Cybersecurity and Incident Response – Practical Issues and Lessons Learned

Robert H. Edwards, Jr., Jon Neiditz & Keith Omsberg

October 31, 2014
1. Using the secrets & lies about privacy & cybersecurity to your advantage.

2. Why cybersecurity will be a key to protecting the value of your company.

3. Current situation and future risks with cybersecurity and the electric grid.

4. Cybersecurity in payments and national defense.

5. Your future in information governance & knowledge asset protection.
Privacy & Cybersecurity Have Become THE Top Concern for GCs

Regulatory issues presenting the greatest risk
- Data privacy law 61%
- Industry-specific regulation 50%
- Anti-corruption laws 31%
- Affordable Care Act 25%
- Labor laws 25%
- Dodd-Frank Wall Street Reform and Consumer Protection Act 25%
- Environmental laws 20%
- Antitrust laws 14%
- SEC Conflict Minerals Disclosure Rules Act 13%
- Other 7%

Top 3 cybersecurity and data privacy concerns
- Customer/client data privacy 57%
- Unknown and unidentified risks 49%
- Legal compliance with data security laws 46%
- Potential for undetected breaches 42%
- Employee and workplace data privacy 42%
- Payment card protection 19%
- Health care privacy 19%
- Cross-border data transfers 19%

Respondents were able to select more than one answer.

Source: Grant Thornton LLP 2014 Corporate General Counsel Survey, conducted by American Lawyer Media
Why Even More Soon: Growing Dominance of Knowledge Assets

3/4 of all Assets = Intangibles
2/3 of Intangibles = Knowledge Assets

- Tangible Assets
- Intangibles: Brand, Goodwill & Employee Competencies
- Intangibles: Knowledge Assets: Databases, Trade Secrets, IP
Why Even More Soon: The Coming Insurance Crisis

2013 CGL Exclusion of Digital Assets
Cyber-Risk Addresses a Tiny Fraction

- 65% Tangible Assets
- 25% Cyber-Risk Coverage for Breaches of PII
- 10% All Other Intangibles Uncovered Under CGL Exclusion
Cybersecurity is Already There

Traditional Information Security
1. Driven by the regulatory frameworks (HIPAA, GLBA, EUDP, FTC)
2. Focused on preventing the disclosure of personal information
3. Imagined that the bad guys could be kept out
4. Supplemented by other sections on resilience (e.g. SLAs, business continuity)

Cybersecurity
1. Driven by global cyberthreats, commercial espionage, and the perceived collapse of a secure internet
2. Focused on data assets (including trade secrets and IP as well as sensitive information)
3. Focused on resilience and adaptability (taking quite a few steps back from the prevention of disclosure)
4. Not yet required by law, but required by NIST, which is shaping standards of care
Generally, there is a movement from compliance structures, consistently applied...
To a more dynamic framework which assumes that protection fails....

<table>
<thead>
<tr>
<th>Function</th>
<th>Unique Identifier</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>ID.AM</td>
<td>Identify</td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td>ID.GV</td>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td>ID.RA</td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td>ID.RM</td>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td>PR</td>
<td>PR.AC</td>
<td>Protect</td>
<td>PR.AC</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td>PR.AT</td>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td>PR.DS</td>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td>PR.IP</td>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td>PR.MA</td>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td>PR.PT</td>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>DE.AE</td>
<td>Detect</td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td>DE.CM</td>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td>DE.DP</td>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>RS.RP</td>
<td>Respond</td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td>RS.CO</td>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td>RS.AN</td>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td>RS.MI</td>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td>RS.IM</td>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>RC.RP</td>
<td>Recover</td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td>RC.IM</td>
<td></td>
<td>RC.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td>RC.CO</td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
</tbody>
</table>
And the need to adapt when repeatable processes fail in response to changing threats

Partial
- Not formulated/ad-hoc
- Unlimited awareness of cybersecurity risk
- Limited ability to collaborate with other organizations for cybersecurity risk management

