拒绝网络攻击与勒索病毒 企业 CEO 应该具备的资安观念与态度

文 | 郭宪志

近年来，企业遭受网络攻击与勒索病毒事件频传，为杜绝黑客恶意攻击，企业应具备正确的资安观念与态度，然而根据 CIO 调查结果显示，企业对于资安的重视程度仍有相当大的成长空间，且多数 CEO 着重于提升企业效率与降低成本，但其实并不一定花大钱才能够做好资安，若能正确建立对于企业资安的战略层级思维，便能降低网络攻击与勒索病毒发生的风险！

多数企业 CEO 其实并不重视资安

今日应该鲜少有企业的运作能够脱离对网路及信息系统的依赖，但是又有多少企业的经营者对于网络与信息安全有充足的认识与了解呢?

根据最近一期的 CIO 大调查（Y2020 ~ 2021），企业的 CIO 直接向 CEO 报告的比例从过去的 45% 上升至 70.9%，这虽然代表着企业对 IT 部门的重视程度正在提高，但却不等同于资讯安全的问题已得到应有重视。

因为同一份 CIO 大调查报告也显示出企业的 IT 预算，最主要还是花在基础架构的采购，包括：服务器、云端服务、储存设备、及网络设备仍占据企业 IT 预算的前四项主要支出，即使报告中“增加资安投资”已进入排名内，但实际的预算支出规模仍远远落在后面。

CEO 关心的是提高效率＆降低成本

我不禁好奇的想问：为什么 CIO 可以不直接报告给 CEO? 如同大家的理解、网络与信息系统对于多数企业的重

2021 中国台湾资安大会，数联与母公司远传参展，众多贵宾与 CEO 莅临参观

要性是毋庸置疑的，但是仍有高达三成的 CEO 不会直接参与及了解 IT 相关的事务，更遑论 CEO 能够体会到信息安全的重要性及应有的投资比重。

在许多企业 CEO 的思维中，IT 就是一个后勤的服务提供单位、简而言之就是一个很花钱、但又不能没有的部门；因此、每当 IT 部门提出预算要求时 CEO 总是会质疑：这些钱现在一定要花吗？花了这些钱之后可以提升多少产值啊？导致 CIO 们对企业 IT 的投资也会随之以“提高效率”或“降低成本”作为主要要求，这也就形成了今天多数企业“明知资安很重要、但花钱时却变得没有那么必要！”的奇怪现象。

