UWIAC	**Date: 11-1-2016** **Time:** **Place:**

Agenda

1. Security Guidelines
2. Phase 2 Work Plan
   a. Review of success of Phase I
   b. Development of additional polices & procedures
   c. Address costs and campus resource availability
   d. Communication
3. Phase 1 Implementation
   a. Security Awareness Implementation Plan and time line
   b. Data Classification training
   c. Authentication
   d. Incident Response
   e. Acceptable Use

Meeting Notes

Security Program

The UWIAC approved the Security Guidelines

Decisions	***Action items (who, what, when):***	***Open Issues:***
UWIAC approved the Security Guidelines	Security Guidelines will be posted on the UW sys web	

<table>
<tr><td colspan="3">Phase 2 Work Plan</td></tr>
<tr><td colspan="3">UWIAC will work on developing the data handling and inventory</td></tr>
<tr><td><b><i>Decisions</i></b></td><td><b><i>Action items (who, what, when):</i></b></td><td><b><i>Open Issues:</i></b></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="3">Phase 1 Implementation</td></tr>
<tr><td colspan="3">1- Security Awareness Implementation Plan and time line ((see Information from Nicholas Davis))
2- Data Classification training
3-</td></tr>
<tr><td><b><i>Decisions</i></b></td><td><b><i>Action items (who, what, when):</i></b></td><td><b><i>Open Issues:</i></b></td></tr>
<tr><td></td><td>• UW system CIO will share the Security Awareness info with HR
•</td><td>• Data Classification training still an open item</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td><b><i>Decisions</i></b></td><td><b><i>Action items (who, what, when):</i></b></td><td><b><i>Open Issues:</i></b></td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

Contents of Law Room Security Awareness Training

Module 1 “Checkpoint, Data Security and Privacy”

Video, overview of the data security problem

10 Riskiest Employee Behaviors

1. Using employee owned devices to connect to enterprise resources
2. Sharing passwords with others
3. Using the same password for multiple logins/sites

4. Using USB storage devices that are not encrypted
5. Not deleting confidential data when done using it
6. Not using privacy screens when working on sensitive data in a public area
7. Accessing the Internet via insecure networks
8. Failure to notify after loss of data
9. Leaving computers unlocked when unattended
10. Carrying un-necessary confidential data while traveling

Social Engineering

Reciprocity - **Definition:** When someone does something for us or gives something to us, we feel obligated to repay the favor.

Example: Someone posing as IT helps us fix our computer. Afterwards, they ask us to help them upgrade computer software by downloading a questionable program. We feel obligated to reciprocate their help, and so download the program despite our misgivings.

Consistency **Definition:** We want to be seen as consistent in our actions and beliefs. So once we commit to doing something, we tend to feel pressure to follow through.
Example: We agree to help a new colleague do something, but soon discover that they don't yet have a password assigned to them. In order to keep our promise to help them, we offer to give them our password for the time being so they can perform their work.

Social Proof **Definition:** We like to do things that other people are doing.

Example: Everyone lets other people in at the front door. So even though we feel uncomfortable doing it, we badge in a few people we don't recognize because everyone else is.

Authority: **Definition:** We are more likely to comply when a request comes from someone with authority.

Example: Someone impersonating a senior executive in your company sends out an email exhorting us to open an attachment. Because the email appears to come from a senior executive, we feel compelled to open the attachment without verifying the attachment's trustworthiness and against our instincts.

Scarcity: **Definition:** When something is scarce (like time or quantity), we're more likely to act. Beware of urgent requests.

Example: An email comes in warning us that if we don't verify our information immediately, IT will close our account. Because we feel we must act *now*, we log onto a fake website and fill out our personal information.

Video of Social Engineering example

SUMMARY

The Data Security Problem

Although we commonly read about data breaches involving sophisticated technological hacks, the fact is that people, not technology, remain the biggest vulnerability to an organization's data security. It's often easier for criminals to trick a person into giving up

Key Takeaways

Know what information is sensitive and needs to be protected.
Be aware of how thieves gain access to private information.
Protect it by taking adequate precautions.

