Harter Secrest & Emery LLP

ATTORNEYS AND COUNSELORS

Time Is Not on Your Side – The Legal Risk of Ransomware

F. Paul Greene, Esq.

October 10, 2018

HSE

Why Legal?

- Ransomware is simple enough, isn’t it?
  - You either pay the ransom or endure the hurt of restoring (or not restoring) from backups?
- Why engage legal if you are already buying BTC and hiring forensics?
- What possible interest could a regulator have in the fact that a criminal locked down my systems?

Why Legal?

- In the current regulatory landscape, every material security incident can have legal implications that far outweigh the incident itself.
  - A 7 BTC ransom can seem small in relation to the expense and disruption of a state AG investigation or FTC inquiry.
- Everyone now has a regulator in relation to information security.
  - Many organizations have more than one.
  - And there’s the court of public opinion to keep in mind, as well as the actual courts, where individuals and organizations can sue over data loss, downtime, etc.

Concerns to address pre-incident

- Nomenclature
  - It's always an event or incident until it's a breach
  - Nomenclature matters
    - The regulators and plaintiff's attorneys want to see the communications
      - Written communications always appear negative post-breach
  - Once you use the "breach" term, your clock could be running
  - "Breach" connotes exfiltration, which isn't often the case in relation to ransomware/cyber extortion

Concerns to address pre-incident

- Nomenclature (cont.)
  - Clocks to consider
    - HIPAA – 60 days, once per year
    - State clocks (if there is unauthorized access or acquisition to protected data)
      - NYS – “in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement . . . or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system”
      - PA – “without unreasonable delay”
      - OH – 45 days
      - FL – 30 days
    - GDPR, 23 N.Y.C.R.R. Part 500 – 72 hours

Concerns to address pre-incident

- Downtime procedures
  - Do you have any?
  - How well have they been drilled?
  - What's the culture surrounding downtime?
    - Where to focus your efforts in socializing acceptance of downtime procedures
  - Analyze what services would be prevented/delayed by downtime
  - Practice retooling staff roles to accommodate downtime changes, where possible
    - In a hospital, chart/image/prescription runners, etc.

Concerns to address pre-incident

- IR Plan
  - What is it?
  - Where is it?
    - Physically?
    - Electronically?
  - Who knows how to use it?
  - What deviations are allowed?
  - Is it tuned to ransomware/cyber extortion?

Concerns to address pre-incident

- IR Plan
  - Framework based?
  - Tuned to all of your regulators?
  - Drilled?
  - Integrated with DR/BC plans?
  - Roadmap for scrutiny post breach
  - But also allows for positive messaging: "we have an established plan in place for just such an incident as this and are following that plan"
  - Does your plan incorporate prior incident learning?
    - Drills and smaller incidents/events are the best way to pressure test your plan

Concerns to address pre-incident

- IR Team
  - – Who's on the team?
  - – Where/how do they meet?
  - – What are their roles?
  - – Internal incident command – who is it?
  - – Integration with legal, internal and external
  - – Is HR on the team? Public Relations? Facilities? (in healthcare) Nursing?

Concerns to address pre-incident

- IR Resources
  - Where is the incident command center?
  - Where is the alternate location?
  - Can you get into and use both locations if your network is down?
  - Cell numbers, home phone numbers
  - Phone chargers
  - Power strips
  - Water/coffee
  - Non-networked PC/laptop(s) with printer(s) and paper
  - Land-line (non VOIP), if possible

Concerns to address pre-incident

- External IR Support
  - Whom do you call?
    - The 800-number in a cyber risk policy is likely not the best option
    - Nor is an 800 number from a security vendor that you don't yet have a relationship with, although it's better than nothing
  - Whom do you call first:
    - Legal then broker (if you have cyber risk coverage)
  - Panel v. non-panel support
  - Location – on premises support v. remote support
  - Types of support needed immediately
    - Legal
    - Security/forensic
    - Ransomware resolution services
    - PR/crisis communications (potentially)

