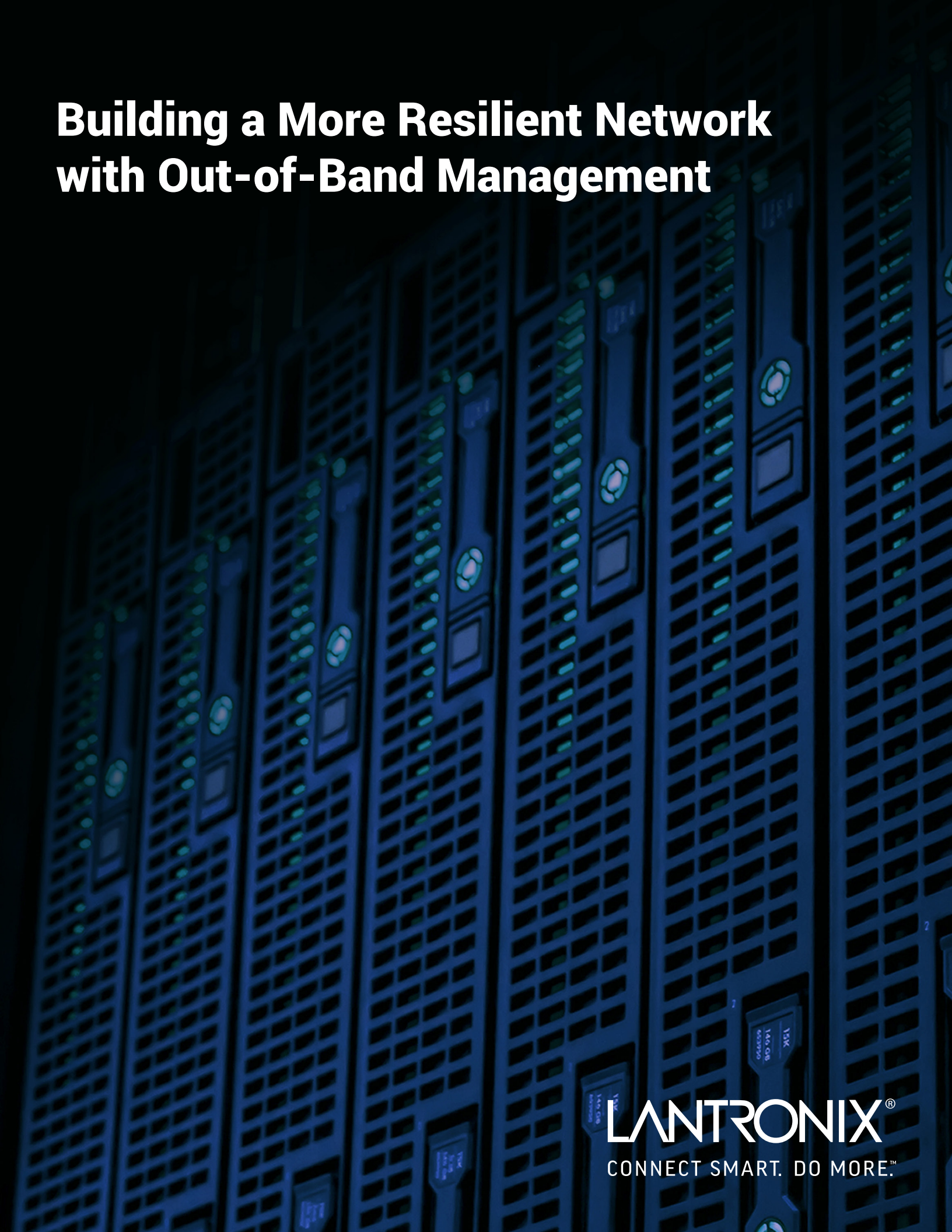
Building a More Resilient Network with Out-of-Band Management



