台湾某大学校务行政系统数据脱敏项目

项目简介

不论是中高级学校还是大学等教育单位，由于拥有学生与家长等大量相关数据，所以随着个资新法的全面实施，势必成为个资法法规遵循的高风险单位与机构。且长久以来学校因为面临内外相交迫的安全攻击，所以学校一直是数据泄露最频繁的地方。尤其是强调自由开放的学校网络，经常成为黑客攻击的目标，近年来无线网路的普及更助长了这类攻击气焰。更重要的是，拥有庞大学生与教职人员的教育单位，自然同时拥有数量惊人的个人敏感信息，这也是学校经常数据泄露的主要原因。同时，这些学校经过事后调查发现，其主要原因绝大多数皆因内部监控疏漏或有内部人员有意为之，也因为如此，从数据库安全，以及与数据库存取息息相关的校务行政系统，到报表输出，再到数据库管理员或相关使用者的相关管理规范，自然成为安全防护上的重点。

面临挑战及现状

当前教育单位在面对对外及对内安全防护上都面临严峻的考验，虽然长久以来，教育单位最主要的安全防护资源几乎都放在对外安全防护上，但随着各级教育单位都导入可随处存取的无线网络，反而成为数据入侵的方便管道。

再将焦点放到对内数据库安全防护上，尽管当前有高达 8 成的数据泄露事件，皆来自于数据库本身与相关管理人员之内部监控疏漏所致，但却一直是教育单位防护最薄弱的一环，结果造成学校经常发生许多数据泄露事件。其中，多半是由拥有对内含敏感个人信息有访问权限的老师、行政人员、数据库管理员、外包开发商不慎或有心外泄而出。最常见的情况是，

解决方案

- Informatica Dynamic Data Masking

收益

- 通过 DDM 动态数据脱敏技术，大幅提升敏感信息的安全
- 符合台湾个资法规遵循的要求
- 完全杜绝因内部 Power User 故意或大意所导致数据泄露的可能性
- 不会对校务行政系统等既有应用系统造成任何影响
- 人力资源及管理效益的提升：不需耗时费工地自行撰写脱敏程序，学校能有充足的人力进行其他重大项目的开发工作。同时，Informatica 灵活又方便的存取政策，让安全管理变得更轻松、更有效率

校内定期或不时举办的校务会议，抑或与外包供应商的系统开发会议上，来自数据库的报表，往往在会后因疏忽或有心而外泄出去，结果造成甚至在网络上都可以搜寻到学生个人信息的可怕情形。

过去即使有数据泄露事件的发生，也顶多只有舆论上的压力而已，但随着台湾个资新法的到来，拥有数量庞大个人信息的教育单位，势将面临层出不穷的诉讼与沉重罚金之风险。

不论如何，如何提升与个人信息相关的数据库与应用系统安全，已经成为教育单位的当务之急。除了数据库本身的安全提升外，当前教育单位首先最关注的安全重点，莫过于校务行政系统。毕竟该系统牵涉许多包括教职人事、学生基本资料、家长通讯录、家庭状况及学生成绩等个人资料，所以经常因为内部人员故意、疏忽或外部入侵等因素而导致庞大个人信息的外泄。但若透过传统数据库加密机制，往往会造成系统效能下降，并增加管理负荷。但若自行撰写程序来进行重要资料的遮蔽保护，难免会造成人力与时间成本的提高，并影响到其他项目的开发进度。也因为如此，许多学校都能立即感受到 Informatica DDM 的高安全性和成本有效性，而毅然决然地实施 DDM 方案，来作为关键数据库与校务行政系统的最佳防护机制。

1. 挑战

(1) 台湾个资新法全面实施：教育单位拥有庞大学生与教职人员信息，稍有安全及管理疏失，势必将面临可观罚金等法规风险。

(2) 如何防止分散在各处的个人信息免遭非法或故意存取与外泄

- 如何保护关键数据库安全
- 如何保护校务行政系统本身与数据存取安全
- 如何保护由校务行政系统所生成的报表的安全性
- 如何防止 DBA、Power User、应用开发合作伙伴滥用权限造成数据泄露

2. 客户问题分析

(1) 台湾个资法法规遵循压力：为了遵循台湾个资法规要求，台湾某大学紧急寻求 Informatica DDM 用以保护个人信息安全。正因为个资法属于跨产业的安全问题，所以除了 B2B 牵涉个人信息较少的行业之外，凡有接触到个人信息的企业和机构，都必须寻求符合个资法规遵循要求的安全防护解决方案，对于金融业、服务业、电子商务及教育单位等无论从个人信息接触数量还是频率都相对较高的组织与单位来说，个人信息泄露的机率及风险自然更高，更需要较严谨且全面的敏感数据安全防护方案才行。

(2) 安全防护比例不均：当前数据泄露约 80% 是由于数据库内部监控不力导致的，来自网络入侵的比例只占 20%。但当前教育单位与企业一样，都不长期将 80% 努力及预算全放在 20% 的网络攻击防护上，而最重要的数据库安全及内控上，却只有少数经费与努力的投入，甚至有许多教育单位完全没有采取安全防护措施，以致数据泄露事件一直上演。

3. 项目难点

(1) 个人敏感数量庞大，类型繁多，造成管理及盘点困难，包括：

- 教职人员人事资料
- 学生基本资料
- 家长联络方式
- 家庭状况
- 班级成绩资料
- 健康检查结果
- 心理辅导档案
- 其他：例如欠费名单、低收入家庭、单亲等身分登记信息。