Concerns to address pre-incident

- External IR Support
  - – Hierarchy of engagement
    - Legal (breach coach)
    - Security/forensics
      - – How well will internal infosec work with external infosec, especially when under stress?
      - – How well will IT work with internal infosec when working with external infosec?
      - – Ideally, external infosec/forensic leads security/response decisions
        - » Have you established that level of trust yet?
    - Ransomware resolution
    - PR/crisis communications

Concerns to address pre-incident

- External IR Support
  - Form of engagement
    - Legal – engagement letter (likely required for separate incident unless you have a general cyber file open)
    - Security/forensic – MSA/SOW
      - Through legal
      - Negotiate pricing and terms beforehand, even if covered by insurance
    - Ransomware resolution – MSA/SOW
      - Also through legal
      - Commodity product, good pricing
    - PR/crisis communications – MSA/SOW
      - Usually through legal
      - Separate engagement

Concerns to address pre-incident

- Insurance support
  - What will your policy cover?
  - Do you have choice of service providers?
  - Who are the panel providers?
  - Considerations of using panel providers
    - Will you get their A-team?
    - How big is your breach in relation to their stable of open matters?
    - Will there be a pressure to pay?
    - But – you can get broader visibility

Concerns to address pre-incident

- Will you pay the ransom and under what circumstances?
  - Cultural question with practical implications
  - No black and white – it depends on the circumstances
  - Paying the ransom takes time, as does decryption
    - Deciding whether to pay the ransom takes time, but the more you can systematize/automate the decision-making process, the less time you will lose
  - Does the amount matter?
  - Will you negotiate?
  - Who has to approve? At what dollar amount?

Concerns to address pre-incident

- Will you pay the ransom and under what circumstances (cont.)
  - Who will actually make the payment?
    - There is value in being able to say that you worked with your insurance carrier and paid through an authorized ransomware resolution vendor provided by the carrier.
  - Why pay: to do everything we can to ensure patient safety and care
  - Why not pay: we were the victim of a criminal attack and had systems in place to recover without paying the criminal involved
  - What does law enforcement think of paying the ransom?
  - How good are your backups?

Concerns to address pre-incident

- Messaging
  - Should be drilled along with downtime procedures
    - Identify possible points of messaging failure
  - Accept (and plan for the fact) that messaging will be imperfect
    - There will be variation among employees
    - The press will get it wrong
    - Patients/community will speak out
  - Practice/drill oral communication
    - Keep writings to a minimum
    - Try to avoid the 8 1/2" x 11" sheet of paper on your door saying "our systems are down"

Concerns to address pre-incident

"Our company has been the victim of a sophisticated criminal attack on its computer systems, and is working with law enforcement and security professionals to resolve the issue. At present, because of the attack and in an effort to protect our **[customers/employees/patients]** and their sensitive data, our computer systems are **[partially/mostly]** down. We are working with our outside professionals to bring our systems up as quickly as possible. We have implemented our standard downtime procedures, which we regularly drill for just such an occurrence, and expect no negative impact upon **[fill in the blank].**"

Concerns to address pre-incident

- Connections with law enforcement
  - Whom do you call?
  - When do you call?
  - Why do you call?
  - What is the role of law enforcement in relation to ransomware?
  - What do they want from you?
    - Sometimes server images (watch out for regulatory issues)
    - Malware executable
    - Ransom note/BTC wallet
    - Victim impact statement

Concerns to address pre-incident

- Non-retaliation policy
  - Number one defense (other than excellent backups) is quick response
  - Every employee should be encouraged to report a suspected incident ASAP
    - Even if the employee was (inadvertently) part of the cause
    - Examples:
      - Clicking on infected link or attachment
      - Not following protocols in setting up a new piece of hardware or system configuration
      - Attempting to negotiate with attacker/pay the ransom

Concerns to address pre-incident

- Preservation of the attorney-client privilege
  - <u>Confidential communication</u> between <u>attorney</u> and <u>client</u> for the <u>provision of legal advice</u>
    - Every element matters
    - Vendors come under the umbrella as “translators”
    - Counsel does not need to be involved in every communication, but default should be to loop counsel in
  - Forensic report will be privileged
    - Do you want/need a report that is non-privileged?
    - Use of the privileged report in a non-privileged fashion will waive the privilege
  - Paper matters (privilege may not be preserved if vendors not engaged through counsel)

