Access Control Practices

* Deny access to systems to undefined users or anonymous accounts.

拒绝未定义的用户或匿名账户对系统的访问。

* Limit and monitor the usage of administrator and other powerful accounts.

限制和监控管理员和其他强大账户的使用。

* Suspend or delay access capability after a specific number of unsuccessful logon attempts

在特定数量的不成功的登录尝试后，暂停或延迟访问能力

* Remove obsolete user accounts as soon as the user leaves the company

一旦用户离开公司，立即删除过时的用户账户

* Suspend inactive accounts after 30 to 60 days.

在30至60天后暂停不活跃账户。

* Enforce strict access criteria.

执行严格的访问标准。

* Enforce the need-to-know and least-privilege practices. (need to know: 只让我们知道应该知道的东西 例如：老师的内容和学生的内容不一样) （least privilege : giving an employee the only enough rights and privilege to carry out what they are supposed to do and nothing more)
* Disable unneeded system features, services and ports.

禁用不需要的系统功能、服务和端口。

* Replace default password settings on accounts.

替换账户上的默认密码设置。

* Limit and monitor global access rules.

限制和监控全局访问规则

* Remove redundant resource rules from accounts and group memberships.

从账户和组成员资格中删除多余的资源规则。

* Remove redundant user IDs, accounts, and role-based accounts from resource access lists.

从资源访问列表中删除多余的用户ID、账户和基于角色的账户。

* Enforce password rotation.

强制执行密码轮换。

* Enforce password requirements (length, contents, lifetime, distribution, storage, and transmission).

执行密码要求（长度、内容、寿命、分发、存储和传输）。

* Audit system and user events and actions, and review reports periodically.

审计系统和用户的事件和行动，并定期审查报告。

* Protect audit logs.

保护审计日志。

**Security controls** 安全控制

* Safeguards to prevent, detect, correct or minimise security risks.

预防、检测、纠正或尽量减少安全风险的保障措施。

* Set of actions for data security

促进数据安全的一套行动

Definition

Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks.

安全控制是一套建议的网络防御行动，提供了具体和可操作的方法来阻止当今最普遍和最危险的攻击。

Advantages

* A principle benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results.

控制措施的一个原则性好处是，它们优先考虑并集中于数量较少的具有高回报结果的行动。

* The Controls are effective because they are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners.

这些控制措施是有效的，因为它们来自于领先的威胁报告中强调的最常见的攻击模式，并在非常广泛的政府和行业从业者社区中得到了审查。

What is it for?

* They were created to answer the question, "what do we need to do to stop known attacks."

它们的创建是为了回答 "我们需要做什么来阻止已知的攻击 "这一问题。

* The key to the continued value is that the Controls are updated based on new attacks that are identified and analysed by groups from Verizon to Symantec so the Controls can stop or mitigate those attacks.

持续价值的关键是，控制措施会根据从Verizon到赛门铁克的团体所识别和分析的新攻击进行更新，以便控制措施能够阻止或减轻这些攻击。

**There are Two ways of categorising Security Controls: 有两种方法可以对安全控制进行分类。**

1. Categorising according to nature of the control 根据控制的性质进行分类

* Administrative Controls 行政控制
* Technical Controls/ Logical Controls 技术控制/逻辑控制
* Physical Controls 物理控制

2. Categorising according to the different phases 阶段 of the control process

* Deterrent 威慑力
* Preventative 预防性的
* Detective 探测
* Corrective 纠正
* Recovery/ Compensatory 恢复性/补偿性

Categorising according to nature of the control

1. **Administrative Controls**

These include the developing and publishing of policies, standards, procedures, and guidelines; risk management; the screening of personnel; conducting security-awareness training; and implementing change control procedures.

这包括制定和发布政策、标准、程序和准则；风险管理；人员筛选；进行安全意识培训；以及实施变更控制程序。

Definition

* Administrative controls refer to policies, procedures, or guidelines that define personnel or business practices in accordance with the organisation's security goals.

行政控制是指根据组织的安全目标确定人员或业务实践的政策、程序或准则。

* Administrative controls are the process of developing and ensuring compliance with policy and procedures.

