MITIGATE CYBER SECURITY RISKS WITH PRE-TESTED SOFTWARE UPDATES

PROTECT MISSION-CRITICAL COMMUNICATION SYSTEMS

CYBER ATTACKS

75% USED VULNERABILITIES THAT COULD BE PATCHED

SECURITY BREACHES

25% ARE CAUSED BY INSIDERS

73% ARE CAUSED BY MISCONFIGURATION OR USER ERROR

CSIS Raising The Bar for Cybersecurity Feb 2013

COMMUNICATION SYSTEMS FACE INCREASED CYBER SECURITY RISKS

As dependency on IP-based systems increases, the risk of intrusion and system compromise becomes an even greater challenge. As mission-critical communications systems become interconnected to other IP-based systems, they are further exposed to continuously evolving cyber security threats.

MAINTAIN COMPLIANCE

Pre-testing and validation procedures enable adherence to various government mandates, specific market regulations and industry best practices set for increased system cyber security measures including:

- European Telecommunications Standards Institute (ETSI)
- International Telecommunication Union (ITU)
- European Committee for Standardization (CEN)
- European Committee for Electrotechnical Standardization (CENELEC)
- ISO 27001
- Payment Card Industry (PCI) Security Standards
- Other privacy directives

PRE-TEST SOFTWARE UPDATES TO PROTECT CONTINUITY OF SYSTEM OPERATIONS

Robust system patching capability is an integral part of the overall organization's cyber security program. Industry best practices suggest that software patches are applied as soon as possible after release from the vendor. However, testing software updates before deploying on a mission critical system is absolutely essential.

Motorola's Security Update Service (SUS) pre-tests the latest anti-malware definitions and all applicable software patches in dedicated test labs. Only the applicable patches needed for the system are identified and selected for testing. This validates that no unnecessary software is introduced via the patching process. Once validated as safe for deployment with the radio network, the updates can be deployed for you by Motorola; or made available to you on Motorola's secure extranet site for implementation.

Rely on Motorola's certified security experts to identify and validate the necessary updates required to maintain cyber security readiness. Security Update Service ensures the right patches are identified, validated and applied in a timely manner to minimize cyber security risk and increase the operational integrity of your mission critical communications system.

MINIMIZE RISK – AND COSTS

Security Update Service delivers:

Increased network availability
Reduce the vulnerabilities addressed by security patches and increase the safeguards of confidentiality, integrity, and availability of mission-critical systems.

Reduced maintenance costs
Dramatically reduce potential for system downtime; resulting in fewer maintenance costs to restore the system back to proper operational state.

Assurance
Motorola assumes responsibility to verify security updates without unnecessary burden to your staff.

Better use of technical resources
Keep staff focused on core responsibilities relying on Motorola to deliver the expertise and support for a proper cyber security regimen.

For more information about Security Services, contact your Motorola representative or visit motorolasolutions.com/services

MOTOROLA