bsi.

2018 全球科技資安風險與法遵議題

The Tech Risk & Compliance

Peter Pu (蒲樹盛), 總經理 , BSI 英國標準協會

UK Superbrands 2018

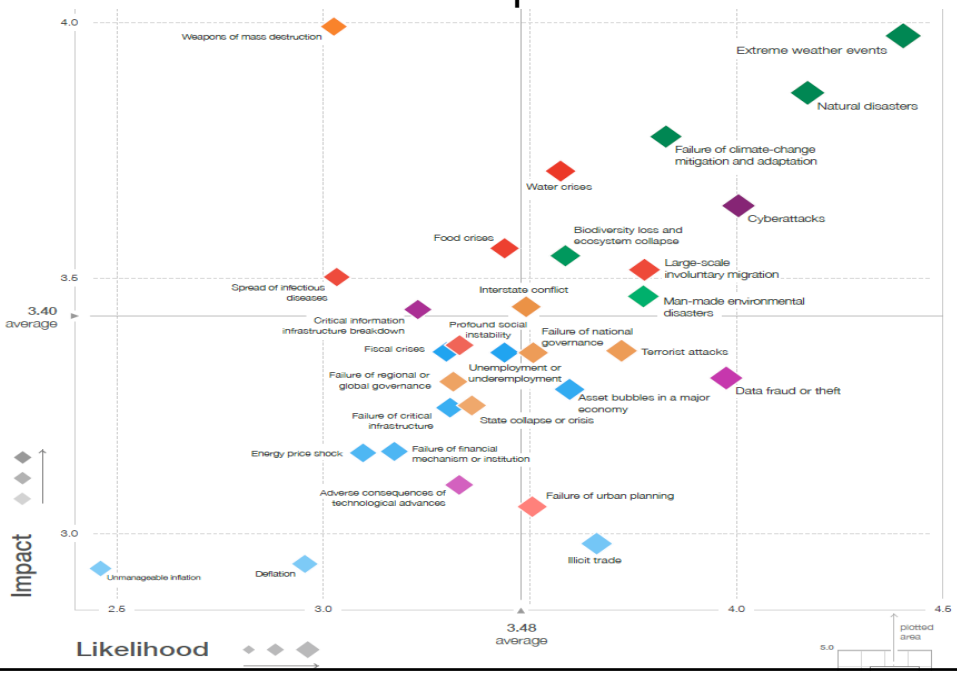
By Royal Charter

INVESTORS IN PEOPLE | Silver

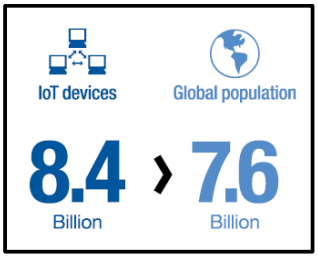
bsi.

2018 Global Risk Report

WEF



bsi.

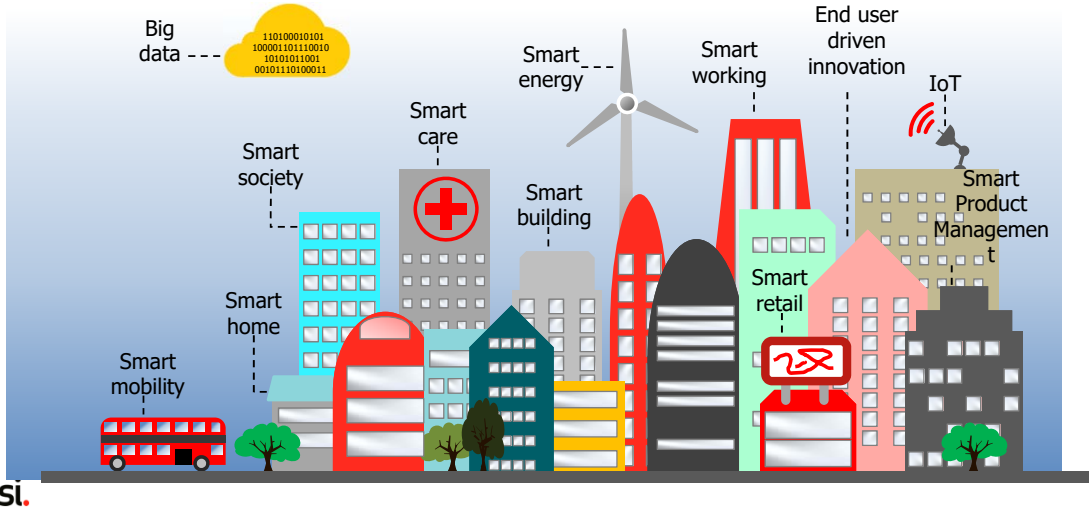


- IoT
- 5G
- Big Data
- AI
- Information Security
- Privacy

bsi.

