Cybersecurity: Interdisciplinary Tips on the New Regulatory Landscape for In-house Counsel

September 25, 2024

Benesch Law
71 S. Wacker Dr., Suite 1600
Chicago, IL 60606

ARMORTEXT Benesch ACC Association of Corporate Counsel CHICAGO

Speakers

Aslam Rawoof

Benesch Law,
Partner, Corporate &
Securities Practice Group

Ryan Sulkin

Benesch Law,
Partner, Intellectual
Property Practice Group

Navroop P. S. Mitter

CEO, ArmorText

Mark Grazman

CEO, Conversant Group

Tabletop Exercise /ˈtābəlˌtäp eksərˌsīz/

Simulations of real-world scenarios that allow organizations to test their incident response plans in a safe and controlled environment.

IBM Cost Of Data Breach Report 2023

50%

Over half of breached companies bolster spending post-incident. Their top investment? Incident response planning and testing.

54 Days

Organizations with both an incident response team and incident response plan testing were able to identify breaches 54 days faster than those with neither. Testing the incident response plan, even without forming a team, was nearly as effective, resulting in a difference of 48 days or 17%.

Tabletop Exercises: Best Practices and Common Pitfalls

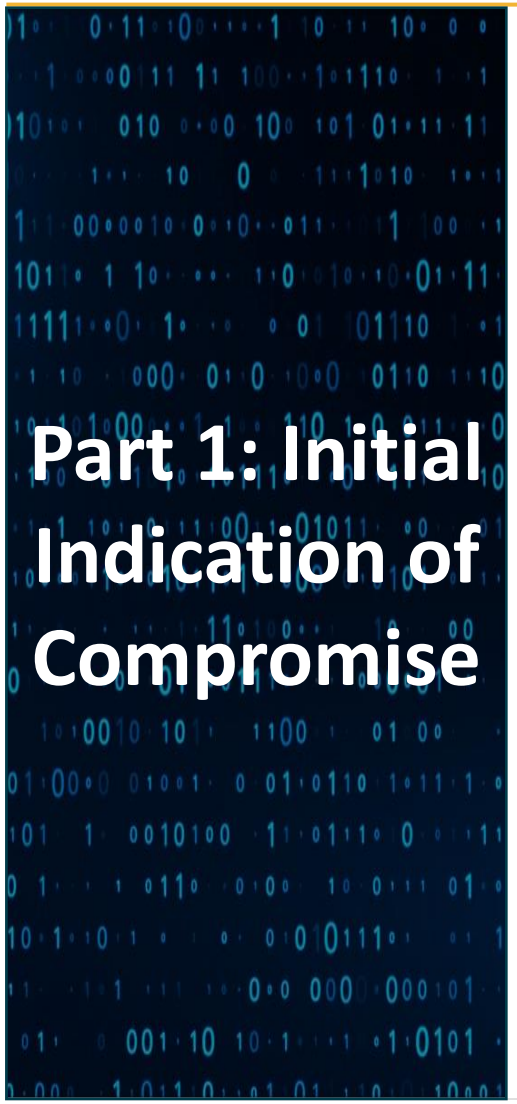
Blind spots

- Outdated plans
- Insufficient cross training
- Overlooking communications

Planning Shortcomings

- Not setting clear objective
- Overly simplified scenarios
- Groupthink / Just in time saves
- Ignoring third party / vendor interdependences
- Letting News vs Actual Risk drive scenarios

