Proposed SEC Cyber Rules for Advisers & Funds

How to prepare, with an emphasis on incident response planning.

Kristin Snyder, Debevoise & Plimpton
Charu Chandrasekhar, Debevoise & Plimpton
Christian Kelly, Xantrion

September 25, 2024

Debevoise & Plimpton

XANTRION
CYBERSECURITY • IT SUPPORT

Before we get started …

Questions are encouraged.

Event recording will be sent next week.

Agenda

1. Introductions
2. Proposed SEC Cybersecurity Rules
3. Cybersecurity Trends
4. Incident Response Preparation
5. Tabletop Exercise

Introductions

Introductions

Kristin Snyder
Debevoise & Plimpton
Partner, San Francisco Office

Charu Chandrasekhar
Debevoise & Plimpton
Partner, New York Office

Christian Kelly
Xantrion
Chief Technology Officer

Debevoise & Plimpton

XANTRION
CYBERSECURITY • IT SUPPORT

Proposed SEC Cyber Rules

A New Cybersecurity Regulatory Regime for RIAs & Funds

Cyber Notification & Disclosure Requirements

- **48-hour** timeline for reporting **significant cybersecurity incidents** to the SEC on Form ADV-C
- **Public disclosure** of significant cybersecurity incidents and cybersecurity risks via Form ADV Part 2A

Cyber Policies & Procedures

- Periodic **risk assessments** of cybersecurity risks
- Controls designed to **minimize user-related risks** and **prevent unauthorized access**
- **Information protection** measures
- **Service provider oversight**, including requiring covered service providers implement the same measures as the RIA/Fund
- Cybersecurity **threat & vulnerability management**
- Cybersecurity **incident response & recovery**

Annual Review & Report

- **Annual review** required of the design and effectiveness of required policies & procedures
- Preparation of **written report** documenting annual review, assessment, and any related control tests
  - In the case of registered funds, a report must be provided to the full board

Books & Records

- Recordkeeping of required policies and procedures, risk assessments, and incident response

A New Cybersecurity Regulatory Regime for BDs & "Market Entities"

Cyber Notification & Disclosure Requirements

- **Immediate notification** required for reporting **significant cybersecurity incidents** to the SEC
  - "Covered Entities" required to provide additional information within **48 hours** via Form SCIR Part I
- **Public disclosure** of significant cybersecurity incidents and cybersecurity risks via Form SCIR Part II

Cyber Policies & Procedures

- Periodic **risk assessments** of cybersecurity risks
- Controls designed to **minimize user-related risks** and **prevent unauthorized access**
- **Information protection** measures
- **Service provider oversight**, including requiring covered service providers implement the same measures as the BD/Market Entity
- Cybersecurity **threat & vulnerability management**
- Cybersecurity **incident response & recovery**

Annual Review & Report

- **Annual review** required of the design and effectiveness of required policies & procedures
- Preparation of **written report** documenting annual review, assessment, and any related control tests

Books & Records

- Recordkeeping of required policies and procedures, risk assessments, and incident response

Amendments to Reg S-P

Applies to broker-dealers, RIAs, & funds

Expanded Scope of Safeguards & Disposal Rules

- Expanded definition of covered "customer information"
- Application of Safeguards & Disposal Rules to transfer agents

Cyber Notification

- **Notification to affected individuals within 30 days** of becoming aware that their personal information has been or is reasonably likely to have been accessed or used without authorization

Cyber Policies & Procedures

- **Incident response program**
- **Service provider oversight**, including requirement for service providers to provide notification of incidents no more than 72 hours after becoming aware of the breach

Annual Privacy Notice

- New exception from requirement to deliver annual privacy notice

Books & Records

- Recordkeeping of required policies and procedures, incident response, and service provider contracts

Outsourcing Rule Obligations

- **DUE DILIGENCE**
- **MONITORING**
- **RECORDKEEPING**
- **DISCLOSURES AND CENSUS-TYPE INFORMATION**
  New Requirements for Form ADV, Part 1A
- **THIRD-PARTY RECORDKEEPING**

