Control 3 Data Protection

One CIS control that is important is data protection. Data protection is a very important control to have because data is important for a business to function properly. If a company doesn't protect its data, they will be at risk of attacks that can cause all their internal information like proprietary data, and personally identifiable data of users to be exposed. If this happens a company will lose the trust of customers and be at risk of legal trouble if they were supposed to follow regulations but didn't.

According to an article written by Ryan Tully at spirion.com some steps for an effective data protection program include defining data, know regulations to follow, decide who can access data, and backup data (Tully, 2021). Data needs to be defined and classified based on its importance to the organization and the harm that could come from an organization not protecting the data. Regulations need to be followed because there can be fines for not following laws and not following laws can cause an organization to not be trusted by others. Also, a company needs to protect data that is vital to their operations more strongly than data that is less important and less valuable. Backing up data is important because if no backups exist and something happens to cause data to be lost then that data is gone forever or will be very expensive to attempt to recover. Daily or weekly backups would be a good start for data protection.

According to the UK information commissioner's office data protection can be implemented by combing many different factors like backups, strong passwords, multifactor authentication, antimalware/virus, limiting data access, proper disposal of data and equipment.

Strong passwords and multifactor authentication can prevent unauthorized individuals from getting access to systems and data. If passwords are strong then it is more difficult for an

attacker to brute force a password without raising suspicion that malicious activity is happening. Also using multifactor authentication can make it so even if someone's password is found there are still other methods of authentication that an attacker needs to get past to get onto systems. Antimalware and antivirus can be used to prevent bad software from being installed on user workstations. If malware can be installed an attacker could use techniques like phishing to get someone to install malware like ransomware or spyware onto a workstation. If a computer gets malware installed on it the device can become unusable without paying money or the device could be sending everything typed and accessed on it to an attacker who can use that information to attack a company's systems.

According to CISA firewalls are also important for data protection. Firewalls can prevent data from leaving a network and heading to certain destinations by opening only necessary ports and blocking IP addresses from getting data sent to them.

According to an article found at eccouncil.org tools like an intrusion prevention/detection system can also be used in the implementation of data protection. They can be used to detect and stop activity that seems to be suspicious. They can detect when a lot of activity looks like it's coming from one address when that isn't normal. They can also be used to detect when activity like attempting to access accounts occurs or when someone is trying to scan a network for information. Using an IPS to stop this traffic can stop an attacker before they ever get onto a company's network or internal systems where data can be accessed.

The CIS security controls include many aspects of data protection. This includes establishing a data management process, maintaining an inventory of data, configuring ACLs, enforcing data retention, encrypting data on end user devices, data at rest, in transit, and data on

removable media. They also include segmentation of data processing based on sensitivity and logging all access of sensitive data.

Data encryption is very important for the protaction of data. This means that data should be unreadable by an attacker even if they do manage to get access to data. An attacker could get access to data if removable media or mobile devices that hold data or can access sensitive data are lost and someone finds the device or media and tries to use it for themselves. Logging access to sensitive data is important because if it is known who accessed data and when it can be used to find who did things with data that shouldn't have happened. Internal threats exist so it might be someone who is authorized who is doing things with data that they shouldn't.

This is why data needs to be encrypted, so even if an insider wants to harm the organization, they will be limited with what they can do and if it's logged then they will be found if they are doing bad things. Also, use of a firewall can prevent data from being sent out of an organization by an employee or an attacker who was able to get into an employee's account and this will be logged when it does happen or is attempted.

There are multiple key performance indicators that could be used to measure if the data is being protected properly. According to an article found at inetsoft.com these include things such as the number of breaches that are successful and this could be looked at over time to see if the data protection is improving. Another metric that could be used could be the number of times employees don't follow data protection standards and policies and if that number gets too high it shows that data protection is not effective.

Some other metrics include the amount of data that is protected and encrypted compared to the total amount of data in an organization. Also, another KPI could be the number of alerts

that are given and the percentage of those alerts that were actual alerts and not false positives. Attempting to measure false negatives may be more difficult but that number could be used to show that IDS/IPS software does not function as expected.

