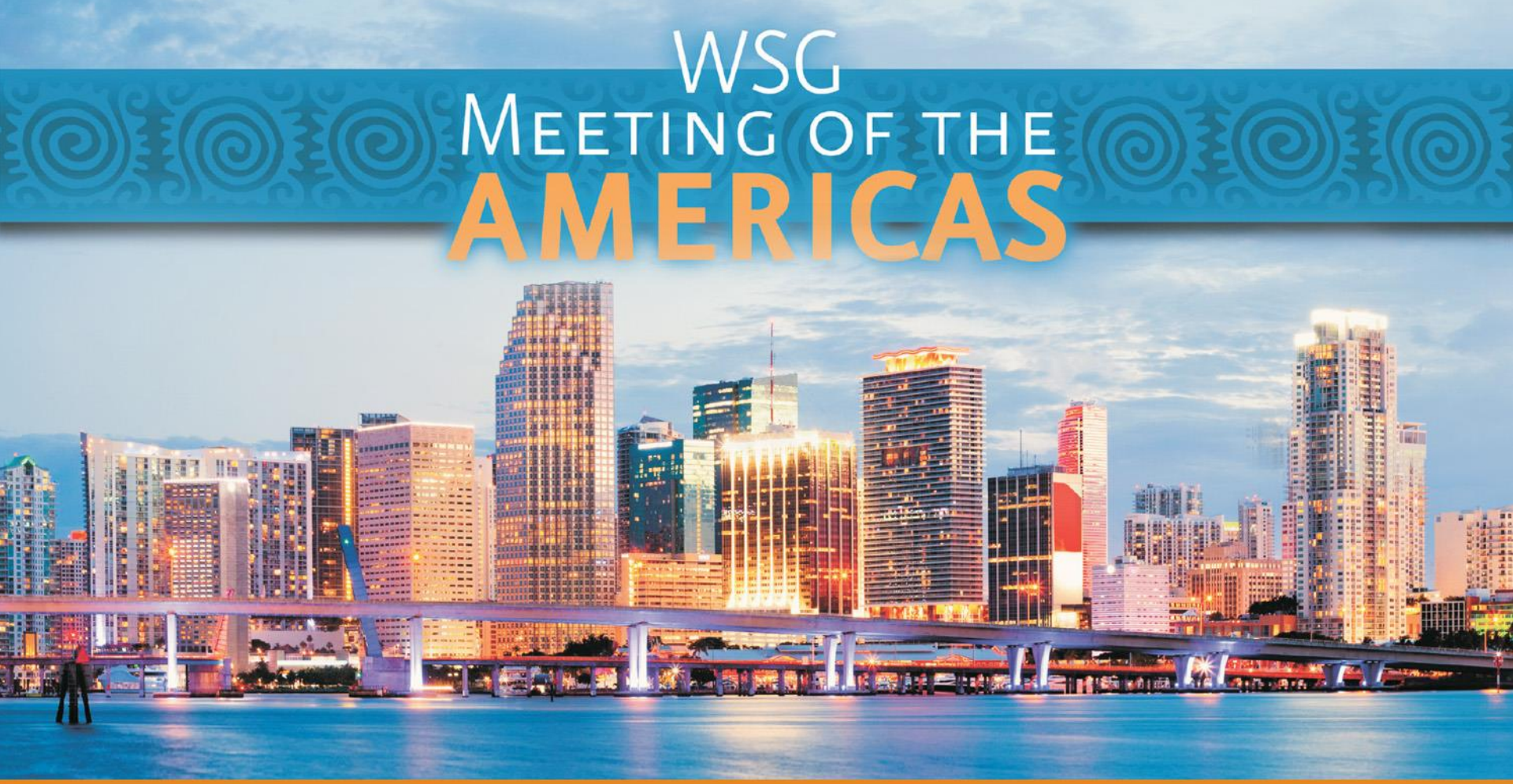
WSG
MEETING OF THE
AMERICAS



MIAMI, FLORIDA

WSG
World Services Group

GrahamThompson
Attorneys

HOET PELAEZ
CASTILLO & DUQUE

MOORE STEPHENS

Cifuentes, Lemus & Asociados, S.C.
RIF J-00296621-1

WSG MEETING OF THE AMERICAS

Cyber Security – International Technology Intelligence and Info Management

GUEST SPEAKER PRESENTATION

Timothy P. Ryan
Managing Director
Kroll

2014 Cybersecurity Guidance to Professional Services Firms

Four Part Outline

1. Anatomy of a Computer Intrusion: How Kroll Hacked a Professional Services Firm
2. Top 10 Mistakes Companies Make When Preparing For and Responding to a Breach
3. Top 5 Mitigation Techniques Against Targeted Attacks
4. Case Study of an Insider Attack and the Use of Multifaceted Investigative Techniques

Download this presentation at:
http://information.kroll.com/timryan

Anatomy of a Computer Intrusion:
How Kroll Hacked a Professional Services Firm

How Kroll Cyber Security Broke into a Professional Services Firm

- Kroll was retained to breach the IT network of ACME Widgets to demonstrate how the company was susceptible to attacks.
- Kroll received the consent of the target company's management.
- ACME Widgets normal website was: ACME.com
- Kroll purchased the name ACME.co for about $10.

ACME.co

What Kroll did:

- Created ACME.co to look exactly like ACME.com
- Created the ACME login page
- Used LinkedIn to find employees of ACME.
- Reviewed the ACME website to create a password reset email

The Phish and Intrusion

- Sent the email to employees and had them “reset” their passwords into the fake ACME site. At this point we had a lot of usernames and passwords.
- With the “stolen” passwords Kroll gained access to corporate workstations, emails, and the company Intranet. Kroll also placed temporary backdoors on the machines so that a password reset would not lock us out.
- During the breach, Kroll had access to corporate legal information, client data, and M&A data.
- Kroll exported the entire company directory (over 7,000 employees) to target additional employees.

Top 10 Mistakes Companies Make When Preparing For and Responding to a Breach

Escalation and Employee Security Awareness

- Define how incidents should be reported and escalated
