FIU | FLORIDA INTERNATIONAL UNIVERSITY

Office of Internal Audit

Audit of University's IT Network Security Controls

Report No. 15/16-02

September 29, 2015

FIU | FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT

Date: September 29, 2015

To: Robert Grillo, Vice President and CIO, Division of Information Technology
Maria-Rosa Drake, Director, IT Network Services and Telecommunications

From: Allen Vann, Chief Audit Executive

Subject: **Audit of University Network Security Controls, Report No. 15/16-02**

Pursuant to our approved annual plan, we have completed an audit of the University's Information technology (IT) Network Security Controls. The primary objective of our audit was to determine if the University's IT network security controls and procedures adequately protect the confidentiality, integrity, and availability of the University's sensitive and/or critical data in transit.

Overall, our audit identified areas where FIU has opportunities to strengthen network security particularly in reducing access privileges, coordinating and formalizing threat identification and mitigation processes, and performing risk assessments. Cybersecurity is not the sole responsibility of the Division of Information Technology but requires the cooperation of the end users in the various departments, particularly their Information Technology Administrators. Accordingly, well-designed centralized security system controls are only as effective as the prevailing governance structure permits. Management agreed to implement the 13 recommendations in this report.

I would like to take this opportunity to express our appreciation for the cooperation and courtesies extended to us during this audit.

Attachment

C: Albert Maury, Chair, FIU Board of Trustees
Gerald C. Grant, Jr., Chair, FIU Board of Trustees Finance & Audit Committee
FIU Board of Trustees Finance & Audit Committee Members
Mark B. Rosenberg, University President
Kenneth Furton, Executive Vice President & Provost
Kenneth A. Jessell, Chief Financial Officer and Senior Vice President
Kristina Raattama, General Counsel
Javier I. Marques, Chief of Staff, Office of the President

TABLE OF CONTENTS

OBJECTIVES, SCOPE AND METHODOLOGY

Pursuant to our approved annual plan, we have completed an audit of the University's Information technology (IT) Network Security Controls. The primary objective of our audit was to determine if the University's IT network security controls and procedures adequately protect the confidentiality, integrity, and availability of the University's sensitive and/or critical data in transit.

During the audit, we observed and tested current practices and processing techniques, interviewed responsible personnel and tested selected transactions on the University's main network. Sample sizes and transactions selected for testing were determined on a judgmental basis. Audit fieldwork was conducted from January 2015 to June 2015.

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* using a risk-based methodology. To accomplish specific Information Technology (IT) control objectives, we applied a governance, risk and compliance framework, which utilizes the *Control Objectives for Information and related Technology (COBIT) 5.0 Framework, Special Publication 800-53A Revision 4 Assessing Security and Privacy Control in Federal Information Systems and Organizations, and the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity version 1.0 dated February 12, 2014*.

Though this was the first internal audit of the University's IT Network Security Control, there were prior internal audit recommendations related to the scope and objectives of this audit requiring follow-up. There were no external audit reports issued during the last three years with any applicable prior recommendations related to the scope and objectives of this audit.

BACKGROUND

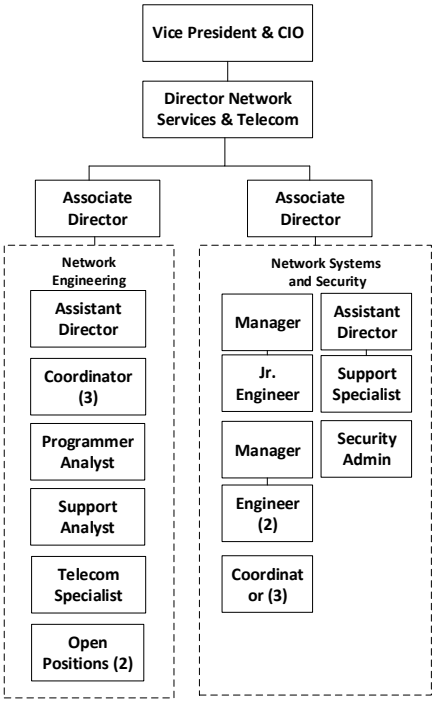
On October 28, 2014, FIU was awarded the Cybersecurity Leadership and Innovation Award by the Center for Digital Government. FIU was recognized for its commitment to data security. The award may be attributed to the University's network security systems maintained by a Network Engineering group and monitored by the Network Systems and Security group. The Network Engineering group maintains the required switches and routers necessary for network security. In turn, these devices are monitored by the Network Systems and Security group. The devices and systems include DNS[1] servers, load balancers, firewalls, intrusion detection systems and the Security Information and Event Management[2] device. Use of the security devices allow the Network Systems and Security group to determine which device is on the network, the amount of network bandwidth transmitted, whether the device's transmitted data is allowed to proceed through the network, and if the data transmitted presents a threat to the network.

Cybersecurity is a collaborative effort between the University's centralized IT services and the end users in the various departments. The Network Systems and Security group provides security tools to the local business units. One security tool, Data Loss Prevention (DLP), identifies which device is transmitting sensitive data. Additionally, local units Information Technology Administrators are alerted of threats identified through the Intrusion Protection System (IPS). Depending on the threat, the IPS either immediately stops the data transmission or alerts the Network System and Security Engineering of its existence. If further clarification is required, the business unit examines the device to determine whether there is a threat to sensitive data.

Personnel

The Network Engineering and Network Systems and Security groups are units of the Network Services and Telecommunications Department within the Division of Information Technology. The two groups have a total of 8 and 12 employees, respectively.

