IOWA DEFENSE COUNSEL ASSOCIATION

DICKINSON BRADSHAW

Ethics of Cybersecurity for Lawyers

John Lande

Shareholder, Dickinson, Bradshaw, Fowler & Hagen, P.C

March 2024: Panera Bread's week-long outage

In March, rans
The incident k
service, offline
program, varic

May 2024: Major disruptions at U.S. healthcare network Ascension

In early May, Ascension
States, had some of its
"event" in question was
organization's IT infrast
records, telephony, anc

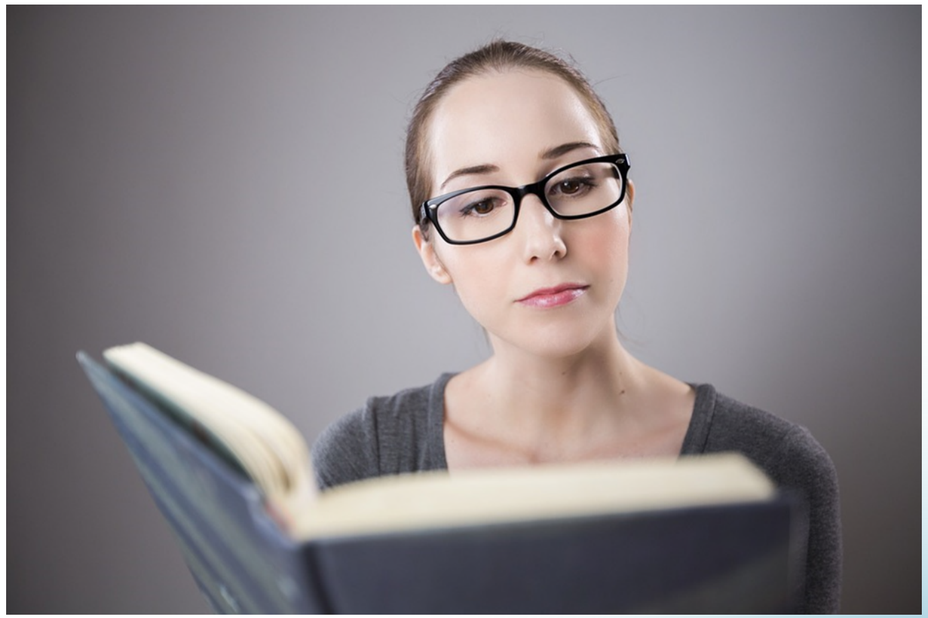
July 2024: Los Angeles County Superior Court shut down by ransomware

The Los Angeles County Superior Court, the largest single unified trial court in the United States, suspended all 36 courthouses in the county due to a ransomware attack. Both external services (such as the court's website and the jury duty portal) and internal resources (including the case management system) were impacted.

ETHICS

Competence

Cmt. 8: To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education, and comply with all continuing legal education requirements to which the lawyer is subject.
Iowa R. Prof'l Resp. 32:1.1



Safekeeping of Property

a. A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property. . . .

Cmt. 1: A lawyer should hold property of others with the care required of a professional fiduciary. . . .

