CYBERSECURITY:
IS THERE ANY SUCH THING?

This educational seminar will teach funeral professionals the basics of protecting their confidential and private data—to the best of their abilities—when using devices connected to the Internet. This will allow them to: a) define conflicts that arise between best and actual practices, b) identify the affected parties and their interests, c) take preventative action (where possible), and d) respond appropriately to errors.

Contact hours: 2 Law

When attended continuously and in full, this 100-minute course provides the professional one credit hour. See Pub. Health Law §3429.

Course Outline

I. Introduction of Speaker and Presentation Goals

A. Nance L. Schick, Esq.
1. Funeral Industry Attorney with a largely virtual practice
2. Employer with Two Part-Time Employees, one of which works virtually from AZ
3. Business Owner with Seven Per Diem Attorney Vendors (independent business owners who also work virtually)
4. Former Early Adopter of Technology Innovations

B. Disclaimer

This course provides a general overview of cybersecurity concerns and how they might affect your work. **It is not legal advice, and I am not your attorney.** If you require information or advice applied to your unique situation, please make an appointment to discuss it with an experienced attorney of your choosing.

C. Presentation Goals

212.804.7041
nance@nschicklaw.com

1. Define conflicts that arise between best and actual practices
2. Identify the affected parties and their interests
3. Take preventative action (where possible)
4. Respond appropriately to errors

II. Introduction of Topic and Key Presentation Points

NOT SO FUN FACT: Forty-three percent of cyberattacks are aimed at small businesses. https://thebestvpn.com/cyber-security-statistics-2018/.

A. You have duties to protect the confidentiality and privacy of certain data.

1. Business processes and other intellectual property protected under copyright, trademark, or patent law
2. Decedents' health records, if not identity and other details
3. Families' credit card, bank account, or other information
4. Employees' social security numbers, immigrant status, residence information, health information, and more

NOT SO FUN FACT: More than 4,000 ransomware attacks occur every day. https://thebestvpn.com/cyber-security-statistics-2018/.

B. Things can go wrong quickly.

1. Patco Constr. Co. Inc. v. People's United Bank (1st Cir. July 2012). Patco was a typical mid-sized business customer of the bank. It regularly withdrew money to pay employees' wages and vendor invoices. Hackers installed malware on Patco's computers and stole money from its bank accounts. Despite seeing the large off-shore withdrawal (which was unusual for the business), the bank manager approved the transaction, overriding an alert. He determined that the log-in identification and password combination were sufficient, so Patco's back account was drained. Patco sued the bank. The court rejected the argument that the bank manager was negligent. On appeal, the court reversed and remanded the case for a trial to determine, among other things, if the bank had taken appropriate cautions to safeguard Patco's information. The case settled before trial.

2. Federal Trade Commission v. Wyndham Worldwide Corporation (3d Cir. 2015). After a security breach, the Federal Trade Commission filed a civil action against Wyndam, alleging that the

corporation misled the public about cybersecurity policies it couldn't keep. The FTC won an injunction that directed, among other things improved recordkeeping and compliance monitoring.

3. Galaria v. Nationwide Mut. Ins. Co., 2016 U.S. App. LEXIS 16840 (6th Cir. 2016). Nationwide's computer network was hacked, exposing sensitive personal information, such as names, dates of birth, marital statuses, genders, occupations, employers, Social Security numbers, and driver's license numbers of more than a million people. A class action lawsuit was filed, due to the "increased risk of fraud" and expenses incurred in mitigating the risk of fraud, such as purchasing credit reports, credit monitoring services, and other mitigation products. (The case has either settled or is still pending.)

NOT SO FUN FACT: Seventy-eight percent of people report they know the risks of clicking links in E-mail messages from unknown sources, but they still click on them. https://thebestvpn.com/cyber-security-statistics-2018/.

C. You must protect yourself, your business, and your clients.

1. Take an inventory of the potential vulnerabilities in your systems.
2. Discuss the vulnerabilities and potential protections with your employees.
3. Facilitate a culture that takes cybersecurity seriously, ensuring you have written procedures regarding:
   a) the use of E-mail, social media, the Internet, websites, software, and personal devices for work
   b) notice of potential malware, ransomware, or other cyberattacks
   c) limitations on access to work accounts and devices
      i. Vendors
      ii. Independent contractors
      iii. Family members
      iv. Friends
      v. Clients
      vi. General public
   d) confidentiality and privacy
4. Consider retaining outside consultants to evaluate your risks.
5. Ensure that your Directors' and Officers' (D&O) and business insurance covers data breach lawsuits.

III. Review of Key Presentation Points

A. You have duties to protect the confidentiality and privacy of certain data. You know the basics. The primary thing that has changed is the form of the data, which makes it more vulnerable to theft. Get protection.
B. Things can go wrong quickly. You and your employees need to know what to do about malware, ransomware, and other data breaches. Get training.
C. You must protect yourself, your business, and your clients. Get disciplined.

IV. Questions

A. Did you define a few conflicts between the best practices and ones you currently have in your funeral homes?
B. Can you identify who is affected by these conflicts and therefore who you need to talk to?
C. Did you learn of at least three preventative actions you can take in the next month to reduce your risk of a cybersecurity attack?
D. Do you feel like you can respond appropriately to errors, if something bad happens?

V. Thank you

Speaker Biography

Nance L. Schick, Esq. is an attorney, arbitrator, and mediator based in New York City. She is the founder of The Law Studio of Nance L. Schick, a largely virtual workshop, where clients can partner with conflict resolution professionals who are also licensed to practice law. She has been representing a multi-national funeral home corporation since 2004, and she has been teaching continuing education courses in the funeral industry since 2012. She is an award-winning entrepreneur, who has been acknowledged by the New York Economic Development Corporation/B-Labs (Finalist, Best for NYC 2015 & 2016), U.S. Chamber of Commerce (2015 Blue Ribbon Small Business), Enterprising Women Magazine (Honorable Mention, 2014 Woman of the Year awards), and Urban Rebound NY/Count Me In (Finalist, 2013 Pitch Competition).