Cyber Attack Understanding the Risk

A guide to the questions to ask your team to verify readiness

February 2021

Private and Confidential

KROLL

Why should State treasurers' care about Cyber attack?

Preservation is your mission

"Preserving public trust and capital through effective management of our cash resources."

The costs and trust risk involved in:

- Improper handling of data
- Poor protection of physical systems
- Loss of system support to State Stakeholders
- Loss of State funds

WHY YOU NEED TO CARE

City of Atlanta- Ransomware attack

- Government computers shut off for 5 days
- 1/3 of city software programs disabled.
- Thousands of legal documents deleted
- Police dashcam video files deleted
- Residents made to pay their bills by paper.
- $2.7 million paid to contractors in order to recover
- $9.5 million in additional recovery costs

Presentation Agenda

01
The Threat

Overview of the threats

- Focus on Ransomware
- “Cyber Attack for Profit”

02
PLANNING

Questions to Ask your team

- Help identify risks
- Prepare for an attack.

03
Legal issues

Regulatory Risks

- Security Standards
- Federal Response to Ransomware

04
Incident Response

4 Stages of an Incident

- Understanding the stages of an attack
- Understanding your role

05
Protections

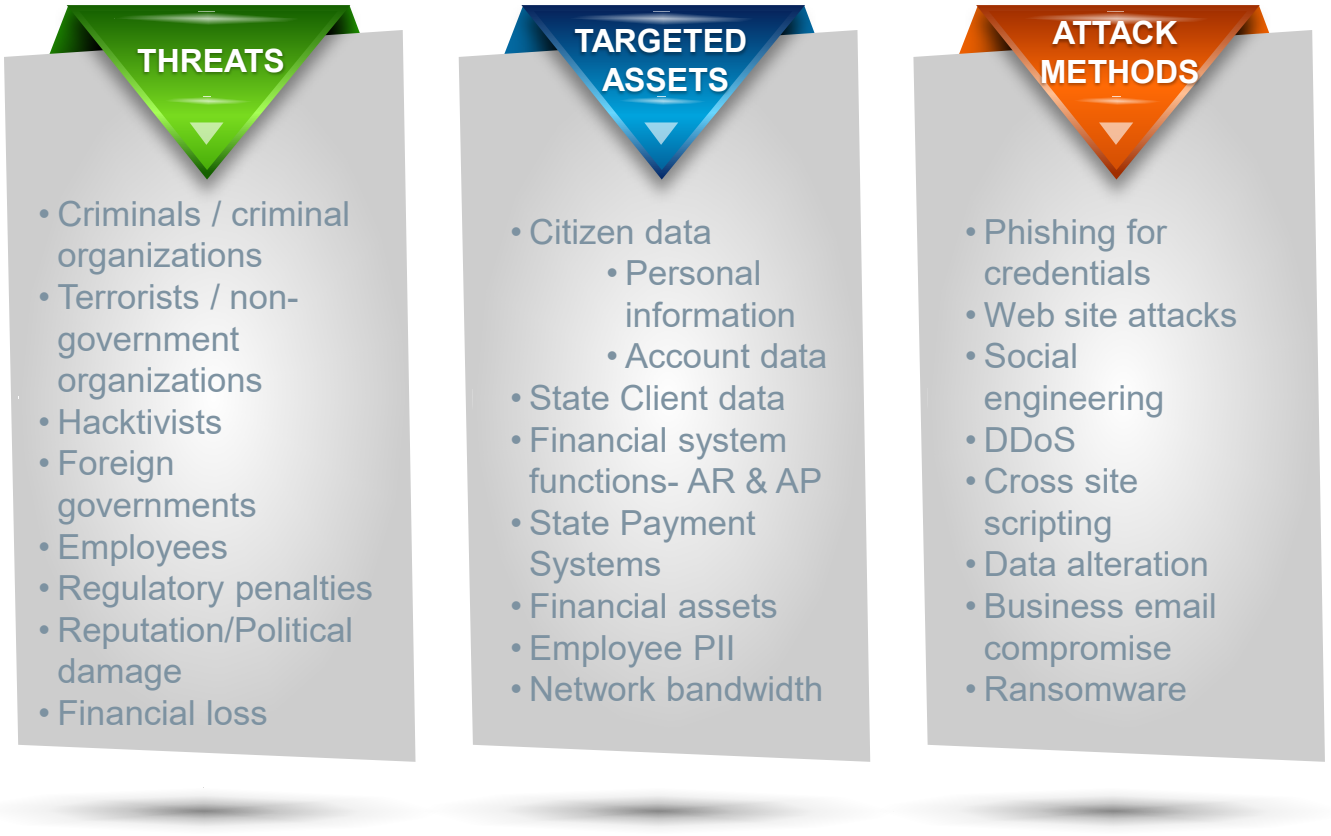
Practical Steps

- Backups
- Whitelisting
- Patch Management
- Access Control
- Endpoint Monitoring

1 The Threat

Cyber Attack for Profit

Cyber Threat Landscape



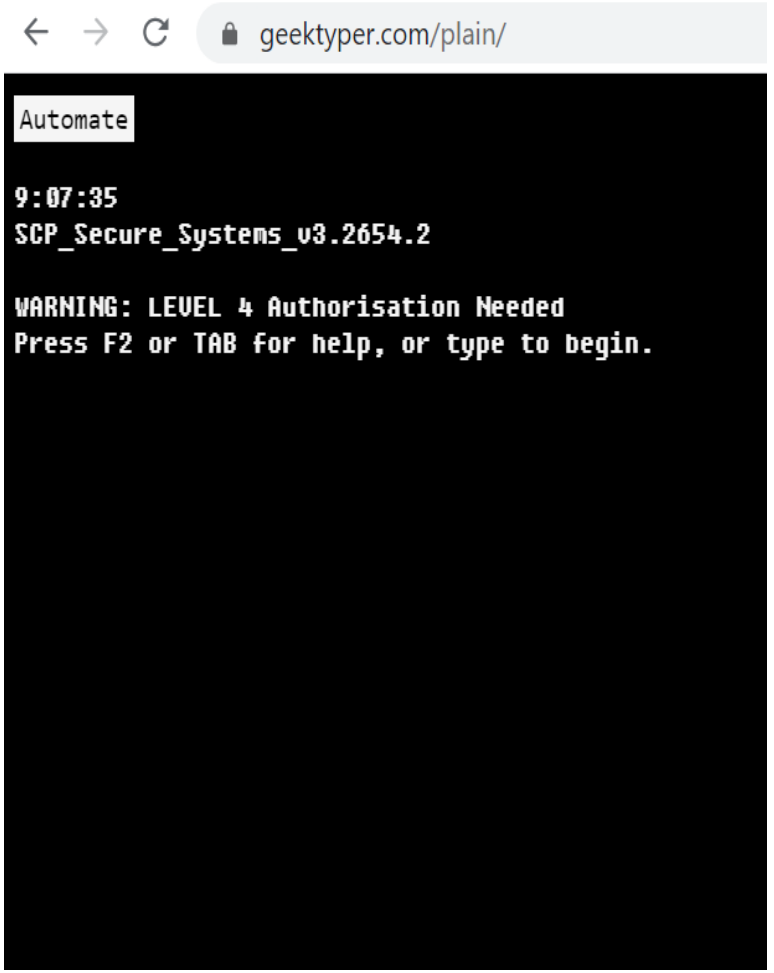
Social Engineering Fraud

- More Dangerous Than Ever
  - Only as strong as your weakest link
  - Must be right 100% of the time
- Types of Attacks
  - Phishing
  - Spearphishing
  - **Delivery and Technical Account Scams**