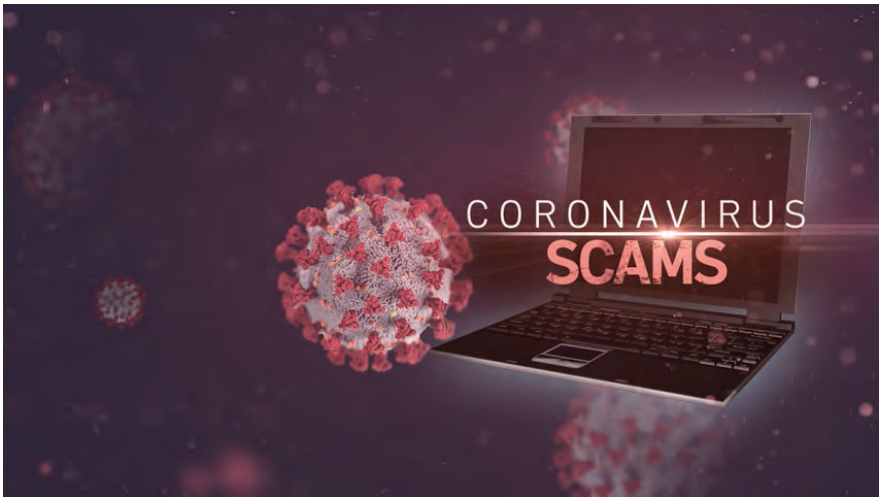
不是花大钱才能做好资安

多数是因为 CEO 不关心与不了解网络与信息系统，所以也很难理解为什么当网络及信息系统出现安全的问题，会影响企业的运作、甚至是让企业经营因此陷入危机。

更因为如此，多数的企业有 IT 部门、却未必有专责的信息安全人员，更普遍的情况是 CIO 兼任着企业的 CSO（Chief Security Officer），但是实务上而言、如前述 CIO 关心的是如何使信息系统的运作更有效率、及如何降低的成本，但 CSO 应该关注的却是：如何让企业免于曝露在网络攻击与信息系统被入侵的安全风险之下，其范畴并非仅是信息系统的效能、更重要的是安全，其中还包括了企业内部的流程管理、内部稽核与控制系统、个人资料保护等等。这两者的角色功能看似雷同、但却是彼此互斥，甚至有类似球员与裁判般的冲突，而当两者角色重迭、也就成为许多企业最终很难将资安落实做好的原因之一。

事实上用 IT 的观点做资安工作，确实比较容易陷入“资安就是要花大钱”的迷思，原因就是：传统信息系的建置以硬件加软件采购为主，但是资安真正的核心却是“服务”！因为网络攻击与黑客行为是不断地在改变，没有哪一套硬设备或是软件可以保证绝对不会被攻破、万无一失！重要的是如何让企业的资安防护措施，持续保持在最能因应当下变化的状态，但企业的 IT 购买硬体、购买软件就是要附赠服务，这服务真的是专业的吗?

我看过许多案例：企业花大钱买昂贵的防火墙系统，但内部的 IT 人员却不具备调校防火墙“关联规则”的能力，



供货商也不是资安专业的厂商，只是价格最有优势的代理或 SI 厂商，因此，从购入设备的第一天到最后这个设备被淘汰更新，能够让它发挥作用的最重要关键设定就是停在出厂值，从未被动过！甚至更多情况是设备早就已经“终止服务”（Endof Service）或是国外原厂已经退出中国台湾市场了（或是被其他公司并购）这个设备都仍装在里，所以、设备未必真正发挥应有的功能，购置这个就是买一心安而已。

企业资安需要的是战略层级的思维（Strategic Thinking）

相信企业的领导者都清楚知道几个常见的商业运作准则，例如：货物交付海运或空运必然会依据其价值办理保险，显而易见的就是运输过程的风险必须有所保障；又例如：保险公司承接医疗或是人寿保险，会根据被保险人的年龄、健康状况，甚至是必须先提供当下的健康检查报告，才能够依据其结果判断是否核保以及可以投保的理赔金额，其目的也是要在风险可控的状况下做生意。

从这些常见的商业运作准则所展现的避险观念不难理解，企业的经营其实就是一个不断面临挑战和冒险突围的过程，而企业要能够永续经营，需要的正是能够在过程中不断地克服困难及规避风险，然而现今已是万物联网的时代，企业已不再因产业类别而有所差异，几乎所有的产业都无法避免的与无线网络或信息化工具有着密切的链接，而关键重要的生产工具与环境，却充满着不可控的风险因素，作为企业的经营者怎么能够视而不见？又怎么能不积极地管理这些风险呢？因此，CEO 对资安至少应有下列几项策略层级的认识：

遭受网络信息安全威胁不再是政府、金融、能源等等关键基础机构的专利！

近年来已经有大量的半导体、电子及 3C 产品生产、传统制造业、服务业等遭受到攻击和勒索，即便遭到攻击的企业都宣称具有极为完备的资安防护措施，但仍无法幸免于难。

网络信息安全并非必然是一般 IT 人员的专业！

即使是学资讯工程的专业也未必是真的懂“网络信息安全”，在资讯工程的领域如同医学系也有内、外科，妇产科、心脏科…等等不同的专业一样，千万不要再要求原有的 IT 必须兼职做资安的工作了，想象一下：你敢请一位牙医帮你动心血管手术吗？请委由专业、专责的资安人员协助企业做好资安工作。

