資訊安全與防護

敦陽科技
資深經理 蘇威侯

資訊安全與防護

- 個人資訊安全與防護
  - 案例說明
  - 威脅與防護
- 企業資訊安全與防護
  - 企業級資安防護簡介

資訊安全

- 資訊的定義
  - 實體/數位
  - 資訊生命週期
- 資訊安全
  - 機密：不被看到
  - 完整：不被篡改
  - 可用：可供使用

威脅的來源

- 網頁
- 電子郵件
- 圖片
- 影片
- 鍵盤側錄
- 無線網路

網頁

- 假冒網站
- 木馬程式
- 跨站連結

電子郵件

- 假冒寄件者
- 有趣的主旨
- 惡意的附件
- 釣魚連結

圖片/影片

- 內嵌程式碼
- 點播即執行

無線網路

- 封包擷取
- 密碼破解
- 資料洩露

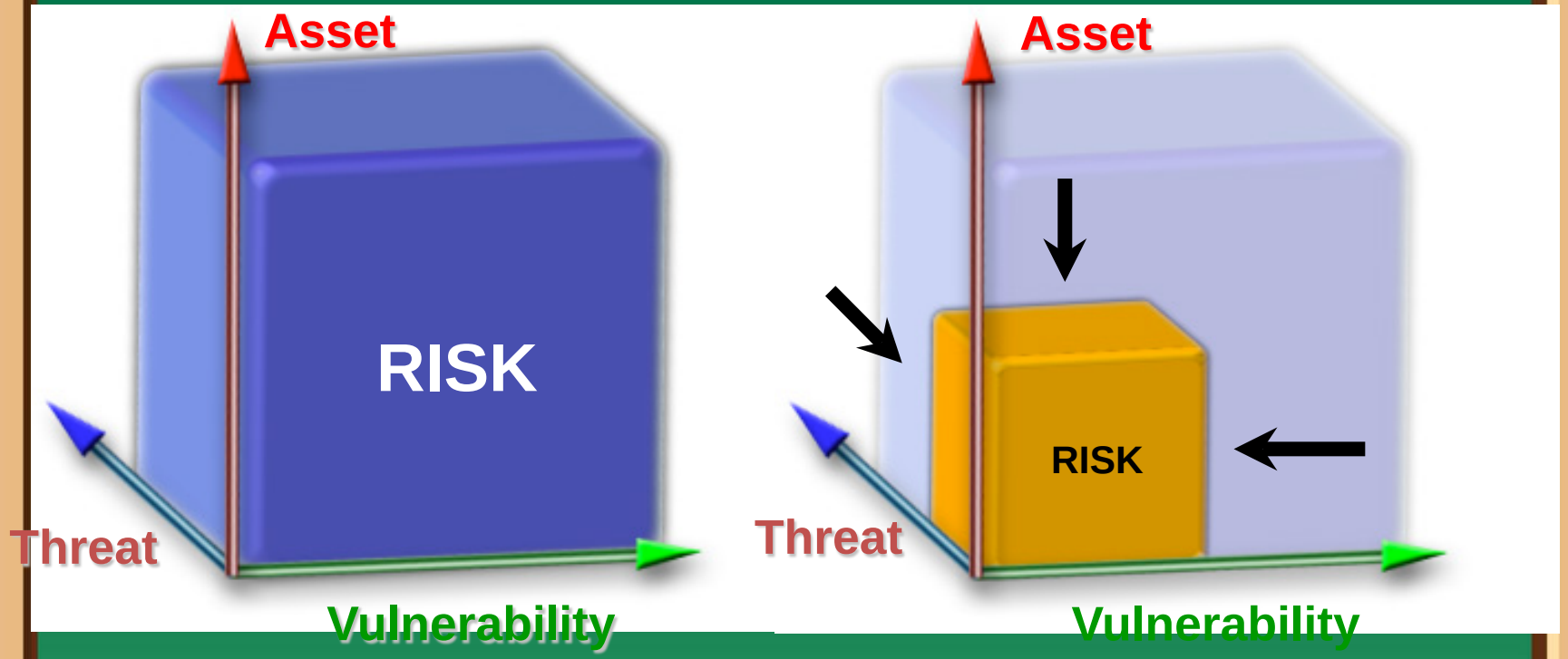
隨身碟

- 傳遞病毒/木馬
- 資料洩漏

安全的使用習慣

- 防毒程式
- 資料備份
- 社群網站
- 自拍影像
- 送修遺失
- 特殊帳密
- 密碼強度
- 更換密碼
- 文件加密
- 傳輸加密
  - SSL/HTTPS
  - VPN

