VIVID ADAPT

Essential Security Controls

WHAT ARE VIVID ADAPT'S 'ESSENTIAL SECURITY CONTROLS'

Cybercrime is constantly evolving and remains the largest threat to organisations across the globe. Cyberattacks are becoming both more numerous and more sophisticated with nearly half targeting organisation with less than 100 employees. The financial and operational damage they cause is rapidly increasing. This is driving the security conversation high on the agenda of boards regardless of size, market, or location.

There is no single strategy that is guaranteed to prevent cyber-attacks, and all organisations implement a series of effective precautions to protect themselves. There are several security frameworks in use around the world of many of which have common components, including, NCSC Top 10 (UK) & NIST (US), however they are designed for 'security and technical staff' to protect a 'large organisation' and don't always translate to the operational or financial needs of small or mid-sized business.

VIVID ADAPT'S ESSENTIAL SECURITY FRAMEWORK

Vivid Adapt's Essential Security Framework (ESC) looks to deliver an approach that streamlines cyber-security compliance that seamlessly integrates into your current IT strategy without requiring extensive re-engineering or heavy investment.

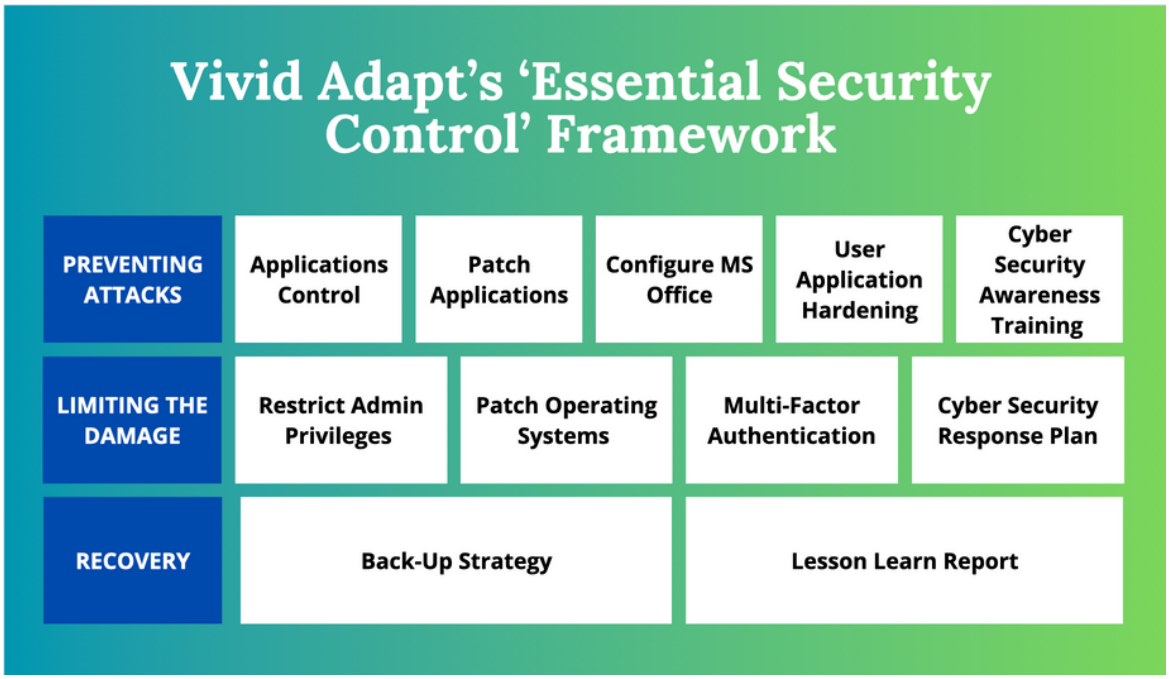
The ESC looks at what a good cyber defence looks like and identifies and organises the different technologies and policies needed into three key risk mitigation layers. These layers combine to ensure holistic protection for any organisation.

The ESC comprises of the following layers:

These three layers need to be in balance to effectively manage the risk and a weakness in one area impacts the total protection across the organisation. For example, an organisation with a strong posture in preventing direct attacks is weakened, if, once the perimeter is penetration by an attack exploiting a lack of user awareness doesn't have the controls in place to limit the spread of the damage across the organisation and wider supply chain. In other words, the chain is only as strong as its weakest link.