FIU's Network Systems and Security staff size appears to be in line quantitatively with the three other Florida Universities that responded to our survey. UF said they had a team of 13 people devoted to network security, whereas FSU had nine staff and USF reported that they had seven people specifically devoted to network security. To the degree that our respective systems are more or less distributive likely impacts the right sizing of centrally devoted resources.



[1] Domain Name System translate computer names to IP addresses.
[2] The SIEM device analyses log files and identifies potential threat events.

FINDINGS AND RECOMMENDATIONS

Overall, our audit identified areas where FIU has opportunities to strengthen network security particularly in reducing access privileges, coordinating and formalizing threat identification and mitigation processes, and performing risk assessments. Cybersecurity is not the sole responsibility of the Division of Information Technology but requires the cooperation of the end users in the various departments, particularly their Information Technology Administrators. Accordingly, we found that FIU's well-designed centralized security system controls are only as effective as the prevailing governance structure permits. Furthermore, we have asked the Division of Information Technology to work with the operating units to address past security related recommendations we made that have not been satisfactorily implemented.

Our overall evaluation of internal controls is summarized in the table below.

INTERNAL CONTROLS RATING			
CRITERIA	**SATISFACTORY**	**FAIR**	**INADEQUATE**
Process Controls		**X**	
Policy & Procedures Compliance		**X**	
Effect		**X**	
Information Technology Risk		**X**	
External Risk		**X**	
INTERNAL CONTROLS LEGEND			
CRITERIA	**SATISFACTORY**	**FAIR**	**INADEQUATE**
Process Controls	**Effective**	**Opportunities exist to improve effectiveness**	**Do not exist or are not reliable**
Policy & Procedures Compliance	**Non-compliance issues are minor**	**Non-compliance Issues may be systemic**	**Non-compliance issues are pervasive, significant, or have severe consequences**
Effect	**Not likely to impact operations or program outcomes**	**Impact on outcomes contained**	**Negative impact on outcomes**
Information Technology Risk	**System controls are effective in mitigating identified data risks**	**System controls are moderately effective in mitigating identified data risks**	**Systems controls are ineffective in mitigating identified data risks**
External Risk	**None or Low**	**Medium**	**High**

According to the *National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Framework*) the following subsets of functional activities should be evident in any organizations efforts to secure critical data residing on its systems:

Function	Description of Essential Activities
1. Identify	a) Network devices should be inventoried and prioritized based on their criticality; b) The roles of the University's network security should be clearly communicated; c) Internal business unit's responsibilities should be adequately defined and properly aligned; and d) The likelihood and impact of threats should be adequately assessed.
2. Protect	a) Access controls to critical network devices incorporate the least privileges allowable to perform job duties and are properly segregated so that no one individual can compromise a critical process; b) All users are properly trained in network security awareness; c) Sensitive data is protected in-transit; and d) Critical devices are properly configured and the settings are backed up.
3. Detect	a) Thresholds are established to detect network irregularities; b) Continuously monitor the network for threats; and c) Threat events are communicated to the proper parties.
4. Respond	a) Appropriate steps are taken once a threat event has been detected; b) The threat event is properly identified and mitigated; and c) Improvements are implemented to mitigate the threats reoccurrence.
5. Recover	a) The recovery process for critical devices should be up to date; b) Network restoration activities are communicated to the affected units; and c) Lessons learned are implemented to improve the future recovery processes.

The areas of our audit observations follow the order of the functions described above.

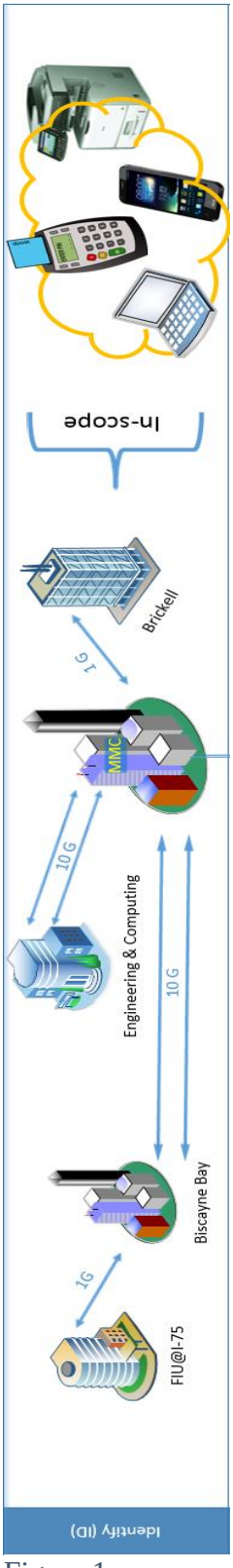


Figure 1

1. IDENTIFY

We examined existing controls' relating to the University's ability to identify network security risk to its systems through Asset Management, Governance, and Risk Assessment as described below.

a) Asset Management

To identify physical devices that contained sensitive data, we examined spreadsheets maintained by Network Systems and Security, Office of the Controller's Accounting and Reporting Services, and the Business Services Departments. The three Departments manage sensitive data in-transit via network devices, credit card machines, and Ricoh printers.

Network Systems and Security's spreadsheet reflect that they manage 568 Switches, 449 Uninterruptable Power Supply units, 93 Routers, 24 Firewalls, 23 Wireless Access Controllers, 4 Load Balancers, 4 Intrusion Detection and Protection Systems, 3 DNS Servers, and 1 Security Information and Event Management appliance. Based on their capabilities, connections and activities, 96 of the devices were self-identified as critical to the University's network security. Also examined were the lists of the Office of the Controller's 37 Point of Sale devices[3] and Business Services 20 Ricoh Printers that accept credit card payments.

