LAC Minutes
October 2, 2018

Present:  John Evans, Shelia Gaines, Jill Green, Shanika Jones, Elizabeth McDonald, Irma Quinones, Joel Roberts, Perveen Rustomfram, Lee Slack

Absent:  Gail Barton, James Singleton

Guests:  Michael Harris, James Hudson, Anna Swearengen, Brannen Varner, Iesha Williams

1.  UL Employee Recognition – James Hudson
    The need for recognition of the accomplishments of University Libraries employees was presented to the council. The possibility of using the kiosk in the rotunda for announcing awards to employees was discussed as well as the reorganization of the LSSA.

2.  Deans and Directors Council – John Evans
    - The following documents were presented at the Deans and Directors Council on September 19:
      - INITIATIVE: Multi-Factor Authentication (MFA) and Security Awareness Training Expansion
      - Communities of Research Scholars (CoRS) Call for Proposals
      - By-Laws of the University of Memphis Research Council (Draft)
      - Reporting Business Related Automobile Accidents
    
    These documents are attached to the minutes.

    - Additional handouts for the No Stress Success Workshop Series, maker Mondays, NEDFLIX, SongWriting Workshop, NEDxStudents, and Acoustic Open Mic Night were distributed to the council.

    - Merit Pay Matrix
      In November, we are submitting information to the University on how merit pay was distributed in the past and how it will be done in the future. In the past, merit pay has been based on employees’ evaluation scores.

3.  Fine Amnesty Day – Shelia Gaines
    University Libraries will sponsor a Fine Amnesty Day on Friday, November 9, to help support the Tiger Pantry. Guidelines for this event are attached to the minutes.
4. Additional Agenda Items

Library Webpage for Events – Anna Swearengen, Greg Woods
A University Libraries webpage for tracking events was suggested. This webpage would include available space in the Libraries, instructions on use of equipment, and fees for moving equipment or cleanup. A more detailed proposal will be presented at a future LAC meeting.

Piano in the Rotunda – Lee Slack
The council discussed tuning the piano in the Libraries’ rotunda and if the piano might be affected by temperature changes in the rotunda. Joel Roberts indicated that since the piano was not on an exterior wall the temperature in the rotunda should not damage it.

Announcements

John Evans
- The Desktop Loan Policy and Liability Statements Agreement is available to UL staff and faculty for checking out older desktop computers. James Hudson developed this form so that this equipment could be available to library employees. Forms are in the Administrative Office.
- A set of flyers for upcoming events will be provided to each LAC council member at every meeting. Please use these to promote all of the events happening at the library.

Bess Robinson
We are trying to get the Friends of the Library organization going again. There will be a meeting on Friday, October 5, to discuss ways to increase membership and upcoming events.

Joel Roberts
- The Song Writing Workshop will be on Thursday, October 4, 6pm, in the Music Library.
- Acoustic Open Mic Night will be on October 25, 6pm, 2nd Floor Commons, McWherter Library.

Brannen Varner
Our first maker Monday went well. We had about 20 people attend. The next maker Monday is on October 22, 3pm – 4pm.

Meeting Adjourned: 10am
Minutes Finalized: October 11, 2018
INITIATIVE: Multi-Factor Authentication (MFA) and Security Awareness Training Expansion

Background

The University of Memphis IT Security, Identity Management, and Compliance team (ITSEC) has previously undertaken projects to deploy the Duo Account Security Multi-Factor Authentication product and SANS Securing the Human training program to provide additional security for those individuals that access to sensitive IT systems or data. While Security Awareness Training has been mandated for the last three years for any individual with access to Banner HR or Finance roles (as well as all IT employees), Duo has largely been left in an opt-in state outside of several specific departments. As the risk of social engineering through email phishing attempts and scams continues to rise, further adoption of Duo MFA and Security Awareness training is vital to lowering the risk of compromised user account credentials in our population.

Duo MFA

Multi-Factor Authentication, or MFA, is a method of authentication where a user is prompted for a piece of information or "factor" that only they possess in addition to their normal username and password. Examples of factors implemented by Duo include acknowledging a "push" message in the Duo mobile application, a PIN sent via text message to a user's mobile device, acknowledging a call on a desk/home/mobile phone, or a PIN number generated by the Duo application. ITSEC has currently enabled Duo support for any resource protected by the ITS Single Sign-On (SSO) system, including, but not limited to the myMemphis portal, Banner SSB and INB, as well as other application whose primary login occurs via the sso.memphis.edu login page. Currently, 545 individuals have enrolled in Duo.