Example Scenario: Scattered Spider

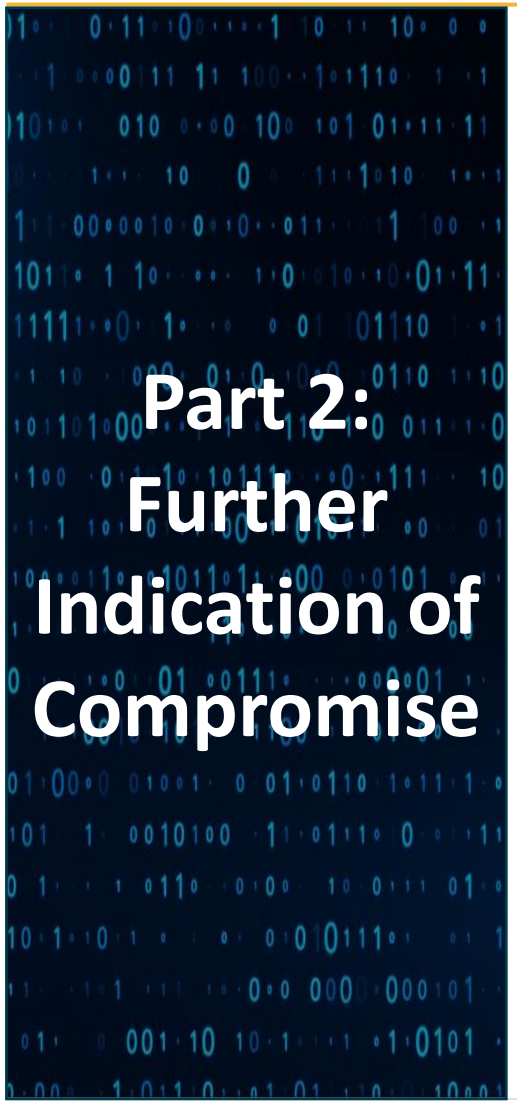


Part 1: Initial Indication of Compromise

Scattered Spider is a cybercriminal group that targets large companies and their contracted information technology (IT) help desks. Scattered Spider threat actors, per trusted third parties, have typically engaged in data theft for extortion.

Your company's IT department detected the installation of unauthorized remote access software on multiple employee workstations. The Help Desk has seen a spike in calls from employees whose multi-factor authentication (MFA) is no longer working. Multiple system administrators report that they are unable to log into their accounts, but the accounts appear to be active and in use.

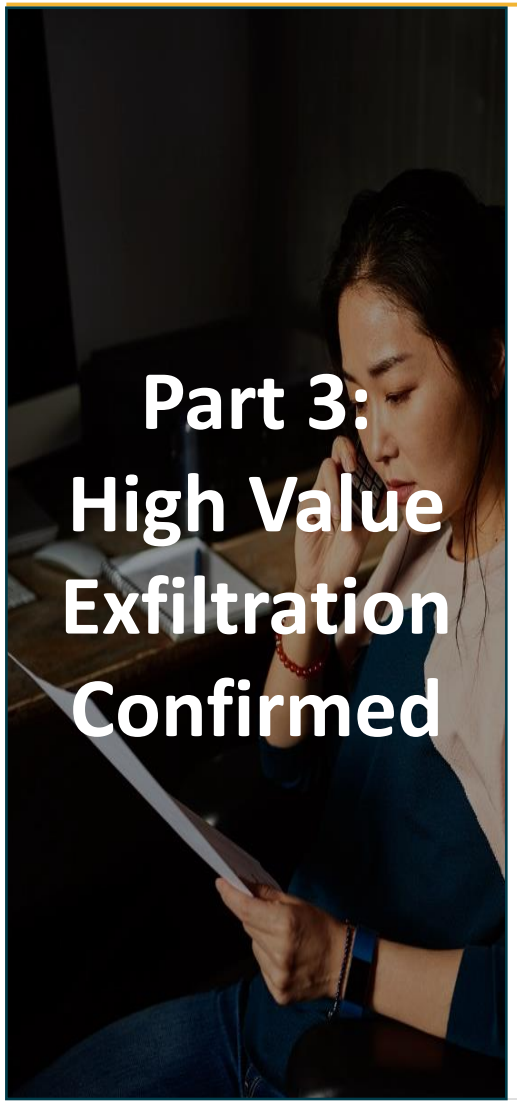
Example Scenario: Scattered Spider



On further inspection, it appears that compromised administrator accounts have been used to elevate privileges for other user accounts. IT teams have identified multiple instances of unauthorized software installations, as well as unusual network traffic to unknown external destinations. Servers supporting key business functions are non-responsive and appear to be encrypted, raising alarms that ransomware deployment may be underway.

This situation is evolving rapidly, and IT leadership is concerned that company email systems may not be secure.

