WINTHROP & WEINSTINE

YOU'VE BEEN BREACHED

THE WHAT, WHEN, AND HOW OF RESPONDING TO A DATA SECURITY INCIDENT

JUNE 29, 2021

LISA ELLINGSON, JD, CIPP/US
P/ 612.604.6573
E/ lellingson@winthrop.com

WINTHROP & WEINSTINE

WHY ARE WE HERE TODAY?

- 2020 saw a huge increase in breached records
- Recent ransomware attacks in many sectors (oil, meat processing)
  - Cox Media Group in June 2021
    - Cyberattack
      - Several TV news stations taken offline
      - Some emails downs

WINTHROP & WEINSTINE

WHAT CAN YOU DO?

- What is a data security incident?
- How to prevent data security incidents?
- How to respond to a data security incident?

WINTHROP & WEINSTINE

WHAT IS A DATA SECURITY INCIDENT?

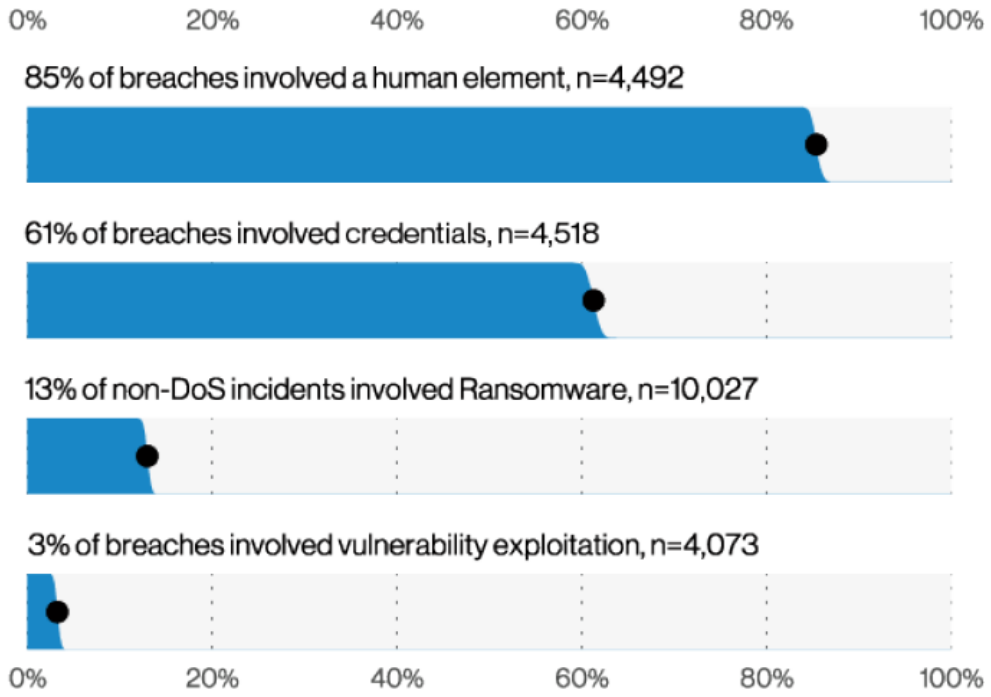
- Unauthorized access to, use, modification, or destruction of data
- Often caused by
  - Phishing – tricking people into clicking a link or opening an attachment with malicious software like ransomware
  - Exploitation of software or system vulnerabilities
  - Disgruntled employees or contractors
  - Misplaced or stolen devices

WINTHROP & WEINSTINE

HOW CAN A DATA SECURITY INCIDENT IMPACT MY BUSINESS?

- Business interruption
- Forensic investigation and data recovery costs
- Legal costs
- Reporting obligations
- Media management
- Civil lawsuits
- Lost goodwill/damage to reputation
- In 2020, on average, a breach cost:
  - $101,000 for a small to medium sized business
  - $1.09 million for a large business

HOW CAN DATA SECURITY INCIDENTS BE PREVENTED?



From the Verizon 2021 Data Breach Investigations Report

WINTHROP & WEINSTINE

HOW CAN DATA SECURITY INCIDENTS BE PREVENTED?

- Train employees!
  - Strong unique passwords, changed regularly
  - Phishing signs
    - Look at the domain name of the sender—is it really from the company's email address?
    - Obvious spelling and grammatical mistakes
    - Generic salutations
    - Requiring urgent action
    - Hover mouse over links before clicking

WINTHROP & WEINSTINE

HOW CAN DATA SECURITY INCIDENTS BE PREVENTED?

- Use “reasonable” security measures
  - Secure configurations
  - Keep software updated
  - Strong unique passwords, changed regularly
  - Multi-factor authentication (what you know; what you have)
  - Grant access on a “need to know” basis
  - Monitor network activity
- Regularly evaluate vendors
- Consider purchasing cybersecurity insurance

WINTHROP & WEINSTINE

WHAT TO DO IF YOU SUSPECT AN INCIDENT?

- Immediately contact legal counsel
  - Guide through legal issues
  - Maintain attorney-client privilege over communications
  - Having an existing relationship with counsel saves valuable time
- Immediately get your IT professionals involved
  - Investigate source and cause of incident – could be technical or physical
  - Assess and stop any ongoing damage

WINTHROP & WEINSTINE

WHAT TO DO IF YOU SUSPECT AN INCIDENT?

- Work with legal counsel to navigate:
  - Reporting to cybersecurity insurer
  - Legal reporting requirements
    - Each state has different data breach laws
  - Media statements
- Recover after incident
  - Eliminate the vulnerability that caused the incident
  - Bring repaired systems back online
  - Determine whether additional changes needed to avoid future incidents

WINTHROP & WEINSTINE

SIMPLE TAKE-AWAYS

- Train employees and test compliance with policies
- Use multi-factor authentication
- Back up data frequently
- Consider purchasing cybersecurity insurance
- Consider creating an incident response plan

WINTHROP & WEINSTINE

THANK YOU.

QUESTIONS?

ATTORNEY
LISA ELLINGSON, JD, CIPP/US
P/ 612.604.6573
E/ lellingson@winthrop.com