Risk-informed
- Risk management practice **not organization-wide**
- Awareness of cybersecurity risk with informal sharing of cybersecurity information within organization
- **No formal interaction** with other external organization for cybersecurity risk management

Risk-informed and repeatable
- **Formal** risk management process
- **Organization-wide** management of cybersecurity risk
- **Receives information** from external organization and uses this in risk management decisions

Adaptive
- Practices **adapt** based on lessons learned and predictions
- Cybersecurity risk management is part of the **culture**
- **Two way sharing** of information with external organizations

Increasing Rigor and Sophistication
Key Secret: Data breach headlines are based on stupid risk assessments

- Target & Home Depot & Staples, Oh My!
  - Target is the poster child for bad response and bad results
  - Even there the consumers aren’t hurt
- Why we can blog about how to do it right without fear of our ideas being stolen:

![The Physics Of: Clown Cars](image)
There are just three big themes: the breached entity:

1. Failed to have in place **adequate measures to protect** the consumer information that was targeted in the attack;

2. Failed to give the consumers in question **fast enough notice** of the potential compromise of their information; and/or

3. **Deceived** consumers regarding adequacy of security in place to protect their information.

And in litigation, there is now just one big answer:

As current types of credit card breaches become a thing of the past with Chip & PIN, Apple Pay and other more secure payments, where will the focus of breaches go? Some thoughts and answers:

1. We already see the business interruption and disaster recovery breach coverage becoming more important than the PII breach coverage.
2. Energy grid breaches that send a big part of the country back into the Stone Age will be one focus.
3. Medical device breaches that kill people (like the VP in Homeland) will be another.
4. Cyberwar.
5. And then, of course, knowledge asset breaches that rip off all of your most significant assets will be a big one.
The Electric Grid and Cybersecurity

• Need to understand the physical characteristics of the electric grid to understand the cyber threat

• Transformation and digitization of the grid has increased vulnerability
  – Smart meters
  – Additions of digital switches and remote communications result in more access points for cyber threats
  – Cyber threats embedded in digital equipment

• Complex and fragmented industry and regulatory structure
Analog Electric Grid
Our Current Electric System, Technologies, and Architecture are 100 Years Old

Edison Would Recognize Most of the System

Central Power Stations

- Transmission congestion and constraints
- Need more transmission for renewables

Alternating Current High Voltage Transmission Lines

- 3,100 Utilities
- Southern Co. serves 4.4M customers
- Altamaha EMC rural electric co-op serves 19,648 customers in Lyons, GA

Distribution Companies

End Users

- 100% availability
- Lowest ¢/kWh
- Unaware of potential of smart grid

[Graph showing energy sources: Nuclear 20%, Natural Gas 21%, Coal 49%, Liquids 1%, Solar, Geothermal, >1%, Wind 2%, Hydro 6.6%]
Implications of the Electric Grid Transformation

- **Grid Digitization and Transformation**
  - The electric industry is making a transformation from a centralized, producer-controlled network to one that is less centralized and more consumer-interactive.
  - Bringing the technologies that enabled the internet to the utility and the electric grid with interoperability based on standards, advanced visualization tools, and low-cost communication.
  - Advanced Metering Infrastructure (AMI and distributed power generation).
  - A two-way flow of electricity and information and will be capable of monitoring everything from power plants to customer preferences to individual appliances.
Digitization of the Electric Grid

A Green and Sustainable 21st Century Electric System Will Have Many of the Following Features….