行政控制是制定和确保遵守政策和程序的过程

* They tend to be things that employees may do, or must always do, or cannot do. 它们往往是员工可能做的事情，或必须一直做的事情，或不能做的事情

Categories of Administrative Controls:

* Policies 政策
* Standards 标准
* Procedures 程序
* Guidelines 准则

Importance of Administrative Controls:

行政控制的重要性：

If overlooked, an experienced attacker will be able to breach the security set up because the issue of information ownership is properly handled.

如果被忽视，一个有经验的攻击者将能够突破安全设置，因为信息所有权问题得到了适当的处理。

Examples:

* Policies (Eg. Business Continuity Plan, Access Control Policy, Disaster Recovery Plan）
* Procedures
* Personnel Controls ( Def: Personnel controlling indicates strengths and weaknesses of the company. Its purpose is to effectively exploit the potential of all employees to achieve the maximum benefit within the organisation. 人事控制表明公司的优势和劣势。其目的是有效地挖掘所有员工的潜力，以实现组织内的最大利益。）
* Supervisory structure 监管结构 (Def: a board of management of which nonmanagerial workers are members, having supervisory powers over some aspects of management decision-making. 由非管理人员担任成员的管理委员会，对管理决策的某些方面拥有监督权。)
* Testing ( Eg. Vulnerability Scanning, Penetration Testing 渗透测试, Security Audit/Review, Risk Assessment , Security Scanning)

1. **Technical Controls (aka Logical Controls)**

These consist of implementing and maintaining access control mechanisms, password and resource management, identification and authentication methods, security devices, and the configuration of the infrastructure. 这些包括实施和维护访问控制机制，密码和资源管理，识别和认证方法，安全设备，以及基础设施的配置。

Definition:

Technical controls are the **hardware** and **software components** that protect a system against cyberattacks.

技术控制是保护系统免受网络攻击的硬件和软件组件。

Firewalls, intrusion detection systems (IDS), encryption, and identification and authentication mechanisms are examples of technical controls.

防火墙、入侵检测系统（IDS）、加密以及识别和认证机制是技术控制的例子。

May refer to：

* identification and authentication methods
* security devices
* configuration of the infrastructure

Importance of Technical controls:

Technical controls perform many critical functions, such as keeping unauthorized individuals from gaining access to a system and detecting when a security violation has occurred.

技术控制发挥了许多关键功能，如防止未经授权的个人进入系统，并在发生安全违规时进行检测。

Examples：

Preventative

* Encryption 加密
* Smart cards 智能卡
* Network authentication 网络认证
* Access control lists (ACLs) 访问控制列表（ACL）。
* File integrity auditing software 文件完整性审计软件
* Patching 打补丁
* IPS (Intrusion Prevention System) 入侵预防系统

Detective

* Security logs
* NIDS (Network Based Intrusion Detection System) 基于网络的入侵检测系统
* HIDS ( Host Based Intrusion Detection System) 基于主机的入侵检测系统

Corrective/Recovery

* IPS (Intrusion Prevention System） 入侵预防系统
* Restore from backups 从备份中恢复
* Patching 修补

1. **Physical Controls 物理控制**

Depending on the organization physical security countermeasures will vary. A government agency such as the Department of Defense may have armed guards at the door of the building. Many organizations are not in the position of breaching national security so armed guards are not a necessity. In many cases a receptionist greets any new visitors and makes the appropriate arrangements for an on-site visit.

根据组织的不同，物理安全对策也会有所不同。像国防部这样的政府机构可能会在大楼的门口配备武装警卫。许多组织并不处于破坏国家安全的地位，因此武装警卫并不是必要的。在许多情况下，接待人员会迎接任何新的来访者，并为现场访问做出适当的安排。

Definition:

These entail controlling individual access into the facility and different departments, locking systems and removing unnecessary floppy or CD-ROM drives, protecting the perimeter of the facility, monitoring for intrusion, and environmental controls.

Importance of Physical controls:

Physical security keeps your employees, facilities, and assets safe from real-world threats. These threats can arise from internal or external intruders that question data security. Physical attacks can cause a safe area to break into or the invasion of a restricted area part.