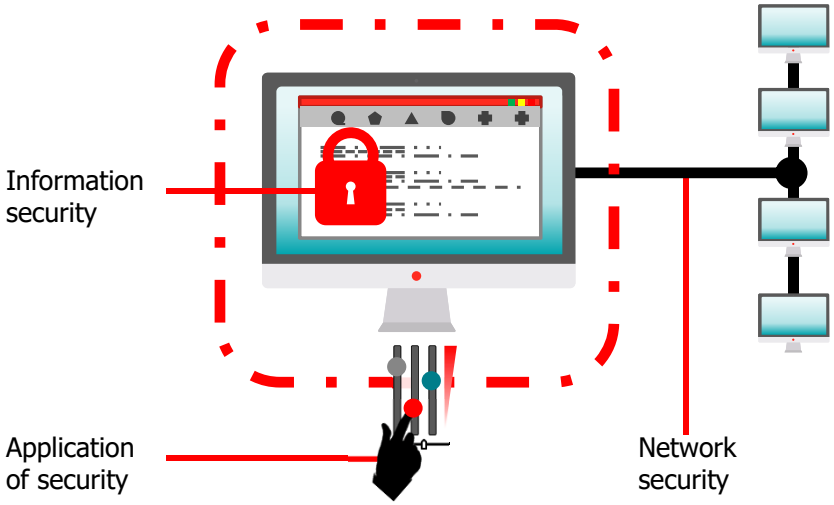
bsi.

IoT potential



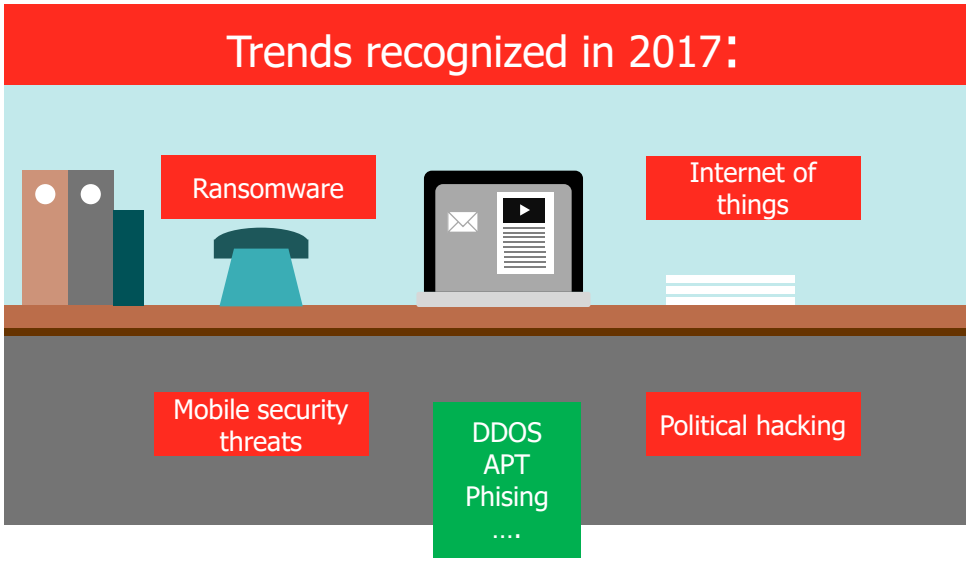
bsi.

The nature of cybersecurity



bsi.