- Case: Intrusion identified 2 months prior to significant destruction

The Need to Preserve Evidence: Competing Interests between Get it Working Again and Preserving Evidence

- The hotel room murder where the hotel cleans everything up and notifies later.

The Ability to Preserve Evidence: Forensic Collection Capabilities

- Many firms can make images but their ability to analyze is not sufficient.
- How to make images in a forensically sound manner versus how the sys admin normally does it.
- How to scale the investigation.
- Comparison of old methods versus current continuous monitoring and diagnostics

The Ability to Demand Evidence: Third Parties

- Must your vendors tell you when they give your data to another vendor?
- Must your cloud providers tell you when there is a breach?
- Must they give you the evidence?
- Had one that demanded legal process.

Log Creation and Centralization

- What and Where are logs
- Why they matter
- Why centralization helps

Internal Conflicts of Interest: IT versus Security

- Organizational structure may encourage and allow a white wash
- Mechanic versus investigator

Network Visibility and Architecture

- The unknown server is hard to hard to protect.
- Can you see connections between computers

Containment and Eradication Strategy

- Unable to identify binaries throughout the enterprise
- Unable to rapidly segment the network

Incident Response Plan

- Actions, People, Place, Tools, Policies

Backups

- Tested
- Backups to respond to data destruction
- Ransomware is proliferating. Backups is one of the only ways to recover if you can’t prevent it.

Top 5 Mitigation Techniques Against Targeted Attacks

Top 5 Mitigation Techniques

- Patching OS
- Patching Third Party Software
  - » Java
  - » Adobe Reader
  - » Flash
  - » Web Browser
- Restriction on Administrative Rights
- Application Whitelisting
- Two Factor Authentication for Remote Connections

Case Study of an Insider Attack and the Use of Multifaceted Investigative Techniques

Why This Case Is Important

- Forensics alone won’t solve the problem.
- Incident Response should look to mitigate damage by dealing with both the technology and the criminal.
- Incident responders should be both technically proficient and trained in investigations.

