December 2, 2014

MEMORANDUM

TO: Presidents, The University of Texas System

FROM: Francisco G. Cigarroa, M. D.

SUBJECT: Enhanced Remote Access Authentication Requirements

No doubt you are aware that cyber-threats and attacks continue to increase in number and sophistication. This past year, The University of Texas System institutions experienced cyber-attacks posing direct financial threat to our employees and institutions. Such attacks often start with a “phishing” campaign wherein criminals send deceptive email messages with the intent of convincing employees to reveal their logon IDs and passwords. Criminals then use the stolen credentials to access and change the employee’s banking information causing the employee’s paycheck to be deposited to an account controlled by the criminals. Similar tactics have been used to submit fraudulent claims for unemployment benefits and to submit bogus income tax returns to steal refunds. The vast majority of these attacks are launched remotely, often from overseas.

These incidents demonstrate that passwords alone are no longer sufficient to protect University data that is of high value to criminals; therefore, I am directing that each U. T. institution implement enhanced “two-factor authentication” in certain high risk situations to prevent criminals from committing these offenses against U. T. System institutions and employees. Most people are familiar with two-factor authentication as it is used when withdrawing funds from an ATM machine. The two factors required for an ATM transaction are the person’s PIN (something the person knows) and the ATM card (something the person possesses). In the University environment, authentication factors will typically consist of the person’s password (something known) along with her mobile phone or a token device (something in possession).

I am directing that two-factor authentication be required in situations that involve remote access to resources, specifically in the following situations:

- when an employee or individual working on behalf of the University (such as a student worker, contractor, or volunteer) logs on to a University network using an enterprise remote access gateway such as VPN, Terminal Server, Connect, Citrix, or similar services;
• when an individual working from a remote location uses an online function such as a web page to modify employee banking, tax, or financial information; or

• when a server administrator or other individual working from a remote location uses administrator credentials to access a server that contains or has access to confidential University data.

Please note, modification of employee banking and financial information from remote locations is to be blocked until two-factor authentication controls are in place. I encourage all institutions to implement these controls as quickly as possible, but no later than by August 31, 2015.

A Frequently Asked Questions (FAQ) document to address anticipated questions is attached. As additional questions arise, the FAQ will be updated and distributed to the U. T. System Chief Information Officers and Chief Information Security Officers. Please direct other questions that you or your staff may have to Mr. Lewis Watkins at lwatkins@utsystem.edu or (512) 499-4540.

Thank you.

FGC:bc
Attachment

cc:  Dr. Scott C. Kelley
     Dr. Pedro Reyes
     Dr. Raymond S. Greenberg, M.D., Ph.D.
     Dr. Wesley Byerly
Q-1. **What is Two-Factor Authentication?**
Two-factor authentication is a method of assuring a person is who he or she claims to be by requiring that person to provide any two of the following when attempting to access resources or conduct transactions:
1. something the individual knows (e.g. a password);
2. something the individual has on his person (e.g. token, mobile phone, ATM card, or other device); or
3. a characteristic that is unique to the person (e.g. fingerprint, handprint, etc.).

Q-2. **Why are U. T. System institutions implementing two-factor authentication?**
The number and diversity of computer security incidents occurring within U. T. System and in organizations throughout the world illustrate that the combination of user-ID and password is no longer sufficient for protecting confidential information. Criminals have devised sophisticated schemes for stealing people’s logon credentials and using them to commit crimes. As a result, there have been instances in which University employee pay deposits were redirected to fraudulent accounts. Also, credentials have been used to illegally access protected health information residing on University servers. Two-factor authentication is a best practice recognized as being effective for helping prevent these types of incidents.

Q-3. **How do criminals obtain people’s logon-IDs and passwords?**
They do so through a variety of methods. A common method is through “phishing” wherein a criminal sends bogus email or text messages in an attempt to trick recipients into revealing their logon credentials (logon-ID and password). Also, criminals continuously scan the Internet searching for technical weaknesses within organizations that can be exploited to steal data – including employee logon credentials. In some cases logon credentials may have been stolen from a business or organization having no relationship to the University. The criminal then attempts to use the stolen credentials at the victim’s workplace in hopes the employee has used the same password at work as in other places. Also, there are black market sites on the Internet where criminals who have stolen credentials offer them for sale to others.