SEC 2024 Exam Priorities

Information Security & Operational Resiliency

Reg S-ID Policies & Procedures

Firmwide Cybersecurity (Across Branch Offices)

Vendor & Third-Party Risk Management

AI Risks

Cybersecurity Trends

Cybersecurity Trends

- AitM credential stuffing
- Ransomware
- Risks from AI
- Increasingly tailored phishing, including targeting of executives
- Unpatched systems
- Attacks targeting sensitive financial events
- Vendor security issues

Frequency of Data Breaches by Initial Attack Vector	
Stolen/Compromised Credentials	16%
Phishing	15%
Cloud Misconfiguration	12%
Unknown (Zero-Day) Vulnerability	11%
Business Email Compromise	10%
Malicious Insider	7%
Social Engineering	6%
Known Unpatched Vulnerability	6%
Accidental Data Loss	6%
Physical Security Compromise	6%
System Error	6%

Source: IBM Security, Cost of a Data Breach Report 2024, p. 13

Risks of Generative AI

Quality Control

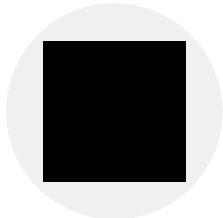
Transparency and Ethics

Regulatory Risk (new and existing)

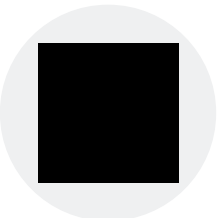
Contractual Compliance

Conflicts, Hiring, ADM, & Other Existing Regulations

Privacy & Confidentiality



Intellectual Property



Vendor Management

Incident Response Preparation

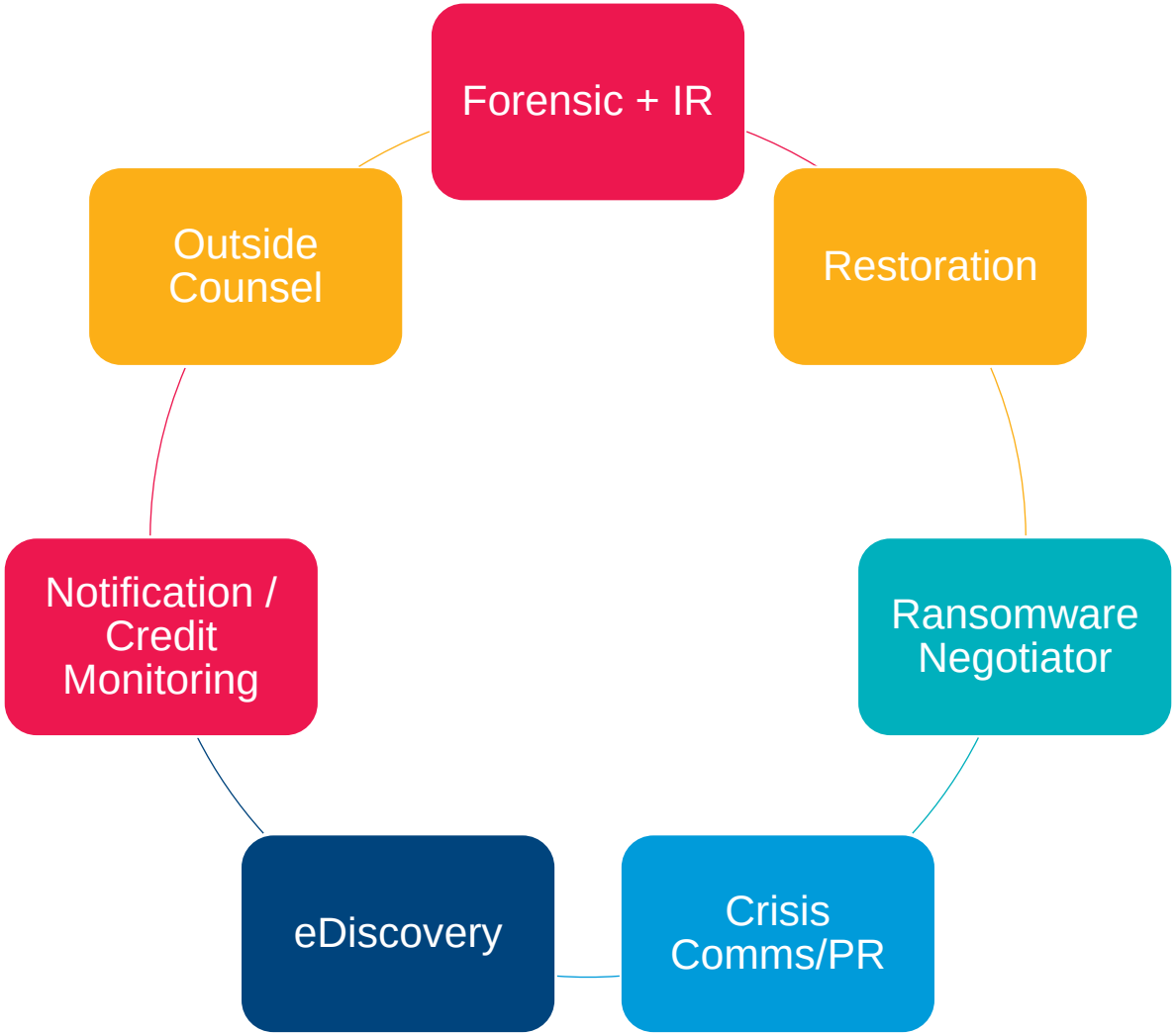
Incident Response Preparation

Non-technical preparations

