DRAFTING TECHNOLOGY POLICIES TO PROTECT YOUR ORGANIZATION'S TECHNOLOGICAL ASSETS

31st Annual Employment Law Conference

John L. Hines, Jr.
(312) 985-5927
jhines@clarkhill.com

Jeffrey A. Steele
(313) 965-8509
jsteele@clarkhill.com

April 29, 2015

CLARK HILL

INFORMATION MANAGEMENT: WHY?

- At bottom, technology is about information and information management
- Information management: exploiting value and avoiding harm to your organization
- Why focus on Information management
  - Protect core properties
  - Controlled information is an asset to your company; uncontrolled information is a liability
  - Enhance reputation, increase enterprise value
  - Enterprise value weighed to intangibles
    - Ocean Tomo study (2015): 84% of value in SAP 500
  - Create internal efficiencies
  - Regulatory considerations

PROTECTION IN GENERAL

- Information management means understanding
  - The types of information
  - The flow of information and the context
  - Threats and vulnerabilities
- Information flow
  - Collection
  - Transfer
  - Storage
  - Processing
- Protections/contexts cutting across all types of information
  - Physical (locks and keys)
  - Technical (encryption, access permissions, strong passwords)
  - Administrative (policies)
  - Regulatory

INFORMATION “BUCKETS”

- Confidential information, trade secrets and inventions
  - Protecting mission critical and core information assets
- Electronic information and social media; externally directed communications
  - Leveraging social media
  - Controlling communication and liability risk
- Data and personally identifiable information
  - Managing the crazy quilt of regulatory regimes

CONFIDENTIAL INFORMATION: TRADE SECRETS – STATUTORY PROTECTION

- Statutes prohibiting *trade secret* misappropriation
  - Michigan Uniform Trade Secret Act
  - Uniform Trade Secret Act adopted by other states
  - Federal Economic Espionage Act
  - Computer Fraud and Abuse Act
- These Protections are available even without a written contract
  - ...*but harder to prove a violation*

TRADE SECRETS – STATUTORY DEFINITION

- Michigan Uniform Trade Secret Act, *MCL 445.1902(d)*
  - "…information, including a formula, pattern, compilation, program, device, method, technique, or process, that is both of the following:
    - Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and
    - Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

SOME COMPONENTS OF TRADE SECRETS PROGRAM

- Administrative, e.g.,
  - Background checks, document destruction/shredding policies, restricted access/need to know, employee and vendor non-disclosure agreements, non-competes, intro and exit interviews, training, enforcement
- Physical, e.g.,
  - Segregation of information, restricted access, card keys, locks and keys, limited replication, marked “trade secret”
- Technical, e.g.,
  - Restricted pathways, restricted permissions, encryption, strong passwords, no email transmission, computer monitoring, searches

CONFIDENTIAL BUT NOT TRADE SECRET

- Trade secrets are subset of confidential information
- Non-Trade Secrets: confidential information protected by contract or fiduciary relationship
- Elements of confidentiality agreement
  - Definition: “confidential;” include data
  - Restriction: use and disclosure; duration; bound regardless of how discharged
  - Carve outs from agreement; litigation
  - Termination: return documents and lose access to systems; exit interviews
  - Remedies
    - Computer Fraud and Abuse Act
      - U.S. v. Batti, 631 F3d 371 (6th Cir. 2011)

EMPLOYEE INVENTION AGREEMENTS

- There is no general duty for employees to assign invention rights to employers
- Employers can take ownership of certain employee inventions through contract
  - Include consideration
  - State that the employer is the sole owner of defined information, and that employee agrees to convey any personal interest to the employer
  - Outline what information is considered the property of the employer
    - What if developed during work hours?
    - What if developed on employer's equipment or computer?
  - Outline who has royalty rights, copyright interests, and use rights
  - Include a provision for the employee to identify beforehand what, if any, inventions they claim for themselves

EXTERNAL COMMUNICATIONS: PLAY OFFENSE / BE PROACTIVE

- Create a robust social media presence
- Profiles and content on relevant social media sites
- Asserting control of relevant domains
- Creating links among your various web presences
- Control your organizational identity, eclipse negative chatter
- Crisis management team and strategy in place

EXTERNAL COMMUNICATIONS POLICIES

- Communications Policy
- Acceptable Use Policy
- Email Policy
- Social Media Policy
- BYOD Policy
- Blogging Policy

COMMUNICATIONS POLICIES: COMMON THREADS

- Personal use, work time
- Prohibited conduct (harassment, defamation, spam)
- Confidentiality
- Expectation of privacy (or lack thereof)
- Personal/individual capacity
- Intellectual property
- General prudence in communication
- Off duty issues
  - Patchwork of rules
  - Protected class
- Access to employee accounts

