Kroll

ESPC
Email Sender & Provider Coalition

Operationalizing Data Security

May 10, 2016

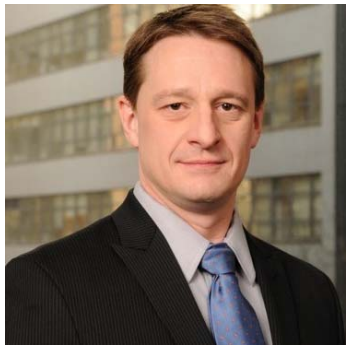
Agenda

1. Bio and Contact Information
2. Kroll Overview
3. Information Security Risk Assessment
4. Operational Security Controls & Processes
5. Security Monitoring & Incident Response
6. Q & A

Kroll

1 Bio and Contact Information

Kroll



Gregory Michaels

Associate Managing Director, Cybersecurity and Investigations
Kroll

+1 201.978.1546
gregory.michaels@kroll.com

300 Harmon Meadow Boulevard, Suite 305
Secaucus, NJ 07094 USA

Greg Michaels is an Associate Managing Director with Kroll's Cybersecurity practice based in Secaucus, NJ. In this role, Greg partners with clients at the strategic and operational level to build proactive information security programs helping them to comply with regulatory requirements and reduce risk according to organizational needs. Greg has deep experience collaborating across functional units and communicating technical matters to executive stakeholders.

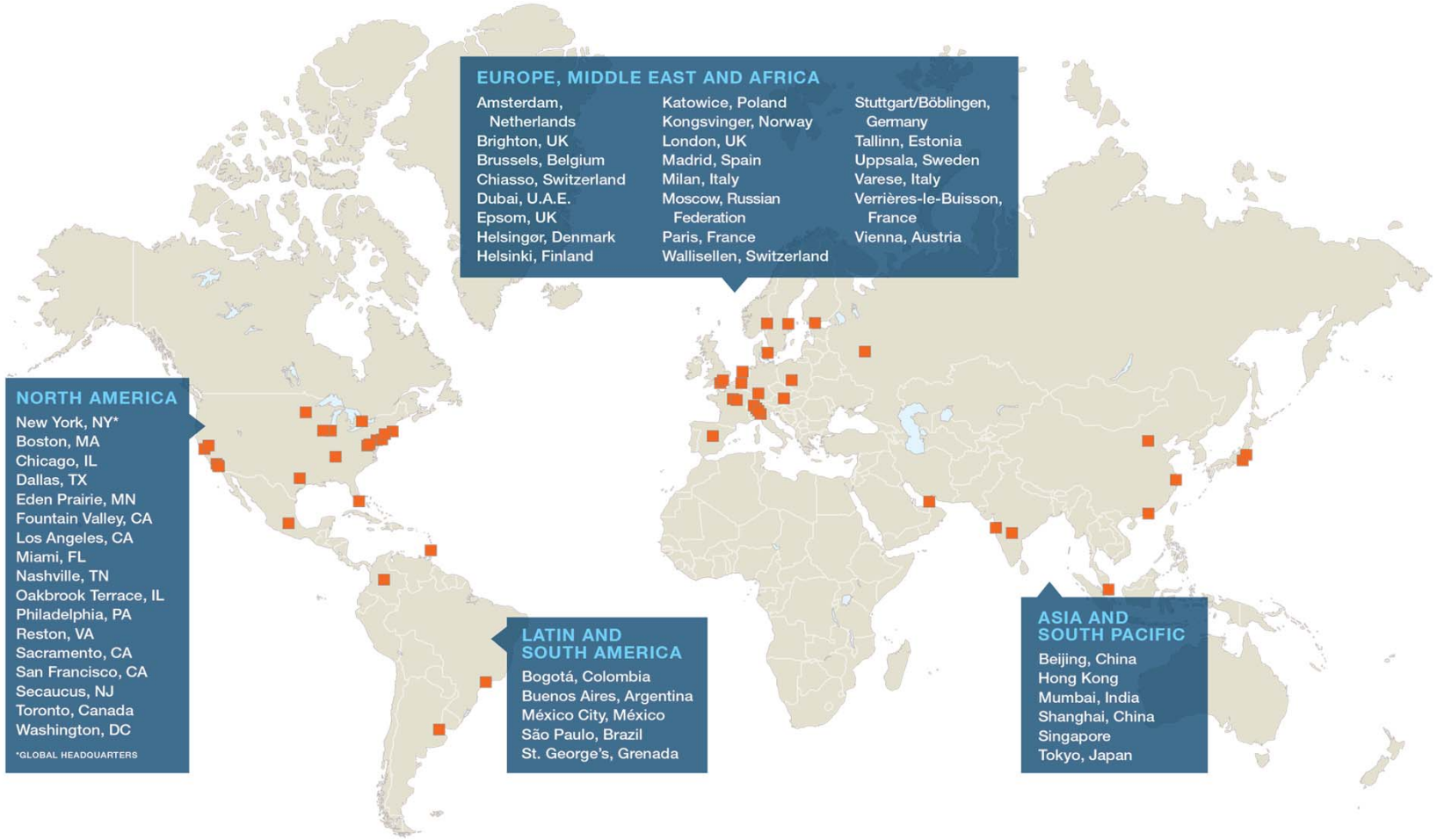
Prior to joining Kroll, Greg worked as Chief Security Officer for BluePrint Healthcare IT where he led the Security, Privacy and Compliance practice for more than five years. Previously Greg worked as an Information Security Analyst for i3 Global (United Health Group) and as a Network & Security Administrator 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 Science from Rutgers University. Greg is certified as a CISSP, CISM, CRISC, CISA, PMP, CBCP and a HITRUST Practitioner and is an active participant in HIMSS, NJ-HIMSS, HFMA and ISACA and a frequent speaker at security and privacy conferences.

