WITN05970124

Hostile Testing - A Discussion Paper

Introduction

This note discusses the concept of "hostile testing" of the Horizon solution, and in particular the desktop, designed to increase the number "real world" problems identified prior to entry into live service. This form of testing is intended to complement the "Live Trial" or "Pilot Trial" approach, but would be run before live users are subjected to the product. Flushing out problems prior to even limited live operation should reduce cost to both ICL Pathway and Post Office Network Unit, allow easier fault resolution, and generally improve the reputation of the product in the field.

Experience from the CSR Live Trial suggests that there were a number of problems related to "real world" use of product which we not exhibited during earlier test phases, but which came to light after a fairly short period of live operation. Hostile testing is intended as an improvement opportunity to detect these forms of problem in advance of live operation.

Note that this "hostile testing" is not intended to provide formal "Penetration Testing", which is attempting to deliberately break the system. "Hostile testing" is therefore intended to simulate, in an accelerated way, the normal but naturally hostile live environment in which the system is likely to have to operate.

Environment and Timing

Hostile testing would take place in a simulated live environment. For this purpose, it would require "final" builds of hardware and software, running in their live configuration (specifically with no security or system management controls disabled), but potentially located within an ICL Pathway or PONU test centre rather than a post office.

This form of testing is best undertaken by a small team consisting of experienced test technicians (with a knowledge of the system and therefore areas of potential weakness) and some real world users (eg former counter staff).

This test activity should be able to be run in parallel (environment and personnel permitting) with existing test phases (MOT or equivalent in the new regime), and therefore should not extend the overall testing duration.

Types of test

The following is an indicative list of the types of "hostile activity" against which various business activites on the system would be tested. It is recommended that, in the development of a test plan for hostile testing, previous failures (from BSM and HSH reports, from existing PinICLs, etc) be used to further populate this list, together with detailed system knowledge within the test team.

- advance button presses (keying/selecting prior to prompt)
- illegal button presses (wrong keys at a prompt)
- unprompted button presses (keys/screen when not prompted)
- unprompted input (smart, mag, scanner)
- duplicate input (smart, mag, scanner)
- interrupting and/or aborting lengthy processes (through button presses)
- interrupting lengthy processes (through reboot and power down)
- failure of printer in various ways prior to and during printing
- quitting from a process before completion - and repeatedly
- conducting an operation repeatedly (eg weekly operation multiple times in a day)
- loss of LAN, degradation of LAN at various points (effect on both gateway and non-gateway)
- loss of WAN, degradation of LAN at various points (effect on both gateway and non-gateway)
- performing conflicting changes (eg on two or more terminals), including during LAN failure

WITN05970124

- .....