Examples:

* Automated barriers & bollards 自动屏障和护柱
* Building management systems like Heating, HVAC, lifts/elevators control, etc. 楼宇管理系统，如供暖、HVAC、升降机/电梯控制等
* CCTV- Closed Circuit TV
* Electronic article surveillance - EAS 电子设备监控 - EAS
* Fire detection 火灾探测
* GIS mapping systems GIS制图系统
* Intercom & IP phone 对讲机和IP电话
* Lighting control system 照明控制系统
* Perimeter intrusion detection system 周边入侵检测系统
* Radar based detection & Perimeter surveillance radar 基于雷达的检测& 周边监控雷达
* Security alarm 安全警报
* Video wall
* Power monitoring system 电力监控系统
* Laptop Locks 笔记本电脑锁

Categorising according to the different phases of the control process

* Deterrent: controls to discourage attacks at the first place, deter people from breaching security, e.g warning, banner, logon message, fake CCTV cameras to warn people, security measures on websites to tell people that they are protected

威慑：控制首先阻止攻击，阻止人们破坏安全，例如警告、横幅、登录消息、假闭路电视摄像头警告人们，网站上的安全措施告诉人们他们受到保护

* Preventive: controls that make it hard for attacks to succeed, e.g. firewall (stops unwelcomed traffic), encryption, locked doors

预防性：使攻击难以成功的控制，例如防火墙（阻止不受欢迎的流量）、加密、锁门

* Detective: controls that detect if an attack has occurred, e.g. checksum, intrusion detection system, rotation of duties, security audits, monitors and sensors, motion sensors installed in the buildings to detect intruders, CCTV cameras, sometimes firewall that tells when an attack has been made on the system, intrusion detection systems that monitor the activity on the hosts and computers over the network

侦探性：检测是否发生攻击的控制，例如校验和、入侵检测系统、职责轮换、安全审计、监视器和 sensors，安装在建筑物中以检测入侵者的运动传感器，闭路电视摄像机，有时会告知系统何时受到攻击的防火墙，通过网络监视主机和计算机上的活动的入侵检测系统

* Corrective: corrective aspects of security, controls that reverse the damage, e.g. version control, incident handling procedures, fire extinguishers, undo, recycle bin, DOS attack (ban the IP addresses to stop from jamming the servers), Fire extinguishers (putting out fires when it has happened), Incident handling procedures (tells employees what to do when an incident happens)

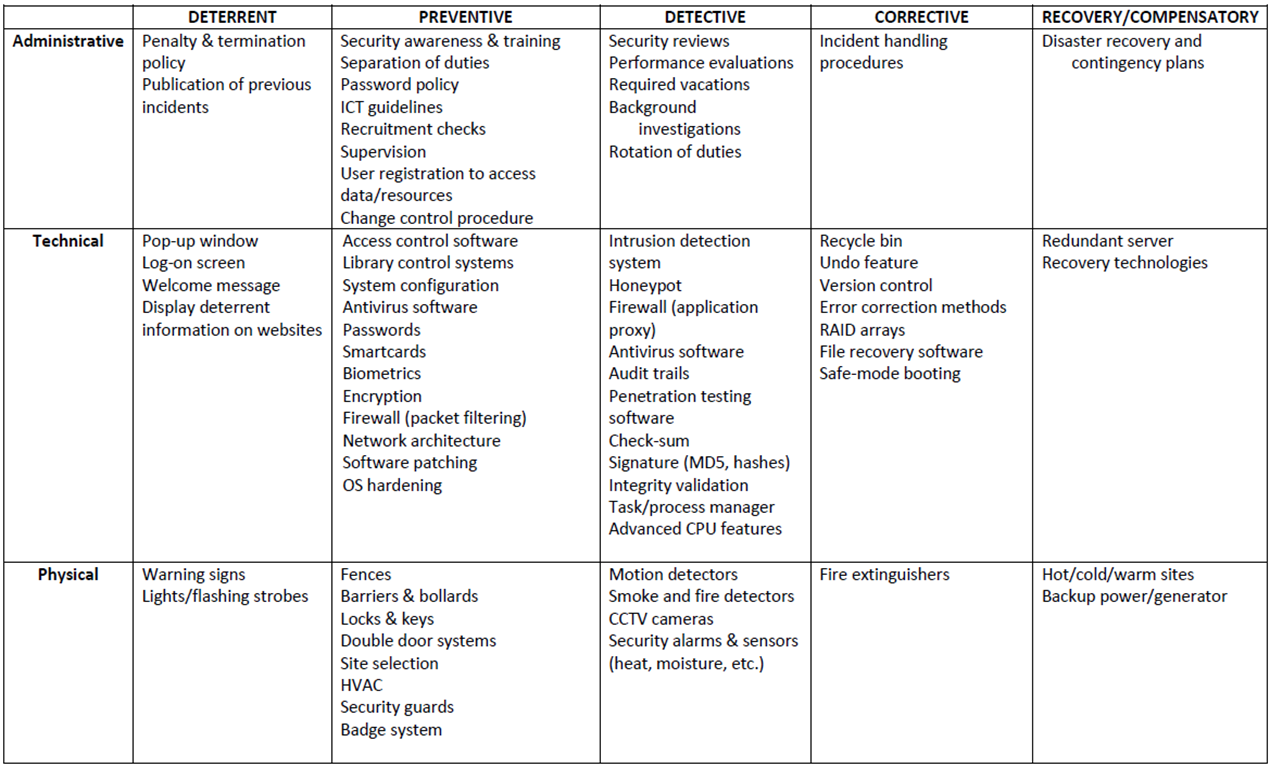
纠正：安全的纠正方面，扭转损害的控制，例如版本控制、事件处理程序、灭火器、撤销、回收站、DOS攻击（禁止IP地址以阻止干扰服务器）、灭火器（发生火灾时灭火）、事件处理程序（告诉员工发生事件时该怎么做）

