HUNTON
ANDREWS KURTH

Privileged and Confidential: For Internal Use Only

Apple Bank
Cybersecurity Tabletop Exercise

November 17, 2021

Lisa J. Sotto
Hunton Andrews Kurth LLP
(212) 309-1223
lsotto@hunton.com
www.huntonprivacyblog.com

Apple Bank:
Cybersecurity Tabletop Exercise

This cybersecurity tabletop is intended to help prepare Apple Bank in the event of a cybersecurity incident and strengthen the bank's incident response processes. This exercise draws from actual cybersecurity events and applies the facts to a complex cybersecurity hypothetical.

THE TROUBLE BEGINS

HUNTON
ANDREWS KURTH

Apple Bank employees are reporting to the Service Desk in droves that they are locked out of documents and apps needed to do their work. Employees are puzzled and seeking answers.

Service Desk escalates to Information Security which begins looking into the issue and a few hours later discovers a message on several of Apple Bank's servers saying:

> *We've hacked your network and now all your files, documents, databases and other important data are encrypted. But don't worry. You can get them back! We also have downloaded a lot of private data from your network.*
>
> *If you don't contact us within 3 days, we'll throw away the key to unlock your files and will destroy your data forever. To contact us, you'll need to visit our website on a hidden TOR network. Follow the instructions below.*

EXTERNAL SUPPORT JOINS THE TEAM

HUNTON ANDREWS KURTH

On numerous servers and laptops, Information Security has detected indicators of compromise suggesting that the issue involves a ransomware variant known as DarkEvil. At this time, little is known about the source of the intrusion.

[Apple Bank Response]

The Bank's General Counsel calls outside counsel and explains the situation. Outside counsel recommends engaging an external forensic expert familiar with the DarkEvil ransomware. They also discuss engaging a ransomware negotiation specialist.

THE NEGOTIATION BEGINS

HUNTON ANDREWS KURTH

Following a strategy session with the bank, the ransomware negotiation specialist contacts the attacker for more information.

The attacker takes credit for the recent ransomware plaguing the bank and claims to have downloaded 300 GB of data from Apple Bank's network, including files containing customer and employee information. The attacker demands $30 million in Monero for the decryptor and deletion of the stolen files, with a threat to double the asking price if Apple Bank does not pay quickly.

The attacker also threatens to publicize the attack against Apple Bank on the attacker's public website if the bank does not pay within 5 days, and to post Apple Bank's stolen files on the website if payment is delayed beyond one week.

INFORMING THE BOARD

HUNTON ANDREWS KURTH

The General Counsel confers with the CEO. They arrange a call with Apple Bank's Board of Directors to discuss the situation.

The CEO convenes a call later that evening. Some Board members raise concerns in light of recent headlines regarding large-scale ransomware attacks and some ask questions about their own potential liability.

Apple Bank also considers reaching out to NYDFS and the FDIC to let them know about the situation.

[Apple Bank Response]

MORE CHAOS ENSUES

HUNTON ANDREWS KURTH

The bank's forensic investigator identifies signs of potential compromise on the bank's MISER BI system and recommends proactively taking down the system until further analysis can be performed.

[Apple Bank Response]

THE BAD NEWS MOUNTS

HUNTON ANDREWS KURTH

Apple Bank's ransomware negotiation specialist receives an evidence pack from the attackers. The evidence pack contains a sample of files allegedly stolen from the network.

Information Security quickly confirms that the sample contains Apple Bank documents and records pertaining to customers and employees, non-public financial figures, confidential regulatory correspondence and strategic plans. The sample is believed to come from various systems that host business information.

Meanwhile, IT continues to look for data backups. Some of the backups are out of date or corrupted and would result in Apple Bank losing new data stored in certain systems over the past 6 months.

[Apple Bank Response]

THE ATTACKER REACHES OUT

HUNTON ANDREWS KURTH

A number of Apple Bank employees are reporting that they received a suspicious email with the following message:

> *Do not try to recover data. Don't forget that your data has been stolen. Stolen data: email correspondence, HR records, customer information, financial documents, etc.*

Attached to the email is a directory listing with thousands of file folders on Apple Bank's network that the attacker is claiming to have stolen.

In addition, several of the bank's senior executives and Board members have received calls that appear to be from the attacker.

THE PLOT THICKENS

HUNTON
ANDREWS KURTH

Communications receives a call from a reporter at BleepingComputer, a news publication notorious for covering (and breaking) stories regarding cybersecurity incidents. The reporter is hearing rumors from sources that the bank's systems were hit with ransomware and that Apple Bank paid to recover its data. She also heard that the bank's ATMs are down as a result of the incident and that the bank has weak security controls that contributed to the incident.

The reporter asks if Apple Bank has any comment and lets the bank know that she intends to publish a story quickly (with or without the bank's input or cooperation).

THE FBI CALLS

HUNTON ANDREWS KURTH

The FBI calls the CISO to let Apple Bank know that the Bureau is seeing chatter on the dark web regarding a cyber attack against the bank. It is possible that a rogue actor affiliated with the DarkEvil group is behind the dark web activity. The FBI warns the CISO that the bank may receive an additional ransom demand from the rogue DarkEvil actor.