The asset lists were stored on individual spreadsheets by each of the respective groups. The Office of the Controller and Business Services lists, however, were not shared with Network Systems and Security. If Network System and Security had access to the asset lists it could better assess the adequacy of network security controls for these devices. When the assets change, adjustments to network security can then be made by Network Systems and Security to mitigate the risk of unauthorized access to sensitive data that reside thereon.

b) Governance

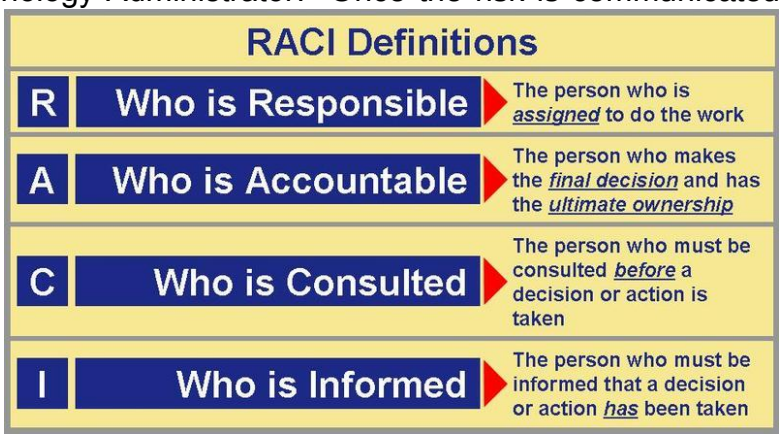
According to the Network Services Department, they provide leadership, guidance, and management of systems to help secure and protect the University's data and Information Technology resources. However, they believe it is the responsibility of each business unit to determine which firewall rules are appropriate for them.

In contrast, 4 of the 7 University department units interviewed stated that they relied on the Network Services Department to (1) know where data is and protect it, (2) provide training on network security, (3)

[3] Type of merchant accounts included IC Verify, mobile card reader, POS, and wireless terminals.

establish and manage network security policies, and (4) assist departments to become compliant and maintain network compliance. It was evident that Network Services Department does provide tools to protect data, security awareness training, and maintain network compliance. However, the University can do more in the area of developing policies and managing compliance. Also, there is a need to develop better communications with business units served so as to better understand each business unit's needs and expectations so as to reduce resultant security gaps.

While Network Systems and Security is responsible for monitoring the network security devices, we found that Intrusion Protection System (IPS) alerts are monitored in an informal manner. The IPS provides alerts of unusual traffic. For example, when FIU devices communicate with foreign countries, Network Systems and Security alerts the business unit's Information Technology Administrator. Once the risk is communicated there are no formal procedures that defines what needs to happen next, who is responsible to do it, who is held accountable, whose input needs to be solicited and how is everyone informed of the final disposition of the concern. The lack of a formal governance structure increases the security risk to the University's data.



c) Risk Assessment

The Network Systems and Security subscribes to 5 information sharing forums. One of the forums is the Education Network Information Sharing and Analysis Center that provides early warning threat advisories and promotes cybersecurity awareness within the Network Services Departments. Information received from forums such as the National Cybersecurity and Communication Integration Center (NCCIC) and the United State Computer Emergency Readiness Team (US-CERT) are communicated via an email group to the colleges and department units' 126 Information Technology Administrators. While the forums are used to identify risks, a formal comprehensive network risk assessment, which is an essential identifying function has not been performed.

A risk assessment would typically evaluate the control activities in high risk areas to ensure that network controls are effective in mitigating risks to the University's data. We noted high risk areas that included:

- Unsupported operating systems: According to FIU Policy No. 1930.020c *IT Security Procedure: System and Application Management*, all computers owned by the University, regardless of which operating system they use, must have current and appropriate operating system and application software patches applied. There were 249 Microsoft Windows XP endpoint devices that are no longer supported by the vendor still active on the network. According to the vendor,

Windows XP is five times more susceptible to viruses and attacks. Endpoint devices' operating systems that are unsupported by the vendor no longer receive security updates to protect malicious software from traversing over the network.

- Non-expiring passwords: There were 822 active accounts that had non-expiring passwords, including 9 individual and 23 test accounts. Over a period of time, the accounts can be compromised.

Recommendations

The Division of Information Technology should:	
1.1	Work with the various units to ensure that it receives notification of any changes to device inventories, especially payment card devices.
1.2	Work with senior management to enhance policies so as to provide for stronger centralized authority over the implementation of security controls and ensure that business units understand their responsibilities.
1.3	Perform periodic formal system-wide security risk assessments.

Management Response/Action Plan:

1.1 The Division of IT will work with the units, particularly Controller's Office and Business Services, to request they keep us informed of changes to device inventories.

Implementation date: June 2016

1.2 Policy revisions providing for stronger centralized authority are planned for implementation this fiscal year. That said, and as the report alludes, many of FIU's fundamental distributed IT security challenges are controlled via current FIU policy. The division believes the risks we find on the FIU network are primarily rooted in lack of resources in our distributed model, and the desire for organizational independence. We will continue to communicate to the units our IT security policies as they are updated.

Implementation date: June 2016

1.3 The Division of IT will be performing periodic security risk assessments. Risk Assessments will be done first in areas of higher risk.

