網站個資防護建議

2021/10/6

國立成功大學
資安弱點掃描團隊

Content

1.

個資洩漏事件

1.1 個資洩漏事件

全國24萬餘名公務人員個人資料遭到洩漏，銓敘部責無旁貸，監察院仉桂美委員、劉德勳委員、包宗和委員促請該部就其資通安全管理制度檢討改善

- 日期：109-02-21
- 資料來源：公關科

去（108）年6月發生含國安局等機敏機關在內之58萬餘筆公務人員個資遭人置於國外論壇販賣乙案，有威脅國家安全之虞，引起監察院仉桂美委員、劉德勳委員、包宗和委員重視並立案調查，監院也於109年1月16日教育及文化委員會通過調查報告，促請銓敘部其資通安全管理制度（Information Security Management System，下稱ISMS）加以檢討改善。

三位委員首先指出，根據相關資料研判，本案為101年6月時外洩，但迄至108年6月22日始被發覺，而外洩內容為該部94年1月1日至101年6月30日間中央及地方機關公務人員送審人員歷史資料，經比對後實際影響人數為24萬餘人，含行政機關、公營事業、衛生醫療機構及公立學校職員等，依據銓敘統計年報，101年底全國公務人員(註)共計34萬3,861人，換言之，本次計有全國70.77%之公務人員個資遭到外洩，等於每3人中至少有2人資料遭到

（監察院，https://pse.is/3jh6es，檢索日期：2021/06/08）

1.1 個資洩漏事件

大考中心遭駭 2千考生個資外洩

2021-06-02 00:20 聯合報 / 記者潘乃欣／台北報導

+ 教育部

讚 24 分享 分享

為讓考生適應一一一學年新型學測試題，大考中心將於今年七月廿八到卅日舉辦試辦考試，開放高二生報名參加。未料昨傳出有兩千名考生報名資料遭駭，教育部證實此事，並說已送司法調查，也將請大考中心檢討並追究相關人員責任，同時強化資通安全防護，避免類此事件再次發生。

大考中心表示，大考中心因應試辦考試設立報名系統，今年四月一日上線，四月十二日開始報名，四月十五日就發現有不明人士透過不當手段，進入試辦考試觸及考生報名資料，約二千筆。

教育部表示，該系統發生少部分學生報名資料遭不明人士瀏覽，大考中心向教育部通報當下，教育部即依資通安全事件通報及應變辦法，要求大考中心緊急應變與損害復原，將損害降到最低。

（聯合新聞網，https://udn.com/news/story/6925/5501972，檢索日期：2021/06/08）

1.1 個資洩漏事件

駭客入侵 新北運動中心個資外洩

04:10 2020/05/14 | 中國時報 | 許哲瑗 、新北

新北市運動中心與學校媒合時間場地一覽表

檔案 編輯 查看 插入 格式 資料 工具 表單 外掛程式 說明

	A	B	C	D	E
1	0	姓名	連絡電話	是否於14天內有出國紀錄	欲使用場地
2	2020/4/28 下午 12:14:24	[redacted]	[redacted]	否	辦公室
3	2020/5/7 上午 10:24:59	[redacted]	[redacted]	否→歡迎來館使用。	籃球場
4	2020/5/7 上午 10:22:41	[redacted]	[redacted]	否→歡迎來館使用。	籃球場
5	2020/5/7 上午 9:14:41	[redacted]	[redacted]	否→歡迎來館使用。	羽毛球場
6	2020/5/7 上午 10:47:47	[redacted]	[redacted]	否→歡迎來館使用。	健身房
7	2020/5/7 上午 8:23:33	[redacted]	[redacted]	否→歡迎來館使用。	一樓社區教室（AOA）
8	2020/5/7 上午 10:25:25	[redacted]	[redacted]	否→歡迎來館使用。	兒童遊戲區
9	2020/5/7 上午 4:47:28	[redacted]	[redacted]	否→歡迎來館使用。	游泳池
10	2020/5/7 上午 8:15:13	[redacted]	[redacted]	否→歡迎來館使用。	3F韻律教室
11	2020/5/7 上午 9:51:09	[redacted]	[redacted]	否→歡迎來館使用。	3F韻律教室
12	2020/5/7 上午 8:28:14	[redacted]	[redacted]	否→歡迎來館使用。	健身房, 3F韻律教室
13	2020/5/7 上午 6:52:12	[redacted]	[redacted]	否→歡迎來館使用。	健身房
14	2020/5/7 上午 9:08:59	[redacted]	[redacted]	否→歡迎來館使用。	3F韻律教室
15	2020/5/7 上午 11:44:52	[redacted]	[redacted]	否→歡迎來館使用。	健身房

（中時新聞網，https://pse.is/3j7u9f，檢索日期：2021/06/08）

1.1 個資洩漏事件

學生個資外洩 校方如何處理?

中正E報 Follow
Nov 6, 2020 · 3 min read

【記者 張雅涵、劉子君 / 中正大學報導】

一封電子郵件 學生個資全洩漏

國立中正大學通識中心在10月12號上午，誤將一份含有大量學生資料的檔案寄給報名講座的學生，其中包含104至108學年度，總共8495筆的入學學生姓名、生日、身分證字號……等重要個人資料，而校方卻在一天之後才向學生寄出道歉信，並請收到外洩資料的220位學生將郵件刪除。許多學生認為校方的處理態度與方式都不夠積極，令人無法接受。

