Sample Tabletop Breach Exercises

What is a Tabletop Breach Exercise?

- Structured data breach response drill
- Triggers your Incident Response Plan (IRP) for testing purposes
- Involves members of your Incident Response Team (IRT) (both internal and external members)
- Tests the effectiveness and accuracy of the workflow of your current IRP and IRT

2

Leaking the Hypothetical Facts

- Break-up the facts into realistic segments.
- Begin with a minimal amount of information, similar to the information you may receive when the incident is just discovered.
- Take a reasonable amount of time to come up with the plan and identify each IRT members' roles in the response process.
- Continue to distribute facts of the incident, giving the IRT time with each additional fact to develop a plan and prepare relevant response roles.

Tabletop Breach Exercise #1

- It’s 7:00 am on New Year’s Day.
- The Director of Alumni Relations just received a call from an Assistant Director that her car parked in her home driveway was stolen on New Year’s Eve.
- A laptop was in the back seat.
- She thinks the laptop contains Alumni information.

Tabletop Breach Exercise #1

IT and Assistant Director add a few more facts.

Known Facts:

The Director of Alumni Relations just received a call from an Assistant Director that her car parked in her home driveway was stolen on New Year's Eve. A laptop was in the back seat.

New Facts:

The laptop contained full names, Social Security numbers, financial account information and Alumni Log-in Information for 29,000 Alumni.

Assistant Director recalls that she was recently assisting in an HR project as well. The laptop also contained full names, Social Security numbers and dates of birth for 175 employees.

The laptop was not encrypted.

Tabletop Breach Exercise #1

36 hours later, Police add a few more facts.

Known Facts:

The Director of Alumni Relations just received a call from an Assistant Director that her car parked in her home driveway was stolen on New Year's Eve. A laptop was in the back seat. The laptop contained full names, Social Security numbers, financial account information and Alumni Log-in Information for 29,000 Alumni. Assistant Director recalls that she was recently assisting in an HR project as well. The laptop also contained full names, Social Security numbers and dates of birth for 175 employees. The laptop was not encrypted.

New Facts:

The Police have informed the Assistant Director that they have located the stolen vehicle a mile away from her home. The laptop is not in the vehicle.

Tabletop Breach Exercise #1

8 hours later, IT adds additional facts

Known Facts:

The Director of Alumni Relations just received a call from an Assistant Director that her car parked in her home driveway was stolen on New Year's Eve. A laptop was in the back seat. The laptop contained full names, Social Security numbers, financial account information and Alumni Log-in Information for 29,000 Alumni. Assistant Director recalls that she was recently assisting in an HR project as well. The laptop also contained full names, Social Security numbers and dates of birth for 175 employees. The laptop was not encrypted. The Police have informed the Assistant Director that they have located the stolen vehicle a mile away from her home. The laptop is not in the vehicle.

New Facts:

The Alumni whose personal information is on the laptop reside in Indiana, Michigan, Ohio, Indiana, Florida, New Jersey, California, Massachusetts and Vermont.

The employees whose personal information is contained on the laptop all reside in Indiana.

Tabletop Breach Exercise #2

- It’s Saturday afternoon.

- The Technical Support Center was just informed that a file server at main campus was impermissibly accessed 19 days ago.

Tabletop Breach Exercise #2

- Computer forensic experts reveal the additional information below **in bold**
- It's Saturday afternoon. The Technical Support Center was just informed that a file server at main campus was impermissibly accessed 19 days ago. **The intrusion first occurred through a Payroll Vendor's cloud server.**
- **The servers contained the PII of 22,515 individuals (ages 16-92) located in Illinois, North Dakota, Massachusetts, Maryland, New Jersey and New York. The PII involved in the breach included names, dates of birth, and SSNs.**

Tabletop Breach Exercise #3

- It’s 3:00 pm on Christmas Eve.
- The Director of HR just received a call from the Assistant Director of HR that she cannot log-in to her account.
- They attempt to call IT together, but everyone has gone home early due to the holiday.
- The Assistant Director takes her laptop home for the holiday break.

Tabletop Breach Exercise #3

- On the day after Christmas, the Assistant Director wants to catch up on some work and attempts to log-in again.
- She still cannot log-in.
- This time, however, she receives a message that if she pays $25, she can gain access to her account.
- Rather than call anyone, she pays the $25.
- After she pays, nothing happens. She is still locked out of her computer.
- She knows the laptop contains sensitive employee information.

Tabletop Breach Exercise #3

IT adds a few more facts.

The laptop was not encrypted in violation of company policy.

IT confirms that the laptop was infected with a type of ransomware/malware that encrypts a computer and prohibits access to certain files, folders and accounts.

IT is able to decrypt the laptop on January 7th.

Tabletop Breach Exercise #3

IT adds a few more facts.

Unfortunately, while working through the process of unencrypting the laptop and restoring it back to the network, IT has discovered that the ransomware could have also affected the student database.

IT cannot yet confirm the extent of the compromise to the student database or whether the incidents are linked.

Tabletop Breach Exercise #3

IT and HR add more facts.

The laptop contained information on 13,500 current and former employees and dependents, including names, Social Security numbers, dates of birth, drivers' license number, ACH information and log-in credentials.

The forensic firm is continuing its analysis of impact on the student database. It appears it may be limited to certain students from certain states.

Tabletop Breach Exercise #3

36 hours later, IT adds a few more facts.

IT confirms that from December 24th through January 6th, the computer was encrypted by an unknown party and files with PII were accessible to this third-party during this time.

The 13,500 current and former employees whose PII is on the laptop reside in California, Arizona, Indiana, and Pennsylvania.

Tabletop Breach Exercise #3

The forensic firm adds more facts.

The forensic firm confirms that the student database was compromised by the malware affecting 119,750 students' names, SSNs, Driver's License numbers, and tuition payment information (ACH / credit card)

The students whose PII is contained on the database that was compromised reside in California, Vermont, Massachusetts, Nevada, and Indiana.