* Recovery: controls that bring the system back after a major disaster like earthquakes or tsunamis , e.g. disaster recovery plan, hot/cold/warm sites, backup power,

恢复：在地震或海啸等重大灾难发生后使系统恢复的控制措施，例如，灾难恢复计划、热/冷/热站点、备用电源。

A general example:

Speeding (have fines and punishment, and preventive controls like speed bumps, detection – security cameras)



Real-life Example

**Speeding:** deterrent - having fines and punishment 罚款，惩罚, preventive controls like speed bumps减速带, detection security cameras 超速监控, corrective - enforcement of fines and punishments 执法, recovery - none

**Fire Hazards:** *deterrent* - flyers or advertisements how to prevent fire hazards from happening, *preventive* - making sure no open stoves are left unattended, power sockets are turned off when not in use 确保没有开放的炉子无人看管，不使用时关闭电源插座, *detective* - smoke detectors 烟雾探测器, cctv at home 家用监控 *corrective -* fire extinguishers 灭火器 , *recovery -* insurance and funds kept for a rainy day 保险和存款

**Commonly Used Security Methods 常用的安全方法**

To address the key requirements of the AIC triad, one can employ a number of commonly used security methods:

* Least privilege
* Defense-in-depth
* Minimization
* Keep things simple
* Compartmentalization
* Use choke points
* Fail securely/safely
* Leverage unpredictability
* Separation of duties

**Least Privilege**

**States that:** do not provide more privileges than are required. This applies to both users and applications. 不要提供超过所需的权限。这同时适用于用户和应用程序。

* Example: No administrative rights to guests accounts, unidentified applications should not be able to have the power to change the system file etc.) 例如。对客人的账户没有管理权限，不明身份的应用程序不应该有改变系统文件的权力等)
* This principle applies not only to privileges of users and applications on a computer system, but also to other noninformation systems privileges of an organization’s staff.

这一原则不仅适用于计算机系统上的用户和应用程序的特权，而且也适用于一个组织的工作人员的其他非信息系统的特权

* The principle of least privilege is a preventive control, because it reduces the number of privileges that may be potentially abused and therefore limits the potential damage.

最小特权原则是一种预防性控制，因为它减少了可能被潜在滥用的特权的数量，因此限制了潜在的损害

* Some examples of application of this principle include the following:
* Giving users only read access to shared files if that’s what they need, and making sure write access is disabled

如果用户需要的话，只给他们阅读共享文件的权限，并确保禁止写入权限

* Not allowing help desk staff to create or delete user accounts if all that they may have to do is to reset a password

如果服务台工作人员只需要重设密码，就不允许他们创建或删除用户账户

* Not allowing software developers to move software from development servers to production servers

不允许软件开发人员将软件从开发服务器转移到生产服务器上

* Privilege : The ability to access data to run processes and applications

特权：访问数据以运行进程和应用程序的能力

* Product: keep system more stable by giving less privilege to untrustworthy users

产品：通过给予不值得信任的用户较少的特权，使系统更加稳定。

**Advantages:**

* Minimizes the attack surface, diminishing avenues a malicious actor can use to access sensitive data or carry out an attack by protecting superuser and administrator privileges.
* Reduces malware propagation by not allowing users to install unauthorized applications. The principle of least privilege also stops lateral network movement that can launch an attack against other connected devices by limiting malware to the entry point.
* Improves operational performance with reductions in system downtime that might otherwise occur as a result of a breach, malware spread or incompatibility issues between applications.
* Safeguards against human error that can happen through mistake, malice or negligence.