MLC 37.271 MICHIGAN INTERNET PRIVACY PROTECTION ACT

- Employer may not condition employment or take adverse action with respect to an employee on being granted access to individual's personal internet account
- Act does not prohibit
  - Requiring access to devices paid for by employer
  - Requiring access to employer provided service or service used for the employer's business purposes
  - Disciplining for transferring work data to personal account
  - Requiring cooperation in investigation involving personal account if personal information suggests violation of applicable laws or employment misconduct
  - Restricting access to certain Internet sites while using employer resources (subject to applicable law)
  - Monitoring in accordance with federal law
  - Viewing, accessing, or utilizing information about an employee or applicant that can be obtained without any required access information or that is available in the public domain

REGULATORY CONSIDERATIONS: DRAFTING CHALLENGES

- NLRB
  - Section 7 and Social Media: can't chill concerted activity
    - Memorandum OM 12-59; Memorandum OM 12-31; Memorandum OM 11-74
    - On March 18, 2015, the General Counsel of the NLRB issued Memorandum GC 15-04, "Report of the General Counsel Concerning Employer Rules"
    - Deals with restrictions on: confidentiality; conduct towards supervisors, fellow employees, third parties; use of company IP; photography/ recordings; restrictions on leaving work; conflict of interest; requiring "accuracy"; permissions; restraining discussion of legal matters; cautioning about harming image of company, etc.

REGULATORY CONSIDERATIONS: DRAFTING CHALLENGES

- NLRB (Cont.)
  - Section 7 and email: personal use restrictions
    - *Purple Communications*: very difficult to justify a total ban
    - May apply uniform and consistently enforced controls to the extent necessary to maintain production and discipline (i.e., no oversize attachments; no unlawful harassment)
    - Eliminate access for some employees?
    - Special circumstances?
    - Emphasize no expectation of privacy: but limits

REGULATORY CONSIDERATIONS: DRAFTING CHALLENGES

- On March 18, 2015, the General Counsel of the NLRB issued Memorandum GC 15-04, "Report of the General Counsel Concerning Employer Rules"
- Non-Discrimination Laws
  - EEOC v. CVS Pharmacy, Inc. (N.D. IL)
    - Dismissed, on appeal to 7th Cir.
      - Claims involve confidentiality restrictions in settlement agreement

REGULATORY CONSIDERATIONS: DRAFTING CHALLENGES

- SEC Whistleblower Rule
  - Rule 21F-17 under the Securities Exchange Act
  - Can't impede whistleblowers from reporting possible securities law violations to the SEC
  - Threatening to enforce a confidentiality agreement regarding such communications
  - KBR, Inc. remediation: letters to employees and $130,000 fine (4/1/15)
  - Consider amending confidentiality agreements

REGULATORY CONSIDERATIONS: DRAFTING CHALLENGES

- Word of Mouth Marketing: FTC Guidelines
  - Bloggers: primary disseminators; must make material disclosures
  - Bloggers and sponsoring advertiser: liability for failing to make material disclosures
  - Remoteness no excuse
  - Importance of having written policies, practices and policing efforts
  - FTC FAQs
    - Ann Taylor Stores Corp., FTC File No. 102-3147 (2010)
    - In the Matter of Reverb Communications, Inc., FTC File No. 092-3199 (2010)
    - In the Matter of Legacy Learning Systems, Inc., FTC File No. 102-3055 (2011)

DATA PROTECTION

- Privacy
  - Your undertakings as to how you are entitled to use
  - Use: collection, storage, transfer, retention
- Security
  - Your undertakings as to physical, technical, administrative safeguards to prevent unwanted internal and third party access/penetration
  - Personally identifiable: name plus e.g., credit card
  - Personal health information
- Regulatory and Reputational Considerations
  - E.g., Sony hack

DATA PROTECTION – REGULATORY LANDSCAPE

- Compliance — a Crazy Quilt
  - HIPAA for health information
  - Gramm-Leach Bliley for financial institutions
  - FERPA
  - PCI-DSS for credit card processing
  - FTC enforcement actions
  - State Social Security number laws, etc.
  - State Security statutes, e.g., Massachusetts (Data of Mass Residents)
  - State breach statutes
- Standards, NIST, ISO, AICPA

DATA PROTECTION

- Applicable Policies
  - Written Information Security Program (“WISP”)
  - Privacy Program
  - Document Retention and Destruction Policy
  - Litigation Hold Policy
  - Social Security Number Policy (MLC 445.84)
    - Policy ensuring confidentiality
    - Prohibiting unlawful disclosure
    - Limiting access
    - Describes destruction
    - Penalties
  - Website and Mobile App policies

