Securing Government Desktops from Cyber Threats with the Latest KVM Technology

Securing Government Desktops from Cyber Threats with the Latest KVM Technology

A Belkin White Paper

Executive Summary

Cyber attacks on government systems are increasing at an exponential rate. Over a three-year period, government agencies reported a 400-percent increase in attempted incursions into federal systems. While there is no current data on the number of attempts to compromise intelligence and defense computer systems, they are no doubt under similar stress as foreign governments, terrorists, and malicious hackers target classified data and government documents, attempt to shut down networks and destroy valuable infrastructure, and steal intellectual property. One of the least understood and most under-utilized preventative measures for thwarting attacks is the use of keyboard-video-mouse (KVM) switching devices that allow government employees to switch between networks with various security levels from one desktop. Firewall protection alone is not enough to deter sophisticated cyber threats. Cyber attacks from within an agency need to be as rigorously addressed as those originating from outside sources. However, government purchasers of KVM products need to thoroughly vet the security features, design, manufacture, and even the packaging of any product before trusting a deployment in any areas that require high security.

Introduction

Foreign nations, terrorists, and cyber criminals see government IT infrastructure as extremely attractive and lucrative targets for data theft, system attacks, and service disruption. The stakes are high. Besides the catastrophe that the loss of state secrets, military data, or classified documents would entail, attacks have taken down entire systems, destroyed valuable equipment, and left many government agencies repeatedly vulnerable in countries throughout the world. The costs of remediation and repair of systems after these attacks is significant. In testimony before the Committee on Homeland Security, Gregory C. Wilshusen, Director Information Security Issues, said:

Many nation states, terrorist networks, and organized criminal groups have the capability to target elements of the U.S. information infrastructure for intelligence collection, intellectual property theft, or disruption.

Cyber-based threats to federal systems and critical infrastructure are evolving and growing. These threats can come from a variety of sources, including criminals and foreign nations, as well as hackers and disgruntled employees. These potential attackers have a variety of techniques at their disposal, which can vastly enhance the reach and impact of their actions. (1)

Threats are ring exponentially as attackers gain greater sophistication and familiarity with known and unexpected system vulnerabilitis in government systems. In accordance with Department of Homeland Security policy, the United States Computer Emergency Readiness Team (US-CERT) collects reports of any known computer breaches or attempted attacks to all federal information systems. The agency reported that the number of incidents grew from 5,503 in 2006 to about 30,000 in 2009—a startling 400-percent increase. Even more alarming is that government performance and accountability reports in 2009 showed that 21 of 24 major federal agencies "noted that inadequate information system controls over their financial systems and information were either a material weakness or a significant deficiency." (1) Many of these inadequacies come not only from external threats but internal infrastructure. Regardless, the trend lines are inescapable—cyber threats to government computing systems will continue to escalate tremendously as both external and internal systems prove vulnerable to attack. The Stuxnet worm is a clear example of how infrastructure can be easily penetrated.

The Stuxnet worm could go down in history as the first shot fired in the age of cyber warfare. The United States and the rest of the world are ill-prepared to defend against it. (4)

The Stuxnet worm, purportedly launched against critical industrial components of the Iranian government's uranium enrichment program, demonstrated that cyber attacks can disable or even destroy military and research equipment that is not technically considered a computing system. The worm was introduced to the centrifuge facilities network from a USB device plugged into a desktop computer. Undoubtedly many more breaches have gone unreported worldwide, and it is uncertain what damages they may have caused to government systems. What is certain, however, is that the number and sophistication of attacks against local, state, and federal computing systems will continue to grow. KVM systems designed with higher security can help reduce data leaks caused by attacks on desktop systems.

