Ransomware Tabletop Exercise—Healthcare

Tabletop Exercise

5:00 p.m. Friday evening.

An IT employee discovers that malware has been detected on the network. Anti-virus software is unable to delete or quarantine the malware. IT has also received a network intrusion alert and is detecting increased network activity related to multiple servers on the network, some of which contain sensitive data.

The suspicious computer network activity appears directed at encrypting various network files. IT receives a demand for 10 Bitcoins to restore encrypted files, payable within 3 days.

Tabletop Breach Exercise

Known Facts: 5:00 p.m. Friday evening.

An IT employee discovers that malware has been detected on the network. Anti-virus software is unable to delete or quarantine the malware. IT has also received a network intrusion alert and is detecting increased network activity related to multiple servers on the network, some of which contain sensitive data.

The suspicious computer network activity appears directed at encrypting various network files. IT receives a demand for 10 Bitcoins to restore encrypted files, payable within 3 days.

- Do you pay the ransom? If so, how?
- Is this a breach? What additional information is needed to determine this?
- Who needs to be notified regarding the incident at this point?
  - Incident Response Team? Insurers? Vendors? Law enforcement?
- What, if anything, can or should be done to remediate this incident?
  - sever access to all hosted applications and servers?
  - shut down cross connections between hospitals?
  - shut down internet connections enterprise-wide?

Tabletop Breach Exercise

6:15 p.m. Friday.

IT reports that the ransomware has spread throughout the network. IT also believes that the increased network traffic could indicate data exfiltration from servers containing sensitive information, but additional analysis is required to confirm. IT recommends engaging an outside forensics firm for assistance with the investigation.

IT advises that it will need to shut down the entire network, including data center circuits, in order to prevent the malware from spreading and to remove the malware.

Tabletop Breach Exercise

Known Facts: 6:15 p.m. Friday.

IT reports that the ransomware has spread throughout the network. IT also believes that the increased network traffic could indicate data exfiltration from servers containing sensitive information, but additional analysis is required to confirm. IT recommends engaging an outside forensics firm for assistance with the investigation.

IT advises that it will need to shut down the entire network, including data center circuits, in order to prevent the malware from spreading and to remove the malware.

- Is this a breach? What additional information is needed to determine this?
- Who needs to be notified regarding the incident at this point?
  - Incident Response Team? Insurers? Vendors? Law enforcement?
- Engage an outside forensics firm? Benefits? Drawbacks? How do you do this?
- Proceed with network shut down?
  - Operational impact?
  - Downtime procedures? Disaster procedures?
  - Communications plan?

Tabletop Breach Exercise

During the shutdown, how will you: (1) communicate; (2) operate; (3) order supplies; (4) pay bills.

An outside forensics firm will be on-site tomorrow to investigate the scope of the malware infection. Outside counsel is also available.

Tabletop Breach Exercise

Known Facts:

During the shutdown, how will you: (1) communicate; (2) operate; (3) order supplies; (4) pay bills.

An outside forensics firm will be on-site tomorrow to investigate the scope of the malware infection. Outside counsel is also available.

- What is the communications and operations plan during the outage?
  - Patient diversion?
  - Communications during outage?
  - Additional resources available to address IT complaints?
  - What is the appropriate explanation for the shut down? Discuss the attack?
  - Address operational impact. (Paper records)?
- Did the shutdown work? How is this confirmed? By whom?
- What preparations are necessary for the forensics firm? Chain of custody?

Tabletop Breach Exercise

8:15 a.m. Saturday morning.

The outside forensics firm arrives onsite and begins its investigation.

At least 1,000 servers and workstations are infected—including those from HR, finance, operations, hospital workstations, and several physicians' workstations. Images of all drives are taken by the forensics firm, as well as log files illustrating network activity. Review of this information could take several days.

Tabletop Breach Exercise

Known Facts: 8:15 a.m. Saturday morning.

The outside forensics firm arrives onsite and begins its investigation.

At least 1,000 servers and workstations are infected—including those from HR, finance, operations, hospital workstations, and several physicians' workstations. Images of all drives are taken by the forensics firm, as well as log files illustrating network activity. Review of this information could take several days.

- Is this a breach? What additional information is needed to determine this?
- Who needs to be notified regarding the incident at this point?
  - Incident Response Team? Insurers? Vendors? Law enforcement?
- What can be done while the forensics review is pending?

Tabletop Breach Exercise

12:00 p.m. Monday afternoon.

The outside forensics firm has confirmed files from various network servers and files from the infected workstations were encrypted by the ransomware.

IT has confirmed that at least some of the affected files contain current and former employees' HR-related information, including names, addresses, Social Security numbers and financial account numbers.

IT has also confirmed that some of the affected files contain clinical and diagnosis information for patients. A review of these files is ongoing.

Tabletop Breach Exercise

Known Facts: 12:00 p.m. Monday afternoon.

