Society of Maritime Arbitrators
January 9, 2019

Cybersecurity & the Maritime Arbitrator

Stephanie Cohen, Independent Arbitrator
www.cohenarbitration.com

Cybersecurity & daily news

Center for Strategic & International Studies (CSIS) – McAfee Report (2018), *Economic Impact of Cybercrime – No Slowing Down*

- close to **$600B** (nearly 1% of GDP) is lost worldwide to cybercrime each year
-  from estimated $445B in 2014

Cybersecurity & maritime industry

Jones Walker LLP 2018 Maritime Cybersecurity Survey

- motivated by increasing digital innovation and connectivity in the maritime industry
- survey of 126 senior executives, CIO/CTO's, key managers from maritime companies across U.S.
- participants from cargo shipping, port operators and support services, owners and operators of vessels

Jones Walker findings & conclusions

- **U.S. maritime industry is being targeted**
  - **38%** of all maritime companies reported cyberattacks in the past year, including **nearly 80%** of large companies (more than 400 employees)
- **maritime industry has false sense of cybersecurity readiness**
  - 69% of respondents expressed confidence in maritime industry's cybersecurity readiness, but only 36% believed their own companies were prepared
- **smallest companies are the least prepared**
  - 94% of small, and 81% of mid-size, companies reported their organizations were unprepared to deal with data breach, compared with 100% of large companies

Cybersecurity & legal industry

- April 2016 – Mossack Fonseca & The Panama Papers
  - 11.5 M documents leaked by an insider
- June 2017 – DLA Piper hit by NoPetya crypto-ransomware
  - major systems (e-mail, internet, phone) down for one week worldwide

Lawyers under attack – big & small

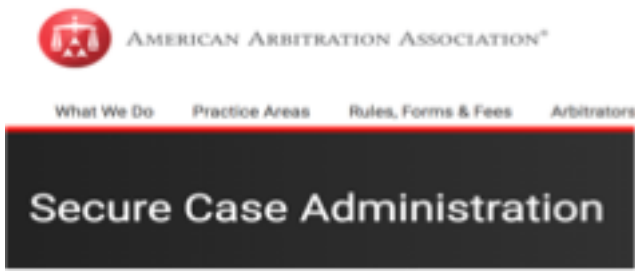
ABA TechReport 2017

- steady increase in security incidents over prior years
- solo lawyers experienced least incidents
- small to mid-size law firms experienced most incidents
  - 10-49 lawyers: 35% reported breach
  - 2-9 lawyers: 27% reported breach
  - 500+: 23% reported breach

Emerging focus on cybersecurity in arbitration

- arbitration is not uniquely vulnerable to cyberthreats, but is susceptible
- cybersecurity is an industry priority – reasonable user expectation that will maintain security in dispute resolution
- consequences of unauthorized use, access, or disclosure of arbitration-related information can be significant
- failure to meet user expectations of privacy and confidentiality may undermine confidence in the integrity and legitimacy of the arbitral process
- cybersecurity measures may be mandated by ethical rules, contract, or applicable law(s)

Cybersecurity initiatives in (international) arbitration



CPR Rule 9.3(f) – at the administrative conference, parties may consider "the possibility of implementing steps to address issues of cybersecurity and to protect

The security of information in the arbitration"

HKIAC Art. 3.1(e) – recognized means of communication may include "any **secured** online repository that the parties have agreed

to use"

Shared responsibility & the weakest link

- **Jones Walker**: "It is our hope that the information we have provided can help shift the balance in a positive direction: **as each stakeholder takes steps to embrace cybersecurity, so too will the entire industry**."

What is the nature and scope of the arbitrator's cybersecurity duty?

