. For example, your law office will probably need to pay penalties, along with attorney and litigation expenses. Your firm's credit rating may drop, making it harder to raise capital. And your firm's cyberthreat insurance premium can increase significantly, even if you make substantial investments to secure your IT infrastructure and processes.and processes.

Direct and Hidden Costs of Data Breaches

Direct Costs

- Technical investigation
- Client breach notification
- Post-breach client protection
- Regulatory compliance
- Public relations
- Attorney fees and litigations
- Cybersecurity improvements

Hidden Costs

- Insurance premium increases
- Increased cost to raise capital
- Operational disruption
- Lost value of client relationships
- Lost contract revenue
- Devaluation of trade name

3 Deloitte https://www2.deloitte.com/bh/en/pages/about-deloitte/articles/deloitte-identifies-14-business-impacts-of-a-cyberattack.html#

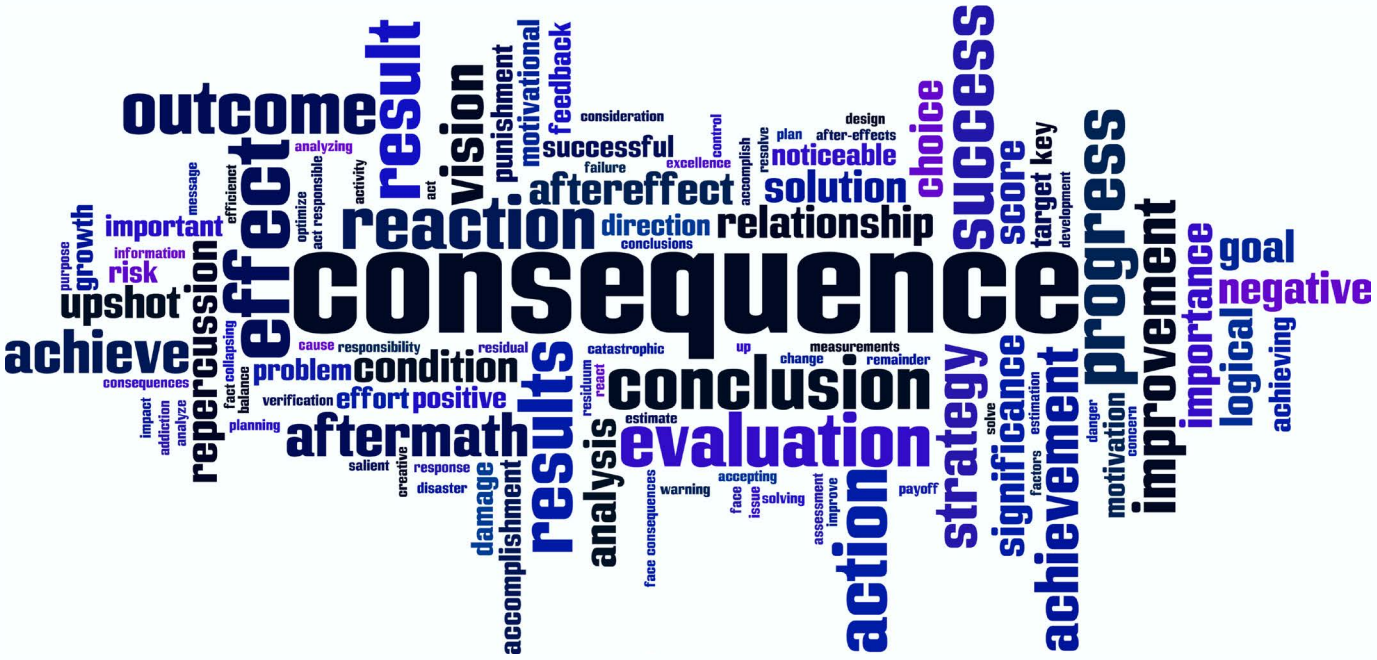
CONSEQUENCES OF DATA BREACHES

Reputational Damages

While the above financial costs may severely impact your law firm or department, they can pale in comparison to your loss of existing clients—and the inability to attract new ones—because they doubt your ability to protect their data. Additionally, you may find it more difficult to keep your current employees or find top talent in the future.

