Queen Mary
University of London

Information Security and the Law

Professor Anne Flanagan
Centre for Commercial Law Studies

Key Module Points

- Value of information, information systems to economies
- Great dependence on ICT and information
  - Critical infrastructure
- Must be able to trust systems and information
  - Situational and relative concept
- Vulnerabilities exist at all levels
  - Great costs if systems/information compromised
- Many threats can trigger such vulnerabilities
- Law in different countries has responded by imposing duties to secure information or by creating incentives to secure information but:

Key Module Points

- No single information security law
  - Different potential sources of liability: statutes, regulation, contract, private law tort
  - Different kinds of information often sought to be protected, e.g.,
    - personal data under data protection laws or
    - financial reporting data under laws regulating companies traded on public stock exchanges
- No single legal definition of information security
- No such thing as perfect information security
  - How can you meet the legal requirements, therefore?
    - Reasonable, appropriate, adequate security?
    - Role of standards for information security

Information and Information Systems

- We live in a networked world that is growing ever more so
  - Internet of things, smart cities,
- Much of our daily activity is conducted over these networks, including the Internet, in digital form
  - Business, social, medical, financial, government activity
  - Digital information is created, collected, and sent over these networks and stored in 'intelligent' data bases

Information

- Information/Knowledge economy
  - Information is the key to producing/ enhancing 'value' in information/ knowledge economies
  - Much value in information of all kinds
    - E.g., marketing, science, health, strategic decisions, efficiencies, etc.
      - E.g., emergence of 'big data': analytics to see trends/relationships in reams of data not possible in smaller amounts
        - » Full potential not known

Information

- Organization today, therefore, have many knowledge/informations 'assets' of potentially great value
  - IP (patents, copyright, trade secret, know how, etc.)
    - Products, designs, services
  - Business/trading partner information
  - Customer information
  - Employee information
  - Financial/operational information

Information

- Personal data of value to others
  - Banking, education, credit history, medical records,
  - What you buy/pay for
  - What you watch/read/listen to/play online
  - What online services you use, subscribe to
  - Where you are: location data
  - Who you call, text, email

ICT Dependency

- Many sectors important to the functioning of society use ICT to operate, including to run the controls or provide the physical architecture for many things:
  - financial markets,
  - money transfers,
  - transport systems,
  - emergency services,
  - health services,
  - power and water supply, business supply chains, etc.

ICT Dependency

- Often such critical sectors are interconnected: eg, energy sector powers communications towers and transport systems
- Great concerns about security of critical infrastructure and the need for ‘circles of trust’
  - Trust is not binary
    - Rather relative reflecting history, nature/value of information, relationship, knowledge, skills, etc., level of security

Trust/Security

- Must be imperfect
- Vulnerabilities, or weaknesses, exist in all systems and at all levels: network, apps, human, enterprise
- These can be triggered by range of threats that can undermine the security of information and the systems it resides on/ is sent over

Information Security

- Attributes of secure information generally agreed to include:
  - Its confidentiality
  - Its integrity
  - Its availability

Related concept of authenticity – from claimed source

Information Security Management

Strategies to secure by technology and procedures

- Confidentiality,
- Integrity, and
- Availability

of Information on systems

According to needs, situations

Confidentiality

Controlling the disclosure of information

(1) protecting it/systems so that unauthorized persons cannot have access to it, and/or

(2) protecting information so that even if unauthorized access is obtained, information is unreadable (e.g. encrypted).

- Authenticating identity of seeker of access
- Access only to authorized level

Integrity

Attribute of information that addresses its:

- Accuracy
- Completeness of information
- Assurance that no unauthorized alterations are made to the data, intentionally or accidentally
  - During communication or
  - While stored

Not modified or destroyed; ensuring authenticity, non-repudiation

Availability

Involves ensuring that computer systems, networks, and data on/over them are:

- operational,
- fully functioning,
- available for use, and
- accessible whenever need

Timely and reliable access to and use of information

Issues: Withstand disruptions; address technological obsolescence and media deterioration

Information Security Law

Growing imperatives for information security:

- Commercial
- Legal
- Regulatory

One component of 'information governance'

The imperatives for information security

- Commercial
  - Trustworthiness of business transactions
  - Growing risk
  - Economic and legal consequences
    - Value, importance of information of various kinds
  - Marketing/image

