NEBRASKA
State Bar Association

Cybersecurity Risks and How to Avoid Them

Nathan Burkman
Koley Jessen, PC, LLO

FRIDAY NOVEMBER 2, 2018 WEBINAR

This page intentionally left blank.

NEBRASKA State Bar Association

The NSBA Health Law Section presents

Cybersecurity Risks and How to Avoid Them Webinar

Fri., November 2, 2018
12:00 pm - 1:00 pm

NE MCLE Accreditation
#164812 (Distance learning)
1 CLE hour

www.nebar.com

This webinar will go over cybersecurity threats specific to businesses in the healthcare industry, legal developments related to data breaches, and what businesses can do now to be better prepared to handle cyberthreat situations in the future.

1. Overview of Cybersecurity Threats
   a. Types of data maintained by businesses in the healthcare industry
   b. Types of cyberattacks
   c. Concerns for businesses
   d. Representative examples
2. Laws addressing data privacy, cybersecurity and data breaches
   a. Federal law
   b. Nebraska law
3. Preventive measures to avoid cybersecurity risks
   a. Employee training
   b. Data breach response planning
4. Responding to a Data Breach
   a. Outside Counsel
   b. Forensic Investigators
   c. Public Relations
   d. Cyber Insurance

Speaker:
Nathan T. Burkman, Koley Jessen, PC, LLO

REGISTRATION FORM: Cybersecurity Risks and How to Avoid Them Webinar - November 2, 2018

- ☐ **$65 - Regular Registration**
- ☐ **$50 - NSBA dues-paying member**
- ☐ **Free - NSBA Health Law Section member**
- ☐ **Free - Law Students**

Please let us know how you heard about this CLE event:

☐ Email (eCounsel, listserv, etc.) ☐ Social Media
☐ *Nebraska Lawyer* ☐ Another NSBA CLE event
☐ NSBA print mailing ☐ Other:_____

Name:_____ **Bar #**_____

Address:_____ **City:**_____ **State:**_____ **Zip:**_____

Telephone:_____ **E-Mail:**_____

_____ **Check enclosed OR Charge to** _____ **MasterCard** _____ **Visa** _____ **Discover** _____ **AMEX**

Amount enclosed or to be charged $_____ **Card number:** _____

Security Code *(located on back of card)*:_____ **Expiration Date:**_____ **Mo/Yr**

Please print name on credit card:_____

Credit card billing address *(if different from above)*:_____

City:_____ **State:**_____ **Zip:**_____

Signature:_____

Make checks payable to NSBA and return completed form to NSBA, 635 S 14th St. #200, Lincoln, NE 68508, or email to Karla Roscoe at kroscoe@nebar.com.

If you do not receive an email confirming your registration, please call (402) 475-7091.

If you need any special accommodation for attending this event, please contact the NSBA.

NSBA CLE Cancellation Policy: • *A full refund will be granted only when a cancellation request is received at least 72 hours prior to the live or distance-learning CLE event.* • *A cancellation request made less than 72 hours of the live or distance learning CLE event or following the live or distance-learning CLE event will be refunded, less a $30 processing fee.* • *You may send a substitute (e.g., someone from your firm) in lieu of cancelling.* • *The cancellation policy for a NSBA sponsored CLE event does not apply to independent third-party CLE providers, and attorneys are subject to their cancellation policy.*

This page intentionally left blank.

FACULTY BIO

Nathan T. Burkman

Koley Jessen, PC, LLO

Nathan Burkman is with Koley Jessen, PC, LLO, and provides counsel to clients on their employment and HR-related matters. He has experience working with clients in multiple industries, including transportation, technology (data privacy and security) and manufacturing. Mr. Burkman also offers particular expertise related to the preparation, analysis, and defense of non-compete agreements, as well as preparation of affirmative action plans for federal contractors. Mr. Burkman's received his JD from the University of Nebraska College of Law.

This page intentionally left blank.

CYBERSECURITY RISKS FOR EMPLOYERS AND HOW TO AVOID THEM

Presented by Nathan T. Burkman
November 2, 2018

KOLEY JESSEN
ATTORNEYS

Threat Assessment

- **Valuable data**
  - Employee census data
  - Protected Health Information
  - Proprietary Documents
- **Cost of Cybercrime has quadrupled since 2013**
- **Small to Mid-Sized businesses are increasingly at risk**

KOLEY JESSEN
ATTORNEYS

Cybersecurity Threats

- **Malware/Ransomware: 7%**
- **Lost Laptop or Device: 9%**
- **Phishing: 12%**
- **Employee Error: 30%**

KOLEY JESSEN
ATTORNEYS

Identifying Threats

- **E-mails**
  - Unknown Senders
  - Missing Signature Block
  - Requests for Personal Information
  - Links

KOLEY JESSEN
ATTORNEYS

4

Trust but Verify…

Urgent information from BBB 1/17/12 3:16 AM

Good afternoon,

Here with the Better Business Bureau would like to notify you that we have been sent a complaint (ID 05349555) from your customer in regard to their dealership with you.

Please open the COMPLAINT REPORT below to view the details on this matter and inform us about your point of view as soon as possible.

We hope to hear from you very soon.

