Cybersecurity

Liberty Data Systems

What is cybersecurity and cyber risk?

Cybersecurity is the body of technologies, processes and practices designed to protect networks, operating systems, applications, databases and devices (collectively, IT systems) and information, including data, on them from compromise (i.e., loss of confidentiality, integrity or availability). Typically, these assets are compromised via the internet or other forms of connectivity. Cyber risk is the possibility that these technologies, processes and practices can be circumvented.

Cybersecurity events

Cybersecurity events can include, among other things, data breaches, email schemes, malware software and ransomware:

- Data breaches: In these events, an unauthorized user accesses a client's IT systems and copies sensitive information (e.g., personally identifiable information (PII), customer or vendor data, intellectual property)
- Email schemes: In these events, an unauthorized user gains access to an email account or uses a fake email address that looks authentic and sends an email that appears to be from a legitimate entity representative asking employees of the entity to disburse cash. In some schemes, an entity's vendor email system is breached, and unauthorized users send emails to the entity requesting changes in the bank account to which payments and sent. Valid payments may then be sent to an unauthorized account rather than the vendor's account.
- Malware software (malware) release: In these events, an unauthorized user gains access to an IT system and loads malware that may deny access to systems or data, may perform keystroke logging or perform other activities of which the user is unaware.
- Ransomware: is a type of malware that blocks access to an IT system until a sum of money (ransom) is paid. Ransomware usually denies access by encrypting programs or data with a key known only to the attacker who deployed the malware.

These events are facilitated by:

- Unauthorized software installation: Unauthorized software, such as keystroke logging software, can be loaded onto an entity's system when an employee clicks on an infected email. The unauthorized software collects the ID and password of that user and also loads credential harvesting software everywhere that user can access. Sufficient credentials are obtained by the unauthorized user to access sensitive information about the entity, its employees or its customers as described above.
- Social engineering: Attackers pose as entity representatives and ask users for their IDs and passwords so they can load software or disburse funds.

SCORE no. 14746-221US_3

Cyber threats are dynamic and ongoing. All connected organizations are subject to cyber risk. Cyber risks exist because of IT connected to the internet. As internet connectivity is so integral to business, cyber risks are enterprise-wide risks that can affect:

- The entity's reputation
- The security of protected or sensitive information (e.g., intellectual property, credit card information, personally identifiable information [PII])
- Computer-controlled operations or online systems
- Costs to remediate breaches or modify weak computer security environments
- Fines and penalties issued by various jurisdictions and government agencies

Cybersecurity controls

Controls to mitigate against cybersecurity attacks are an important component of an entity's overall IT control environment and are especially important in protecting intellectual and physical assets. As such, it is increasingly important for external auditors to be aware of the risks that clients face because of poor or inadequate cybersecurity processes and controls. For this case, consider yourself an external auditor performing the audit for the public company Liberty Data Systems (Liberty).

You are tasked with evaluating and testing internal controls, more specifically, you will evaluate and test one aspect of the access controls component of information technology general controls (ITGCs) — passwords. ITGCs are controls that protect an entity's data and IT systems (all data and software, IT operations and physical hardware). ITGCs exist to make sure that the IT environment functions as intended and is protected from unauthorized access or manipulation due to error or fraud.

Note: If you would like a better understanding or review of ITGCs, please consider utilizing the EYARC internal controls ITGC curriculum materials.

Password management is one important part of strong ITGCs. Passwords are one of the primary defenses that mitigates against unauthorized access to IT systems. As such, it is important for the auditor to perform tests around password management. As part of the audit, your team members have already performed the following tests and found the following:

- Inquiry. The auditors inquired of Liberty's management team about the design and use of passwords at Liberty. Management relies heavily on the recommendations from the Center for Internet Security (CIS) Controls Version 8 guidelines (available for download at https://learn.cisecurity.org/cis-controls-download). "The CIS Controls reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals), with every role (threat responders and analysts, technologists, information technology (IT) operators and defenders, vulnerability-finders, tool makers, solution providers, users, policy-makers, auditors, etc.), and across many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT, etc.), who have banded together to create, adopt, and support the CIS Controls." Especially relevant to the task at hand is that management tries to follow the guidelines for user passwords in the CIS Password Policy Guide (available for download at https://www.cisecurity.org/white-papers/cis-password-policy-guide/), although management indicates they have not implemented everything in this guide.
- Observation. The auditors have observed that access to any of Liberty's systems requires users to enter a password. The auditors have not examined whether Liberty is following password best practices, but they have confirmed that you cannot enter the system without entering a password. They also have confirmed that multi-factor identification is used and it works successfully.

SCORE no. 14746-221US_3

Required

Your task is to perform each of the following steps as part of reviewing password management as a key ITGC for the Liberty audit. For the purposes of this case, assume that the date is May 4, 2022.