Q-4. **Am I a target? Why would criminals want my logon-IDs and passwords?**
All University employees are potential targets. Everyone has information about themselves that criminals can potentially use for identity theft. Also, University employees have access to and come into contact with confidential personal, student, or patient information (e.g., social security numbers, bank accounts, credit card numbers, etc.) and valuable information related to research and scientific discoveries. Criminals may also use employee credentials when performing other illegal activities because it makes it more difficult to detect unauthorized activities.
Q-5. Why has U. T. System not implemented two-factor authentication sooner?
More sophisticated attacks have become prevalent mostly within the past two years, and until recently, costs and lack of available user-friendly technology posed barriers to widespread adoption of two-factor authentication. These barriers have diminished significantly over the past year. There are now a good number of low cost, easy to use, two-factor authentication products that work as apps on mobile phones.

Q-6. How will the two-factor authentication requirements impact users?
Users who access University resources only from on-site (i.e. campus) locations will not be impacted by this requirement. Users who sometimes access resources from on-site locations and sometimes from off-site locations will be impacted only when doing so from off-site in the situations described in Q-7. Until two-factor authentication capabilities are in place, employees’ ability to change their University banking and financial information will be restricted to on-site locations.

Q-7. Under what circumstances will two-factor authentication be required?
Two-factor authentication is to be required in each of the following situations:
1. when an employee or individual working on behalf of the University (such as a student worker, contractor, or volunteer) logs on to a University network using an enterprise remote access gateway such as VPN, Terminal Server, Connect, Citrix, or similar services;
2. when an individual working from a remote location uses an online function such as a web page to modify employee banking, tax, or financial information; or
3. when a server administrator or other individual working from a remote location uses administrator credentials to access a server that contains or has access to confidential University data.

Q-8. How is “Remote Location” defined?
A location is “remote” or “off-site” if it lies outside the physical boundaries of the Institution. Some examples of a remote location would include the McDonald’s just across the street from campus, an employee’s home, a hotel room, Starbucks, France, etc. Two-factor authentication is required for access from these locations.
Some examples of locations that can be considered as being within the borders of the Institution – not remote locations - include satellite facilities, clinics, observatories, and other teaching, research, or patient care facilities that are owned/operated by the Institution. Two-factor authentication is not required for access from these locations.

Q-9. How is “Remote Location” determined in shared application situations such as the shared PeopleSoft applications hosted at the ARDC?
Again, remote location is based on the location of the individual accessing resources relative to the individual’s Institution. For example:
- A UTSA employee would be on-site when accessing ARDC hosted PeopleSoft data from a UTSA location. Two-factor authentication is not required.
- The same UTSA employee is considered to be at a remote site when accessing PeopleSoft from any other location (e.g., from home). Two-factor authentication is required.
• If the UTSA employee visits another U. T. Institution and uses that Institution's Guest network to access PeopleSoft, the employee is at a remote site in relation to her institution. Two-factor authentication is required.

Q-10. How does “Cloud Computing” impact the two-factor authentication requirement?
The location of an application and/or data being accessed does not impact the two-factor authentication requirement in any way. The requirement to use two-factor authentication is based solely on the location of the individual accessing the resource in relation to the person’s institution. If the individual is working from on-campus, two-factor authentication is not required. If the individual is working from outside the campus boundary, then two-factor authentication is required.

Q-11. If an employee’s only use for remote access is to retrieve and send email (including calendar and contacts), must the employee use two-factor authentication?
It depends on how the employee chooses to access his email. There is no U. T. System requirement to use two-factor authentication if the employee accesses email using Outlook Web Access (OWA) or a similar approach that prevents access to resources other than email. However, if an employee uses VPN or one of the other services noted in Q-7 to connect to the network prior to accessing email, two-factor authentication is required when authenticating to the network. Contact your institution’s help desk for assistance if you wish to change how you access your University email.

