《資訊管理與資通安全》

一、請回答以下關於資訊安全的問題：

(一)在瀏覽器進行瀏覽時，常可見到「網站的安全性憑證不可靠」的訊息，請說明跳出這訊息的可能原因與可能發生的風險。（5分）

(二)某政府機構遭到駭客偵測出網路管理員的機構信箱master@abc.gov.tw，之後駭客製作零時差漏洞打造的遠端存取工具寄送至該信箱，致使該電腦遭感染後，持續遭到駭客控制與進行橫向擴散，並導致重要機密文件外流。請進行上述事件分析，並請提出可能的改善措施。（20分）

試題評析	第一題為基本的時事題，同學只要對於SSL與傳輸協定有基本認知即可。 第二題較為活潑，除了要對零時差攻擊的防治有認知外，也要知道針對特定情況的處理方式，答題上一樣圍繞在基本防治方法，只是舉例時要切合題目即可。
考點命中	《高點・高上資訊管理與資通安全講義》第二回，蕭老師編撰，頁36-37

答：

(一)SSL（Secure Sockets Layer）是網頁伺服器與瀏覽器加密連線的通訊標準，終端使用者存取網頁時以https加密傳輸通道來傳送資料，便是運用了SSL加密技術。網路認證發放機構在確認申請的網頁伺服器的身份與資訊正確之後，會發放SSL憑證，此時網頁伺服器的SSL即可通過瀏覽器檢查認可為「正牌」網站並建立SSL加密連線。

(二)若瀏覽器發現發放的SSL憑證不是從合法的組織所釋出，則會跳出該錯誤訊息。依照以上論述其所產生的風險則是在傳輸時若是用到假的憑證，則資料加密回無效，其中傳遞的資料也會被竊取。

(三)預防與改善零時差攻擊的方式可以分為四個階段

1.快速阻擋階段

針對進來的連線作惡意程式庫的比對，當發現符合的連線時，及時阻擋這些惡意連線。故系統平時要維護惡意連線資料庫，透過快速且較為全面的比對方式，能夠在不消耗過多運算資源下達到初步的阻擋，且惡意程式庫都是可以被更新的，因此雖然系統或軟體供應商無法及時提供更新檔，但是防禦設備的廠商如果可以針對這些攻擊撰寫偵測攻擊的特徵碼，就可以讓防禦設備阻擋該攻擊。

2.靜態分析階段

當第一階段沒有偵測到惡意攻擊時，就應該要開始做一些靜態的分析，這一階段主要是要透過一些分析機制(例如協議分析)，將確認是正常的連線直接放行；並且將懷疑是惡意攻擊的連線送到下一階段做進一步的分析。

3.動態分析階段

主要是利用沙盒(Sandbox)或虛擬主機(Virtual Machine)，對懷疑是惡意攻擊的連線作分析，分析方法是讓這些連線在裡面執行，然後分析它是否會感染其他的程式或系統檔案，也會分析這些連線是否會背後偷偷地連到外面的主機，透過這樣的一個機制我們就可以很清楚的知道這些惡意連線的行為。

4.阻擋規則的產生

一個好的防禦設備是要能夠將第三階段分析的資料拿來自動產生阻擋規則，然後自動地把這規則更新到惡意程式庫裡，這樣的防禦設備才能發揮最好的效能。

二、許多資訊安全事件的資料外洩都是因軟體開發不安全所引起，如何撰寫安全的軟體資訊系統已成當務之急，請論述至少三個面向以說明如何撰寫一較具安全的軟體資訊系統。（25分）

試題評析	此題看似中規中矩，但是將軟體開發與資訊安全結合，考驗同學融會貫通的能力，答題上要圍繞在資訊安全上，並且在開發流程中實際呈現與掌握資安原則才是此題的回答心法。