What About Pretending a Breach Never Happened?

Beyond being unethical and irresponsible, simply ignoring that a breach has occurred is illegal in most cases. The vast majority of countries around the globe have set (or are in the process of setting) breach notification laws that include mandatory reporting to protect individuals whose personal information might be at risk. Ignoring these laws can carry harsh civil—**and criminal**—penalties.



PREVENTING EMAIL DATA LOSS

In light of the severe consequences that can arise from data breaches and the associated laws addressing them, most legal entities proactively choose to invest in cybersecurity, with "protection and prevention" being their primary spending priority. When it comes to email, there are three key strategies your team should consider in order to minimize your risk of data theft and loss:

1. Authentication & Encryption

Hackers may try to attack your systems directly to access confidential data, or they can catch emails as they transit via an insecure transport link. The good news is that protocols (including DKIM, DMARC, SPF and TLS) are designed to prevent most instances of unauthorized interception, content modification and email spoofing. Encryption and authentication, however, do not safeguard you against human errors and misdeliveries.

2. Policies & Training

It is vital that your firm or legal department develops and implements security guidelines and rules regarding the circulation and storage of sensitive information—as well as clear steps to follow when a security incident happens. Once you have defined these policies and procedures, you must also ensure that employees are fully aware of them, and undergo training when they join the team—or after every significant security update.

3. Data Loss Prevention

Despite such policies and employee training, there is always a risk that sensitive internal information will leave your law offices. Human errors often occur in fast-paced legal environments, and accidental emailing due to autocomplete lists is a prominent example of that. Autocomplete caches save time because recipients can be selected after typing just a few letters instead of entire email addresses.

However, this added convenience can encourage your employees to let their guard down and forget to check whether they have selected the right person before sending a message. Disabling auto-complete and requiring your colleagues to type each email address manually for every message they send is one answer, but highly inefficient and frustrating to users.

Alternatively, you can choose to install an email data loss prevention (DLP) solution to prevent misdeliveries without hindering productivity within your law firm.

VIPRE SAFESEND:
HOW EMAIL DLP WORKS

In a nutshell, email DLP solutions like VIPRE SafeSend enable your law firm to implement security measures for the detection, control and prevention of risky email sending behaviors. This technology doesn't impede the working practices of your colleagues (unlike a policy of disabling autocomplete cache) while still minimizing the risk of accidental emailing.

Consider these fictional use case examples, and the markedly different outcomes they produce based on whether VIPRE® SafeSend® is deployed:

Example: Confirm Recipients and Attachments

Lara is a contracts attorney who interacts with a wide variety of internal stakeholders, and frequently exchanges confidential documents with colleagues in her firm's corporate law department. She also directly supports many external contracts clients. As such, Lara sends dozens of emails every day—and due to her extensive contact lists, there's always a risk that someone unintended ends up in the TO or CC fields.