- Renewable Generation
- Battery Storage as Generation
- Robust Transmission Capacity
- Smart Transmission
- Utility Scale Storage
- Smart Storage
- Smart Grid
- Distributed Generation
- Microgrids
- Roof Top Solar
- Battery Storage
- Electric & Plug-In Hybrid Vehicles
- Smart Consumers
Implications of Digitization of the Electric Grid

• Digitization of the grid involves
  – Smart Grid/Smart Meters Two Way Communications with Grid Operators
  – Remote Controlled switches for routing electrons
  – Increasingly sophisticated controls systems integrating traditional generation resources with battery storage
  – Increasing distributed generation and local points of control

• More points of entry to disturb grid operations

• Points of entry can be accessed remotely because the various parts of the grid are now digitally controllable and linked through wireless communication
Example of Cyber Threats to the Electric Grid -- Aurora

- **Simulated Aurora Attack**
  - In 2007 the Idaho National Laboratory (INL) conducted a demonstration for the Department of Homeland Security
  - Aurora attack results when a circuit breaker or breakers are opened and closed, resulting in an out-of-phase condition that can damage alternating current equipment connected to the grid
- **Response**
  - North American Electric Reliability Corp. (NERC) issued an Advisory Alert and proposed remedies to be implemented by utilities
- **Ex-Post Alerts and Proposed Remedies are clearly not sufficient**
Significant Progress Since 2007

- **While Not Perfect – Significant Regulatory Response**
  - FERC, NERC and States

- **Obama Administration Prioritizes Protecting Critical Infrastructure Assets**
  - 2009 Cybersecurity Working Group established and Deputies Committee Develops Framework
  - In 2010 the Department of Energy Required Cybersecurity Plans to be signed by C-Suite Executive as a Condition of the $3.4 billion Smart Grid Investment Grant Program
  - February 2013 President Obama Issues an Executive Order – Improving Critical Infrastructure Cybersecurity

- **Industry Response**
  - Building In Protections to Smart Grid and related grid upgrades
  - Implementing improvements to security of SCADA systems
The Electric Grid and Cybersecurity – Regulatory Framework

- Need to understand how the electric grid is regulated in order to understand the governmental and private sector responses to address cybersecurity
  - Federal Energy Regulatory Commission – Bulk Power
  - National Energy Reliability Commission
  - 50 State Public Utility Commission and Public Service Commissions
  - Regional Trading Organizations (RTOs)
  - Independent System Operators
There is no a single national grid: approximately 60% of the U.S. electric power supply is managed by ISO/RTOs while the Southeastern region remains regulated and vertically integrated.
Fragmented Regulatory Oversight of the Grid

• Federal Regulation
  – FERC
  – NERC

• RTO/ISO Regulations
  – ERCOT
  – NY ISO
  – PJM
  – Others

• State PUCs
  – States generally regulate the “distribution” of electricity to end users
  – Each State PUC must develop its own cyber security standards or adopt FERC approach
Federal Regulation of Electric Grid Cybersecurity

• Bulk power system cybersecurity reliability standards are developed by the North American Electric Reliability Corporation (“NERC”) and approved by FERC.
  – EPAct 2005 made FERC responsible for overseeing the reliability of the bulk power system in continental U.S.
  – Section 215 of the Federal Power Act authorizes FERC to approve and enforce mandatory reliability standards for bulk power systems, which include cybersecurity standards.

• Smart grid system cybersecurity reliability standards are developed by the National Institute of Standards and Technology (“NIST”) and adopted by FERC.
  – On February 12, 2014, NIST announced its Framework for Improving Critical Infrastructure Cybersecurity, in response to the President’s Executive Order 13636.
  – On October 1, 2014, NIST announced the release of the final version of the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0, which contained revisions to its guidelines for smart grid cybersecurity.

• NIST and NERC collaborate to ensure that smart grid technologies and systems integrate into the reliability standards set for bulk power systems.
State Regulation of Electric Grid Cybersecurity

- **California**
  - Estimates the market for cyber security to be more than $70 billion in 2014. The California economy expects to benefit as a result of this industry growth.
  - California complies with the NIST standards.
  - California Cyber Security Task Force was launched in May 2013 to identify critical threats.
  - AB 2200 (introduced on February 20, 2014) proposes to create the California Cyber Security Steering Committee in the Governor’s Office of Emergency Services and to continue in existence the California Cyber Security Task Force until January 1, 2020.

