Time Boundary Model

A method from op1digital, turning strategic plans into real-world results since 2016.

Time Boundary	Focus
Before purchase	Threat Modeling risks; awareness controls
Before device power-on	Supply Chain risks; device acquisition controls
Before networking	Physical Security risks; locking controls
Before loading data or apps	Network Security risks; network setting controls
Before device use by an end user	Application Security risks; updates and settings
Before leaving physical control	Latent Data risks; lifecycle management controls
Before too much time passes	Compliance risks; audit controls

This model covers the complete device lifecycle, cradle to grave, considering each change in the threat landscape. The model can be adapted for different devices, environments, and landscapes.

To avoid waste from unnecessary cost and burden without delivering value, controls should be both right-sized and right-timed.

Control right-sizing is extensively addressed in vendor guidance but the timing of control implementation is almost entirely absent from the literature. While many vendors document available security features, they do not provide detail on the optimal time for implementation.

Time Boundary Model (TBM) provides a framework enabling controls to be implemented before exposure to the threats they are designed to mitigate.

Implementation Steps

1. Identify user needs (function, accessibility, usability)
2. Identify relevant threats and control needs using a user-centered threat framework, such as Objective Threat Model (OTM) from op1digital (Appendix A)
3. Align control implementation to changes in threat exposure (Appendix B)

Small and Large Adopters

Right-timing of controls allows for risk reduction even by individual users and small organizations who do not employ Mobile Device Management (MDM) solutions or configuration tools such as Apple Configurator.

When adopted by large organizations, TBM enables verifiable documentation of risk mitigation and facilitates rapid assessment of potential impacts from exposure to emerging threats.

About the Technique

TBM is a systematic and MECE (mutually exclusive, comprehensively exhaustive) approach to control implementation for maximum risk reduction. It can be used with desktops, laptops, mobile phones, and tablets from any vendor. Human training, LLM and implementation materials are available.

Time Boundary Model
Appendix A

Sample Threat Model

Security controls should be implemented in consideration of your needs. A threat model is a structured approach to identifying and responding to risks. Your threat model should align with your specific situation, personal needs, and the way your device will be used. This sample has been formed with Objective Threat Model (OTM) by op1digital.

The target of this threat model is an individual mobile device user. These seven risks form our sample threat model. By reading about the threats, you can understand what threats this set of controls may help to counter. If you see blind spots or have unique needs, you can extend or adjust this threat model and the controls to meet those needs.

A. **Increased Overhead:** As an individual user trying to implement security, you will have increased overhead as compared to users at a big company supported by a large security team. You will need to do your own reading to understand device security features and implement those features yourself. Reading this document will help you understand both the threat model and the security controls that can help respond to those threats.

B. **Device Dependency:** Many users are dependent on their phone to access important data and use applications to get work done. Since we are placing trust in the phone, we should make sure that trust is well-founded. We will consider ways to make sure our phone is trustworthy when acquired.

C. **Vessel or Vehicle for Attack:** We want to make sure our phone is not tampered with by anyone, so nobody can modify or damage our phone and so nobody can use our phone to attack other devices on the network. We can protect our phone so only we can unlock it, and by using security features that protect the phone from unauthorized changes.

D. **Manipulation:** Many types of scams can reach us through a mobile device, whether by SMS text message, phone call, email, or through an application. Network security choices can limit how we are reached, and improve the likelihood that we are communicating with the expected servers over the Internet.

E. **Reputation Attack:** Your reputation can be at risk if someone is able to impersonate you or expose your personal data. Security updates, good application choices, and application settings can reduce the ability of an attacker.

F. **Decreased Capability:** Many types of events can limit our ability to use our phone and access our data. If our phone is lost or stolen, we will need to take steps to make sure our phone is either recovered or wiped. If we forget our password, we'll need to recover our ability to access our data. As part of our consideration of lifecycle management, we'll think about incident response – what to do if our security is breached.

G. **Longitudinal Risk:** As an individual user, we probably don't need to comply with any regulatory requirements like big companies do. However, since we're implementing security controls, we probably want to be able to check that our device is secure. In this way, compliance is a concern for us, and to verify our security we can use audit tools just like the big companies do.

Time Boundary Model Appendix B

Sample Considerations for Apple iPhone

When	What
• Before purchasing or implementing controls on a device.	• Read this document. • Understand the threat model. • Adjust the threat model and controls if they do not meet your specific needs.
• Before purchasing or unboxing a new device. • Before powering on a device.	• Create and secure a vendor account (Apple Account). • Acquire an iPhone from a reputable source. • Verify device integrity.
• Before connecting to a cellular network. • Before connecting to a WiFi network.	• Keep the phone in a physically secure location. • Install a phone case and screen protector. • Set up device locking. • Uninstall unneeded applications. • Consider enabling Lockdown Mode.
• When connecting to the cellular network. • When connecting to a WiFi network.	• Choose appropriate networks. • Configure network connections for security. • Configure VPN (if supported by VPN provider).
• When configuring the Apple Account on our phone. • When installing applications. • Before device use.	• Configure OS and application automatic updates. • Install applications, including secure application alternatives. • Configure applications and features. • Configure VPN (if dependent on an application).
• Before the iPhone leaves our physical control.	• Configure features for remote device wipe. • Make an encrypted backup. • Configure anti-theft features. • Configure cloud security permissions.
• Before excessive time passes.	• Set up audit reporting features. • Check for malware on your phone. • Confirm OS and application updates are applied. • Confirm controls are configured as expected. • Subscribe to vendor emails. • Monitor your Apple Account email address for vendor security notices.