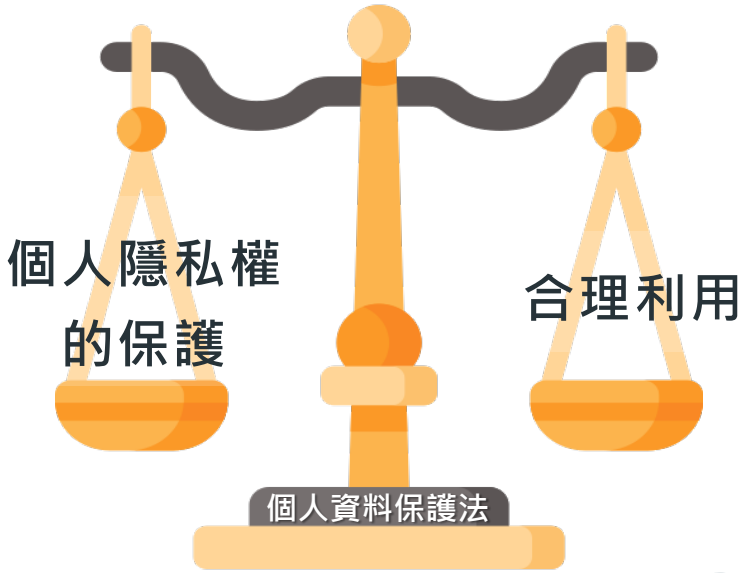
國立中正大學學生：「當下知道這件事情的時候覺得蠻錯愕的，因為很誇張，這件事情沒有人想到會發生。」

國立中正大學學生：「感覺他們（校方）就知道他們錯，但是沒有做出相對應的處理。」

（中正E報，https://pse.is/3gs7sk，檢索日期：2021/06/08）

1.2立法目的

為規範個人資料之蒐集、處理及利用，避免人格權受侵害，並促進個人資料之合理利用（§1）



2.

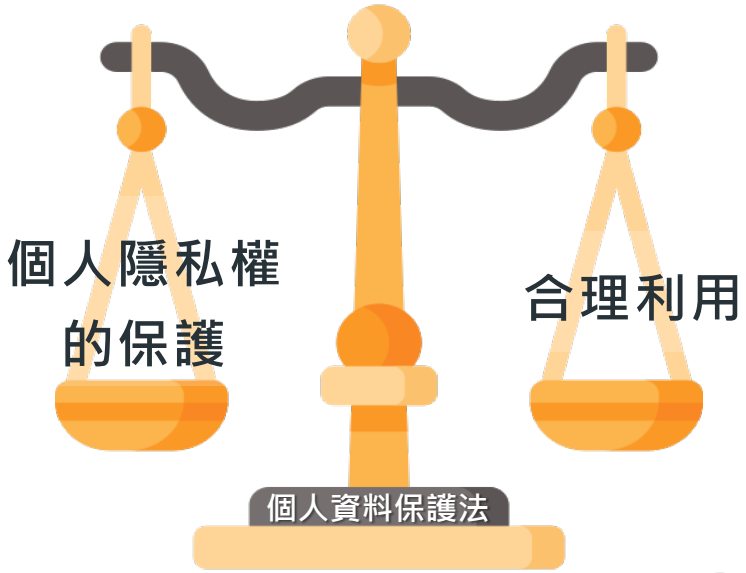
淺談個資法

2.1 個資法架構

(資料來源:iThome)

2.2個人資料定義

為規範個人資料之蒐集、處理及利用，避免人格權受侵害，並促進個人資料之合理利用（§1）



2.2個人資料定義（§2）

一般資料

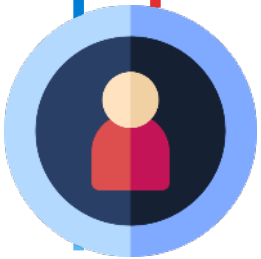
姓名、出生年月日

身分證字號、護照號碼、特徵

指紋、婚姻、家庭、教育、職業

聯絡方式、財務情況、社會活動

其他可以直接或間接辨識個人之資料



特種資料

病歷、醫療、基因、性生活、

健康檢查、犯罪前科

2.3一般個人資料（§2）

一般資料

姓名、出生年月日

身分證字號、護照號碼、特徵

指紋、婚姻、家庭、教育、職業

聯絡方式、財務情況、社會活動

其他可以直接或**間接辨識**個人之資料

間接辨識

藉由資料持有者所保有的其他資料

互相對照、組合、連結

才能識別到特定個人

2.3一般個人資料（§2）

一般資料

姓名、出生年月日

身分證字號、護照號碼、特徵

指紋、婚姻、家庭、教育、職業

聯絡方式、財務情況、社會活動

其他可以直接或間接辨識個人之資料

原則上可合理蒐集、處理、利用

2.4特種個人資料（§2）

原則上不可蒐集、處理、利用

*特殊情況除外（請參考個資法§6）

基於衛生教育法有權對學生病例做適當的處理

只是仍須謹記保密原則

蒐集前後需有適當安全維護措施

特種資料

病歷、醫療、基因、性生活、

健康檢查、犯罪前科

例：學生罹患特殊疾病(如AIDS或開放性肺結核)

新生入學健康檢查體液(尿液、血液)篩檢

2.5適用主體與保護客體

適用主體

現生存之自然人

- 包括**各行各業**及**個人** (§2)
- 受委託蒐集、處理或利用個人資料者，視同**委託機關** (§4)

適用客體

- 以**任何方式**（包括紙本）**留存**的資料
- 以**任何方式取得**個人資料 (§2)

2.6不受個資法規範的情形

1 為了個人或家庭活動的目的而蒐集、處理、利用個人資料

2 在公開場所或公開活動中所蒐集、處理、利用之未與其他個人資料結合之影音資料

2.6公務機關之法律責任

刑事責任

- 違法蒐集處理或利用敏感性資料
- 違法蒐集及處理個人資料
- 違法利用個人資料
- 違法進行國際傳輸

→ 意圖營利：五年以下有期徒刑

- 非法妨害個人資料正確性

→ 五年以下有期徒刑

公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。(§44)