Example Scenario: Scattered Spider



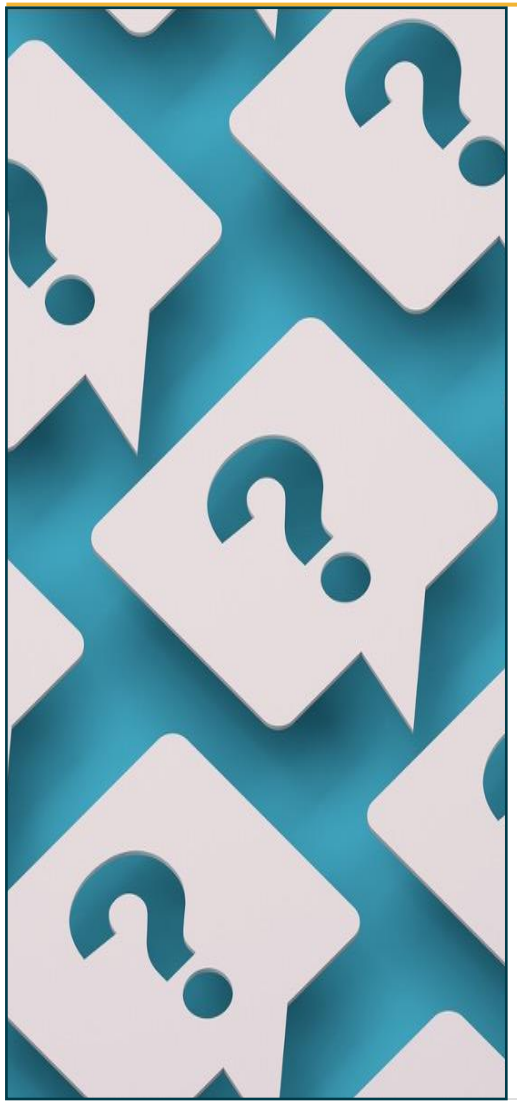
It appears that a Help Desk employee aided a caller identifying herself as an executive who needed urgent help to set up MFA on a new phone, to access files needed to close a deal before a critical deadline. Logs show that the executive's account subsequently downloaded critical files related to an upcoming product launch to an IP address in a location where the company has no operations.

Example Scenario: Scattered Spider

Company IT has confirmed that mission critical systems are inaccessible and appear to be encrypted. The company has been contacted by a ransomware operator, stating that it has company files and demanding significant payment for a decryption key and to not post the files publicly. Company operations will be seriously hindered if the outage continues.

IT teams continue to identify new activity by compromised user accounts.

There’s a Lot to Consider. Here’s a brief glimpse…



General / Plan / Initiation

Does your company have a plan to respond to this type of incident?

- If so, who is responsible for initiating it?
- Is the plan available if company systems are unavailable?

Team

Who are the key employees/teams who need to be involved at this stage?

- Do those employees know their roles?
- Who has decision-making authority for the company?

Communications / Collaboration

How are responsible personnel expected to communicate under these circumstances?

Impact / Return to Normal Operations

How would the threat actor’s social engineering, account compromises and ransomware attack mission-critical operations of the company?

What are the company’s immediate concerns regarding mission-critical systems accessed?

Remediation / Restoration

Does the company have immediately known remediation or restoration options?

