Distributed Servers

Division of Information Services

December 11, 2019

Office of Internal Audit and Risk Management

Report No. 158-19

DATE: December 11, 2019

TO: Jeff Coiner, Chief Information Officer
Rob Martin, Information Security Officer

CC: Clifton M. Smart III, University President

FROM: Donna Christian, Director of Internal Audit and Risk Management
Natalie B. McNish, Senior Internal Auditor

Distributed Servers
Division of Information Services

BACKGROUND

The Division of Information Services is a centralized asset composed of various information technology (IT) personnel who assist with the development, installation and user support functions of information services needed to secure and maintain various administrative and educational operations the University. The Division is comprised of four units, Computer Services, Networking and Telecommunications, Information Security, and BearPass Card. The Division's mission is to contribute to the effectiveness of information services by actively participating in the planning, development, and implementation of information technology for the University. The Division is responsible for University wide email services, Banner, Blackboard and SUDERS applications, providing user support to most administrative functions, and more.

As the University has increased its use of technology overtime, individual colleges and units wanted dedicated personnel to increase response time and expedite technology implementation. From this desire for dedicated service, distributed system personnel were hired to develop distributed IT systems, including servers. These personnel are supervised by their individual colleges and units and charged with the development and management of IT assets not provided by Division of Information Services.

During the most recent Cybersecurity Risk Assessment completed in April 2018, it was noted management should take a closer look at potential risks existing in the distributed environment.

OBJECTIVE AND SCOPE

The objectives were to review the distributed servers to determine the sufficiency of established controls. The scope included only the main campus located in Springfield, MO, and focused on procedures in place during the fiscal year ending June 30, 2019.

SUMMARY

We determined the Division of Information Services and the distributed service personnel could benefit from an organizational structure which links these two similar and yet distinctly different areas. There is a need for new policies to be developed and/or current policies to be revised to address risks existing in the distributed environment, a need to improve physical asset management and security controls and a need for specific oversight of virtualization. We further noted areas of information security, such as vulnerability assessment, backups and disaster recovery, the use of unsupported or under supported operating systems, and the use of network isolation for testing environments where improvement is necessary.

Donna Christian

Donna K. Christian, CPA, CGFM
Director of Internal Audit and Risk Management

Natalie B. McNish, CFE, CGAP
Senior Internal Auditor

Audit Field Work Completed: October 31, 2019

OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT RESPONSES

1. Control environment

Improvement of the control environment for distributed systems is necessary. An organization’s control environment is the foundation for all other control activities. It includes the attitudes, awareness and actions of management, the governance policies and organizational structures, and the overall mission, values and principles that set the tone for the implementation and achievement of strategic objectives.

A. Organizational Structure

The University’s overall information technology environment could be strengthened by joining the distributed and centralized personnel through a dotted-line or secondary solid-line relationship within the organizational structure.

The distributed environment is supported by 36 employees. Of these 36 employees, only one employee directly reports to the Division of Information Services. The other 35 employees work for other units of the University and report to their respective Department Head, Dean, or Vice-President. Distributed personnel have unique and specialized knowledge of their units and the roles played by distributed systems. Using the varying structures, resources, and tasks confronted, each has built a system which serves the direct educational and support needs of their unit. Some have pioneered differing or new methodologies successfully, and through those challenges, have built knowledge which can benefit the entire University.

Likewise, the Division of Information Services has its own unique and specialized knowledge of centralized systems, risks and resources. This unit is charged with the responsibility of ensuring all University information system needs are met in the most secure manner possible.

By adding an organizational relationship between the distributed and centralized systems, both environments could benefit from shared knowledge, resources, advancements and challenges.

B. Policy

The Division of Information Services has not established a policy specifically addressing distributed systems and most existing operating policies are not clear as to their application in the distributed environment.