Keeping up to date with latest developments



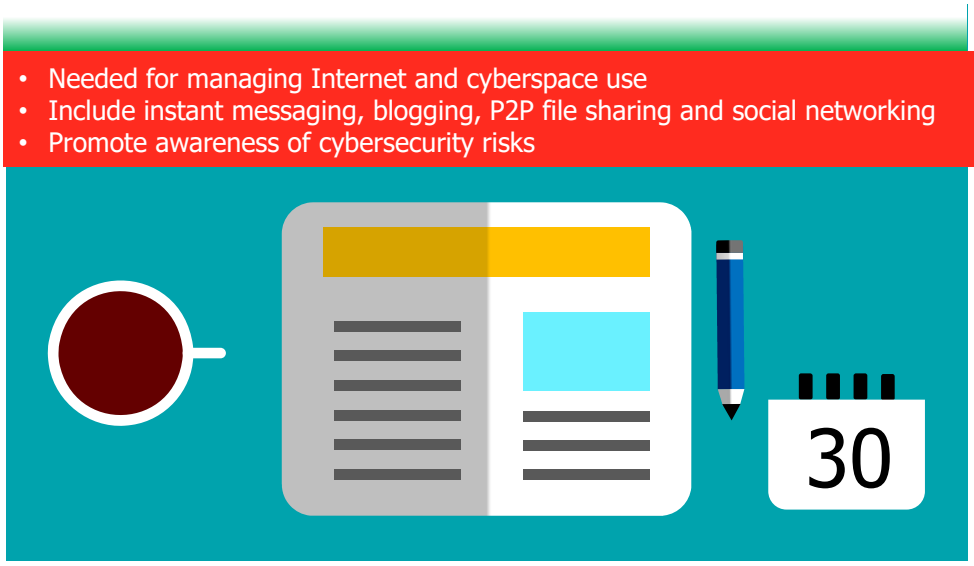
bsi.

- **Risk Assessment**
- **Management System:**
  - ✓ ISO 27001 Information Security
  - ✓ ISO 27032 Cybersecurity
  - ✓ ISO 22301 BCM
  - ✓ .....

bsi

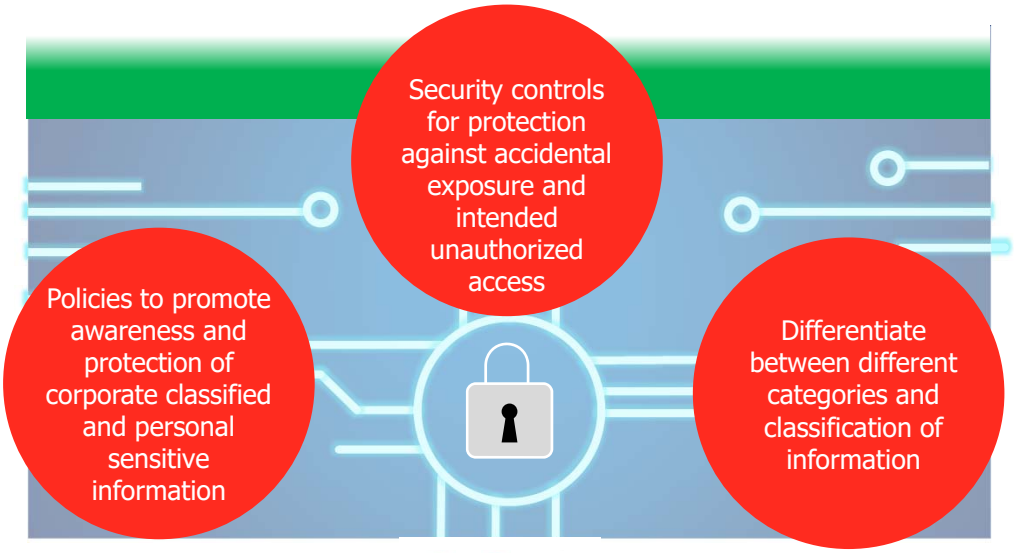
Policies

- Needed for managing Internet and cyberspace use
- Include instant messaging, blogging, P2P file sharing and social networking
- Promote awareness of cybersecurity risks



bsi.

Categorization and classification of information



bsi.

Awareness and training

- Regular updating of relevant knowledge and learning
- All parties to undergo minimum duration of training

bsi.

Be an effective gatekeeper 做一位有效的守門者

Beware of fakes

Do you think that you know who this is?