Delivery and Technical Account Scams

Amazon, Apple, Google and FedEx

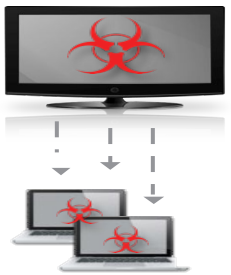
- Pandemic modified scams
  - Victim receives call from person claiming to be from Amazon/Apple/Google/FedEx
  - States there is issue with account
  - Feeds back contact data to victim
  - Offers to trouble shoot account
  - Provides link to enter to ‘see’
    - Link is actually automatic code to share computer with threat actor
  - Once threat actors has access- they show fake ‘attack data’
  - Attacker Uses access in background to enter firm site



NEW RANSOMWARE TACTICS

Hacking skills increasing within specialized groups- with targeted attacks

Persistence and lateral movement



Attackers are “living” off the network tools- and using existing FTP or transfer protocols to transfer data

Backup Destruction Email Monitoring

The attackers are monitoring emails, and destroying backups to force payment

Data review for pricing, data theft for Blackmail

Attackers are reviewing finances to cost payment. Data is taken to threaten shame if payment not made

LATEST ATTACK VECTORS

MalDoc Pfishing

Fake FedEx, Dropbox and fake voice mail messages have been joined by fake DocuSign.

VPN / Data transfer targeting

Attackers look for old, unpatched VPN's or data transfer systems and comprise them, allowing for Can Credential theft and even MFA 'seed' harvesting

Data Mining

Data research techniques and password reuse allow for credential bypass

02

Planning

Questions to Ask your Team

Things you need to know from your team to understand where you are the road to cyber security

.

What data and systems must we protect?

Data inventory

What, where, who and why?
Do we know what data we have?
How long are we keeping it?
Where are we keeping it?
Why are we keeping it?

The test

Can we inventory our data in real time, and control access?

Verification ‘Asks’

Data inventory/Map, Data classification policy, Data Loss Prevention (DLP) tools, Data Retention policy, Data use policy

Verification methods

Audit committee, third party audit

ELECTED ISSUE: Avoid keeping state financial data that can contain PII connected to networks for longer than operationally needed

Where is our data, and Who can access it?

What third parties hold state data?

Data transfer tools, Cloud Services, PCI services, Web hosting providers, Banks and payment systems

Due Diligence?

Contractual right to access, Duty to assist, Regular security review

Verification points

Legal review of vendor contacts that hold data, Copies of vendor security assessments

Verification methods

Include 3rd parties in testing; Ask for regular security updates, Onsite inspection of 3rd party

ELECTED OVERSIGHT: Ensure that third parties meet the same security standards as the State, and budget for auditing of the controls on a regular basis.

Can we identify attacks quickly?

Have we defined an incident?

Use State resiliency and data protection regulatory requirements to guide the definition of incident.

Notification

What are the ways we get notified about incidents?

Verification points

Review and discussion of Incident definition; Periodic review of system alerts, SOC/NOC escalation, Threat or vulnerability report

Verification methods

Audit- internal & third parties

Elected OVERSIGHT: Review the definition of an incident with management team to ensure that focus is directed on the proper financial risks

Have we the ability to respond quickly?

Do we have an IR team?

Who are the key members? Legal counsel, Senior management, CISO

Team Leader?

Decision-making authority, Familiarity with the IR Plan

Verification points

IR team org chart, IR plan documentation, Training plan, IR response software, Playbooks

Verification methods

Tabletop exercise, Red team testing, Review of testing reports

ELECTED OVERSIGHT -: Ensure that management has in place the ability to respond to data issues (team & plan)

Pre-Breach Work - Refining the Incident Response Plan

Have you reviewed the Incident Response (IR) Plan?

- Does it define what an incident is?
- Does it establish a team with decision-making authority?
- Does it define criteria for declaring an incident?
- Does it define criteria for escalation?
- How often is it tested?
- How is it deployed?

