Morgan Lewis

RANSOMWARE CHECKLIST

PHASE I
Alert and Organization

1. Upon detection of suspicious activity, record date, time, and method of alert
2. Contain incident, including by possible shutdown or disconnection of affected systems, to be approved by CEO, CIO, CISO, GC, or equivalent
3. Notify internal Incident Response Team (IRT):
   a. Information Technology
   b. Legal/Compliance
   c. Outside Counsel (Morgan Lewis)
   d. HR
   e. Public Relations
   f. Customer Service
   g. Executive
   h. Other as necessary given incident
4. Identify an Incident Lead – performs as project manager
5. Contact outside counsel at Morgan Lewis
6. Notify insurance carrier/understand approved vendors or limitations on reimbursement
7. Convene conference call of IRT
8. Outside counsel hires forensic technology partner
9. Check with counsel on attorney-client privilege in the data breach investigation
10. Issue document preservation directive and get instructions on preserving evidence
11. Gather any ransom notes or other indicators of threat actor activity, identify threat actor
12. Consider having outside counsel contact law enforcement

PHASE II
Initial Scoping

1. Identify, document, and preserve scope of compromise within 24–48 hours
2. Undertake steps to prevent harm
3. Consider engaging with threat actors through negotiator hired by outside counsel

PHASE III
Contain the Breach

1. Be sure that the full scope of compromise, including encryption and status of backups, is understood to the extent possible within 24–48 hours
2. Contain/arrest the breach—stop encryption and any possible flow of data to unauthorized recipients
3. Document results of containment effort
4. Explore discussions with threat actors as a method of containment or recovery

PHASE IV / V -- SIMULTANEOUS
Threat Actor Negotiations

1. Obtain and evaluate history of this particular threat actor's conduct
2. Establish criteria for potential payment
3. Obtain approval from CEO or equivalent. Inform Board or equivalent. Obtain insurance approval
4. Have special negotiator conduct all negotiations
5. Be clear about what will be provided in exchange for payment
6. Justify payment in terms of harm prevented

7. Understand the risks involved with the currency requested and the fluctuation of any currency conversion
8. Before any payment is made, conduct checks for OFAC or other potentially relevant AML/sanctions requirements

Investigation

1. Root cause analysis
2. Identify date, time, and cause of initial point of entry
3. Identify nature of compromise of any data – access, encryption, exfiltration, other including from any information provided by threat actors
4. Full identification of data compromised through data mining if necessary
   a. Type of information compromised
   b. Individuals whose information was compromised, including where they reside
5. Determine nature of any unauthorized recipients
6. Assess potential use of compromised information
7. Undertake security updates necessary before notification
8. Minimize distractions to investigative team, including deferring requests for conference calls with outside stakeholders if possible

PHASE VI / VII SIMULTANEOUS

Notifications (In Light of Information Developed in Phase IV)

1. Before notifications
   a. Develop PR plan for potential media inquiries
   b. Consider notification to Board or others who should be notified before public
   c. Prepare for inquiries from affected individuals—call center or other
2. If required by law or contract, or recommended because individuals could prevent further harm to themselves, make notifications to affected individuals. If made,
   a. Include what happened, what the company has done, and what the individual can do to prevent any harm
   b. Include legally required information and resources available from government agencies
   c. Consider an offer of identity theft prevention/credit monitoring depending on nature of information compromised
3. Notifications to government agencies and Attorneys General as required by law
4. Other notifications as required by information at issue
5. Evaluate feedback and determine if additional steps/notifications are required.
6. Respond to any government follow ups
7. Anticipated inquiries from financial auditors

Recovery

1. Only bring systems back online when safe, back doors are eliminated, and vulnerability is understood and addressed
2. Develop a timeline for recovery, anticipating recovery will take longer than expected
3. Provide updates on adjustments to timeline

PHASE VIII

Post-Notifications

1. Disclosures to investors, stockholders, SEC, securities disclosures, etc.
2. Cost recoveries—responsible third parties, insurance, other
3. Consider longer-term security upgrades or other measures to prevent reoccurrence or similar events
4. Analyze data breach notification plan/checklist for necessary changes in light of lessons learned
5. Prepare final reports
   a. Executive report with a summary of what happened, how it was addressed, what notifications were provided, and steps taken to prevent future incidents of the same or similar nature
   b. Technical report with detailed background of the event; evidentiary backup for analysis, decisions, and conclusions; and evidence of preventative measures

REMINDERS

- Maintain confidentiality—update IRT and executives frequently; otherwise need to know basis only
- Preserve evidence and information for future investigations
- Document events with dates and times; record reasons for determinations made
- The EU GDPR has a 72-hour deadline for some notifications; check early with outside counsel about whether it applies and how to manage it

Morgan Lewis

HOW WE CAN HELP

If we can be of assistance regarding your data collection, maintenance, protection, or suspected breach, contact a Morgan Lewis lawyer listed below:

Gregory T. Parks
Philadelphia
+1.215.963.5170
gregory.parks@morganlewis.com

Reece Hirsch
San Francisco
+1.415.442.1422
reece.hirsch@morganlewis.com

Mark L. Krotoski
Silicon Valley
+1.650.843.7212
mark.krotoski@morganlewis.com

Pulina Whitaker
London
+44.20.3201.5550
pulina.whitaker@morganlewis.com

Ezra D. Church
Philadelphia
+1.215.963.5710
ezra.church@morganlewis.com

Kristin M. Hadgis
Philadelphia
+1.215.963.5563
kristin.hadgis@morganlewis.com

Connect with us

www.morganlewis.com

061421_211040