

Setting the Table for Minimizing Liability in Data Breaches

ACC San Diego

Sharon R. Klein, Partner, Blank Rome
Linda Kornfeld, Partner, Blank Rome
Alex Nisenbaum, Partner, Blank Rome
Benjamin Bresnick, Managing Director, Ankura
Lisa Taylor, Managing Director, Ankura

May 25, 2023
La Jolla, CA

Cyber Situation Manual – Days 1-2

Day 1 

IT conducts their routine review of intrusion detection system logs and discovers unusual traffic on your organization's printer ports. There is a significant amount of data leaving the printer ports and going to external IP addresses.

Day 2 

Employees notice several cosmetic changes to the organization's website and report to IT. They also note that a commonly used link now directs users to an unrelated website. They do nothing with this information.

Cyber Situation Manual – Day 3

Day 3 **09:00** AM

Computers throughout your organization now display a blank red screen. A ransom message then appears demanding \$ 2M Ransom Amount worth of bitcoin for the decryption key and a warning that the key will expire unless payment is received within 48 hours. This event is reported to IT immediately.



BLANKROME

Cyber Situation Manual – Day 4 – Pt. 1

Day 4


09:30 AM

A security researcher uncovers a series of posts from a well-known hacker group on the Dark Web and contacts your IT organization. The researcher believes that the posts are legitimate, and the threat actors have gained access to personally identifiable information (PII), including **employee social security numbers, bank account and routing number information, etc.** The hacker group has provided a small number of data records to verify their claims and are willing to sell the information for “the right price.” The CIO is made aware of the situation and brings in the FBI.



BLANKROME

Cyber Situation Manual – Day 4 – Pt. 2

Day 4 

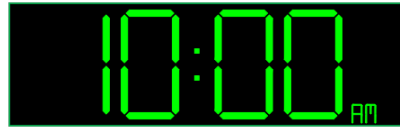
Today your organization files its normal securities/SEC filings stating that it has not had any security incidents in the past year.



BLANKROME

Cyber Situation Manual – Day 5

Day 5

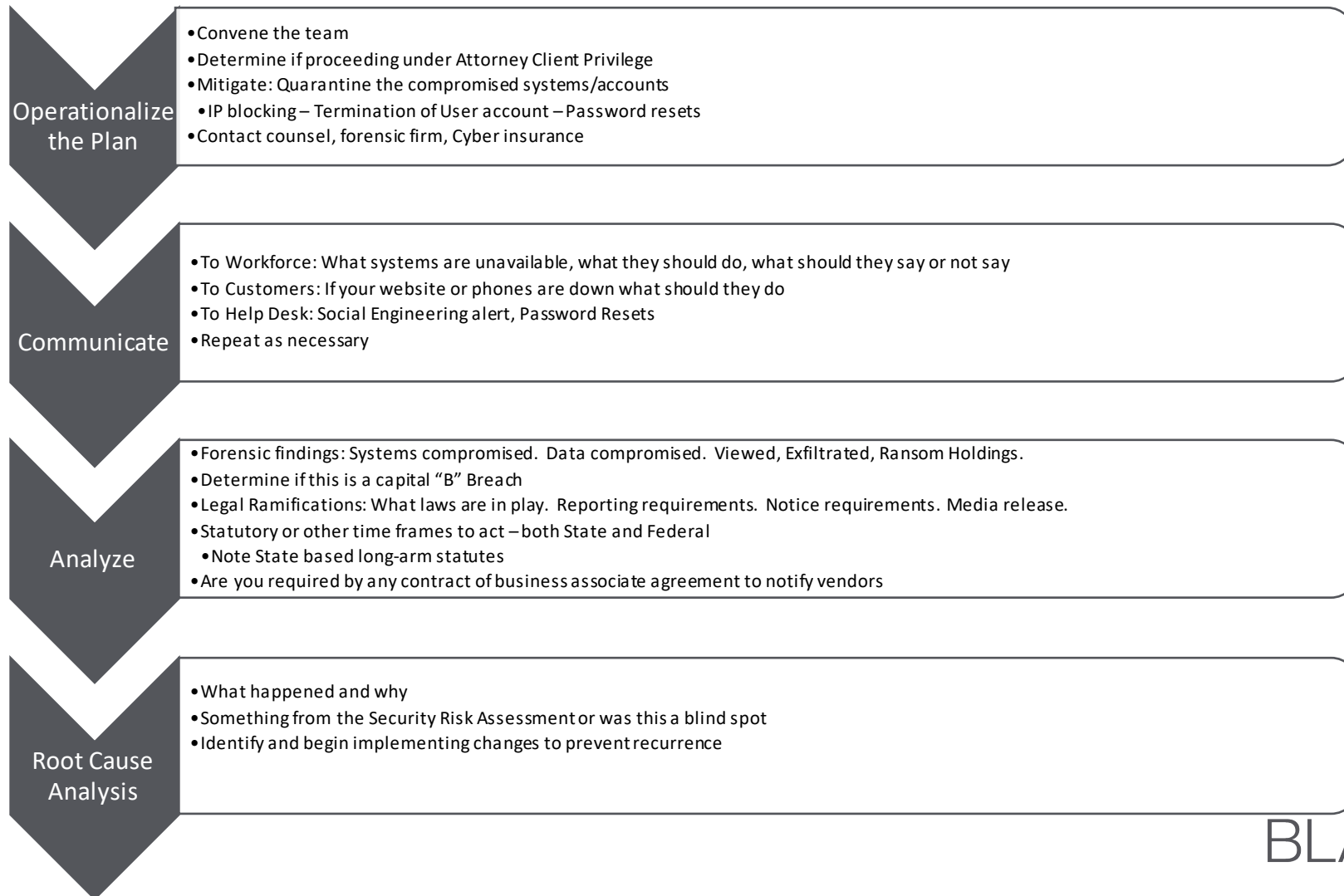


Immediately the tag **#<Insert Organization>HACKED** goes viral on multiple social media platforms. Several news media outlets contact your organization seeking comment about your ransomware infection and the data breach.