The ESC looks at all these areas together to balance the security posture and then can be used a predictive tool to understand the type of attack any organisation is likely to be protected from and vulnerable to, and provide leadership with an objective view if they have the appropriate level of protection in place based on their risk appetite.

The ESC comprises of the following control areas:

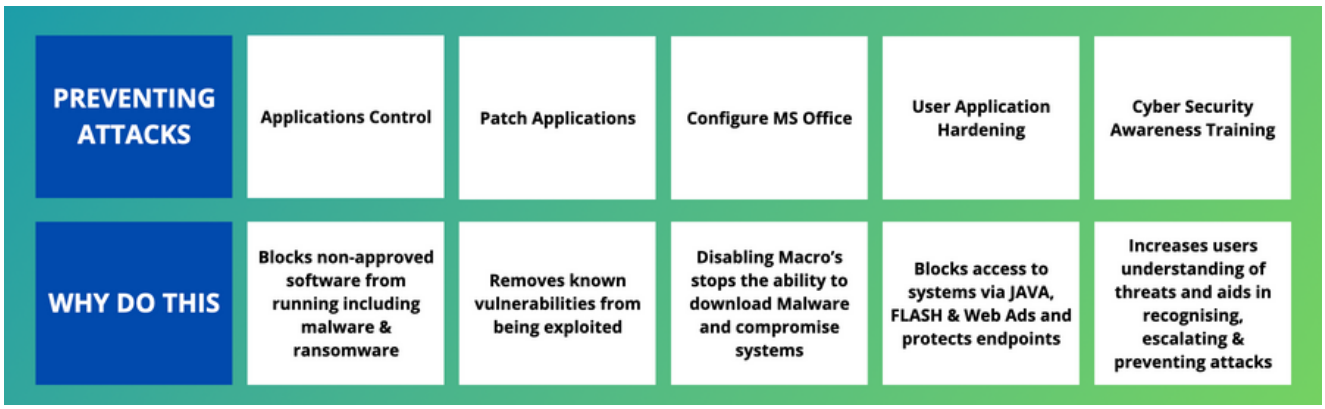


WHAT DOES THE ESC FRAMEWORK COVER?

A level of protection is needed to ensure an organisation can reduce their overall risk and limit the number of attacks, by firstly limiting the threat surface an organisation has and secondly by limiting the ability of malware running in the environment, and finally ensuring a swift and safe return to normal business operations.

At a strategic level, the ESC enables a business to use a 'technical & policy checklist' to understand just how well they are protected, what they are protected against, how much damage different types of attack could cause, and how quickly normal business function can be restored. The more mature each layer is the smaller the threat surface and the greater control you have over limiting malware from running.

PREVENTING ATTACKS



Application Control

This means that only software that you have approved is allowed to run can run within your environment and all non-approved software is blocked. This helps stop threat payloads from gaining access to your systems and prevents malware and ransomware from executing on that system.

Patch Applications

Companies release patches to close security gaps and improve performance. If patching isn't up to date, adversaries will use these publicised and well-known security vulnerabilities to target computers and gain access to systems. Most vulnerabilities found on an endpoint are going to be in the software running on the system and new vulnerabilities are identified regularly.

Microsoft Macro's

Disabled untrusted Microsoft Office macros Microsoft Office applications can use software known as "macros" to automate routine tasks. Macros are increasingly used to enable the download of malware, compromising a system through legitimate functionality rather than a known software vulnerability. Adversaries can then access sensitive information.