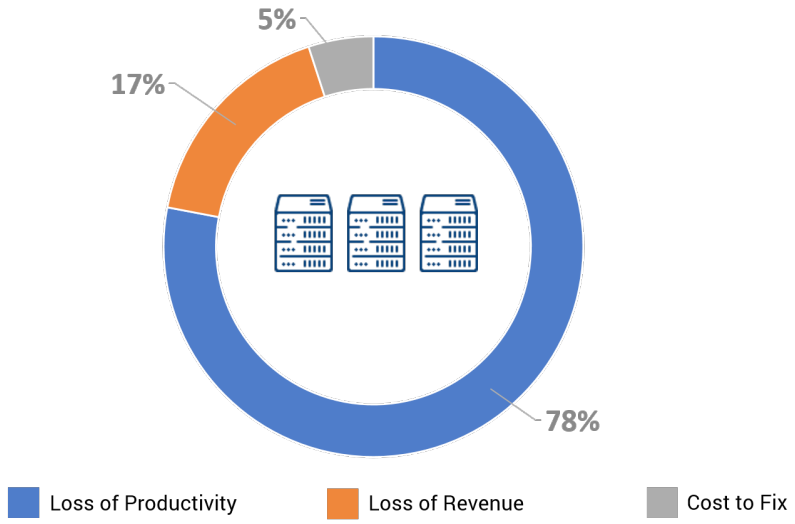
LANTRONIX®

CONNECT SMART. DO MORE.™

EXECUTIVE SUMMARY

In today's fast-paced digital economy, ensuring consistent IT network performance is imperative to business. Customers expect 24/7 IT asset availability, regardless of how complex it is to manage distributed network infrastructure. And when networked equipment inevitably crashes, so do profits and productivity. According to an IHS study, businesses lose $700B annually due to IT downtime[1]. Given the dependence businesses have on network performance, IT administrators need a robust set of tools at their disposal for bringing mission-critical devices back online, especially when the primary production network fails. The good news is that secure and reliable remote access to IT infrastructure is possible using Out-of-band Management (OOBM) technology, which is now a core capability of many remote management plans. This white paper examines the trends and tools of OOBM infrastructure as well as reviews Lantronix's market-leading IT management product portfolio for deployment in data centers and remote branch office environments.

Figure1: IT downtime costs businesses $700 billion annually



THE CASE FOR OUT-OF-BAND MANAGEMENT AS A NECESSARY ELEMENT OF EVERY IT NETWORK

OOBM is a capability that every data center and remote site should have to improve overall performance, support upgrades and local network repairs, and reduce response times for outages. This cost-effective method of reaching equipment allows IT personnel to remotely access and control connected assets outside of the production network. In most cases, enterprise production networks are based on Ethernet, but could also include devices using InfiniBand and fibre channel. OOBM networks can be 100% dedicated or leveraged hybrid models. The type of assets that require OOBM can include the mission-critical routers, switches, KVMs, firewalls, servers, storage, and appliances that serve as the backbone of an enterprise's IT infrastructure.

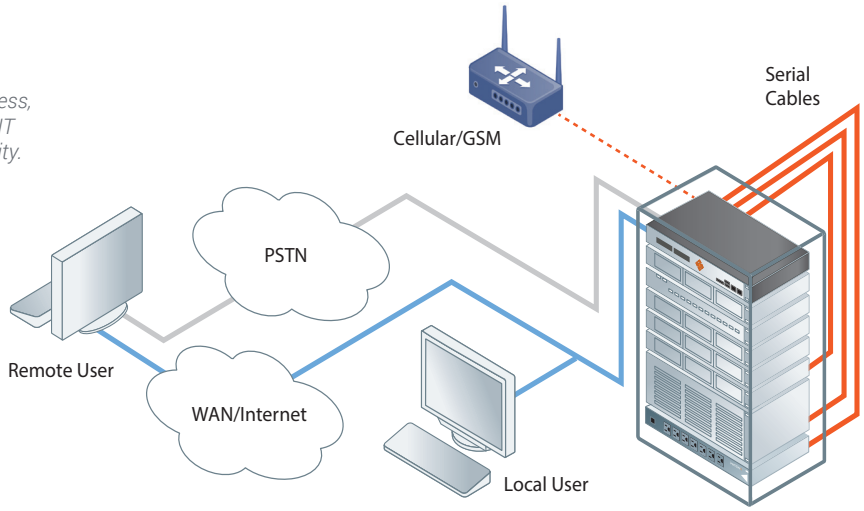


Figure 2: IT administrators can utilize an existing IP network, cellular gateway or a modem to remotely access, monitor and manage a whole room full of servers and IT equipment, while maintaining unsurpassed data security.