(2) 学生相关信息公布

学校经常会透过校务行政系统，在网络或校内公布栏上，进行学生成绩、选课、奖惩等资讯的对外公告。

如何兼顾资讯公告与敏感信息不外泄的目的，亦即相关学生可以从中获得资讯的同时，又能保护自身信息的安全。

(3) 大量纸质资料需求

常有透过校务系统输出报表的需求：除了报表档的输出外，为了方便校务会议的召开与讨论，经常会有纸质报表输出的需求。

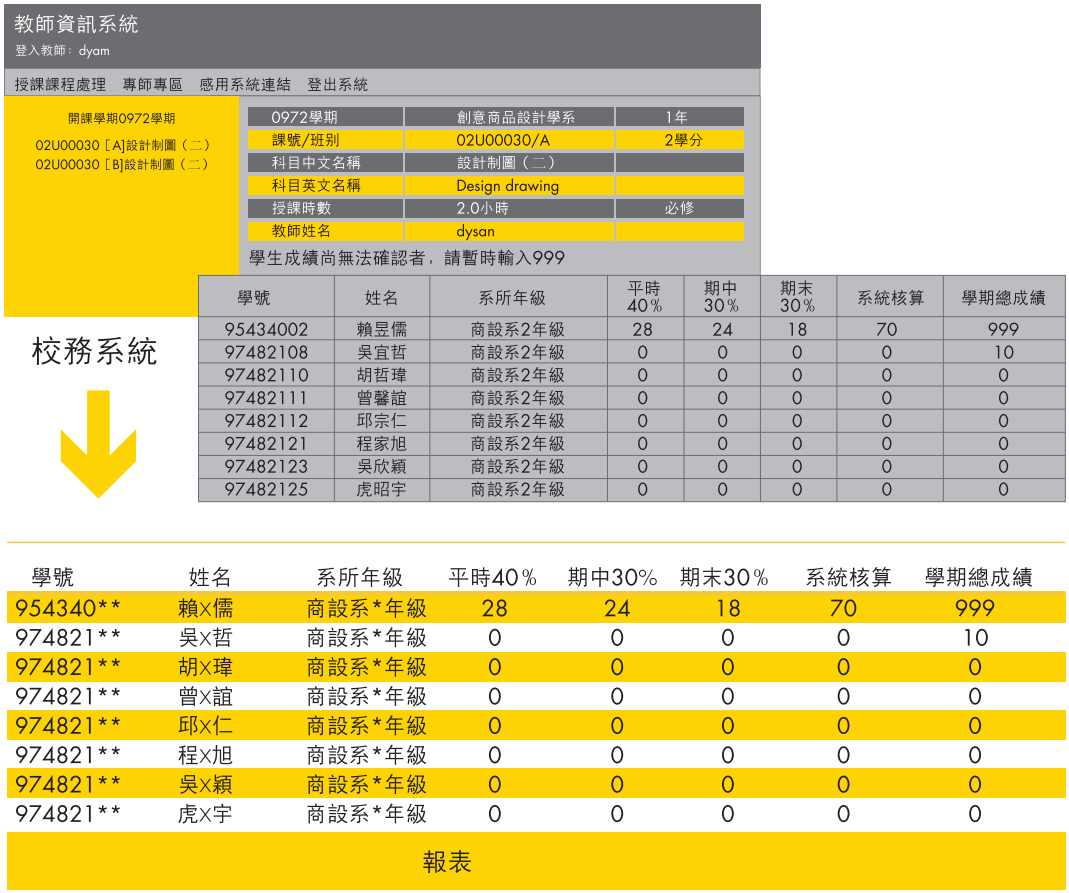
安全上的隐患：不但容易出现数据泄露风险，同时纸质报表也会有防护不易的问题出现。

(4) 不能对既有校务行政系统有所修改、变更或造成其他影响：必须在不修改、变更既有校务行政系统的前提下，同时达到保护敏感数据的作用。

(5) 许多教育单位在报表脱敏与 Power User 安全防护之后，下一阶段多半都希望能将数据库脱敏技术，拓展至应用系统上：

- 如此一来，势必需要对学校校务行政等应用系统进行修改
- 无缝导入仅限于 Query-Only 的应用，而不会有升级的需要。否则可

台湾某大学通过 Information DDM 保护校务行政系统架构图



能出现版本紊乱的问题，进而导致查询错误的可能情形发生。

- 许多学校应用系统多半透过第三方开发商撰写，若要进行应用系统修改，势必得与其开发商一同开会，致使整个项目会变得异常复杂，客户最终可能因而却步。

4. 项目实施目标

(1) 在不对校务行政系统有所变动的前提下，达到敏感信息防护与不外泄的要求。

(2) 即凡涉及个人敏感信息的电子档或纸质文件都能受到安全规范和保护。

(3) 防止 Power User 的非法存取、滥用及外泄。

项目流程及阶段

1. 第一阶段：输出报表的动态脱敏

(1)Information DDM 调查与 POC 测试

(2) 预算评估

(3) 导入与验收

2. 第二阶段：针对 DBA 等 Power User 的安全管控

(1) 权限管控

(2) 对所存取数据进行脱敏

(3) 设定存取政策 (Access Policy)

3. 第三阶段：校务行政系统等应用系统的安全脱敏

项目过程与困难

1. 项目时间：约 1-2 个月

2. 最大挑战

(1) 避免现有应用系统的变动下，兼顾敏感信息的保护。

(2) 将数据库脱敏技术，直接运用到应用系统上。