SUBTERRANEAN HOMESICK BLUES…ADVICE AND INSIGHTS FROM BOB DYLAN

1. General Advice.
2. I'm on the pavement, thinking about the government
3. Lookin for a new Friend…
4. Stay away from those that carry around a fire hose…
5. Better jump down a manhole…
6. Light yourself a candle…
7. Questions or comments (no complaints)

BETTER JUMP DOWN A MANHOLE

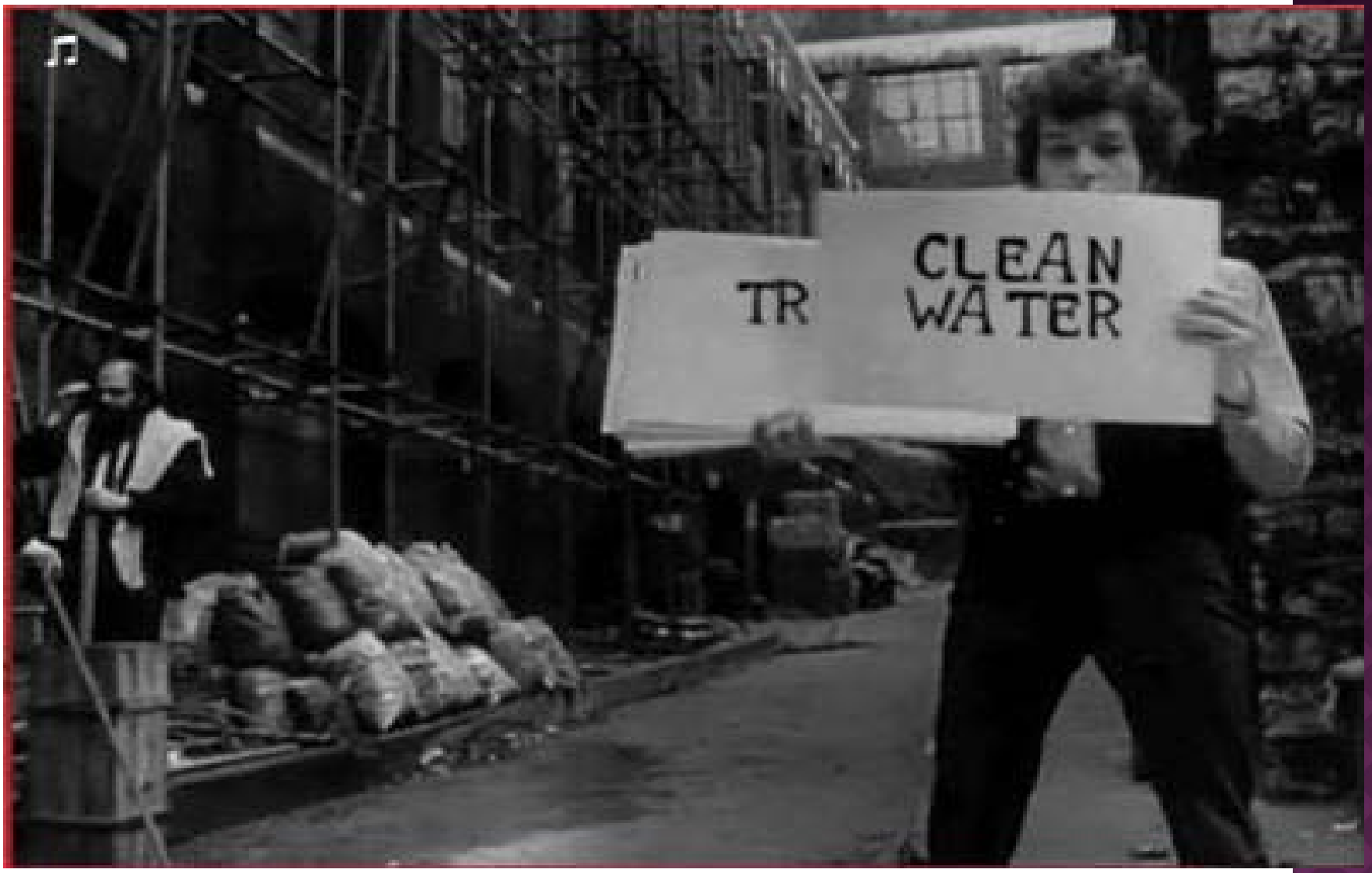
- Don’t wanna be a bum, better chew gum
- Don’t need a weatherman to know which way the wind blows.
- Don’t follow leaders, watch the parking meters
- Keep a clean nose, watch the plain clothes
- Stay away from those that carry around a fire house
- Walk on your tip toes
- Don't tie no bows