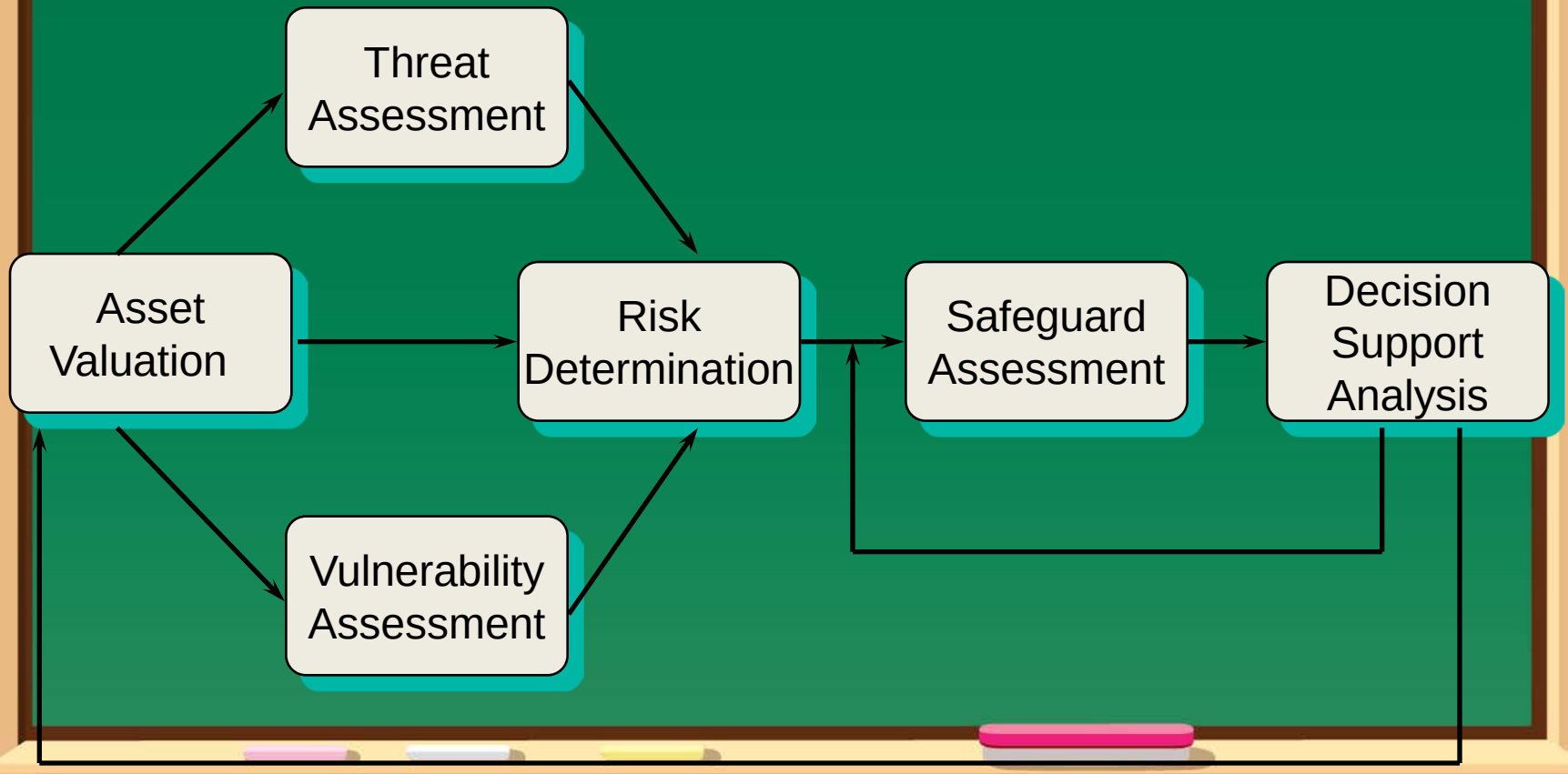
衡量資安風險



風險底線

對策應用後剩餘風險

風險評估流程



防止資料外洩S.M.A.R.T. 五步驟

S: Sort--那些是屬於公司的機密資料？

M: Manage--機密資料由哪些單位/人員經手、處理與負最終責任?

A: Aware--機密資料的流向為何?哪些是高風險的外洩管道?

R: Review--檢視目前的防護機制與措施是否足夠?

T: Tackle--如果發生了機密資料外洩，應如何處理?