Implementation date: August 2016

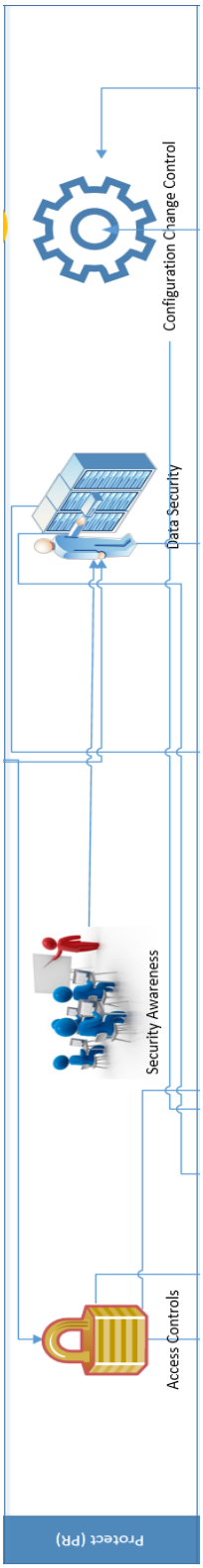


Figure 2

2. PROTECT

We examined whether existing security controls adequately safeguard sensitive/critical data residing on the network infrastructure. We focused on FIU's ability to limit the impact of potential network security events by evaluating its Access Controls, Security Awareness, Data Security, and Configuration Change Control processes.

a) Access Controls

According to COBIT 5.0 Deliver, Service and Support (DSS) 05.04.01 and DSS06.03.03, user access privileges should be allocated and maintained based on what is only necessary to perform their job activities, business functions and process requirements. Access may be controlled by the AAA[4] server or directly at the device level.

Our testing revealed that the Associate Directors of the Network Services Network Engineers and Network Systems and Security had Administrator privileges to 78 of the 96 critical devices. Additionally, the Director of Telecommunications had administrator privileges to 3 of the 96 devices. Directors typically should approve changes to devices but not necessarily perform the specific tasks themselves.

Administrator access was also found on:

- 21 devices that contain an active terminated user account.
- 11 devices with generically-named user accounts.
- 7 devices with user accounts not listed in active directory.
- 5 devices that include the Systems Programming Manager from the School of Computing and Information Sciences.

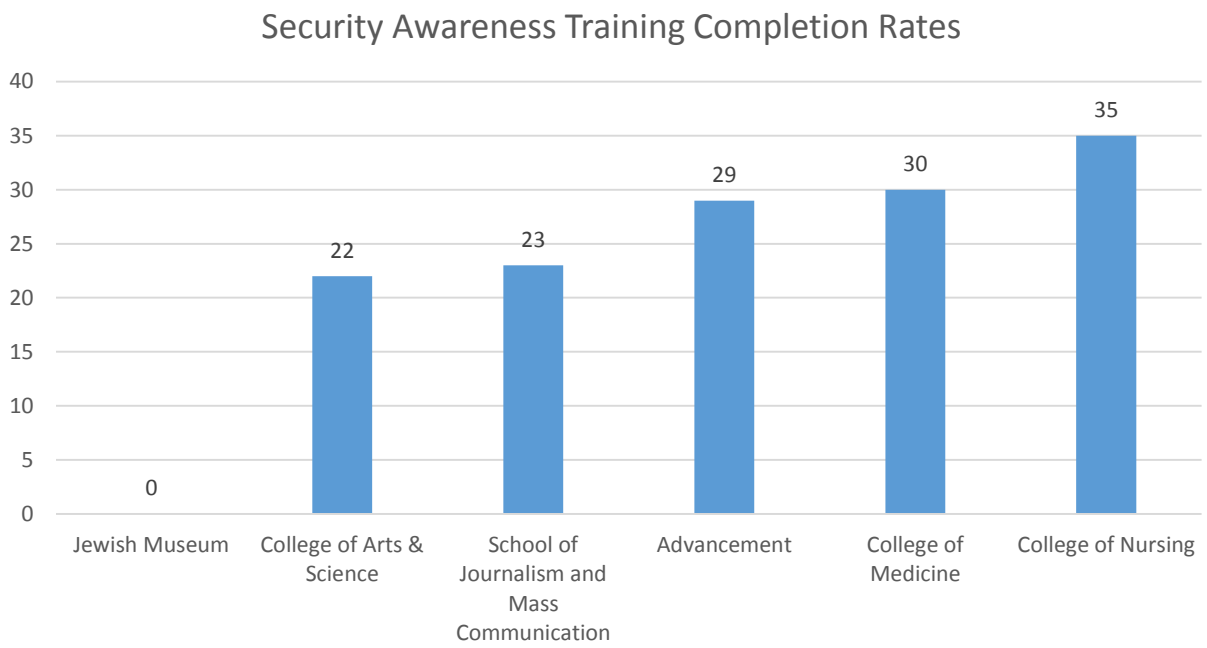
Strengthening Least Privileged Access controls along with disabling the account listed above reduces the likelihood that an inappropriate data change can be made.

b) Security Awareness

On March 20, 2014, the Vice President of Information Technology and CIO asked the entire Faculty and Staff to take part in an online security awareness training program. The training module instructed network users on IT related policies and procedures, their own responsibilities in identifying and protecting sensitive data and how to prevent their loss or unlawful disclosure. As of January 2015, only 51% of the University's employees completed the online security training. Though monthly

[4] Network Authentication, Authorization and Accounting.

reminder emails were sent by the Information Technology Security Office, 6 of the 40 Units still have a completion rates of less than 36%.