OUT-OF-BAND MANAGEMENT CONNECTIVITY

Data center management and connectivity technologies are rapidly advancing and manufacturers are continually improving methods of controlling and monitoring IT assets. At the same time, the exponential growth of the Internet of Things has moved more mission critical applications and workloads to the data centers, further increasing the need for maximum uptime. Below are four major drivers for OOBM connectivity changes over the past five years:

Mobile Devices
As mobile devices have become a prevalent method for accessing IT assets, the need for Wi-Fi and cellular connectivity options for OOBM have grown.

Laptops
The laptop is still the primary connectivity tool for most IT assets whether the IT person is local or remote. In recent years, traditional serial and RJ45 connectors are being replaced with USB (Universal Serial Bus).

Front/Back Real Estate at a Premium
Increasing demand for rack front and back panel real estate has led to the desire for higher operational port density on every device in the data center. Also, as data centers are moving towards hyper-converged and cloud-focused platforms, such as Open Compute, every opportunity is being used to reduce, shrink or eliminate extra connectors.

The Move to USB in IT Equipment
Manufacturers of IT infrastructure equipment such as Cisco, Juniper and Brocade are increasingly moving towards USB ports, and in some cases Micro-USB, for local management ports versus traditional connector options (serial, DB-9, RJ-45).

Internet of Things
With the growth of machine to machine communication and IoT, many mission-critical workloads and analytics require maximum data center uptime more than ever before.

KEY OOBM ENVIRONMENTS

There are many different data center environments and situations where OOBM may be required. Below are three major environments for deploying OOBM today:

On-site Data Center
Whether the data center is used for enterprise, telco or cloud purposes, on-site IT personnel typically use a dedicated Ethernet network for OOBM connectivity. For those in the physical data center in front of the actual device, the most likely direct/local connectivity options are serial or USB ports. Public switched telephone network (PSTN) modems are still a commonly used option for disaster recovery (DR) purposes in many data centers and PSTN can also be used as a last resort option for remote access.

Remote/Co-location (COLO) Data Center
Ethernet is still the primary connectivity option for accessing a remote data center. However, the growing use of mobile devices is adding the requirement for cellular and/or Wi-Fi connectivity options.

Remote Office and Branch Office (ROBO)
Again, Ethernet is still the primary connectivity option, but Wi-Fi and cellular are becoming much more popular and viable outside of the data center. Given that almost every IT and field service person receives notifications on their mobile devices today, the ability to connect and correct issues remotely with a smartphone or tablet is now a requirement for IT.

OOBM TOOLS

When it comes to identifying how devices are managed, there are variety of points to consider. Fortunately, there are several products for secure and remote management listed below:

Centralized Remote Management Software: provides a single-pane-of-glass for real-time visibility of connected IT assets for proactive network monitoring and maintenance.

Console Managers: provide network administrators with consolidated access to virtually every piece of equipment in the data center using one appliance.

Remote Power Managers: provide the ability to power cycle or reboot the network without interrupting all the equipment attached to the UPS.

