Cybersecurity

July 2018

Alisa Chestler, CIPP/US

Shareholder, Baker Donelson

Chair, Data Protection, Privacy and Cybersecurity Team

615.726.5589

achestler@bakerdonelson.com

CYBER ATTACKS

Cyber attacks are in the headlines everyday.

Our enterprises, our vendors and their vendors are under constant attack by hackers trying to gain access to computer networks!

Partially Taken from Source: DynaSis

Yahoo Security Breach

- September 2016, Yahoo announces data associated with 500 million user accounts was stolen in 2014. Allegedly a "state-sponsored actor" was behind the attack.
- December 2016, Yahoo discloses that another 1 billion accounts were hacked in 2013.
- CEO Marissa Mayer forfeits financial incentives, chief counsel resigns.
- Verizon's $4.83 billion acquisition of Yahoo is delayed and the price lowered by $350 million.

Equifax

- Patch Management Issue
- 30 Class Action Suits Filed the Next Day
  - Small Claims Litigation Strategy of Plaintiffs
- CEO, CIO and CISO Out
- 8 State AGs - Settlment

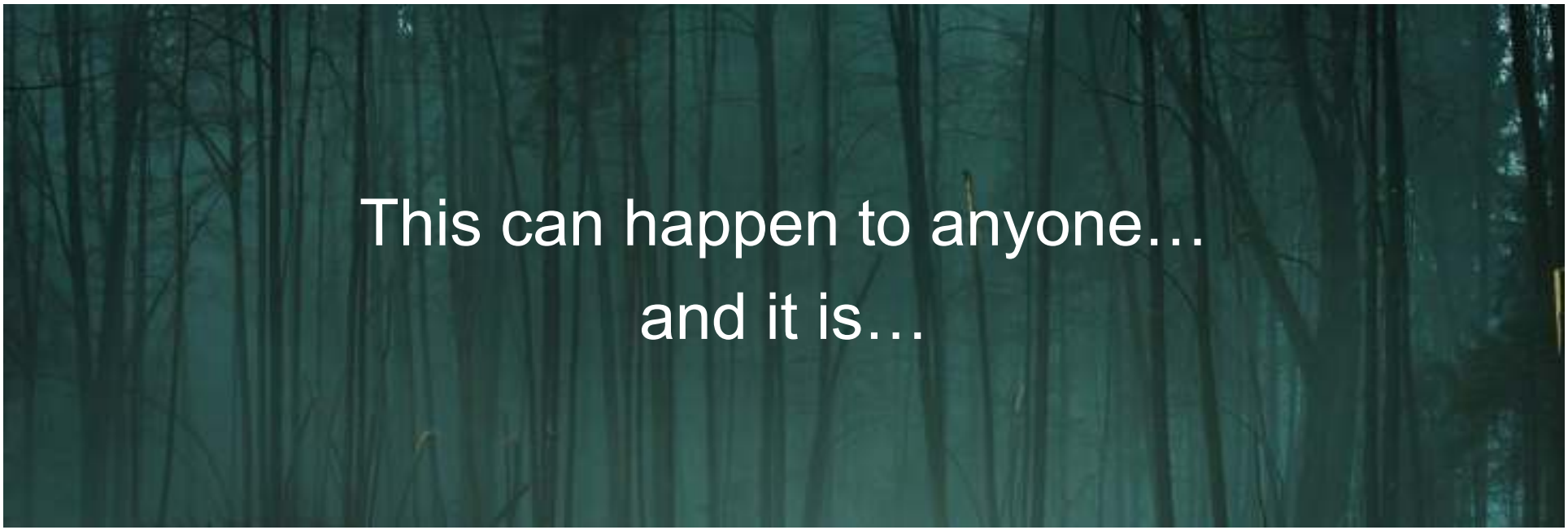
Microsoft Emails

- Password Compromise
- Lay In Wait
- Wire Transfer
- Investigation- Not all Forensics are the same

WannaCry & NotPetya

- Supply Chain Issues
- Processing to a Halt
- Disaster Recovery
- Business Continuity

Nightmare



Step 1- Know What Information You Are Protecting

- Corporate Information
- Customer Information
- Employee Information
- Operations
- Trade Secrets

Step 2- Know Where it Is

- Internal Servers and Systems
- Cloud Servers
- Shared Drives
- Electronic Media
- Subcontractors

Step 3- Know Compliance Obligations

- Corporate (SEC)
- Personal Information (Federal & State Laws)
- Sectoral (HIPAA, NY State)
- International Issues- GDPR
- Data Notification Issues

Step 4- Incident Response

Are you Really Prepared?

- Who Are the Team Members?
  - Experienced Counsel
  - Contracted Forensic Investigator
- What Are Their Roles?
- Communication Channel?
- When is Management Informed?
- Emergency Mode Operations?
- Will All Information be Preserved?

Every Organization MUST Have a Written Incident Response Plan.

Nightmare 2.0 – You Don't Know What You Have Before the Incident

- Do You Really Know The Answers to the Above Issues?
- Have You Hired an Expert In Advance?
  - Still Working With Your Partner's Brother-In-Law?
- Information Governance:
  - Document Retention Policy
    - Systematic review, retention and destruction

- Why?
  1. Business Efficiency
  2. Litigation
  3. Compliance Obligations

Step One: Preparation

- Written Incident Response Plan:
  - What Information is Being Protected
  - What are Legal Responsibilities
  - What Does Insurance Coverage Require
  - Who is on the Response Team
- Test the IRP:
  - Insider
  - Outside Hack
  - Environmental Issue
  - Vendor Issue

Step Two: Alert Appropriate Internal Parties

Alert **KEY** persons as soon as possible if a Breach is believed to have occurred:

- CEO/Administrator
- Privacy/Security Officer
- Local Police; Secret Service; FBI
- Liability Insurance Carrier
- Chairman of the Board of Directors, etc.