Application Hardening

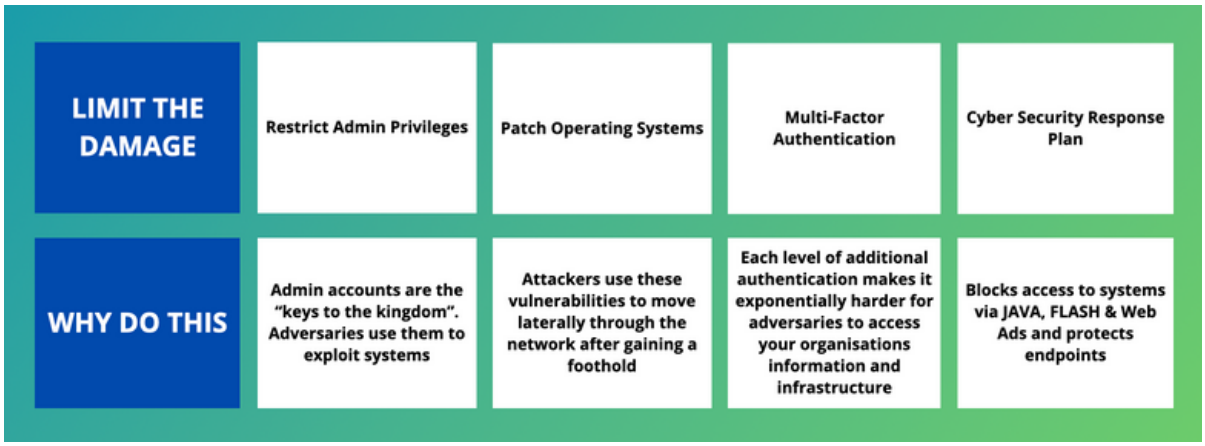
Attackers pick popular apps that are likely to exist in most environments. Apps such as Flash and Java have long been popular ways to deliver malware. User-targeted vulnerabilities are the fastest way to gain a foothold in an organisation. Updating these applications is critical; but where they are not needed, remove or block them.

Cyber Security Awareness Training

Cyber awareness refers to the level of awareness and understanding end users have about cybersecurity best practices and the cyber threats that their networks or organizations face every day. As the volume of cyber threats becomes more rampant and new threats come into focus, what remains consistent is that human error and sophisticated impersonation attacks are behind 90%+ of cyber breaches.

LIMIT THE EXTENT OF INCIDENTS

The ESC provides protection within the current IT environment to manage and reduce the impact of any successful attack. Each element prevents access to key areas of your IT environment and creates firebreaks to ensure attacks do not spread into key data sources. The Response plan manages the critical first stages of an attack and ensures a co-ordinated response is delivered quickly and effectively.



Restrict Administrative Privileges

Admin accounts are the "keys to the kingdom". Adversaries use them for full access to information and systems. There are many vulnerabilities that, if exploited, give the attacker permissions equal to the current user. Some companies can enforce a total lockdown of permissions, but generally, users require some ability that leads to granting them admin privileges.

Patch Operating Systems

Adversaries will use known security vulnerabilities to target Mobiles and Desktops. Most vulnerabilities found on an endpoint are going to be in the software running on the system, and new vulnerabilities are identified regularly. The biggest difference between a typical OS vulnerability and a Software vulnerability is that an OS vulnerability will often be exploitable without involving a user.

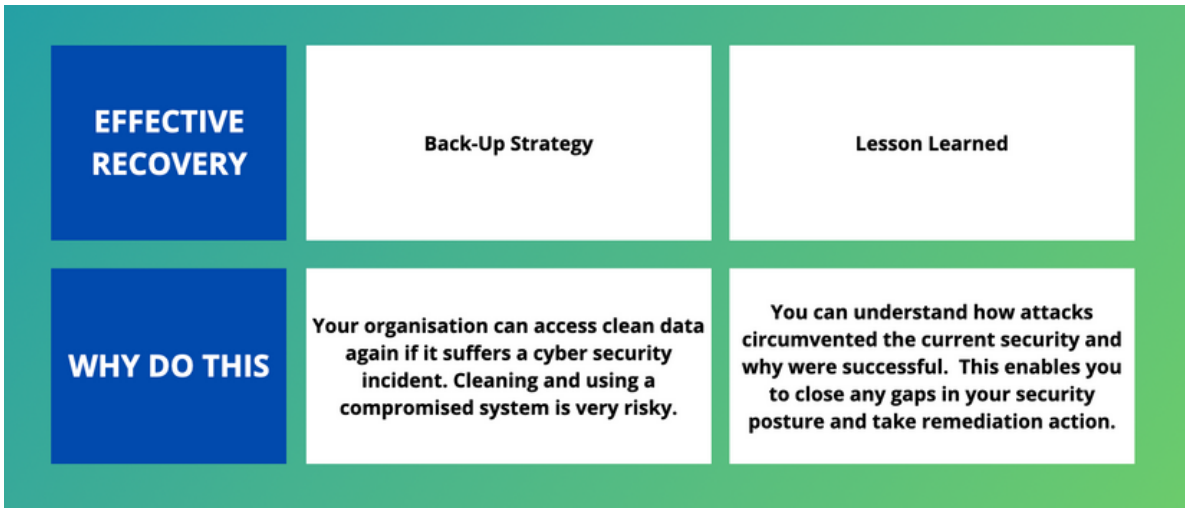
Multi-Factor Authentication

More than half of all malicious cyber incidents involve compromised or stolen credentials. One of the best ways to start building a strategy against credential and access-based threats is by leveraging a modern MFA solution. Many organisations have a level of Single Sign-On and/or basic MFA to validate their users, but the method of setup and validation is typically reliant on passwords and the human end user.