Drivers of Information Security

- Legal
  - Growing legal frameworks addressing information security issues/obligations/liability prompted by concerns regarding cybercrime, privacy, safety of critical infrastructure and economic security
- Regulatory
  - Enforcement at various levels as a response to ineffective self-regulation

IS Legal Trends

1. Expanding legal duties, including general duties, to provide appropriate information security for an organization's data and electronic transactions;
2. Legal standards for what is 'reasonable' security emerging;
3. Legal duties to warn those affected (stakeholders) affected by security breaches
   - US states, EU Framework Directive (PECN), GDPR

Results of Legal Imperatives

- ISM a growing corporate management concern
  - Function outside of IT departments? CSO
  - Higher level of management
    - Board level involvement growing trend
      - *Wyndham Worldwide* (October 2014)(NJ DC)(Board exercised 'business judgement'
- Growing spend for IS budgets
  - Legal compliance one of 'biggest factors' for increased security budgets

Growing Consequences

- Enhanced fines
  - e.g. European data protection legislation; HIPAA
- Payment of damages
  - e.g. Failure to exercise reasonable care, failure to adhere to PCI DSS
- Possible decrease in legal protections under law
  - e.g. Finding of criminal offences to computer system contingent on the bypass of security (e.g. Netherlands);
- Financial liability
  - Various sources
- Imprisonment
  - e.g. not respecting corporate governance obligations on internal risk management).
- Losses arising from breaches
  - Direct and indirect

Characteristics of legal duties to protect information

- Evolving and expanding
- Global impact
  - US, EU, OECD (soft law), etc.
- Growing scope:
  - Kinds of information
  - Who is target of protection; of duty
- Variety of sources
  - Patchwork with possibility for multiple obligations

Sources of Obligations

- Statutes
- Regulations
- Private law
  - Business partner obligations (contract)
  - Victims (tort)
- Common Law
  - Evidentiary Rules

Statutes

Privacy

- EU Data Protection Directive (article 17); GDPR
- US Gramm-Leach-Bliley (financial information privacy) and
- US Health Insurance Portability and Accountability Act (health information privacy)

– Telecommunications

- E Privacy Directive
- Electronic Communications Framework Directive
- US Telecommunications Act
  - FCC presumes inadequate security where customer proprietary network information (CPNI) is breached.

Statutes

Corporate Governance Laws

- Financial transparency and securities market reporting and audit obligations
  - U.S. Sarbanes Oxley Act (SOX)
- General corporate (company law) liability

Other

- E.g., US Federal Rules of Evidence 901(a)
  See American Express v. Vinhnee (9th Cir. 2005)(test of admissibility of electronic records)
- UK Financial Services and Markets Act
- Section 5, FTCA

Privacy

- EU Data Protection Directive principles and CIA:
  - Obligations to ensure the accuracy, update and completeness of data.
    - Inaccurate or incomplete data should be rectified or erased;
  - Appropriate technical and organizational measures to protect against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure of data or unlawful access or other forms of processing;

EU Data Protection Directive

- Level of security appropriate to the risks represented by the processing, nature of the data to be protected, taking into account the state of the art and the costs of implementation of the measures;

– Controller has security obligations for transfers to 3rd parties
  - Must choose processor with sufficient guarantees as to security and ensure compliance with them
  - Contract necessary

– Security measures are consideration for 'adequacy' under art 25

GDPR

- Defines data breach
- Imposes data breach notification obligation
  – Within 72 hours to NSA (art 30)
    - Nature, scope, data, possible harms, measures taken, DPO contact, documentation provided
  – To controller by processor without undue delay
  – To data subjects individually without undue delay if high risk to rights and freedoms
    - Not required if data not intelligible due to TOM or risks are mitigated by controller
    - Public announcement if disproportionate effort

GDPR

- Specific suggestions for security actions m "appropriate to the risk," including:
  - Pseudonymisation. and encryption
  - Ability to ensure the ongoing CIA and resilience of systems and services
  - Ability to restore availability and access to data in a timely manner in event of physical or technical incident.
  - Process for regularly testing, assessing and evaluating the effectiveness of TOM.

GDPR

- Adherence to either an approved code of conduct or an approved certification mechanism may demonstrate compliance
- Recital 38 – processing of data strictly necessary to secure information and systems is a legitimate interest

Privacy

- US Privacy Protection Act of 1974

Any government agency that maintains system of records about an individual must establish:

appropriate administrative,

technical, and

physical safeguards

to insure security, confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

(5 U.S.C. § 552a (e)(10) (2000)

Privacy

U.S. Gramm-Leach-Bliley

"[E]ach financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." (15 U.S.C. § 6801(a) (2000)).