**Disadvantages:**

The two big problems with least privilege are minimal access and expiration of access.最小访问权限和访问权限过期。

* Minimal access

When assigning or providing access, in many cases an admin is not sure whether or not someone needs access. In the past, if an admin was not sure if a user needed access, the default rule was to go ahead and provide the user with access. While this potentially minimized support desk calls and user frustration, it introduced considerable risk.

在分配或提供访问权限时，在许多情况下，管理员不确定是否有人需要访问权限。过去，如果管理员不确定用户是否需要访问权限，默认规则是继续并为用户提供访问权限。虽然这可能会最大限度地减少支持台呼叫和用户挫败感，但它带来了相当大的风险。

If you provide additional access and it is not needed, no one ever notifies the help desk. Ultimately, providing access to a user beyond what he or she needs to perform his/her role leads to a massively increased attack surface that leaves organizations wide open to damage from hackers and insiders.

如果您提供了额外的访问权限并且不需要，没有人会通知服务台。最终，向用户提供超出他或她执行其角色所需的访问权限会导致攻击面大幅增加，从而使组织对黑客和内部人员的破坏敞开大门。

* Expiration of access

The second big problem with data access is expiration. In most organizations, once access is provided to a piece of information, it is never removed.Over the course of employment at an organization, as a user’s role and responsibilities change (or the technologies they need to access grow), more access is granted to the user. However, rarely is the previous access, when no longer relevant to a user’s role, removed.

数据访问的第二大问题是过期。在大多数组织中，一旦提供对一条信息的访问权限，就永远不会删除。在组织的就业过程中，随着用户角色和职责的变化（或他们需要访问的技术的增长），将授予更多访问权限给用户。但是，以前的访问权限很少会在不再与用户的角色相关时被删除。

**Importance:**

* The principle of least privilege is an important information security construct for organizations operating in today’s hybrid workplace to help protect them from cyberattacks and the financial, data and reputational losses that follow when ransomware, malware and other malicious threats impact their operations.

对于在当今混合工作场所中运营的组织而言，最小特权原则是一个重要的信息安全结构，有助于保护他们免受网络攻击以及勒索软件、恶意软件和其他恶意威胁影响其运营时随之而来的财务、数据和声誉损失。

* The principle of least privilege strikes a balance between usability and security to safeguard critical data and systems by minimizing the attack surface, limiting cyberattacks, enhancing operational performance and reducing the impact of human error.

最小特权原则通过最小化攻击面、限制网络攻击、提高操作性能和减少人为错误的影响，在可用性和安全性之间取得平衡，以保护关键数据和系统。

**Defense in Depth** (multiple types of security controls in different layers)

深度防御（不同层次的多种类型的安全控制）

* The principle of defense in depth is about having more than one layer or type of defense.

深度防御的原则是指拥有一个以上的防御层或类型。

* **Advantage**: The reasoning behind this principle is that any one layer or type of defense may be breached, no matter how strong and reliable you think it is, but two or more layers are much more difficult to breach.

这一原则背后的理由是，任何一层或一种类型的防御都可能被攻破，无论你认为它多么强大和可靠，但两层或更多的防御则更难攻破。

* **Disadvantages:** It is usually more costly and time consuming to implement many layers of security.
* Defense in depth works best when you combine two or more different types of defense mechanisms—
* such as using a firewall between the Internet and your LAN, plus the IP Security Architecture (IPSEC) to encrypt all sensitive traffic on the LAN. In this scenario, even if your firewall is compromised, the attackers still have to break IP Security to get to your data flowing across the LAN.

例如，在互联网和你的局域网之间使用防火墙，加上IP安全架构（IPSEC）来加密局域网上的所有敏感流量。在这种情况下，即使你的防火墙被破坏，攻击者仍然必须打破IP安全架构，以获得你在局域网上流动的数据。

Eg.