External Vulnerabilities

Attacks on computing systems generally fall into two categories: those initiated in real time by a hacker or group of hackers actively working systems in real time, or software attacks by bots, worms, and Trojan horses that propagate and carry out their activities automatically once launched. As examples, denial of service and some worms are designed to take down systems. Sniffing and phishing programs are designed to gain access to passwords, logins, and even entire data systems. With an increased reliance on wireless devices, many government computer systems are attacked via wardriving, where equipment is used to seek out holes in wireless security.

Automated cyber-attack tools in particular can be extremely devastating as they replicate and propagate throughout entire networks quickly and with little or no initial detection. Many lie dormant until triggered by pre-determined system states, such as scheduled data backups or specifically set dates and times, or initiated by a command from an outside operator or a person working within an organization. These automated "code bombs" do not necessarily need the Internet to exploit systems. Any system that is used for data input can introduce these potentially devastating and destructive software payloads, particularly KVM systems that do not completely secure and isolate data paths. Lawrence Husick, Senior Fellow in the Foreign Policy Research Institute's Center on Terrorism, Counter-Terrorism and Homeland Security, has aptly called these types of attacks "software guided missiles." (4) Once they are set loose in a system, they can make their way through virtually every attached network component, including servers, routers, desktops, and even industrial equipment and controls that rely on computer-based information for operating instructions. As our power grid, military command-and-control facilities, and physical security systems increasingly rely so heavily on computer components, these escalating threats have an ever-richer field of targets to exploit.

> These deficiencies continue to place federal assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, and critical operations at risk of disruption. – The U.S. Government Accounting Office, 2010

Internally Introduced Vulnerabilities

While external threats are the most publicized and common, lapses and errors in security procedures by employees within government agencies can either intentionally or unintentionally introduce threats into computer systems with equally devastating effects. Worms and viruses carried into secure facilities on disk or flash drives, careless access to data or login procedures, and a myriad of other user errors can bring down systems as quickly as coordinated attacks by outside hackers, with all the same disastrous results. KVM systems need to clearly prevent the introduction of worms, viruses, or other means of attack through peripherals. Hackers and criminals have become increasingly aware of these types of "soft spots" in government systems, and have many methods to circumvent internal security from willing or unwilling internal personnel.

Cyber Targets

The primary targets for criminal hackers, terrorists, and malicious software agents are far-ranging and can affect both government and civilian assets. According to a 2010 GAO report, among the chief motivations for cyber terrorists and criminals are the following:

- **The disruption of operations, such as those supporting critical infrastructure, national defense, and emergency services.**
- **Denial of service and system shutdown attacks that can result in loss of reputation and trust in agency and government systems.**
- **National security information, taxpayer data, Social Security records, medical records, and proprietary business information could be accessed and used for identity theft or espionage.**
- **The theft of government payments and financial records. (1)**

The motivation for criminal and terrorist attacks is often reflected in the techniques they deploy to exploit, destroy, or disable individual systems or entire networks.

Data Theft

Stolen classified documents can jeopardize national security. Terrorist organizations and foreign governments have made repeated attempts to gain access to U.S. computer-based data. While most of these attempts have come from well-orchestrated attacks over the Internet, there are many reports of lapses in security within organizations themselves.

While hacking that results in financial gain and retrieval of intellectual property is perhaps the most damaging of all, terrorists and malicious hackers often find it just as strategically advantageous to steal information critical to government and military. Computers connected to a secure network through an unprotected KVM system can be leaked over to an unsecured network that is linked to the outside.

Destruction or Disruption of Infrastructure

Another goal of hackers and cyber terrorists is the shutdown of critical computer systems and infrastructure. Destruction of data can disable agencies and operations for days or even weeks. While all systems have adequate backup and emergency disaster recovery procedures in place, operational efficiency can grind to a halt or become extremely unreliable as remediation and repair takes place. As system data is restored it must be tested and verified as "clean" and reliable. Meanwhile, new work must be carefully incorporated into the newly restored systems.

Hackers have other means of disrupting government services. Distributed denial-of-service attacks can overwhelm systems to the point that they become completely non-functional. While networks and network servers are often the prime targets, even desktop, laptop, and other network-attached devices are vulnerable.