Module 2, What We Need To Protect

Video – Drunken Tweet, disclosure of proprietary information

Slides on implications of data exposure, citing:

Cheaters Beware
A data breach can cost more than just money. Sometimes it's personal.

Data Security Program
Learn about data security programs and what they usually include.

Safeguarding Credit Card Info
Learn about industry standards for protecting credit card information.

Summary

Knowing what to protect and why we need to protect it helps us focus our efforts to make data secure. It can be surprising to discover how much information you have access to that needs to be protected. Remember, some information is valuable to thieves only because it can help them gain access to other information. Take a moment to think about the sensitive information you work with every day.

Key Takeaways

We need to protect everything from our physical workstations to our Wi-Fi connections.

Even if you don't have access to primary information, thieves may target you for enabling information.

Private information includes personal information, sensitive information, and organizational information.

Module 3, Information Thieves

Information Thieves
It's not only important to know what information to protect but also who is after it and how they intend to get it. Keep going to learn how information thieves can manipulate you into being unwitting accomplices to their crimes.

Types of hackers

Types of phishing (phishing, spear phishing, whaling)

Pharming

Identity Theft

Privacy Invasion

Malware

Man in the Middle

Dumpster Diving

Shoulder Surfing

Pretexting

Mail Theft

Video on how not to click on fake hyperlinks

How to spot phishy emails

Why Tax Time is Spam Time
Learn how phishers exploit news events to defraud users like you.

Spam: Art?
Is spam changing the possibilities of human communication?

Why Is Spam So Badly Written?
Are bad spelling and outlandish claims the sign of effective spam

SUMMARY

Information Thieves
& Their Tactics

Information thieves use a range of tactics from social engineering to malware in order to steal sensitive information from individuals and organizations. Though some of their tactics are technically sophisticated, many are surprisingly low-tech and rely instead on exploiting human psychology. Being aware of these tactics is the first step to protecting yourself against them. In the next section, we'll offer more tips on how to keep your data secure.

Key Takeaways

Information thieves attack organizations for many reasons. Their ranks include everyone from politically conscious hacktivists to criminal groups.

Information thieves use a variety of high-tech tactics, but most of their attacks involve a human element.

Thieves may create believable pretexts to access information. Spear phishing, for example, involves phishing emails crafted to target specific individuals.

Module 4 How Can We Protect Data

Despite the thieves' clever tactics, you're not helpless. There are simple, practical steps you can take to protect your and the organization's data. Up next you'll learn what to do and what to avoid.

Be Discreet
It is important to guard against unintentional disclosure of private information:

- Speak quietly in public areas (waiting room, hallways, elevators)
- Avoid using specific names and individualized information in public areas
- Use a private office when discussing sensitive information
- Disclose private information only to those who have a need to know
- Be cautious when entering your password or personal information on an untrusted computer
- When in public, remove or hide organizational badges, scammers can use these to identify you as a potential target
- Avoid posting non-public information to social media
- Check the recipients of email messages before responding

Always check with your supervisor before publicly discussing or posting information about your organization.

Video – mobile mixup

Video - Wireless security

Safeguarding devices

Secure

Protect your device with an authentication credential. Most commonly, you can set a PIN or password to protect your device. Some devices may also offer other authentication methods, such as your fingerprint or granting access only if a trusted Bluetooth device (like a smartwatch) is nearby.

For a mobile device, **consider putting contact info on the lock screen**, so if you lose the device, the person who finds it can reach you. You may have to download an application to add your contact information, so talk to your IT department first.

Comply

Follow your organization's policy regarding your devices. For instance, most organizations will have guidelines for regularly backing up data. That way if your device is lost or crashes, you can still recover the information on it.

Similarly, follow your organization's software policy. **Only download and install authorized programs and applications.**

Turn Off

Turn off your device when you won't be using it for a while, and when finished working, **log out** of applications that have access to sensitive data like work related email or an organization's network. These simple steps make your devices less vulnerable.

Turn off settings like Bluetooth and Wi-Fi when you're not using them. Otherwise, your device may be sending out information and connecting to networks and devices, which makes it vulnerable to hacking.

information and connecting to networks and devices, which makes it vulnerable to hacking.

