GROSS MCGINLEY LLP
ATTORNEYS AT LAW

Recognizing the Risk

John F. Gross
610-820-5450
33 South Seventh Street
Allentown, PA 18101
jgross@grossmcginley.com

GROSSMCGINLEY LLP
ATTORNEYS AT LAW

Introduction

- Based on a penetration test by an IT consultant, 93% of business networks were susceptible to penetration.
- In excess of 99% of US businesses are small businesses (up to $40 million annual revenue)
- Most mid to large size businesses are taking at least some of the required steps to prevent penetration.
- Small businesses are starting to understand the risk

GROSS MCGINLEY LLP
ATTORNEYS AT LAW

Statistics

- First 6 months of 2022 – an estimated 236.1 million ransomware attacks globally.
- There were 623.3 million ransomware attacks globally in 2021.
- Ransomware accounted for around 20% of all cyber-crimes in 2022.
- 20% of ransomware costs are attributed to reputation damage.
- 93% of ransomware are Windows-based executables.
- The most common entry point for ransomware is email phishing.

GROSS MCGINLEY LLP
ATTORNEYS AT LAW

Example One

- Law Firm/Title Agency in central Pennsylvania.
- $900,000 sale of a personal residence.
- Involved paying off a $600,000 mortgage to Wells Fargo.
- Day before closing, Sellers' realtor emailed wiring instructions for the mortgage payoff to Title Agent.
- After closing, Law Office wired $600,000 to Wells Fargo based on wiring instructions.
- 45 days after closing, Sellers get a notice from Wells Fargo that their mortgage is in default.

GROSSMCGINLEY LLP
ATTORNEYS AT LAW

Example One Continued

- Sometime in the month before the closing, the realtor's network was compromised; likely through a phishing attack.
- Criminal did nothing in the account but monitor it.
- Day before closing, the criminal took control of realtor's email to send an email to the Title Agent with a payoff wiring instructions for a Wells Fargo account.
- Title Agent did not verify the wiring instructions, no one noticed anything because the payoff amount was correct, and the sale closed.
- $600,000 wire sent to what appeared to be a Wells Fargo account. In realty the wire information was false, and the money was sent to the Cyber Criminals, who then emptied the account and transferred money to overseas accounts.
- By the time incident was discovered, the money was gone and could not be recovered.

GROSSMCGINLEY LLP
ATTORNEYS AT LAW

Example One Continued

- Lawyer/Title Agent spoke to his title insurance company and E&O company – both explained that they would either refuse coverage or pay the claim and sue him to recover their loss.
- Lawyer was threatened by Sellers because he was a fiduciary and agreed to use sale proceeds to payoff the mortgage.
- Total loses from incident were approximately $650,000.
- Decision – close the business or pay the $650,000 (lost money plus expenses) from personal funds.
- Lawyer/Title Agent mortgaged his home and business property to pay the amounts and stay in business.

Legal Basics

- Personally identifiable information (PII), is any data that could potentially identify a specific individual.

- In the U.S., no single federal law regulates the protection of PII. Instead:
  - federal and state laws;
  - sector-specific regulations;
  - common law principles; and
  - industry self-regulatory programs
  - Pennsylvania definition of PII - first name or first initial and last name in combination with any one or more of the following when not encrypted or redacted:
    - (1) Social Security number;
    - (2) driver's license number or state ID card number;
    - (3) financial account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;
    - (4) medical information;
    - (5) health insurance information;
    - (6) a username or email address, in combination with a password or security question and answer that would permit access to an online account.

Legal Basics

- Alphabet Soup of federal government agencies and laws - Partial list of Federal laws that could apply - Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Telephone Consumer Protection Act (TCPA); Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM); Children's Online Privacy Protection Act (COPPA); Fair Credit Reporting Act (FCRA); and Electronic Communications Privacy Act (ECPA) and the Computer Fraud and Abuse Act (CFAA).
- Protected Health Information (PHI) – part of the HIPAA Privacy Rule – DHHS has rules.
- Financial Information that is PII – SEC has rules
- If there is an incident that involves actual or potential disclosure of PII, including PHI, the legal consequences are significant, and requirements complicated.

GROSS MCGINLEY LLP
ATTORNEYS AT LAW

Example Two

- Healthcare provider within excess of 100,000 patients in its 30+ years in operation (**not** Lehigh Valley or Eastern PA based company).
- Implemented multi-factor ID for login but made exceptions for certain individuals;
- Phishing or spearing phishing attack targeted an individual who logged in without using multi-factor ID;
- Ransomware shut down the entire system for 2 weeks. Doctors returned to paper charts and calendars to see patients;
- No billing for services during lock-out;
- Claim was insured and ultimately a ransom in excess of $1 million was paid;
- FBI was notified and has a unit dedicated to investigating these cases, but you should not expect they will be able to recover your data.

Example Two Continued

- Although often no evidence of improper use in ransomware attacks, the unauthorized access to the PHI requires notice to patients and the Office of Civil Rights of DHHS.
- Notifications had to be sent to all 100,000 patients.
- DHHS is conducting its own investigation of the provider and potentially of all other related business associates.
- The patient notice process in this case cost in excess of $200,000.
- It is impossible to measure reputation damage.
- Growing trend of class action litigation involving data breaches.
- Despite recovering data, the entire computer system needed to be rebuilt and, a year later, data integrity issues continue.

Enforcement – What happens if you don't follow the Law

- Criminal Penalties
  - October 2022 – Former CSO of Uber was convicted of federal crimes for covering up a data breach
  - CSO was responsible to supervise response to the breach and to the FTC investigation of the breach
  - Judge found that CSO's actions were designed to prevent disclosure of breach
    - Uber paid ransom to hackers
    - Uber obtained NDAs from the hackers
    - Hackers were caught and are also facing federal prison

Civil Penalties - SEC

- CETERA ADVISORS
  - SEC investigated Cetera Advisors related to an unauthorized access to approximately 4500 customer accounts involving disclosure of PII.
  - Cetera had not followed its own policies regarding protecting customer accounts.
  - Cetera sent notifications to customers, but they were misleading about the incident.
  - Cetera agreed to a $300,000 SEC fine and agreed to additional SEC requirements.

Civil Penalties - FTC

CafePress

- Online Retailer
- The FTC alleged that it failed to implement reasonable security measures before an incident
- After an incident, FTC discovered its systems contained plain text Social Security numbers, inadequately encrypted passwords, and answers to password reset questions.
- FTC seeking an order requiring it to bolster its data security and require its former owner to pay $500,000 in compensation

GROSSMCGINLEY LLP
ATTORNEYS AT LAW

International Issues

- General Data Protection Regulation (GDPR) – EU DAT Protection Regulation
- UK Data Protection Act of 2018

GROSS MCGINLEY LLP
ATTORNEYS AT LAW

Contact Information

John F. Gross
33 South Seventh Street
Allentown, PA 18101
610-820-5450
jgross@grossmcginley.com