Cybersecurity in our World

Megan Hardiman
Co-Chair, Privacy, Data & Cybersecurity Group
Katten Muchin Rosenman LLP
Chicago
+1.312.902.5488
megan.hardiman@kattenlaw.com

Katten
Katten Muchin Rosenman LLP

So… What Happened?

- Several critical files containing individually identifiable financial information appear to be encrypted, and now cybercriminals are demanding a ransom.
- A reporter informs you that a large volume of your organization's records is for sale on the dark web.
- Your CEO receives a very angry call from an individual who just found confidential treatment records of a deceased relative on the internet.
- Four unencrypted desktop computers were stolen from an office building during a late night break in.

Katten
Katten Muchin Rosenman LLP

Fact:

- What happens in the first 48 hours after you learn of a data breach is entirely dependent upon what you have done in the months and years leading up to the breach.

Katten
Katten Muchin Rosenman LLP

Risk Management: A Basic Checklist

- Have we identified our “crown jewels”?
- Do we perform ongoing assessments of our security risks?
- Do we have security and privacy policies and procedures?
- Do we train on them?
- Do we have a strong vendor management program?
- Have we done an insurance coverage assessment?
- Do we have an incident response plan?
- Do we have a crisis communications plan?
- Do we have a disaster recovery/contingency plan?
- When did we last test/validate these plans?

Katten
Katten Muchin Rosenman LLP

The Questions Go Like This….

- "Who's in charge here?"
- "What does our incident response plan say?"
- "Do we have a backup?"
- "Do we really have a breach?"
- "Do we have a safe harbor?"
- "Who, exactly, do we have to notify?"
- "When does the notification clock start ticking?"
- "What's our notice plan?"
- "So….now what?"

Katten
Katten Muchin Rosenman LLP

…. And the Consequences/Source of Stress Look Like This…

- Possibility of Negative Press Coverage
- Reputational Risk
- Loss of Business/Data
- Underwriting "Demotion"/Industry "Write Down"
- Regulatory Investigations/Enforcement Actions, Fines & Penalties
- Private Litigation
  - Individual or Class Action
  - Client/other Stakeholder

Katten
Katten Muchin Rosenman LLP

Threat Trends - Healthcare

- Cybercriminals are increasingly focused on health care:
  - Criminal attacks are the number one cause of data breaches in health care.
  - Ransomware, malware and denial-of-service (DOS) attacks are the top cyber threats facing healthcare organizations.
  - Other threats include: employee negligence, third-party snafus, stolen device, mobile device insecurity.
  - OCR enforcement has increased significantly.

Source: Ponemon Institute 6th Annual Benchmark Study on Privacy & Security of Healthcare Data (May 2016)

Katten
Katten Muchin Rosenman LLP

Threat Trends - Education

- According to Verizon's 2016 Data Breach Investigations report, the education sector ranks 6th in the U.S. for total number of reported "security incidents" in 2016, 153% higher than healthcare and 160% higher than retail.
- Education is the biggest target for ransomware.

Source: BitSights Insights Report: The Rising Face of Cyber Crime: Ransomware; available at: https://info.bitsighttech.com/bitsight-insights-ransomware

Katten
Katten Muchin Rosenman LLP

What Do These Sectors Have in Common?

- High value/data rich
- "Soft Target"
- Average global cost of data breach per record: $158/record, but this varies by industry:
  - Healthcare industry: $355/record
  - Education industry: $246/record

Source: Ponemon Institute 2016 Cost of Data Breach Study: Global Analysis

Katten
Katten Muchin Rosenman LLP

The Odds Favor the Hacker

- Continual attacks
- Continually evolving threats
- Sophisticated attackers, some with deep resources
- It only takes one chink in the armor

Katten
Katten Muchin Rosenman LLP

An Ounce of Prevention…

- Big data breaches/cyberattacks require crisis management.
- Preparation is the best defense.
  - Have an Incident Response Plan in place before you are breached.
    - Consider likely scenarios
    - Scale to your organization
    - Practice it regularly

Katten
Katten Muchin Rosenman LLP

Key Considerations – Incident Response Plan

- Identify the team, internal and external (*i.e.*, outside counsel, security/forensics, PR/crisis communications, notice/call center vendor, credit monitoring vendor, etc.)
  - Who is in charge? What are the roles & responsibilities?
  - Outside experts are generally retained through counsel
    - Better to engage your experts ***in advance***
    - Include 24/7 contact info

Katten
Katten Muchin Rosenman LLP

Key Considerations – Incident Response Plan

- The plan establishes a basic framework for your response:
  - Procedures to investigate/contain/mitigate/eradicate and restore the lost data/resume business as usual.
  - Procedures to collect and preserve evidence.
  - Method for confidential/secure response team communications.
    - How will you communicate if the network is compromised?