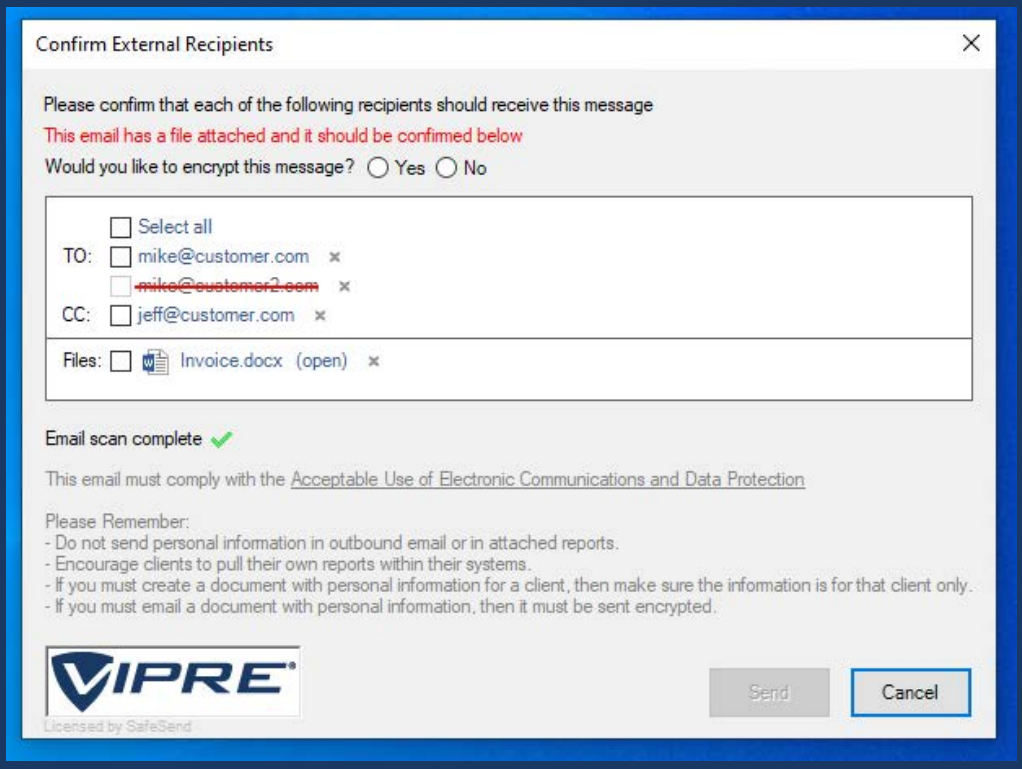
If Lara makes that mistake...

Without VIPRE SafeSend

She's in big trouble. Her email has likely been delivered already, and there's little she can do except try to recall it—with a high probability of failure.

With VIPRE SafeSend

A window would have popped up and flagged any personal, misspelled or spoofed email address that Lara selected, giving her the opportunity to go back to her email draft and remove any unwanted recipients.



VIPRE SAFESEND:
HOW EMAIL DLP WORKS

Example: Advanced Content Scanning

Your colleagues may not always remember which files contain highly-sensitive information, or they can get distracted when hurriedly working. That is exactly what happened to Anna, who attached the wrong file after receiving an urgent request from Jim (the firm's marketing director) to send him sales collateral targeting prospective clients.

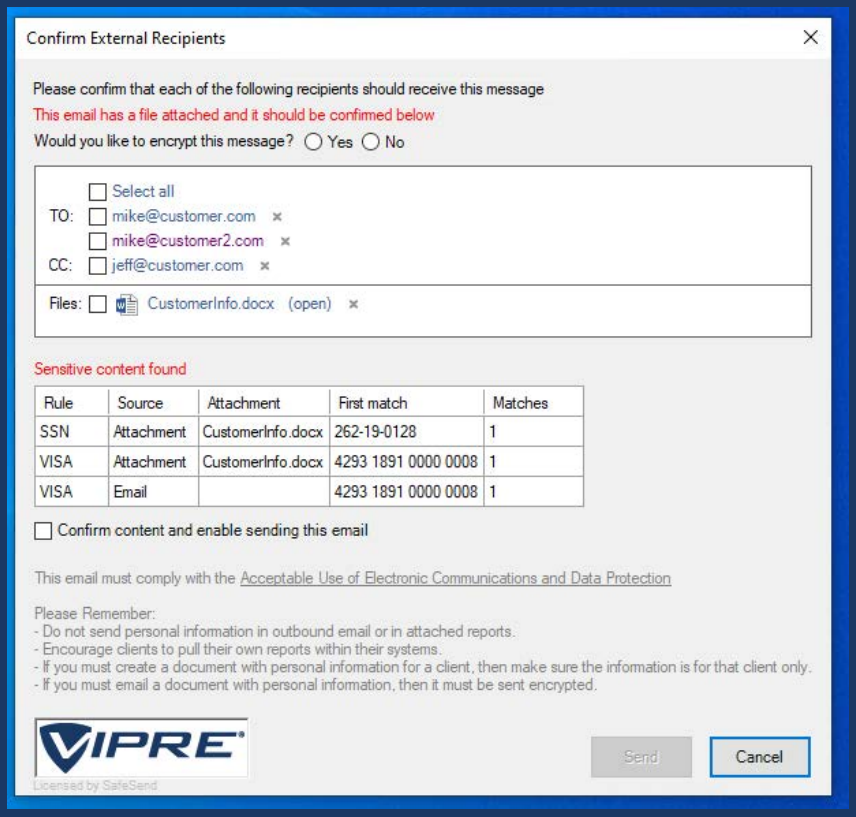
Neither Anna nor Jim knows that the document she mistakenly sent contains a list with thousands of credit card numbers.