Pre-Breach Work - IR Team Vetting

How to evaluate preparedness

Do we have an IR team?

- Who are the key members?
  - Legal counsel
  - Senior management
  - CISO
  - PCI implementer
  - Others

Who leads the team?

- Decision-making authority
- Competence
- Familiarity with the Incident Response Plan

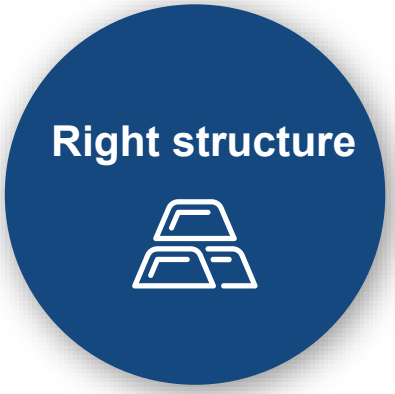
What is the team's purpose?

- Reduce business risk to the organization
- Minimize the impact of an incident on the reputation, operations, and finances of the organization if an incident occurs

Are we providing effective support to the IR team?

- Are we providing continuous training to the team and our staff?
- Does the team have access to all business units and groups?
- Does the IR team have access to details about vendor security?
- Has the IR team identified all third-party dependencies?

Preparation: Is this risk properly managed?



Who is responsible for cyber security?

Who do they report to?, Do they have their own budget?, Do they have the right staff?, Are they cross silo?

Governance & Planning

Is there a governance framework?, Is there a cyber defense strategy and growth plan?

Verification points

Assigned staff position, Reporting lines, Staff org chart, Budget, Written governance framework, Written cyber defense plan

Verification methods

Board presentation by staff, Audit of governance by third party

ELECTED OVERSIGHT: Review the governance of data and security with management to ensure that it is being overseen by a specific team member who can report to the senior team.

Preparation: Is help lined up?

Existing relationships?

With an IR firm?, Crisis PR firm?, Privacy law firm? Law Enforcement?

Existing MSAs?

Verification points

MSA with firms, Participation in local task forces

Verification methods

Board presentation from 3rd party, Board presentations for local LE, Working with them in training and assessment work

ELECTED OVERSIGHT: Ensure that external resources have contracts pre-approved for state contracting

Preparation: Ensure training

Train the IR team

Mock IR response. Red teaming, Yearly cyber fire drill

Train management

Tabletop exercises, Security awareness Training

Train the Elected

Quarterly cyber updates, Elected should complete the same security awareness training

Train staff

Regular security awareness, Quarterly security refreshers, Social engineering tests, Yearly cyber fire drill

03

Legal and regulatory risk

What Constitutes Reasonable Security?

The 20 Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet.

The failure to implement all the Controls that apply to an organization's environment **constitutes a lack of reasonable security**.

California Data Breach Report (Feb 2016) Attorney Gen. Kamala D. Harris

Top 20 Critical Security Controls

1	Asset Inventory
2	Software Inventory
3	Secure Hardware & Software Configurations
4	Continuous Vulnerability Assessment and Remediation
5	Controlled Use of Admin Privileges
6	Maintenance, Monitoring and Analysis of Audit Logs
7	Email and Web Browser Protections
8	Malware Defenses
9	Limitation and Control of Network Ports, Protocols & Services
10	Data Recovery Capability

11	Secure Network Configurations
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Skills Assessment and Training
18	Application Software Security
19	Incident Response and Management
20	Penetration Tests and Red Team Exercises

REGULATORY SUPERVISION IS INCREASING

Department of Treasury Office of Foreign Asset Control (OFAC)

OFAC

Ransom payment to sanction entity or person – company is strictly liable.