The purpose and structure of each distributed system is unique to its own environment and some of that uniqueness may be crucial to its operation; however, there are many areas in which policy would add value to these systems. An established criteria for allowing a system to be distributed in nature, criteria for allowing the system to be housed outside of a data center, and identified physical and informational security requirements would provide a foundation for these systems. In addition, these policies should provide the Division with oversight of the machines operating on the University’s network.

Recommendations

The Division of Information Services should:

A. Consider establishing an organizational relationship with distributed staff.

B. Revise current and/or develop new policies that address risks within the distributed environments.

Management’s Responses

The Division of Information Services provided the following responses:

A. *Information Services will work to strengthen the coordination, communication, trust and transparency between the Information Services Division and the distributed IT staff within the framework of the existing organizational relationship defined by the Chief Information Officer's job description, which states: "The CIO serves as the executive officer responsible for providing leadership and management to the units of Information Services Division and is responsible for system-wide planning, management, security, and coordination of the technology resources of the Missouri State System."*

B. *Information Services will work with IT Council to establish or identify a committee that will develop a policy to address risks in the distributed environment. The committee will also help determine solutions and funding sources to support the necessary long-range technology requirements.*

2. Physical & Virtual Security

Physical security of distributed environment assets is critical to the functionality of both the distributed and centralized systems. Our audit determined current physical security controls could be improved. In addition, the distributed environment appears to be moving in the direction of virtualization and while this offers many benefits to these distributed environments, it also presents a host of risks. Our audit determined there is low/no oversight of these virtual machines (VMs) by the Division of Information Services.

A. List of Distributed Servers

The list of distributed servers maintained by the Division of Information Services is incomplete, sometimes inaccurate, and the application used to maintain the list is cumbersome for users. The Division has developed an application which tracks distributed servers on the University network. This list provides a place for server name, location, college or unit served, department head, system administrators/primary technicians, server make/model/type and serial number, current operating system, purpose, data sensitivity, and an audit log showing when the information was last updated and by whom.

A review of the information held on this list, captured on November 26, 2018, February 13, 2019 and again on July 19, 2019, and discussions with the distributed staff determined:

- Distributed system staff did not feel they were provided with clear instruction regarding what assets and information should be included on this list, and are often unable to view or change information recorded by a different user, even if they are the system administrator.

- The list does not specifically require certain vital information, such as identification of host machine for virtual servers or an indicator of activity level (active or inactive).

- At least 20 active servers were not included on the listing as of June 30, 2019. In addition, at least 8 servers listed as of June 30, 2019, had been taken offline, or were test entries which were never deleted.

- One distributed server system administrator documented on the list identified two of the servers listed as personal assets.

- Some information recorded was incomplete or out-of-date. For example, 11 servers were recorded with "n/a" department head, 7 servers were recorded with "Unknown" data sensitivity, and serial numbers for physical machines and operating systems installed were not always recorded or updated. We also noted 42/149 entries in the November 26, 2018 date list were last updated in 2014. These are all indicators of areas where information was less likely to be accurate

A complete and accurate list of all assets connected to the University network is necessary to ensure both the accountability and security of University assets. In addition, the Division should establish procedures to review the information reported and investigate inaccuracies, risks, and other issues such as the personal assets noted above.

B. Physical Safety

Physical controls for many distributed servers are not sufficient. University operating policy 12.07-5 Physical Security, requires, “facilities that house data systems and data storage, workstations, and other computing devices will be protected from unauthorized physical access, as well as natural and environmental threats that may compromise confidentiality, integrity, or availability.” For a physical machine to be considered secure, minimum controls in place should include:

- Physical access to servers should be restricted to authorized users only.
- Protection from electrical system surges and failures should be provided.
- The environment should be heat and humidity controlled.
- Storage areas should be free from water intrusion or leakage.
- Fire suppression mechanisms, such as fire extinguishers rated for electronic equipment, should be installed in close proximity.

During our review of physical controls in various distributed environments, we found servers stored in open workspaces accessible to the public, on the floor and beneath windows of offices, in cabinets trying to keep machines away from known HVAC or other water intrusion issues, and in storage closets without HVAC vents. In addition, fire suppression mechanisms were not immediately available, were not sufficient, or consisted of sprinkler systems which would only compound the risk of loss of information and functionality in the event of a fire.