Privacy (cont'd)

US HIPAA

- Each person . . . who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards

  (A) to ensure the integrity and confidentiality of the information;

  (B) to protect against any reasonably anticipated -

  (i) threats or hazards to the security or integrity of the information; and

  (ii) unauthorized uses or disclosures of the information; and

  (C) otherwise to ensure compliance with this part by the officers and employees of such person.

(5 U.S.C. § 1320d-2(d)(2)) .

Telecommunications Privacy

- EU E Privacy Directive
  - Requires Member States to implement national measures to secure the confidentiality of electronic communications and related traffic data
    - Protect against interception, tap, storage of communications and traffic data unless consent, legally authorised or necessary for network operation
    - Obligation to erase or make traffic data anonymous when no longer needed for transmission of a communication (exceptions exist)
    - PECNs to take appropriate technical and organisation measures to safeguard the security of their services where necessary with the network provider
    - Service provider obliged to notify the user of unaddressed risks of breach outside its security measures and steps the user can take to remedy those risks.
      - Breach notification reform

Statutes: Security

- US E Government Act 2002, Title II (FISMA)
  - Obligation on all federal agencies to develop and implement information security management systems
  - NIST to develop risk management guidelines for all but national security agencies
    - Extensive ISMS standards
    - Recently mapped to ISO to avoid compliance conflicts
      - Government service suppliers

UK FSMA 2000: Sector Control

Nationwide Building Case (2007)(loss of laptop with consumer information)

- FSMA 2(2): reduce extent to which it is possible for a business carried on by a regulated person to be used for purpose connected to financial crime
- FSMA, Principle 3, duty to exercise reasonable care to organize and control its affairs responsibly and effectively with adequate risk management systems

Nationwide Bank

- Inadequate controls
- Different locations
- Inconsistent policies
  - Lacked prioritization
  - Clarity
- Generic training with limited oversight
- Poor incident management procedures
  - Further ability to use for financial crime

FSMA 2000

Norwich Union Life

- fined £1.26m for failings in its antifraud systems, controls (2006)
- fraudsters could satisfy customer verification requirements with publicly available information to access and change account and insurance policy information
  - Poor controls

Norwich Union

- Failure to respond timely by management even though compliance department identified
  - £3.3 million policies surrendered in one year (74policies)
- Unclear policies as to who was responsible for response management
- Failure to give adequate risk balancing with customer service

FSMA 2000

Zurich Insurance (UK branch) – 2010 fine of £2,275,000 for loss of 46,000 policyholder's details

– Failure to ensure effective systems and controls to manage the risks relating to security arising out of outsourcing K with another Zurich company in SA

– Lack of due diligence re: data security controls of SA company and sub-contractors

Zurich Insurance

- Reliance on group policies w/o considering whether comprised adequate security, whether in place
- Failure to identify adequately lines of
- responsibility- many people task with IS duties but no one with overall responsibility
- Poor system controls in failing to discover that unencrypted back up tape with details missing for over a year

FCA Financial Crime Guide I and 2

Non binding but failure to comply may be considered

• Governs all regulated firms (including e money and payment institutions) subject to

• Data security guidance (Ch 5, Pt 1; Ch 6, Pt 2)) includes:

– Governance, staff hiring and vetting, training, specific controls (eg, access, portable media, back-up, etc), data disposal, 3rd party suppliers

Statutes: Sector Security

- EU Electronic Communications Framework Directive 2002/21/EC as amended 2009
  - ENISA to set standards
  - NRAs to have power to get information re: status of network security
  - PECNs and PECS to take the necessary technical and organisational measures to appropriately manage risk to security of networks and services or to ensure the integrity of their networks
  - Commission power to adopt technical implementing measures where common EU network security requirements needed; NRA power to investigate, impose sanctions for failure to comply

Statutes: Sector Security

US E Government Act 2002, Title II (FISMA)

- Obligation on all federal agencies to develop, implement information securitymanagement systems

  – NIST to develop risk management guidelines for all but national security agencies

- Extensive ISMS standards
  - Recently mapped to ISO to avoid compliance conflicts
    - Government service suppliers

Sector Obligations: US FDIA

Law providing federal deposit insurance to financial institution customers

- Under Sec 39 –safety and system controls
  - Unsafe or unsound practice standard
- Directors of 16,000 federally insured banks, savings institutions and credit unions are legally obligated to safeguard information assets including from identity theft.
  - Interagency guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect CIA