As risks from malware, ransomware, phishing and other attack vectors increase, protection of data solely through authentication by username and password has quickly become ineffective. MFA safeguards against these threats by ensuring that an attacker who has compromised a user password is still unable to gain access to protected resources without possession of the additional factor.

Security Awareness Training

While technical controls such as Duo MFA can alleviate some of the impact of user account compromise, MFA alone cannot alter individual behavior to prevent account compromise from occurring in the first place. Security Awareness training can be effective in altering individual behavior if the program is designed in a way that promotes learning and retention, rather than simple compliance. In previous years, the program was designed around segmenting the population so that only high-risk users, defined as anyone having Banner Finance and HR access, were included and other users were not required to receive any training. This created a situation in which the required users questioned why they were mandated to receive the training, and other users who could have benefited from the program did not have access to the content. The segmentation, combined with the overall length of the training program, led to numerous faculty member complaints and the appearance of very low attention to the material. While the program achieved its highest level of completion compliance in FY 2018 (93% completion rate — 1102/1188), the number of complaints over previous years rose as well.
**INITIATIVE: Multi-Factor Authentication (MFA) and Security Awareness Training Expansion**

Members of the ITSEC team have identified multiple risks related to social engineering and compromised user credentials. Below are three of the risks identified, each of which can be mitigated by use of an MFA solution as well as a functional Security Awareness Training program:

<table>
<thead>
<tr>
<th>Threat</th>
<th>Impact</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial Access</strong></td>
<td>A high-level user account with finance access is compromised through phishing and is then used to transmit funds to an external entity through a wire transfer or other form of payment.</td>
<td>Medium</td>
</tr>
<tr>
<td><strong>Impact</strong>: Potential trigger of state breach notification, loss of funds, negative publicity, and damage to reputation potentially impacting student retention, student recruitment, and research grants.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Confidential Data Release</strong></td>
<td>A user account with access to restricted data is compromised through phishing and is then used by a remote attacker to steal bulk personally identifying information (PII) or research-related intellectual property ('P).</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Impact</strong>: Trigger of state breach notification, compensation/fraud monitoring for impacted individuals, negative publicity, lost market opportunity, and damage to reputation potentially impacting student retention, student recruitment, and research grants.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Account Escalation</strong></td>
<td>A user account without significant access to restricted data is compromised through phishing or other social engineering. The account is then employed by an attacker to send large numbers of phishing or scam emails to other accounts inside the University, bypassing external filtering and increasing the chance of a high-level user being compromised.</td>
<td>Medium</td>
</tr>
<tr>
<td><strong>Impact</strong>: Trigger of state breach notification, disruption of University day-to-day functioning, negative publicity, and damage to reputation potentially impacting student retention, student recruitment, and research grants.</td>
<td></td>
<td>Medium</td>
</tr>
</tbody>
</table>

**Recommendations**

Given the threats identified above and the risk they represent to the University, the ITSEC team recommends that all regular employees, defined as all faculty, staff and course instructors, should be required to use Duo MFA and participate in annual Security Awareness Training. As of current metrics, this population accounts for just under 4000 individuals at the University.

**Implementation**

Security Awareness Training: All regular employees will be required to complete a base security training program at least once every fiscal year covering the base topics of social engineering, phishing, and other critical cybersecurity topics. Employees will be given 4 months to complete the training, and metrics will be provided to
INITIATIVE: Multi-Factor Authentication (MFA) and Security Awareness Training Expansion

HR and other division leaders. New hires will be required to complete the training program at or shortly after onboarding. Additional training may be provided or required of other employee populations, depending on risk and job function.

Duo MFA: All regular employees will be provided an opt-in window to enroll in Duo MFA. If the employee does not enroll within the opt-in period, their account will automatically be enrolled in Duo and they will not be able to login to SSO-protected pages until they complete the enrollment process. ITSEC reserves the right to grant exceptions to the opt-in window depending upon the situation.

Timeline: ITSEC proposes an announcement of both required programs on Wednesday, October 17, 2018. Duo would be required for all new hires beginning on November 1, 2018 and for all existing employees by Monday, February 4, 2019. Security Awareness Training for FY2019 would require completion by Friday, February 1, 2019.