Without VIPRE SafeSend

Their firm is on the verge of a massive data breach because Jim did not open the file first—and is about to send it to a multitude of potential clients.

With VIPRE SafeSend

With SafeSend's advance scanning functionality, this breach would have been prevented from the start. Anna would have seen a confirmation window like the one below and realized the attached file was filled with credit card numbers.



VIPRE SAFESEND:
HOW EMAIL DLP WORKS

Example: Centrally-Managed Settings

To put it bluntly, how good are a law firm's security policies if they can't be enforced? You must have the ability to consistently implement your departmental and employee-specific rules concerning data circulation if those rules are to be truly effective.

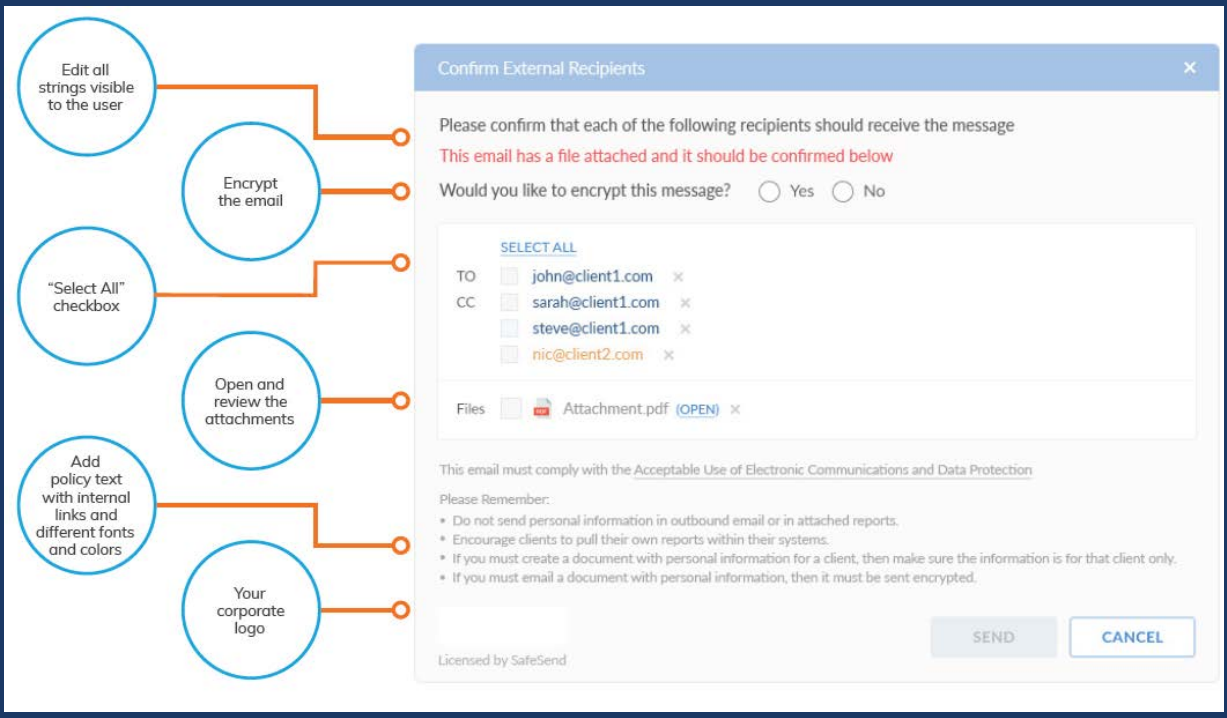
How can lawyers be sure everyone is following its security policies?