The Company: ACME Logic

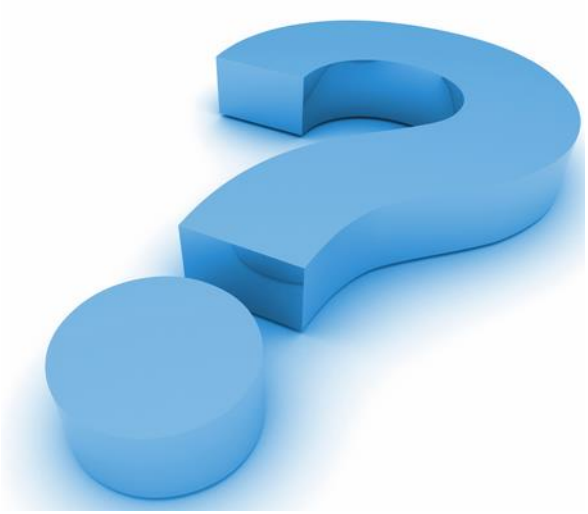
- Very profitable financial institution using proprietary algorithms
- Had strong information and physical security measures. VDI, multifactor authentication, biometric physical access controls, CCTV.
- Incident response was not as developed as were the security controls.

What was Reported to Kroll

- AV alert: Attached USB
- CCTV review showed Joe over 2 weekends
- Joe had been fired
- How he got in

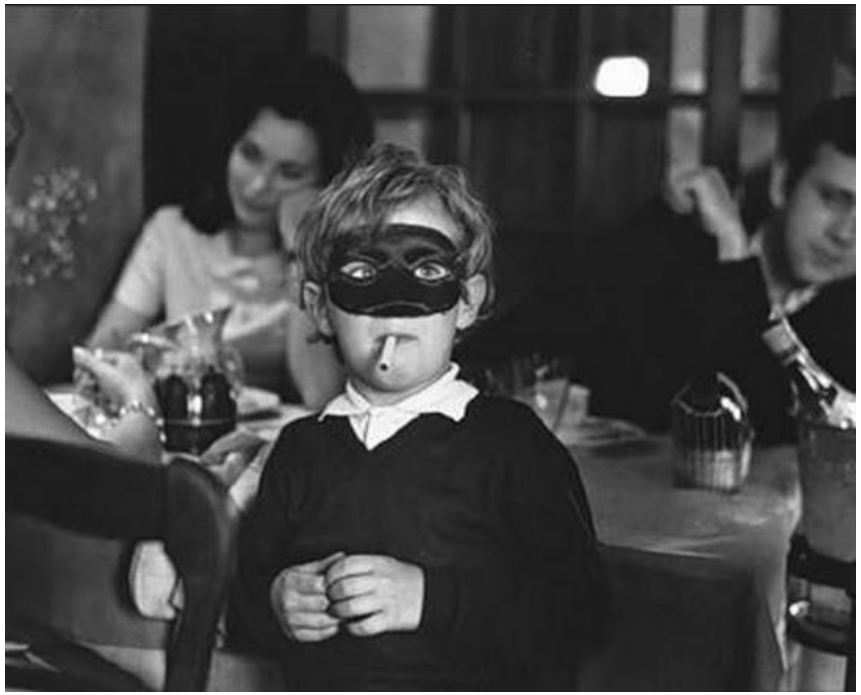
Scope and Complications

- What the company wanted Kroll to determine
- Complicating factors



What was Known About the Subject

- Joe had been employed by the company for approximately 2 years.
- Had low work performance.
- Was a foreign national in the US on a work visa.



