BRIGGS

BRIGGS AND MORGAN®

PROFESSIONAL ASSOCIATION

Cybersecurity for Small & Mid-Size Businesses

Phil Schenkenberg, J.D., CIPP/US
Cyrus Malek, J.D., Certification in Cybersecurity and Privacy Law

Legal Considerations and Case Studies

CYBER SECURITY SUMMIT 2017

A SMALL/MID-SIZE BUSINESS' LEGAL LIABILITY DEPENDS IN PART UPON ITS CYBER RISK.

- The goal: pursue the company's core mission.
- Need to know company's cyber risk in the context of that mission.
- Be smart about mitigating risk.
- Be proactive rather than just reactive.
- Use trusted consultants wisely – pay now or pay much more later.

BEING PROACTIVE STARTS WITH A DATA SECURITY PROGRAM

- Companies often don’t know whether they need a formal data security program.
- Most companies are subject to some legal obligation to have a security program—or can mitigate their risk by having one.

SECURITY PROGRAMS (CONT'D)

- **Highly regulated information:**
  Special concerns in the highly regulated financial services and healthcare areas.
- **Outside the highly regulated space:**
  Laws obligate companies to maintain robust security programs.
  -Protects the company
  -Protects vendors
  -Protects customers

SECURITY PROGRAMS (CONT'D)

1. Massachusetts Data Privacy Rule

- Applies to companies that process, use, maintain or have access to PI (name plus SSN, DL, or financial account number) of a Mass. resident.
- Requires companies to implement a data security program meeting specific standards, and to impose restrictions on vendors by contract, if those vendors will have access to PI.

SECURITY PROGRAMS (CONT'D)

- Any company that takes payment from individuals by credit card or check, whether or not located in Mass., may be subject to this law.
- Any company that maintains information about its employees (and their dependents) is at risk of holding information of one who is or may become a Mass. resident.

SECURITY PROGRAMS (CONT'D)

2. Delaware Law Regarding Destruction of Employee Information:

- Applies to corporations incorporated in Delaware, and to companies that employ (or used to employ) a Delaware resident.
- No limiting language suggesting it applies only to employees or business located in Delaware.

SECURITY PROGRAMS (CONT'D)

- Broad definition of PII that includes much information regularly kept by employers (SSN/payroll information/ DL number, etc.).
- Requires destruction of information to be done in a secure manner, i.e., by shredding hard copies or destroying electronic records.

SECURITY PROGRAMS (CONT'D)

3. Nevada Data Encryption Statute:

- Applies to any corporation doing business in the state. Statute's applicability is not limited to data of Nevada residents.

SECURITY PROGRAMS (CONT'D)

- Data collectors that do any business in Nevada must use encryption for:
  1. All electronic transmissions of PI, except faxes, outside the secure system of the data collector; and

  2. Any movement of a data storage device (broadly defined) containing PI outside the confines of the workplace of the data collector or its data storage contractor.

SECURITY PROGRAMS (CONT'D)

4. Other States' Legal Obligations:

- Report breach to state attorney general (e.g., IL, MT, OR, NE, ND)
- Specific content required in breach notification (e.g., CA, IL, RI, TN, WA)
- Free credit monitoring for one year following breach (CT)

SECURITY PROGRAMS (CONT'D)

- Notification required even if the information was encrypted (TN)
- Exemption from notification of compromised encrypted data if NIST cybersecurity framework followed (WA)
- European Data Security Obligations (GDPR – much broader protections than US laws, Privacy Shield or SCCs)

SECURITY PROGRAMS (CONT'D)

- **Federal Trade Commission/Unfair or Deceptive Trade Practices**
  - The FTC regulates commerce generally, and so FTC regulation is not limited to certain areas.
  - It is a deceptive trade practice not to follow a published privacy policy. If a company does not keep its promises the FTC can take enforcement action.

CONTRACTS

Contracts Matter

- Legal obligations may be stem from promises made through contracts.
- Many companies have not focused on the importance of contract terms relating to data security (*e.g.*, confidentiality obligations in merger v. asset sale).

WHAT TO DO?