Concerns to address pre-incident

- Role of the risk assessment
  - Ransomware/cyber extortion should likely be a risk identified on your risk assessment
  - Anderson Cancer Center fine
    - $4.3 million fine upheld by ALJ for 33k record breach
      - Lost laptop/thumb drives
    - Lack of encryption on mobile endpoints/storage media identified as material risk, but not addressed
  - Your risk assessment is a roadmap to second guess your risk management
  - Role of privilege in relation to risk assessment

Concerns to address pre-incident

- Miscellaneous
  - Budgeting for incident response
  - Nomenclature for backup servers
  - Testing your policies/procedures concerning vulnerabilities that could give rise to an attack
  - The ironic value of encryption at rest in relation to ransomware
    - State-law carve-outs for reporting in relation to encrypted information
    - HIPAA breach analysis tips (strongly) toward no breach if ePHI is properly encrypted

Concerns during incident

- Staffing
  - – Ransomware will strike at the worst time imaginable
    - New staff
    - Staff in transition
    - Vacations
    - Holidays
    - Transactions
    - New facilities
    - Hardware changeovers

Concerns during incident

- Staffing (cont.)
  - Ransomware stresses both infosec and IT production
    - Pulling cables/re-imaging systems v. gathering logs, working on containment, gathering artifacts
  - Do you have flex support for each?
    - If internal, is it sufficient?
    - If external, how are those resources engaged?
      - Will privilege be protected?
  - External support for proprietary systems
    - Privilege will likely not attach

Concerns during incident

- Staffing (cont.)
  - Is your IR team ready to run 24x7 until containment reached and recovery begun?
    - Likely at least 3-7 days, if you are lucky
    - What about weekends/holidays?
    - Even if you have external forensics, someone from the internal IT/ infosec team needs to be there too
    - Who are the team back-ups?
    - How will they cycle for 24x7 support?
    - What about 3 am ET to 11 am ET (or even earlier if we are not dealing with Eastern Europe)
  - Do you have flex security support, if your building security system goes down?

Concerns during incident

- How will disrupting the kill chain affect your systems?
  - In the containment phase, you often need to set fires to stop the fire
  - If you disable network A, how will that effect network B?
    - Critical areas of failure include:
      - website
      - Phone
      - Billing
      - HAVC
      - Power management
      - Faculties access/security
      - In healthcare:
        - imaging
        - e-prescribing
        - EMRs

Concerns during incident

- How will disrupting the kill chain affect your systems? (cont.)
  - How will segmentation or data separation effect your systems?
  - If you segment, where do you need access to the segmented network?
    - How long will it take to set up those endpoints?
  - When you disconnect and then reconnect systems, are you reinfecting your system?

Concerns during incident

- Where is your protected data?
  - Ransomware tends to be data agnostic, but can trigger reportable events
  - Having a comprehensive data map and network diagram will save time and avoid distraction in response to an incident
    - Organizations usually do not know the full scope of the data they have or where it is kept
  - Quick identification of areas containing protected data can help with messaging:
    - "Currently we have seen no indication of exfiltration of patient or employee data, nor have we seen any improper access to such data."

Concerns during incident

- Where is your protected data? (cont.)
  - It's never (just) what you think
    - PII/ePHI certainly, but what about:
      - Employee data
      - Retiree data
      - Volunteer data
      - Donor data
      - Biometrics
      - On-line account credentials
      - Digital signatures
      - Anything else that individuals might reasonably expect that you would keep private and secure, especially in light of privacy policies

Concerns during incident

- The ransom process
  - – Timing – is there a clock or not?
  - – Currency – usually BTC
  - – Ransom amount
    - Can vary – one price for everything or pay by the encrypted server/endpoint
  - – Try before you buy?
    - Test decryption

Concerns during incident

- The ransom process (cont.)
  - Method of communication with threat actor:
    - Message board
    - E-mail address
    - Help-line (group chat)/FAQs
  - Timing of communication with threat actor:
    - Usually responsive, but often a delay due to differing time zones
  - Negotiating with the threat actor:
    - Can be helpful, especially with known ransomware resolution vendors, but can take time