FDIA

- Risk of termination of federal deposit insurance for depositor's assets for breaches of info security related controls:
  - fiduciary breaches of information security
  - inadequate internal controls per COSO on safeguarding information assets,
  - unfair and deceptive acts, and
  - violations from other federal regulations, including:
    - GLBA, FTC ACT, FDICIA, Sarbanes-Oxley 404, SEC 13a-15f, Auditing Standard No. 5 (internal controls)

Statutes: Financial Accounting

Sarbanes Oxley Act 2002 (SOX)- US publicly traded companies (and their subsidiaries wherever)

- Corporate statute regarding transparency and ethical conduct
  - Intended to protect shareholders and the general public from:
    - accounting errors, overstated earnings, fraudulent practices, self dealing
      - Off books accounting to hide losses, sales of management shares during prohibited times

SOX II

- Make specific people in company accountable
  - Management to be held responsible for information in financial reports
- Enhance disclosure, transparency
  - More information that could affect company stability and value required to be disclosed
  - Not only conclusion, but how reached and documentation
- Requires more regulatory oversight
  - More frequent SEC reviews required

SOX III

- Increased financial reporting obligations to ensure greater transparency for investors
  - – Reporting of significant events that can affect value of company (e.g. change in management)
    - Various time limits (e.g., 4 days)
  - – Sign-off by executive management that reports are accurate
    - Criminal sanctions

SOX IV

- Enhanced obligations for records retention (5 years), records accuracy, integrity and availability.
  - – Possible criminal sanctions for failure to comply
- Section 404: establishes the need for creating internal controls of an organization and certification by CEO/CFO that these are effective

SOX V

Each public company must develop individual approach to compliance and reporting.

- Self-assessment of the internal controls the organization has for its financial reporting process.
  - Internal and external audit teams
  - Evaluate under some standardized framework (e.g. COSO) to identify the gaps in compliance, as well as any associated risks.
    - Allows audit firms to map internal control objectives back to SOX requirements,

SOX V

(Organization can apply an Information Management System process of choice)

- To address the relevant gaps for compliance.
- To implement processes to ensure controls for integrity, accuracy, availability of corporate information
  - To monitor and evaluate these

SOX and ISM

- Indirect but significant impact of law
  - – CEO cannot sign off on accuracy of financial information if possibility that based on corrupted, invalid or incomplete data
  - – CEO cannot sign off that has internal controls in place if systems that run these are not up and secure
  - – Cannot meet specific records provisions if not secure systems and information

UK Companies (Audit, Investigations and Community Enterprise) Act of 2004

Directors must issue a statement in auditor's report, confirming that they provided the auditors with all of the relevant information needed to properly prepare the report.

- Directors who fraudulently or negligently make statement – or who fraudulently or negligently allow the statement in the report – commit an offence punishable by fine or imprisonment.

Likely commensurate impact on IS

SEC: Corporate Disclosure

- Investor Transparency Reporting under Securities and Exchange Act of 1934
  - 2010 guidance issued re: material risks concerning information security and intrusions of concern to reasonable investor
    - Eg. whether caused a loss of intellectual property, sparked lawsuits against the company, damaged its sales, harmed its customers or suppliers or prompted it to "materially increase its cybersecurity protection expenditures.
    - Other cyber risks including the "consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption".

Statutes: Consumer Protection

U.S. Federal Trade Commission Act, s. 5 Unfair and deceptive practices

Over 50 personal data security cases to date

- In re Snap Chat (2014)(various deceptive practices)
- In re Card Systems Solutions (2006)(failure to secure customer information is unfair trade practice even where no representation as to security of system)
- Wyndham Hotels (2016) (failure to secure)

Statutes: US Breach Notification

Regulations

- Records retention obligations in laws
  - US Internal Revenue Service regulations requiring security for electronic tax records
- Consumer Protection

  U.S. Federal Trade Commission Act
  - *In re CardSystems Solutions, Inc*., FTC File No. 052 3148 (Feb. 23, 2006)(failure to secure customer information is unfair trade practice even where no representation as to security of its system.)
  - But see, Wyndham Hotels countersuit
    - Victim, FTC lacks exertise and authority to address IS under 'unfair' and 'deceptive' ; no standards

Discussion re: Amex v. Vinhee