Encrypt

Encrypt important information. Encryption is especially important for a mobile device. You should not copy data onto a mobile device, nor carry one containing private information, unless you are authorized to do so AND the data is encrypted or otherwise indecipherable. We will cover encryption in more detail later in the course.

Enable remote wiping and find features on mobile devices. That way, if your device is lost, you can delete sensitive information. These features may not be available on all devices. Talk to your IT department about the organization's policy before enabling these features on the organization's devices.

Update

Update your device regularly with the latest software and security patches. In 2015, 99.9% of exploited vulnerabilities were compromised more than a year after information about the vulnerability had been made publicly available

Don't jailbreak your device. Jailbreaking is the process of removing a device's built-in restrictions. Jailbreaking can make your device more vulnerable to malware.

Update your device regularly with the latest software and security patches. In 2015, 99.9% of exploited vulnerabilities were compromised more than a year after information about the vulnerability had been made publicly available

Watch

Carry mobile devices with you at all times or, if that is not possible, lock the devices in a safe or attach to a stationary object.

Keep an eye on laptops, phones, and other mobile devices when going through security lines.

Working Safely in the Cloud

In order to share information easily, you may be tempted to use cloud storage services (such as Google Drive or Dropbox) that have not been approved by your IT department. Doing so introduces security risks, since you may be storing important information in a place outside your organization's control.

In general, follow your organization's policy regarding cloud services, and consider these best practices:

- Don't use unauthorized cloud storage sites
- Only share files with colleagues who are approved to access the information
- Only login to cloud services through a secure connection
- Don't send confidential information to your personal email account
- Store data in as few places as possible and only duplicate when necessary

CREATING STRONG PASSWORDS

Strong Strategies

You will need a password to access most virtual information. To create a strong password you want to make it long, complex, and random so that it is hard to guess and will resist brute-force attempts to crack it—that is, using computers to try every combination until one works.

Don't use your name or other information that is publicly available (e.g., birthdays or children's names), and don't use common phrases or combinations (e.g., "BlueCar," "qwerty," or "12345"). These are easy to guess.

Make your password at least eight characters long— though many experts now recommend passwords of at least 12 characters. Longer passwords are harder to crack.

To make your password more complex, combine letters (both upper and lower case), numbers (e.g., 1, 2, 3, etc.), and symbols (e.g., !, #, @, etc.). Avoid easily guessed substitutions like "0" for "o."

CREATING STRONG PASSWORDS

Memorable Methods

The problem with long, complex, random passwords is they're hard to remember. Here are two methods that can help create memorable passwords that are hard to crack.

Combine four or more random words from the dictionary then randomly insert a symbol—for example, juiceexorbitantple%adfrizzy. Using words makes the password easier to remember. The strength of the password comes from its length and the randomness of the selected words.

Make an acronym out of an easy-to-remember phrase. For instance, "I live on 5555 Fake Street in Walnut Creek" could become Ilo5555fsiWC. You can insert or substitute symbols to make it even harder to crack, Il@#5555fs^WC.

CREATING STRONG PASSWORDS

Best Practices

Use different passwords for different sites, so if one is compromised, hackers won't have access to all of your secure sites.

Protect your password. Don't write your password on a "sticky note" and stick it to your computer. And never share your password with others.

If you need to provide answers to security questions such as your mother's maiden name or the city where you were born, consider giving answers unrelated to the question. For instance, you might list "Tomato Soup" as your city of birth. Hackers can often find the answers to these kinds of security questions online or guess them. Using unrelated answers makes them harder to guess.

CREATING STRONG PASSWORDS

Two-Factor Authentication

Consider using two-step verification or two-factor authentication (2FA). 2FA requires you to verify your identity in two ways (or with two factors). The two factors may include a password and a physical object (e.g., a phone, USB key, or a bank card). For instance, to access your email, you might have to enter your password and then input a code texted to your phone. Debit cards are a common example of 2FA. Many email providers offer 2FA.

Encrypt Your Devices

Basically, encryption scrambles the information on your device so it's unreadable unless someone enters the correct PIN or password (sometimes called a "key"). Encryption helps ensure that only authorized individuals who possess the key can read the data.