Department of Treasury Financial Crimes Enforcement Network (FINCEN)

Facilitating payment of ransom may require SARS notice and reporting

Department of Justice- Cyber Crime Division

Overview of legal issues when Purchasing Data from Illicit Sources

https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

https://www.justice.gov/criminal-ccips/page/file/1252341/download

FIN-2020-A00X, “Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments,” October 1, 2020

04

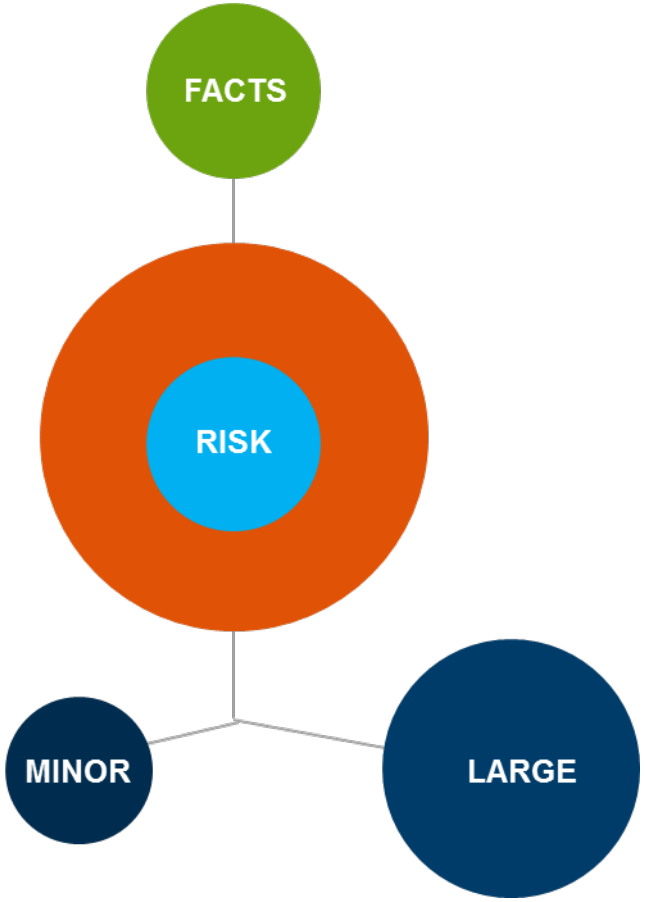
Understanding an Incident Response

Steps involved in a proper response
The Elected’s role in an IR

4 Stages of Incident Response

Determining resources and impact

The act, event or information that starts the process



IT defines the facts

- System accessed
- Facts showing access

Legal supplies the law

- Data type
- Regulatory impact

Business measures risk

- Notice?
- Regulatory effect?
- Customer effect?

Elected makes decision

Implications for the Elected

Responsibilities you cannot shift to IT

1 RESPONSIBLE FOR RISK

If a Cyber risk is raised to you, either mitigate it or risk accept it; do not ignore it.

2 MAKE CYBER RISK A PRIORITY

Make Cyber a regular topic

3 SHOW OVERSIGHT

Get the right metrics on status of security regularly

Review Cyber incident reports to monitor attacks and trends

4 KNOW THE LAW

Get advice on privacy and data regulation in markets you operate

5 GET RISK ASSESSED

- Internally
- By third parties

6 USE KNOWN FRAMEWORKS

- NIST
- ISO
- COBIT

7 TEST RESPONSE

Test the company response

05

Protections

Practical Steps to consider for Protecting networks

1

Back up data regularly and secure backups offline

Backups are essential: if you're infected, a backup may be the only way to recover your data

- Ensure backups are not constantly directly connected to the system they are backing up- add separation and additional credentials.
- Verify the integrity of backups and test the restoration process
- TEST systems regularly

2 Restrictively configure firewalls, use whitelisting and segment your network

Block all but known IP's, applications and users

- Use block list data to identify and Block access to
  - Known malicious IP addresses
  - 'new' IP addresses
  - Ip locations outside customer and user base
- Whitelist applications by verify a business purpose to the application and its use
- Segment the network- If every user and server is on the same network, new variants can spread
- No shared local admin creds!