Vendor Engagement (cyber forensic, crisis comms)	Incident Response Plan + Playbooks	Operational Decision-Making Preparation	Communications (strategy, templates)
Law Enforcement	Notification Obligations Assessment	Negotiation Preparation	Sensitive Information Protection Measures
Training (handling sensitive data, phishing)	Cyber Insurance Coverage	Tabletop Exercise	Establishing Contacts (law enforcement, regulators)

Incident Response Preparation

Vendor Coordination



Incident Response Preparation

Technical preparations

Periodic Penetration Testing	Comprehensive, Air-Gapped Backups	Backup Restoration Sequencing & Testing	Managed Endpoint Detection & Response	Managed Identity Monitoring
Network Segmentation	Lateral Movement Detection	SIEM & Logging	Continuous Security Monitoring	Privileged Access Management
MFA & Trusted Devices for Data Access	24/7 SOC Threat Response	Encryption of Sensitive Data (in transit + at rest)	Process for Deleting Old Data	DLP Controls for Bulk Exfiltration

Tabletop Exercise

Tabletop Exercise – Background Facts

1. Global institutional asset manager.
2. Over $30 billion assets under management.
3. Headquartered in London, with a large presence in New York and offices around the world.
4. Primary data warehouse is managed centrally in Ireland.
5. Systems are backed up live on an hourly basis.

