GT GreenbergTraurig

Breach Tabletop Scenario

Reena Bajowala | reena.bajowala@gtlaw.com | 312.456.1018
Jena Valdetero | jena.valdetero@gtlaw.com | 312.456.1025

September 14, 2023

GT GreenbergTraurig

Our Victim Company – Silicon Valley Tech

- SVT is a California-based fintech company
- Create software utilized by financial institutions to reconcile deposits and debits
- 1,000 employees, mostly in California
- 500 B2B clients, including major banks
- Recently went public on NYSE

GT GreenbergTraurig

Friday, January 5, 2024

9:00 AM

- **SVT** employees arrive at work and find a ransom note on their computer screens advising that computer networks have been encrypted, claiming data was exfiltrated, and demanding **SVT** contact the threat actor to discuss payment.

- **SVT's** production service databases have all been encrypted, including email, which is hosted on premise. All relevant services are currently down and nonfunctioning, impacting functionality for all financial institution customers.

- Employees begin contacting supervisors and IT demanding information.

GT GreenbergTraurig

Friday, January 5, 2024

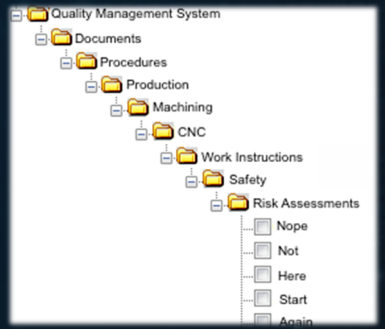
5:00 PM

- IT believes that the backups are available. To get a sense of whether data was exfiltrated, the IRT begins negotiations with the threat actor.
- The IRT has retained legal counsel, who has retained a forensic investigator and **vendor** to negotiate the ransom.
- **SVT** contacts the hacker, who demands bitcoin worth approximately ***$12 million USD*** to provide the decryption key and delete stolen data.

GT GreenbergTraurig

Monday, January 8, 2024

8:30 AM



- During the course of negotiations, the threat actor confirms that it has exfiltrated **600 GB** of data. As proof, they provide a file tree showing the file structure of the exfiltrated data.
- The file tree contains documents from the Windows file server, including folders with data that is several years old and contains sensitive PII belonging to at least 50 business customers.
- If **SVT** does not pay the ransom, the threat actor will release the files contained on that file tree onto its dark web shame site.

GT GreenbergTraurig

Monday, January 8, 2024

12:30 PM

- **SVT** begins receiving calls from clients, complaining about the continued delay of restoration of their services and expressing concern about possible lateral infection of their systems. Some are threatening to withhold paying invoices.
- Multiple clients are demanding individual daily update calls until the situation is resolved.
- The threat actors begin to get restless and begin making phone calls to SVT's executives, including at their homes.

GT GreenbergTraurig

Thursday, January 11, 2024

4:00 PM

- After extensive negotiations, **SVT** has paid the ransom, received the decryption keys, and is mostly operational while it continues to restore its networks.
- The IRT has hired an additional vendor to review the exposed data and to determine which business clients and individuals were impacted.

GT GreenbergTraurig

Friday, January 12, 2024

9:00 AM

Brian Krebs, from the website ***Krebs on Security***, contacts **SVT's** Director of Communications and tells her that he intends to run a story at **6 p.m.** focusing on the ransomware attack and references rumors that data belonging to multiple financial institution clients was leaked on the dark web.

KrebsonSecurity
In-depth security news and investigation

GT GreenbergTraurig

Monday, January 15, 2024

9:00 AM

- The **Krebs Article** runs. The article immediately starts trending on social media and is picked up by several national news outlets as part of larger stories about increased cybersecurity attacks on third party service providers of major companies.
- **SVT** receives calls from ***The New York Times***, ***The Washington Post***, and ***USA Today*** seeking comment. Customers see the articles and begin to contact their relationship managers.

The Washington Post

The New York Times

GT GreenbergTraurig

Friday
January 19, 2024

1:00 PM

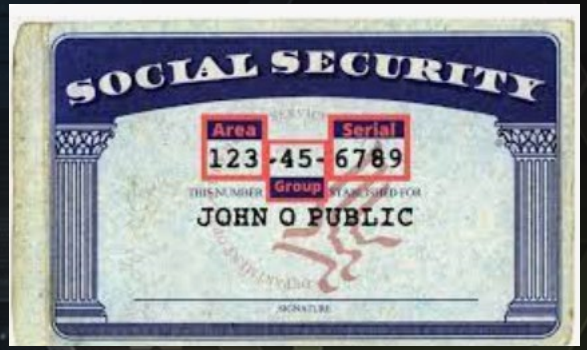
SVT's investigator determined that the attack vector was malware downloaded and installed by a user who was attempting to install what they believed to be a legitimate software update. The earliest date of access is September 14, 2023.

GT GreenbergTraurig

Thursday, March 1, 2024

12:00 PM

- The document review vendor gives **SVT** a list of individuals whose sensitive PII was found in the exfiltrated data.
- The list has SSNs for 2M individuals.



GT GreenbergTraurig

Monday, March 11, 2024

12:00 PM

- **SVT** finishes matching sensitive PII of individuals in the exfiltrated data set to the B2B financial institution client who owns the data.
- **SVT** sends notification to each affected B2B client, providing information about the affected data and offering to send notification letters on their behalf.

GT GreenbergTraurig

Friday, March 29, 2024

- **Greenberg Traurig** identifies a class action lawsuit filed in the **Central District of California** on behalf of individuals that received a letter relating to the disclosure of their sensitive personal information.
- The lawsuit seeks actual damages and statutory damages of <u>up to $750 per person</u>.

GT GreenbergTraurig

Key Takeaways

- Cyber incidents are not solely an IT issue
- Prepare for the unknown
- Engage outside counsel early
- Actively manage communications with stakeholders (employees, customers, business partners, Board, regulators, public)

GT GreenbergTraurig

Jena M. Valdetero

312.456.1025

jena.valdetero@gtlaw.com

Jena M. Valdetero serves as Co-Chair of the firm's U.S. Data Privacy and Cybersecurity Practice where she advises clients on complex data privacy and security issues. She has led more than 1,000 data breach investigations. A litigator by background, Jena defends companies against privacy and data breach litigation, with an emphasis on class action lawsuits. She has designed and conducted dozens of data breach tabletop exercises to empower clients to respond effectively to a data security incident. She is a certified privacy professional through the International Association of Privacy Professionals (CIPP/US), for which she is a former KnowledgeNet Co-Chair.

GT GreenbergTraurig

Reena R. Bajowala

312.456.1018
Reena.Bajowala@gtlaw.com

Reena Bajowala has deep experience with data security, information technology, and privacy law issues, and litigating class, collective, and plan-wide litigation. She regularly conducts risk assessments, develops privacy and information security compliance programs, and leads proactive planning for potential data security incidents, including drafting incident response plans, communications plans, and conducting tabletop exercises. In addition, Reena helps evaluate legal risks relating to emerging technologies, including artificial intelligence, connected devices, and drones.

Questions