一、試分析中信銀在此次事件中，犯了哪些錯誤?你覺得個資外洩的問題，誰該負責?

Ans:

1.1

1.內部程式設計有問題:資料庫程式設計的問題(Injection)，導致查詢資料條件過於寬鬆，使用者能查詢到的資料遠多於其權限所賦予的。

2.系統上線前的測試環節不夠嚴謹:測試的案例不夠完備，導致連最容易發生的狀況都沒有檢查到。

1.2

程式設計人員和系統測試人員都該負責，但我覺得系統測試人員該負較大的責任，因為這個錯誤相當明顯，所以在測試時應該不難發現這個問題。

二、如果你是中信銀資訊部門的最高主管，對於個資保護的資訊安全做到的程度，在成本、安全控制、及使用者便利性三者中，你會如何權衡取捨呢?

Ans:

天下沒有絕對完美的防禦，因此資訊安全是一種取捨(tradeoff)。應在有限的條件下，將資源投資在最容易受到攻擊或是對組織衝擊最大的安全弱點上。例如:一家五位員工的小企業可能最該做的是為每台電腦安裝防毒軟體，而不是花幾千萬元建立一個安全營運中心(Security Operation Center, SOC)。

另外，防禦措施需要在安全與便利之間做合理的取捨。過度防禦會造成使用者的不便，反而違背資訊科技帶給人便利的初衷。例如:有一家企業安裝了安全性極高的門禁管制系統，員工進出任何門都需要刷卡並輸入 PIN 碼。公司追求高安全性的立意極佳，但由於操作不方便，員工乾脆不關門，反而形成始料未及的安全漏洞。

因此在成本、安全控制、使用者便利性三者的取捨中，我認為要看要保護的機密資料機密性而定。若是相當重要的資料，就該盡可能地關注在安全控制上；若是資料並沒有那麼重要，那麼我覺得可以捨棄一些安全控制來換取更低的成本及更好的使用者便利性。

三、你若是中信銀資訊部門最高主管，針對此次個資外洩事件，你覺得公司內部資訊安全管理制度如何能夠改善呢?是否需增加人手進行分工呢?

Ans:

3.1

雖然這次可能只是一些簡單的資料庫程式碼問題，但我覺得為了以防萬一以後可以請一些外面的廠商來做一些滲透測試(Penetration test, PT)，讓公司了解自身的安全漏洞，並演練招到入侵後之標準作業流程。

3.2

我認為要增加人手進行監督的動作，因為會發生問題，就代表一定是有哪些方面出了問題，所以一定要多加派人手進行監督的動作，或是乾脆直接成立一個部門來負責這方面的問題。

四、發生個資外洩事件這類事件，「成本」與「商譽」何者較為重要?

Ans:

我個人認為商譽一定比較重要，因為在台灣銀行或金控實在是太多了，所以代表著客戶擁有著很多的替代方案，那麼如果企業無法證明把個資或錢存放在你這裡是安全的話，那麼就很難吸引客戶來你這裡辦業務。

五、根據本個案提供的資料，你認為中信銀高層對於資訊管理部門的定位是什麼呢?如果你是中信銀資訊部門最高主管，你會如何因應呢?

Ans:

5.1

根據文中「中信銀之 e 化及資訊安全管理」的第二段敘述提到，中信銀的 IT 部門，成立之初就被要求要支援業務，4、5 年前更被要求要實現業務的發展，至今變成只要與業務有關的應用，IT 的老闆就是各事業單位的主管。因此我認為資訊管理部門的定位，就是全力協助業務部門，讓各項業務不僅要衝第一家，也要衝最快。而對 IT 來說，就是要資訊系統要能跟得上。

5.2

我會將工程師依小組分別對接到各事業單位中，去熟悉或詢問到各部門對資訊系統的需求，然後盡可能讓工程師了解各部門是如何運作的，這樣就不會造成工程師開發出來的資訊系統讓各部門使用不便的情形發生。