This is one of the most important security controls for an organization to have. This control is very important because data is very valuable to a company and if they don't properly protect their data that could cause severe financial harm. If a company gets attacked and data is stolen that data could be used by competitors or if it's personally identifiable information of customers and employees, the data could be sold on the dark web and used to harm the individuals the data is for. If an organization isn't properly protecting data, then they will not be seen as trustworthy by the public which will hurt their abilities to expand their customer base and make money.

Control 6 Access Control Management

Another control that is useful is access control management. According to an article found at linkedin.com some aspects include confidentiality and integrity. Confidentiality includes only letting users access what is needed, also known as least privilege. Integrity ensures that data isn't changed when it shouldn't be, including when it is in transit (Taieb, 2023). Access control also allows tracking what users have done to data, ensuring that only authorized changes have been made. Access control management involves only letting certain individuals access certain resources. Access control management is important for keeping secret data secret. If only authorized users can access data and resources then data will remain confidential, and systems will remain secure.

According to CIS some things involved in access control management include role-based access control, centralized access control, multifactor authentication, and a process to remove or add access. Centralized access control would be useful for more easily changing the access that users have. If access had to be changed across multiple systems that would increase the chance of errors occurring, preventing users from accessing resources they need or granting too much access and not following the concept of least privilege. Role based access control is a simpler way to define who has access and what they have access to. If they are put in a group based on their job, then that group can have access updated as needed and employees could come and go, and it would be simple to change the access an employee has by assignment to a group based on job needs.

There should be a defined process of adding and removing access because if a process is defined then it can guarantee that access is removed when it should be if processes are followed. Also, having a set process ensures things are done the same way every time and if something is

done out of expected there can be concerns raised and the thing that occurred out of normal can be evaluated.

Multifactor authentication is important to ensure that someone is who they say they are. According to the CIS multifactor authentication (MFA) should be used on externally exposed applications, in remote network access, and for administrative access. These are critical areas that if not protected properly can leave the company's systems vulnerable to attacks.

Externally exposed applications are more vulnerable because they have a direct connection to the internet. This means that it could be easier for an attacker to find these systems and make it more likely that attacks are targeting those systems. This means that all user accounts to be secured as good as possible to limit the chance of an attacker being able to brute force their way into an account. According to a blog found at conscious.net internet facing applications are the most vulnerable because they are the easiest to access and a list of public facing applications needs to be maintained to ensure that they are all protected properly to be safe from external attacks.

Requiring remote access to use MFA is also important because remote access can possibly be used to access internal systems that can't be accessed outside of a company's internal network. Remote access allows users to access these systems from locations outside of the company and could be used by employees who are working from home or working while traveling. If an attacker was able to attack these resources by connecting to the VPN through an unsecured account, then that would be an easy way for data to be accessed by someone who isn't authorized.

Accounts that have administrative access are among the most important to secure with MFA. Microsoft says MFA on admin accounts is an easy way to reduce the risk of compromise and recommends that admin accounts have MFA on them (MicrosoftGuyJFlo et al, 2023). This is because accounts that have administrative access can make changes to systems and have more access than regular user accounts. They can be used to change what users can access and change settings for where data can and can't go. If someone was able to access an administrator account, they could bring a lot of harm to a company and its systems.

There are many key performance indicators that could be used to measure the effectiveness of access control management. According to an article found at indentitymanagementinstitute.org these could include the number of accounts that have administrator or privileged access, the amount of data that a user accesses, the number of times accounts are unsuccessfully accessed, and the time it takes to respond to an incident.

Tracking the number of accounts that have higher privileges is important because if that number is too high there is concern that too many people are getting access that should be limited and that least privilege isn't being followed. Also, it could be beneficial to track the amount of time those accounts are logged in and what is done on those accounts to make sure that employees are only using those accounts when needed. If administrator accounts are used for regular tasks that is riskier to an organization.

Tracking the data that users access is useful for seeing what data is used the most and could be at the most risk of being attacked. Also, if users are accessing data that they shouldn't need to access that can be used as a sign that there might be malicious activity happening or that there needs to be better definitions of what employees can do on computers. If user accounts have a lot of unsuccessful login attempts this could be a sign that someone is trying to access an

account that they aren't authorized to access, and this indicates that the company is a target of an attack.