BLANKROME

Steps to Consider When Facing a Possible Breach



BLANKROME

Top 6 Things That Lower Cyber Risk

- Annual Risk Assessment
- Awareness and Training
- Cyber Crisis Management Team/ Table-Top Exercise
- Strategic IT Investments
 - Assessments
 - Multi-Factor Authentication
 - Intrusion Detection
 - Redundant Data Back-Up
- Vendor Management Security Commitments



BLANKROME

Presenters

BLANKROME



Sharon R. Klein

Sharon.Klein@blankrome.com



Linda Kornfeld

Linda.Kornfeld@blankrome.com



Alex C. Nisenbaum

Alex.Nisenbaum@blankrome.com

ankura 



Benjamin D. Bresnick

benjamin.bresnick@ankura.com



Lisa Taylor

Lisa.Taylor@ankura.com

BLANKROME

Sharon R. Klein – Blank Rome



Sharon R. Klein

Partner, Chair, Orange County Office
Chair, Privacy, Security & Data Protection
Orange County, CA
Sharon.Klein@blankrome.com

- **Sharon Klein** advises businesses on assessing and mitigating risks related to the privacy and security of personal data, ownership, and commercialization of data artificial intelligence; planning, drafting, and implementing privacy, security, and data protection policies and “best practices”; compliance with global, federal, and state privacy and security laws, regulations, and rules; data governance; and breach response, crisis management, and remedies for non-compliance. She is certified as an information privacy professional by the International Association of Privacy Professionals.
- Sharon has deep experience in negotiating and drafting complex technology and cloud transactions, licensing, and strategic IT and commercial agreements. She is active in many organizations involved in technology, data privacy and security, and health information.

Linda Kornfeld – Blank Rome



Linda Kornfeld

Partner, Co-Chair, Insurance Recovery
Los Angeles, CA
linda.kornfeld@blankrome.com

- **Linda Kornfeld** is one of the nation’s most prominent insurance recovery attorneys, representing corporate policyholders in high-stakes litigation for more than 25 years. Using strategic, creative approaches in her trial and appellate practice, Linda assists her clients in the recovery of hundreds of millions of dollars in insurance assets. She is a strategic adviser to senior executives and in-house counsel on mitigating risk and maximizing insurance recoveries.
- Whether through settlement or trial, Linda cost-effectively resolves complex insurance matters for her clients, such as:
 - Losses related to the COVID-19 pandemic
 - Data breach and privacy issues
 - Directors’ and officers’ liability
 - Business interruption and extra expense
 - Employee fidelity
 - Professional errors and omissions
 - Employment
 - Entertainment industry liabilities
 - Intellectual property infringements
 - Construction defects
 - Asbestos, environmental, and product liabilities

BLANKROME

Alex C. Nisenbaum – Blank Rome



Alex C. Nisenbaum

Partner, Privacy, Security & Data
Protection
Orange County, CA
Alex.Nisenbaum@blankrome.com

- **Alex Nisenbaum** advises clients on data privacy and information security laws and regulations, including compliance with HIPAA/HITECH; Gramm-Leach-Bliley; the California Consumer Privacy Act; cross-border data transfer; and state privacy, data protection, and breach notification requirements. Alex is able to synthesize the patchwork of state and federal legal requirements to assist clients in bringing innovative products to market and operationalize compliance programs that are in line with their business goals.
- He handles technology and data privacy and security matters in a variety of industries, including healthcare, FinTech, financial services, pharmaceutical, medical device, consumer goods, e-commerce, and manufacturing.

Benjamin D. Bresnick - Ankura



Benjamin D. Bresnick
Managing Director
Chicago IL, 60606
benjamin.bresnick@ankura.com

- **Benjamin D. Bresnick** is a Managing Director in the Chicago office, specializing in healthcare compliance and regulatory matters. An attorney by background and former hospital executive who has served in numerous leadership roles over two decades in healthcare, Ben combines his former legal expertise with hands-on managerial experience to help clients navigate the complexities that exist where operational considerations touch governance and regulatory constraints.
- Ben is a trusted advisor to boards of directors seeking counsel on fiduciary duties, the business judgement rule, and setting risk appetite, among other critical issues. He also guides healthcare providers in creating enterprise risk-management programs that consider risks holistically -- from compliance, governance, and patient care -- to better measure the contributing factors and to recommend ways to keep them in check.

Lisa Taylor - Ankura



Lisa Taylor
Managing Director
Chicago, IL
lisa.taylor@ankura.com

- **Lisa Taylor** is a Managing Director at Ankura based in Chicago. She has over 22 years of experience in privacy, audit, risk assessment, leadership reporting, and development of overall compliance and ethics programs in both healthcare and manufacturing.
- In addition to working at Ankura, Lisa teaches breach reporting and privacy effectiveness at privacy academies offered by the Health Care Compliance Association. She also is an adjunct professor at Xavier University teaching healthcare legal aspects in the masters in healthcare administration program.

Resources

Privacy Security Download



Biometric Privacy Insider Blog