Why Encrypt?. Tab to view slide text. Completed slide. Why Encrypt?
How to Encrypt. Press Shift-Enter to view this slide. How to Encrypt
Downsides. Press Shift-Enter to view this slide. Downsides

Why Encrypt?

Encryption helps protect you from the determined hacker who may be able to bypass the login password or other access controls. Hackers have many ways of getting your data, especially if they gain physical access to your device. On an encrypted device, your data would still be unreadable.

How to Encrypt

How you encrypt a device or file will depend on what device or what file you're trying to encrypt. On a smart phone, for example, you can usually find the option to encrypt in your security settings. Many versions of Windows for Professionals include an application called BitLocker that allows you to encrypt the data on your computer or flash drives. Other encryption applications are also available. Talk to your IT personnel for more information.

Downsides

For most users, there are only a couple of downsides. Once you encrypt a device, there's no going back without restoring factory settings. So don't forget your password or you could permanently lose access to the data you encrypted. Encryption can also slow performance on a device, which may frustrate some users.

Our Organization's Data Security Policy

The confidentiality, integrity, and availability of our data are important to us and our stakeholders. Our data security policy helps protect our data from unauthorized usage while defining the expectations for authorized access and use. Our policy also enables our compliance with relevant state and federal laws.

It is crucial that you read and understand our policy so you know your role and responsibilities in helping us keep our data safe.

SUMMARY

How We Can
Protect Data
Good data security isn't hard. We covered some basic steps you can take to protect the data you can access, from securing your physical space to creating strong passwords and encrypting your mobile devices. Before moving on, ask yourself: how many of these best practices are you following? What can you start doing today to make your data more secure? A few minutes now could make all the difference tomorrow.

Key Takeaways

Make sure to use only secure and trustworthy wi-fi networks, and always follow best practices when you're online.

Create strong passwords to protect your devices and files, and consider encrypting devices that store sensitive information.

Be discreet when discussing sensitive information to avoid unintentional disclosures.

Module 5, Responding and Reporting

INTRODUCTION

Responding & Reporting

Unfortunately, data breaches do happen. When they do, it's critical to respond quickly and effectively. In this section, we offer pointers on how you can help stop information thieves in their tracks.

Reporting Data Breaches

State and federal laws may require notice to individuals affected by a data breach so it's important to promptly report all suspicious events, and actual and potential security breaches.

WHAT should you report?

- Unauthorized use, access, or disclosure of information
- Lost or stolen documents, files, disks, security badges, or hardware
- Erratic computer activity that may signal hacking or other intrusion into the organization's network

To WHOM should you report?

- Your supervisor
- IT department or security official

WHEN should you report?

- Immediately

SUMMARY

Responding
and Reporting

You are the front lines of data security and can help spot and stop incidents before they turn into a data breach. Stay alert, and report any suspicious activity. In the event of a data breach, the most important thing you can do is notify the proper personnel. Clear communication will be crucial to managing the situation.

Key Takeaways

If you receive a suspicious message, don't click on any links in it. Report it.

Report data breaches immediately to your supervisor, IT department, or security official.

Always be cautious when responding to requests for private information.

Information Security Guidelines

Distribute Information Security Guidelines to the institutions by November 10, 2016.

Implementation of the Authentication Policy

	January 9, 2017	September 1, 2017	September 3, 2018
UW-Madison & UW-Milwaukee	Roadmap of compliance for institution-wide ERP systems and departmental administrative and business systems	Compliance for institution-wide ERP systems and departmental business systems	Compliance for all known systems
Comprehensive Institutions & UW Colleges | Extension	Compliance for institution-wide ERP systems and departmental administrative and business systems	Compliance for all known systems	

Implementation of the Security Awareness Policy

- Review LawRoom Modules - DONE
- Determine process for distributing LawRoom Modules to the covered parties at the UW System institutions (unless an institution already has another security training program that meets the requirements of the systemwide policy.)
- Pilot the LawRoom modules at 3 institutions during the spring 2017 semester
- If the pilot is successful, implement the LawRoom training at the remaining institutions during Security Awareness Month, October 2018.
- Continue the LawRoom training annually in October unless a better, feasible alternative is found in the meantime.