Tabletop Exercise – Unfolding Events

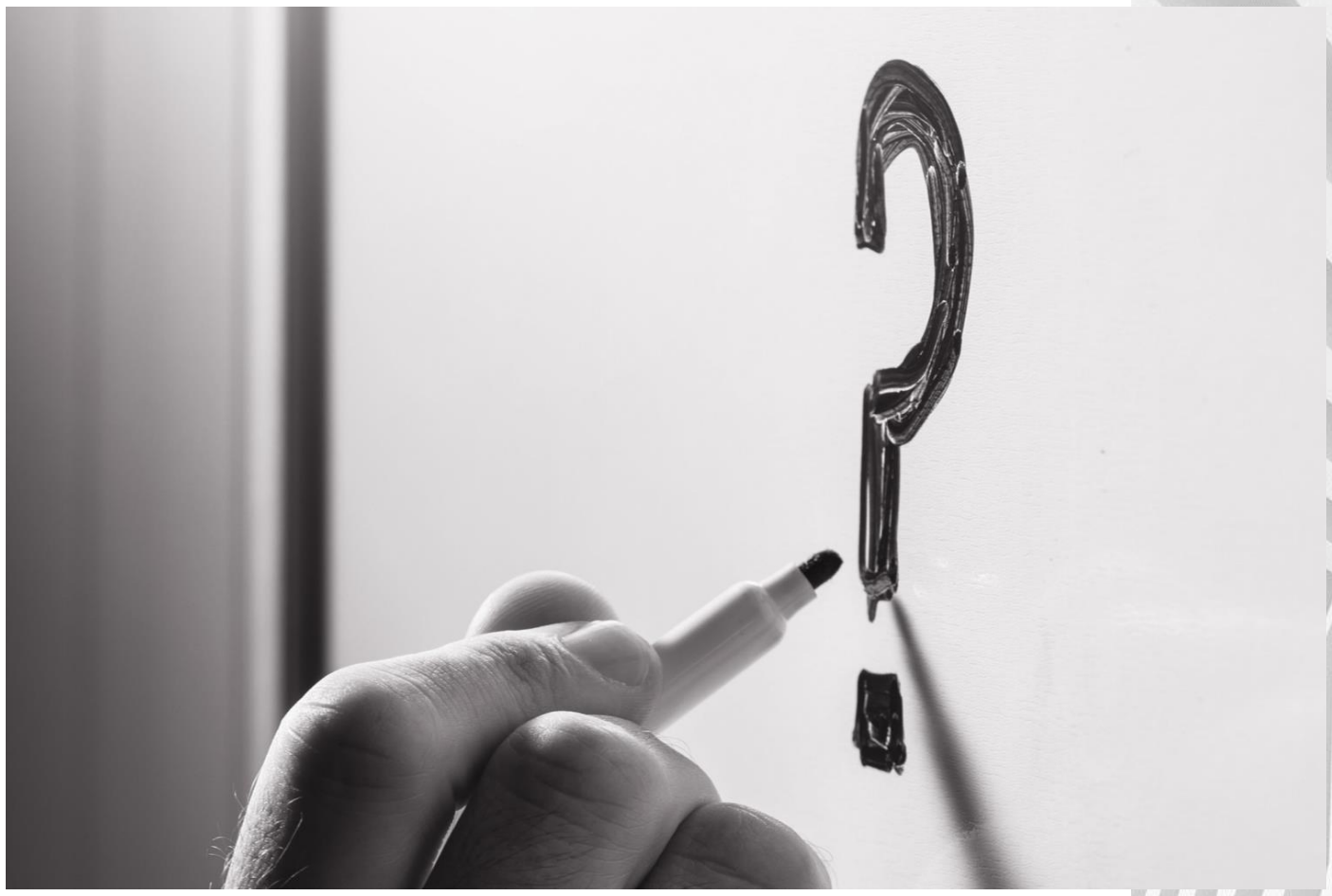
August 19 – September 23, 2024

- On August 19, the company's incident response team receives an **alert from CrowdStrike** that four computers have been **infected with malware** that could be associated with ransomware. There are no reported system impacts or outages, no operational impact, and the impacted devices have been contained.
- On September 23, after further review, the incident response team sends the following note to a risk officer:
  - On August 19 we found malware on four computers. They were cleaned and no operational impact resulted. On September 18, the incident response team identified five more computers with the same malware from August 19. The investigation now reveals that an attacker managed to exploit an unpatched vulnerability and used Remote Desktop Protocol (RDP) to gain access to an employee laptop. The laptop belongs to an employee group that works in London and provides support across our businesses.
  - We conducted a forensic review and believe that there was limited access to the laptops or beyond the laptops. The malware contains signatures consistent with many types of attacks. However, the laptops include only a few files containing employee contact information and compensation data and that information is in a separate folder for which there is no evidence of access or of data exfiltration.
  - Upon being alerted to this, our response team reset the relevant passwords and is working to patch the vulnerability. The response team has found no other indication of malicious activity tied to this event.
- The Risk Officer calls the CISO.