As the Stuxnet worm demonstrated, unprotected desktop systems can be a key target for attack. Military assets, the power grid, and other essential government and civilian infrastructure systems if taken off-line for even a brief period of time would introduce extremely dangerous vulnerabilities for public safety and national defense. Therefore, KVMs must make certain they do not allow the attachment of unauthorized peripherals.

Budget Impacts

The mitigation of cyber threats is a costly and perpetual battle for government security professionals. Besides the capital expenses of ever-more sophisticated security equipment and IT training and management, cyber attacks can destroy equipment and data and cause hours in remediation and repair in the aftermath of a breach or even an attempted intrusion. Government agencies must be vigilant yet judicious in allocating resources to prevent attacks. Nevertheless, the most costly effect of cyber terrorism is any successful destruction or theft of government assets. Theft or destruction from cyber terrorism has a far higher price tag than any preventative measures an agency can deploy. As agencies spend millions on protecting against external threats with sophisticated firewalls and routers, they should also protect desktop systems with the latest in KVM technology, which delivers an additional, highly effective solution at a reasonable cost. The deployment of KVM systems needs to be evaluated very carefully as they are used to bridge multiple computers from multiple networks and different security requirements.

Loss of Trust and Reputation

Finally, the impact of cyber attacks on government resources can cause irreparable harm to the reputation of the government itself. Hostile foreign governments, cyber criminals, and terrorists are emboldened by any sense of weakness in the government's computing infrastructure, giving rise to even greater threats in the future. Foreign allies and the public at large lose trust and faith in the government to secure data and its ability to function safely and efficiently on their behalf. Even if cyber attacks do not successfully disable or cripple critical government services, cyber terrorists can significantly erode public and foreign confidence in the government. This loss of trust and reputation has no price tag, and it carries heavy, long-term negative perceptions that take significant effort to restore.

Limiting Desktop Threats: KVM Switching Solutions

For good reason, network and datacenter security systems are the primary concerns for government IT professionals. These are the most traditional and common attack points for threats from outside sources. As noted, internal threats and errors are equally dangerous. For this reason, many government agencies have introduced layered, secure access to systems by end users in the form of keyboard-video-mouse (KVM) switching systems. Using these switches, users can have access to multiple computing systems from one desktop console, switching between various systems as their jobs require. This system helps segregate secure and non-secure computing use. For example, a government employee accessing internal email systems with a lower level of security can then switch and log into a more secure system to perform more sensitive tasks.