- **New York**
  - Implements the NERC CIP Standards as benchmarks for cybersecurity procedures.

- **Hawaii**
  - Added a new chapter on Cybersecurity to the Hawaii Revised Statutes, effective July 1, 2014.
  - Appointed a full-time Hawaii coordinator on cybersecurity and infrastructure security issues, placed within the Hawaii department of defense.

- **Texas**
  - SB 1134 (effective September 1, 2013) directed the Texas department of information resources to develop strategies and a framework for securing risk assessment and mitigation planning for critical infrastructure assets.

- **District of Columbia**
  - Resolution 20-330 (effective November 5, 2013) adopted in response to the Executive Order 13636, exempts from disclosure certain critical infrastructure information.
State Regulation of Electric Grid Cybersecurity

- **Pennsylvania**
  - Utilities are required to maintain physical security and cybersecurity plans.

- **Ohio**
  - In the process of developing standards for cybersecurity.

- **Missouri**
  - Utilities are required to have reliability plans in place and to certify compliance with FERC Order No. 706 adopting NERC CIP Standards.

- **Washington**
  - Washington Senate Joint Memorial No. 8016 (adopted on March 5, 2012) voted to implement the Beyond the Border Action Plan (that was released in December 2011) between Washington State and Canada on cooperation on trade, law enforcement, and critical infrastructure and cybersecurity.

- **Many states have rules in place where utilities are audited periodically for compliance with cybersecurity measures.**
• Critical Cyber Asset Identification
  – Identify an entity’s critical assets using a risk-based assessment methodology.

• Security Management Controls
  – Develop and implement security management controls to protect critical cyber assets.

• Personnel and Training
  – Perform identity verification, criminal background checks, and employee training to personnel with access to critical cyber assets.

• Electronic Security Parameters
  – Identify and protect electronic security parameters encompassing the critical cyber assets and access points.

• Physical Security of Critical Cyber Assets
  – Create and maintain a physical security plan to keep critical cyber assets within an identified perimeter.

• Systems Security Management
  – Define methods, processes, and procedures to secure cyber assets within the perimeter.

• Incident Reporting and Response Planning
  – Identify, classify, and report cybersecurity incidents related to critical cyber assets.

• Recovery Plans for Critical Cyber Assets
  – Create recovery plans using established business continuity and disaster recovery practices.
Utilities must balance digitization to achieve greener and cleaner electric grids with safe and prudent adoption of digital technologies.

Utilities must revise their procurement practices to avoid acquisition of digital equipment with embedded cyber threats.

While Federal and State regulators promulgate new regulations, utilities themselves must stay ahead of the evolving threats.

While focusing on cyber threats, do not overlook physical threats:
- Physical attack on key electric infrastructure can do as much and perhaps great harm to grid security.

Major energy users taking matters into their own hands:
- Data centers are increasingly designing islanded operations with less reliance on local utilities.
- Cities and communities are considering re-design of the basic grid structures to improve resiliency and security.
- Identify an entity’s critical assets using a risk-based assessment methodology.
Why Cybersecurity in the Payments Industry Is Unique

• Scope and volume of transactions
• Unique and sensitive personally identifiable information
• Emerging technology, networks and platforms
• Industry specific regulatory structure
  – Card companies, processors and vendors
  – EFTA/Regulation E (ATM; POS; Debit/credit; gift cards;)
  – Bank Secrecy Act; FinCEN; OFAC; money transmitter; Anti-money laundering
  – Payment Card Industry (PCI) Data Security Standards (DSS)
  – Gramm-Leach-Bliley (GLB)
  – Regulation Z; FACTA, etc….
  – National Institute for Standards and Technology
  – SEC disclosure obligations
Emerging Payments:
MCX/Current C, Apple Pay, Leaf, Revel, Square, Green Dot
How a Card Transaction is Processed