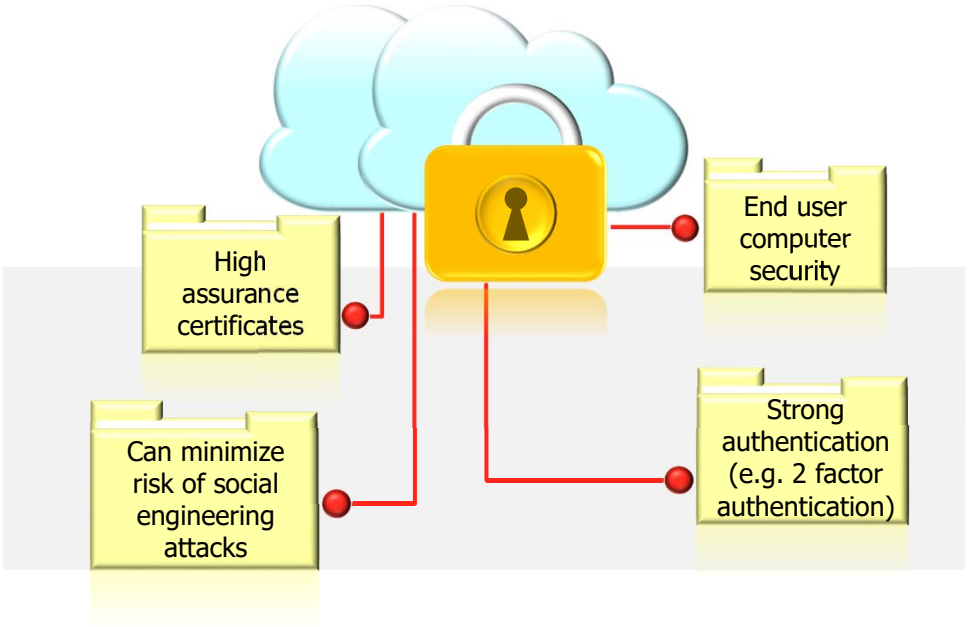
They look like Elvis, but are they? Things are not always what they seem.

bsi.