The chief advantage is to make certain that employees do not log into an unsecured system and inadvertently work on data on a secure system, exposing sensitive data over the less secure network connection without relying on multiple computer desktops. Not all KVM switching systems are secure, however. While they do a good job of reducing user error in working between various levels of network security connections, unsecured KVM systems are vulnerable to both intentional and unintentional security vulnerabilities.
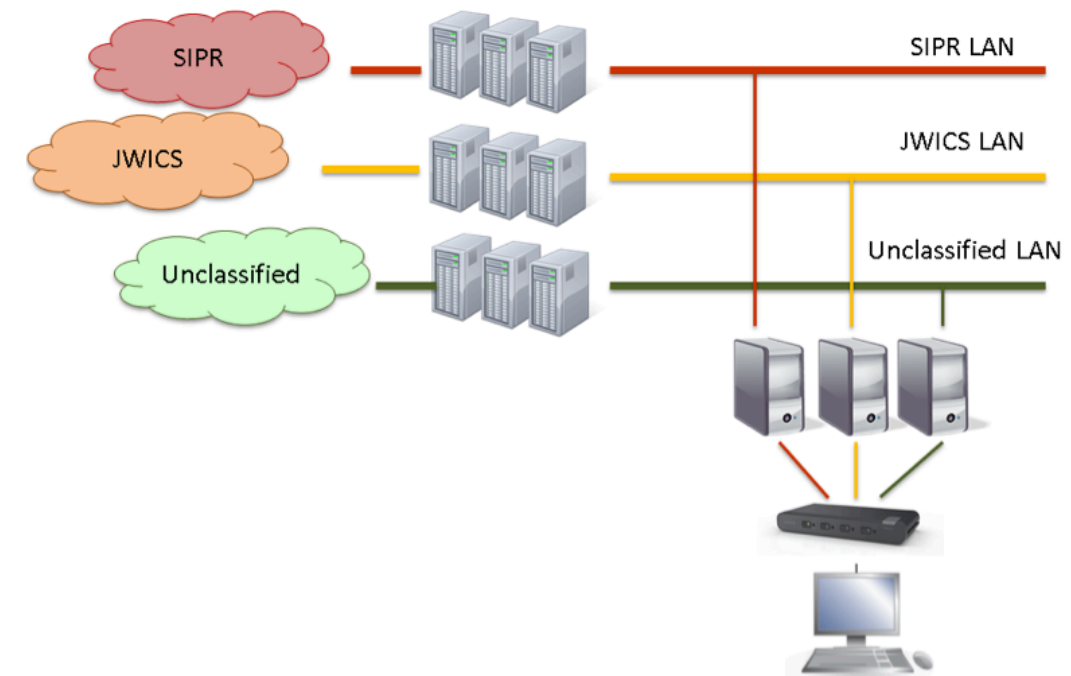

Figure 1. Typical secure KVM environment.

Known Deficiencies in Many Current KVM Switches

Experiencing first-hand the inadequacies of non-KVM secure desktops, state and federal agencies have begun to deploy KVM switch technology to remediate security lapses at employee user consoles. Unfortunately, not all perform to the highest standards possible for eliminating security threats. Products run the gamut from simple desktop boxes to highly sophisticated and automated devices. Any purchaser of KVM switching technology should thoroughly investigate and vet the capabilities and features of these systems before trusting them within multi-security-level environments. Non-secure KVM switches should be used only in situations where users have access to virtually no sensitive data and are on isolated networks with no chance of connecting to more secure systems. The most effective means to mitigate any data leakage from the PC to and from the network is to ensure that all data coming into and out of the KVM switch is completely isolated whenever the operator switches from one secure network to the next. Below are some of the known deficiencies and vulnerabilities of some KVM solutions currently in the market:

USB Peripheral Vulnerabilities—USB ports on modern desktops have vastly improved the performance and standardization for attaching peripherals to desktop computers. Everything from high-performance scanners to keyboards utilize the same plug-and-play interface to communicate with the desktop system. One of the primary features of the USB port is its high speed, bidirectional flow of data to and from the computer. This is also a potential threat. Much of this bidirectional efficiency is shared along the entire USB bus, effectively enabling maliciously altered peripherals to gain control, intercept, and/or access resources beyond the PC itself and into any computer network that the PC is attached to. In addition, the USB bus architecture does not completely isolate individual USB ports—a feature for some applications, but a potential for data leakage in a secure environment, as data moving from one peripheral USB port could be captured through any other port if the port is not completely isolated. Furthermore, only authorized devices should ever be allowed to connect to a secure computer's USB port, particularly flash drives or external hard drives that could be used to introduce viruses or download restricted data.

Video Vulnerabilities—LCD monitors store display parameter data in the form EDID, which could be exploited. EDID can be used to leak data from a secure network to an unsecured network by using the monitor display memory as a vehicle to transport data when being used with a KVM system. KVM devices must prevent the reading or writing of display memory with a protected display interface to stop leakages.

Microphone Vulnerabilities—The use of microphones for conferencing and note-taking are susceptible to sniffing, capture, and re-direction as well. The AC'97 codec input used for audio in desktop PCs is a highly sophisticated signal processor that could be intercepted by sniffer software, capturing any conversation used over the input channel.