Iowa R. Prof'l Resp. 32:1.15

Confidentiality

(d) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

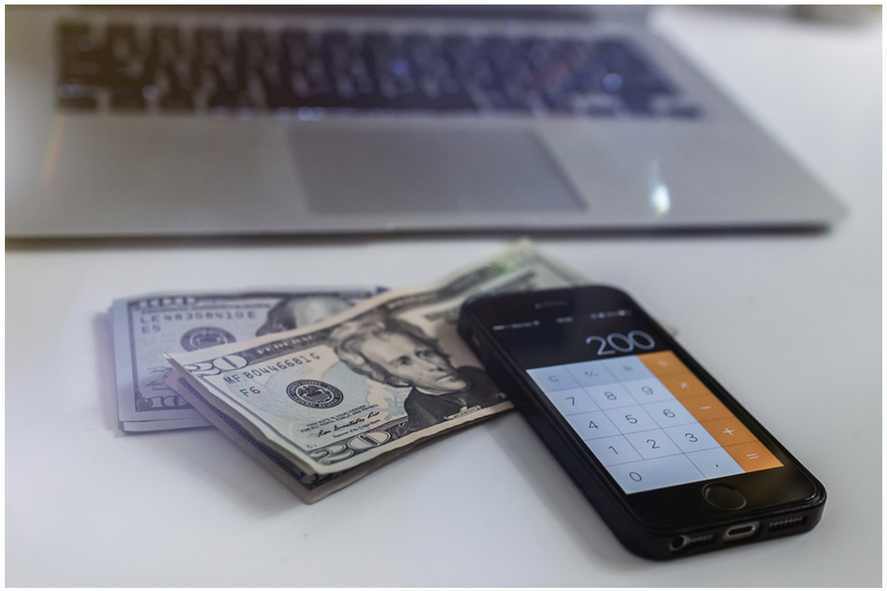
Iowa R. Prof'l Resp. 32:1.6

SAFEKEEPING OF PROPERTY

THERE IS NO COMPLETELY SECURE PAYMENT SYSTEM

PSG v. Ironshore Indemnity (N.D. Ga. 2016)

- PSG: wealth management company
- 9:10 am: Controller received fraudster email
- 10:15 am: “Lawyer” called controller
- “Lawyer” claimed director authorized wire transfer



PSG v. Ironshore Indemnity

- “Lawyer” emailed wire instructions
- Controller forwarded email to bank
- Bank required online submission
- Controller prepares wire via online system
- Fraud prevention unit at the bank contacts controller
- Controller calls “lawyer” to confirm authority
- Bank released $1.7 million

How did this happen?

- Fraudster’s fault?
- Controller’s fault?
- Managing director’s fault?
- Bank’s fault?

Preventing *PSG v. Ironshore*

- “Lawyer” sent an email with wire instructions
- Controller forwarded email to bank
- Bank required online submission
- Controller prepares wire via online system
- Fraud prevention unit at the bank contacted controller
- Controller called “lawyer” to confirm authority
- Bank released $1.7 million

Can't I just?

Regulations E & Z

- Electronic Funds Transfer Act (“EFTA”)
- Truth in Lending Act (“TLA”)
- Does not apply to accounts for:
  - Operations
  - Trust/Fiduciary
  - Business

UCC: Legal Framework

- Governs non-EFTA/TLA
- Default: Banks are liable for loss
- Banks can shift liability to account holders
- Bank & account holder agree to verify authenticity of payment orders using a commercially reasonable security procedure
- Bank follows the procedure in good faith

Waiver: *Choice Escrow* (8th Cir. 2014)

- Real estate escrow company
- Used online wire transfer system provided by bank
- Multiple/irregular wires
- Fraudsters took $440,000

Choice Escrow Security Procedure

- User 1 enters user ID and password
- User 1 authorizes wire transfer
- User 2 enters user ID and password
- User 2 authorizes transfer
- Daily limits for each user
- Daily limits for total activity

Choice Escrow Agreement

- Choice Escrow didn’t opt for daily limits
- Choice Escrow didn’t want “dual control”
- Problematic for its business
- Choice Escrow executed a waiver

But Wait?

- Banks have a duty to monitor for fraud!
- Bank Secrecy Act (“BSA”) and Anti-Money Laundering (“AML”)
- “Plaintiffs fail to cite ***any courts recognizing*** a duty arising from a company’s internal policies or the Bank Secrecy Act and numerous courts have rejected such an argument.” *Rosemann v. Sigillito*, 956 F. Supp. 2d 1082, 1111 (E.D. Mo. 2013)

Common Threats to Payments

- Client is supposed to receive settlement payment
- Fraudsters infiltrate client's email and recognize incoming settlement
- Fraudster sets up rule diverting emails from Lawyer to hidden folder, and begin corresponding on Client's behalf
- Fraudster provides Lawyer with "new" bank information
- Lawyer sends wire to Fraudster's bank account

How do Fraudsters do it?