The outside forensics firm has confirmed files from various network servers and files from the infected workstations were encrypted by the ransomware.

IT has confirmed that at least some of the affected files contain current and former employees' HR-related information, including names, addresses, Social Security numbers and financial account numbers.

IT has also confirmed that some of the affected files contain clinical and diagnosis information for patients. A review of these files is ongoing.

- Is this a breach?
- Who needs to be notified regarding the incident at this point?
  - Insurers? Vendors? Law enforcement?
- Timing concerns?
  - What is the discovery date?

Tabletop Breach Exercise

4:45 p.m. Tuesday afternoon.

IT begins application/systems restoration process based upon clinical priorities.

Tabletop Breach Exercise

Known Facts: 4:45 p.m. Tuesday afternoon.

IT begins application/systems restoration process based upon clinical priorities.

- Which systems and applications have priority? How is the plan communicated?
- What can be done while the forensics review is pending?

Tabletop Breach Exercise

8:15 a.m. Next Wednesday morning.

Further review has determined that the following information was encrypted during the event and is not recoverable (and the time to pay the ransom has passed).

- Patient Info: Names, addresses, and clinical and diagnosis information for 2,320 patients with addresses in CT, RI, MA, and NY.

Additionally, forensics has found evidence of potential exfiltration of data related to the HR systems, including:

- Staff Info: Names, mailing addresses, SSNs, and health insurance identification numbers for 554 current and former staff with addresses in CT, RI, MA, and NY.

Tabletop Breach Exercise

Known Facts: 8:15 a.m. Next Wednesday morning.

Further review has determined that the following information was encrypted during the event and is not recoverable (and the time to pay the ransom has passed).

- Patient Info: Names, addresses, and clinical and diagnosis information for 2,320 patients with addresses in CT, RI, MA, and NY.

Additionally, forensics has found evidence of potential exfiltration of data related to the HR systems, including:

- Staff Info: Names, mailing addresses, SSNs, and health insurance identification numbers for 554 current and former staff with addresses in CT, RI, MA, and NY.

- What do you do with this information? How do you determine notification obligations?
- How many letter versions are necessary? What language must be included?
- Should credit monitoring be offered? To whom? How?
- Do state/federal regulators need to be notified?
- Can [Organization] mail over 2,500 letters? Engage a notification vendor?
- Is [Organization] equipped to handle calls from those affected? Call center?

Tabletop Breach Exercise

4:15 p.m. Wednesday afternoon.

The CEO is requesting an immediate update as to the status of the investigation in order to advise the Board.

Tabletop Breach Exercise

Known Facts: 4:15 p.m. Wednesday afternoon.

The CEO is requesting an immediate update as to the status of the investigation in order to advise the Board.

- What is the appropriate response for leadership?

Tabletop Breach Exercise

8:15 p.m. Wednesday night.

Additional analysis of the affected files indicates the following:

- Patient Info: 500 of the 2,320 affected patients are deceased.

Tabletop Breach Exercise

Known Facts: 8:15 p.m. Wednesday night.

Additional analysis of the affected files indicates the following:

- Patient Info: 500 of the 2,320 affected patients are deceased.

- How is your notification strategy impacted by decedents? Additional letter versions? Credit monitoring considerations? Regulatory notification?
- How quickly can you mail notices?

Tabletop Breach Exercise

3:15 p.m. Thursday afternoon.

A local TV station reporter interviews a current employee and several former employees about the incident. The TV station contacts [Organization]'s media contact one hour before they are scheduled to broadcast the interviews.

Tabletop Breach Exercise

Known Facts: 3:15 pm Thursday afternoon.

A local TV station reporter interviews a current employee and several former employees about the incident. The TV station contacts [Organization]'s media contact one hour before they are scheduled to broadcast the interviews.

- How do you handle the media reports?
  - Go public?
  - Who should respond? Scripting?
  - Expect additional calls from media / concerned citizens?
- What should be done regarding the employee interviewed?

Tabletop Exercise Discussion

- When was the Incident Response Team notified?
- Do you need to notify? If so, who? How?
- Do you need a fulfillment house that can generate the necessary notification letters, or handle in-house?
- Are you going to handle calls internally or rely on a vendor?
- Risk assessment per HHS ransomware guidance?
- Report to law enforcement?
- Prepare notifications
- Call center? Prepare scripts and escalation procedure
- Finalize discussions with re: credit monitoring firm?
- Notify AG office(s)?
- Prepare press release to media?
- Website notice?
- Internal communications? employees, senior management, Board

Tabletop Exercise Discussion

Self-Assessment

Questions to ask yourself at the end:

- Walk through the Incident Response Team's analysis and plan of action
- Discuss each step in the plan of action
  - Look for missed steps
  - If the Incident Response Team made mistakes, identify problems that would have ensued
  - Discuss potential alternatives

Post Mortem

- What went right?
- What went wrong?
- Did the plan work as intended?
- How can the plan be improved?