Memory Buffer Leaks—As mentioned, peripherals, keyboards, displays, and even network interface cards can rely heavily on buffered data to increase performance. Surprisingly, some KVM switches also use buffering onboard, and have the potential to inadvertently leak data from channel to channel as they use the same switching processor for multiple ports. A keyboard buffer can be an area of vulnerability to transferring information from one port to another.

Inadequate CAC Implementation—Many KVM systems do not support CAC or have limited support of CAC readers. However, even those that provide CAC-reader support do not fully isolate the CAC reader from other peripherals. By not isolating the CAC port, the keyboard and mouse are vulnerable to attacks. In addition, the KVM must have a port that only detects and supports CAC readers—no other device should ever be allowed to connect to this isolated port.

Poor Casing and Design—Because so much security enforcement relies on the integrity of the KVM components themselves, it is important that purchasers take a close look at the internal and external components that go into the manufacture and design of the KVM switch. Since the KVM is responsible for safeguarding many channels of data, it is important that the external housing of the switch is demonstrably tamper-proof, ensuring that it cannot be opened and modified at any time. Similarly, the internal components of the switch must be constructed to prevent tampering of any kind. Finally, government purchasers, particularly those in highly classified installations, should make certain that only trusted, domestic vendors with proven security measures in place are designing and manufacturing the devices they will be using. In fact, most KVM switches currently on the market are designed and manufactured in foreign countries, many of which are assembled and shipped from Asia.

Requirements for Improving Desktop Security and Reducing Risk

In an effort to continually improve the security and reduce vulnerabilities in computing systems used by the government, the National Information Assurance Partnership (NIAP), a government-sponsored agency based within the National Security Agency, formulates specific requirements and recommendations to secure nearly every aspect of computing environments. These directorates are used as the basis for testing and certifying commercial components and serves as a trusted security conduit between manufacturers and consumers of computer products used in secure environments. One aspect of the NIAP program is the evaluation and recommendation for improvements in KVM switches. The agency's latest directorate, *Protection Profile - Protection for Peripheral Sharing Switch (PSS)* Version 3.0 was published in February, 2015.

As a part of its program, NIAP tests devices submitted by manufacturers for security compliance. Devices receive evaluation assurance levels that purchasers can use in making certain that any potential KVM device they purchase conforms to the NIAP recommendations.

The directorate describes a number of potential issues in testing KVM switching devices, any of which could cause significant security problems. The following are a few of the most concerning scenarios that the NIAP testing program examines:

- **Users should not be allowed to connect unauthorized USB devices to the peripheral switch.**
- **The KVM must prevent residual data transferred between peripheral port groups with different IDs.**
- **Connection shall not be accessible by any other peripheral group with a different group ID.**
- **The KVM should prevent a user error when setting shared peripheral connections from one computer system to a different one.**
- **A connection, via the KVM, must not allow information transfer between computers.**

These concerns are directly related to most of the detailed deficiencies in some current KVM switching devices already discussed in this paper when handling USB (peripheral), video, audio, and memory buffering.

Solutions for True Data Path Isolation

Most of the discussed deficiencies of current KVM switches are directly attributable weaknesses in maintaining data path integrity. To achieve true data path isolation, a KVM switch must be purposefully engineered to completely isolate each data path connection in the switch. The following are advanced methods for implementing more tightly secured KVM operations:

- **The first imperative for data path isolation is to provide single, unbuffered, dedicated processors for each KVM switch port.**
- **No buffering of data should be allowed anywhere on the data path or within the KVM switch. When an operator switches to another network/port, the port must be completely closed before the new port is opened. Any other method can leak data.**
- **To guarantee the safe switching of video displays, rather than rely on the PC's built-in plug-and-play interface, which introduces inherent and unavoidable vulnerabilities, the KVM switch itself should handle the video data path through isolated emulators.**
- **While the use of microphone input may be convenient in some applications, it introduces too many opportunities for malicious hacking or voice capture.**