Concerns during incident

- The ransom process (cont.)
  - Acquiring BTC
    - Need a vendor with enough BTC in its wallet
    - Panel vendors will often front the BTC if a carrier involved
    - If not, have you planned how to get a wire out while your systems are down?
  - Paying the ransom
    - Can take time for payment to be acknowledged
    - Threat actors can double-dip, esp. in Bitpaymer attack

Concerns during incident

- The ransom process (cont.)
  - Obtaining the key
    - Keys often work, but not on their own
    - The software used to apply the key is often poorly written/ buggy
      - Ransomware resolution vendors sometimes have their own software you use to apply the key
    - Key and software must be sandboxed and analyzed by vendor to check for malware
    - Probably 8-24 hours between payment and when you can use the key

Concerns during incident

- The ransom process (cont.)
  - Using the key
    - Keys often work, but sometimes they don’t
    - Can take 2-3 tries or more to decrypt a specific system or endpoint
    - Once you decrypt a system or endpoint, it may not work
      - E.g., database corruption
    - Decrypting can take much longer than encrypting
      - Sometimes 2-3x or more
    - What systems do you decrypt first and in what order thereafter?
    - Once you decrypt, the system is still compromised
    - Decrypt only where necessary to restore data
      - Reimage/replace compromised system thereafter

Concerns during incident

- The ransom process (cont.)
  - Other considerations
    - Even if you don’t plan on paying, it’s probably good to keep the threat actor engaged
    - You can (sometimes) get an extension
      - Or at least keep track of whether a clock is running
    - A lower ransom amount may change your payment analysis
      - As can a doubled demand
    - Keep your options open in case your backups turn out to be not as robust as hoped

Concerns during incident

- Messaging
  - To disclose or not to disclose
    - Cultural question with practical and legal implications
    - Controlling the narrative is helpful, but not guaranteed to succeed
  - You won’t have much time to preemptively disclose if some or all of your systems are down
    - The message will get out, usually within 24 hours
  - If you don’t use external PR/crisis communications, who will monitor media outlets for coverage?
  - Who will monitor social media?
  - Use the news cycle in your favor
    - If there’s nothing to report, the media can lose interest
  - Nothing kills a story like good news

Concerns during incident

- Messaging (cont.)
  - Vet all public-facing statements with counsel
    - Can start the clock running in relation to notification
  - Have one point person for external communication, to keep the message consistent
  - Media inquiries will often be focused on data exfiltration
    - Potential to re-focus on “good news” of no exfiltration
  - Never lose an opportunity to praise your staff in its incident response or focus on other good news concerning the incident
    - E.g., no impact on patient care, no rescheduled procedures, all facilities still open an accepting patients

Concerns during incident

- Messaging (cont.)
  - Key points:
    - Victim of sophisticated, criminal attack
    - Working with law enforcement
    - Working with experienced security professionals
    - No impact on patient care
    - No evidence of exfiltration
    - We drill for just such an occurrence

Concerns during incident

- Other concerns
  - – Was this a ransomware-only attack, or are there other vectors to consider (e.g., banking trojan)
  - – Document preservation
    - A preservation notice will issue from counsel
    - Preserve it all (notes, messages, e-mails, executables, images, etc.)
      - – When in doubt, preserve
      - – But – you can likely reimage systems if you preserve the ones that were likely material, e.g., patient zero

Concerns to address post-incident

- Insurance claim
  - Will you handle internally or externally?
  - Business interruption
    - what is covered under your policy?
    - how long will it take to measure BI effect?
    - how will you measure BI effect?
  - Involve counsel for narrative, inclusion of valid BI elements under policy
  - Count on a discount from what you claim
  - Know what isn't covered
    - E.g., endpoint replacement

Concerns to address post-incident

- IR Plan
  - How well did it run?
  - What were the stress points?
  - What did you forget to include?
  - How can you make it shorter?
  - IR team debrief
    - Get input from all material stakeholders
    - Engagement will fuel engagement
  - Review and revise, or document why you are not reviewing and revising
    - Make all judgment calls under privilege