How Kroll Responded

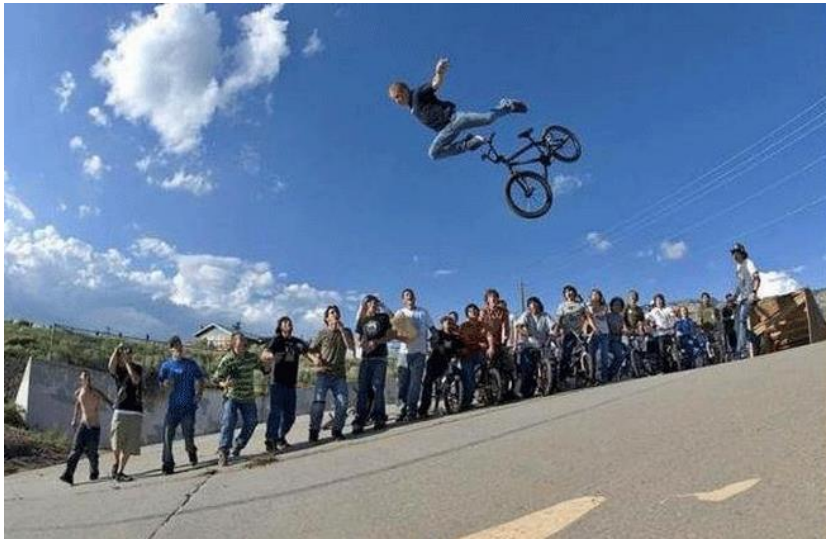
- Initial Forensics
- Search of his former work space
- Phone and email logs
- CCTV Review
- The Ruse

The Ruse

- Designed to enlist the subject's cooperation
- Consent to enter his house
- Obtain the data he took from the company

Introduction, Interview, and Confrontation

- CEO warm up
- Introduction of Kroll
- Minimization of conduct
- Use of confrontation material



Confession and Consent

- Joe confessed to taking the papers
- I advised that we needed to retrieve the papers from his house.
- He consented.
- Once we had the papers I told him he had to hand over the USB drives.

Second Interview

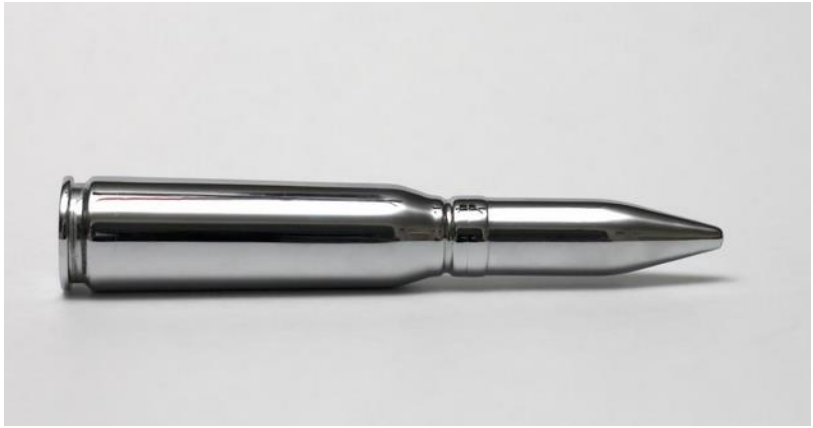
- Centered on motivation and corroboration.
- Refused to discuss previous employment

Forensic Review and Findings

- Immediate access by the company
- Nature and extent of information was determined.
- Algorithms were the target.
- Kroll's finding: the data was copied but never accessed.

Conclusion

- The CEO advised that the company had “dodged a $30 million bullet”
- The proprietary data was recovered.