民事責任

- 最高賠償總額 2 億元
- 非財產損害得請求賠償相當金額

每人每一事件

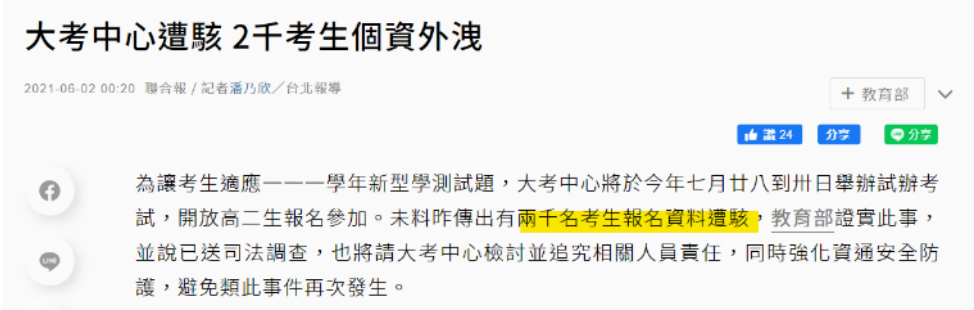
新臺幣五百元以上二萬元以下計算(§28)

2.6個資的價值

每人每一事件

新臺幣五百元以上二萬元以下計算

對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新臺幣二億元為限。(§28)



假如每筆求償金額為1萬元

2,000 x 10,000 = 2千萬

清點所有的個人資料

3.

蒐集個資注意事項

3.1自我檢查五步驟

步驟一：清點所有之個人資料

步驟二：清查蒐集個人資料之途徑與方式

步驟三：確認是否須履行告知義務並建立告知機制

步驟四：確認蒐集、處理、利用之特定目的

步驟五：檢視利用的範圍與方式

（資料來源：台南市教育局個人資料保護法與案例宣導）

3.2 蒐集者的告知義務（§8）

應明確告知個資當事人：

1. 公務機關或非公務機關名稱
2. 蒐集之目的
3. 個人資料之類別
4. 個人資料利用之期間、地區、對象及方式
5. 當事人依第三條規定得行使之權利及方式
6. 當事人得自由選擇提供個人資料時，不提供將對其權益之影響

3.2 當事人所擁有之權利（§3）

1. 查詢或請求閱覽
2. 請求製給複製本
3. 請求補充或更正
4. 請求停止蒐集、處理或利用
5. 請求刪除

3.2 個資保護聲明範例

本OO計畫辦公室，為辦理「OO研討會」，於報名網站所蒐集之姓名、連絡電話與email，目的在於進行活動辦理之相關行政作業，以電子文件、紙本方式使用，至活動結束後一年為止，保存您的個人資料，以作為查詢、確認證明之用，您的個人資料將用於活動主辦單位提供服務之地區，您的資料可能會提供給本計畫辦公室之合作推廣單位。

依據個資法第3條規定，報名者對個人資料於保存期限內得查詢或請求閱覽、 請求製給複製本、 請求補充或更正、 請求停止蒐集、處理、利用或刪除，如欲行使以上權利，請致電06-xxxxxxx。

提醒您，可自由選擇提供個人資料，若其提供之資料不足或有誤時，將導致無法報名此次活動。

3.2 個資保護聲明範例

公務機關或非公務機關名稱　　個人資料之類別

本OO計畫辦公室，為辦理「OO研討會」，於報名網站所蒐集之姓名、連絡電話與email，目的在於進行

蒐集之目的

活動辦理之相關行政作業，以電子文件、紙本方式使用，至活動結束後一年為止，保存您的個人資料，

利用之期間、地區、對象及方式

以作為查詢、確認證明之用，您的個人資料將用於活動主辦單位提供服務之地區，您的資料可能會提供

給本計畫辦公室之合作推廣單位。

依據個資法第3條規定，報名者對個人資料於保存期限內得查詢或請求閱覽、 請求製給複製本、 請求補

當事人依第三條規定得行使之權利及方式

充或更正、 請求停止蒐集、處理、利用或刪除，如欲行使以上權利，請致電06-xxxxxxx。

提醒您，可自由選擇提供個人資料，若提供之資料不足或有誤時，將導致無法報名此次活動。

當事人得自由選擇提供個人資料時，不提供將對其權益之影響

3.2 當事人所擁有之權利（§3）

1 查詢或請求閱覽

2 請求製給複製本

必須在15日內給予答覆
延長時間不得超過15日
(應將延後原因以書面通知當事人)

蒐集者注意事項

3 請求補充或更正

4 請求停止蒐集、處理或利用

5 請求刪除

必須在30日內給予答覆
延長時間不得超過30日
(應將延後原因以書面通知當事人)

3.3 小結

蒐集資料前，請先取得「學生事先授權同意」

可加註在報名表上 / 類似辦理活動保險時之警語

獲得學生本人親簽較妥當，未成年人（20歲）須有法定代理人或監護人簽名

例如：

輔導課程請學生填寫人格測驗、性向測驗

應讓學生填寫授權同意書，並讓其勾選是否同意讓導師知道結果

(未成年人須有法代之同意簽署方為有效)

3.3 小結

Q.若家長來電要求查看學生的測驗結果，是否可以提供?

先確認當事人為未成年或成年

未成年人：父母為未成年子女之法定代理人

3.3 小結

Q.若家長來電要求查看學生的測驗結果，是否可以提供?

先確認當事人為未成年或成年

成年人：須當事人同意才可提供

- 請家長先和學生溝通，取得學生的測驗結果。
- 讓家長得知學校會告知學生，確認取得學生同意才提供。

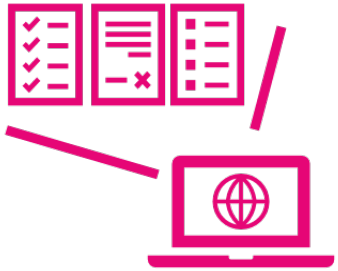
4.