1st layer – Deterrent control (easy to implement, use it to warn hackers to not attack, breaching policies may not be legal)

第一层——威慑控制（容易实现，用来警告黑客不要攻击，违反政策可能不合法）

2nd layer – Preventive control (Firewall installed on server that monitors all the traffic gg btw the internet and internal network and intercept any suspicious activities)

第二层 - 预防控制（防火墙安装在服务器上，监控所有流量 gg btw 互联网和内部网络并拦截任何可疑活动）

3rd layer – Detective layer (Network monitoring tools like intrusion detection systems that will alert ppl on any attacks being made on the system)

第 3 层 - 侦探层（网络监控工具，如入侵检测系统，会在系统受到的任何攻击时提醒人们）

4th layer – Corrective layer (software installed like antivirus that could get rid of virus that the computer has been infected)

第四层——纠正层（安装杀毒软件等软件，可以清除计算机被感染的病毒）

5th layer – Recovery layer (Data backup, another image of the system software for recovery in the event that the system breaks)

第五层——恢复层（数据备份，系统软件崩溃时恢复的另一个镜像）

Generally, different types of controls should be used together:

* first, preventive controls should be in place to try and prevent security incidents from happening at all;
* second, detective controls are necessary so that you can know whether preventive controls are working or have failed;
* and third, corrective controls are needed to help you respond effectively to security incidents and contain damage.
* However, the defense in depth principle does not mean that you should indiscriminately不分青红皂白地 apply all the controls and security measures you can get your hands on: balance has to be found between security provided by the defense in depth approach and the financial, human, and organizational resources you are willing to expend following it. This balance is addressed by the cost-benefit analysis.

必须在纵深防御方法提供的安全性和您愿意为此花费的财务、人力和组织资源之间找到平衡。这种平衡通过成本效益分析解决。

**Minimisation**

***Purpose/Definition/Principle/****States that:*  the system should not run any applications that are not strictly required to complete its assigned task

规定：系统不应运行任何非严格要求的应用程序，以完成其指定的任务

* The minimization principle is the cousin of the least privilege principle and mostly applies to system configuration.

最小化原则是最小特权原则的表哥，主要适用于系统配置

* For **example**, a computer whose only function is to serve as an e-mail server should have only e-mail server software installed and enabled. All other services and protocols should either be disabled or not installed at all to eliminate any possibility of compromise or misuse.

例如，一台唯一功能是作为电子邮件服务器的计算机应该只安装和启用电子邮件服务器软件。所有其他服务和协议应被禁用或根本不安装，以消除任何妥协或误用的可能性。

* **Advantages/Importance**:
* Adherence to the minimization principle not only increases security but usually also improves performance, saves storage space, and is a good system administration practice in general.
* Minimisation is also one of the cheapest methods as no additional costs are needed and it can help an organisation save cost on storage as well.
* Data minimization can help you reduce data theft by decreasing your data footprint that requires security. The principle also allows you to limit the number of records that may be affected in case of a data breach, thereby protecting your business against costly fines.

优点。坚持最小化原则不仅可以提高安全性，而且通常还可以提高性能，节省存储空间，一般来说是一种良好的系统管理实践

**Keep Things Simple**

Definition/ Principle： a security system should be kept simple as any complexity introduced leads to insecurity in the overall system

安全系统应保持简单，因为引入的任何复杂性都会导致整个系统的不安全。

* Complexity is the worst enemy of security. Complex systems are inherently more insecure because they are difficult to design, implement, test, and secure.
* The more complex a system, the less assurance we may have that it will function as expected.

一个系统越复杂，我们就越不能保证它能按预期运行

* Although complexity of information systems and processes is bound to increase with our increasing expectations of functionality, we should be very careful to draw a line between avoidable and unavoidable complexity and not sacrifice security for bells and whistles, only to regret it later.

尽管随着我们对功能的期望值越来越高，信息系统和流程的复杂性必然会增加，但我们应该非常小心地在可避免的和不可避免的复杂性之间划出一条界限，不要为了铃声和口哨而牺牲了安全，事后才后悔

* When you have to choose between a complex system that does much and a simple system that does a bit less but enough, choose the simple one.

**Compartmentalisation区划化**

to prevent the compromise of the entire system, use a compartment approach to the system design and implementation

为防止整个系统受到损害，使用隔间方法进行系统设计和实施

* Compartmentalization, or the use of compartments (also known as zones, jails, sandboxes, and virtual areas), is a principle that limits the damage and protects other compartments when software in one compartment is malfunctioning or compromised.