- "If a payment order received by the beneficiary's bank identifies the beneficiary both by name and by an identifying or bank account number and the name and number identify different persons, the following rules apply:
  - a. [ ] [I]f the beneficiary's bank does not know that the name and number refer to different persons, ***it may rely on the number as the proper identification of the beneficiary of the order***. ***The beneficiary's bank need not determine whether*** the name and number refer to the same person."
- Iowa Code § 554.12207

Consequences

- Client's real bank information: Client at US Bank Acct. 1234
- Fraudster's instructions: send to "Client" at US Bank Acct. 7890
- Fraudster's Actual bank acct: Fraudster at US Bank Acct. 7890
- Bank deposits funds in Acct. 7890
- Client does not discover problem until they ask when settlement proceeds will be sent

Why do we care?

- Defense counsel may be directing settlement payments
- **If the plaintiff does not get the money, you still owe the money**
- "[T]he originator of a funds transfer pays the beneficiary of the originator's payment order at the time a payment order for the benefit of the beneficiary ***is accepted by the beneficiary's bank*** in the funds transfer and in an amount equal to the amount of the order accepted by the beneficiary's bank, but not more than the amount of the originator's order." Iowa Code § 554.12406

Tips

- Ensure counterparty has verified payment instructions over the phone by calling a trusted phone number
- Then verify wire instructions by calling the counterparty directly
- We want to be paid by wire transfer and make payments by check

INSURANCE

Two Different Issues

- Coverage for hacking: computer fraud coverage will likely cover hacking

- Social engineering: disputes between insureds and carriers over coverage

Coverage for Hacking

- Computer fraud provisions in policies provide: “We will pay for loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises . . . ”
- Question: Did the loss arise from the unauthorized access?

PSG Insurance Claim

- Coverage for: “Loss resulting directly from a ‘fraudulent instruction’ directing a ‘financial institution’ to debit your ‘transfer account’ and transfer, pay or deliver ‘money’ or ‘securities’ from that account.”
- Issue: Fraudsters “direct” cause?
- “[T]he Court must construe the policy in the light most favorable to Plaintiff and provide coverage.”

Mississippi Silicon Holdings v. Axis Insurance

- Company: social engineering & computer fraud coverage
- Social Engineering: $100,000; Computer Fraud: $1,000,000
- A/P Fraud: Fraudster infiltrated vendor & provided fraudulent bank account info for vendor payments
- Claim: Computer fraud applies, because fraudulent emails were dominant & efficient cause of loss
- Court: No computer fraud coverage; Social engineering

Confidentiality

State Bank of Bellingham (8th Cir. 2016)

- Bank's computer for initiating wire transfers was compromised
- Hackers transferred $940,000 from bank to accounts in Poland
- Fraudsters initiated DDOS attack when bank employees identified fraud
- After reversing some of the transactions the bank lost $485,000

How did the hackers get in?

- Failed to implement automatic security updates;
- Clicked on spam that downloaded malware;
- Malware allowed hackers to obtain passwords/usernames;
- Bank employees left secure token in computer;
- Antivirus software detected malware; bank employees failed to remove it;
- Computer was accessible by any employee because the computer was not password protected.

Office 365 Exploits

- Phishing email leads to compromised credentials
- Fraudsters gain access to mailbox
- Re-direct email communication
- Limited logging by default; Difficult to know what fraudsters wanted
- Mailboxes often massive repository of sensitive information

Ransomware

- Ransomware prevalence has been increasing since 2016
- Encrypting Backups and Replicas
- Name and Shame

Obstacles to Negotiation/Payment

- Pay the Ransom?
- Communication with Fraudsters
- Collecting Bitcoin

QUESTIONS?

John Lande
jlande@dickinsonbradshaw.com
515.246.4509

DICKINSON
BRADSHAW

DICKINSON, BRADSHAW, FOWLER & HAGEN, P.C.