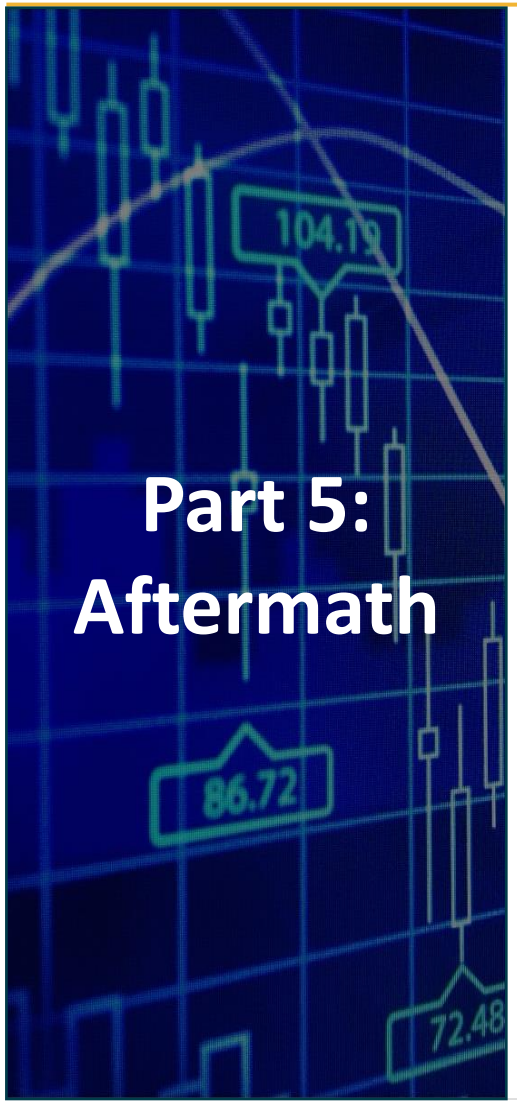
Notification Obligations / Timelines

Does the company have any immediately known notification obligations?

Insurance Coverage / Timeline

Does the company have insurance coverage for an event like this?

Example Scenario: Scattered Spider



Weeks after the incident has been resolved, the company's General Counsel requests a copy of all electronic communications from security and incident response personnel involved with the remediation of the incident in case of future legal or regulatory action.

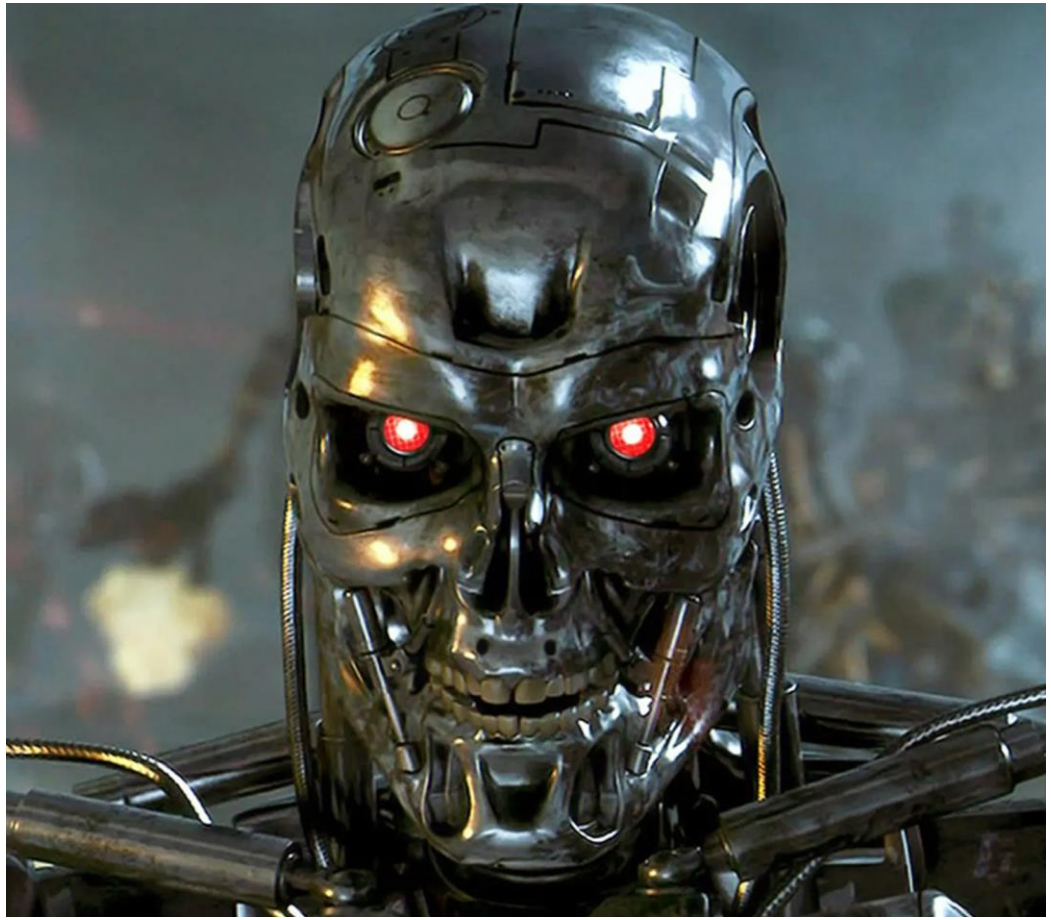
Later, the company receives a request for information and document preservation request from the Department of Justice regarding the incident. Because there is no centralized audit trail for consumer encrypted messaging platforms (e.g., Signal, WhatsApp) used by incident responders, the company counsel initiates a process to capture and retain communications from these platforms.