資料外洩管道

駭客或惡意程式入侵

主機安全防護

員工意外資料遺失

資料加密

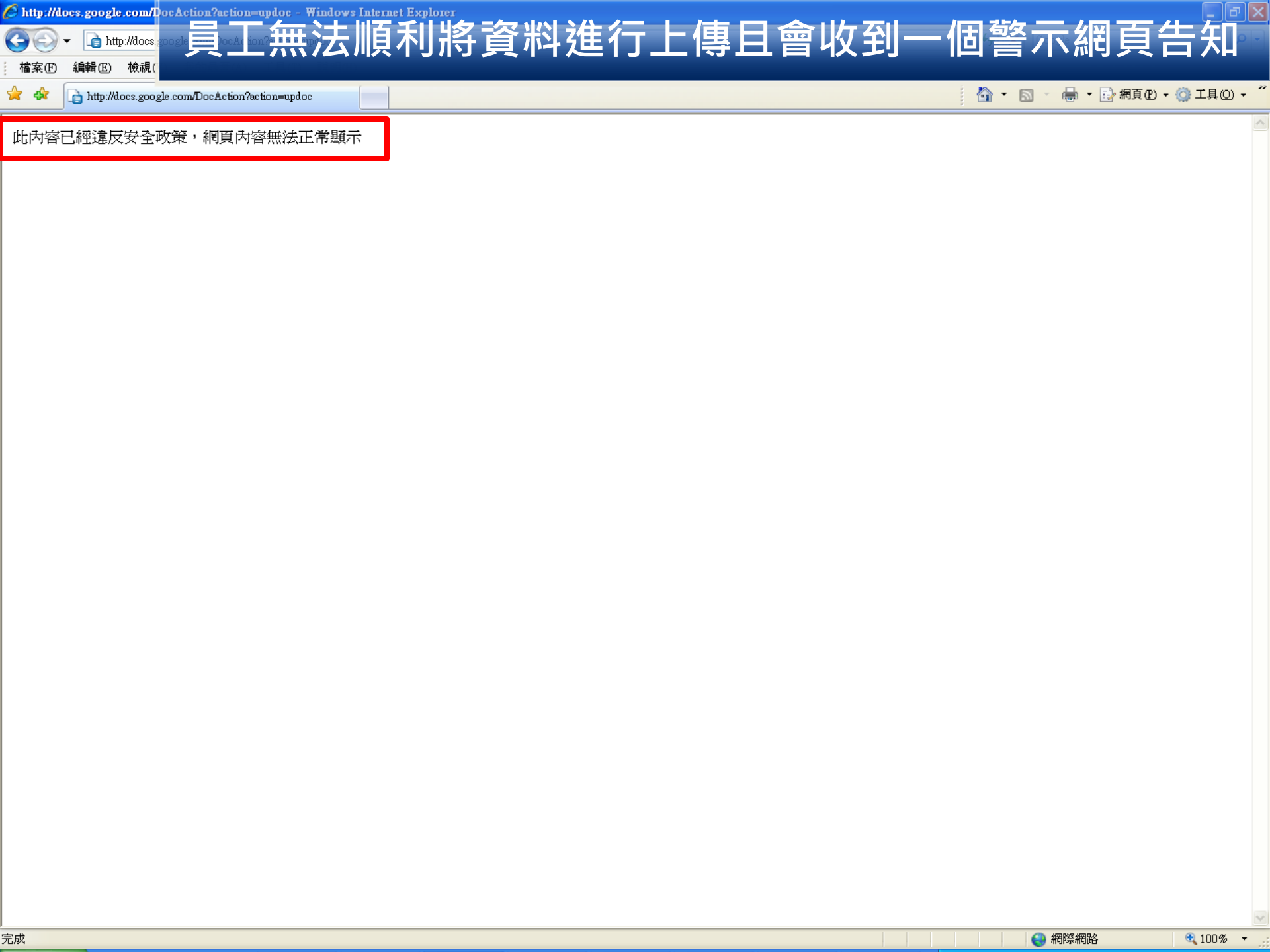
訪客或廠商資料外洩

存取控管機制

內部人員
進行外洩資料

資料外洩
防護

資料來源：
Ponemon Institute 2010


http://docs.google.com/DocAction?action=updoc - Windows Internet Explorer
員工無法順利將資料進行上傳且會收到一個警示網頁告知
檔案(F) 編輯(E) 檢視(
http://docs.google.com/DocAction?action=updoc
網頁(P) 工具(O)
此內容已經違反安全政策，網頁內容無法正常顯示
完成
網際網路
100%

外洩事件分析畫面

Vontu Data Loss Prevention

Administrator logout | profile | help

Reports

All Reports

- **Network**
  - Exec. Summary - Network
  - Incidents - All
  - Incidents - New
  - Policy Summary
  - Status by Policy
  - High Risk Senders - Last 30 Days
- **Endpoint**
  - Exec. Summary - Endpoint
  - Incidents - All
  - Incidents - New
  - Policy Summary
  - Incident Status Summary
  - Highest Offenders
  - Endpoint Location Summary
- **Data at Rest**
  - Exec. Summary - Discover
  - Incidents - All Scans
  - Incidents - New

Policy

- Policies
- Response Rules
- Discover Targets
- Discover Servers
- **Protected Content**
  - Exact Data
  - Indexed Documents

Administration

- **System**
  - Overview
  - Events