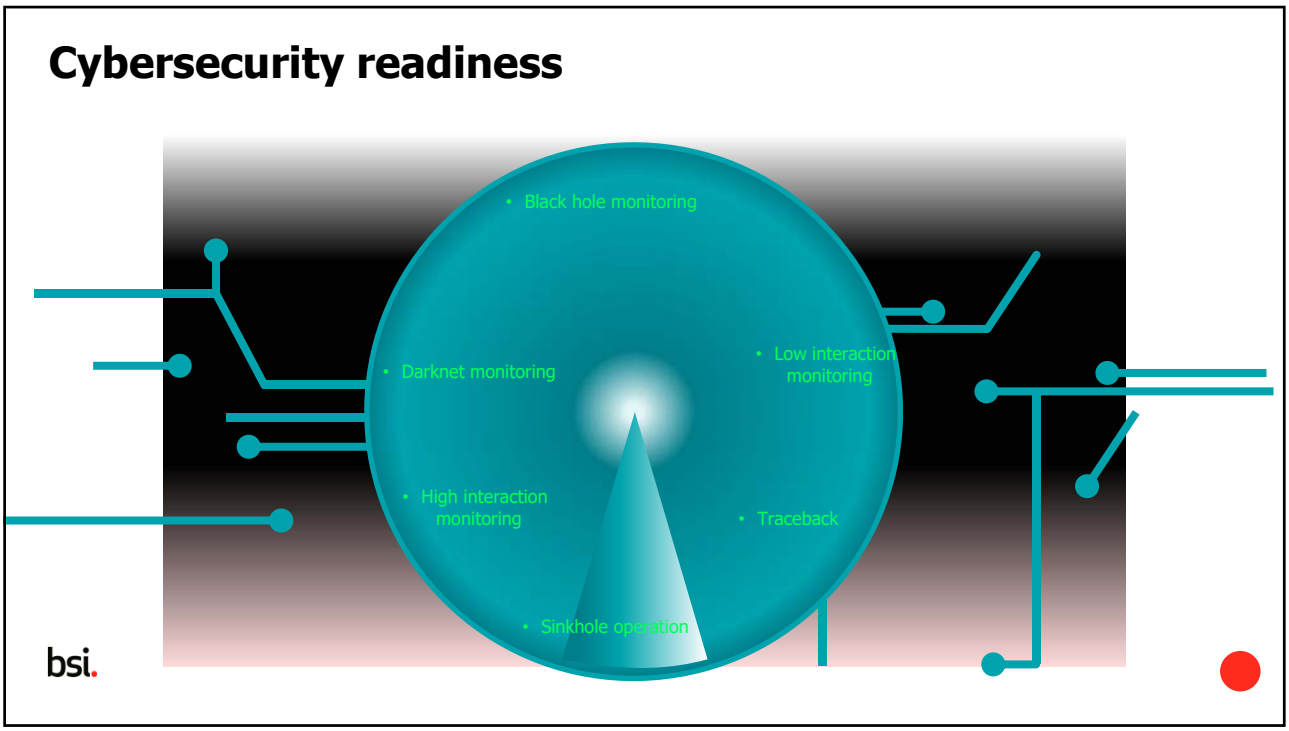
Testing

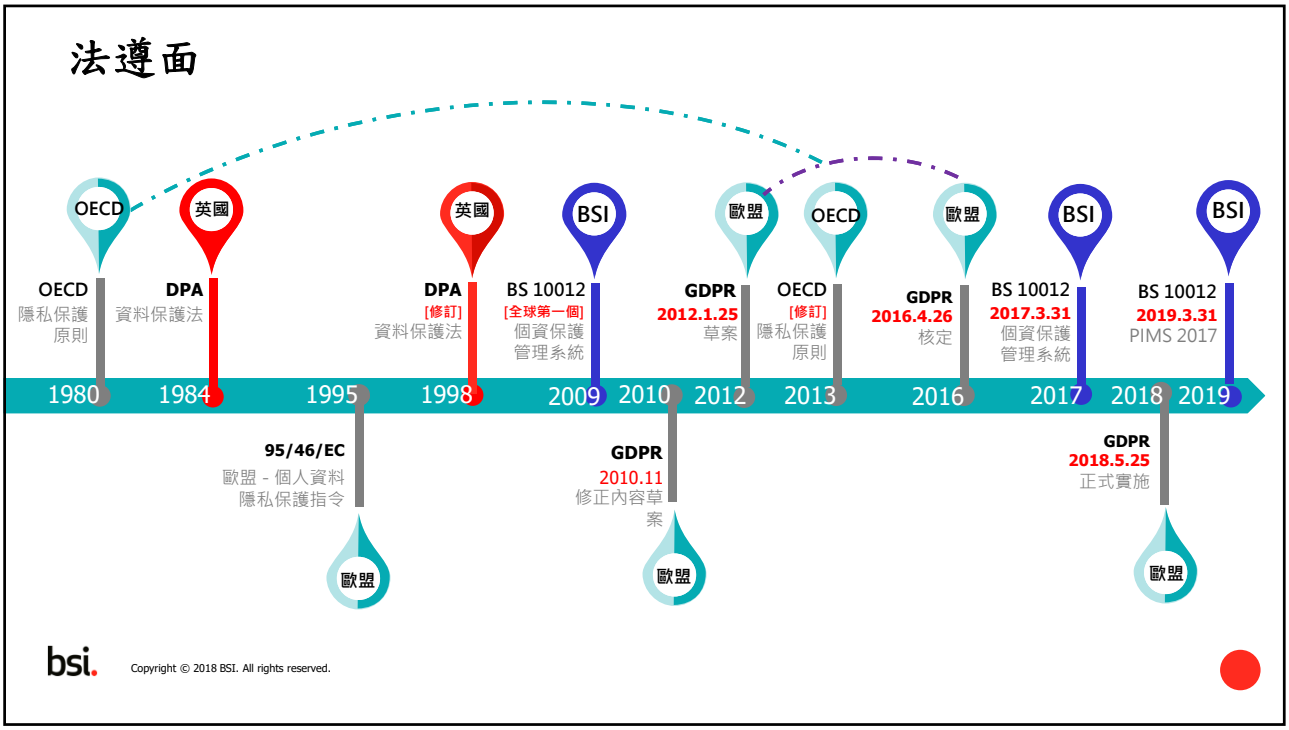
bsi.

Technical



bsi.


Cybersecurity readiness
Black hole monitoring
Darknet monitoring
Low interaction monitoring
High interaction monitoring
Traceback
Sinkhole operation
bsi.


法遵面
OECD
隱私保護原則
1980
英國
DPA
資料保護法
1984
95/46/EC
歐盟 - 個人資料隱私保護指令
1995
歐盟
英國
DPA
[修訂]
資料保護法
1998
BSI
BS 10012
[全球第一個]
個資保護管理系統
2009
GDPR
2010.11
修正內容草案
2010
歐盟
歐盟
GDPR
2012.1.25
草案
2012
OECD
[修訂]
隱私保護原則
2013
歐盟
GDPR
2016.4.26
核定
2016
BSI
BS 10012
2017.3.31
個資保護管理系統
2017
GDPR
2018.5.25
正式實施
2018
歐盟
BSI
BS 10012
2019.3.31
PIMS 2017
2019
bsi.
Copyright © 2018 BSI. All rights reserved.

歐盟一般資料保護規範(共11章99條)
General Data Protection Regulation (GDPR)

- 歐洲議會於2016年4月27日通過歐盟法規2016/679，亦即「一般資料保護規範（General Data Protection Regulation, GDPR）」
- 自2016年5月24日起生效，並取代歐盟1995年的「資料保護綱領」。
- GDPR規定2年過渡期，自2018年5月25日起全面施行新法。
- GDPR不僅適用於歐盟地區註冊的企業，非屬歐盟企業組織但在歐盟境內營運，蒐集、處理或利用歐盟人民的個人資料者均適用本法。
- GDPR提升個資保護強度，大幅提高了罰款金額上限，最高可處罰鍰 2 千萬歐元或年度全球總營業額 4% 的金額。

bsi.

