Scenario 1

Assumption: Non-anonymized drone data is retained for a month (for customer service reasons) before being discarded. Video is only retained for 24 hours, as specified in the Privacy Notice.
Assumption: The Sheriff sent the email the morning after the incident.
Assumption: The email was precise enough to allow identification of the problematic delivery.

Detect and Respond

- Open a new incident and log the initial details, formally starting the Incident Response process
- Working Hypothesis: The Sheriff is demanding a very broad range of information, some of which no longer exists. Our strategy is based on the premise that the Sheriff is more likely to back away from excessive demands if Tinkerbell provides prompt and relevant cooperation.
- Severity: S4 (Low). This situation should not inconvenience any customers except those who are breaking both the law and the terms of service.
- Activate Privacy IR Team: Despite the low severity, this team will need to include representatives from Legal, PR, Analytics, InfoSec and Privacy.

Contain

- Relevant data includes all aspects of the problem delivery
- Tinkerbell will retain and analyze the records connected to the delivery.
    - Video of the delivery
    - Sender and Receiver accounts for problem delivery
    - Non-anonymized drone data associated with those accounts
    - Pickup and delivery confirmation photos (if available)
    - Payment information
    - Other account information
- Business may continue as normal during this process

Communicate

- Public image assessment: Association with drug trafficking will tarnish Tinkerbell's image, but indiscriminate data disclosure will damage customer trust.
- Internal Communication: This does not need to be communicated to the staff outside of those directly involved with the investigation due to need-to-know
    - If successful incident resolution leads to successful prosecution, the incident could be placed in an internal newsletter with a "good corporate citizen" spin.
- External Communication: Assign a PR specialist to provide a single point of contact for all external communication on this incident
- Communicate with Sheriff:
    - Tinkerbell is regretfully unable to comply with the full request due to privacy and retention policies
    - Tinkerbell was able to retrieve video of the incident due to prompt notification

    - Tinkerbell has prevented other data on this delivery from autodeleting.
    - Tinkerbell will gladly share this information with the Sheriff
    - Tinkerbell is the foremost expert on its own data, so please let us know if more information needs to be extracted
- In case of media inquiries, the response will be that Tinkerbell does not comment on investigations, but is cooperating with law enforcement

Notification

- No notifications required or needed.

Follow-up

- Tinkerbell will monitor and track all confirmed instances of contraband delivery.
    - The analytics department will use this data to identify accounts that are being used to distribute illegal goods.
    - A team will be created to determine the best course of action for Tinkerbell when such accounts can be reliably identified.
- Tinkerbell will revisit its data retention policies with the goal of minimizing company risk.
- Standard procedures will be created to address future law enforcement requests

Review

- Not a common trend yet, but will probably become one.
- Reduce future incidents by creating the perception that using the Tinkerbell service for contraband is too risky.
- We have started the creation of an analytic process that should lead to earlier detection of triggering circumstances.
- This incident needs to be added to the Tinkerbell Risk Assessment program
- Evaluate the success of this response
    - Analyze Tinkerbell's actions and results using post-event considerations and the review checklist

Scenario 2

Assumption: CISO has already taken the compromised server offline and transactions are being processed by a clean backup image.
Assumption: tens of thousands of payment card records were exposed
Assumption: The server contained no European records due to border-crossing regulations
Assumption: The unusual server activity was caused by sophisticated spyware
Assumption: Spyware had root privileges on the infected host, but not on the network

Detect and Respond

- Open a new incident and log the initial details, formally starting the Incident Response process
- Working Hypothesis: A major privacy breach has likely occurred. Tinkerbell must determine the extent of the breach and work quickly to contain the damage
- Severity: S1 (Very High). An unknown amount of PII (Personally Identifying Information) and PCI (Processing Card Information) data has been exposed to a hostile actor.
- Activate Privacy IR Team: This breach will trigger legal, regulatory and social obligations that will have organization-wide impacts. The team will need to include representatives from Legal, PR, HR, Analytics, InfoSec, IT, Privacy and executive leadership.