Access control management is very important for an organization to successfully implement. This is because if access control is not properly managed then unauthorized individuals will have access to things that they should not be able to access. If this happens there is no confidentiality in the organization.

If there is no confidentiality, then a company cannot be trusted to keep sensitive information private which harms how others will view the organization. Also, this could help a hacker have an easier time of stealing data and lack of access control management harms data protection. Also, if no logs are kept because of lack of access control it can be more difficult to track when unauthorized access or changes to data are made.

There is also no integrity if there is no access control management. If anyone can access and change any document, then there is no way to guarantee that data only has had proper changes made to it.

Access control goes together with data protection because improper access control leads to data that is not properly protected. Having proper data protection is another very important thing to an organization so this makes access control very important to properly manage.

Measurements of success of access control management include number of times accounts are attempted to log into but fail, number of accounts that have access to certain files or data, number of accounts that have privileged access, and the number of times someone tries to access resources that they should not have access to. Also, tracking when and how long accounts

are used for to make sure it matches with when someone is supposed to be working is useful to make sure that accounts are not being accessed when they are not supposed to be used.

Control 11 Data Recovery

Another control that is important for an organization to follow is data recovery. According to CIS this includes establishing a data recovery process, automating backups, protecting recovery data, maintaining an offline or isolated instance of data backups, and test data recovery. Data backups and recovery provide better availability of data depending on how fast backups can be restored. Data recovery is important because storage devices will fail and if there aren't multiple copies of data then that data will be lost forever. A company can't function properly without its data. The most valuable data should have the most frequent backups and have the most resources devoted to implementing data recovery.

An established process of data recovery will ensure that backups are made at the proper intervals and when backups are needed, they will be properly restored. The process should guarantee that data is restored quickly and that there is minimal data loss. The amount of time for data to be lost varies from company to company. A frequency of backing up at least daily will probably be needed.

Automating the process of backing up data ensures that it always happens at the correct intervals and that the same steps are followed ensuring that the data is backed up in a way that is useful to an organization. An article found at rubrik.com says that data backups should occur outside of main business hours like at night or on weekends. This is ideal because then there would be less disruption of business processes and data backups could be more complete. This article says that data should be backed up to a cloud or other offsite location. Backing up data offsite is important because if a disaster occurs onsite that destroys data the backups could also get destroyed making them useless. If the process occurred manually there would be issues with humans making mistakes that make backups not valid or humans missing the intervals to back up

their data. This is especially important when not all data is backed up at every backup. If some backups were lost it could make recovery of all backups not possible.

Data that is backed up still needs to have the same controls protecting it as regular data. An article found at networkworld.com says there are many ways to protect backup data. These include encrypting backups, making backups undeletable, storing backups offline, and storing backups on a different operating system to help airgap the backups (Preston, 2023).

All data, including backups, should be encrypted. Encrypting data prevents bad actors from being able to read the data unless they have the encryption keys which should be stored securely separate from the data so that if the data is found the data still cannot be read.

If backups are marked to be immutable or unable to be deleted, then a bad actor could not get into a system and destroy the backups. If they have gained administrative privileges, they may be able to do this still so it's important to secure accounts that have administrative access to systems where data is stored. Data could also be stored offline and only accessible by authorized individuals who should be trusted to not delete backups.

If data backups are stored on a different operating system, then it will be more difficult for an attacker to get access to both actual data and data backups. Storing on different operating systems is a way to prevent the backups from being exposed to the same threats and vulnerabilities as the actual data. This helps ensure that one copy of data is still trusted and is kept secure.

This is because the data is still going to be vulnerable to attacks unless all data is kept offline. Even if it is kept offline if a user has access to the backups, they could damage them if they weren't protected in the same way as regular production data. If an attacker can get access

to backup data, they could use that in ways that are harmful to the organization and helpful to the attacker, even though it isn't the most recent data.

Backups needs to be tested to ensure that data is being backed up and to ensure that the backups can be used in the case of needing to recover data because of data loss. If a backup method isn't tested and no backups are ever made, that could prevent a company from being able to operate properly and could cause severe damage. Also, backups should be tested regularly to ensure that backups are happening and able to be restored if the need ever arises.

