dentons.com

DENTONS

Insights and Commentary from Dentons

The combination of Dentons US and McKenna Long & Aldridge offers our clients access to 1,100 lawyers and professionals in 21 US locations. Clients inside the US benefit from unrivaled access to markets around the world, and international clients benefit from increased strength and reach across the US.

This document was authored by representatives of McKenna Long & Aldridge prior to our combination's launch and continues to be offered to provide our clients with the information they need to do business in an increasingly complex, interconnected and competitive marketplace.

McKenna Long & Aldridge LLP

TechAmerica EUROPE

The most recent initiatives in the US and the EU on cybersecurity, their implications for businesses and how to protect your information from cross-border cyber attacks.

mckennalong.com

OUTLINE

I. Changing Landscape and Why Should You Care?
II. Definitions
III. EU Initiatives in the context of the Digital Agenda
IV. US Initiatives
V. Case Studies
VI. Technical Solutions
VII. Risk Management Solutions
VIII. Conclusions

I.1. Changing Landscape

- Companies are facing a constantly changing landscape (with regards to addressing cybersecurity issues), which includes: the White House executive order and legislation; evolving regulatory requirements; increases in penalties and fines; and, liability from class action lawsuits
- In order to minimize, it's important to keep abreast of changing transatlantic requirements as they are being proposed so that you have the opportunity to affect the process

I.2. Why Should You Care?

- Used to be the responsibility of the firm's tech/IT point person, but now in recognition of the liability that cybersecurity carries, it has become a "c-level" issue
- We face a persistent sophisticated threat and a determined adversary
- So why should you care?
- Your data, your IP, and your reputation are at risk

II. Definitions

Fundamental terms to be defined: (definitions finally not included in published version of Communication)

- Cybersecurity
- Cyberspace
- Cyberattack
- Cybercrime

III. EU Initiatives in the context of the Digital Agenda

- Comprehensive EU Strategy on Cybersecurity (February 2013)
- Proposal for an EU Directive on the Security of Networks and Information Systems (February 2013)
- EC Communication – Tackling Crime in Digital Age: Establishing a European Cybercrime Center (within EUROPOL) (March 2012)
- Draft General Data Protection Regulation (January 2012)
- Draft Regulation on e-identification and trust services for electronic transactions in the internal market (June 2012)

BUT: Network Information Security (NIS) already addressed in Directive 2002/21/EC on a common regulatory framework for electronic communications, networks and services.

SEE ALSO: Council of Europe's 2001 Budapest Convention on Cybercrime

III.1. Comprehensive EU Strategy on Cybersecurity

EU core values apply in the digital world:

- Protection of fundamental rights (freedom of expression, personal data, privacy)
- Access for all
- Democratic and efficient multi-stakeholder governance
- Shared responsibility to ensure security

III.1. Comprehensive EU Strategy on Cybersecurity

Priorities:

- Cyber resilience
- Reducing cyber crime
- Cyber defense policy and capabilities related to the Common Security and Defense Policy (CSDP)
- Develop the industrial and technological resources for cybersecurity
- Coherent international cyberspace policy for EU

III.2. Proposal for a Directive on the Security of Networks and Information Systems

Subject matter: Measures to ensure High Common level of Network and NIS

- Obligations on Member States to handle security risks and incidents
- Cooperation Mechanism between Member States
- Security Requirements for market operators and public bodies

Foreseen difficulty: minimum harmonisation with no rule on jurisdiction and applicable law

III.2 Proposal for a Directive on the Security of Networks and Information Systems

Negative scope of security requirements: Do not apply (Why?) to:

- Providers of public electronic communication networks and publicly available electronic communication services (Directive 2002/21/EC)

- Trust Service Providers (proposal for a Regulation on electronic identification and trust services)

III.2. Proposal for a Directive on the Security of Networks and Information Systems

Obligations of Member States:

- Adopt a National Network Information Security (NIS) Strategy within a year after the entry in to force of the Directive (ENISA's implementation guide on National Cybersecurity Strategies, December 19, 2012)

- Designate a National Authority for NIS

- Set up a Computer Emergency Response Team (CERT)

III.2. Proposal for a Directive on the Security of Networks and Information Systems

Cooperation between Member States:

- Network between the National Competent Authorities
- Coordinated Response of National Competent Authorities within the Network to an early warning
- International Cooperation with third countries or international organizations

III.2. Proposal for a Directive on the Security of Networks and Information Systems

Market Operators:

- **Providers of Information Society Services** (Annex II, non-exhaustive list):
  - E-commerce platforms
  - Internet payment gateways
  - Social Networks
  - Search Engines
  - Cloud computing services
  - Application stores

III.2. Proposal for a Directive on the Security of Networks and Information Systems

- **Operators of critical infrastructure:**
  - Energy
  - Transport
  - Banking
  - Financial Markets
  - Health sector

III.2. Proposal for a Directive on the Security of Networks and Information Systems

Obligations of Market Operators and Public Administrations to:

- Take appropriate technical and organizational measures
- Notify incidents
- Inform the public, when deemed necessary by the competent authority

III.2. Proposal for a Directive on the Security of Networks and Information Systems

- Provide information (no specification yet) to National Competent Authorities for assessment of the security of their networks

- Undertake a security audit by a qualified independent audit or national authority

- Abide by standards and/or technical specifications as will be determined by EC implementing acts

III.2. Proposal for a Directive on the Security of Networks and Information Systems

Enforcement:

Companies that will not comply with the national legislation introduced pursuant to this Directive will be subject to important penalties, including substantial fines; also companies will be subject to binding instruction from supervisory authorities.