- Stephanie Cohen & Mark Morril, *A Call to Cyberarms—The International Arbitrator's Duty to Avoid Digital Intrusion*, 40 FORDHAM INTERNATIONAL LAW JOURNAL 981 (2017)
- presiding actor in an arbitration, unique position of trust
- no one can guarantee perfect security
- duty to take **reasonable measures** to safeguard against cyber intrusion into the arbitral process
  - duty of confidentiality
  - duty of competence
  - duty to protect integrity and legitimacy of arbitral process

Reasonable cybersecurity measures

- Cybersecurity concerns the **integrity of electronic data**
- It is the steps that we take to protect that data – our digital assets– from **unauthorized access, use, and/or disclosure**

1 – baseline cybersecurity

2- case-specific cybersecurity

Reasonable cybersecurity measures –

2- case-specific cybersecurity

ICCA-CPR-New York City Bar Association Draft Cybersecurity Protocol for Arbitration

- **risk-based framework** for parties and arbitrators to determine reasonable cybersecurity measures for their particular arbitration
- emphasizes **party autonomy** while empowering tribunals to decide in the event of conflict or superseding interests
- **no one-size fits all**
- factors to be considered include, among other things, identity of the parties and the sensitivity of the information being exchanged, applicable law, the views of any administering institution, party preferences based on cost, other burden, risk tolerance, proportionality, and relative resources

Procedural directions – in preparation for the case management conference

1- whether the Tribunal should issue "any procedural directions relating to confidentiality and/or measures that should be taken to protect information security"

2- appropriate protocols for communications and information exchange in the arbitration, including whether the Tribunal should order that any particular protective measures be taken to safeguard the cybersecurity of arbitration-related information from unauthorized access, use, and/or disclosure, in view of any applicable confidentiality obligations, the likely exchange of sensitive commercial or personal information in the arbitration, or other relevant circumstances of the case

Reasonable cybersecurity measures

1 - baseline cybersecurity

Keep abreast of cybersecurity risks/ vulnerabilities of technology you rely upon

- **FTC Cybersecurity for Small Business** - https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity
- **IBA Cybersecurity Guidelines (2018)** - https://www.ibanet.org/LPRU/cybersecurity-guidelines.aspx
- **ABA Cybersecurity Handbook (2d ed. 2017)** - https://www.americanbar.org/products/inv/book/309654847/

Reasonable cybersecurity measures

1 - baseline cybersecurity

Know your digital architecture and assets

- ***what*** arbitration-related data do you have and how sensitive is it?
- ***who*** has access to the data?
  - is access based on need (workflow)?
  - authorized third parties and their practices
- ***where*** is data being stored and how is it being transmitted?
  - inventory hardware and software
  - devices: desktops, laptops, smartphones, tablets, USB drives, back-up media
    - folders; within apps and software-as-a-service
  - servers, networks, cloud, routers
- ***when*** will you destroy the data?
  - do you have a legitimate need to keep it? for how long?
- ***why*** do you need the data in the location(s) where it is stored?
  - do you store according to need (workflow)? unnecessary redundancies?
  - can data be archived?

Reasonable cybersecurity measures

1 - baseline cybersecurity

Individual vigilance and responsible conduct in everyday practice - good cyber hygiene

- **file management**
- be mindful of **freeware** - use professional e-mail and cloud storage
- secure devices with strong **passwords** (stored safely) and **multi-factor authentication** where available
- use a **privacy screen**
- avoid public wifi - investigate **VPN**'s and mobile hotspots
- **update** systems and software on a timely basis
- run **anti-malware, virus protection**
- beware of **suspicious e-mails** – pick up the phone
- be **breach ready**
  - back-up data (3 copies – 2 different storage types - 1 offsite)
  - enable full disk encryption and remote tracking/ wipe
  - note device serial numbers

Verizon Data Breach Investigations Report 2018 (11th annual report)

53,308 security incidents, 2,216 confirmed data breaches, 65 countries

- 62% of breaches involved hacking
- 81% of hacking-related breaches leveraged **weak and/or stolen passwords**
- 51% of breaches involved **malware**
- 43% of breaches involved **social attacks** (e.g., phishing)
- 58% of incidents victimized small businesses
- 68% of breaches took months or longer to discover

Biggest breaches –SONY, Equifax, DLA Piper –can be traced to basic mistakes – poor password management, failure to implement patches

Questions?

cohen@cohenarbitration.com