答：

需要先將資訊安全的三大面向，分別為「私密性」、「資料完整性」以及「可用性」來分析所要開發的資訊系

統，以決定需要投入多少的工夫與成本來滿足安全性的需求。
實際開發上可以利用以下幾點來達到以上三面向：
1.不要信任來自系統外部的輸入資料
在程式中要針對「使用者手動輸入的資訊」與「程式模組間傳遞的參數」做內容合法性與正確性的檢查，在實際上可以針對以下幾點：
(1)避免SQL Injection
程式中如果有需要對資料庫做新增、刪除、修改和查詢等動作，針對使用者自行輸入的部分務必要做內容格式與字串長度的檢查，如此將可避免產生出的SQL 查詢指令內包含了預期以外的SQL指令，而達到攻擊的目的。
(2)避免Buffer Overflow
由於語言的特性，針對外來提供的資料需要考慮其大小會不會大於內部所指定的緩衝區，當開發人員並未預先考慮此情況時，溢位會導致記憶體中的資料結構破壞，而這種問題經常會導致攻擊者得以執行惡意程式碼。
(3)避免Cross-Site Script
通常是撰寫Web-based程式時會遇到的狀況。如果在輸出HTML資訊到使用者的瀏覽器的過程中，用到了使用者所輸入的資訊，或者利用其他模組所得到的結果字串來組合字串時，就特別需要執行特殊的內容檢驗程序，以避免輸入內容夾帶惡意的JavaScript，輕者破壞頁面排版，嚴重造成使用者的私密資訊被POST到其他網站中。
2.最低權限原則
(1)針對每一種使用者需要事先規劃好其使用的場景，並給予最低的使用者權限即可。若應用系統對資料庫只需查詢資料時，就不需要搭配具有寫入資料權限的帳號。
(2)注意程式的錯誤處理
開發者一定要花足夠的時間重新檢查錯誤、另外偵測、攔截與處理的相關程式中，並且確認所模擬的任何錯誤情境，都會正確地走到你預先埋好的錯誤處理函式中。

三、因應快速發展及市占率日高的行動商務及新零售市場，如何完整規劃行動支付開發專案，是每位資訊系統規劃人員所需要面對的立即挑戰。某企業欲規劃開發行動支付系統專案，請申論說明企業可進行什麼樣的改變及可提出那些創新服務的營運模式。（25分）

試題評析	行動支付是現在的趨勢，許多企業都想要採用，但是其中一個問題是系統方向的資訊流向有可能會與現有的系統不一致，資訊人員在規劃的時候需要考量到其營運的實際狀況，並且在不影響既有業務下，發展適合企業與組織的行動支付方案。 答題上要先針對行動支付簡單的論述與說明，再針對可行的方案作論述，並要以不影響既有業務的情況下來闡述即可。
考點命中	1. 《高點・高上107地特題神》資訊管理與資通安全，蕭老師編撰，頁2-10。 2. 《高點・高上資訊管理與資通安全講義》第二回，蕭老師編撰，頁67-68

答：
根據 2012 年國際清算銀行(Bank for International Settlements)所發表的零售支付工具創新報告中，對於行動支付的定義為：「舉凡以行動存取設備(如手機及平板電腦等)透過無線網路，採用語音、簡訊或近場無線通訊(NFC)等方式所啟動的支付行為均屬之」。
故企業可以針對以下幾點來提升企業的行動支付融合性與開發新穎的服務模式：
1.流程串接需要增加彈性
相較於傳統的現金流，企業或組織需要針對不同的金流有更廣泛的接受程度。目前提供行動支付的業者非常多，導致串接的API與對口也相對多元，企業在與其他組織串接時要隨時保有彈性，才可以因應不同的行動支付行為。
2.企業需要全盤的調整零售方式來接受多元的付款流程
行動支付的影響並不僅止於改變了付款型態和流程。相對於現金或實體卡片，行動裝置本身是一個資訊化的載具，能結合電腦視覺、深度學習、感測器等先進技術提供服務業更多的可能性。例如，當顧客進入商店使

用行動支付（如手機QR Code、NFC、密碼、指紋、虹膜、人臉輪廓）驗證身分與付款帳戶時，就能開始偵測並捕捉顧客在店裡的移動軌跡以及所挑選的商品種類和數量，並實現顧客所謂「拿了就走」的無人商店模式。這種「新零售」模式顛覆了顧客入店、店內選購、離店結帳的全部消費流程，這也表示需要重新全盤思考零售店的營運方式。

3.結合數據，提升資料的價值

服務業可以結合物聯網及人工智慧等先進技術，衍生出多元的新型商業模式，且可更進一步透過分析所收集的大數據資料，發掘市場潛藏的各類商機；亦即行動支付不只驅動了新零售的轉型，舉凡服務相關行業，在顧客管理、交易結帳、營運流程乃至於商業模式，都會受到影響。