3

Develop a patching process, regularly update ‘Master’ images with patched software

Patching OS, software, and firmware on all devices minimizes chance of a successful exploit

- Consider using centralized patch-management for regular patching
- Regularly update the standard server and endpoint install to include patches and monitoring tools
- Ratify an emergency patch process for special incidents
- Pay attention to VPN and MFA vulnerabilities

Use a Hardening Guide and Benchmarks

- There are many small steps that can be taken on a computer to disable and secure processes that can be exploited by an attacker.
- Rather than trying to determine the best approach- use the CIS Benchmark system to get a set of updated, free safeguards.
- Make sure that your IT team/provider uses the guides and explains why any hardening step is not being implemented

4

Develop a hierarchy for user permission and data access

Determine what types of users need what types of data and implement controls to limit unnecessary access

- No users should have administrative access unless absolutely needed
- Include system and process accounts in the review
- Physically and logically separate networks and data for different organizational units

Manage Permissions and Active Directory

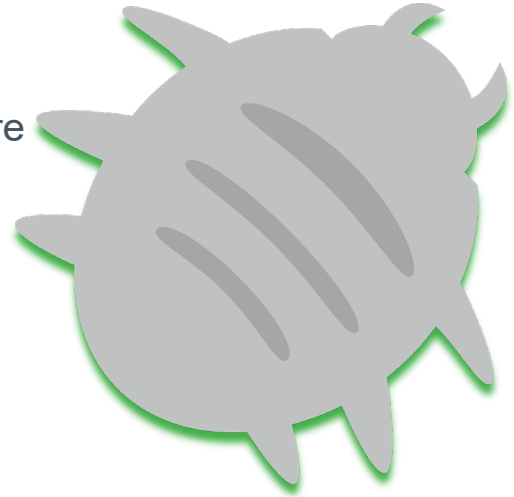
- Who is responsible for deciding the permission levels of staff and processes?
- Who has permission to create new accounts
- What rules do they use to decide permission levels?
- How often do were audit the user accounts against the staff?
- Who gets an alert when a new user account is created?
- How does that person validate the existence of the account?
- What are the settings for AD?
- Who selected them?
- Are they standard?

- The permission provided to users and to processes running on your network must be regularly reviewed
  - Use the least privileged approach- only the permission level needed to do the tasks assigned
  - Regularly audit administrative accounts
  - Create standard limited account permission sets, and require exceptions to permissions must be approved beyond IT
  - Involve HR in reviewing to ensure that all accounts belong to active employees.
- Active Directory must be regularly monitored and cleaned up
- Make sure that you are using MS rulesets, and have a permission process in place to change these rules

5 Engage in Network and Endpoint Monitoring

Next-gen platforms use automation and cloud-based intelligence to back up your best practices

- Inspect files and identify malicious behavior before it strikes
- Block malware and non-malware attacks that exploit memory and scripting languages like PowerShell
- Increase scale and efficiency of highly-touted practices like application whitelisting



Engage in threat detection

- Do we have a monitoring tool watching activity on our endpoints?
- Who reviews the alerts from it?
- How often do they check?
- How were they trained to understand and respond to alerts?
- How do we get alerts on off hours and holidays?
- How did we select things to alert on?