I'M ON THE PAVEMENT...THINKING BOUT THE GOVERNMENT

LOOKING FOR A NEW FRIEND

DON'T STEAL, DON'T LIFT….

BETTER JUMP DOWN A MANHOLE



LIGHT YOURSELF A CANDLE…

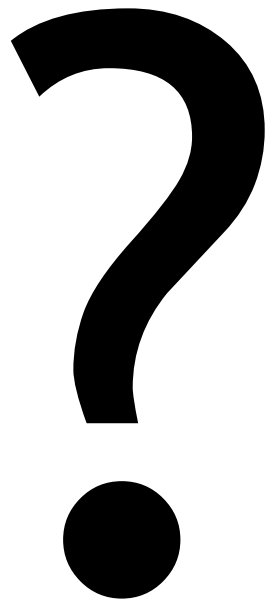
- Resilient cities have a pre and post-attack plan in place. Prior to a cyberattack, cities must set up a response policy that includes:
- Pre-established relationships with third party vendors.
- In-depth scenario planning that trains staff for responding to all types of cyber threats.
- Employee security awareness and education programming.
- Business continuity and process playbook which outlines how staff will continue performing job duties in case of attack
  - communicating with the staff through an alternative email exchange if the network email goes down

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

- Installing and maintaining a firewall configuration to protect cardholder data. The purpose of a firewall is to scan all network traffic, block untrusted networks from accessing the system.
- Changing vendor-supplied defaults for system passwords and other security parameters. These passwords are easily discovered through public information and can be used by malicious individuals to gain unauthorized access to systems.
- Protecting stored cardholder data. Encryption, hashing, masking and truncation are methods used to protect card holder data.
- Encrypting transmission of cardholder data over open, public networks. Strong encryption, including using only trusted keys and certifications reduces risk of being targeted by malicious individuals through hacking.
- Protecting all systems against malware and performing regular updates of anti-virus software. Malware can enter a network through numerous ways, including Internet use, employee email, mobile devices or storage devices. Up-to-date anti-virus software or supplemental anti-malware software will reduce the risk of exploitation via malware.
- Developing and maintaining secure systems and applications. Vulnerabilities in systems and applications allow unscrupulous individuals to gain privileged access. Security patches should be immediately installed to fix vulnerability and prevent exploitation and compromise of cardholder data.

PCI

- Restricting access to cardholder data to only authorized personnel. Systems and processes must be used to restrict access to cardholder data on a “need to know” basis.
- Identifying and authenticating access to system components. Each person with access to system components should be assigned a unique identification (ID) that allows accountability of access to critical data systems.
- Restricting physical access to cardholder data. Physical access to cardholder data or systems that hold this data must be secure to prevent the unauthorized access or removal of data.
- Tracking and monitoring all access to cardholder data and network resources. Logging mechanisms should be in place to track user activities that are critical to prevent, detect or minimize impact of data compromises.
- Testing security systems and processes regularly. New vulnerabilities are continuously discovered. Systems, processes and software needs to be test frequently to uncover vulnerabilities that could be used by malicious individuals.
- Maintaining an information security policy for all personnel. A strong security policy includes making personnel understand the sensitivity of data and their responsibility to protect it



Las Preguntas?
Wenti?
Les Questions?

GOODLAND Kansas Begins Here