Included ECLS Codes: F9, FD, FA, CH, AD, AE, AM, AB, AF, -rs, TH, TR, TE, GA (if also GRI) Other: Sponsored Employee and Emeritus Faculty
The UofM Division of Research & Innovation is pleased to launch a new Communities of Research Scholars (CoRS) Program designed to cultivate new interdisciplinary discourse and nurture the growth of research affinity groups across campus.

We will award up to ten (10) CoRS start-up grants of $2,500 each to seed development of new communities. Funds will be available for 1 year to support activities that will result in a focused plan to pursue and secure support for ongoing research, scholarship, and/or creative activity and an organizational membership structure to enable ongoing community activities. Eligible expenses may include food for meetings; facilitators or external speakers; modest staff or hourly student support to assist with activities; or up to $500 in faculty summer support for the convener for activities directly related to the CoRS. Proposals must be submitted via e-mail to Researchdev@memphis.edu by Midnight, October 15, 2018.

Full details, including the proposal requirements, may be found here.

For more information, contact Mary Earheart-Brown, Sr. Associate Director for Research Development, at mary.earheart.brown@memphis.edu or x 491 1. Two question and answer sessions will be held to assist in proposal development. Email Researchdev@memphis.edu for details.
Call for Proposals to Establish Communities of Research Scholars (CoRS)

Program Description: The UofM Division of Research & Innovation is pleased to launch a new Communities of Research Scholars (CoRS) Program designed to cultivate interdisciplinary discourse and nurture the growth of research affinity groups across campus. These groups are created by faculty, for faculty, and are self-governing and self-directed within the framework of the program. Each ‘community’ will include faculty representing multiple disciplinary perspectives and research approaches with shared interests in exploring a common research theme. Each community is encouraged to involve research partners from area community organizations and other regional academic institutions as appropriate to the target theme.

Funds Available: We will award up to ten (10) CoRS start-up grants of $2,500 each to seed development of new communities. Funds will be available for 1 year to activities over that will result in a focused plan to pursue and secure support for ongoing research, scholarship, and/or creative activity and an organizational membership structure to enable ongoing community activities. Eligible expenses may include food for meetings; facilitators or external speakers; modest staff or hourly student support to assist with activities; or up to $500 in faculty summer support for the convener for activities directly related to the CoRS. At the end of the staff-up period, results will be evaluated, and selected Communities identified for further development support towards becoming new interdisciplinary research clusters or centers.

Proposal deadline: Midnight October 15, 2018 via e-mail to Researchdev@memphis.edu

Proposal Content: 1-3 page, single spaced document that includes:

1) The name of the convener: Who will be responsible for organizing and documenting the group's activities? This should be a tenured or tenure-track faculty member who will submit the Community's plan and membership structure at the end of the project period.

2) A description of your proposed topic: What is the thematic area of inquiry your group would like to explore? This could be something broad like water contamination, gender equity, poverty, climate change, alternative energy, or social media. It could also be a bit more focused, like childhood asthma or undergraduate STEM retention.

3) The Community of Scholars to be involved: This is more than providing a list of names and departments. We are looking for involvement from 5-10 faculty who will bring different disciplinary perspectives or approaches to the conversation. Identify these faculty and the perspective/interests each brings to the table. Everyone identified should be copied when you email the proposal, so we know they are invested.

4) Description of the novelty of the idea: We are interested in supporting new communities and new conversations, not simply adding a person or two to a group of people who have previously worked together. In this section, help us understand what is new or different about the Community you are proposing and how it will bring together people and perspectives who have not previously interacted. The more interdisciplinary the community is, the better. To the greatest degree possible, we want to see artists, engineers, and educators or philosophers, lawyers, and nurses, etc. talking to each other around an area of shared interest and scholarship.

Evaluation, Award Notification, and Project Start Date: We will notify recipients on or before November 1, 2018, and your start date will also be November 1st.
Have questions about how to prepare your CoRS proposal? We are holding two question and answer sessions to assist you in developing your proposal. The sessions are voluntary and will be informal.

Session 1:
Friday, September 28, 2018
Fed Ex Institute, Room 203/205
2:00-3:00 pm

Session 2:
Wednesday, October 3, 2018 Fed
Ex Institute, Room 225
12:00 pm-1:00 pm

For more information, contact Mary Earheart-Brown, Sr. Associate Director for Research Development, at mary.earheart.brown@memphis.edu or x491 1.
BY-LAWS OF THE UNIVERSITY OF MEMPHIS
RESEARCH COUNCIL (Draft)

ARTICLE 1 NAME
The name of this council shall be the University of Memphis Research Council (UMRC).