The low completion rates increase the risk that University personnel do not know and or may not appreciate how important it is to the University to maintain the confidentiality of sensitive data and appropriately secure it from loss.

c) Data Security

The Network Services Department risk strategy uses a layered approach to protect the University's sensitive data in-transit. Depending on the data type, it is segregated through

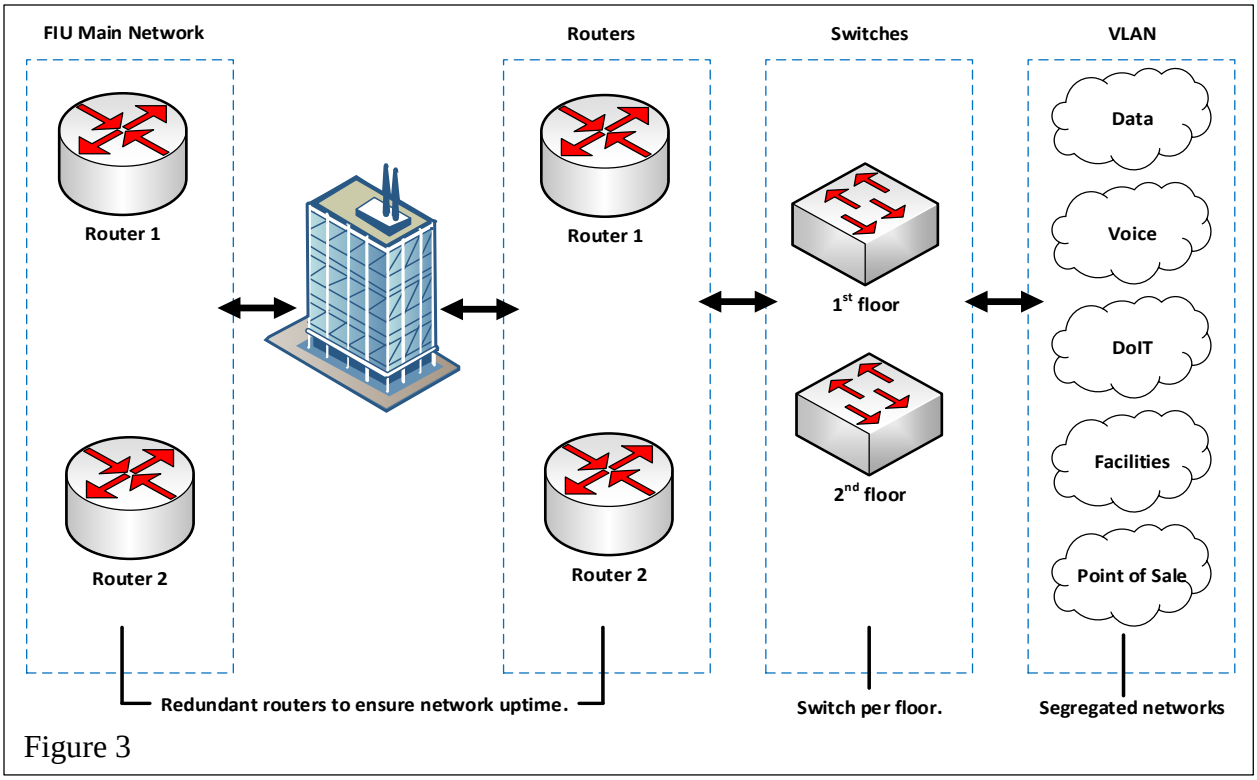


Figure 3

specific VLANs[5]. Redundant devices maintain network uptime and Intrusion Protection Detection and Data Loss Prevention Systems monitor the network. According to Network Services, University buildings are connected to the main network by redundant routers that provide data to each floor's switch. Data is then sent to a specific VLAN based on the devices IP address. See Figure 3 above.

Point of Sale:

The Point of Sale VLAN is the only network that has specific rules to protect credit card data from traveling on open networks while in-transit. There are 13 buildings throughout the University that have Ricoh printers. Students can pay by credit card or their FIU OneCard on the Ricoh printers. Of the 19 Ricoh printers examined, none were transmitting payment information on a Point of Sale VLAN.

Additionally, 6 of 37 Point of Sale locations used cell phone or PC based computers to transmit credit card data. Point of Sale computers that are used for other purposes, such as email and web browsing, may become infected by malware through phishing and spam attacks. By not transmitting sensitive credit card data over

[5] Virtual Local Area Network

separate VLANs unnecessarily increases the risk of unauthorized access to sensitive data and the PCI compliance risk to the University's network.

SSL Certificates:

Sensitive data transmitted via the Internet is encrypted through the Secure Socket Layer (SSL) protocol. SSL certificates (1) encrypt the data and (2) verifies the server's identity. Checking the server's SSL certificate helps ensure that the data is going where it is supposed to be and not to an unauthorized location. Though the data is still encrypted, 2 of the 53 unique SSL certificates had expired. Without a valid certification, expired sites may become exploited by a man-in-the-middle attack. Another danger of expired certificates is that it will train uninformed users that it is acceptable to click through an expired certificate, which increases the risk of URL exploits.

Wildcard certificates:

A wildcard certificate allows the verification process to be valid for multiple machines. Wildcard certificates are used by the Windows, Engineering, Network Management Services, and Web Communication Departments. Since wildcard certificates are used by multiple domains, the servers also share the same vulnerabilities to SSL exploits. One such SSL exploit is the use of obsolete TLS 1.0 cryptography that could allow an attacker to decrypt encrypted traffic. In addition, the Network Services Department may not be informed which servers have applied the wildcard certificates. Discontinuing the use of Wildcard certificates would reduce the risk to sensitive data in-transit.

d) Configuration Change Controls

Each of the 24 critical firewalls identified by Network System and Security contain thousands, if not tens of thousands of rules. They receive countless rule requests thru their email group where one of the team members then implements the requested changes. We examined 38 rule request changes, which included open ports requests for windows shares, VPN and MSSQL connections. In examination of the 38 firewall rule requests, we noted that:

- 29 did not explain the purpose or justification for the request change.
- 3 rulesets were implicitly based on other devices.
- 1 temporary request did not contain an end date.