1. Identify two financial statement risks that could occur because of failures in password policies. Describe each risk and the effect it could have on the financial statements. Additionally, describe a test you could perform to evaluate Liberty's potential exposure to the risk. Use the following table, with one response already provided as an example, as a guide for preparing your answer.

Description of the risk	How the risk may influence the financial statements	Possible test to perform to evaluate exposure to the risk
Fake transactions are being entered.	Financial statements could be misstated because of falsified transactions.	Review journal entries by username to look for unusual patterns (such as time of day, unusual volume, entries in unusual journals or ledgers, unusual descriptors, etc.).

2. Search the guidance from https://www.cisecurity.org/white-papers/cis-password-policy-guide/ for recommendations about each of the following topics. Record what is recommended and why it is recommended.
   a. Length of passwords
   b. Special character requirements in passwords
   c. Capitalization requirements in passwords
   d. Passwords on Deny Lists
   e. Dictionary words vs. passphrases
   f. Multi-factor authentication

3. A member of your audit team pulled a sample of 30 users and their passwords from the system. The full data pull is presented in the appendix. A subset of just the username and password for the 30 users is listed below. Based on your answers listed to question 2. and review of the information in the appendix, what concerns do you have about each of these passwords? Complete the table below. If you have no concerns about the password, list No concerns.

No.	Username	Password	Concerns
1	BowenM655	xLY]d_!gzp	
2	EPage919	Tom_Ere_2k9	
3	ChappellA672	password123	
4	WalkerA614	LisaMaria-9412	
5	RamirezC557	Password1!	
6	BarclayH562	&K{EN^M5nVde7	
7	MccullloughL594	Champions=1995	
8	LugoK615	8$}y-kDnKx)3	
9	VassC676	SuzieAndRocco	
10	WalkerS706	L@n3y!	
11	VinceJ198	Marines#1	
12	KnightA631	daisy	
13	NortonA410	ilovecandy	
14	SwanH279	Maja&Hayden4ever!	
15	JanssenS126	E=mc2	
16	SwanH279	Jennifer1!	
17	JenkinsR89	xLY]d_!gzp	
18	HallidayM689	Maja&Hayden4ever!	
19	DonnellyB513	S@tbfflad1	
20	NorrisM666	teddybears	
21	ReddenZ703	yC4}FvJ=qb>NS	
22	ReidK706	C@veGirl93	
23	LiL867	PA$$word11	
24	EllisM154	}/*!GAxT	
25	BakerD760	babycakes	
26	BillingsN726	>/CRe6}Uxn%EA	
27	LambertM256	H@mish300595	
28	ShafferN129	{&TgVj3*dbZUrWPf?	
29	BakerB512	BHU*8uhb	
30	WheelerW440	xLY]d_!gzp	

For problems 4., 5. and 6., complete the requirements using Alteryx or Python as directed by your instructor:

Alteryx: submit your completed workflows in a packaged Alteryx workbook (.yxzp file type [Options > Export Workflow >]) saved with a naming convention to include your full name, e.g., Cybersecurity_case_studies_LibertyDataSystems_FirstName_LastName.yxzp. In addition, annotate each step in your workflow to indicate the purpose of that step. Also use comments to indicate the part of the workflow that answers each question posed.

Python: submit your completed code in a .py or .ipynb file (as directed by your instructor) saved with a naming convention to include your full name, e.g., Cybersecurity_case_studies_LibertyDataSystems_FirstName_LastName.

4. While you performed your initial review of the risks regarding the passwords manually, it is now time to automate these procedures using Alteryx. The sample of 30 users and passwords from the appendix is contained in the file labeled, **Cybersecurity_case_studies_LibertyDataSystems_ Sample.xlsx** (SampleData tab). Using Alteryx, perform the following tests by creating a workflow and providing a list of the results using a Browse Activity, as specified. Sort each answer by UserName in ascending order.

    a. How many passwords are less than eight characters in length? Using a Browse Activity, list the username, password and computed password length for each employee who matches the criteria. The header for your results should look like this:

    b. How many passwords only contain letters, regardless of whether the letters are uppercase or lowercase (i.e., they do not contain numbers or symbols)? Using a Browse Activity, list the username and password for each employee who matches the criteria. The header for your results should look like this:

    c. How many passwords do not contain both capital and lowercase letters (i.e., they do not have mixed capitalization for the letters)? For this question, the passwords may or may not contain other numbers or characters. Using a Browse Activity, list the username and password for each employee who matches the criteria. The header for your results should look like this:

    d. How many users have repeated passwords in the file? Using a Browse Activity, list the username and password for each employee who matches the criteria. For this problem only, sort the data first by password (ascending) and then by username (ascending) so it groups users with the same password next to each other. The header for your results should look like this:

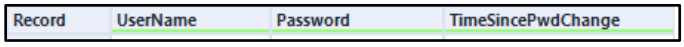
    

    e. How many users have never changed their password? Using a Browse Activity, list the username and password that matches the criteria. The header for your results should look like this:

    f. How many users have not changed their password in the last 90 days? Using a Browse Activity, list the username, password and the number of days since the last password change for each

employee who last changed their password more than 90 days ago (remember to use the May 4, 2022, date as the current date). The header for your results should look like this:



5. The file **Cybersecurity_case_studies_LibertyDataSystems_PasswordDictionary.csv** contains a curated list of about 2 million passwords that were previously discovered from data breaches of various organizations. Compare the sample of passwords with this list. How many passwords are already contained on this list? Using a Browse Activity, list the username and password for each employee who matches the criteria. The header for your results should look like this:

6. Prepare a final output of all usernames and passwords that are *not* problematic. That is, use a Browse Activity to show the username and password for each employee who has a password that is not less than eight characters, contains a number or symbol, contains both uppercase and lowercase letters, is not repeated with another user, has been changed and the change was within the last 90 days, and is not on the curated list of discovered passwords. The header for your results should look like this:

7. Based on your analysis, what do you believe should be the next steps for the external audit?
8. What other concerns do you have from reviewing the data? List at least three concerns you have and explain why you are concerned.

Appendix – Sample of 30 users and passwords

UserName	FirstName	LastName	JobDepartment	Password	PwdChangeDate	PwdInitial
BowenM655	Maribel	Bowen	IT Department	xLY]d_!gzp		1
EPage919	Emily-Renee	Page	CEO	Tom_Ere_2k9	2/8/2022	0
ChappellA672	Agnes	Chappell	Accounting and Finance	password123	4/7/2022	0
WalkerA614	Audrey	Walker	Accounting and Finance	LisaMaria-9412	4/11/2022	0
RamirezC557	Carlos	Ramirez	CFO	Password1!	4/25/2022	0
BarclayH562	Hannah	Barclay	Accounting and Finance	&K{EN^M5nVde7	3/29/2022	0
MccullоughL594	Leslie	Mccullough	Accounting and Finance	Champions=1995	4/21/2022	0
LugoK615	Kendal	Lugo	Accounting and Finance	8$}y-kDnKx)3	3/6/2022	0
VassC676	Chad	Vass	Accounting and Finance	SuzieAndRocco	4/11/2022	0
WalkerS706	Sienna	Walker	Accounting and Finance	L@n3y!	2/16/2022	0
VinceJ198	Julius	Vince	IT Department	Marines#1	4/26/2022	0
KnightA631	Aleksandra	Knight	Accounting and Finance	daisy	4/7/2022	0
NortonA410	Adina	Norton	Accounting and Finance	ilovecandy	2/14/2022	0
SwanH279	Hayden	Swan	IT Department	Maja&Hayden4ever!	4/21/2022	0
JanssenS126	Sharolyn	Janssen	Accounting and Finance	E=mc2	2/7/2022	0
SwanH279	Hayden	Swan	IT Department	Jennifer1!	4/7/2022	0
JenkinsR89	Rita	Jenkins	Accounting and Finance	xLY]d_!gzp		1
HallidayM689	Maja	Swan	Accounting and Finance	Maja&Hayden4ever!	4/21/2022	0
DonnellyB513	Bianka	Donnelly	Purchasing	S@tbfflad1	2/17/2022	0
NorrisM666	Mark	Norris	Accounting and Finance	teddybears	2/10/2022	0
ReddenZ703	Zoe	Redden	Accounting and Finance	yC4}FvJ=qb>NS	3/8/2022	0
ReidK706	Kurt	Reid	Research and Development	C@veGirl93	3/5/2022	0
LiL867	Lucas	Li	Research and Development	PA$$word11	4/3/2022	0
EllisM154	Moesha	Ellis	Accounting and Finance	}/*!GAxT	3/6/2022	0
BakerD760	Daniel	Baker	Accounting and Finance	babycakes	4/3/2022	0
BillingsN726	Naida	Billings	Accounting and Finance	>/CRe6}Uxn%EA	3/6/2022	0
LambertM256	Marjorie	Lambert	Accounting and Finance	H@mish300595	11/11/2021	0
ShafferN129	Nicky	Shaffer	Accounting and Finance	{&TgVj3*dbZUrWPf?	3/15/2022	0
BakerB512	Bob	Baker	Purchasing	BHU*8uhb	3/19/2022	0
WheelerW440	Wayne	Wheeler	Accounting and Finance	xLY]d_!gzp		1

The columns are defined as follows:

UserName: A unique username assigned to each employee used to access the system.

FirstName: The employee's first name.

LastName: The employee's last name.

JobDepartment: The employee's currently assigned job department.

Password: The plain text password for each employee.

PwdChangeDate: The date the employee most recently changed their password. If null, then the employee has not reset their password.

PwdInitial: An indicator variable = 1 if the employee has not changed the initial password assigned by the IT Department when the employee's account was started and = 0 if the employee has changed their initial password.