Kroll

Thank You

Timothy Ryan, Managing Director

Cyber Investigations Practice Leader

Jim Faulkner, Managing Director

Miami Office Head

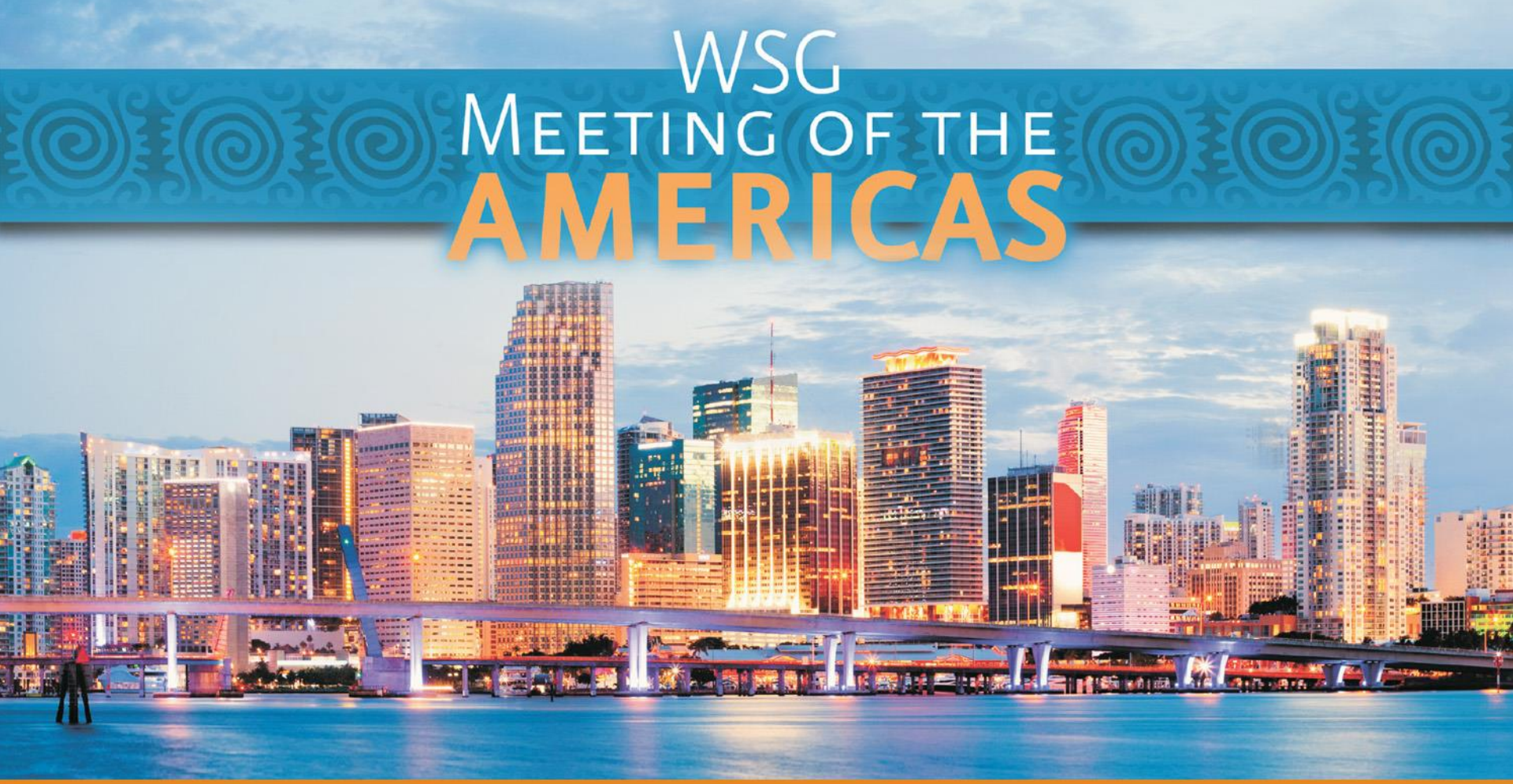
1395 Brickell Avenue, Suite 1150

Miami, FL 33131

305-789-7130 (office) | 786-801-8214 (cell)

jfaulkner@kroll.com

WSG
MEETING OF THE
AMERICAS



MIAMI, FLORIDA

WSG
World Services Group

GrahamThompson
Attorneys

HOET PELAEZ
CASTILLO & DUQUE

MOORE STEPHENS

Cifuentes, Lemus & Asociados, S.C.
RIF J-00296621-1