Company is public and has determined the incident was material from a securities law perspective and must file public disclosure.

Ephemeral messengers

- Regulators are placing a spotlight on the use of platforms like Signal, WhatsApp and WeChat
  - DOJ and FTC this year updated their preservation notices to include communications on ephemeral messaging platforms
  - Billions in civil penalties have been levied for failing to preserve
- Are your employees using unauthorized communication apps?
  - What are the message deletion practices of these apps?
  - Do they align with record retention requirements?
- See our Client Bulletin “Staying Ahead of the Curve: Adapting to Evolving Cyber Regulatory Enforcement” (Sept. 24, 2024)
  - https://www.beneschlaw.com/a/web/8WTj44yf5wsXfYyemakFLU/9q5a43/staying-ahead-of-the-curve.pdf

Incident Response in the Age of AI



Where do we go from here? What scenarios might we be overlooking?

September 24, 2024

STAYING AHEAD OF THE CURVE: **Adapting to Evolving Cyber Regulatory Enforcement**

Marisa T. Darden, Aslam A. Rawoof, Parth Y Patel, Dave Walters, and Navroop Mitter

ARMORTEXT

Benesch

September 24, 2024

STAYING AHEAD OF THE CURVE:
Adapting to Evolving Cyber Regulatory Enforcement

Authors

MARISA T. DARDEN
Chair, White Collar, Government Investigations & Regulatory Compliance Practice Group
mdarden@beneschlaw.com | T: 216.363.4440

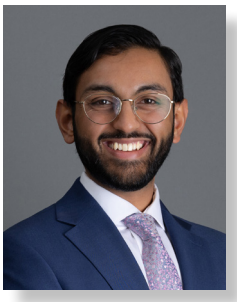
Marisa T. Darden is a partner and the chair of Benesch's White Collar, Government Investigations & Regulatory Compliance Practice Group. Marisa is a former state and federal prosecutor. Marisa has a distinguished career assisting clients across various industries. She actively advises companies and individuals in defense of civil and criminal investigations and prosecutions brought by law enforcement and regulatory agencies. Marisa has successfully tried more than 15 complex criminal cases to verdict and has argued before the Sixth Circuit Court of Appeals. Marisa clerked for the Honorable Morrison C. England in the Eastern District of California, and worked as an Assistant District Attorney in the New York County (Manhattan) District Attorney's Office.

Her extensive experience includes handling investigations related to the Foreign Corrupt Practices Act, bribery, corruption, the Racketeer Influenced and Corrupt Organizations Act, wire and mail fraud, and complex financial investigations. Marisa also conducts corporate inquiries into sexual harassment allegations, workplace discrimination, civil rights, and Title IX violations.

ASLAM A. RAWOOF
Partner
arawoof@beneschlaw.com | T: 646.593.7050

Aslam A. Rawoof is a partner in Benesch's Corporate & Securities Practice Group. Aslam has a broad transactional practice includes capital markets transactions and corporate governance matters. Aslam represents issuers, underwriters, and servicers on a variety of complex securities matters, including initial public offerings, other public and private equity offerings, investment-grade and high-yield debt offerings, acquisition financings, debt tender offers, exchange offers, securitizations, and other refinancing transactions.

In addition to his transactional work, Aslam advises clients on general corporate and corporate governance matters, including those related to Artificial Intelligence (AI). He has a history of representing clients in various industries, including transportation, where he has provided counsel on corporate governance, financing, and securities law matters.