  - Alerts
  - Traffic
  - Web Archive

Endpoint
Incident Snapshot 00000467

Report Run 5/6/09 - 2:57 PM

Status: New | Severity: High | Next | Report

IM:MSN

Incident Context

Server	Monitor
Agent Response	Action Blocked
Occurred On	5/6/09 - 2:42 PM
Reported On	5/6/09 - 2:55 PM
User	XP_SP2\administrator
User Justification	User Education: "我不知道傳送這個檔案是違反公司安全政策"
Machine Name	XP_SP2
Machine IP (Corporate)	10.160.11.128
Endpoint Location	On the Corporate Network
Application	Windows Live Messenger, Microsoft Corporation (msnmsgr.exe)
Sender	changdragon@hotmail.com
Recipient	ustock0800@msn.com
Destination IP	64.4.37.26:1863
Attachments	Credit Card _List.xls

Credit Card _List.xls 20 Matches

... **T123501150** 李大寶 (02)-2222-1112 0000-000-000 台北市南京東路五路一八九號八樓 4013 8466 9161 2637 **M104084003** 陳大寶 (02)-2222-1113 0930-111-224 台北市南京東路...30 台北市南京東路五路一九六號八樓 4013 0188 0347 6265 **V126614147** 錢大寶 (02)-2222-1120 0930-111-231 台北市南京東路...32 台北市南京東路五路一九八號八樓 4013 6664 2626 0563 **0214478727** 武大寶 (02)-2222-1122 0930-111-233 台北市南京東路五路一九九號八樓 4013 1511 6670 3304 **R230081949** 蕭大寶 (02)-2222-1123 ...