End-to-End, Tamper-Proof Systems

One of the most overlooked threats to true KVM security is in the design and manufacturing process. Government purchasers have the right to demand how and where the KVM switch is designed and manufactured. KVM technology is complex, and either malicious or unintentional weaknesses can easily be built into systems during the engineering phases or in the physical construction of the units themselves. Customers should have answers to the following critical questions before making a purchasing decision:

- **Who engineered the product, and where?**
- **Does the system contain reprogrammable components (a potential stealth threat)?**
- **Does the switch include safeguards such as security seals and tamper-proof components?**
- **Where is the product assembled, packaged, and shipped from?**

As mundane as some of these questions may seem, any technology claim made about a KVM product could be easily circumvented by either faulty or malicious design or in the engineering and packaging of the switch. Any switch that is not secure from the design stage through delivery can put data systems at risk. End-to-end, tamper-proof design and delivery is essential.

The Belkin Solution

Based in California, Belkin is one of the most respected and successful computer component designers and manufacturers in the world. Its secure KVM switch solution is NIAP-listed and approved to the latest KVM testing standard (PPv3.0). One of its exclusive innovations is the use of true data path isolation.

Optical Data Diodes

Isolated processors are an integral part of the Belkin solution, but its next-generation engineering takes a unique step forward by introducing optical data diodes to provide unidirectional data paths to completely eliminate the opportunity for data leaks or data capture on keyboards and mice. The Belkin optical diode connects input and output data paths with a signal that uses light in the following process. First, it transforms input signals, such as keyboard strokes, into light signals. This light signal is sent along a dielectric channel where the light is captured on the output side of the circuit. Within the isolated diode, this light signal is then transformed back into an electric signal. This innovation goes far beyond isolated processor engineering because data to and from peripherals is never exposed to any form of electrical sniffing or capture. Signals pass, in light form, in one direction, eliminating the typical peripheral vulnerabilities of bidirectional signaling through copper.
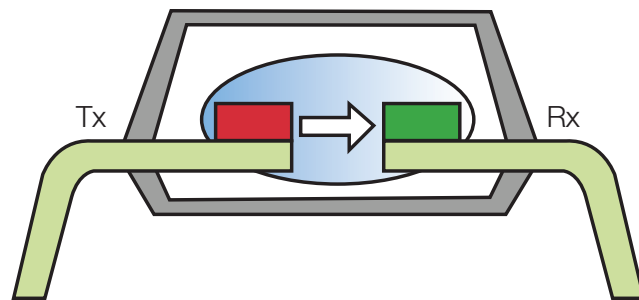

Figure 2. Cross section of optical data diode.

Dedicated Processors for Every Port

The Belkin Secure KVM Switch contains dedicated, program-once processors with up to 16 emulators for each KVM, completely isolating the data path between every post and peripheral. Each component is hard-soldered to the electrical board and any removal or tampering renders the entire KVM inoperable. Audio, USB, video, and peripheral ports support the latest standards yet and are isolated and secure.
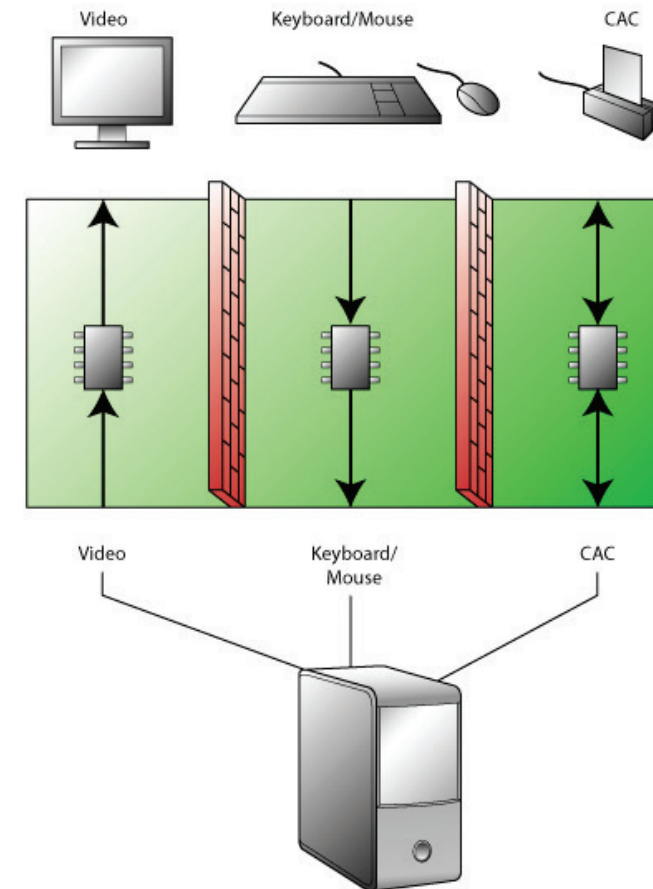