- All companies should have a:
  1. Privacy policy (that they follow);
  2. Data security program meeting basic states' standards.
  - Vendors can help you establish a data security program, but input of a data privacy lawyer is important to mitigate risk.

WHAT TO DO? (CONT'D)

- Evaluate contract language
  - Work with data privacy lawyer to ensure that negotiators understand promises that can/cannot be made (*e.g.*, merger v. asset sale).
  - Companies that enter into many contracts should consider establishing standard terms and conditions relating to data security.

CASE STUDY 1: INFILTRATION AND WIRE FRAUD

- ABC Corp. is involved in many financial transactions that involve wire transfers. Leadership thinks the company is OK on cyber, and has a third party IT company managing the network.
- Day 1: Five employees receive emails purporting to be from the CEO asking them to open an attachment. One employee clicks the link, malicious code is brought into the network and the hackers are in.

CASE STUDY 1: INFILTRATION AND WIRE FRAUD (CONT'D)

- Day 30: Just before a long-planned transaction is about to close, an email is sent from an ABC Corp. email to another party changing the routing instructions for payment.
- Day 31: The wire is sent per the new instructions, to a bank in Poland.
- Day 32: The parties to the transaction realize the money went to the wrong bank; it is too late to reverse the transfer. Fingers are pointed.

CASE STUDY 1: INFILTRATION AND WIRE FRAUD (CONT'D)

- Day 35: A lawyer is called for the first time.
- Day 40: After much analysis, ABC's IT consultant uncovers the root cause.
- Day 200: ABC has spent a disproportionate amount of money on remediation and technical upgrades, is struggling to regain business it lost, and has had its insurance claim denied by its carrier.

CASE STUDY 1: LESSONS TO BE LEARNED

- ABC Corp. isn't as well prepared as it thinks. There were a number of ways for this to have avoided.
- Day 1: This is an obvious and intentional attack on the business. Why was it not thoroughly investigated?
- Day 30: The hacker has been waiting to strike, but the email was out of the ordinary. Why was this not caught by anyone involved?

CASE STUDY 1: LESSONS TO BE LEARNED (CONT'D)

- Day 31: What is the policy on wiring funds?
- Day 32: Why did it take 24 hours to see the error?
- Day 33-40: What is the most effective response plan?
- Day 200: This was more disruptive and expensive than it could have been.