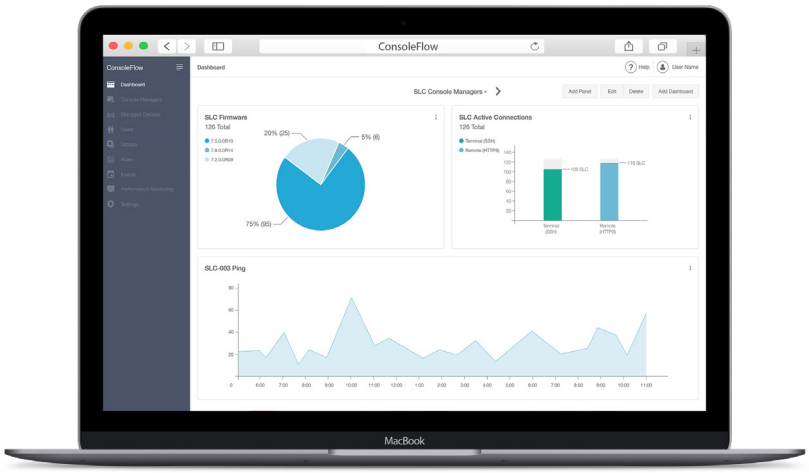
KVM Switches: offer remote management over an Internet connection of servers regardless of their physical location.

Cellular Gateways: enable out-of-band access to critical IT infrastructure via cellular networks.

COMPREHENSIVE OOBM PORTFOLIO FROM LANTRONIX

Lantronix's market-leading portfolio of IT Management products offer a range of solutions to meet the growing dependency of NetOps and DevOps personnel on out-of-band networks. This complete set of OOBM tools allow IT managers and network engineers to:

- Remotely configure, monitor, and manage equipment
- Access equipment over the network (in-band), through a single modem connection (out-of-band), or via the Internet (IP-based management)
- Proactively monitor network performance and notify key personnel when events are triggered
- Deliver a truly scalable and cost-effective solution



ConsoleFlow™ CENTRALIZED MANAGEMENT SOFTWARE

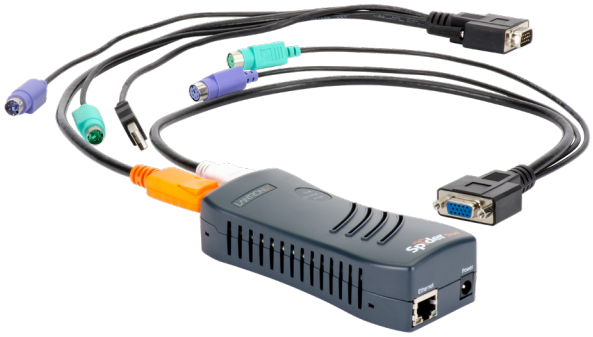
ConsoleFlow is Lantronix's on-premise and cloud-hosted management software that provides centralized management and automated monitoring of all deployed Lantronix Console Managers and connected IT equipment. ConsoleFlow's performance monitoring feature helps network engineers identify the root cause of network issues by measuring and reporting on network traffic performance in real time using IP SLA. Users can create rules to monitor built-in and custom metrics such as network availability, network performance, active connections and firmware distribution for faster response times to network issues. The ConsoleFlow mobile application untethers the network administrators from their desk, allowing them access and full visibility to their out-of-band network on the mobile devices.

SLC 8000 ADVANCED CONSOLE MANAGER

The Lantronix® SLC™ 8000 advanced console manager is the industry's first modular unit that provides secure remote access to IT equipment with user-swappable RJ45 and high-density USB port modules, allowing for easy, cost-effective upgrades and deployment in data center and test lab environments. The new SLC 8000 models with dual SFP ports provide IT administrators with the flexibility of easily adding out-of-band management functionality to their fiber network infrastructure equipment via a small form-factor pluggable unit. The SLC 8000 SFP capability is compatible with a wide range of SFP transceiver modules. The SLC 8000 is FIPS 140-2 compliant and support the highest standards of security and enhanced encryption algorithms.

SLB BRANCH OFFICE MANAGER

The Lantronix® SLB™ Branch Office Manager is ideal for system administrators looking to remotely manage a handful of branch office IT equipment, or unmanned sites that include IT assets such as distribution substations of electric utilities. With proven applications in a variety of industries such as banking, telecom, finance, education and retail, the SLB appliance provides real-time visibility and access to distributed networks of IT equipment quickly and securely.