We found that firewall rules are not periodically reviewed. There is no readily available information on how many rules exist. For example, for one of the 24 critical firewalls Network Systems and Security was able to identify 23,573 rules. These rules as stated earlier, allow for server to server communication, open secure VPN connections to internal devices, and MSSQL ports connections. We asked Network Systems and Security to identify the number of inactive rules on that server. From their test, it was determined that 4,184 (17%) of the rules were not active. There are likely thousands of inactive rules on the other 23 critical firewalls that were not tested. Having thousands of

inactive rules that are no longer needed on firewalls and the related ports they reside on, provide unnecessary potential entry points for attacks.

IPS and ePO system rules were automatically updated through software and security checks on a daily basis by their vendors. Network Services uses a 3rd party application to save the current configurations for 536 devices in the event that they need to be replaced. The backup application checks the devices every 60 minutes for any changes to their configuration. The automated configuration files are adequately updated and backed up.

Recommendations

The Division of Information Technology should:	
2.1	Review privileged user accounts to ensure terminated account are disabled; senior management administrator access is disabled; and staff access is limited to the least necessary to perform their job duties.
2.2	Continue to work with senior management to increase participation in security awareness training.
2.3	Ensure credit card data is transmitted on a secured VLAN.
2.4	Discontinue the use of unnecessary wildcard certificates.
2.5	Review all critical firewalls and at a minimum disable all non-active rules.

Management Response/Action Plan:

2.1 The Division of IT will review user accounts to ensure that terminated accounts are disabled and that senior management administrator access is disabled. Due to the dynamics and nature of our business, the current staff access is adequate to ensure continuous operations and troubleshooting as needed.

Implementation date: January 2016

2.2 The Division will continue to improve the quality of the material, making it easier, more convenient and more relevant for users. We will also continue to incent management to encourage their community to participate.

Implementation date: June, 2016

2.3 The Division of IT is placing new Point of Sales (POS) devices on POS vlans as we are being notified. However, there are several instances where credit cards are being accepted without the knowledge of the Division of IT and the Controller's office.

Implementation date: December 2015

2.4 The Division of IT will discontinue use of wildcard certificates where applicable.

Implementation date: December 2015

2.5 The Division of IT will define a process to regularly review and disable firewall rules that have not been used.

Implementation date: December 2015

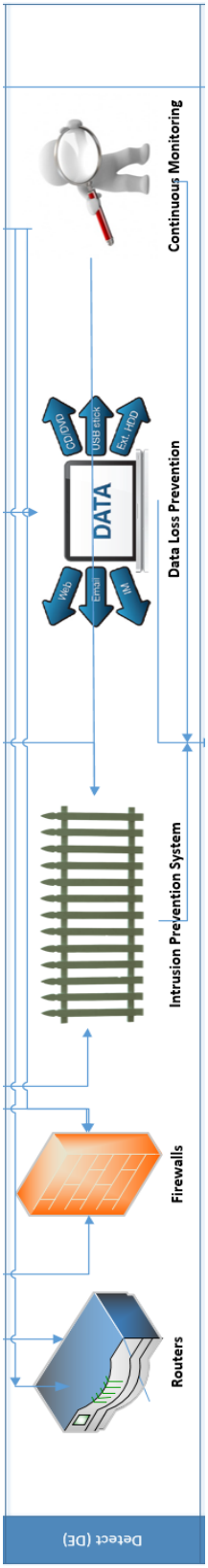


Figure 4

3. DETECT

We evaluated whether Network Services adequately identifies the occurrence of network security events in a timely manner. The functional controls we examined include Anomalous Events and Continuous Monitoring.

a) Anomalous Events

A data flow baseline has been established to monitor the network for abnormalities, including unusual spikes in data traffic. The IPS malicious activity thresholds are automatically provided by UTS' IT security vendor. It is deployed on a daily basis. The IPS contains 7,161 total rules to identify abnormalities that could impact the network. Though most of the rules are automatically created by the vendor, there were 27 rules informally activated by Network System and Security. A more formal review and approval process would strengthen the process by decreasing the likelihood that a harmful rule is implemented.

In addition to the IPS, the McAfee ePO reporting dashboards provide for the monitoring of identified threats in real-time. In particular, the Threat Monitor Dashboard permitted the Network Systems and Security Engineering Department to identify specific computers that were a risk to the network. Data Loss Prevention software is also used to monitor the data transmission of specific personally identifiable information. Electronic reports detailing the event are automatically sent to the business unit's Information Technology Administrator for their review.

b) Continuous Monitoring

The network is continuously monitored by Network Systems and Security through the Intrusion Prevention System and vulnerability scanning tools to detect potential security events. With the recent inclusion of prior ITSO staff, vulnerability scans are now performed by Network Systems and Security. Prior to the move, the Department was not informed of vulnerabilities identified by the scans. The scan reports help the department focus on the most critical vulnerabilities by providing risk ratings based on the vendor's vulnerability scoring algorithm. Presently there are 19 vulnerability scans automatically performed on either a weekly, biweekly, or monthly schedule. Nine of the 19 scans are departmental scans, which represents only a 14% participation rate of the University's business unit population that receive Data Loss Prevention reporting. In the past a passive approach to vulnerability scans participation was taken, as scans were only performed on units that requested it. With vulnerability scanning now being performed by

Network Systems and Security, a proactive approach to attain greater unit participation rates would likely increase the effectiveness of continuous monitoring.

Recommendations

The Division of Information Technology should:	
3.1	Formally review and approve IPS rules that are made by its Network Systems and Security unit.
3.2	Work with the business units to increase vulnerability scan participation.

Management Response/Action Plan:

3.1 The majority of the IPS rules are signature based which are automatically downloaded to the IPS by the manufacturer as they discover new vulnerabilities. In some occasions the Division of IT does create custom IPS rules in order to address certain vulnerabilities specific to our environment. A process will be defined to review manually created rules.