CASE STUDY 2: A VENDOR IS THE VICTIM OF A CYBER ATTACK

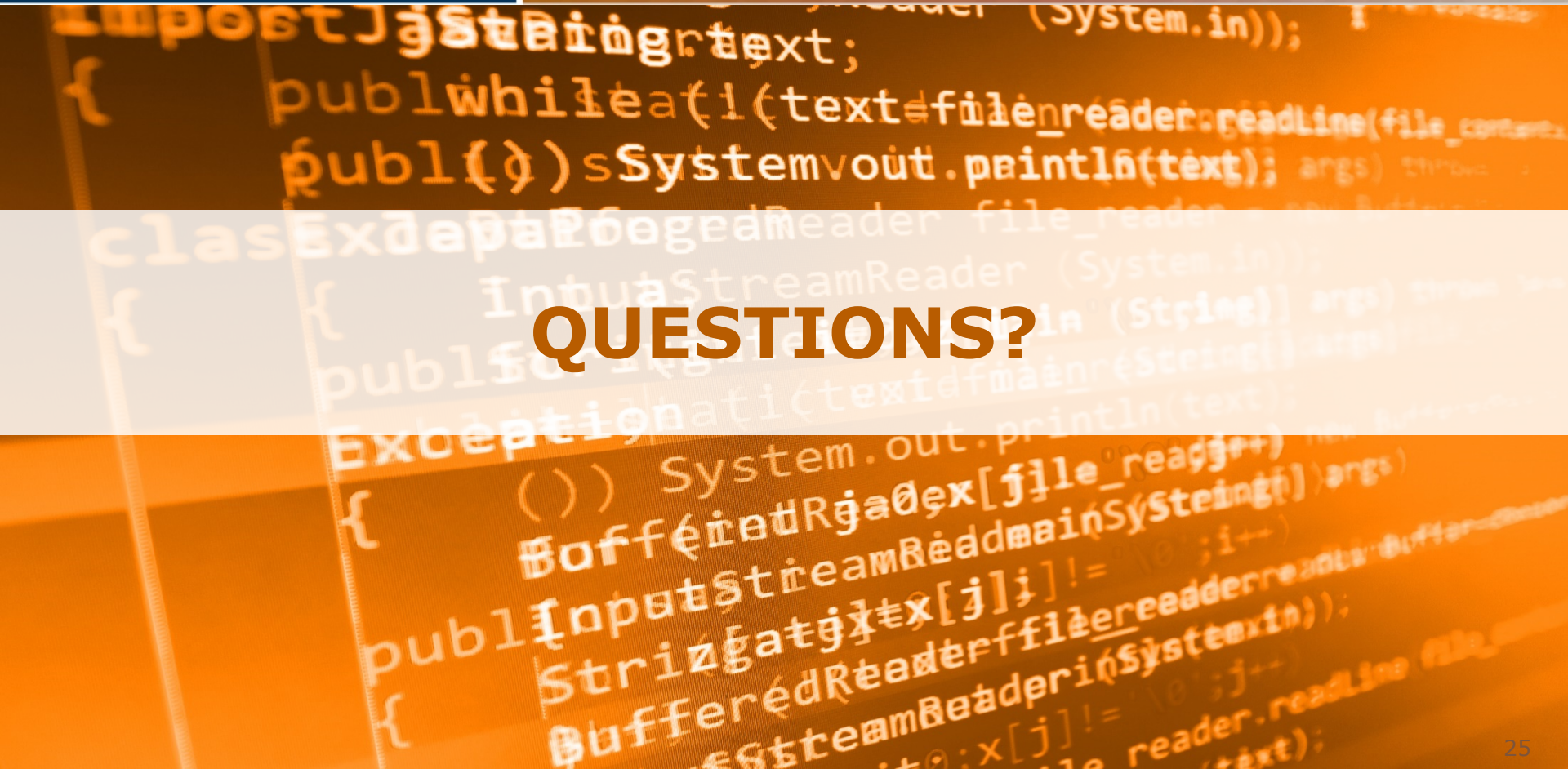
- XYZ Corp. has a customer rewards program. It collects information about customers, and customer purchases and preferences, uses that to generate customer loyalty.
- The company it uses to hold and process the data, Feel-Good Inc., seems to be doing a good job.
- Feel-Good Inc. is hacked. XYZ customer information is stolen and sold on the dark web, and bad actors pretending to be XYZ start to target customers.

CASE STUDY 2: A VENDOR IS THE VICTIM OF A CYBER ATTACK (CONT'D)

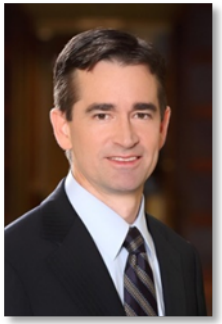
- XYZ immediately emails all customers saying that Feel-Good has lost their data and that XYZ has no culpability.
- Feel-Good and XYZ both retain counsel and make litigation threats.
- XYZ sends a breach notification letter to customers that seems to contradict its prior statement.

CASE STUDY 2: LESSONS TO BE LEARNED

- XYZ should confirm that Feel-Good has a robust data security program and the right technical controls.
- What does the contract between XYZ and Feel-Good say? What does the XYZ privacy policy say?
- For purposes of breach notification, XYZ is holding its customers' data, even if the data is lost by a vendor.
- As a result, the first communication to customers did more harm than good.



QUESTIONS?



Phil Schenkenberg J.D. CIPP/US
Cyber Attorney, Shareholder

pschenkenberg@briggs.com
https://www.linkedin.com/in/philschenkenberg

Cyrus Malek J.D.
Cyber Attorney, Associate
Certification in Cybersecurity and Privacy Law

cmalek@briggs.com
https://www.linkedin.com/in/cyrus-malek-86631b4

The **Privacy, Data Security and Cybersecurity** practice group at Briggs and Morgan offers a full range of services to help clients prevent, prepare for, and minimize the impacts of data security breaches and cyber attacks. We also represent clients in litigation following data breaches.