问题 1

用于身份验证的三 (3) 个不同因素是什么？对于每个因素，请举例说明。最后，描述需要至少两个因素组合的情况，并简要解释为什么

三个差异因素

1. 一个人知道（Pwd Pin）
2. 一个人拥有（令牌）
3. 一个人是（生物识别指纹，拇指，虹膜）

两个必要因素（ 2 从上面

* 公司卡访问和生物识别来验证身份
* 公司 Pin 和指纹
* 网上银行 Pin 和消息发送到电话

**问题 2**

为身份分配价值时的一个重要要求是该值必须是非描述性的。

解释“非描述性”的含义以及为什么需要这样做。

信用集的任何一部分都不应指示帐户的用途，

例如。administrator) - 没有显示它属于谁

**ceo**

,保护通用 PC 实验室免遭未经授权的进入。

门禁卡、生物识别、Pin（个人身份证号码）

低安全性 - 生物识别、Pin、门禁卡，

\* 需要写什么类型的生物识别

**问题 4**

描述可用于建筑物访问的两种技术控制，并说明您将使用哪一种用于保护通用 PC 实验室免遭未经授权进入所需的低安全性设置。

能够

检测入侵

Recon ev 和 system cond

提供钻机材料并产生

**问题 5**

在开发安全系统时，物理控制通常被忽略，但它们仍然是有效安全解决方案的关键组成部分。描述两种物理预防类型的控制以及两种物理检测类型的控制，并指定需要将两者结合的场景。

物理预防措施

* 十字转门
* 自动路障
* 护柱

物理侦探

* 闭路电视
* 烟雾探测器

场景

闭路电视和生物识别技术（数据中心）

**问题 6**

在开发安全系统时，重要的是要针对现有预防措施失败并因此损害系统完整性的情况进行规划。从安全角度来看，通常考虑用于服务连续性/恢复的两个主要途径是什么？

Access controls fail

If fail, integ comprom

(Backup - offsite storage backups(Offline)

确保服务恢复，测试备份，使备份不会失败（6个月一次或一年一次）

**问题7**

上下文中的完整性原则数据安全性处理数据的正确性，目的是防止组织内部或外部人员的破坏。帮助数据完整性保护的首要措施是什么？

实施访问控制。用户将只有有限的访问权限，这减少了基本雾对受保护数据造成重大损害的可能性。

**问题 8**

解释纠正控制和恢复控制之间的区别。

恢复控制用于从损坏中恢复更严重的情况。

**纠正控制**

示例：

Windows 中的回收站有助于更正意外删除。当一个项目被意外删除时，它会进入回收站，用户仍然可以在特定时间内检索文件。

**恢复控制**

示例：

Chkdsk ，它有助于恢复已被删除的文件。

**CHKDSK**

它不是数据恢复工具，不会恢复丢失或损坏的文件。 CHKDSK 将简单地确保当前磁盘上的信息处于一致和安全的状态。如果文件损坏，CHKDSK 实用程序会尝试分离损坏的文件并将剩余文件另存为 Filenn.chk。这种坏扇区的重组可能会导致进一步的问题。有许多讨论或论坛指出 CHKDSK 修复文件失败并使情况变得更糟！我们能给出的最佳建议是永远不要在启用自动修复选项的情况下运行 CHKDSK。

<http://www.datarecoveryspecialists.co.uk/blog/chkdsk-data-recovery#:~:text=Will%20CHKDSK%20recover%20data%3F,save%20the%20remnants%20as%20Filenn>。

**问题 9**

许多组织开发的安全系统完全专注于物理和技术安全控制。解释为什么这是不够的，并提供安全性如何受到损害的例子。

网络安全有 3 个主要方面：人员、流程、系统

我们也需要 **管理控制** 。

如果被忽视，有经验的攻击者将能够破坏安全设置，因为信息所有权问题得到妥善处理。

因此，攻击者可能不需要闯入更好的保护系统，因为不太可能完全控制对机密信息的访问。

例子 缺乏的 **管理控制**

将电子邮件发送给所有用户，而不仅仅是那些应该有权访问它的用户。

旧硬件的处理不是以安全的方式进行的，硬盘驱动器只是被扔进垃圾箱，攻击者可以从垃圾箱中提取密码或机密记录等关键信息。

**问题 10**

什么是 CERT-Australia？什么是 AusCERT？什么是自闭症？为什么从数据安全的角度来看，了解它们中的每一个都很重要？

**CERT -** 计算机应急响应小组

**CERT Australia** 是国家计算机应急响应小组。 CERT Australia 为澳大利亚关键基础设施和其他国家利益系统的所有者和运营商提供有关网络威胁和漏洞的建议和支持。

**AusCERT** 是一个非营利组织，为网络安全威胁和漏洞提供建议和解决方案。该组织通过会员订阅、年度 AusCERT 会议的与会者和服务合同来支付费用。

CERT 教育人们为可能影响他们所在地区的灾害做好备灾工作，并培训他们掌握基本的灾难应对技能，例如消防安全、轻型搜救、团队组织和灾难医疗操作。了解它们中的每一个可以让我们更好地准备应对网络安全威胁。

**问题 11**

什么是发件人策略框架 (SPF)？解释 SPF 解决的攻击类型。

发件人策略框架 (SPF) 是一种电子邮件身份验证协议，也是用于阻止网络钓鱼攻击的电子邮件网络安全的一部分。它允许您的公司指定允许谁代表您的域发送电子邮件。

这很有用，因为在典型的网络钓鱼攻击中，威胁行为者会欺骗发件人地址，使之看起来像官方企业帐户或受害者可能认识的人。

**目标**

* 电子邮件欺骗
* 网络钓鱼攻击

**如何**

保护出站电子邮件是通过在您的公共 DNS 中配置一条 TXT 记录来实现的，该记录列出了允许从您的邮件域发送电子邮件的服务器。邮件服务器本身没有配置任何内容。

发件人政策框架 (SPF) 电子邮件身份验证方法旨在通过让电子邮件发件人更难隐藏其身份来减少垃圾邮件和欺诈。 SPF 通过提供一个流程来验证谁可以代表您发送电子邮件来检测电子邮件欺骗。