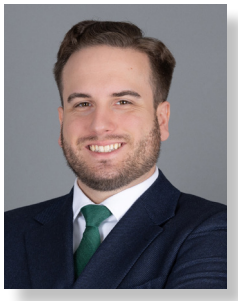
PARTH Y. PATEL
Associate
ppatel@beneschlaw.com | T: 216.202.2576

Parth Y. Patel is an associate in Benesch's Litigation Practice Group in Illinois and Ohio, Parth focuses his practice on guiding clients in highly specialized industries through the complex landscape of litigation and investigations. He has extensive experience counseling clients in the healthcare, technology, and manufacturing sectors, leveraging his academic and professional background to provide exceptional value.

ARMORTEXT

Benesch

Authors



DAVE WALTERS
Associate
dwalters@beneschlaw.com | T: 216.363.6132

Dave Walters is an associate in Benesch's Litigation Practice Group. Dave focuses his practice on pre-trial, trial, and appellate advocacy in the contexts of complex commercial litigation and white-collar matters. Dave draws on his extensive experience from Case Western Reserve University School of Law's nationally ranked Mock Trial program, where he competed at the national level in both the National Trial Competition and Tournament of Champions. He also won the CWRU School of Law Dean Dunmore Moot Court Competition and competed on the National Moot Court Team.

NAVROOP MITTER
CEO & Founder, ArmorText

Navroop Mitter is the visionary CEO and founder of ArmorText, a leader in secure out-of-band communications. With a deep understanding of the evolving cybersecurity landscape, Navroop accurately predicted the vulnerabilities in enterprise communications and the critical need for compliant, secure channels. Under his leadership, ArmorText has been recognized as a leader in The Forrester Wave™: Secure Communications Solutions, Q3 2024, and has become a category leader for out-of-band communications, particularly for incident response and security operations. Navroop's unique blend of patience, grit, and informed insight has driven ArmorText to outclass competitors, safeguarding critical infrastructure against sophisticated cyber threats. His strategic vision continues to shape the future of post-breach resilience, ensuring that organizations can effectively communicate during crises.

Navroop is a trusted advisor to senior leaders across industries, including C-suite executives, CISOs, and board members, and frequently collaborates with strategic partners and law firms to enhance corporate resilience. His work is a testament to his commitment to protecting enterprises and critical infrastructure from the growing onslaught of cyberattacks.

Update from Benesch's Corporate & Securities and White Collar, Government Investigations & Regulatory Compliance Practice Groups

STAYING AHEAD OF THE CURVE: Adapting to Evolving Cyber Regulatory Enforcement

As calls for executive accountability for cybersecurity intensify, it is essential for companies to scrutinize the adequacy of ephemeral messengers, such as Signal, WhatsApp, WeChat, and Snapchat, in light of both present and future regulatory frameworks. Our analysis delves into the present enforcement actions centered around data retention while also casting a forward-looking perspective on other compliance controls that may soon come under scrutiny. By preemptively addressing potential regulatory changes, organizations can avoid costly overhauls and ensure their communication practices remain ready for an evolving regulatory landscape.

Messaging Ephemerality in the Cross-Hairs

The concept of a disappearing message isn't new. Many modern communication platforms allow for some level of automatic message deletion. While these features may serve to enhance privacy, how companies utilize them can result in legal exposure. Since 2023, the United States Department of Justice (DOJ) has continued to update its Evaluation of Corporate Compliance Programs to address how companies police the use of personal devices and third-party messaging applications.[1] Earlier this year, DOJ and the Federal Trade Commission (FTC) announced that the agencies were updating their preservation notices to include communications on ephemeral messaging platforms.[2] The government has been quick to enforce this new guidance,[3] seeking attorney's fees, civil penalties and potentially even obstruction of justice charges for failing to preserve information on third-party messaging applications. Other regulatory agencies, such as the Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC), have already levied billions of dollars in civil penalties in the banking sector and beyond.[4]

On August 14, 2024, in a broad enforcement action, the SEC fined 26 financial firms a combined amount exceeding $390 million.[5] The firms were found to have engaged in pervasive and longstanding use of off-channel communications methods. In these cases, the SEC considered these failures to preserve required records to amount to violations of the Securities Exchange Act, the Investment Advisers Act or both. The CFTC separately announced settlements with three other banks for related conduct.