Physical controls for many of these distributed servers could be improved by relocating the physical machine to the data centers established in Cheek or Blair-Shannon Halls. These data centers were constructed to meet all physical control standards and have capacity to house more machines than currently exist. When discussing this option with various distributed system staff, several barriers were identified. Current barriers include: the need for physical access to certain machines based upon current configuration or maintenance requirements, the contractual requirements to maintain all assets on one local network, the use of non-rackable machines, and the increased costs charged by the University’s Office of Networking and Telecommunications for use of these data centers.

C. Virtual machines

The Division of Information Services should provide oversight or guidance with regard to the use of virtual machines (VM). VMs are computer software developed to function as a completely separate system within the system they are installed (hosted). Each host can provide the foundation for several VMs. This technology has several benefits, including lower costs and greater flexibility; however, it also comes with unique risks which require additional oversight. The Cloud Security Alliance released a whitepaper titled “Best Practices for Mitigating Risk in Virtualized Environments” in April 2015. This whitepaper noted 11 significant risks found in the virtualized environment.

Based upon our review, 70 of the 156 distributed servers are VMs. These 70 VMs are hosted on 13 physical servers. During our discussions with distributed personnel, we noted a general trend in the virtualization of servers across campus. As physical servers are meeting their end of useful life, many areas are looking toward virtualization as a cost-effective replacement. Without direct guidance establishing basic controls, it is probable security risks could exist without the Division’s knowledge.

Recommendations

The Division of Information Services should:

A. Maintain a complete list of distributed servers. Correct functionality issues within the application used to track distributed system assets, more clearly communicate what information is needed, add specific fields to request additional critical information, and establish procedures to ensure information recorded is complete and accurate.

B. Work with each distributed environment to address barriers which exist in an effort to consolidate physical machines to data centers. In instances where moving physical machines to data centers is impractical or inefficient, establish policies to ensure the distributed system machines are protected and the minimum physical controls required are in place.

C. Develop structured oversight through policy regarding the development and configuration of virtual machines to ensure risks are properly mitigated.

Management's Responses

The Division of Information Services provided the following responses:

A. Information Services will collaborate with distributed IT staff and IT Council to maintain a complete inventory of distributed servers. Information Services will make improvements to the distributed server inventory application to improve usability and data collection.

B. Information Services will work with the distributed IT staff and IT Council to address barriers that prevent physical machines from being housed in the University's data centers and to develop minimum physical controls standards.

C. Information Services will work with the distributed IT staff and IT Council to develop server configuration standards for virtual machines.

3. Informational Security

Security of the information stored on distributed servers is at risk due to a lack of vulnerability assessments performed, tested offsite backups of some systems, lack of documented disaster recovery plans, use of unsupported or under supported operating systems, and incomplete controls over virtual machines.

A. Vulnerability Assessments

Most distributed servers are not scanned for vulnerabilities on a scheduled basis. The Information Security Unit has various tools to scan servers for certain vulnerabilities, such as misconfiguration, defect or error in an operating system. We asked the Division of Information Services to complete scans of 2 servers selected based upon risk assessments. One server appeared to be well protected; however, the other server was misconfigured and access to folders containing restricted information was allowed to more users than necessary.

B. Backups & Disaster Recovery Plans

Procedures to backup electronic data stored on distributed machines are in need of improvement, and formal documented disaster recovery plans for each distributed environment do not exist.

We determined many machines are not being backed up at all, and some which are being backed up are not storing backups off-site or testing the data to ensure it is complete and reliable. Some distributed personnel cited cost and space barriers as reasons certain data was not being backed up. Further, we noted none of the distributed environments had documented a disaster recovery plan to guide users who may have never worked in their environment to recover all systems and data needed for continued operations in the event of a major disaster.