划分或使用隔间（也称为区域、监狱、沙箱和虚拟区域）是一种原则，当一个隔间中的软件出现故障或受到损害时，它可以限制损害并保护其他隔间。

* Real life example: It can be best compared to compartments on ships and submarines, where a disaster in one compartment does not necessarily mean that the entire ship or submarine is lost.

现实生活中的例子：最好将它比作轮船和潜艇上的舱室，其中一个舱室发生灾难并不一定意味着整艘船或潜艇都损失殆尽。

* **Definition**: Compartmentalization in the information security context means that applications run in different compartments are isolated from each other. In such a setup, the compromise of web server software, for example, does not take down or affect e-mail server software running on the same system but in a separate compartment.
* **Advantages/Importance:** In information security, compartmentalization is equally about spreading the risk so if there’s any impact (breach) we’ve limited the damage to our personal information and the harm and recovery effort are far less.

**Use Choke Points**

**Purpose:** the traffic can be easier to analyse and control by using choke points

Security is very much about control, and control is so much more effective and efficient when you know all ways in and out of your systems or networks.

**Definition:** Choke points are logical “narrow channels” that can be easily monitored and controlled.

**Example:** An example of a choke point is a firewall—unless traffic can travel only via the firewall, the firewall’s utility is reduced to zero. Consider the example of controlled entrances to buildings or facilities of high importance, such as perimeter fencing and guard posts.

**Importance:** Enforcing choke points increases efficiency.

Attackers typically must go through a series of steps to steal assets. They will often breach defenses, move laterally, escalate privileges, evade detection, then exfiltrate data.

Mapping and prioritizing the choke points that attackers move though when launching attacks is a key approach for ensuring that critical assets stay safe. This strategy can also solve resource constraints — an important advantage for perennially understaffed/under-provisioned IT departments.

**Advantages:** The greatest advantage of the Choke-Point architecture is its single point of installation. This provides simple installation and reduced IT management. In the case of a Web Proxy Server, access performance may be enhanced due to the caching nature of the proxy.

**Disadvantages:** There are, however, a number of disadvantages to this architecture. The benefits of having a single point of installation also create a potential single point of failure that must be addressed with redundancy. Since the web filtering and reporting functionality in a Choke-Point environment requires all Web access to occur through a single point, the workstations in the managed environment must be configured to direct Web access to the Choke-Point. It is therefore possible for a user to change their configuration or use alternate means to access the Web. This could include a readily available WiFi connection or a portable Internet access device. In addition, monitoring and filtering remote or mobile users that are not in the managed environment requires the remote workstations to be directed back into the Choke-Point – a highly inefficient means to manage traffic.

**Conclusion from advantages and disadvantages:** Although somewhat offset by its caching capabilities, Choke-Point installations create a bottleneck to Internet content which, depending on traffic dynamics, may actually cause performance to suffer. In general, with respect to filtering, Choke-Point architectures are used primarily for Web content and typically do not address other Internet communication protocols such as content exposed in email, chat, IM and dark web postings.

Not cost effective as one would need to hire people and funds might be needed to install Choke-points.

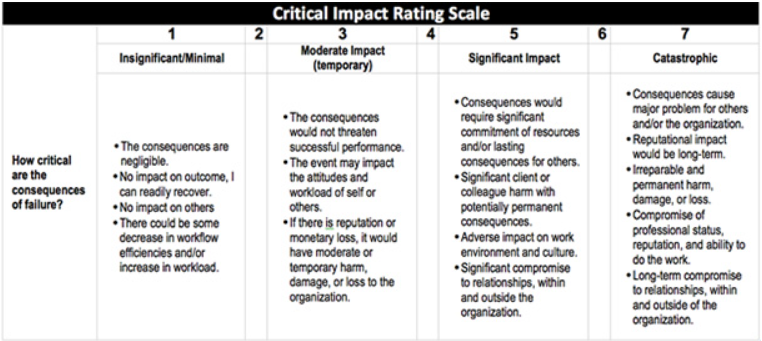
**Fail Securely**

**Definition:** Failing securely means that if a security measure or control has failed for whatever reason, the system is not rendered to an insecure state.