Tabletop Exercise – Round 1 Questions

September 23

- Would you expect to learn about the CrowdStrike alert?
- What does this CrowdStrike alert mean for your role?
- Would you expect the COO or CISO to call you?
- Does this require escalation outside of Legal/Compliance? Does this require notification externally? To LPs? Other third parties?
- Would you notify any regulators?
  - The ICO, Irish DPC, or other EU regulators?
  - Does this trigger SEC notification obligations under any of the proposed rules? Who is involved in these determinations?
- What additional information do you need to know?



Tabletop Exercise – Unfolding Events

September 24

The company suffers from a **ransomware attack shutting down system access**. All access to investment and Limited Partner data is down. Online trading services are unavailable. While essential trading may be possible to a limited extent over the phone, any quick reaction to market events will likely be delayed. Email is available but may have been compromised.

The company holds a wealth of confidential Limited Partner data, including personal data (name, contact information, account information), lists of sovereign wealth fund investors, investment plans, books of investor portfolios and trading activity, investment data from pension funds, as well as proprietary information, including trading strategy and algorithms, compensation data, and asset management fees. The extent to which this data may be compromised is unclear.

Online backups have been encrypted. A number of offline backup tapes exist, but their operational status is not currently known.

A ransom note, readme.txt, appears on the affected systems.