BREAKING NEWS

HUNTON
ANDREWS KURTH

BleepingComputer has published its story and the media is beginning to disseminate it. Various national media outlets, bloggers and trade journals have picked up the story and are buzzing about a possible cyber attack against Apple Bank. The story is lighting up social media. Some aspects of the stories are clearly inaccurate, but some quotes attributed to Apple Bank executives lead people to wonder if there is a leak inside the bank.

In the meantime, IT and the investigator have isolated the systems known to be infected and believe the ransomware contagion may be contained.

Apple Bank chose not to pay the ransom.

THE ONSLAUGHT

HUNTON ANDREWS KURTH

Apple Bank is expected to have answers to questions that are coming from all angles.

- The bank has received a barrage of calls and emails from news media asking about the cyber attack.
- Individuals are Tweeting @applebankcare asking about the bank's handling of the issue. Most of the Tweets are snide and highly critical.
- CustomerLine has reached maximum capacity. Many customers are asking if their data is safe and how they will be notified and compensated.
- Employees are calling HR asking if their data is at risk and whether they'll be offered credit monitoring services to protect their information.
- Visa has called with questions regarding the impact of the incident on Apple Bank's payment card data.
- The bank's external auditors ask for details about the incident to understand whether financial controls may have been affected.
- The Board requests an update.

PATIENT ZERO IS DISCOVERED

HUNTON ANDREWS KURTH

IT and the forensic investigator have been working around the clock taking snapshots of affected systems, restoring backups and reconfiguring or rebuilding affected systems. Some of Apple Bank's backups unfortunately were encrypted by the ransomware and others can only be partially recovered. The attacker also has dropped the demand to $12 million in Monero. Meanwhile, employees continue to ask when their access to the bank's systems will be restored.

The forensic investigator also is sifting through mounds of logs to detect indicators of compromise on systems across the network. In a new development, the forensic investigator has identified a VPN misconfiguration and suspects that the misconfiguration enabled the attacker to gain a foothold inside Apple Bank's network. IT immediately begins fixing the misconfiguration.

NEW DEVELOPMENT

HUNTON ANDREWS KURTH

Apple Bank receives calls from two of the bank's largest business customers claiming that they have identified files with their confidential financial information on the DarkEvil website. The website claims the files came from Apple Bank's systems and takes credit for the recent ransomware attack against the bank.

The customers demand answers and request that their own forensic investigators be granted immediate access to Apple Bank's systems to conduct an onsite investigation.

WHAT THE INVESTIGATION FINDS

HUNTON ANDREWS KURTH

Apple Bank's forensic investigator has determined that the attacker deployed anti-forensic tools to delete most of its tracks from Apple Bank's systems. Nevertheless, the forensic investigator found signs of access to systems maintaining:

- Customer information (including customer names, contact information, SSNs, bank account details and online banking access credentials)
- Business customer information (including business names, bank account details, tax ID numbers and loan records)
- HR records (including a spreadsheet storing employees' unencrypted SSNs, bank account information and tax data)
- Apple Bank employee emails (including several executive email accounts containing embarrassing personal details and highly sensitive customer communications)
- Confidential regulatory information (including confidential supervisory information, correspondence with regulators, and regulatory filings)
- Highly sensitive business information (such as strategic plans and forecasts, non-public financial data and confidential regulatory information)

INVESTIGATION WRAP-UP

HUNTON ANDREWS KURTH

The forensic work wraps up:

- The investigator has found signs that the attacker had broad and persistent access to the bank's systems for a month and exfiltrated data from many of the affected systems.
- The attacker continues to post Apple Bank data on its shaming website. The data contains some, but not all, of the suspected files and records from a number of the affected systems.
- Apple Bank has identified which customers and employees are impacted. Individuals in numerous U.S. states and some overseas jurisdictions are affected.
- NYDFS has asked for a meeting to discuss the incident and requested a copy of any formal investigation reports that have been prepared.
- Apple Bank's external auditor has asked for an on-site audit to review systems affected by the incident and also sends a list of information requests.

WHAT HAPPENS NEXT?

HUNTON ANDREWS KURTH

Fast forward one month. Apple Bank has notified affected individuals and business customers and relevant regulators. The bank now receives notice about a number of actions brought in the wake of the incident:

- Apple Bank receives putative class action complaints filed in state court from customers claiming that their compromised personal information was used to commit fraud and identity theft.
- Certain business customers whose financial information was impacted are seeking contractual remedies under their agreements with the bank, claiming that the compromise caused a loss in revenue and company value.
- The FDIC has sent the bank a list of questions regarding the incident. They also have asked the bank to provide a comprehensive report regarding the confidential supervisory information impacted by the incident.
- NYDFS is conducting an investigation into the incident and Apple Bank's data security practices.
- Senators Schumer and Gillibrand have sent Apple Bank a letter expressing grave concern over the security of the bank's systems and requesting information about the bank's cybersecurity program.

LESSONS LEARNED

HUNTON ANDREWS KURTH

- Would Apple Bank ever pay ransom and how?
- What did Apple Bank do right?
- What will Apple Bank do differently next time?

Lisa J. Sotto
Partner
Privacy and Cybersecurity Practice
Hunton Andrews Kurth LLP
(212) 309-1223
lsotto@hunton.com
www.huntonprivacyblog.com

@hunton_privacy