Scenario 1
Turn by turn slides

These help the incident along.

Change the master slides to fit your company brand or templates

Cyber Incident

Gold team exercise

March 05 (@RSAC) | 2:20 pm

1: An email is received

MONDAY | 1:00 pm

- An email was sent to our Finance Director at 09:00 a.m. this morning. The sender claims to have direct access to our systems and to have extracted hundreds of thousands of our Customer/3rd Party details including credit card data.
- They say that unless they receive a ransom of $500,000 paid in bitcoin …
- Two deadlines:
  - Respond with intention by 3pm today
  - Pay the money by 1pm tomorrow
- If we don’t pay, data will be released to the public

1: An email is received

MONDAY | 1:00 pm

- We have 50 sample records from the attacker
- IT says they ”look credible”

I have direct access to your systems and have already taken hundreds of thousands of details including all your credit card data.

You need to pay me a ransom of $500,000 in bitcoin into 1AvAASEYstWetqTFn5Xu9m4GFg7xJgNVN2 by Tuesday 13:00 or I will put it all out there for all to see.

Contact me by 15.00 today confirming that address or I will tell all the media and everyone else that you have lost this data and lost all your systems. Here’s some of your data to show you.

2: Half an hour before the deadline

MONDAY | 2:30 pm

- IT say they have found no evidence yet of external access onto our systems; they're continuing to perform checks and monitor networks.
- Good news: Credit Card data provided by the attacker in those 50 records does not match live data held for those customers or companies. It only looks plausible; it can't be used directly in fraud.
- Bad news: but the data does contain valid Customer IDs, Names, Addresses, Phone Numbers, Email Addresses. The Customer IDs are unique to us so it's definitely our data. Customers could be vulnerable to Social Engineering attacks if contacted by fraudsters who know of their relationship to us and have this data.

3: End of the day

MONDAY | 6:00 pm

- There has been no further contact from the attacker
- IT think it could be test data
- There's noise on Twitter
- Reuters has contacted public relations
  - Have we lost data?
  - Have we lost Elon Musk's data?
- Twelve fraudulent payments have been found (and stopped) in the accounting system.
  - Entered by a colleague who is on holiday

4: It is definitely test data

TUESDAY | 9:00 am

- No evidence of intrusion
- Definitely system test data
  - Found a file of 50K customers like the attacker's
  - BUT credit card data all randomized!
  - i.e. Credit card numbers definitely of no use to the attacker in direct fraud
- We (sadly) don't have Elon Musk as a customer
- General media reporting of the data breach
- Another email from the attacker

```
Don't mess me around! If I don't have the money by the deadline
all the data will go to the media!!
```

5: The deadline for payment

TUESDAY | 1:00 pm

- No further contact from the attacker
- No further fraudulent payments
- Media claim to have the file

6: The attacker’s gone quiet

TUESDDAY | 5:00 pm

- No attacker contact
- Significant media reporting
- Lots of social media comment
- Requests for CEO interviews

Incident Wrap-up

Handout # 1.7

Questions

1. Response Planning Processes
2. Data
3. Communications
4. Ransom
5. Bitcoins
6. Overall