網站個資防護建議

(資料來源:網站安全管理注意事項-台灣學術網路危機處理中心)

4.1 個資外洩主要途徑

網站上的數據洩漏



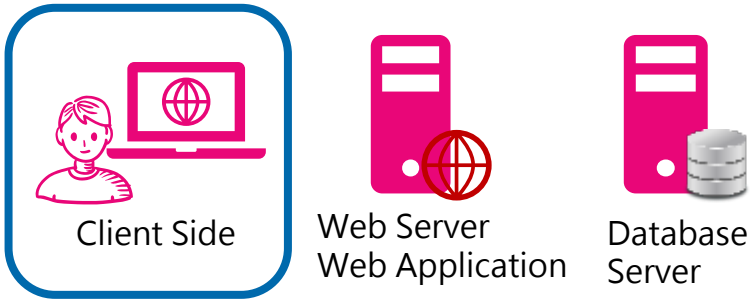
設備送修、遺失或被竊

過期資料未銷毀

駭客入侵竊取

4.2 事前預防

網站、系統主機安全



資料安全

4.2事前預防：禁止使用弱密碼、加強帳號管理

強化帳戶密碼安全性

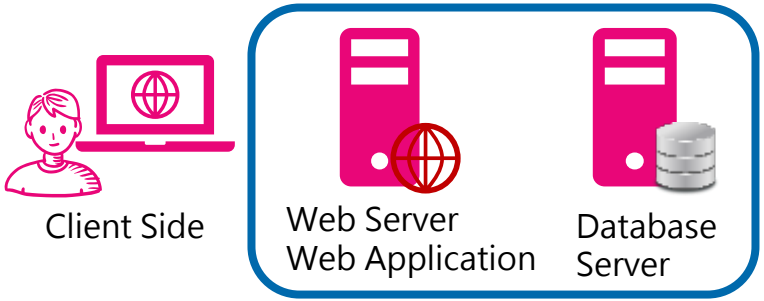
- 強化帳戶密碼安全性
- 應包含**英文字大小寫、數字、特殊**符號等

加強帳號管理

- 職務異動應**重置密碼**，並**定期清查使用者**
- **禁止多人共用**單一帳號
- 儲存使用者密碼進資料庫時，開發人員應該將使用者的密碼作雜湊(Hash)處理

4.2 事前預防

網站、系統主機安全



資料安全

4.2事前預防：定期檢查網站、系統主機安全

定期執行網站與系統主機弱點掃描

- 發現並修正網站、系統主機的潛在威脅。
- 如委外建置網站系統，建議要求廠商配合定期執行網站、系統主機的弱點掃描，並需修正弱點。
- 根據 OWASP 網頁安全指引，檢視網站安全
- 安裝網站應用程式防火牆(WAF)，強化網站安全性

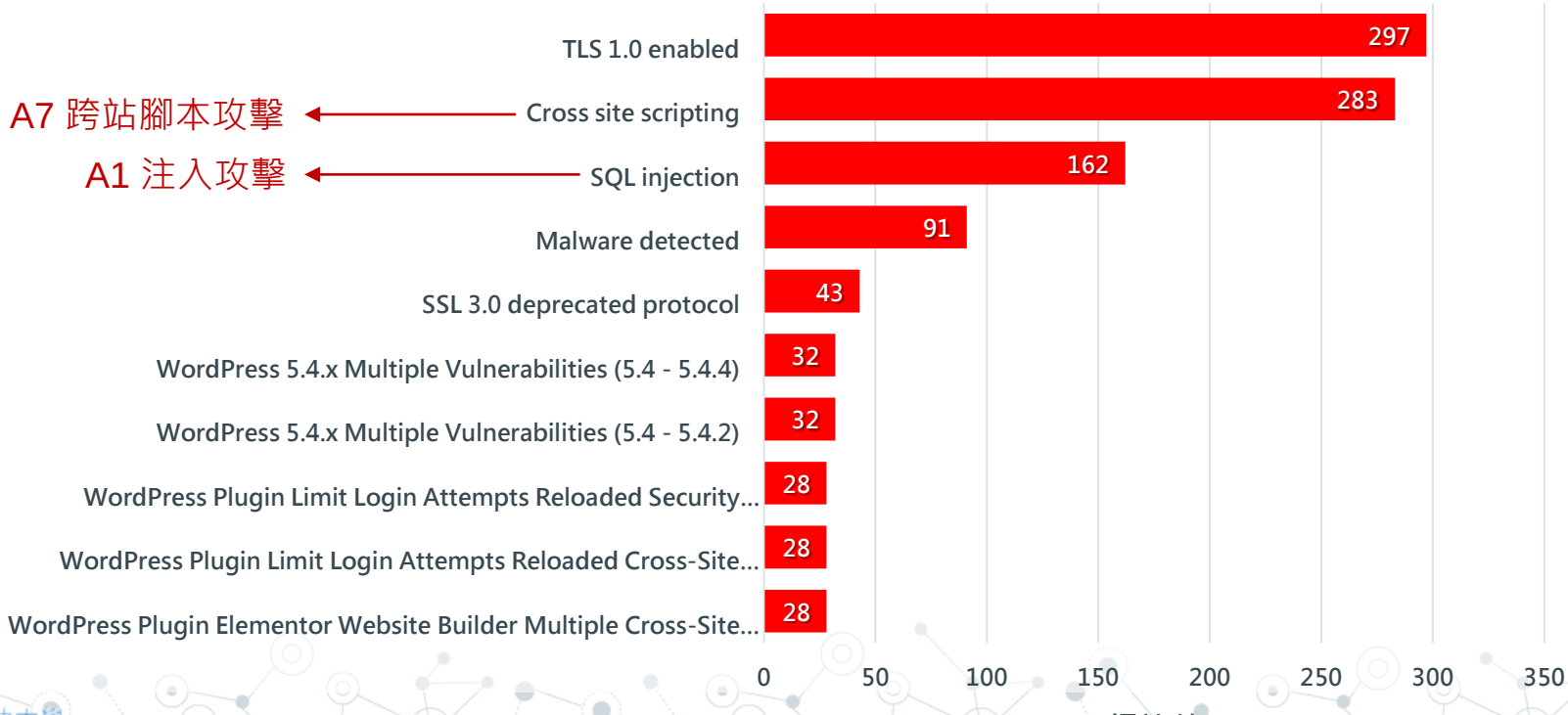
4.2事前預防：定期檢查網站、系統主機安全

OWASP Top 10 (https://owasp.org/www-project-top-ten/)