GDPR 適用範圍

第 2 條第 1 項
- 適用於完全或部分以自動化方式處理個人資料，構成或擬構成整理彙集系統一部分的自動方式除外。

第 3 條
- 適用設立於歐盟之控制者或處理者處理個人資料，不論其是否在歐盟內處理。
- 適用非設立於歐盟之控制者或處理者處理資料主體之個人資料，且處理活動與下列業務有關：
  - 提供產品或服務，不論是否需付費予歐盟內之資料主體；或
  - 監控當事人在歐盟內之行為者
- 適用非設立於歐盟之控制者處理個人資料，惟該會員國法律適用國際公法。

bsi.

10 Key Things - 1

Scope & Deadline

- 自2016年5月24日起生效，並取代歐盟1995年的「資料保護綱領」。
- GDPR不僅適用於歐盟地區註冊的企業，非屬歐盟企業組織但在歐盟境內營運，蒐集、處理或利用歐盟人民的個人資料者均適用本法。
- GDPR規定2年過渡期，2018年5月25日起全面施行新法。
- 處理或持有歐盟居民之個人可識別資訊(PII)的組織實施適切的安全性措施，以防止個人資料遺失。

bsi.

10 Key Things - 2

設置「資料保護長Data protection officer，DPO」

- 為確保企業(條文所稱「資料控制者 data controller」或「資料處理者 data processor」)之有效遵循法規，GDPR歐盟要求企業必須設立資料保護長(DPO)。
- 核心業務涉及到對歐盟居民的資料處理
- 此一職位並必須有效依法履行職責，若違反GDPR之規範，DPO將被追究法律責任。

bsi.

10 Key Things - 3

資料蒐集與處理須取得明確有效同意

- 強化同意書的條件，公司將不可再使用充滿法律術語及難以了解的條款與細則。同意書必須是以可理解且容易存取的形式提供，並包括資料處理用途，且能明確與其他事項區分。
- 撤銷同意書必須和提供同意書一樣容易
- 賦予消費者不希望共用資料的相關權利

bsi.

10 Key Things - 4

個人資料可攜權Data portability

GDPR使歐盟公民能對自己的個資擁有更大的控制權，包括「資料可攜權」，也就是在不同服務之間移動個資的權利，用戶可以將其個人資料以及其他相關資料從一個網路服務提供者（ISP）轉移至另一個ISP(例如可將郵件連絡人資料從gmail移動至其他ISP郵件地址)

bsi.

10 Key Things - 5

刪除權

■增加刪除權利，賦予個人可更有效的控制其個人資料。也被稱為「資料抹除」，可讓資料當事人要求資料控制者抹除其個人資料、停止使用個資，包括其供應商或其他第三方。

■抹除條件可包括: 與處理目的不同、非法處理個資，或資料當事人撤銷同意書等，均可要求刪除。

■歐洲法院過去已有判例裁定個人可以要求搜尋引擎(Google)從包括「不相關」或「過期」的個人資訊結果中移除連結。

bsi.

10 Key Things - 6

個人資料外洩通報 (Data breach notification)

■組織(含資料控制者或資料處理者) 若發生個資外洩事件(data breaches)，必須於知悉後72小內通報其資料保護主管機關(Data Protection Authority)。

■若對資料當事人之權益有重大危害之虞，應及時(without undue delay)(未明確規範期限)通知資料當事人。

bsi.

10 Key Things - 7

系統之資料保護設計(Data protection by design and by default)

- 蒐集與處理個人資料，除須符合明確同意等規範外，亦須遵循個人資料蒐集最小化原則(data minimization)。
- GDPR引入「資料保護設計(Data protection by design and by default)」制度，企業於新資訊系統建置與設計時，即應將資料保護設計納入考量，需要與IT廠商充分協商，並通過技術、合約、管理等措施落實遵循GDPR之要求。必須將這些資料處理標準納入與第三方服務提供者簽訂的合約(如個人資料/個人可識別資訊 (PII)之儲存及傳輸加密)。
- 適用至「雲端」之資料控制者及處理者。

bsi.