Figure 3. Dedicated processors and emulators.

Tamper-Proof Design, Packaging, and Shipping

Belkin KVM products are designed, built, and shipped in the U.S. under the strictest security. Every Belkin KVM switch includes tamper-proof seals on external and internal components as well as on the outside shipping container. Customers are assured that the product is in its original, securely manufactured state from one end of the process to arrival at their facility.

Advanced USB and Cabling Technology

USB signals are monitored in real-time and never allow unauthorized traffic or the attachment of unauthorized devices such as flash drives, disk drives, or unapproved peripherals. The unit's unique chassis design includes high-retention USB connectors that prevent accidental disconnection of USB cables. Unlike many other KVM switches, the Belkin KVM switch supports legacy USB peripherals as well as the full range of CAC card readers, preserving customer equipment investments.

Belkin provides smart cabling that enables government agencies to connect their Belkin KVM switch simultaneously to legacy VGA computers and newer DVI computers with USB peripherals. In addition, the Belkin KVM switch allows for CAC-reader connectivity on dedicated ports that are separated from the keyboard and mouse ports. All cabling is tested in a secure lab and include interfaces common to many agencies including the DoD.

Other Advanced Features

The Belkin KVM switch incorporates many other advanced features:

- **No memory buffering of any type**
- **Protected video-display switching through plug-and-play emulators**
- **Multi-platform compatibility and support**
- **Color-coded, user-friendly interface to reduce user error**
- **Intelligent Common Access Card switching to prevent unwanted system log-off**
- **No keyboard or mouse delays when switching ports**
- **Integrated mounting track to allow under-desk or side-wall mounting to improve desk space**
- **Customizable port-coloring to facilitate network identification**
- **High-resolution support for graphic-intense applications used on larger displays**
- **Dual-monitor support to increase user productivity**

Conclusion

Threats are on the rise, with government data and computer systems as prime targets for hostile foreign governments, terrorists, and cyber criminals. The internal threat posed by improperly secured desktops in government agencies should be addressed with as much due diligence and vigorous security measures as firewalls, intrusion detection, and other external threat mitigations. Government purchasers of KVM equipment need to carefully weigh all the security and functional features of these devices to make certain the units provide the safest, most secure and user-friendly functionality to prevent any possible compromise of government assets.

References

1. *CYBERSECURITY: Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats*. Statement of Gregory C. Wilshusen, Director Information Security Issues. Testimony before the Committee on Homeland Security, House of Representatives. GAO. June 16, 2010.

2. *Cyber Attacks Put U.S. at Risk*. PBS News Hour. July 2009.

3. CNN. December 1996.

4. Piper, Andy. *Expert: Web worms way into warfare*. April 14, 2011.

5. NIAP. *Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile*. September 2010.

belkin™
GOVERNMENT

www.belkinbusiness.com/government