Tabletop Exercise – Readme.txt File Appears on Network

September 25, 1:00 AM

~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

>>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

---BEGIN ID---
Ns5WQ4hUEqxZRO4Ls1WW8wn8K95FKrkEKLxyjXjdwmjbpLosviDzWlNlarhNiY
---END ID---
~~~

Tabletop Exercise – LockBit Ransomware-As-A-Service

- Initial contact with LockBit reveals a request of $1M.
- LockBit claims they also stole 3.2 TB of data and offers to show the contents of two files if company provides names of two encrypted files.
- Ransomware negotiator says that they can likely bring the payment down from $1M to as low as $250,000, but such negotiation will take about 10 days. The earlier the payment is made, the more it will be.
- The amount of time to restore the system with the encryption key from LockBit appears to be 5 days, plus 2 days for integrity testing, if desired.

Tabletop Exercise – Unfolding Facts

September 25

Company decided to engage with LockBit. The sample data provided by LockBit relates to businesses in Europe and the U.S., and appears to include the U.S. employee compensation data from 2023.

The CEO reports that she and her family received multiple suspicious calls at home and threatening emails within the last day, demanding ransom payment.

The incident identified on August 19 was not the root cause, but activity associated with an ongoing attack. The initial attack vector is still being identified, but relevant logging activity only goes back for 30 days.

Due to flat network and domain trusts, a server accessed in one business unit allowed access into the wider business infrastructure.

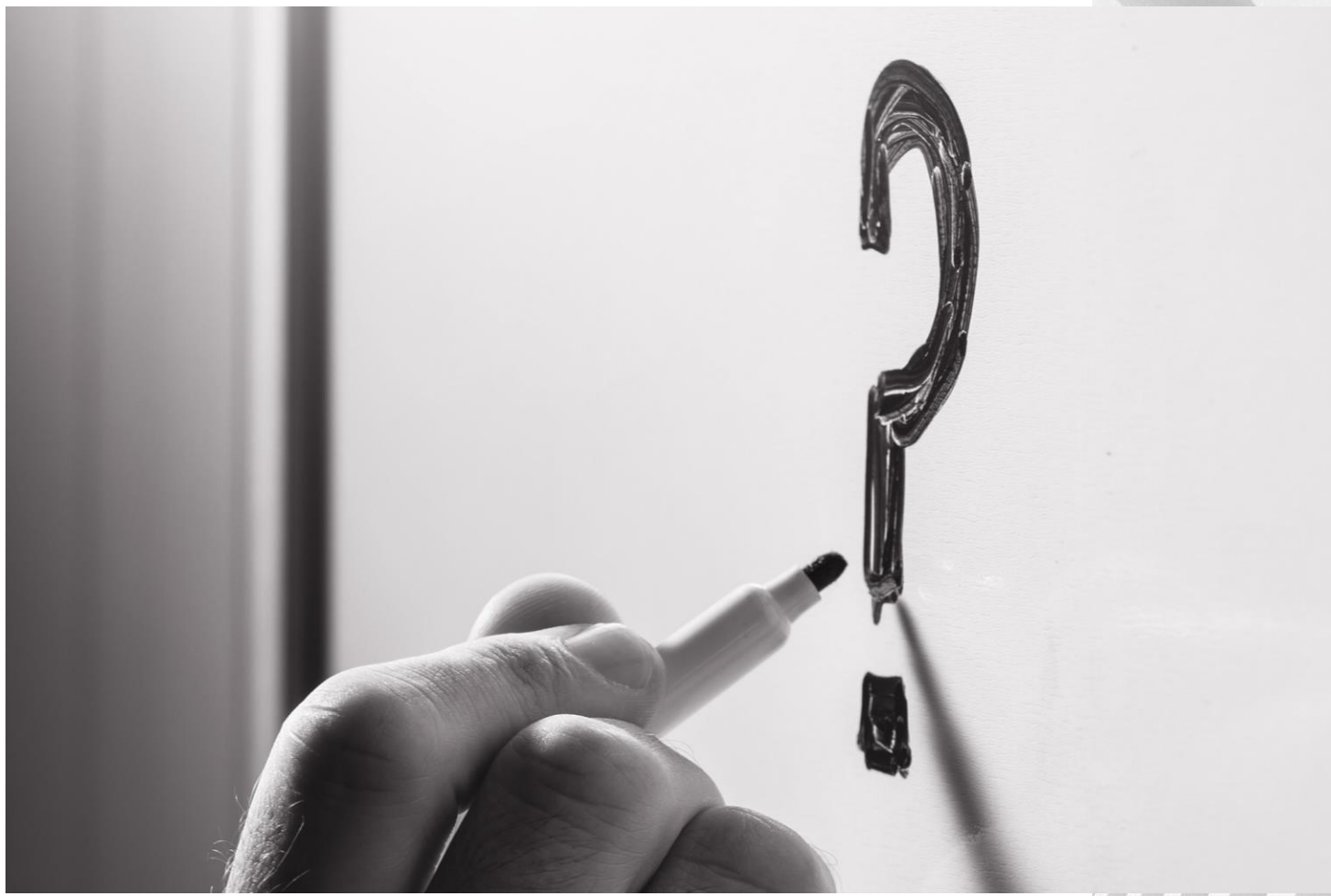
Forensics have identified a number of account credentials that were used by the hacker, and one in particular with privileged access to a global server hosting data across all businesses.

Logging for that server is only kept for 30 days. Within those 30 days, we see the account query about 1,000 records relating to Limited Partners associated with businesses across 10 countries. However, we believe the account also logged into that application numerous times prior to 30 days back. There is **no evidence of exfiltration** of the data.

Tabletop Exercise – Round 2 Questions

September 25

- What internal and external notifications / communications will you make? What will you tell employees?
- How do the factual developments impact your analysis of notification under proposed SEC rules?
- How would you determine if the ransom should be paid?
- How do you address LP questions, like:
  - What data was involved? Sensitive or personal data?
  - Did you or will you pay a ransom?
  - What remediation efforts were undertaken? What controls have been put in place?
- What do you still not know about the incident?



Q & A

Kristin Snyder

Partner, Debevoise & Plimpton (San Francisco)

kasnyder@debevoise.com
(415) 738-5718

Kristin Snyder is a litigation partner in Debevoise & Plimpton's San Francisco office and member of the firm's White Collar & Regulatory Defense Group. Her practice focuses on securities-related regulatory compliance, examinations and enforcement matters, particularly for private investment firms and other asset managers. Prior to her role at Debevoise, Ms. Snyder served at the SEC for 18 years, most recently serving as the Deputy Director of the Division of Examinations resident in its San Francisco Regional Office. In her role, she spearheaded the development of examination priorities for the national and international examination programs covering a spectrum of SEC registrants including investment advisers, investment companies, and broker-dealers. At the Commission, she also served as National Associate Director of the Investment