- A key measure of a modern, effective information security program is its ability to rapidly detect **and** effectively respond to an intrusion.
- Given the widespread use of cloud data, detection capacity must exist on desktops
  - Identify and flag known bad executables
  - Analyze the behavior shown on a computer against attack methods and processes
  - Get data from Multiple threat intelligence sources and 'learn' IOC.s
  - Be able to conduct threat hunting and get identification of threats
  - Rapid notification of **validated** threats

6

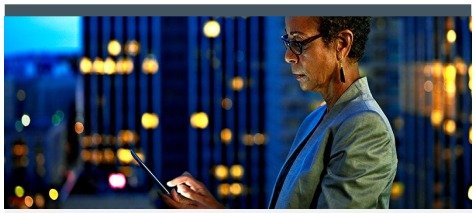
Plan for an attack

Run regular drills to test response capability to recover from and manage with loss of data

- Create a data map and an IR plan that supports it
- Actively supervise your IR plan and team
- Put in place relationships in the event assistance is needed- plan on how to manage vendors

ENHANCING VALUE ACROSS A RANGE OF EXPERTISE

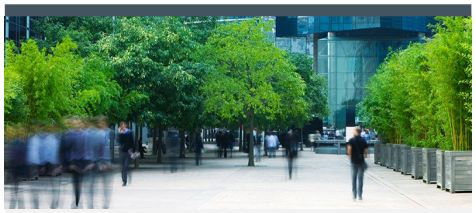
Our service areas



VALUATION ADVISORY

Valuation and consulting for financial reporting, tax, investment and risk management purposes

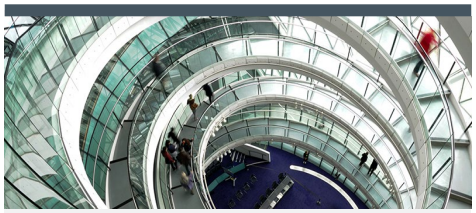
- Valuation Services
- Alternative Asset Advisory
- Real Estate Advisory
- Tax Services
- Transfer Pricing
- Fixed Asset Management and Insurance Solutions



CORPORATE FINANCE

Objective guidance to management teams and stakeholders throughout restructuring, financing and M&A transactions, including independent fairness and solvency opinions

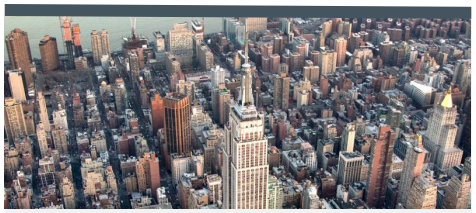
- M&A Advisory
- Fairness and Solvency Opinions
- Transaction Advisory Services
- ESOP and ERISA Advisory
- Private Equity - Financial Sponsors Group
- Distressed M&A and Special Situations
- Private Capital Markets and Debt Advisory



GOVERNANCE, RISK, INVESTIGATIONS AND DISPUTES

Risk management and mitigation, disputes and other advisory services

- Business Intelligence and Investigations
- Compliance and Regulatory Consulting
- Compliance Risk and Diligence
- Cyber Risk
- Disputes Consulting
- Global Restructuring Advisory
- Legal Management Consulting
- Security Risk Management



BUSINESS SERVICES

Complex legal and business solutions through our proprietary technology and team of experts

- Prime Clerk Restructuring
- Kroll Corporate Actions
- Lucid Issuer Services
- Lucid Agency and Trustee Services
- Kroll Class Action Administration
- Kroll Mass Tort Administration
- Kroll Notice Media Solutions
- Kroll Business Technology
- Kroll Agency Cloud

Joseph Marcelonis

Managing Director
Government Solutions

Joseph.Marcelonis@Kroll.com +1 (203) 232-5895

Joseph Marcelonis is a managing director in the Government Solutions practice of Kroll, based out of the New York office. He has over 24 years of experience handling unclaimed property matters.

Joseph joined the firm through the acquisition of Verus Analytics by Kroll in July 2020.

Prior to joining Verus in 2010, Joseph was involved in the day-to-day operations and acted as a client liaison for state clients with the ACS Unclaimed Property Clearinghouse. He developed and improved workflow efficiencies and ensured proper delivery of unclaimed property to clients. He also conducted webinars, provided internal training, and communicated regularly with clients on new developments, important unclaimed property issues and new initiatives.