[1] Office of Public Affairs | Assistant Attorney General Kenneth A. Polite, Jr. Delivers Keynote at the ABA's 38th Annual National Institute on White Collar Crime | United States Department of Justice

[2] FTC and DOJ Update Guidance That Reinforces Parties' Preservation Obligations for Collaboration Tools and Ephemeral Messaging | Federal Trade Commission

[3] *See e.g., Fed. Trade Comm'n v. Amazon.com, Inc.*, 2:23-cv-01495 (W.D. Wash. April 25, 2024); *Fed. Trade Comm'n v. Amazon.com, Inc.*, No. 2:23-CV-01495-JHC, 2024 WL 3342701 (W.D. Wash. July 9, 2024); *In re Google Play Store Antitrust Litig.*, 664 F. Supp. 3d 981 (N.D. Cal. 2023).

[4] JPMorgan Chase Consent Order (occ.gov)

[5] SEC.gov | Twenty-Six Firms to Pay More Than $390 Million Combined to Settle SEC's Charges for Widespread Recordkeeping Failures

One thing is clear: *ignorance is no longer an excuse*. So, what's a business to do? Address the immediate need first:

- **Conduct a Risk Assessment.** To understand whether ephemeral messaging poses a risk to your organization, you need to know how and how often these applications are being used for business purposes. Potential questions to ask in an assessment, which may be in the form of anonymous surveys or small independent focus groups, include:
  - Whether your organization has approved the use of platforms that automatically delete messages at scheduled intervals.
  - Whether these schedules are in line with your organization's record-retention policies and obligations.
  - Whether employees are using unauthorized platforms or devices to circumvent existing controls.
- **Identify Approved Messaging Platforms.** Ephemeral messaging applications can be tempting due to their promises of increased privacy and low cost of deployment, but companies that confuse privacy for security can end up creating liability for themselves.[6] A company's approved secure communications tool should provide end-to-end encryption but security also includes compliance features like data, access and identity controls. Modern encrypted collaboration technologies intended for this use case often address both requirements, but if unable, companies should consider implementing compensating controls like device imaging to meet preservation requirements.
- **Develop Effective Policies and Procedures, Including Consistent Retention Protocols.** While each organization's needs will vary, as a general matter, effective policies and procedures should:
  - Contain device policies that include personal phones and expand the description of retention policies to include text messaging, etc.
  - Explain what platforms and devices are approved for business use with clear consequences for using unapproved platforms or devices. Appoint senior leadership members to oversee and track consequences for violations.
  - Establish and adhere to consistent retention guidelines. The statute of limitations for most federal fraud claims is five years. Securities Exchange Act record retention rules apply preservation periods of at least three or six years, depending on the nature of the records. Investment Advisers Act rules generally apply five-year preservation periods. Guidelines should reflect laws and rules applicable to the organization.
- **Train, Audit, Enforce and Train Again.** Policies and procedures that exist on paper but not in practice will offer little protection if the DOJ comes knocking. Organizations should ask themselves:
  - How are we training our employees on policies and procedures? Are employees required to attend training sessions on newly deployed policies and procedures? Are employees tested on their knowledge of these topics?
  - How are we evaluating our organization's compliance? Are we checking for employee use of unauthorized platforms on company devices? How often are message deletion settings revisited?
  - What steps are we taking to enforce these policies and procedures? Are there realistic disciplinary measures in place for when employees violate these policies? Are these policies applied equally across the organization?

[6] Compliance and Security Considerations Checklist for Consumer Privacy Messengers at Work (armortext.com).

– Are we preserving incident response communications in line with our obligations under record retention rules?

Beyond Retention: Navigating the Future of Messaging Compliance

As regulatory landscapes evolve, it is increasingly clear that enforcement will come to extend beyond data retention. While regulators are currently focused on ephemerality, this is not because regulatory and compliance requirements around retention are the only ones that matter. In fact, regulations across sectors are now more frequently requiring user access controls, multi-factor authentication (MFA), regular comprehensive tests and reviews to ensure organizations have strong access control mechanisms to protect sensitive data and mechanisms to address issues that may arise.

