College/Division Administrator Meeting
Room 302, Melcher Hall
January 10th, 2019 - 9 AM to 11 AM

Agenda

Mary Dickerson, AVC/AVP for IT Security and CISO

- Current security incidents
  - The types of incidents that are occurring are primarily scam emails
    - Requests to go and buy gift cards because they are needed immediately, and the person asking is in a meeting and can't talk on the phone. Then the person is asked to email the gift card numbers. People usually use their own funds for this.
    - Requests for wire transfers.
    - Fake purchase orders
    - Attempts to change vendor shipping addresses and payment information
    - Emails to change the direct deposit information for payroll
    - Offering students jobs that seem too good to be true; once the student responds and gives their cell phone number, they then use text messages to contact them because it's more difficult to track. Students are mailed checks and asked to cash them, keep part of the funds, and send the rest to another address. The check is returned to them as non-sufficient funds, and they are out the funds. If the student figures out that this is a scam and doesn't do anything with the check, they sometimes receive text messages that threaten physical violence.
  - They work because
    - The person uses our online information to find the name of someone you know, like your boss or an executive
    - The person uses our online information to find the name of someone in a position of authority
    - The person is preying on our desire to be helpful
    - The ask for things that don't seem to be too hard to do
  - How do you identify them – Ask questions
    - The request may seem unusual or for a large amount for the particular type of transaction, such as a request for thousands of dollars of gift cards
    - The request may be from someone that would not normally come to you for assistance with this – an Executive in another College or Division, for example that has their own business staff.
    - The email account is not a UH email account.
      - Even if a someone is answering email from their phone, the email address should still be their UH email account
    - The request will seem unusual – why would you take pictures of gift cards instead of just dropping them off?
    - The person says they can't be reached by phone or meet with you.

    - These are criminal matters (fraud and theft) and are turned over to the police. The FBI has a cybercrime task force and is actively arresting people for these types of crimes.
    - When our employees and students fall for these scams, the funds are not often recovered. Sometimes gift cards can be canceled if the company is notified quickly enough.
    - Encourage your areas to follow all university procedures (even if they need to be expedited)
        - Pay attention to the red flag emails sent by HR and Finance when your personal information (Direct Deposit, etc.) is changed. Respond to them immediately.
        - By policy, university business must be done from university email addresses. Sometimes people may use their personal email for some communication, but you should make sure it's really them if you're getting information from a non university email address.
        - Follow procurement policies, and if someone asks you to go around them, ask why.
        - Ask questions for unusual requests, or request from unusual (non-UH) email addresses.
        - If someone is using your name in an external email account, the email provider cannot shut down an email account just because we ask. People should notify their teams that they do not use this address and any emails from the address should not be considered valid.
    - Develop validation procedures for any changes you or your staff can or does to anyone's information.
        - It's best to try to get them to help themselves via self service systems.
        - You may need different checklists for in person and remote (emailed or phone) requests.
        - Check bio/demo data, previous information (such as previous account number)
    - If anyone is receiving physical threats they need to be directed to go to the police immediately.
- Cybersecurity Audit Findings – changes in processes and procedures
    - IT Security is now centralized at the System level
        - 24 hour a day, 7 days a week coverage and response including holidays
        - Allows expertise to be shared across the System
    - SAM updates are coming out
        - 2 were MAPP's that are being elevated to SAMs
        - 1 is an existing SAM that is being updated for the reporting structure
    - ePARs must be done timely
        - ePARs are used to drive system changes for terminations and changes in positions
        - late ePARs result in system access that should not occur
    - Improving documentation of Level 1 data
        - Data Classification and Protection SAM 07.A.08 defines three levels of information.

        - Level 1 data is security sensitive, confidential, or mission critical data
        - As part of the annual Information Security Compliance Survey, due January 31, additional information will be collected. College/Division ISOs will be receiving the Survey for completion. IT Security will follow-up with the College/Division for any Surveys not submitted by the deadline.
    - Improved monitoring of endpoint updates
        - All machines must be patched and use supported operating systems
        - IT Security has regular scans of the network to identify machines without patches and with older operating systems. They obtain scans from a variety of private and government sources.
        - These machines present a risk in that they are a vulnerable spot in the network.
        - IT will require updates and will escalate the issue if it is not addressed.
    - Improved Incident Response
        - There is a University wide plan for incident response, but all departments and divisions are required to have their own plan.
        - In addition to the plan, areas should make sure their staff knows what to do to respond to an incident.
    - Hosted Service processes
        - Hosted services are when university data is stored on a non-university system (example: Office 365, DropBox, YouTube)
        - There are different levels of data; Level 1 data is the most critical
        - Any Hosted Services of Level 1 data must be on a contract.
        - There is a Hosted Services Checklist that goes with the contract for Level 1 data.
            - Specific data must be identified in the form for IT Security to adequately review.
            - Departments should work with OGC when they have Level 2 or Level 3 data and are using a click-through agreement.
        - IT Security will review the contract for the security of the data. They must have the final version (that will be sent to OCA) of the contract.
        - For Level 1 data, the department is responsible for monitoring the agreement for data security compliance:
            - If the company makes a change to their security structure, notify IT Security.
            - If you decide to end the service, or not renew, there are specific requirements for the return or destruction of the data. IT Security must be contacted; they will provide guidance on the close-out and disposition of the data.

Karin Livingston, AVP for Finance & Controller

- Vendor Direct Deposit Information
    - AP requires sufficient information to prove that someone that needs to change their banking information is the actual person. This is usually through knowledge of the

previous banking information, but if a vendor for some reason does not know that, AP has alternate verification procedures.
    - The University requires all new vendors to set up direct deposit. We can approve a one time check payment for an invoice. If there is an unusual and compelling reason why a vendor cannot accept direct deposit, contact the AP Director who will determine if an exception can be granted.
- Discussion of adding a checkbox to the Gift Card Request Form to identify "Approved IRP Protocol attached (Grants Only)" that will assist areas that use Gift Cards for payments to Human Subjects in confirming that appropriate approvals have been obtained.
    - Finance will update the form
- Credit card receipts should not be picked up by the police if that's all you have to pick up. The police department picks up cash only.
- Upcoming changes in the Purchasing department
    - Relocation is in progress to accommodate increased staffing size
    - Increasing staff size by 3 over the next year to improve service levels.
    - Teams of purchasers will be assigned to specific Colleges and Divisions to allow continuity, relationship development, and improved services.
    - Purchasing will be reviewing their procedures and processes to streamline and standardize them, and will develop more departmental training on procurement regulations and navigating the procurement processes
    - Purchasing is working on seeking increases to spot-purchase thresholds and identifying non-value adding purchase orders that can be eliminated.
    - Purchasing will increase their focus on providing institutional contracts and clear identification of useful cooperative agreements.

Other items from the group

- Finance will work with Contracts Administration to review the use of 3rd party delivery services, the need for contracts, and fiscal responsibility.
- Facilities Business Operations has identified several useful queries for obtaining payroll information. Finance will distribute them when received from the Facilities Business Office.