SPIDER AND SPIDER DUO

The Lantronix® Spider® KVM-over-IP computer networking solutions provide secure remote one-to-one keyboard, video and mouse management of servers and PCs over the enterprise network. With compact "zero footprint" form factors, the Lantronix Spider and Spider Duo products deliver flexible, scalable and affordable CAT5-based remote access and management suitable for everything from high-density data centers to test labs.

PremierWave® XC HSPA+

The Lantronix® PremierWave® XC HSPA+ intelligent gateway is an industrial grade 3.5G cellular solution offering Penta-band HSPA+ performance, network redundancy, and enterprise-level security for mission-critical applications, time-sensitive event tracking and global M2M connectivity.

LTE CONNECTIVITY KIT

The LTE Connectivity Kit provides reliable 4G LTE connectivity via an industrial-grade and secure gateway designed to provide an enterprise-level remote connectivity solution. With state of the art global LTE coverage, the LTE gateway provides broadband connectivity for Lantronix IT Management solutions.

A CUSTOMER'S PERSPECTIVE: DEPLOYING A SECURE OUT-OF-BAND MANAGEMENT SOLUTION

A central IT service provider responsible for developing and operating all IT applications for a prominent financial institution required an IT management solution that enabled remote out-of-band management access for multiple administrators with distinct areas of expertise, permissions, and access rights. In addition to upgrading their IT management system, the customer requested a tailored security feature that provided a clear audit trail of who did what and when, and to which system. The customer chose the Lantronix SLC 8000 advanced console manager to provide out-of-band access over the administrator's Ethernet channel to critical systems comprised of routers and servers. Administrators could remotely manage essential IT equipment and deploy cost-effective upgrades as they became available.

The next challenge was ensuring that machine access was given to administrators with the appropriate credentials. In many cases, a security issue arises when an administrator logs out of the console server but fails to log out of the target machine. The danger is that a second administrator could then log into the same console server port and access the active connection. This is considered a security breach since the second user is logged in under the identification of the first administrator.

Normally when networks require a system administrator to connect to a target system through a console server, they are first challenged to identify themselves. Once connected to the port leading to the target system, they will be challenged again by the target machine's security system – so they must log in a second time. The SLC 8000 eliminates these added steps by customizing the end user's software to include self-terminating security strings that automatically disconnect administrators from active sessions. Now, if an administrator disconnects from the SLC 8000 without continuing to log out of the target machine, the console manager will automatically send a logout command and end the session. This will leave the target machine protected when a second administrator tries to access the same target after the first administrator departed.

CONCLUSION

In today's highly competitive global marketplace, companies of all sizes cannot afford lost productivity or lack of access to information when network infrastructure fails. Out-of-band management solves the challenge of bringing equipment back online and there are many tools for deploying this solution. With many organizations' network infrastructure spread across many environments, there is considerable demand for next-generation OOBM solutions specifically designed for the distributed IT environment.

ABOUT LANTRONIX

Lantronix, Inc. is a global provider of secure data access and management solutions for the Internet of Things (IoT) assets. Our mission is to be the leading supplier of IoT solutions that enable companies to dramatically simplify the creation, deployment, and management of IoT projects while providing secure access to data for applications and people.

Lantronix is headquartered in Irvine, California. For more information, visit www.lantronix.com. Learn more on the Lantronix blog, www.lantronix.com/blog, featuring industry discussion and updates. To follow Lantronix on Twitter, please visit www.twitter.com/Lantronix. View our video library on YouTube at www.youtube.com/user/LantronixInc or connect with us on LinkedIn at www.linkedin.com/company/lantronix.

REFERENCES:

1. Machowinski (2016) The Cost of Server, Application, and Network Downtime: North American Enterprise Survey and Calculator. https://technology.ihs.com/572369/businesses-losing-700-billion-a-year-to-it-downtime-says-ihs

lantronix.com

Corporate Headquarters
Lantronix, Inc.
7535 Irvine Center Drive
Suite 100
Irvine, CA 92618
Tel. 949.453.3990