Q-12. Can an institution choose to require two-factor authentication in situations other than those outlined above?
Yes, two-factor authentication is currently recognized as a best practice. The circumstances identified in Q-7 are a minimum requirement and pertain specifically to this initiative. There are many other situations in which prudent practice suggests that two-factor authentication be used. Based on risk, and as time and resources permit, Institutions are encouraged to expand use of two-factor authentication.

Q-13. Can adaptive techniques that require different levels of authentication based on risk level be used?
They cannot be used in the above situations because these situations have been identified as being high risk thereby warranting a traditional two-factor process. Based on risk, institutions may choose to use adaptive technologies in other situations as appropriate.

Q-14. Is there a requirement to use specific products?
No, institutions are not required to use a specific product. Toopher and Duo are recommended products because each of these are part of the Internet2 Netplus program and as such have been vetted for use in higher education. Also, these products are easy to use and relatively easy to deploy. However, there is no requirement to use either product.
Q-15. What costs are involved?
As a result of a contract that U. T. Austin secured, there is no licensing cost for use of Toopher. The cost for Duo licenses depends on the size of an institution and whether or not licenses are being purchased for faculty and staff only or for faculty, staff, and students. Duo costs are explained here: http://www.incommon.org/duo/fees.html Also, under certain circumstances the institution may incur a small communications charge.

Q-16. What about employees who do not own mobile phones or who do not want to load an app on their mobile phones?
If the employee is one who must utilize remote access to perform his/her duties, the employee can use a token hardware device. These devices are about the size of a USB memory stick. Whenever the user is required to provide a second factor credential, the device will display a one-time numeric code for the user to enter. This is in addition to the user’s password. The numeric code proves that the user is in possession of the token device. Token devices vary in cost, and we do not have a specific brand to recommend.

Q-17. What will the institution pay for? Phone? Token?
Each institution has guidelines regarding to whom a university purchased phone might be provided. There is no intent or expectation that this two-factor initiative will impact an institution’s current mobile phone policy. It is an institutional decision whether and under what circumstances it might provide a token device to an employee.

Q-18. What if a situation exists that requires two-factor authentication but for technical or other reasons it is not possible, or is imprudent, to implement the requirement?
A temporary exception may be granted by the institutional Information Security Officer. Exceptions must be documented and include the following elements:
1. a statement defining the nature and scope of the exception;
2. the rationale for the exception;
3. an expiration date for the exception;
4. a description of any compensating security measures that are to be required; and
5. the signature of the Information Security Officer and the Owner of the business function controlling the Information Resources potentially put at risk.

Q-19. What are the two-factor authentication requirements in medical work settings wherein U. T. physicians or other health professionals work in a facility owned/operated by an affiliated business partner?
Based on the criteria noted in Q-8, these locations meet the criteria for being considered “remote.” Therefore, two-factor authentication should be used for accessing University resources unless there are factors that make it impossible or imprudent to do so. Any decision to not use two-factor authentication should be based on risk assessment and be documented as noted in Q-18.
Q-20. At my institution, employees access their banking and financial records through our self-service portal which uses Shibboleth for authentication. How does this impact our moving to two-factor authentication? Use of Shibboleth simplifies implementation of two-factor authentication. Shibboleth can easily determine whether a transaction is initiated locally or from a remote location and will initiate the two-factor requirement only when needed. Depending on the version, Shibboleth may need to be upgraded prior to turning on two-factor authentication.

Q-21. Are resources available to assist with implementation? U. T. System has several employees who are available to provide assistance. Assistance may consist of providing consulting and guidance on deployment of two-factor in various situations. Assistance can also be provided relating to upgrade and integration with Shibboleth. Project management and training development and delivery is also available. Send inquiries to CISO@utsystem.edu.

Q-22 Where can I obtain more information? Direct technical questions to Paul Caskey at: pcaskey@utsystem.edu Direct policy questions to Lewis Watkins at: lwatkins@utsystem.edu

Q-23. What is the deadline for implementation? August 31, 2015