Without VIPRE SafeSend

The firm probably lacks the control required to verify compliance with its policies, and can only hope its employee training was enough to encourage best security practices in email communications.

With VIPRE SafeSend

The law firm can easily ensure its security policies are being observed, and seamlessly manage rules and exceptions both internally and externally. This is particularly convenient if the firm wants to add an extra confirmation step only for attorneys and staff working with client-sensitive information.



CHOOSING AND INSTALLING AN EMAIL DLP SOLUTION

Despite what you might think, the selection and installation of a sophisticated email DLP solution can be remarkably simple. Below is an overview of the steps you should follow when evaluating and deploying VIPRE SafeSend (or other email DLP products):

1. Check System Requirements

First, make sure to check the email DLP solution you're considering fits with your existing IT infrastructure and systems. For example, SafeSend is compatible with all recent versions of Outlook and Windows used in today's law firms and legal departments.

2. Link Your Email User Policy

Next, ensure the email DLP solution you choose offers you enough flexibility to implement your legal team's information security policy. For example, you might need the ability to:

- Notify users when an email address seems to be added by mistake (e.g., all addresses end in "@client1. com" but one ends in "@client2. com")
- Remind users about key rules and other info before they send an email
- Set different permissions, security measures for internal/external contacts
- Specify content scanning rules (e.g., flagging 16-digit credit card numbers)
- Notify users when their message is addressed to more than XX recipients
- Distinguish between safe, unsafe, and forbidden domains

3. Deploy Solution

Installing the email DLP solution should be as simple as possible, with the option to deploy the software either individually on each machine or all computers at once. Your IT administrator should also be able to configure and manage the security settings centrally, without requiring redeployment.

4. Inform End Users

The email DLP solution you select should be intuitive to use and promote best sending practices. For example, every SafeSend confirmation window tells users why a breach may occur if they send the email as is, and provide them with a link to your information security policy for more information if needed. (Educational material—articles, how-to guides, videos—can also help train your colleagues.)

5. Monitor Security Performance (optional step)

Keeping an eye on how employees are using email can help your legal team strengthen its security and implement better policies. For example, SafeSend integrates with SIEM applications such as Splunk, enabling you to analyze how much sensitive information is being transmitted by employees, so you can detect and remediate any bad email sending practices.

CONCLUSION

Email is the most widespread form of business communication, and virtually no legal professional could effectively function without it. But email is also a common cause of data breaches which can result in massive fines and irreparable reputational damages.

To combat these breaches, savvy law firms and large legal teams invest heavily in email security technologies with authentication and encryption capabilities. These solutions and protocols may do an excellent job tackling intentional external threats (hacking, malware, spoofing, phishing) but offer little help when it comes to stopping inadvertent disclosure of sensitive data to the wrong recipient.

BOTTOM LINE

The risk of revealing confidential information exists in every email that's sent by your employees. That's why we offer SafeSend, a powerful and user-friendly solution that enables firms to prevent accidental emailing without disrupting the day-to-day business practices of their attorneys and staff.

SafeSend is an industry leader in the prevention of accidental emailing, and is designed to meet the needs of mid-size and large organizations by offering over 70 configurable settings, as well as a variety of API integration capabilities for email encryption, SIEM, and incident management.

Trusted by over 200,000 users around the world, SafeSend processes more than 5 million emails every day, and is compatible with Outlook and Windows. Visit www.VIPRE.com to request a free trial today.

ABOUT VIPRE

VIPRE is a leading provider of internet security solutions purpose-built to protect businesses, solution providers, and home users from costly and malicious cyber threats. With over twenty-five years of industry expertise, VIPRE has one of the largest threat intelligence clouds, delivering unmatched protection against today's most aggressive online threats. Our award-winning portfolio of protection includes comprehensive endpoint, email, user and network security with threat intelligence for real-time malware analysis. VIPRE solutions deliver easy-to-use, comprehensive layered defense through cloud-based and server security, with mobile interfaces that enable instant threat response. VIPRE, a subsidiary of J2 Global, Inc., is headquartered in Florida and operates globally across North America and Europe. www.VIPRE.com