Cyber Security Response Plan

The response plan ensure that the business knows what is needs to be done in an attack, who is responsible for what and what actions need to be undertaken to protect the business, limit any potential damage and recovery quickly. The plan ensures the time taken to respond is limited and the correct actions are taken quickly.

EFFECTIVE RECOVERY



The ESC enables a business to restore normal business function from a clean dataset and mitigate the risk of ransomware.

Back Up Strategies

The fastest way to recover from a malware incident, especially ransomware, is to re-provision the system and restore access to user data. Reimaging and restoring a system to a known good state and then restoring the data is recommended. In the case of ransomware, it's critical for remediation, as paying the ransom is not recommended and not guaranteed to recover the system.

Lesson Learn Report

A lessons learned Report is a collaborative feedback session in which you document what happened and the successes and missteps of a cyber-attacks. The report identifies where the attack originated from, how the cyber penetrated the security perimeter and effective the response was in restoring business functions. The report will provide recommendations to prevent further attacks and limited damage.

THE ESC ASSESSMENT

The ESC assessment provides an analysis of the current security posture and evaluates how effective it is in protecting your business against the most common and dangerous cyber-attacks. The assessment presents the information in a simple way to enable technical and non-technical teams to understand and visualise your current IT security maturity, and objectively establish business and technical goals to mitigate the risk of data breaches, limit the damaged caused, and recover from an attack.

The Essential Security Controls Assessment is delivered as a standalone ‘snap-shot’ that provides an immediate understanding of your current security posture, the risk you are carrying, and any GAPs you have or as delivered regularly as part of a structured security policy to maintain high levels of protection as the threats continue to change.

Based on a one-day workshop, run by the technical and business leaders, Vivid Adapt will categorise each control into one of four categories that relate to the risk an organisation faces related to increased levels of cybercriminals resources and tradecraft.

Level 0 – Evidence of significant weaknesses in the overall cyber security posture and exposure to a high risk of a successful attack.

Level 1 – Evidence to support an organisation will hold its own against non-committed attacks using basic and unsophisticated tradecraft and tools.

Level 2 – Evidence that the organisation can withstand most attacks using readily available tradecraft and tools from a committed attack.

Level 3 – Evidence the organisation can mitigate attacks from highly committed threats using sophisticated tradecraft and techniques.

By the end of the assessment, you will have an outside view of your current security posture, what you are protected against and what you are vulnerable to, how much damage an attack would cause, and how quickly you can recover normal business operations. It enables any business to select the level of cyber security and threat mitigation they deploy based on their risk appetite and make investment decisions accordingly.

ABOUT VIVID ADAPT

Vivid Adapt is a Pan European IT Consultancy, Managed Security & Service Provider based out of Cambridge, UK, with 20 years of experience in supporting businesses achieve their business goals, reduce their operational risk and enable their users to do their jobs.

We have created a unique way of working with our customers that enables them to work smoothly, effectively, and securely. We admit that it is not easy to keep the balance, but at Vivid Adapt, we are a type of different managed service provider. We understand that supporting your business isn't just about the 'technical'. It takes a combination of management consultancy, service maturity, and technical excellence to get it right, with each customer having a different balance to achieve success.

So, we look deeper into your business beyond IT support, lines and minutes, and hardware to create valuable solutions that support your business strategy, manage your risks, and transform your IT services into measurable and controllable tools.

Our approach is based on generating trust across all our engagements with no long contracts and easy exits for our customers. This ensures we keep our customers' visions for service at the heart of our delivery and perform at the highest level of technical expertise and service excellence.

With offices across Europe, we have access to a large pool of experts in End-User, Public, Hybrid, and Private Cloud technologies as well as on-premises environments and support critical environments like they are our own.

GET IN TOUCH

Vivid Adapt is a team of IT and Security experts passionate about supporting businesses and delivering IT that makes a difference. Our mission is to bring technical expertise and service excellence to everyone.

VIVID ADAPT

St John's Innovation Centre,
Cambridge, United Kingdom,
CB4 0WS

www.vividadapt.com