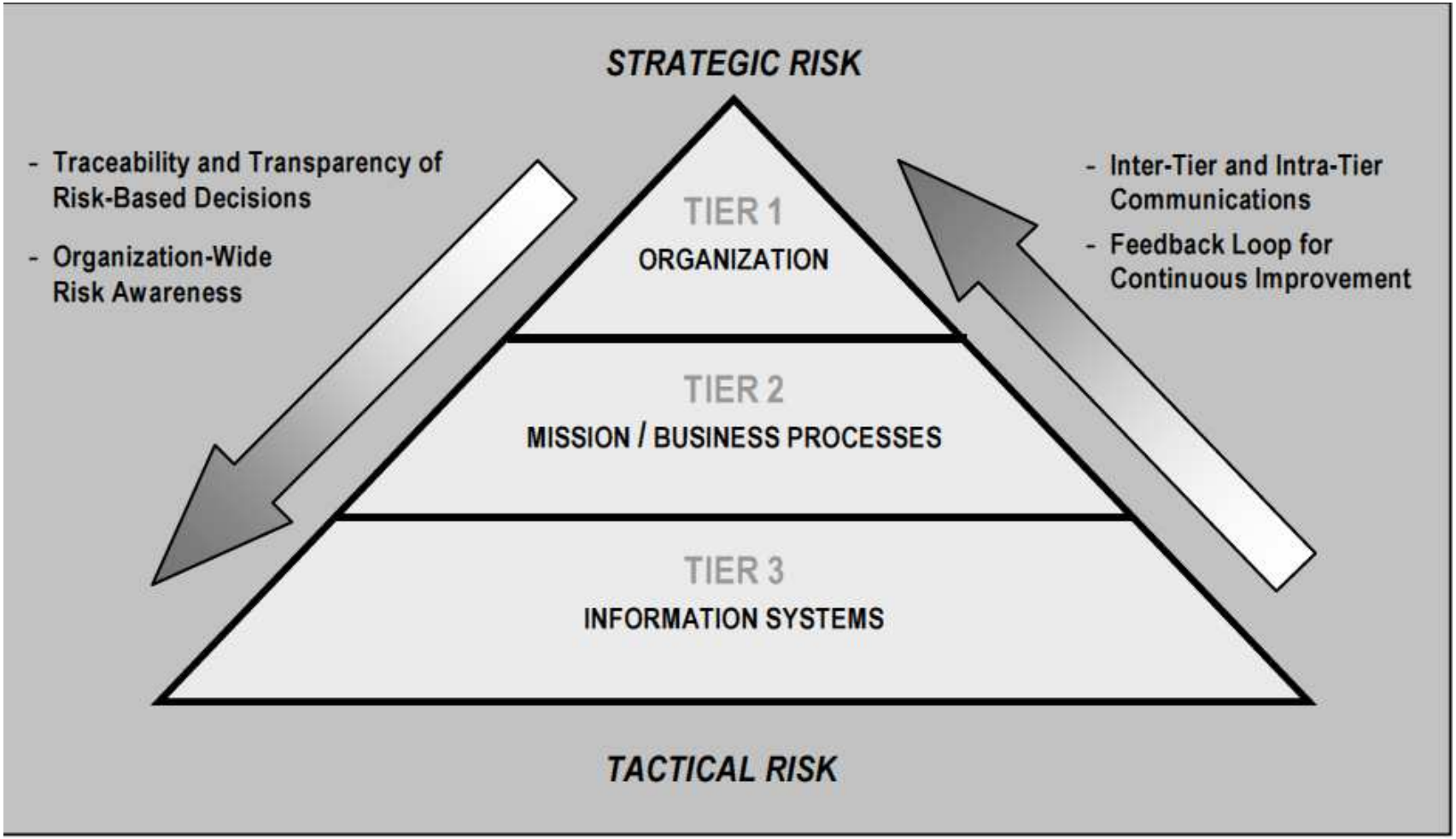
WRITTEN INFORMATION SECURITY PROGRAM

- Accountability
- Risk-based assessment
- Response/creation of proportionate controls
- Monitoring
- Review and reassessment
- Training

RISK ASSESSMENT

- Key: organizational risk assessment
- Team with HR, IT, Facilities Management, Compliance, Division Leaders, and other key stakeholders
- Mapping policies and WISP to identified risks
  - Risk is a function of…
    - Threats (internal and external)
    - Vulnerabilities
    - Potential Harm

STRATEGIC RISK PYRAMID



CONCLUSION

- Controlling information is not just compliance matter, goes to enterprise value, which is a function of corporate reputation

- Strong reputation pays of with (i) pricing power, (ii) lower operating costs, (iii) greater earning multiples, (iv) lower stock volatility, (v) lower credit costs

  — *"The compilation of beliefs and perceptions that key reputation stakeholders have in the strength of the values and processes defined by these policies is in large measure the reputation of a company. More specifically, reputation is a function of the key stakeholders' perception of critical business intangibles, including ethical and legal compliance, innovation, quality, safety and security."*

  — Kossovsky and Miller, "Mission Intangible" (2010)

QUESTIONS?

CLARK HILL

Thank You

John L. Hines, Jr.

(312) 985-5927

jhines@clarkhill.com

Jeffery A. Steele

(313) 965-8509

jsteele@clakhill.com

LEGAL DISCLAIMER

Note: This presentation/document is not a substitute for or intended to give legal advice. It is compromised of general information. Employees facing specific issues should seek the assistance of an attorney.