**Principle:** Whenever access, privileges, or some security-related attribute is not explicitly granted, it should be denied.

**Example:** For example, when a firewall fails, it should default to a “deny all” rule, not a “permit all.” However, fail securely does not mean “close everything” in all cases; if we are talking about a computer-controlled building access control system, for example, in case of a fire the system should default to “open doors” if humans are trapped in the building. In this case, human life takes priority over the risk of unauthorized access, which may be dealt with using some other form of control that does not endanger the lives of people during emergency situations.

**Advantages/Importance:** Fail securely is especially important for systems that are accessible to everyone as the traffic flow of such systems would be high, leading to an increase in probability of error or malicious attacks. Failing securely gives operators more time to figure out what went wrong and prevent any undetectable damage.



**Disadvantage:** Fail securely should not be used for systems where the impact of failure is significant or catastrophic. The consequences of failure, no matter how secure, could cause other major and significant damage such as reputational impact or adverse impact on work environment and culture for some organisations. Thus an organisation should weigh their impacts on the consequences of failure before using the Fail Securely method.

May not be the most expensive option, but is not cheap either because of the cost of such software and human resources to detect errors whenever fail securely happens.

**Secure the Weakest Link**

Many information security principles and approaches may sound like little more than common sense. Although that may well be the case, it doesn’t help us much, because very often we still fail to act with common sense.

**Definition/Principle:** Securing the weakest means to spend your security budget securing the biggest problems and the largest vulnerabilities.

**Advantages/Importance:** Instead of securing the weakest link, whatever it may be, resources are spent on reinforcing already adequate defences. The weakest link is the one most likely to be compromised by a hacker. An organisation's security model should not fall apart just because a part of the business, or a business partner, has weak security. Therefore securing the weakest link is important to decrease the chances of hackers exploiting the flaws of an organisation.

**Examples:** For example, there are technological solutions already employed to protect the system but no training on how to handle attachments in email messages. Securing the weakest link is the training of employees to handle attachment in email messages.

**Real life examples:** Addressing the weakest link means you avoid a strategy similar to erecting a gate and expecting an attacker to run straight for it while there are no walls around the gate to limit their access. With a focus on the weakest link, you expend your time and energy on the risks that matter most.

**Disadvantages:** Should be paired with other methods as well as may not work as well alone.

**Leverage Unpredictability**

**Definition/Principle:** Do not provide any information about the system's security setup - users and clients can know that a system is in place but they do not need any specific details

**Example:** Don’t publicise the specifics of their armaments, exact locations, or numbers of armed forces, you should not publicize the details of your security measures and defenses.

**FYI:**This principle should not be seen as contradicting deterrent security controls—controls that basically notify everyone that security mechanisms are in place and that violations will be resisted, detected, and acted upon. The important difference here is that deterrent controls don’t provide details of the defenses but merely announce their existence so as to deter potential attackers without giving them detailed information that later may be used against the defenders.

**Examples:** In practical terms, this means you can, for example, announce that you are using a firewall that, in particular, logs all traffic to and from your network, and these logs are reviewed by the organisation—there is no need to disclose the type, vendor, or version number of the firewall; where it is located; how often logs are reviewed; and whether any backup firewalls or network intrusion detection systems are in place.

**Importance:** Providing excessive information about a system’s security set up can lead to key information being lost or stolen, create a poor experience for customers and reputational harm.

**Segregation of Duties**

**Purpose/Definition:** The purpose of the segregation (or separation) of duties is to avoid the possibility of a single person being responsible for different functions within an organisation, which when combined may result in a security violation that may go undetected. Segregation of duties can prevent or discourage security violations and should be practised when possible.

**Principle:** Although the actual job titles and organizational hierarchies may differ greatly, the idea behind the principle of separation of duties stays the same: no single person should be able to violate security and get away with it. Rotation of duties is a similar control that is intended to detect abuse of privileges or fraud and is a practice to help your organization avoid becoming overly dependent on a single member of the staff. By rotating staff, the organization has more chances of discovering violations or fraud.

**Most Cost Effective Method**

"Keep things simple" would be the one that would be the cheapest and easiest to implement as its aim is to have less complex solutions and reduce attack surface area and potential vulnerabilities. This can be achieved by reducing the number of components, protocols and systems in a network and reducing the amount of customization. Having a simple design makes it easier to secure, monitor, and maintain.