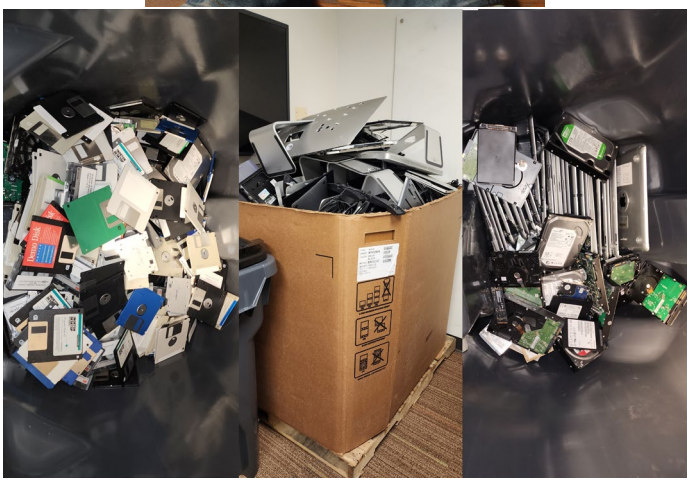
THE UNIVERSITY OF CHICAGO | Biological Sciences Division Information Security Office

July 2024

Cybersecurity Awareness Newsletter

Protecting yourself and information from cybersecurity threats.

A big **THANK YOU** to everyone who brought in items to the secure destruction event! Your commitment to preventing the loss of data helps us all comply with data protection laws and regulations, which in turn helps maintain our institution's integrity and reputation! Every step counts in data security so your efforts are truly appreciated!



For this month, our intern Nik, under the guidance of our team, will be addressing the importance of rebooting or restarting a system. Following that, we will also continue last month's newsletter topics of data handling and data protection.

System Rebooting – System and Application Health

While it can be inconvenient to regularly restart your system, there are numerous benefits to doing so, which extend beyond just enhancing security. Here are three such benefits:

<u>Clears system memory:</u>

- When an application is opened, the temporary data from the application is placed into memory (RAM). This is done to speed up the application's processing power. If an application is experiencing performance issues, then a good troubleshooting step is to save your data first and restart the system to clear problematic use of RAM.

<u>Releases locked resources:</u>

- Sometimes programs will experience bugs and not release the memory that is intended to be held temporarily. Overtime the systems memory gets filled up with old useless data leaving less space for new tasks. This can slow down your computer and even cause crashes, which can be problematic when documents are being worked on over long periods of time.

<u>Updates and patches:</u>

- Rebooting a system can apply updates and patches that are normally downloaded but not yet installed. These can fix bugs and improve system, as well as application, performance.

Patching and the interruption of a reboot

One of the most important reasons to reboot a device is for system updates or patches to be applied. This is usually because the update modifies certain parts of the system or application that are currently in operation and can only be changed when they are shut down. This highlights the necessity to consistently apply updates to fix vulnerabilities and bugs on systems.

How often should updates occur?

The BSD Information Security Office and the Technology Solutions and Services Teams (TSS) have a monthly program in place to apply patches to systems and reboot at given schedules. If your computer system is already serviced by TSS, your computer is already part of a patching program. If you require your system to become part of a patching cadence and for whatever reason it was not added to a patching cadence, you may reach out to BSD TSS via our service portal here:
Request Solutions Consulting

Patching times may vary depending on the criticality of a vulnerability or bug. The recommended guidelines are as follows:

- Critical vulnerabilities that are actively being exploited by hackers across the internet should be promptly addressed within a span of 5 days.
- Critical vulnerabilities (not actively exploited) should be addressed within 10-15 days.
- Medium/High vulnerabilities should be addressed within 20 days.
- Low vulnerabilities should be addressed within 30 days.

Vigilance

CVSS v4.0 Ratings

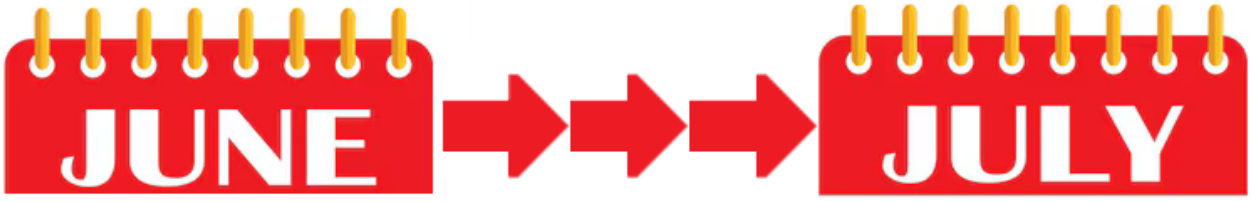
Severity	Severity Score Range
None*	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Scoring Metrics for the CVSS standard

To ensure that vulnerabilities are patched, and those patches are properly applied, it is important to remain vigilant about patching and rebooting in the timeframes given above. The criticality levels given above should be used to determine the timeframes needed to patch and reboot a system. The above guidelines from the National Institute of Standards and Technology (NIST) rank vulnerabilities on a level of severity from None to Critical, called the Common Vulnerability Scoring System (CVSS), which classifies the severity of a vulnerability on a scale of 0-10. Further information regarding the scoring metric and vulnerability search services can be found here:

National Vulnerability Database Metrics

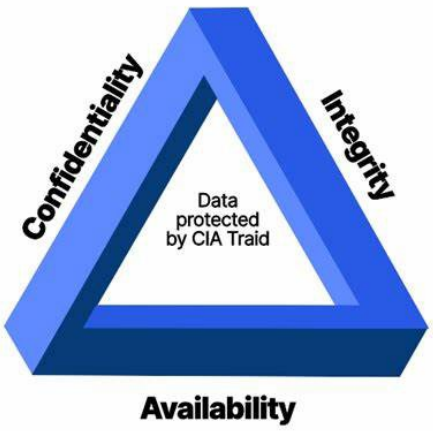
While we don't expect folks to check the National Vulnerability Database, we do encourage that they remain vigilant when news of critical threats emerge. If a vulnerability is being actively discussed in the news, then it is most likely being actively exploited. We recommend that in these cases the vulnerability is patched within the appropriate timeframes given above. If one is aware of newly discovered threats, and ensures that their devices are actively updated and rebooted, they will remain secure by having the latest protections and fixes in place to guard against vulnerabilities. We hope this section has encouraged you to remain vigilant about patching and rebooting your systems to remain secure against computing threats.



Last month we discussed the importance of data discovery and data classification. This month we want to go over two more crucial components that go hand in hand with discovery and classification: data handling and data protections. **Data handling** is about the processes of managing data: collecting, storing, cleaning, transformation, analysis, and presentation. **Data protection** involves implementing measures to safeguard data from unauthorized access, breaches, and other potential security threats.

Data Protection

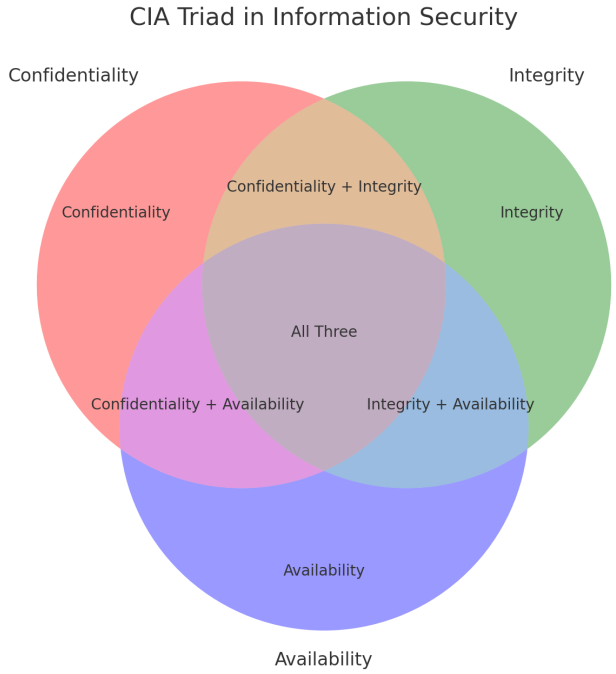
To determine the security protections that should be added, we need to look at the security protection model called the CIA triad. CIA stands for **C**onfidentiality, **I**ntegrity and **A**vailability and it is the cornerstone of any security infrastructure guide for determining the impact level and protection of data.



- **Confidentiality**: Ensures that information is accessible only to those authorized to have access to it.

- **Integrity**: Safeguards the accuracy and completeness of information and processing methods.
- **Availability**: Ensures that authorized users have access to information and associated assets when required.

The CIA triad principles often need to be carefully balanced. Excessive protection controls on **Confidentiality,** for example, can lead to a lack of **Availability** for those who need access to the data, which could hinder productivity. The diagram below shows areas where these principles overlap each other.



The Importance of Data Handling

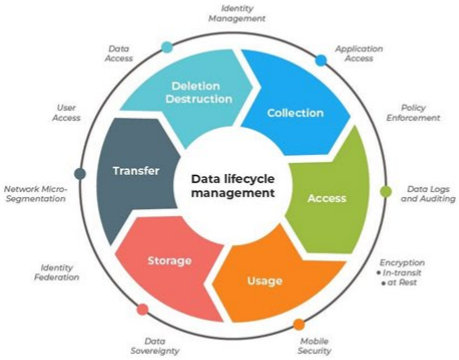
The BSD policy "**BSD Policy for Data Handling and Classification" is** located here: https://spservices.uchicagomedicine.org/sites/PoliciesAndProcedures/HIPAA%20Security/1%20-%20IT%20Security%20Policies/02_POL-DC%20Data%20Classification.pdf

All data are subject to some form of governance, making it crucial to understand that a data management lifecycle plan is necessary for all data. This lifecycle spans from the data's creation or

acquisition to its eventual disposal. Data management lifecycle plans can vary widely, ranging from simple to extremely complex. Two quick examples:

Example 1: I just received an e-mail advertisement for a sale occurring on the 4th of July. An e-mail of this nature is normally not needed after that date and can be discarded to help save space.

Example 2: A patient visited a hospital (a covered entity) and as a result Protected Health Information (PHI) data were generated. Per the HIPAA Privacy rule, PHI must be retained for 6 years beyond the expiration date of the authorization or the completion of a health care event. However, this could vary depending on state laws and guidelines governing record retention, as well as usage agreements.



Data can be subject to various regulatory and legal frameworks that dictate how it must be secured, collected, stored, processed, shared and disposed of. This is especially true for some of the more sensitive data, such as PHI.

As always, we welcome your feedback and any suggestions for topics that you would like us to cover in the next newsletter. Please send us an e-mail at security@bsd.uchicago.edu .