Contain

- Communication from the compromised server was immediately disabled by the cybersecurity team
- The compromised server has been isolated for forensics by the cybersecurity team.
- Relevant data includes:
    - The list of transactions processed on the server
    - The data present in these transactions
    - Log files, especially those showing unusual activity
    - Details about the spyware present on the server
- Identify all assets present on the compromised server.
    - The initial assumption should be that all of them have been leaked.
    - Classify data by type (PII, PCI, etc)
- Determine the mechanism for compromise
    - Technical analysis of the spyware
    - Infection vector of the spyware
- Determine how long the server has been compromised
    - Determine if any information was exposed and then removed from the server during that time
- Determine the access level of the compromised system
    - Does this affect the list of exposed assets?
- Collect available information on SCAR54 to determine their usual techniques
    - Check the compromised server for additional SCAR54 malware
    - Check other systems for compromise, checking for known SCAR54 malware first

Communicate

- Public image assessment: This is a major breach that will make the news. Public perception will depend on Tinkerbell's handling of the incident. The public is largely aware that state-sponsored hackers are highly formidable, so Tinkerbell's image should be fine in the long term as long as it responds with integrity and accountability.
- Internal Communication: All employees of both Tinkerbell and Arachnid should be notified of this breach.
    - Administrators will be contacted first with instructions on how to notify the employees in their departments
    - Administrators will conduct staff meetings where they will stress the ongoing investigation and the company's commitment to doing the right thing
- External Communication: Assign a PR specialist to be our spokesperson for all external communication on this incident. The spokesperson will be provided with all necessary support and will be the single point of contact for all external entities.
- PR and Legal will collaborate on a press release.
    - The statement should be brief but transparent
    - The statement should include Tinkerbell's belief that it is the victim of state-sponsored cyber terrorism
    - The statement will commit to the prompt notification of all affected individuals by means of email
    - The same team will also compose a brief notification message to be displayed as a banner on the websites for Tinkerbell and Arachnid. The banner will include a link to the press release

Notify

- PR and Legal will collaborate on individual notifications
    - Use the same notification process for individuals in all jurisdictions
    - Legal will ensure that the notification content meets all standards
    - PR is responsible for tone and clarity
    - Notifications will be delivered by email
    - Legal will determine if any other delivery methods are required
- Legal determines what regulators and other entities must be notified
    - Attorneys General in all states
    - Regulatory agencies
    - Law enforcement
    - Media
- Legal and PR will determine the method of notification for all entities
    - Records will be kept of all notifications

Follow-Up

- Investigate
    - Perform forensic analysis on compromised server
        - What was the attack vector that led to the breach?
        - Did human action contribute?

        - When did this occur?
    - Besides leaking the transaction records, is there evidence of any other unusual activity?
    - Determine the extent of the breach as precisely as possible
        - Ensure that no other systems are affected
- Mitigation/Correction
    - Document the technical fixes for the vulnerability
    - If human negligence contributed to the breach, work with HR to determine if any disciplinary action is required
    - Policy Review
        - IT policies to improve patching consistency
        - IT policies to improve PCI DSS compliance
        - IT training policy
        - Information security policy
    - Document any decisions and changes about these policies
    - Intrusion detection and monitoring systems will be evaluated for effectiveness and upgraded if needed
    - Customer support
        - A year of credit report monitoring will be offered to affected customers
        - Edit the website notification banner to link to resources for affected customers

Review

- Not a trend. The goal of this review is to ensure that it doesn't become one.
- Advanced Persistent Threats cannot truly be countered, but effective security policy can both reduce our appeal and decrease the time until detection.
- Tinkerbell should partner with a security specialist such as Cheshire.
- This scenario was considered to be a high-impact threat by our risk assessment team
- Evaluate response success
    - Analyze our response using post-event considerations and the review checklist
    - Update Incident Response Plan as needed