10 Key Things - 8

反對權（Right to object）

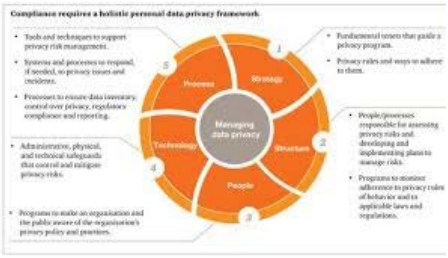
- 個人反對權係資料當事人有權，在特定情況下，反對資料之處理，除非資料控制者證明處理該資料有重大正當理由。
- 當資料當事人提出反對時，資料控制者應立即停止處理該個人資料。
- 亦適用於以大量個人資料所自動化產生之「剖析（profiling）」活動，資料當事人有權瞭解一項特定服務是如何做出特定決策的，此一規範將對以大數據為基礎，運用機器學習、人工智慧技術進行資料分析與研判的服務，將形成重大挑戰，機器學習技術很難適用「反對權」。

bsi.

10 Key Things - 9

資料保護影響評估(Data Protection Impact Assessments，DPIA)

GDPR 要求企業必須進行「資料保護影響評估(Data Protection Impact Assessments，DPIA)」，用以辨識業務活動中涉及個人隱私權利的風險，並加以衡量、管理與因應，並於蒐集與處理個人資料前，評估該等風險與業務活動必要性與對稱性。DPIA與許多企業已實施之「隱私影響評估(Privacy Impact Assessments，PIAs」類似，惟PIAs並無明確的規範與定義，DPIA則強化了其內涵與一致性。



bsi.

10 Key Things - 10

提高罰則金額

GDPR大幅提高違規罰款，依違反情節給予不同程度罰款：

■沒有合法理由，拒絕用戶刪除個人資料請求，沒有建立企業對用戶資料保護的文件化管理，最高將被處以1000萬歐元或全球營業總額的2%的罰款；

■第三類違規行為：非法處理個人資料；沒有合法理由，拒絕用戶停止處理個人資料的請求；在資料洩露事故發生之後，沒有及時通知監管機構；沒有執行隱私風險評估；沒有任命資料保護官，違法向第三國傳輸個人資料；最高將被處以2000萬歐元或全球營業總額4%的罰款。

bsi.

「金融服務業網路安全要求規範」
23 NYCRR Part 500

bsi.

29

美國金融網路安全保護計畫

- 全球金融產業面臨嚴重資安威脅:
  - ✓ 2016孟加拉銀行遭駭客組織入侵，損失達8700萬美元
  - ✓ 2017年4月北韓對18個國家和地區銀行發動攻擊
  - ✓ 金融交易環境仍不夠嚴謹，導致犯罪組織有機可趁。

- 美國紐約州金融廳 (NYDFS)日前發表「銀行業交易監控與制裁名單過濾機制之規範與聲明」(簡稱Part 504)與「金融服務業網路安全要求規範」(23 NYCRR Part 500)相關規則與法案
  - ✓ 要求金融機構應嚴格落實防制洗錢的交易監控機制及制裁名單過濾機制
  - ✓ 規範監管金融機構必須以風險基礎訂定網路安全計畫，降低資安威脅帶來的衝擊。
  - ✓ 紐約的消費者能夠更加信賴金融機構在保護網路安全和個人資訊方面的能力。保護消費者資料和金融系統免受恐怖組織和其他網路罪犯攻擊。

bsi.

30

資安法案「金融服務業網路安全要求規範」
23 NYCRR Part 500

5 Key Points – 1　Scope & Deadline

- 2017/3/1正式生效，NYDFS給予180天緩衝時間落實規範，2018/2/15前必須向NYDFS遞交法遵聲明書
- 適用於紐約州境內處理企業/個人資料的所有金融服務業組織，僅有極少數員工極少或者收入或資產很低的金融機構能夠豁免。
- 法規要求銀行、保險公司和金融服務部監管的其他金融服務機構建立和維護網路安全計畫，旨在保護消費者的私人資料，並確保紐約金融服務業的安全和健全。

bsi.

31

資安法案「金融服務業網路安全要求規範」
23 NYCRR Part 500

5 Key Points – 2 任命資訊安全長(CISO)

- 以確保網路安全計畫之執行的實施和執行情況。
- 資訊安全官可以由企業僱用，或來自其所屬企業或第三方供應商。
- 如網路服務外包，必須任命一名高階職員，作為與第三方網路供應商與該企業的聯絡人。
- 企業須具備“有能力的網路安全人員”，無論該人員是在企業內部還是在所屬企業或第三方服務商。該網路安全人員需管理網路安全風險、安排與網路安全計劃相關的各項事務等。

bsi.