...000 台北市南京東路五路一八九號八樓 **4013 8466 9161 2637** M104084003 陳大寶 (02)-2222-1113 0930-111-224 台北市南京東路五路一九零號八樓 **4013 3099 5736 8360** D175056598 林大寶 (02)-2222-1114 0930-111-225 台北市南京東路五路一九一號八樓 **4013 0118 7589 2824** Y234322492 周大寶 (02)-2222-1115 0000-000-000 台北市南京東路五路一九二號八樓 **4013 0545 2525 6859** U152012538 許大寶 (02)-2222-1116 0930-111-227 台北市南京東路五路一九三號八樓 **4013 8703 7327 3377** B157259491 趙大寶 (02)-2222-1117 0930-111-228 台北市南京東路五路一九四號八樓 **4013 8794 4922 2615** X175614470 鄭大寶 (02)-2222-1118 0000-000-000 台北市南京東路五路一九五號八樓 **4013 5208 0851 6185** R196190596 莊大寶 (02)-2222-1119 0930-111-230 台北市南京東路五路一九六號八樓 **4013 0188 0347 6265** V126614147 錢大寶 (02)-2222-1120 0930-111-231 台北市南京東路五路一九七號八樓 **4013 5142 3630 2607** S253159656 孫大寶 (02)-2222-1121 0930-111-232 台北市南京東路五路一九八號八樓 **4013 6664 2626 0563** O214478727 武大寶 (02)-2222-1122 0930-111-233 台北市南京東路五路一九九號八樓 **4013 1511 6670 3304** R230081949 蕭大寶 (02)-2222-1123 0000-000-000 台北市南京東路五路二零一號八樓 **4013 1857 9591 7661** K167205190 彭大寶 (02)-2222-1124 0930-111-235 台北市南京東路五路二零三號八樓 **4013 6566 7634 8275** A273274828 廖大寶 (02)-2222-1125 0930-111-236 台北市南京東路五路二零四號八樓 **4013 8589 4510 4436** Y165440790 羅大寶 (02)-2222-1126 0000-000...-2222-1127 0930-111-238 台北市南京東路五路二零六號八樓 **4013 8415 8049 7257** Page

Policy

	#match
Creadit_Card_Narrow [view policy]	20
Narrow)CreaditCard	15
ROCID	5

Correlations

Find Similar

Value	#Incidents/#days	/7	/30	All
User				
XP_SP2\administrator		2	2	2
Machine Name				
XP_SP2		2	2	2
Sender				
changdragon@hotmail.com		2	2	2
Recipient				
ustock0800@msn.com		2	2	2
Destination IP				
64.4.37.26		1	1	1
Attachments				
Credit Card _List.xls		2	2	2
Policy				
Creadit_Card_Narrow		2	2	2

