Written Response Part

Q1

a) For security, traditional password is vulnerable. For example, attackers can use brute force method to find what the password is. Then, by knowing the password, attacker can get all parallel universe information of a person.
For usability, to make traditional password to be secure, user may set a password of complex combination of characters, which may also be difficult to remember the password, which means, there exists the possibility that user may forget the password they set. If user forget the password, then they may lose their parallel universe information and may not be able to do the verse jump.

b) Since password is something the user knows, we can add more authentication factors that can protect the information better.
One way of it is add something that user has. For example, add two-factor authentication. When attacker get the user' s password, then cannot get the information that is protected without 2FA. This reduces the risk of unauthorized accesses. But it is possible that user who own the information does not have the trusted device with them, or battery out.
Another way of it is add something that use is. For example, add biometrics. This make extremely difficult for attackers to access the protected information since fingerprint or iris are different for different people. This also reduces the risk of unauthorized accesses. But there may exists some concerns about the security and privacy of biological information.

Q2

- Prevent: Trying to avoid thieves entering the laundromat. For example, enhance the lock of doors and windows. This considered to be Prevent since this prevents the attack from origin.
- Deter: Add more locks for the customers' personal belongings. This considered to be Deter since it makes attack(steal) harder.
- Deflect: Avoid put something that seems valuable near windows and doors. So that thieves will pay less attention. This considered to be Deflect since this make laundromat less attractive to attacker(thieves)
- Detect: Install a alarm system that detects if someone try to open doors or windows in strange way. This considered to be Detect since this makes people notice that the attack(stealing) is occurring.
- Recover: Backup the item list of customers, after stealing happened, provide the information to police so that it helps recovery and compensation. This considered to be Recover since this mitigate the effects of the attack(stealing)

Q3

a) It is a phishing. In this situation, attackers mimic the way of cloud service provider to send an email that trick Jobu to change password (but in fact get his personal information and password without authorized). The confidentiality is compromised.
b) Server may receive an DoS attack, which means a lot of request is receive by it, and it is not powerful enough to process all the requests. The availability is compromised.
c) Data tampering attack. Since the user data are deliberately modified through unauthorized way. The integrity is compromised.

Q4

a) Stuxnet

   This is both worm. For air-gapped system, it spreads by installed manually (USB drive). It can also spread through network. It targeted Siemens SCADA systems installed on Windows. And used 4 different zero-day attacks to spread. It can destruct industrial control system and can be used for human-computer interaction and monitoring the important industries. It infected over 200,000 computers can caused 1,000 machines to physically degrade.

b) Sobig

   This is a worm and Trojan horse. It is spread through email as an email attachment. It infects a host computer by attachment, when this is started, they will replicate by using their own SMTP agent engine. E-mail addresses that will be targeted by virus are gathered from files on the host computer. (Wikipedia) It get email addresses form host computer and use them to spread further. It opens a backdoor on the infected computers so that attacker has the ability to do further malicious action.

c) CIH

   This is a Trojan horse. It spreads under the Portable Executable file format under the Windows 9x-based operating system, Windows 95, 98, and ME. It infects portable executable file by splitting the bulk of its code into small slivers inserted into the inter-section gaps commonly seen in PE files and writing a small re-assembly routine and table of its own code segments' location into unused space in the tail of the PE header. It is highly destructive to vulnerable systems, overwriting critical information on infected system drives and, in some cases, destroying the system BIOS. (Wikipedia)

d) BlackCat

   This is a Ransomware. It spreads relies on phished, brute-forced, and illicitly purchased credentials-typically for RDP connections and VPN services- as well as vulnerabilities published as CVEs. After infection, it can establish reverse SSH tunnels to BlackCat-controlled command-and-control infrastructure. Attacks are fully command-line driven, human-operated, and highly configurable. Attackers can attack active directory user and administrator accounts and the exfiltration and encryption of sensitive files, then making individual ransom demands for the decryption of infected files. (Blackberry).

Format String Vulnerability

Format String Vulnerability is in “fprintf(stderr, err_buf)” in line 95 of submit.c file. If the file located at src_name is read-only, then src_file will be the NULL pointer, and will enter the branch which contains line 95. At that line, string containing %n may be inserted by src_name (which contains some part that input from sploit program) can lead to overwrite the return address to access the shellcode.
This can be fixed by changing line 94 and 95 into
“fprintf(stderr, “Failed to open source file: %s\n”, src_name)” ;
so that formatting stuffs inside src_name will only be consider to be a single string.
Note that line 101 will never be reached since dst_file will never be NULL.