32

資安法案「金融服務業網路安全要求規範」
23 NYCRR Part 500

5 Key Points – 3 訂定網路安全政策及相關法規

- 須建立適當政策和規章，以強化自身或其第三方服務商之網路安全。
- 網路安全政策，包括:
  - ✓ 資訊安全、
  - ✓ 資料管理、
  - ✓ 存取控制、
  - ✓ 系統及網路監控、
  - ✓ 資料加密、
  - ✓ 事件應變等....網路安全事項。

bsi.

33

資安法案「金融服務業網路安全要求規範」
23 NYCRR Part 500

5 Key Points – 4 以風險為導向的最低安控措施

- 從 NIST 標準衍生而來
- 受監管金融機構必須以風險基礎訂定網路安全計畫
- 存取控制
- 資料保護加密
- 事故應變程序
- 保全資料
- 向DFS通知重大事件
- 矯正計畫
- 年度DFS合規報告/認證
- 管理第三方服務提供者
- 年度滲透測試/ 一年兩次的弱點評估

bsi.

34

資安法案「金融服務業網路安全要求規範」
23 NYCRR Part 500

5 Key Points – 5 建立網路安全治理框架

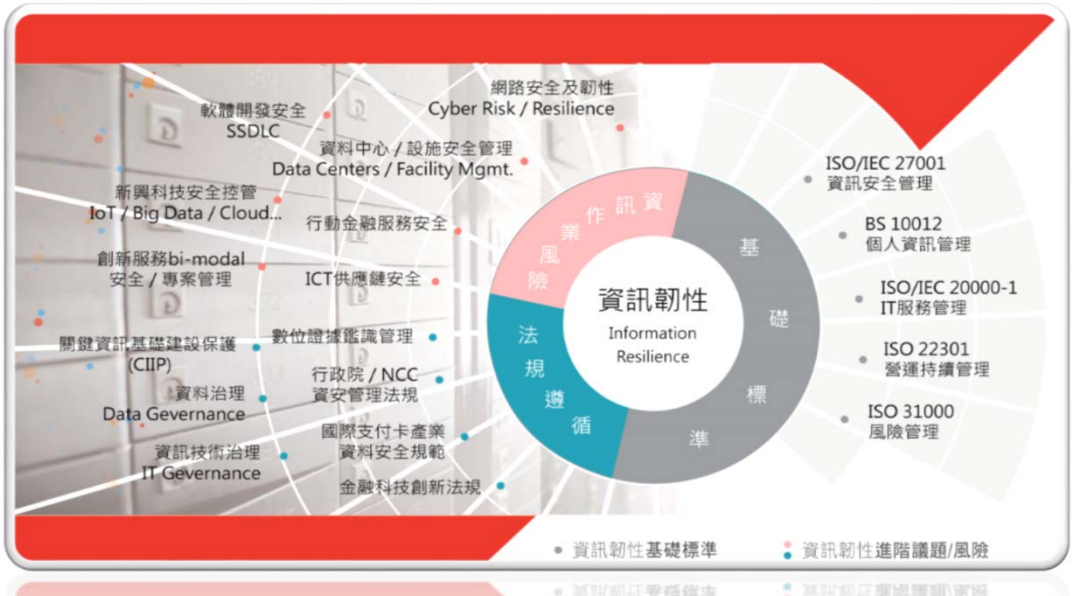
- 建立文件架構
- 管理階層支持與承諾:由管理層監督並定期向最高管理機構報告計畫
- 充足資金和人員配備
- 定期風險評估，已確定技術及系統已達最低安全標準
- 公司高階主管必須每年證明確實遵循 NY DFS 法規(包含紐約州銀行法、紐約州保險法及因蓄意對 DFS 進行不實陳述而導致的刑事和民事罰款)
- “突發事件”的定義，法規表示“任何行為或預備性的行為，無論其成功與否，只要判斷該行為是否獲得了未經授權的途徑，擾亂或者不當使用資訊系統或儲存在資訊系統上的資訊。”
- 事件通報應儘可能迅速，最遲不能晚於事件發生後的72小時。
- 董事會及“高階官員”必須遵守網路安全規則

bsi.

35

Information Resilience 資訊韌性

組織必須**因應數位化所帶來的風險及機會並採取必要的行動**，以有效的提升組織在網路安全及資安治理的能量，以滿足內外部關注方 (interested party) 的期望及要求。



bsi.


bsi.
...making excellence a habit.™