- A1 Injection 注入攻擊
- A2 Broken Authentication 無效身分認證
- A3 Sensitive Data Exposure 敏感資料外洩
- A4 XML External Entity, XML 外部處理器漏洞
- A5 Broken Access Control 無效的存取控管
- A6 Security Misconfiguration 不安全的組態設定
- A7 XSS (Cross-Site Scripting) 跨站攻擊
- A8 Insecure Deserialization 不安全的反序列化漏洞
- A9 Using Components with Known Vulnerabilities使用已有漏洞的元件
- A10 Insufficient Logging & Monitoring 紀錄與監控不足風險

教育網站Top 10高風險弱點

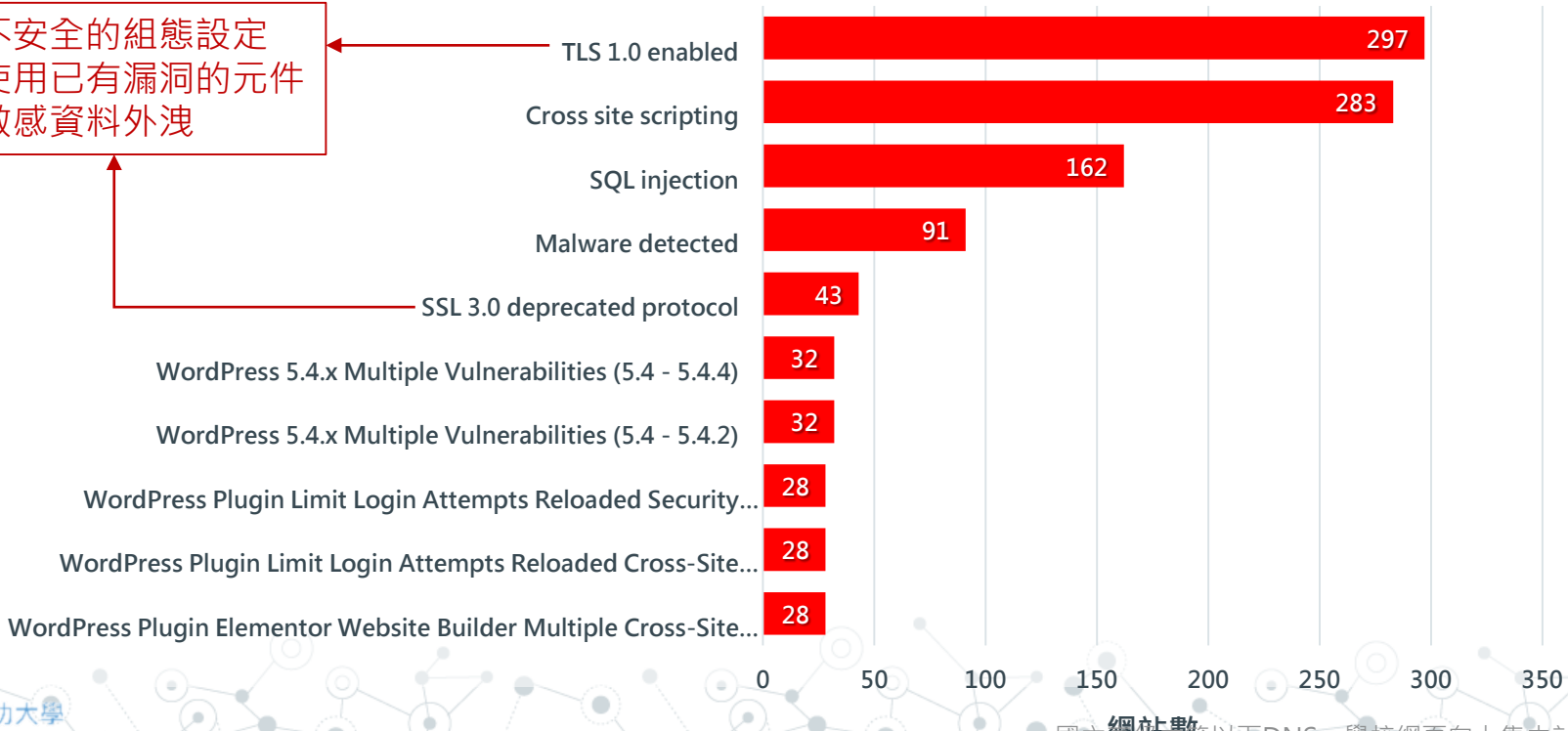
統計期間:110/01/01-110/08/11



教育網站Top 10高風險弱點

統計期間:110/01/01-110/08/11

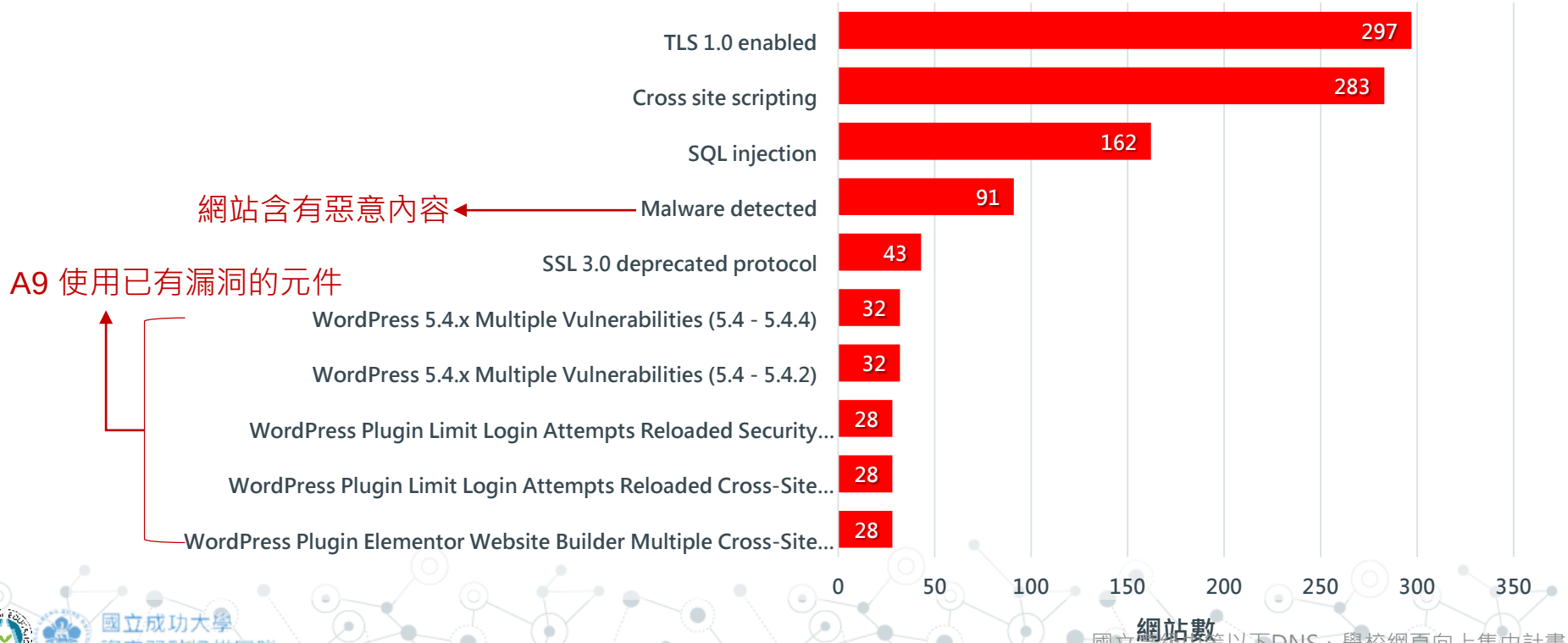
A6 不安全的組態設定
A9 使用已有漏洞的元件
A3 敏感資料外洩



國立機關(構)等以下DNS、學校網頁向上集中計畫

教育網站Top 10高風險弱點

統計期間:110/01/01-110/08/11



4.2事前預防：定期檢查網站、系統主機安全

定期執行網站與系統主機弱點掃描

建議弱掃時機

- 服務公開上線前
- 開發程式過程中，可檢視使用的套件是否有弱點
- 被開立DEF資安事件單者
- B級單位網站每年執行一次
- C級單位網站每兩年執行一次

4.2事前預防：網站資料存取控制

