1. Wilderness Trailhead, Inc. (WTI) faces certain risks from its storage of customer credit card numbers on its database server. Cyber crackers and hackers may try to access the credit card data for intentions to commit theft through fraudulent purchases, resulting in potential damage to the victim’s credit and the monetary loss of the transactions, usually covered by the credit card companies. Such an event would also cause irreparable damage to the reputation of the company to WTI’s customers and partners. The database server’s security safeguards against unauthorized access to this data and can be affected by the following threats:

* The complexity of the database software can be directly related to the probability of any coding errors and security weaknesses, which can be exploited to gain authorized access.
* The server’s configuration can compromise secrecy by allowing ‘automatic directory listings’ that reveal the server’s hard-drive content to the potential criminal’s web browser. Critical files can be deleted, access rules changed, or the database file itself can be downloaded, and further exasperated if the database file was designed to store login data in unencrypted tables; allowing access to all the private, login and credit card data.
* A valid user’s login data (username/password pair) must be submitted over the Internet, via an encrypted transmission called a Secure HTTP (HTTPS) connection; otherwise the transmission can be intercepted and the secrecy of the data compromised.
* Cookies are normally stored on the user’s client computer hard-drive and can hold the user’s login data to afford the convenience of remembering the login by the operating system. But the data should be encrypted with a hash algorithm, so it is not human-readable, and should never be stored as plain text. And cookies should be configured to expire in a short span of time, to limit automatic access. These efforts are taken to thwart the loss or theft of a user’s notebook PC and the unauthorized access to private data.
* Passwords can be a threat if the user selects a weak password that can be guessed easily, such as a mother’s maiden name, a child’s name, telephone number, or birthdate. Dictionary attack programs can cycle through electronic dictionaries with repeated login attempts to gain unauthorized access.
* Valid user login data can be unscrupulously attained, by deceiving the person to give the information under false pretenses, called spoofing. It is essential to train employees about combating spoofing; especially, the employees that have administration permissions to the server’s database.
* The login data itself can potentially damage the database server, called SQL Injection. A criminal can submit login data that is designed to gain unauthorized access (authentication success is always true) or maliciously delete data (drop tables).

2. We will write a security policy for the operation of the WTI database server, which will address the threats listed in the previous exercise, above. This policy will define practices, procedures, and schedule to ensure the best configurations and operations to safeguard the database. The following “Computer Security Policy resources” will assist writing WTI’s policy:

* There are many online courses at the CERTS Organization[[1]](#footnote-1) and the SANS Institute[[2]](#footnote-2) to learn more about Information Security. There is much to consider when implementing a Security Policy so it may be worthwhile to pursue additional training for WTI personnel.
* [[3]](#footnote-3) The *SOS Information Security Policies* available [online](http://www.eon-commerce.com/rusecure/policies.asp?tracker=affilspsg), at a cost of $595, has policies covering topics.... securing hardware, peripherals; controlling access; information security of E-Commerce; commercial software; planning for business continuity.

3. WTI is considering moving its existing Web and database server computers to a colocation service provider (CSP) in a co-location arrangement. This is a good choice for a company of WTI’s medium size. [[4]](#footnote-4) The security features that WTI should ask a CSP to provide as part of this co-location service, include:

* A Colocation service should have a means of a continuous power source to keep the server computers running and thus, sustaining website operations. There must be a backup power source to ‘kick-in’ in case there is a power outage. Does the CSP have a backup power source such as a high-capacity battery-backup system? There also has to be line switches that disconnect the location’s bus circuit from the community grid, otherwise the battery backup power can electrocute an electric company linesman while working on the community power outage.
* Such a large infrastructure of computers, generate heat and the location must have a reliable air-conditioning cooling system throughout the building. Does the CSP has adequate equipment cooling capability?
* To quickly respond and recover from an electrical fire, the CSP needs to have an automatic fire-retardant delivery system that is safe for electrical fires, such as Halon, not water. And a warning system because Halon is not breathable very long.
* The CSP should have the information technology staff that is familiar with Web programming and scripting languages, e-commerce packages, and database management systems. This allows WTI to not need such expertise in-house, on their payroll. Does the CSP have experience and personnel with skills that meet the business needs of WTI?

1. CERTS Organization. <http://www.cert.org/training/>. [↑](#footnote-ref-1)
2. SANS Institute. Downloaded from <http://www.sans.org/courses/security>. [↑](#footnote-ref-2)
3. Information Security Policy World. Downloaded from <http://www.information-security-policies-and-standards.com/>. [↑](#footnote-ref-3)
4. Electronic Commerce, 11th Edition, Gary Schneider. Review of CSPs at <http://books.google.com/books?id=X4XAAgAAQBAJ&pg=PA2063&lpg=PA2063&dq=CSP+co-location+services&source=bl&ots=S8IfsoNz6z&sig=4z7eGC_ix3WcZqOpLhgbD-VqCwo&hl=en&sa=X&ei=Hf8lVKfLBYmkigKZ14C4Dg&ved=0CF4Q6AEwBA#v=onepage&q&f=false>. [↑](#footnote-ref-4)