ARTICLE 11 OBJECT
The UMRC is the primary liaison between faculty researchers and university leadership on all issues related to our research environment, research policies, research compliance and strategic research directions. The UMRC serves in a consultative role and reviews research and compliance policies, contemplates growth opportunities, identifies areas of excellence, catalyzes crossdisciplinary and trans-institutional collaborations, and unifies divergent goals and objectives of local research and exploration thrusts with institutional mission and priorities. In the spirit of faculty governance, it also serves as an important feedback loop for the University's research efforts. Members of the Council also help to promote research discourse at the local level and serve as local champions for research in their respective units.

ARTICLE 111

Section 1: REPRESENTATION
The UMRC which will be comprised of 36 faculty member representatives as follows:

- Associate Dean(s) for Research or designees from the University's Colleges or Schools, appointed to 2 year terms by the respective Deans: o College of Arts and Sciences, o College of Communications and Fine Arts, o College of Education, o Fogelman College of Business and Economics, o Herff College of Engineering, o Lambuth Campus, o Cecil C. Humphreys School of Law, o Loewenberg College of Nursing, o Kemmons Wilson School of Hospitality and Resort Management, o School of Communication Sciences and Disorders, o School of Health Studies, o School of Public Health, and o University College.
- Three (3) representatives nominated by the President of the Faculty Senate for 2 year terms.

The rules contained in the latest edition of Robert's Rules of Order Newly Revised shall govern the UMRC to the extent that they are not inconsistent with these bylaws or with any special rules of order the UMRC may adopt.

Section 2: OPEN MEETINGS
Meetings of the UMRC are open to all faculty members. If confidential issues are on the table, then the chair has the right to call the UMRC into executive session.
ARTICLE vul - AMENDMENT TO BYLAWS

These bylaws can be amended at any meeting of the UMRC by a two-thirds vote, provided that the amendment has been submitted in writing at the previous regular meeting.

ARTICLE rx APPROVAL

All motions and actions of the UMRC will be subject to approval by the EVP for Research & Innovation and the President of the University.
The State of Tennessee has implemented a new procedure for reporting business-related automobile accidents.

Effective immediately, any UofM employee, volunteer or student involved in an automobile accident while on official business, whether driving a state-owned, rental or personal automobile, must report the accident to the State of Tennessee Auto Accident Call Center immediately, while on the scene, at 855.253.0629 and follow the instructions below.

1. Do not leave the scene. Be prepared to communicate ALL details of the incident to the state's call center representative.
2. Call emergency services (911 or police non-emergency number) as needed.
3. Take at least four photos of both vehicles, license plates, parking situation, insurance card of other party and any notable unrelated damages. Enclude photo of the other party if applicable.
4. Call the State of Tennessee Auto Accident Call Center at 855.253.0629 to immediately report the incident. Then call your supervisor and follow your department's applicable procedures.
5. Do not admit fault in the accident or promise coverage or reimbursement to anyone.

Department heads must ensure:
1. Both the Accident Reporting Instructions and a Damage Notification Card are placed and maintained in their department's University vehicles, and
2. Employees or students that may operate a vehicle for official University business must receive Auto Accident Reporting Training, available online through Learning Curve.

More information is available at http://www.memphis.edu/vehicles. Any questions should be directed to the Finance Office at FinanceOffice@memphis.edu.
Fine Amnesty Day Proposal for Circulation

LAC, October 2, 2018

A flyer will be created and handed out at the desk, shown on the lobby screens, and posted to other appropriate campus news networks.

Suggested Dates

Friday, November 9th

Friday, April 12th

Students must make a minimum one item donation from the list and must have the book and the donation with them at the time.

Tiger Pantry suggested that since donations will be coming from students that we should stick to:

Non-perishable food item donations

Pasta, Pasta Sauce
Soup
Macaroni & cheese
Cereal
Oatmeal
Canned beans
Granola bars, breakfast bars

Peanut butter & jelly
Rice
Canned protein (chicken, tuna)
Salt & pepper
Fruit Cups, canned fruit
Snack crackers

We will only waive current fines less than $7.50 that have not already been charged to the students' accounts. This essentially means that the books must be less than 30 day late. No replacement fees will be waived.

Questions

Does this have to go through legal?

Is this a good time to have library staff make some donations to Tiger Pantry?
Other questions/concerns?