Kind regards,

Fernando Grodhaus

Dispute Counselor
Better Business Bureau

BBB Start With Trust

Council of Better Business Bureaus
4200 Wilson Blvd, Suite 800
Arlington, VA 22203-1838
Phone: 1 (703) 276.0100
Fax: 1 (703) 525.8277

KOLEY JESSEN
ATTORNEYS

5

Cybersecurity Example

KOLEY JESSEN
ATTORNEYS

6

Cybersecurity Laws

- **FEDERAL**
  - No comprehensive structure
  - Most laws focus on Government response / voluntary cooperation programs
    - Cybersecurity Act of 2015
- **INTERNATIONAL**
  - Europe: GDPR
  - Canada: PIPEDA
- **STATE**
  - Nebraska Financial Data Protection and Customer Notification of Data Security Breach Act (87-801 to 87-807)
    - Unauthorized acquisition of unencrypted data that compromises personal information
    - Must provide notice to affected individual and the Nebraska Attorney General

KOLEY JESSEN ATTORNEYS

7

HIPAA Privacy Rule

- The Privacy Rule protects all "individually identifiable health information" ("PHI") that is held or transmitted by a covered entity or its business associate.
  - Attorneys who represent health care providers or other covered entities and who must obtain access to PHI as part of that representation are treated as business associates.
- PHI may not be used or disclosed, except: (1) as the Privacy Rule permits or requires; or (2) as the individual authorizes in writing.
  - Required disclosures are: (a) to the individual and (b) to HHS pursuant to a compliance investigation or enforcement action.

KOLEY JESSEN ATTORNEYS

HIPAA

- **HIPAA requires business associates to**
  - implement reasonable safeguards to prevent the improper use or disclosure of PHI and
  - implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic PHI

KOLEY JESSEN ATTORNEYS

9

ABA Formal Opinion 477

- *Securing Communications of Protected Client Information*
- "[A] lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks of technology*…"
- In order to comply with their general obligations under the Rules, lawyers must continuously analyze how they communicate electronically about client matters, applying the following factors to determine what efforts are reasonable:
  - The sensitivity of the information;
  - Likelihood of disclosure without additional safeguards;
  - Cost of and difficulty in employing additional safeguards; and
  - Extent to which the safeguards adversely affect the lawyer's ability to represent clients.

KOLEY JESSEN
ATTORNEYS

Associate of Corporate Counsel Model

Clients are Requiring Security – The Associate of Corporate Counsel Model requires internal security and privacy policies that include:

- Security policy; organization of information security; asset management; human resources security; physical and environment security, communications and operations management, access control, etc.
- Retention; return/destruction; certification of destruction of records.
- Encryption in transit, at rest, stored on portable devices, etc
- Data security breach reporting.
- Physical security protections.

KOLEY JESSEN
ATTORNEYS
11

Associate Of Corporate Counsel Model (continued)

- Logical access controls.
- Monitoring.
- Vulnerability controls and risk assessments – at least annually.
- System administration and network security.
- Company has security review rights to inspect, examine and review outside counsel records, practices and procedures used in rendering services.
- Cyber liability insurance with minimum coverage level of $10,000,000.

KOLEY JESSEN
ATTORNEYS
12

ABA Formal Opinion 483

- **Attorney ethical obligations following a data breach involving information relating to the representation of a client**
  - Data breach: an event where material client confidential information is misappropriated, destroyed, or otherwise compromised, or where ability to perform legal services engagement is significantly impaired
  - Must be taking reasonable efforts to monitor potential cyber intrusions
  - Must act reasonably and promptly to stop/mitigate a detected breach
  - Must investigate what occurred to evaluate data lost or accessed
  - "When a data breach occurs involving, or having a substantial likelihood of involving, material client confidential information a lawyer has a duty to notify the client of the breach"
  - Ethical obligations do NOT affect required notices under any other applicable laws

KOLEY JESSEN ATTORNEYS

13

Employee Training

- **Change passwords**
- **Awareness / Threat Identification**
- **Set expectations for data handling**
- **Contact protocol in event of lost device**
- **Valuable Company Information:**
  - Limit Access
  - Segment Data
  - Back Up Information
- **Create a culture of security awareness**

KOLEY JESSEN ATTORNEYS

14

Data Breach

- **Create a data breach response plan**
  - Identify key players
  - Develop reference sheets for IT / HR teams
  - Protect critical data
  - Mitigate potential of continuing damage
- **Guidance: DOJ Cybersecurity Unit – Best Practices for responding to cyber incidents (April 2015)**

KOLEY JESSEN ATTORNEYS

15

Responding to a Data Breach

- **Engage outside legal counsel**
  - Attorney-client privilege for investigation
- **Third-Party Forensic Investigators**
  - Standard Data Breach
  - PCI/DSS concerns
- **Cyber Insurance**
  - Notification timelines
  - Have a good understanding of what is covered under your policy
- **Public Relations**
  - Be deliberate; don't rush to make a statement
- **Law Enforcement**
  - Determine whether law enforcement may be able to assist as part of investigation efforts

KOLEY JESSEN
ATTORNEYS

16

Questions?

KOLEY JESSEN
ATTORNEYS

17