Considerations: Investigate and Mitigate Potential Breach Under Attorney – Client Privilege

The investigation should include the following (as applicable):

- Interviews of knowledgeable persons
- Interviews of potential privacy/security violators
- Forensic examination of computer hardware, software, etc. to determine extent of potential Breach and to determine what exact information was Breached, if applicable
- Communication with police officers/law enforcement to file theft or other reports and to review the police report(s)
- Implement Litigation Holds

Nightmare 3.0 – Have Not Practiced the Incident Response Plan

- Expectations are High
- Short Timeline
- Laws are Changing Constantly
- Industry Expectations In Constant Flux
- Mistakes and Delays will Cost You
- Don’t Have Vendors Under Contract or Attorney-Client Privilege

Compliance vs. Risk Management

- Corporate Culture Barriers
- Frustration Regarding Expense and Budget
- Communication Barriers
- Organizational Design

Goal?

- Information Governance Program
- Classification of Information
- Vendor Management Program
- Disaster Recovery
- Vulnerability & Penetration Testing

Diligence

"Only as Good As the Weakest Link"

Diligence (Continued)

- Vendors:
  - Managed Services Provider
  - Key vendor with vast personal or sensitive information
  - Security Risk Assessment & Remediation
  - Termination Programming
    - Are they destroying information?

Due Diligence

- Has the Organization Performed a Security Risk Assessment? A Real One?
- Do they Know Where their Information Assets Reside?
- Who Owes the Data?
- What Controls are in Contracts?
- Any Documented Procedures?
- Any Vulnerability Testing?

Engagement with Board of Directors

Boards are anxious about the issues:

- Bad news every day
- Broad encompassing set of issues
- M&A concerns
- Class action lawsuits heating up
- And most of all they don't understand

Gartner estimates that by 2020, 100% of large enterprises will be reporting issues to the Board at least annually. Only 40% reported cybersecurity and technology risk at least annually.

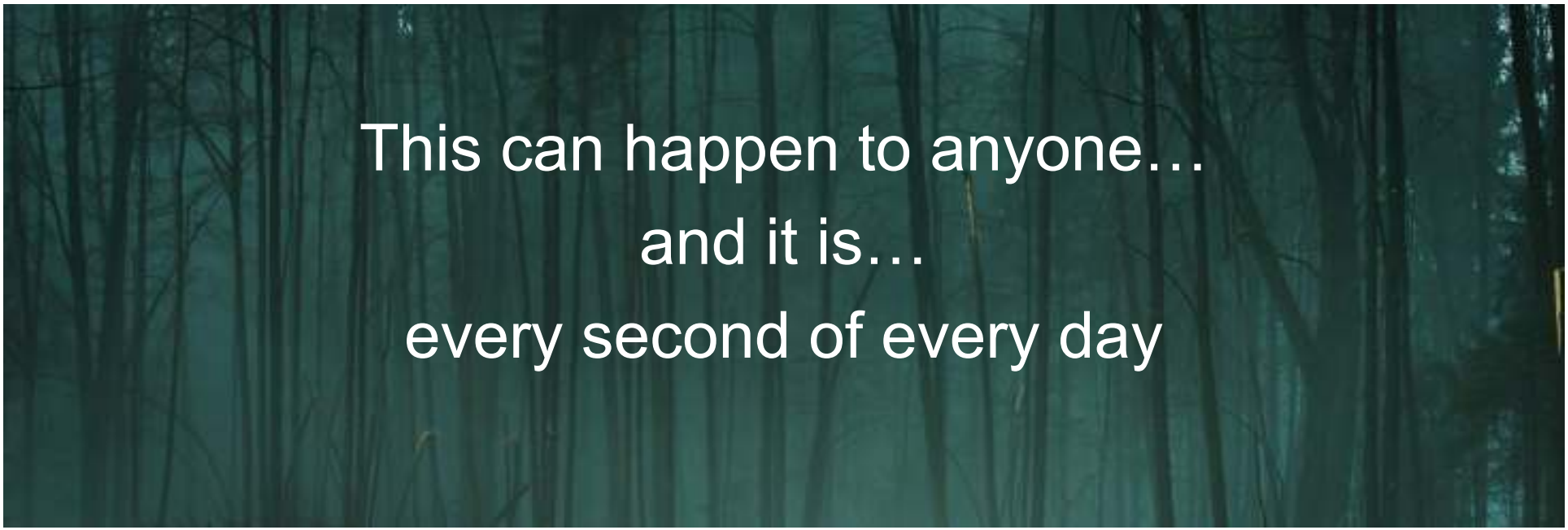
What to Present to the Board

- Strategy
- Maturity Metrics
- External Developments
- Risk Position
- Business Execution and Remediation
- Set the expectations… Back to Lesson #1

Training

- Ensure workforce knows the basics:
  - When to call (better safe than sorry)
  - Who to call if they suspect an incident
  - What to say and what (not) to put into writing

Nightmare



Questions?

Contact

Alisa Chestler, CIPP/US
Shareholder, Baker Donelson
Chair, Data Protection, Privacy and Cybersecurity Team
Nashville, TN
615.726.5589
achestler@bakerdonelson.com