Jonathan Fairtlough

Managing Director
Cyber Risk

Jfairtlough@Kroll.com | +1 (213)598-4181

Jonathan is a managing director with Kroll's Cyber Security & Investigations practice based in Los Angeles. A member of Kroll's cyber management team, he joined Kroll after a distinguished career with the Los Angeles County District Attorney's Office where he served as both a prosecutor and co-founder of the office's High Technology Division. At Kroll, Jonathan has lead teams for the past eight years that provide comprehensive investigative services for digital forensics, data breach response and complex crimes related to loss of information.

Prior to joining Kroll, Jonathan was the assistant head deputy and co-founder of the High Technology Division of the Los Angeles County District Attorney's Office, a role he held for 13 years. Jonathan has successfully investigated and prosecuted hundreds of hacking, IP and ID theft cases, as well as civil cases for the District Attorney. During his career, Jonathan held a number of positions within the District Attorney's Office and was involved in many high-profile cases, including the first major data breach filed in Los Angeles County for which he received the IAFCI (Southern California Chapter) award for Prosecutor of the Year in 2006.

Jonathan is an internationally known lecturer on the nature and scope of Cybercrime, IP theft and the trends that are affecting businesses globally. He is a regular instructor for the United States Department of Homeland Security's National Computer Forensic Institute, where he teaches classes on the use of Computer Forensics and Cyber Investigations for prosecutors. Mr. Fairtlough is an active member of the California state bar and a Certified Information Systems Security Professional (CISSP).

Gregory Michaels

Managing Director
Cyber Risk

Gregory.Michaels@Kroll.com

+1 (201) 978-1546

Greg is a Managing Director with Kroll's Cyber Risk practice. In this role, Greg partners with clients to build strategic and operational information security programs, comply with regulatory requirements and reduce enterprise risk. Greg has deep experience collaborating across functional units and communicating technical matters to executive stakeholders.

Greg manages a global team of technical, operational and strategic cybersecurity specialists and leads engagements across industries. Services provided by Greg's team include, but are not limited to, network and application penetration testing, vulnerability testing, social engineering, cybersecurity risk assessments, and threat analysis and monitoring.

Prior to joining Kroll, Greg worked as Chief Security Officer for BluePrint Healthcare IT, where he led the Security, Privacy, and Compliance practice and led client HITRUST certification engagements. Previously, Greg worked as an Information Security Analyst for i3 Global (United Health Group), and as a Network and Security Administrator for PXRE Group, Ltd.

Greg holds Master's degrees in Information Assurance from Capitol College and Health and Technology Law from Seton Hall Law School. He also holds a bachelor's degree in Biological Sciences from Rutgers University. Greg is certified as a CISSP, QSA, CISM, CRISC, CISA, PMP, and CBCP, and is a frequent speaker at international security and privacy conferences.

ABOUT KROLL

Kroll is the world's premier provider of services and digital products related to **governance, risk and transparency**. We work with clients across diverse sectors in the areas of valuation, expert services, investigations, cyber security, corporate finance, restructuring, legal and business solutions, data analytics and regulatory compliance.

The firm's nearly **5,000 professionals** are located in **30 countries and territories** around the world.

~5,000

TOTAL PROFESSIONALS GLOBALLY

13,400

CLIENTS INCLUDING NEARLY

48% **OF THE S&P 500**

THE AMERICAS

2,000+

PROFESSIONALS

EUROPE AND MIDDLE EAST

1,100+

PROFESSIONALS

ASIA PACIFIC

850+

PROFESSIONALS

For more information, please contact:

About Kroll

Kroll is the world's premier provider of services and digital products related to governance, risk and transparency. We work with clients across diverse sectors in the areas of valuation, expert services, investigations, cyber security, corporate finance, restructuring, legal and business solutions, data analytics and regulatory compliance. Our firm has nearly 5,000 professionals in 30 countries and territories around the world. For more information, visit www.kroll.com.