Katten
Katten Muchin Rosenman LLP

Key Considerations – Incident Response Plan

- Framework for identifying and managing multiple, time-sensitive external notifications:
  - Notice to/coordination with law enforcement where applicable
  - Timely notifications to insurer
  - Required data breach notifications (for example, applicable regulators/attorneys general, affected individuals, and in some cases, the media)
  - Notices and communications to multiple other internal/external stakeholders

Katten
Katten Muchin Rosenman LLP

Key Considerations – Incident Response Plan

- Logistics of data breach notifications:
  - Vendors (call center, microsite, notice vendor)
  - Template notice forms and holding statements
  - Situations where the data belongs to a third party
- Dealing with follow-on investigations/audits/litigation
- Post-mortem/corrective action/process improvements

Katten
Katten Muchin Rosenman LLP

Key Considerations – Crisis Communications Plan

- Identifies potential stakeholders (internal and external), such as:
  - Board, C-suite, employees, students, customers, affected individuals, business partners, media, insurers, state Attorneys General, other federal/state regulators, threat-sharing organizations, etc.
  - Draft scripts/holding statements, FAQs for rapid revision and deployment.
- Identifies roles and responsibilities and basic procedures:
  - Centralized point of communications
  - Consistent messaging
  - Minimize leaks
  - Manage legal privilege where applicable

Katten
Katten Muchin Rosenman LLP

Disaster Recovery/Contingency Plan

- Disaster Recovery/Contingency Plan questions include:
  - How frequently is data backed up?
  - Do we regularly test our data recovery process to see if it actually works?
  - Is it feasible to maintain backups offline/unavailable from the network?

Katten
Katten Muchin Rosenman LLP

Making the Plan Actionable

- Test your response plans via tabletop exercises and/or simulations:
  - Test your response plans (and teams) regularly
  - Involve all key players
- Regular drills will identify gaps/holes, build knowledge and confidence among team members, and enhance your response capabilities.

Katten
Katten Muchin Rosenman LLP

Further Guidance

- United States Government Interagency Guidance Document, *How to Protect Your Networks from Ransomware,* available at https://www.justice.gov/criminal-cips/file/872771/download).
- United States Department of Health & Human Services Fact Sheet, *Ransomware and HIPAA*, available at http://www.hhs.gov/blog/2016/07/11/your-money-or-your-phi.html).

Katten
Katten Muchin Rosenman LLP

Katten Muchin Rosenman LLP Locations

AUSTIN
One Congress Plaza
111 Congress Avenue
Suite 1000
Austin, TX 78701-4073
+1.512.691.4000 tel
+1.512.691.4001 fax

CHARLOTTE
550 South Tryon Street
Suite 2900
Charlotte, NC 28202-4213
+1.704.444.2000 tel
+1.704.444.2050 fax

CHICAGO
525 West Monroe Street
Chicago, IL 60661-3693
+1.312.902.5200 tel
+1.312.902.1061 fax

HOUSTON
1301 McKinney Street
Suite 3000
Houston, TX 77010-3033
+1.713.270.3400 tel
+1.713.270.3401 fax

IRVING
545 East John Carpenter Freeway
Suite 300
Irving, TX 75062-3964
+1.972.587.4100 tel
+1.972.587.4109 fax

LONDON
125 Old Broad Street
London EC2N 1AR United Kingdom
+44.0.20.7776.7620 tel
+44.0.20.7776.7621 fax

LOS ANGELES – CENTURY CITY
2029 Century Park East
Suite 2600
Los Angeles, CA 90067-3012
+1.310.788.4400 tel
+1.310.788.4471 fax

LOS ANGELES – DOWNTOWN
515 South Flower Street
Suite 1000
Los Angeles, CA 90071-2212
+1.213.443.9000 tel
+1.213.443.9001 fax

NEW YORK
575 Madison Avenue
New York, NY 10022-2585
+1.212.940.8800 tel
+1.212.940.8776 fax

ORANGE COUNTY
100 Spectrum Center Drive
Suite 1050
Irvine, CA 92618-4960
+1.714.966.6819 tel
+1.714.966.6821 fax

SAN FRANCISCO BAY AREA
1999 Harrison Street
Suite 700
Oakland, CA 94612-4704
+1.415.293.5800 tel
+1.415.293.5801 fax

SHANGHAI
Suite 4906 Wheelock Square
1717 Nanjing Road West
Shanghai 200040 P.R. China
+86.21.6039.3222 tel
+86.21.6039.3223 fax

WASHINGTON, DC
2900 K Street NW
North Tower - Suite 200
Washington, DC 20007-5118
+1.202.625.3500 tel
+1.202.298.7570 fax

Katten
Katten Muchin Rosenman LLP
www.kattenlaw.com