- Consumer
  - Requests $100
  - Authorizes Transaction

- Merchant
  - Requests Authorization
  - Provides Point-of-Sale
  - Collects $1.50 Interchange Fee, Sends $98.50

- Payment Processor
  - Requests Authorization
  - Collects $0.15 Network Fee and Sends $98.35

- Issuing Bank
  - Collects $1.50 Interchange Fee, Sends $98.50
  - Authorizes Transaction
  - Charges a $0.35 Mark-Up Fee and Deposits $98.00

- Acquiring Bank
  - Collects $0.15 Network Fee and Sends $98.35
  - Authorizes Transaction
Major Card Theft Liability

**TJX (2006)**
- 100 million records lost
- TJX failed to comply with 9 of 12 PCI mandated controls (wireless protocols; encryption, storage of track 2 data, etc.)
- Cost to TJX of $256 Million

**Heartland (2009)**
- 130 million records lost
- Certified by QSA as PCI compliant at time of incident
- Cost to Heartland $140 Million

**Target (2013)**
- 110 million records lost
- Cost $148 Million (to date); estimate of $500 Million to $1 Billion!
- Cost to banks $200 Million (to date)
Cybersecurity Safeguards Puzzle

Physical
- Facility security
- Device security
- Workstation security
- Mobile security
- Inventory control

Technical
- Threat/Vulnerability analysis
- Encryption
- Network access
- Authentication
- Passwords
- Audit control
- Data integrity
- Data retention and destruction

Administrative
- Culture
- Risk analysis
- Authority/structure
- Responsibility
- Internal Controls
- Security Policies and Procedures
- Cyber Insurance
- Training and Compliance
- Access
- Contractual allocation of risk
Payments Technology Safeguards Landscape
Access Controls, Facility, Workstation, Mobile Devices, Passwords, Logoff, Encryption, Authentication, Industry standards, (Coso; CoBIT; Nist; ISO; PCI), Audit Controls, Data Integrity

- What is my confidential data?
- Where is it stored?
- Who is using it and how?
- Is it secure?

- Is my card data secured in the event it is lost?
- Can my data be copied to this device?
- Can a specific user access this data?
A security-conscious culture in the payments industry:

- Leadership awareness (Board and CEO)
- Governance safeguards (Committee)
- Company Cyber Security Officer
- Bank Secrecy Act Compliance Officer
- Cyber insurance coverage
- Cybersecurity qualified partners & vendors
- Monitoring, enforcement and remediation
- Training and security mentoring
- Audit and risk profile, metrics and heat map
Cybersecurity Administrative Policies and Procedures Checklist - Payments

- Cybersecurity Policy
- Data Breach Incident Response Plan
- Document Management Policy
- Privacy Policy
- Mobile Device Policy
- IT Security Policy
- Investigative Guidelines & Procedures
- Employment procedures (front/back end protections)
- Anti-money laundering policy
- Identity theft “Red Flag” Policy (FTC)
Cybersecurity in the Defense Industry: Executive Order 13636

• Executive Order on Cybersecurity released 2/12/2013
  – Increased coordination/information sharing with critical infrastructure
  – High level: (DHS; Attorney General; Director of National Intelligence)
  – NIST to lead “Framework” as baseline; “Shall meet NIST requirements”
  – “Risk based” to keep pace with evolving threats
  – Sets specific dates for action items, reporting and goals

• Critical Infrastructure: “Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”
  – Maximize cyber information; sharing and analysis centers
  – Cross sector collaboration; sector specific agencies in EO
Executive Order Update

• NIST Framework 1.0 released 2/12/2014
  – Framework core (identify, prevent, detect, respond, recover)
  – Framework implementation tiers

• C³ (C-Cubed) Critical Infrastructure Cyber Community Voluntary Programs (sponsored by DHS launched 2/13)
  – Support use of Framework with 16 critical infrastructure sectors
  – Increase awareness of Framework and cyber resilience
  – Encourage outreach, communication & feedback