管制使用者的權限

- 使用者只能存取權限內的系功能統與資料，以維護系統的完整性與機密性。
- 存放在Web伺服器上的檔案除了針對後台功能進行控管外，**可透過URL直接存取到的檔案**也必須加以限制。

4.2事前預防：網站資料存取控制

以Google表單設定為例

4.2事前預防：網站資料存取控制

管制使用者的權限

- 具有權限的人員才可上傳檔案
- 針對網站應用程式增加檢測上傳檔案之合法性

  例：檔案類型、大小
- 具有機敏資料的檔案加上觀看權限

4.2 事前預防：其他防護措施

- **檢視主機對外開啟的Port**

  建議關閉駭客常會攻擊的Port，如445port與3389port

- **限制RDP連線主機的來源IP**

  如需使用遠端桌面連線，務必限制可連線的IP

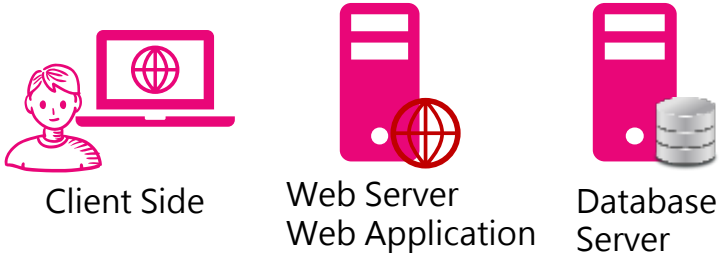
- **Log管理機制**

  保存必要之使用紀錄、軌跡資料及證據

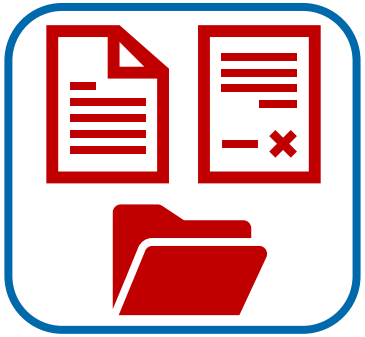
  如系統操作紀錄、個資變更歷史紀錄、操作員日誌等

4.2 事前預防

網站、系統主機安全



資料安全



4.2事前預防：保護機敏資料

應遮蔽個資檔案 或銷毀過期檔案

- 定期/加強審視網站上檔案是否合宜

  例：下架逾期公告 **保存的依據可以參考評鑑（４年1輪）為目標**

  個資檔案遮罩或去識別化 **Ex王O明**

4.2事前預防：盤點網站上的個資檔案

盤點網站上的個資檔案

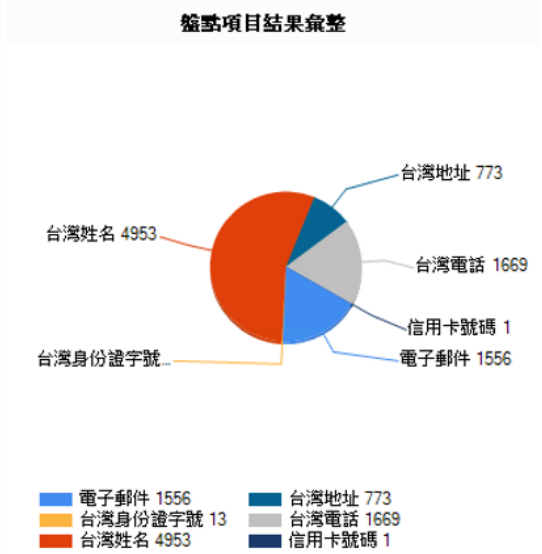
盤點狀態	Finished - Uploaded
盤點耗時	00 天 07:06:54
預估尚餘時間	00 天 00:00:00
盤點檔案合計	2607
盤點成功檔案數	2510
盤點失敗檔案數	97