Implementation date: January 2016

3.2 The Division of IT has started to increase the areas scanned for vulnerabilities. Areas of higher risk are being addressed first.

Implementation date: December 2015

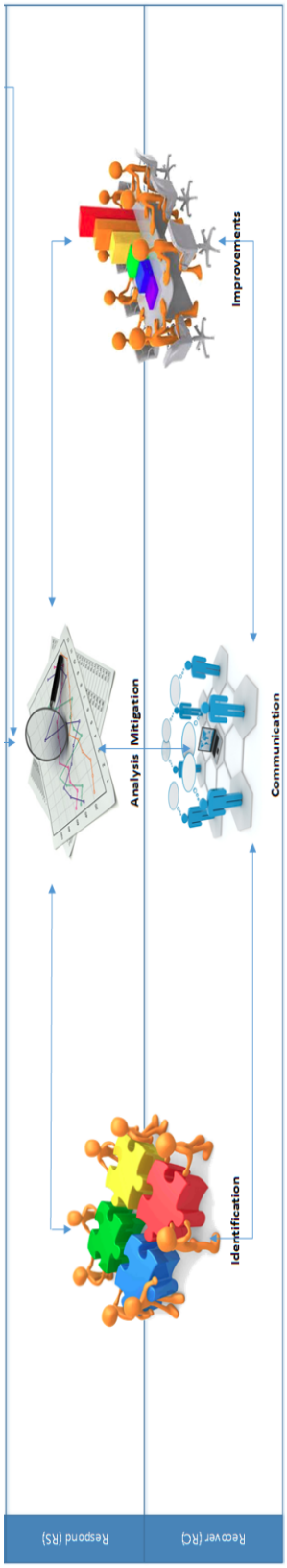


Figure 5

4. Respond

For the respond function, we determined whether appropriate actions are taken when a network security event has been identified. The impact of network security events is lessened by understanding the event, mitigating them, and learning how to avoid or handle a future event.

a) Identification

The FIU IT Security Incident Communication Procedures Manual requires that all security incidents be categorized in one of the three categories, as follows:

Level 1: Low volume impact and no data breach.

Level 2: Service interruption and no data breach.

Level 3: Sensitive data breach or threat to University.

For example, when a Level 1 system compromise incident is identified through network monitoring, an email is sent to the local Information Technology Administrator within 24 hours. If the incident is determined to compromise sensitive data, then the incident would be escalated to Level 3.

Based on the documentation provided by Network Systems and Security, there were no to dates to determine when the event was triggered by the security monitoring controls. Without an event date, management is unable to determine if the Information Technology Administrator was notified in a timely manner or how long the threat has been active on the network.

In April 2015, an EPO Incident Response Process was implemented by the Network Services Department to address the process after the Information Technology Administrator is notified of a network security detection. The process covered threats and infected files of the affected endpoint devices.

At the time of our fieldwork, the process generated 9 case files: 3 were closed and 6 were open. The closed case files adequately documented that one computer had recurring viruses, the second was low risk, and the third device had an offending application removed. However, 4 of the 6 open case files did not contain information about the event. The case files also did not include a lessons learned review of events. Lack of this information reduces the effectiveness of formally tracking IPS, DLP and other continuous monitoring initiatives. Thus, this reduces the monitoring

controls ability to ensure a timely and complete response to a network detected event. Fully documented case files and lessons learned reviews increases management's ability to make improvements to the network security controls.

b) Analysis / Mitigation

Per the IPS Incident documentation examined, the Information Technology Administrator notified of the security event is expected to determine whether the compromised device contained sensitive data. The documentation suggests the easiest way for this to be done is by inquiry i.e., asking the user if they store any sensitive information such as social security numbers, names, and date of birth on their computer. However, an inquiry by itself does not adequately analyze the device's actual threat level. Additional proactive measures can be taken by Network Security, such as, scanning the device using Data Loss Prevention tools to determine whether the device contains sensitive data. The use of security tools by the Network System and Security increases the likelihood that the security incident level is correctly identified.

In January 2015, the Security Information and Event Management (SIEM) device was implemented to correlate logs from the IPS, ePO, Border Routers, and Data Center firewalls. This allows the Network Services Department to analyze the current threat landscape in a holistic manner. Management stated that currently 45 of the 96 critical devices provide logs to the SIEM system and that adding 14 devices would increase the SIEM effectiveness to alert them of threats to the network. However, they believe that the remaining 37 devices would not add a quantifiable improvement to the SIEM. In the past each network security incident reported or identified was reviewed as an isolated incident, but the Network Services Department was unable to track how many incidents occurred during a period of time or the number of incidents handled. Formal tracking of network security detected incidents reduces the risk to the network's data. The anticipated plan is to connect the Security Information to the Remedy tracking system to formally track each security incident.

Recommendation

The Division of Information Technology should:	
4.1	Formally track and review network security events identified by the detection controls and perform lessons learned with the affected Information System Administrator.

Management Response/Action Plan:

4.1 Security Events are currently being tracked through internal case functionality on the SIEM as well as through Remedy. The Division of IT does communicate with the end user or IT Administrator throughout the process. Depending on the incident, the Division of IT will perform a debrief with the user or IT Administrator.

Implementation date: Immediately

5. Recover

We wished to determine whether appropriate controls for network resilience have been implemented. The Recover function supports timely recovery of network operations through the planning, communication, and improvements activities.

a) Planning

The Network Service Department has two manuals: Disaster Recovery Plan and the FIU Ready Continuity Plan, which are used for network security planning. Also, in the event of a switch failure, four standby units are available as replacements to minimize downtime.