• White House Statements, Encouragement
  – Incentives?
DFARS Rule on UCTI
Section 252-204-7012

• Final Rule issued November 18, 2013
• Contractors with “unclassified controlled technical information” (UCTI) resident on or transiting through their information systems
  – Minimum set of enhanced proactive measures and security controls
  – Notify DOD of any cyber intrusions that have an effect on UCTI
  – Requirements flow down to subcontractors and vendors
Additional UCTI Considerations

• Risk/vulnerability assessment (preamble comment 22)
  – Consider doing assessment now before cyber incident

• When to apply UCTI standards?
  – DOD designation

• When to report cyber incident?
  – Inadvertent release
  – 72 hours to DIB Cybersecurity Information Assurance for voluntary disclosure
  – Subcontractors
13 Items to disclose online
- DOD Programs impacted
- What compromised
- Malicious or inadvertent
- Other systems, intrusions

DOD Damage Assessment possibility

Mandatory sharing of info with DOD unless “legal restrictions”
- NDA
- Written permission

Export Control Considerations

Impact of non-compliance
Next Steps on UCTI Compliance

• RFP responses
  – Certification requirement? When?
  – Statement of compliance

• Guidance (but not revised Rule) from DoD
Growth in Breach Risk from the Internet of Things

Worldwide number of internet-connected devices, forecast, bn

- Fixed communications
- Mobile communications
- Computers
- Consumer electronics & medical devices
- Industrial devices (Includes military and aerospace)

Source: Cisco; The Economist, July 12, 2014
Make your auditors happy, but do not follow their instructions

Risk Assessment
- Core team
- Clarify basic risks, opportunities & goals
- Prioritization

Foundations
- Policies
- Products
- Contracts
- Culture
- Levers

Mapping as Necessary
- Assets
- Owners
- Gaps
- Vulnerabilities
- Strengths

Develop New Programs
- New owner buy-in
- Establish metrics
- Roll-out strategy

Train, Implement, Audit
- Audit against program metrics
Aside: Where will you put your Information Governance function?

1. CISO / Information Security
2. CTO / Information Technology
3. Compliance
4. Legal
5. Privacy Office
6. Records and Information Management
7. Marketing?
1. “independence from any particular department or division” (Principle 2)
2. “All information stakeholders should participate” (Principle 3)
3. “should be established with the structure, direction, resources, and accountability” to meet program objectives (Principle 5)
4. “effective, timely, and consistent disposal of physical and electronic information that no longer needs to be retained” (Principle 6)
5. Acting in good faith to reconcile conflicting laws and obligations should establish reasonableness (Principles 7 & 8)
What Do Information Governance Lawyers Do?

1) **Regulatory** – designing solutions to global privacy and cybersecurity challenges

2) **Risk Assessment** – Identifying our clients’ big information risks and how to address them

3) **Breach Response** – Where we use our time-tested approach to recovery from the incident that also prevents lawsuits and customer losses

4) **Policy and Program Redesign** – for all corporate information, including e-communications, trade secrets, surveillance, retention, security, privacy and holds; operational risk management

5) **Contract Strategy** – creating and protecting rights in data; vendor management; contractual risk management

6) **Communications** – Assuring effective narration of information issues with consumers, regulators and the public
Thank you!

Robert H. Edwards, Jr.
Partner, Kilpatrick Townsend & Stockton LLP
rhedwards@kilpatricktownsend.com
LinkedIn: www.linkedin.com/pub/robert-h-edwards-jr/20/b6/6a0

Jon Neiditz
Partner, Kilpatrick Townsend & Stockton LLP
jneiditz@kilpatricktownsend.com
Twitter: @jonneiditz
LinkedIn: www.linkedin.com/in/informationmanagementlaw

Keith S. Omsberg
General Counsel, A-T Solutions, Inc.
KeithOmsberg@a-tsolutions.com
LinkedIn: www.linkedin.com/pub/keith-omsberg/0/887/938