Backing up electronic data safeguards the University against viruses, equipment failure, physical damage to machines and theft. Failure to backup electronic data could cause significant interruptions in the learning environment or with the business operations of the University. Operating policy 12.07-12 requires, “Each department with separate information systems is responsible for developing and maintaining their own disaster recovery plan in consultation with the Information Security unit of Information Services.”

C. Unsupported/Under Supported Operating Systems

Some distributed servers are running unsupported, under supported, or soon to be unsupported operating systems (OS).

The OS is software installed on a device to manage all other associated hardware and software installed and facilitate various processes to ensure each portion of the system operates as it should. The developer of each OS determines how long general support and technical guidance will be provided. During the phase of general support, the developer provides access to new and existing maintenance updates/upgrades, security patches, bug fixes, etc. However, at the end of this phase, the developer is no longer making new updates, upgrades, patches or fixes to help the OS battle new problems. As a result, security risks begin to surface and the OS runs less effectively and is no longer as effective at protecting the user or the data stored on the device.

During our review of 156 listed distributed servers at June 30, 2019, we identified 7 servers listed with unsupported OS (no general support or technical guidance provided by developer), 4 servers listed with under supported only (technical guidance only) and 46 servers listed with OS which will become unsupported in 2020 (no general support, but technical guidance still available at June 30, 2019). With the ever changing threat of cybersecurity, running unsupported OS creates a significant risk to University systems and data.

D. Testing environments

Network isolation is not always used in distributed testing environments. Testing environments are used by various distributed personnel to develop, test and refine software applications needed for their operations. During the testing phase, the distributed personnel install and begin processing information in the application to determine its functionality, limitations, and methods to assist users in its use. At the time of installation, distributed personnel may not know the vulnerabilities existing within the software application and therefore, use of network isolation is critical to the protection of all other assets. This allows vulnerabilities to be addressed while protecting other information assets.

Recommendations

The Division of Information Services should:

A. Complete vulnerability assessments of distributed machines on a periodic basis. The Division should communicate all risks identified and ensure corrections are made to safeguard university assets.

B. Work with distributed environment staff to remove barriers related to backups, ensure backups are completed on a scheduled basis, ensure backups are tested and stored off-site, and require formal documented disaster recovery plans to be filed with the Information Security Unit.

C. Require all machines to update to a supported operating system. If it is determined a machine cannot be updated, the Division should take steps to isolate these machines from the rest of the University network.

D. Require network isolation be established for testing environments.

Management's Responses

The Division of Information Services provided the following responses:

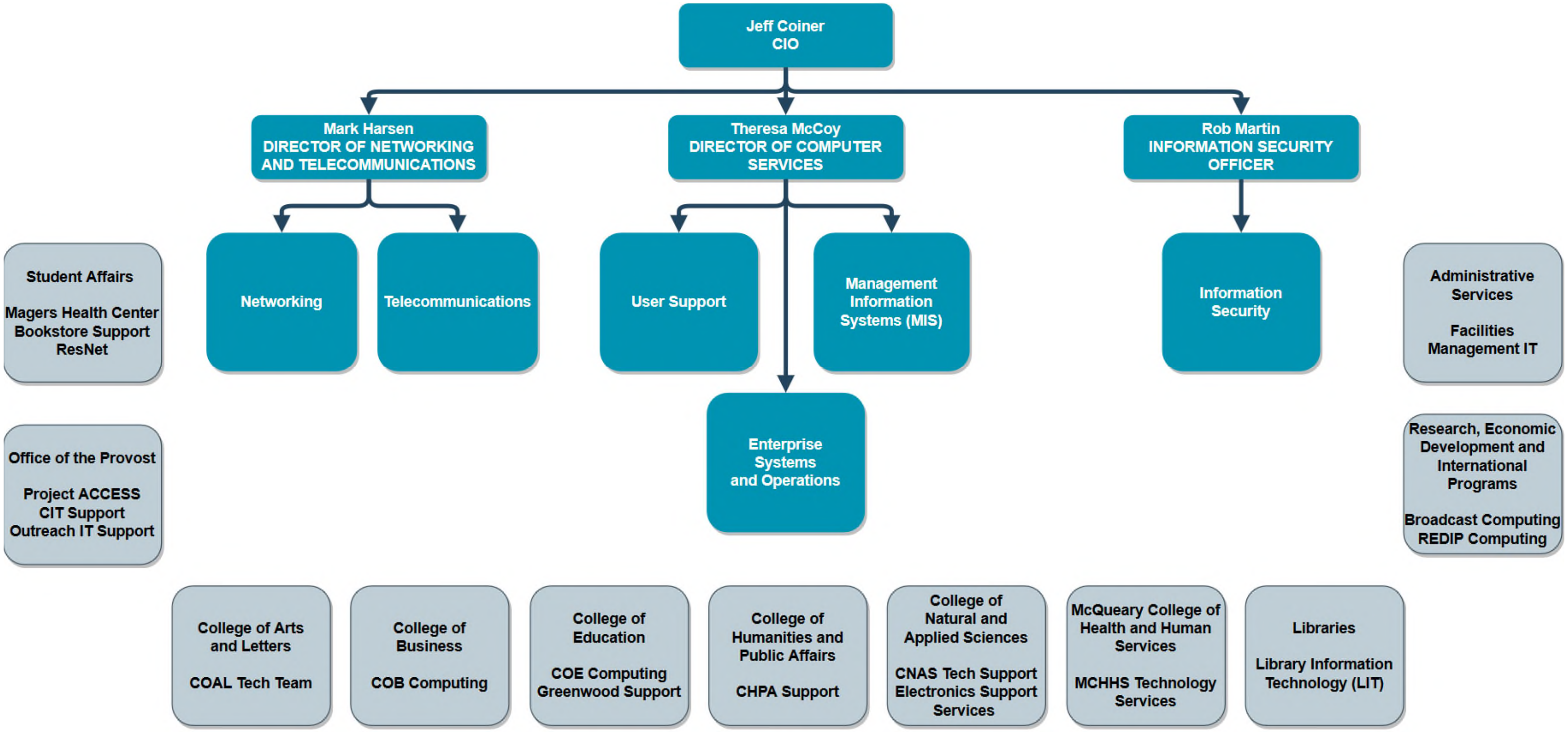
A. Information Services will periodically conduct vulnerability scans of all servers registered in the distributed server inventory application, and notify distributed IT staff of items that need to be addressed.

B. Information Services will work with the distributed IT staff to identify critical servers that are not backed up and develop a solution to resolve the issues. Information Security is updating the Disaster Recovery Plan for core systems and services, and will work with the distributed IT staff to assist in the development of their respective DR plans at their request.

C. Information Services will work with distributed IT staff and IT Council to develop a process to identify and remediate any non-conforming server operating systems

D. Information Services will work with distributed IT staff and IT Council to ensure test environments are separated from critical IT resources.

Distributed and Centralized Information System Organization Chart



Jeff Coiner
CIO

Mark Harsen
DIRECTOR OF NETWORKING AND TELECOMMUNICATIONS

Theresa McCoy
DIRECTOR OF COMPUTER SERVICES

Rob Martin
INFORMATION SECURITY OFFICER

Networking

Telecommunications

User Support

Management Information Systems (MIS)

Enterprise Systems and Operations

Information Security

Student Affairs

Magers Health Center
Bookstore Support
ResNet

Office of the Provost

Project ACCESS
CIT Support
Outreach IT Support

Administrative Services

Facilities Management IT

Research, Economic Development and International Programs

Broadcast Computing
REDIP Computing

College of Arts and Letters

COAL Tech Team

College of Business

COB Computing

College of Education

COE Computing
Greenwood Support

College of Humanities and Public Affairs

CHPA Support

College of Natural and Applied Sciences

CNAS Tech Support
Electronics Support Services

McQueary College of Health and Human Services

MCHHS Technology Services

Libraries

Library Information Technology (LIT)