IV. US Initiatives

a) "Cyber Security is a matter of national and economic security." President Obama

b) 2012 Legislative Summary

c) Despite bipartisan alarm over the threat of cyber attacks, Democrats and Republicans never narrowed differences about the scope and nature of federal government involvement in protecting privately owned networks

d) Expect new U.S. legislation in 2013

IV.1.Obama Executive Order

- Covers critical infrastructure-February 12, 2013
- http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
- The National Institute of Standards and Technology will initiate a process where industry and the federal government will create cybersecurity standards
- DHS will turn the voluntary program into completion
- Information-sharing system builds off current work at DHS and DoD with the defense-industrial base

IV.2. Designated Critical infrastructure Sectors

- Presidential Policy Directive Critical Infrastructure Security
- http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
- Chemicals; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare; Information Technology; Nuclear Reactors; Transpiration; and Water and Wastewater systems.
- DHS will focus on water; electricity; nuclear; and transportation

IV.3. The Big Picture in the United States

- "Cyber Security is a matter of national and economic security." President Obama
- Former Defense Secretary Panetta said the US has reached a pre-9/11 moment on cyber security
- International Cybercrime nets more revenue than narcotics traffic
- Hacktivism-political causes
- Cyber War-Iranian centrifuges
- Espionage-Chinese hacking into your corporate network
- Every company has been penetrated-80% do not know it
- Your network is compromised; there is no silver bullet

V. Case Studies

- Cyber espionage is seen as a direct threat to US economic interests- $25 billion to $100 billion in losses
- Saudi Aramco-network compromised-lost 30,000 -60,000 machines
- RSA token compromised-Lockheed Martin attacked
- DHS identified an unidentified US power plant that was crippled for week by cyber attacks
- 2012 US National Intelligence estimate identifies China as the nation most aggressively seeking to penetrate US corporate systems

VI. Technical Solutions

- Use of the state of the art technical measures to counter cyber attacks to avoid liability
- Cooperate with skilled and experienced technical consultants
- Conduct frequently technical reviews
- Train personnel to operate effectively the technical mechanisms against cyber threats

VII. Risk Management Solutions

- Standard contractual clauses (for outside IT providers)
  - liability/direct and indirect losses
  - change of control clauses

- Compliance schemes (in line with applicable employment regulation)

- Insurance

VII.1. Compliance Schemes

- Design self-compliance internal program

- Draft a universal cybersecurity policy to apply to all departments of the company; include provisions on crisis management, notification of security breaches to competent authorities and clients, internal audits etc.

VII.2. Insurance

Increasing number of corporations from multinational to SME's consider purchasing insurance against cyber threats

Insurance products cover:

- First party liability
- Third part liability

VII.2. Insurance

- First party liability usually includes:

a) Loss of Digital Assets Coverage
b) Network Business Interruption
c) Cyber Extortion
d) Cyber Terrorism (Law dated April 1, 2007 on the Insurance against Damage resulting from Terrorism)
e) Security Event Costs

VII.2. Insurance

- Third party liability usually includes:

a) Network Security and Privacy Liability
b) Identity Theft
c) Employee Privacy Liability
d) Electronic Media Liability
e) D&O liability

VIII. Conclusions

- You are not going to stop cyber attacks
- Perimeter defense does not suffice anymore
- You must manage and mitigate risk and protect the most important assets of the corporation
- Raise awareness among employees
- Create an internal culture of privacy and security
- Develop a crisis management plan and conduct ongoing drills and exercise

VIII. Conclusions

- MLA's interdisciplinary Cybersecurity team is at the forefront of cybersecurity issues. We advise on all aspects of government affairs, government contracts, corporate, IP, and litigation including developing compliance programs to prevent attacks, conducting breach response plans, advising on compliance and risk management, and cultivating effective government relations strategies.

- Continued evolution of cybersecurity regulations on both sides of the Atlantic along with increased risk of breaches from mobile devices, and other sources will challenge corporate counsel to develop compliance and security programs that satisfy regulatory obligations, preserve sensitive corporate information, and respect privacy.

More Info

- Dan Caprio, Senior Strategic Advisor, dcaprio@mckennalong.com
- Orestis Omran, Associate, oomran@mckennalong.com
- Zoltan Precsenyi, Government Affairs Manager at Symantec, zoltan_precsenyi@symantec.com
- Christian Wagner, EU Security and Privacy Policy Manager at TechAmerica Europa, christian.wagner@techamerica.org
- Nora Wouters, Partner, nwouters@mckennalong.com