Disaster recovery tests were performed on November 14, 2014 and November 16, 2014, which covered five PantherSoft modules and the MyAccounts central authentication system. The purpose of these tests were to demonstrate the FIU Division of Information Technology's ability to failover critical services in the event of an emergency from its main Data Center to the Disaster Recovery Site. The tests included 13 of the 96 critical network security devices. The Director of Network Services stated that 79 of the 96 devices were fully redundant and should failover transparently; however, the remaining 4 devices did not have recovery abilities. Ensuring that all critical network security devices have recovery procedures would reduce the overall risk to the University's data in the event of a disaster.

b) Communication

There were 21 project members involved in testing that included staff from the UTS Operations, UTS Support Center, UTS Administration, PantherSoft, and the Network Services Department. Also included was the Director of Network Services who informed the CIO on the Disaster Recovery Plan test results. The test results were adequately communicated to internal stakeholders and management.

In July 2014, an IT Alerts web page was created to notify IT Administrators of emergency outages, problems, routine maintenance and any schedule downtime events. An email is automatically sent to the IT Administrators that describes the type of event, who is affected and its current status. All 6 network IT Alerts examined during the audit period listed the issue, who was affected and were notified when it was resolved. The IT Alerts system provide adequate communication to internal users.

c) Improvements

A Lessons Learned section was included in the restoration testing documentation. The page document included what went well, challenges and mitigation methods, and what can be done better. Test feedback from the participants included staff from PantherSoft and Network Services. The section contained adequate information necessary to make improvements to the next Disaster Recovery Tests.

Recommendation

The Division of Information Technology should:	
5.1	Assess the four remaining critical devices and consider adding similar redundancies or include them separately in the Disaster Recovery Plan.

Management Response/Action Plan:

5.1 One of the critical devices has been decommissioned; two of them cannot have redundancy, but there are other mechanisms we can use if necessary for the same functions; the fourth one does have redundancy, however it was omitted from the list provided.

Implementation date: Immediately

6. Implementation of Prior Audit Recommendations

In prior audit reports of University user departments there were 12 network security related recommendations reported by management as completely implemented. Our examination of the completed recommendations included observation of actual processes, interviews with University personnel and testing of selected devices.

Overall, our examination revealed that 8 recommendations were fully completed and 4 recommendations were not completed. Though the recommendations were reported to us as completed, we found that vulnerability scans, File Transfer Protocol encryption, and firewall rule reviews were not performed. The test results for each prior recommendation examined are as follows:

University's Office of Internal Audit Report			
#	Recommendation	Implementation	
		Fully	Not
(2008/09-09) FIU Safeguards Over Credit Card Holder Data			
2.2	Develop a plan for isolating the cardholder data environment from the remainder of the University network.	✓	
3.3	Implement a formal process for approving and testing network connections and changes to firewall and router configurations.		✓
(2011/12-02) PantherCard Services Financial Information Systems Controls			
18.1	Define the frequency for reviewing exceptions to PantherCard traffic flow.	✓	
18.2	Perform a review of firewall and router rule sets every six months.	✓	
(2012/13-10) FIU Online Program			
6.1	Perform periodic vulnerability scans.	✓	
6.3	Work with the UTS Network Services Department to ensure that all folders and hard drives of the workstations are encrypted.	✓	

University's Office of Internal Audit Report			
#	Recommendation	Implementation	
		Fully	Not
(2012/13-11) Wolfsonian Museum			
10.2	Have the FIU Network Systems and Security Engineering department centrally manage all the Museum servers' antivirus.	✓	
(2013/14-07) HCN Billing, Collections and Electronic Medical Record Systems			
7.1	Review all firewall rule sets to ensure firewall rules are appropriate.	✓	
(2013/14-12) Frost Art Museum			
5.1	Ensure that the two endpoint devices are centrally managed by the UTS Network Systems and Security Engineering group.	✓	
7.1	Encrypt and limit the FTP connection to appropriate personnel.		✓
7.2	Periodically review firewall rule sets to ensure active connections are appropriate and adequately authorized.		✓
(2013/14-15) School of Computing and Information Sciences			
3.2	Establish periodic external vulnerability testing with the ITSO and work with the NSSE department to connect devices, where appropriate, to the University's IPS.		✓

Listed below are the recommendations determined to be not implemented accompanied by the results of our current observations.

Prior Recommendations Not Implemented:

1. (2008/09-09) FIU Safeguards over Credit Card Holder Data Recommendation 3.3 Implement a formal process for approving and testing network connections and changes to firewall and router configurations.

   Current Observation:

There is no formal process of approving or testing of network connections. However, network rules were implemented as per the department's request.

2. (2013/14-12) Frost Art Museum Recommendation 7.1 Encrypt and limit the File Transfer Protocol connection to appropriate personnel.

   Current Observation:

   The File Transfer Protocol connection was still unencrypted.

3. (2013/14-12) Frost Art Museum Recommendation 7.2 Periodically review firewall rule sets to ensure active connections are appropriate and adequately authorized.

   Current Observation:

   Firewall rules have not been reviewed.

4. (2013/14-15) School of Computing and Information Science Recommendation 3.2 Establish periodic external vulnerability testing with the ITSO and work with the NSSE Department to connect devices, where appropriate, to the University's Intrusion Protection System.

   Current Observation:

   Vulnerability scans have not been performed nor have devices been added to the IPS.

Recommendation

The Division of Information Technology should:	
6.1	Work with the effected business units to help them implement the cited recommendations.

Management Response/Action Plan:

6.1 The Division of IT will work with identified units to implement cited recommendations.

Implementation date: March 2016

Appendix A: FIU's Network Security Framework Diagram