网络信息安全不是筑一道防火墙就可以高枕无忧！

不要再用购置生财器具的观念来做资安了！因为网络信息安全是一场不断在变化的战争，就像是企业在市场上与竞业不断地相互竞争一样，我们必须不断的提防竞争对手攻进我们的市场抢走客户，企业不可能一成不变，或是购置一套机器生产之后，就可以不必再做任何创新、甚至从此不需再做研发新产品的工作；同样的道理、黑客会不断地透过不同的方式企图渗透进入企业，或是企业内鬼会恶意的外泄公司机密或客户个资，这些都是企业必须面对的网络信息安全挑战，无法用单一手段就能解决的问题，因此，网络信息安全的工作必须是一个长期的企业政策。

网络信息安全必须提升至公司治理的层级！

从企业经营的角度而言，网络信息

数联资安以中国台湾自主资安研发厂商资格参加中国台湾资安馆参展，
推广提供中小企业简易订阅的 3S 资安订阅服务

安全影响的不仅是公司的营运效能，更有可能对企业的重大利益、声誉、持续营运等等产生极大的影响，所以企业不应再将资安视为信息部门的一部分，而应该将层级提升，并由公司领导决策层级制定资安的政策框架，避免基层执行者因权限不足或无法担负如此巨大的责任，而保守以对或是裹足不前，反而致使企业低估网络信息安全风险，或是因缺乏可遵行的政策而徒增内部沟通的流程，导致无法及时有效反应资安相关危机。

网络信息安全真正的挑战是政策的落实！

再怎么昂贵的硬件保护、再强大的软件功能，都抵挡不住一个人为的疏漏，就如同资安业界最常聊到的一个笑话：当发生资安事件的第一动作就是检查老板的计算机，因为唯一的例外与破口最常发生在那里！坦白说，网络信息安全不必然是花大钱才能做好，但舍不得花钱当然不容易做到完善，可是相较于预算的投入规模，对于资安影响更大的是公司高层的态度，因为要做好资安就必须有“不厌其烦”的管控措施，包括：计算机设备存取的限制、相关设备的密码管理、外部联网的控管…等等，当企业从上到下都有正确的观念、能确实遵守应有的规范，企业的网路信息安全一定可以达到一定的安全水平。

CEO 决定了企业的资安健康指数

企业领导人切勿因为不是信息专业背景而无视资安的重要！因为正如大家所预期无线网络的发展将会更加迅速，今日已是 5G 联网爆发成长的世代，应用服务也将从实体的信息系统（OnprivateIT）快速迁移到云端（Cloud），在这些环境与技术的变革过程中，一直没有改变的就是应该要如何确保系统与数据的安全，只是过去缺乏迅速方便的网络环境，所以即使有风险，病毒仍无法快速深入与扩散，企业有足够的时间防御与围堵，但现在的网络环境变得更快、更方便，企业对网络与信息系统的应用越加依赖，所以一旦发生问题将很容易演变成重大灾难。

企业必须随着科技的发展与潮流不断的进步，而作为领导企业的 CEO 更应该及时地掌握趋势的脉动，对企业的未来做出最好的指引，网络信息安全已经成为未来企业经营的重大风险之一，无论企业 CEO 的专业背景为何都不应该再置身事外，应透过建立正确的资安策略思维，并且合理投资企业的资安人才与环境，必能建构一个健全且完善的企业资安防护机制。一个企业的资安是否做得好？是否值得信赖？端看企业 CEO 对于资安的认知程度与态度即可窥知一二，据此，企业的 CEO 应该从自身开始改变，带动企业重视资安的观念，这不仅可以降低企业经营的风险、更是企业社会责任的展现，毕竟资安所涉及的层面也包括公司、客户个资与机敏数据的保护。

我相信多数企业 CEO 并非不重视资安、只是过去多数做信息安全决策时都只着重在技术层面的沟通，而缺乏观念上的厘清与建构，因此我由衷的期望看见中国台湾的企业能重视信息安全，并用正确的观念投资做好资安工作，而 CEO 也会是企业信息安全是否能够成功做好的关键。MFC