四、企業資源規劃（Enterprise Resource Planning，ERP）系統是國內眾多公民營企業均導入的資訊系統，請回答下列問題：

（一）企業資源規劃系統導入勢必牽涉到企業流程再造，請問企業流程再造包含那四個要素？（12分）

（二）請申論說明為何ERP系統導入失敗的案例不少。（8分）

（三）請申論說明為何導入過程，常需要專業的ERP顧問協助？（5分）

試題評析	ERP系統一直是國家考試中常出現的題型，同學除了對於基本觀念要掌握外，也要理解其在企業應用的實際範例，提升答題的準確度與價值。 此題為活潑的題目，從基本概念一直到實例應用都包含，針對二三題答題的心法為掌握ERP導入的關鍵成功因素即可。
考點命中	1.《高點・高上107地特題神》資訊管理與資通安全，蕭老師編撰，頁2-10。 2.《高點・高上資訊管理與資通安全講義》第一回，蕭老師編撰，頁50-56

答：

(一) 企業流程再造具有「流程化」、「根本」、「徹底」及「顯著」之四要素：

1.流程化（Process）：指一連串為達到特定目的或產出且具相關邏輯性作業的程序，是改造的核心，透過相關部門流程之合作與協調，發揮企業最大之效益。

2.根本（Fundamental）：藉由詢問一些基本的問題，強迫人們思考他們工作時所使用的既有規則，是否適當與正確，進行企業流程再造的同時不可受限於現況，應檢討企業根本之問題，透過檢討與反省，提出因應之策略與方針。

3.徹底（Radical）：企業應徹底革新現有不合理之組織及流程，重新規劃新的運作流程，使企業能進行革命性再造。

4.顯著（Dramatic）：改造所尋求的是組織績效顯著、跳躍式的改變，而非邊際性的、漸進式的改變。

(二) ERP系統的導入是全面性的，若企業在導入時遇到以下幾點，都可能造成導入失敗

1.未選擇適當的ERP系統

企業並沒有充分瞭解自己的需求，產業的特性，經營管理的方式（如依計劃生產、訂單生產或訂單裝配），以致於上線後發現系統無法套用到實際的作業上，最後迫使企業「削足適履」，再搭配人工作業方式勉強使用，或者再花一大筆錢作客製程式修改

2.企業願景規劃不完整

企業在建置 ERP前，必須與全體員工共同描繪出企業的未來願景，引導企業資源投入的方向，如此才不會因為侷限於目前的企業規模或業務形態，而選擇一套不適用的 ERP 系統。

3.輔導與訓練成效不彰

若企業員工沒有接受充分的 ERP 教育訓練，或顧問師的輔導能力不足，結果當然是瞎子摸象般難以一窺全貌，只知其然而不知其所以然，只瞭解局部的模組功能，而缺乏對整合系統的完整認識。

4.使用者抗拒

舊的系統行之有年已經非常熟練，如資料欄位，報表格式都很清楚，一旦啟用新的 ERP 系統又要重新摸索學習，主觀上先認定新系統沒有舊的好，心態上難免有所抗拒。

5.高階主管不支持

在導入 ERP 系統時，有許多公司的作業流程也許要改變，部門組織的權責也許要重新定義，這些都需要高階主管的親身參與，若無法得到支持，則導入很容易胎死腹中或失敗。

6.公司策略與流程不變

許多公司使用新的 ERP 系統，但仍沿用過去的策略和作業流程來管理，就像新瓶裝舊酒般，無法真正發揮企業資源的重新規劃和運用。

7.缺乏定期的績效評估

導入 ERP 系統之後，對於企業的營運是否產生正面的效益，應該經常加以評估，例如成本結算時間是否縮短？存貨是否下降？準時交貨率是否提高？生產排程的達成率是否提高…。只有透過定期如每月的績效評估，才能適時改善。

(三)大部分企業在導入ERP系統時通常都沒有前例可循，也因為沒有歷史經驗可供比對、參照來建立符合公司需求的評估基準，評估ERP系統就比較需要顧問的協助，或是尋求同業導入ERP系統的經驗，以其經驗來建立自己的評估基準。

一般而言，顧問必須對於特定產業的企業營運模式及資訊科技、系統方面有相當程度的認知、了解，才能協助企業在導入ERP時尋求最適合企業運作的系統流程。