Adviser/Investment Company (IAIC) Examination Program, and as the San Francisco Regional Office's Associate Director for Examinations. In these roles and her Deputy Director role, she oversaw more than 1,000 employees in the Division of Examinations, directed the SEC's Private Funds Unit, a specialized group within the exam program that has conducted hundreds of examinations of many of the largest and most complex private funds managers in the world, and managed referrals of examination findings from the Division of Examinations to the Division of Enforcement. She also led the SEC's National Examination Program Office for the IAIC Examination Program, which develops priorities and initiatives covering investment advisers, including private fund managers, and investment companies.

Charu Chandrasekhar

Partner, Debevoise & Plimpton (New York)

cchandra@debevoise.com
(212) 909-6774

Charu A. Chandrasekhar is a litigation partner in Debevoise & Plimpton's New York office and a member of the firm's White Collar & Regulatory Defense and Data Strategy & Security Groups. Ms. Chandrasekhar has significant experience representing global financial institutions, private equity firms, hedge funds, broker-dealers, public companies, and audit and accounting firms in a broad range of securities-related government investigations, examinations, and enforcement matters. She frequently represents clients before the SEC, FINRA, and PCAOB and has defended matters involving allegations of securities fraud, investment adviser and broker-dealer regulations, cybersecurity, artificial intelligence, accounting and corporate disclosure issues, and whistleblowers. She also advises public companies, investment advisers, and broker-dealers on the development and implementation of policies designed to ensure compliance with the federal securities laws, and has substantial experience in counseling clients on the SEC's cybersecurity regulations, recordkeeping requirements, and artificial intelligence examinations and enforcement. Ms. Chandrasekhar previously served as an Assistant Regional Director in the SEC's Division of Enforcement and as the Chief of the Division's Retail Strategy Task Force. Ms. Chandrasekhar also served as a Senior Advisor and Senior Counsel in the Division of Enforcement's Market Abuse Unit. Prior to joining government, Ms. Chandrasekhar clerked for the Honorable Sonia Sotomayor when Justice Sotomayor sat on the U.S. Court of Appeals for the Second Circuit.

Christian Kelly

CTO, Xantrion

ckelly@xantrion.com
(510) 558-8269

Christian Kelly is the Chief Technology Officer for Xantrion and a Certified Information Systems Security Professional (CISSP) with over 22 years of IT experience. During his 12 years as CTO at Xantrion, he has developed Xantrion's Managed Security program and currently oversees the security and compliance group. He is responsible for ensuring the availability and security of client systems as well as conformance to regulatory requirements. Christian also serves as the point person for Xantrion and client security incidents.

Xantrion's dedicated teams — including technical experts and strategic advisors — work closely with our clients to develop a thorough understanding of their unique business needs and challenges. Our unwavering commitment to building deep, enduring partnerships with clients allows us to provide customized, proactive IT solutions that address clients' immediate concerns while also aligning with their long-term business objectives.

By combining our industry-specific expertise with cutting-edge technology and a proactive approach to IT management, we help clients navigate the changing digital landscape, stay ahead of potential threats, and ultimately achieve their goals.