Concerns to address post-incident

- Vulnerability Assessment and Pen Test
  - – Conduct after sanitized network is in place
  - – Benchmark to show that network has indeed been sanitized
    - Effectively an “all clear” bell
  - – Without this, hard to claim good faith in making use of sanitized network
  - – Will your carrier pay for this? Look at the policy.
  - – Conduct under privilege

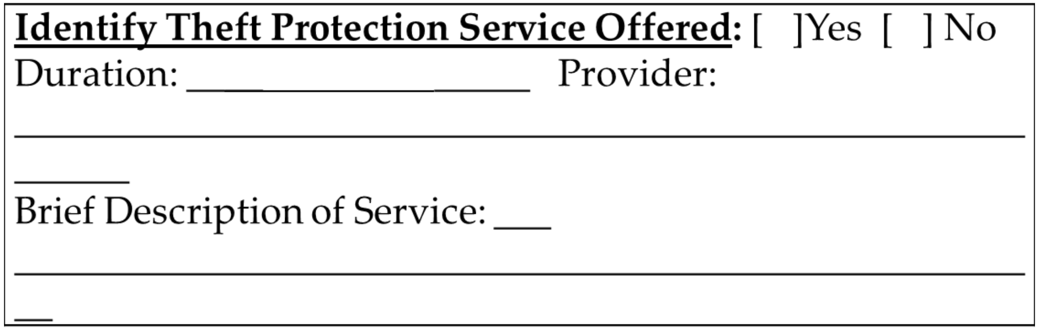
Concerns to address post-incident

- Reporting
  - States – unauthorized acquisition or access is the key
    - Sometimes likelihood of harm required
  - HIPAA guidance: ransomware is security incident, rebuttable breach presumption applies if ePHI affected, taking into account:
    - the **nature and extent** of the protected health information involved, including the **types of identifiers** and the likelihood of re-identification;
    - the **unauthorized person** who used the protected health information or to whom the disclosure was made;
    - whether the protected health information was **actually acquired or viewed**; and
    - the extent to which the risk to the protected health information has been **mitigated**
  - Should I report in all affected states, even though some state rules may not apply?

HSE

Concerns to address post-incident

- Credit Monitoring/ID Theft Protection
  - Should I offer it?
  - Pricing is low (<$4 per individual upfront and <$35 per *subscribed* individual for 3 agencies for 1 year, <20% subscription rate); price goes down as numbers go up
  - Required in some states, but not in New York, officially



Identify Theft Protection Service Offered: [ ]Yes [ ] No
Duration: ____________________ Provider:
____
______
Brief Description of Service: ___
____
__

Concerns to address post-incident

- If you paid, will you be a target again?
- How will you address ransomware in your next risk assessment?
- Can you replicate the attack vector in the next pen-test/vulnerability assessment
  - If you pass, document
  - If you fail, correct, document, and re-test
- Any changes necessary to:
  - Downtime procedures?
  - Messaging?
  - Ransom considerations?
  - Vendors?
  - Carrier/policy?

And now the fun begins . . .

- All 50 states have data breach reporting standard that can be triggered by a ransomware attack
  - NAAG may become interested in a multi-state incident
- 23 N.Y.C.R.R. Part 500 can require reporting to the Department of Financial Services, even if the attack is unsuccessful
- HIPAA requires reporting of a ransomware attack if it meets the HIPAA definition of a breach
- The FTC Act certainly applies if you were partially at fault for the attack, or made promises you didn’t keep, and there is a negative effect on consumers (or employees)

HSE

Harter Secrest & Emery LLP

ATTORNEYS AND COUNSELORS

ROCHESTER • BUFFALO • ALBANY • CORNING •NEW YORK CITY

This presentation is provided as a service to clients and friends of Harter Secrest & Emery LLP. It is intended for general information purposes only and should not be considered as legal advice. The contents are neither an exhaustive discussion nor do they purport to cover all developments in the area. The reader should consult with legal counsel to determine how applicable laws relate to specific situations. Attorney Advertising. Prior results do not guarantee a similar outcome.