At a minimum, organizations should consider:

- **Developing Effective Policies and Procedures for Reviewing Access.** Messaging applications designed with consumers in mind may lack user management. As a result, organizations should consider policies and procedures to address:
  - Determining which users have enrolled and how to confirm their identities.
  - Determining when accounts or phone numbers may have been spoofed.
  - Removal of departing personnel, providers whose agreements with your organization have come to an end and unwanted parties.
- **Determining Means for Enforcing Password Policies and MFA.** Ephemeral messaging applications without centralized policy management may not provide mechanisms for determining whether strong passwords or MFA are in use. Approved platforms should not run afoul of cybersecurity policies and practices adopted by your organization, as future regulatory actions may include a review of whether approved applications met management's approved security standards.
- **Determining What May be at Risk When Devices Are Lost or Stolen.** While ephemeral messaging applications may provide configurable expiration settings that can be established up front, they may lack capabilities such as remote-wipe. As a result, in cases of lost, stolen or compromised devices, organizations should be prepared to:
  - Determine what messages may still be present on lost or stolen devices.
  - Determine what, if any, expiration settings may still be applicable to messages present on lost or stolen devices.
  - Leverage alternate means, such as mobile device management solutions, if previously installed, to uninstall ephemeral messaging applications remotely while clearing associated data.

The very presence of ephemeral messaging applications within the enterprise poses an inherent risk to companies subject to these compliance obligations, since they are designed specifically to thwart those controls. A lack of consistent framework from regulators to ameliorate these issues, and also establish protocols for retention, further muddy the waters for well-meaning companies and organizations. Seek legal and professional counsel before adopting modern communications technologies that could introduce compliance concerns, as well as assistance in drafting policies, procedures and guidelines aimed to prevent regulatory scrutiny. Beyond avoiding regulatory scrutiny, thoughtful adoption of modern communication technologies designed with enterprises in mind—ones that utilize end-to-end encryption without weakening compliance posture—can mitigate costs associated with systems that will inevitably come under scrutiny.

The future of effective compliance will require more than monitoring software settings. It will require adopting secure, compliance-oriented platforms and robust policies and procedures with clear consequences for employees who conduct business in ephemeral messaging apps like Signal and WhatsApp.

Using Signal or WhatsApp for Work? Here's a Checklist of Compliance and Security Considerations

Consumer privacy: better than nothing...

Consumer messaging apps like Signal and WhatsApp prioritize individual privacy through end-to-end encryption. That means that messages are fully encrypted before leaving your mobile device and aren't decrypted until after reaching your recipient's device.

But, they lack centralized enterprise controls that are crucial for regulatory, statutory, and legal compliance, as well as best practices for organizational security and policy requirements. Signal and WhatsApp have:

- ***No*** centralized user management
- ***No*** audit trails / retained archives
- ***No*** centralized remediation controls (e.g. admin initiated remote wipe)
- ***No*** centralized policy enforcement
- And, ***No*** centralized way to define who can speak with whom

Just a sampling of what you'll need to address with policies, procedures, and compensating technologies...

	Onboarding/Offboarding
	◉ Determine involved conversation participants ◉ Notify conversation owners for participant removal ◉ Alert owners when to shut down specific conversations ◉ Reevaluate participant presence in conversations
	Collection/Reconstruction of Audit Trails
	◉ Collect phones of participants ◉ Manually review and capture relevant communications ◉ Exclude non-relevant communications ◉ Assign responsibility for this activity ◉ Securely store and verify newly reconstructed archives
	Remediation/Risk Reduction
	◉ Disappearing Messages (***Note***: Can impact audit trails) ◉ Adopt Mobile App/Device Managers (***Note***: May incur costs)

	Policy Enforcement
	◉ Implement Endpoint Management ◉ Use Mobile Application Management ***Note***: Costs may apply and may not work on new devices brought in for incident response
	Federation Governance/Participant Management
	◉ Define authorization for adding external participants ◉ Establish conversation participation moderation/ termination ◉ Report unknown/unverified participant additions

Special Note

Given the U.S. Department of Justice's stance on ephemeral messaging, and regulatory actions by the SEC, CFTC, and other international bodies, organizations should emphasize preserving and accessing relevant communications on platforms like Signal, WhatsApp, and iMessage.

Or, find out if ArmorText isn't a better fit for you.

Thank you!