檔案探尋彙整紀錄

磁碟/目錄	目錄數	檔案數	符合檔案數
/	6,846	30,929	2,607

風險處理狀態

風險	已處理	檔案合計	已處理...	最低比率
低	0	1,226	0.00%	0.00%
中	0	27	0.00%	0.00%
高	0	1	0.00%	0.00%



4.2事前預防：盤點網站上的個資檔案

盤點網站上的個資檔案

類	檔案名稱	風險	符合	盤點項目	前次變更
	/h[redacted]	中	254	3	2020/11/25 上午 11:
	/h[redacted]	中	240	3	2021/1/13 上午 10:
	/h[redacted]	中	188	4	2021/1/13 上午 10:
	/h[redacted]	中	188	4	2020/12/14 上午 09:
	/h[redacted]	高	157	2	2020/11/25 下午 02:
	/h[redacted]	低	154	2	2020/12/30 下午 05:
	/h[redacted]	低	151	3	2020/11/27 下午 02:

盤點項目名稱	符合數
台灣姓名	13
電子郵件	81
台灣身份證字號	1

陳x民,許x智,楊x琇,楊x琦,王x美,陳x郎,歐x秀,李x穎,郭x嘉,張x涓,賴x君,陳x君,葉x民

4.2事前預防：檢查網站上的公開資料

Google 搜尋語法檢查

常用關鍵字

- site: 搜尋特定網址
- inurl: 搜尋特定連結
- intext: 搜尋網頁內文字
- intitle: 搜尋網頁標題
- filetype: 搜尋特定檔案格式
- link: 搜尋互相連結的網頁

4.2事前預防：檢查網站上的公開資料

用Google搜尋語法測試

4.2事前預防：檢查網站上的公開資料

用Google搜尋語法測試

	A	B	C	D	E	F	G	H	I
1	學號	身份證字號	班級	座號	姓名	八月(實)	九月(實)	十月(預)	繳費單金額
2	[redacted]	[redacted]	101	01	王O芝	160	665	700	1525
3			101	02	白O妮	160	665	700	1525
4			101	03	吳O珊	160	665	700	1525
5			101	04	吳O瑄	160	595	700	1455
6			101	05	呂O儒	160	665	700	1525
7			101	06	林O錡	160	665	0	825
8			101	07	俞O伶	160	665	0	825
9			101	08	徐O嫻	160	665	700	1525
10			101	09	徐O婷	160	665	700	1525
11			101	10	張O婕	160	665	0	825
12			101	11	許O雯	160	665	0	825
13			101	12	郭O妤	160	665	700	1525
14			101	13	彭O芸	90	0	0	90

4.2事前預防：檢查網站上的公開資料

用Google搜尋語法測試

4.2事前預防：檢查網站上的公開資料

用Google搜尋語法測試

104學年度 [redacted] 校內賽參賽學生名單

時間13：05~14：10

編號	學號	中文姓名	科系	英文姓名（羅馬拼音）	身分證字號(即密碼)	帳號 (E-mail)	出生年月(西元年)	性別
1	4	[redacted]	管一甲	W[redacted]	R1[redacted]8	15[redacted].edu.tw	1999.12.17	男
2	4	[redacted]	管一甲	HON[redacted]	D1[redacted]6	15[redacted].edu.tw	2000.03.17	男
3	4	[redacted]	管一甲	KANG[redacted]	D1[redacted]9	15[redacted].edu.tw	1999.09.09	男
4	4	[redacted]	管一甲	HUAN[redacted]	R2[redacted]0	15[redacted].edu.tw	1999.09.11	女
5	4	[redacted]	管一甲	WAN[redacted]	R2[redacted]8	15[redacted].edu.tw	2000.02.12	女
6	4	[redacted]	管一甲	CHE[redacted]	R1[redacted]8	15[redacted].edu.tw	2000.06.14	男
7	4	[redacted]	管一甲	JHEN[redacted]	R2[redacted]8	15[redacted].edu.tw	2000.06.17	女
8	4	[redacted]	管一甲	CHE[redacted]	D2[redacted]8	15[redacted].edu.tw	2000.06.11	女
9	4	[redacted]	管一甲	CHEN[redacted]	R1[redacted]5	15[redacted].edu.tw	2000.09.13	男
10	4	[redacted]	管一甲	WAN[redacted]	D1[redacted]8	15[redacted].edu.tw	2000.06.14	男
11	4	[redacted]	管一甲	SI[redacted]	D1[redacted]8	15[redacted].edu.tw	2000.08.17	男
12	4	[redacted]	管一甲	W[redacted]	D1[redacted]6	15[redacted].edu.tw	1999.10.03	男
13	4	[redacted]	管一甲	YAN[redacted]	D2[redacted]7	15[redacted].edu.tw	2000.08.17	女
14	4	[redacted]	管一甲	CHE[redacted]	D2[redacted]8	15[redacted].edu.tw	2000.01.11	女
15	4	[redacted]	管一甲	CAI,M[redacted]	R1[redacted]2	15[redacted].edu.tw	2000.04.24	男
16	4	[redacted]	管一甲	MA[redacted]	R2[redacted]9	15[redacted].edu.tw	1999.12.18	女
17	4	[redacted]	管一甲	SHIH[redacted]	R2[redacted]5	15[redacted].edu.tw	1999.10.13	女
18	4	[redacted]	管一甲	LIN[redacted]	R1[redacted]8	15[redacted].edu.tw	1999.08.24	男
19	4	[redacted]	管一甲	CH[redacted]	D1[redacted]2	15[redacted].edu.tw	2000.07.19	男