2 Kroll Overview

Kroll's Global Footprint

A 40+ Year History of Handling IT-Focused Threats and Compromises



Kroll

Lessons Learned

- Cyber events are inevitable
- Proactive vs. Reactive – Approach is key to readiness and resiliency
- Difficult to quantify cyber risk, and no common standards exist
- One size does not fit all

Kroll

3 Information Security Risk Assessment

Kroll

Pre-Assessment – Information Gathering

- Determine organizational risk profile
- Determine scope and timeframe
- Identify critical information assets
- Identify where these assets are located
- Identify who manages and who has access to these assets
- Identify what regulatory requirements are relevant
- Select an information security framework

Assessment - Overview

- Review policies and procedures
- Review previous assessment reports and remediation activity
- Review network diagrams
- Review system and device standard configurations
- Review third party contracts and Cyber Insurance policy
- Identify security management solutions in place
- Identify security detection and response capabilities

Assessment – Policy Categories

Information Security Strategy	Business Continuity Management
Security Risk Management	Disaster Recovery Management
Access & Account Management	Incident Response & Management
Training & Awareness	Systems Development Security Management
Asset Management & Data Classification	Application Security Management
Physical Security	Third Party Security Management
Systems & Network Security	Mobile Device & Media Security Management
Security Audit & Monitoring	Personnel Security
Cyber Vulnerability Management	Acceptable Use
Change & Patch Management	Retention & Destruction

Assessment – Interviews & Walkthroughs

- Interview IT teams
- Interview System Development teams
- Interview key third parties that host or access critical assets
- Interview key business unit leaders throughout the organization
- Conduct physical security walkthroughs of the perimeter
- Conduct internal security walkthroughs
- Conduct third party site visits (if applicable)

Assessment – Technical Review

- Evaluate security controls for systems, network devices, applications, databases, etc.
- Compare controls and processes to policies and procedures
- Evaluate training and awareness methods, content and frequency
- Conduct routine vulnerability assessments
- Conduct periodic penetration testing with social engineering
- Evaluate monitoring, detection and response capabilities

Assessment – Ratings & Recommendations

- Rate risks by probability of occurrence and impact to the business in order to prioritize
- Create manageable recommendations with identified solutions
- Identify options as necessary based on the risk profile
- Document security controls and processes that meet framework standards
- Document recommendations in a risk register for tracking

4 Operational Security Controls & Processes

Kroll

Executive Role

- Determine capability and level of involvement
- Lead the Development of the Risk Profile
- Provide support for the Security program
- Lead by example
- Start the conversation
- Insist on regular updates
- Identify escalation points

Strategic Security Program

- Designate person Responsible for Security (e.g. CISO)
- Policies and Communication
- Cyber Insurance?
- Executive Leadership Risk Committee
- Training and Awarenes
- Enterprise Risk Management (include third parties)
- Proactive and Continuous Monitoring
- Incident Response and Management

Security Controls & Processes

- Remove local administrator access
- Two-factor authentication
- Review and revise access controls for the network, systems, applications, databases, web sites, etc.
- Patch network devices, systems, applications, databases, etc.
- Ensure that endpoint malware protection is updating
- Utilize encryption for data in transit and at rest
- Restrict media access and destroy paper-based data

Security Management Solutions

- Security Information and Event Management (SIEM)
- Endpoint Threat Analysis
- Data Loss Prevention (DLP)
- Intrusion Detection/Prevention System (IDS/IPS)
- Encryption
- Mobile Device Management (MDM)
- Email Security

5 Security Monitoring & Incident Response

Kroll

Logging & Auditing

- Ensure that logging and auditing are enabled where possible
- Retain logs for at least 6 months but 1 year is better
- Implement centralized log management capability
- Track access activity (especially privileged access)
- Create alerts for high priority log events
- Audit periodically to ensure relevance and accuracy

Security Event Monitoring

- Monitor access to critical assets and information
- Monitor endpoints and network devices for potential security events or incidents
- Monitor perimeter devices for signs of intrusion
- Monitor remote access into the organization
- Monitor third party access
- Monitor mobile devices

Incident Response

- Identify core and secondary stakeholders
- Determine internal technical capabilities
- Identify third party stakeholders
- Develop IRP and align with DRP/BCP
- Conduct periodic tests through table-top exercises
- Update plan as necessary

Continuous Security Process

- Conduct risk assessments often (at least annually)
- Measure results and track remediation
- Scheduled Vulnerability Testing (monthly)
- Penetration Testing (at least annually)
- Security Monitoring (continuous)
- Training & Awareness (continuous)
- IRP/DRP/BCP Testing (at least annually)

6 Q & A

Kroll

Gregory Michaels
Associate Managing Director
Cybersecurity and Investigations
T: +1 201.978.1546
gregory.michaels@kroll.com