Attributes

Edit

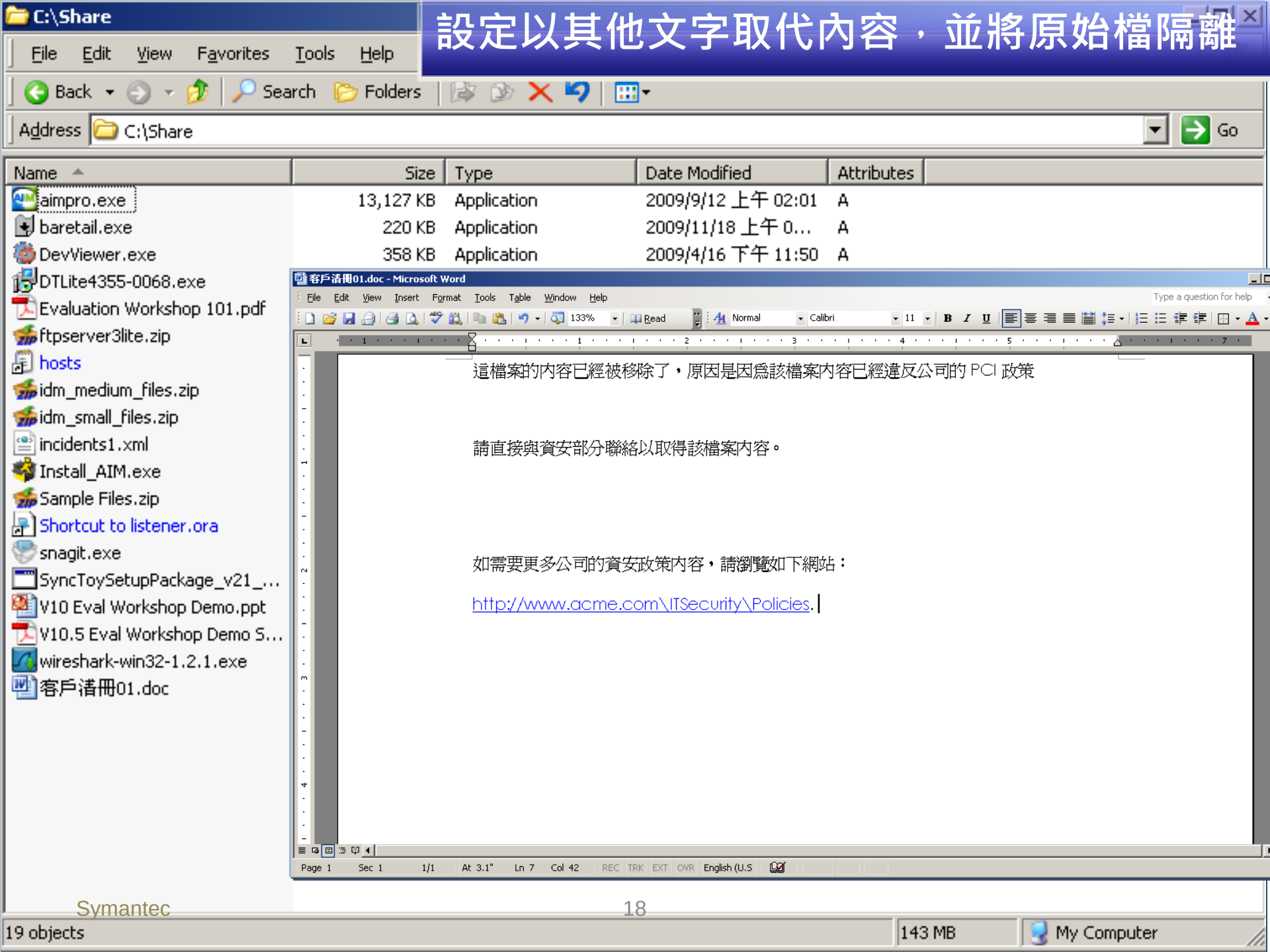
Attribute	Value
NEWS Attribute	NEWS Attribute

History

Add Comment

5/6/09 - 2:55 PM Administrator	**Status Changed** New
5/6/09 - 2:42 PM Administrator	**Severity Changed** High
5/6/09 - 2:42 PM Administrator	**Action Blocked** Blocked a file write or copy
5/6/09 - 2:42 PM Server: Monitor	**Detected**

設定以其他文字取代內容，並將原始檔隔離



外洩事件分析畫面

Symantec Data Loss Prevention

Logged in as: [Administrator] | Logout | Profile | Help

Home | Incidents | Policies | System

Print | Send

Incident Reports | Dashboards | Network | Endpoint Prevent | Discover

Incidents > Discover > Incidents - New > Incident Snapshot

Previous | Next

Incident attributes were saved successfully.

