The Threat of Ransomware Continues to Grow

How Can In-House Counsel Prepare for the Battle?

By Jeff Dennis & Kyle Janecek

ACC San Diego

September 29, 2021

Agenda

- Background – Rise of Ransomware
- Proactive Preparation for Ransomware Attack
- During a Crisis – Best Practices
  - Privilege
  - Notification
- Post-Event Considerations

NEWMEYER DILLION

Ransomware Stats

- Attacks Increased by 288% in H1 (NCC Group, 2021)
- Average Ransom fee increased from $5,000 in 2018 to $200,000 in 2020. (National Security Institute, 2021)
- Ransomware remains the most prominent malware threat. (Datto, 2019)
- Malicious emails are up 600% due to COVID-19. (ABC News, 2021)
- 42% of companies with cyber insurance policies in place indicated that insurance only covered a small part of damages resulting from a ransomware attack. (Cybereason, 2021)

NEWMEYER DILLION

The Horror Stories

- Colonial Pipeline (2021)

  Colonial Pipeline has spurred a variety of litigation from various stakeholders, not just information owners.

- Scripps Health (2021)

  FOUR Class action lawsuits from impacted individuals whose information was exposed in ransomware attack.

- Target

  Settled with $10 million to consumers, $39 million to banks.

- Home Depot $17.5 million settlement for data breach.
- The 3 AM phone call.

NEWMEYER DILLION

Poll Question #1

NEWMEYER DILLION

Why does this Matter?

- Courts are becoming more willing to award damages due to a breach of personal information
- States are passing new laws regarding rights of individuals over their personal information
- It’s not Just PII
  Trade Secrets
  Confidentiality Agreements
  Supply Chain/Breach of Contract issues
- It’s easier than ever to launch ransomware attacks with “Ransomware as a Service” aka “RaaS”

NEWMEYER DILLION

Ransomware Lifecycle for In-House Counsel

- Pre-Event
  - Compliance with local cybersecurity laws
  - Cyber Insurance
  - Table Top Exercises
  - Develop Contacts and plans
- During Event
  - Preserve Evidence
  - Gather Information
  - Inform Law Enforcement
  - Restoration/Negotiation
- Post-Event/Aftercare
  - Giving Notice
  - Provide mitigation to affected persons (if required)
  - Defend in lawsuits (if required)
  - Recover costs from insurance

NEWMEYER DILLION

Proactive Steps

- Cyber insurance
- Incident Response Plan
- Tabletop
- Develop outside contacts

NEWMEYER DILLION

Prevention

- TRAINING
- IT consultants
- White-Hat Hackers
  (Penetration testing)

NEWMEYER DILLION

During Event

Who to contact, when, what order

- Outside Counsel
- Insurance
- Internal IT team
- Outside IT team(s)

Poll Question #2

NEWMEYER DILLION

Privilege concerns

- Retain outside counsel to manage the investigation (don’t do it yourself if you can afford not to)
- Use a two-track approach
  - One IT team (yours) focuses on patching the breach and getting everything back up and running
  - Have outside counsel ADD a vendor to provide services necessary for legal advice and have them work alongside your internal IT team
- Don’t use stock language in the statement of work - tie it to potential litigation
- “Data-map” your findings and prepare a non-privileged incident report.
  - Keep all intel on a need-to-know basis, and segment the party into the “legal team” “operations team” and “security team”

NEWMEYER DILLION

Clear Privilege line

- The main focus is if it is related to litigation. Conversations with counsel may not be privileged if:
  Counsel is engaged in general fact finding
  Counsel is giving *general* advice regarding security measures

NEWMEYER DILLION

Case Law

- In Re. Rutter’s Data Security Breach Litigation (Pennsylvania)
- Capital One 2019 Data Breach Litigation (Virginia)
- In re Target Corp Customer Data Security Breach Litigation (Minnesota)
- Premera Blue Cross Customer Data Sec. Breach Litigation (Oregon)

NEWMEYER DILLION

Best Practices

- All communications via counsel
- Engage third-party forensics via counsel, in anticipation of litigation
- Third-party forensics not someone you already utilize – specially engaged for limited purpose
- Forensics report not shared throughout company – limit review to GC, if possible
- Can have oral conversations with other key stakeholders about findings
- LINK LITIGATION PREP TO THE STATEMENT OF WORK

Specific issues that arise:

- Who’s calling the shots?
- Are we going to negotiate?
  - Will this change depending on severity?
- Will you get sanctioned for paying?
  - The OFAC dilemma – recent guidance
- What about your carriers?
  - Carrier approval issue

NEWMEYER DILLION

Communication during an event

- Internal
  - Out-of-band communication
- External
  - Pre-determined holding statements
- The transparency conundrum

NEWMEYER DILLION

Notification concerns

- Regulatory Bodies
- Customers
- Employees
- California Civil Code-1798.82

NEWMEYER DILLION

Notification Requirements

Title

- “Notice of Data Breach,” with the following headings:
  - “What Happened”
  - “What Information Was Involved”
  - “What We Are Doing”
  - “What You Can Do” and
  - “For More Information”

Format

- The format of the notice shall be designed to call attention to the nature and significance of the information it contains.
- The title and headings in the notice shall be clearly and conspicuously displayed.
- The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

NEWMEYER DILLION

Post-Event: The Notices and Mitigation

- Look to state laws to determine what notices and mitigation needed

  Remember, some states have different requirements on what is required for notice, so a one-size fits all approach may not work.

  Mitigation efforts may also vary, so impacted persons within certain states may be entitled to more protection than others.

NEWMEYER DILLION

Post-Mortem

- Evaluate what you learned
- Outline issues where you could improve
- Patch security & improve processes

Questions?

NEWMEYER DILLION

Speaker Information

Jeff Dennis

949.271.7316

Jeff.dennis@ndlf.com

Kyle Janecek

949.271.7252

Kyle.Janecek@ndlf.com

NEWMEYER DILLION

Thank You!

About Newmeyer Dillion

Growing and thriving businesses throughout California and Nevada trust us for advice that propels them to success. From advising on best practices to keep your information safe, to mitigating risk when a breach occurs, we help companies in diverse industries prepare for what’s ahead.