4.2事前預防：檢查網站上的公開資料

要求Google移除搜尋資訊

- 移除過舊的內容:
  https://support.google.com/websearch/answer/6349986?hl=zh-Hant
- 要求 Google 移除特定資訊:
  https://support.google.com/websearch/troubleshooter/3111061?visit_id=1-636154605133777232-1381521632&rd=1

4.2事前預防：禁止搜尋引擎爬取相關文件

設定 robots.txt

- 使用方式：上傳到網站的根目錄
- 檔案內容：
  - ✓ User-agent：填入搜尋引擎（* 號代表全部）
  - ✓ Disallow：希望搜尋引擎不要檢索的頁面路徑
  - ✓ Allow：禁止檢索的頁面中，希望能被檢索的頁面路徑

4.2事發應變 確認事件與進行通報

- 了解外洩的網址、原因、資料筆數與個資欄位等內容
- 評估影響範圍
- 完成資通安全事件通報

4.2事發應變 確認事件與進行通報

1. 通報階段

2. 應變處置階段

3. 結報階段

4.2事發應變 確認事件與進行通報

教育機構資安通報平臺

https://info.cert.tanet.edu.tw/

4.2事發應變 個資外洩檔案處理

- 保存個資外洩事件的證據

  例：外洩原因、欄位等，或網站主機的系統日誌

  保存多久的時間?

  當事人求償的時效

  損害事件發生**5年內**提出求償

  知道損害事件後，**2年內**提出求償

- 將外洩個資檔案從網站上移除（包含搜尋引擎的庫存頁面）

3.2事發應變 個資外洩公告

- 個資外洩事件查明後，應通知當事人(個資法§12)

個人資料被侵害的事實
+
已採取的因應措施

言詞、書面、電話、簡訊、電子郵件、傳真、電子文件等方式

4.3 十一項安全維護措施

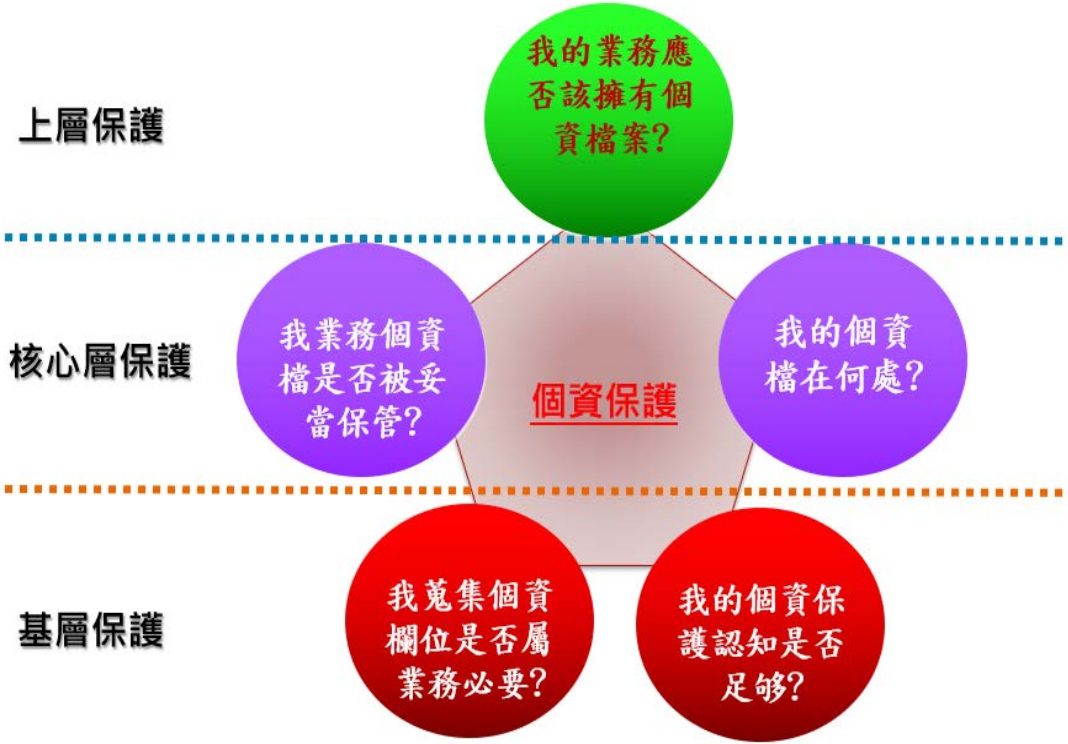
1. 配置管理之人員及相當資源
2. 界定個人資料之範圍
3. 個人資料之風險評估及管理機制
4. 事故之預防、通報及應變機制
5. 個人資料蒐集、處理及利用之內部管理程序
6. 資料安全管理及人員管理
7. 認知宣導及教育訓練
8. 設備安全管理
9. 資料安全稽核機制
10. 使用紀錄、軌跡資料及證據保存
11. 個人資料安全維護之整體持續改善

(個資保法施行細則§12)

防止個人資料被竊取、竄改、毀損、滅失或洩漏

- 團隊組成
- 個資盤點
- 風險評鑑、隱私權衝擊分析
- 建立事故應變SOP
- 制定流程規範/程序書
- 含存取權限、防範措施等
- 法令與內部規範宣導
- 明確的載具使用規範
- 定期內部或第三方稽核
- 以利日後舉證(當事人5年內可求償)
- 定期評估制度的落實程度

4.4總結 個資保護五問



(資料來源：國家衛生研究院莊育秀主任-個資外洩的防範及應變)

Thanks!