Remediation: Escalate | Launch Investigation | Manual Quarantine | Notify Mgr and Escalate | More

Customize Layout

Incident 00010645

Status: 最新

File System

Severity: High

Key Info | History | Notes

遭不當曝露的資料內容與筆數資訊

關聯分析資訊

適用的政策規範

違反的檔案位置

遭不當曝露的檔案存取權限資訊

外洩者的個人資訊

Policy Matches

	Matches
1客戶資料偵測 [view policy]	17
客戶資料 (EDM)	17

Incident Details

Server	Local Detectio
Target	File Servers
Scan	9/16/10 1 M
Detection Date	9/16/10 5 AM
Seen Before	First s less than 1 day earlier.
File Location	\\Enforcedemo\Share\客戶清冊01.doc [go to file | go to directory | go to Data Insight console]
Document Name	客戶清冊01.doc
File Owner	ACME\Dragon
Scanned Machine	Enforcedemo
File Created	6/9/10 1:44 PM
Last Modified	6/8/10 5:15 PM
Last Accessed	9/16/10 12:45 AM

Access Information

File Permissions

Name	mission
ACME\Administrator	GRANT READ
ACME\Administrator	GRANT WRITE
ACME\Dragon	GRANT READ
BUILTIN\Administrators	GRANT READ
BUILTIN\Administrators	GRANT WRITE
NT AUTHORITY\SYSTEM	GRANT READ
NT AUTHORITY\SYSTEM	GRANT WRITE

Matches (matches found in 1 component)

客戶清冊01.doc (17 Matches):

王大賓 E157205281 4012 3420 1938 3887 (02)-2222-1111 0930-111-222 台北市南京東路五路一八八號八樓

李大賓 T123501150 4013 8466 9161 2637 (02)-2222-1112 0000-000-000 台北市南京東路五路一八九號八樓

陳大賓 M104084003 4013 3099 5736 8360 (02)-2222-1113 0930-111-224 台北市南京東路五路一九零號八樓

林大賓 D175056598 4013 0118 7589 2824 (02)-2222-1114 0930-111-225 台北市南京東路五路一九一號八樓

周大賓 Y234322492 4013 0545 2525 6859 (02)-2222-1115 0000-000-000 台北市南京東路五路一九二號八樓

許大賓 U152012538 4013 8703 7327 3377 (02)-2222-1116 0930-111-227 台北市南京東路五路一九三號八樓

趙大賓 B157259491 4013 8794 4922 2615 (02)-2222-1117 0930-111-228 台北市南京東路五路一九四號八樓

鄭大賓 X175614470 4013 5208 0851 6185 (02)-2222-1118 0000-000-000 台北市南京東路五路一九五號八樓

莊大賓 R196190596 4013 0188 0347 6265 (02)-2222-1119 0930-111-230 台北市南京東路五路一九六號八樓

錢大賓 V126614147 4013 5142 3630 2607 (02)-2222-1120 0930-111-231 台北市南京東路五路一九七號八樓

孫大賓 S253159656 4013 6664 2626 0563 (02)-2222-1121 0930-111-232 台北市南京東路五路一九八號八樓

武大賓 O214478727 4013 1511 6670 3304 (02)-2222-1122 0930-111-233 台北市南京東路五路一九九號八樓

Correlations

Find Similar

Value	Last	All
File Location: \\Enforcedemo\Share\客戶清冊01.doc	1	2
File Owner: ACME\Dragon	3	3
Policy: 1客戶資料偵測	8	16
File Name: 客戶清冊01.doc	3	6

Attributes

Lookup | Edit

主管資訊

主管職稱	協理
主管姓名	Tina
主管郵件資訊	tina@symantec.com

員工資訊

員工編號	061427
員工姓名	Dragon
員工職稱	技術顧問
員工郵件資訊	dragon@symantec.com
電話號碼	02-8722-7076
部門	

補充資訊

事件原因	
案件編號	

Q &A