There are many useful key performance indicators that could be used to measure the effectiveness of data recovery. These include things like mean time to recovery, mean time between failures, the amount of data that is recovered, recovery point and time objectives (Garn, 2022).

Measuring the amount of time, it takes to recover data is important for ensuring that the amount of time is acceptable, and this can be tested in simulations to see if there are ways to improve before data needs to be recovered. The mean time between failures is important to know because if data is needing to be recovered frequently that shows that the systems in use are not reliable and that means more data will be lost and more money will be lost as data is lost and needs to be recovered. It's important to track how much data will be lost when a failure occurs and before data is recovered to ensure that the amount is acceptable. Recovery time objectives measure how long a company can accept a recovery taking. Recovery point objectives measure what point a company wants data to be recovered from and how much data they are okay with not having been backed up.

Data recovery is one of the top security controls that an organization should focus on. If data can't be recovered properly then an organization will be harmed when there is a failure or

disaster of some kind that causes data to be lost. A company saves data for a reason and if they lose data that they need then there could be financial losses, or the public could lose trust in this company if they are not able to properly store data that they need. Also, if data recovery is not properly managed and there is backups, but they are not securely stored then hackers could get data that way. This means that proper data recovery is very important to have.

Measurements of success for data recovery would be how much data is lost when a failure does occur. If large amounts of data are unrecovered after a failure occurs and this hurts the company and needs to be lowered, then that could be used to see that more backups are needed. If the data takes a long time to recover when a failure occurs, then that would also be bad because that could hurt the ability of the organization to operate properly. Another measurement could be the amount of data backups that are successful and able to be recovered from. If a backup cannot be used in a recovery, then that is bad because the backup is not valuable if it is not usable.

References

11 practical ways to keep your IT systems safe and secure. ICO. (n.d.). https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/11-practical-ways-to-keep-your-it-systems-safe-and-secure/

Cybersecurity and Infrastructure Security Agency CISA. (2023, February 23). *Understanding firewalls for home and small office use: CISA*. Understanding Firewalls for Home and Small Office Use. https://www.cisa.gov/news-events/news/understanding-firewalls-home-and-small-office-use

EC-Council Cybersecurity Exchange . (2023, December 15). *IDS vs. IPS: Key difference and similarities best for Cybersecurity*. IDS and IPS: Understanding Similarities and Differences. https://www.eccouncil.org/cybersecurity-exchange/network-security/ids-and-ips-

differences/#:~:text=Protecting%20sensitive%20data%3A%20By%20blocking,complying%20with%20data%20privacy%20standards

Garn, D. M. (2022, January 26). *5 it disaster recovery measurements to know*. CompTIA. https://www.comptia.org/blog/disaster-recovery-measurements

Imi. (2021, September 21). *Top identity and access management metrics - set your IAM benchmark*. Identity Management Institute®. https://identitymanagementinstitute.org/top-identity-and-access-management-metrics/

inetsoft. (n.d.). *How to leverage key performance indicators to measure and enhance data protection effectiveness*. How to Leverage Key Performance Indicators to Measure and Enhance Data Protection Effectiveness. https://www.inetsoft.com/business/bi/data-protection-kpi-dashboards/#:~:text=The%20KPIs%20you%20select%20should,in%20a%20given%20time%20period.

MicrosoftGuyJFlo, BryanLa, alexbuckgit, baardhermansen, davidspooner, BakkerJan, curtand, Oechiih, thepaulmacca, SaurabhSharma-MSFT, MarileeTurscak-MSFT, & Saisang. (2023, October 23). *Require MFA for administrators with Conditional Access - Microsoft entra ID*. Require MFA for administrators with Conditional Access - Microsoft Entra ID | Microsoft Learn. https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-admin-mfa

Internet-facing applications – a big security threat?. Conscious Networks. (2023, November 7). https://www.conscious.net/blog/internet-facing-applications-a-big-security-threat/

Preston, C. (2023, January 10). *7 ways to secure backup data*. Network World. https://www.networkworld.com/article/971812/7-ways-to-secure-backup-data.html

Rubrik. (n.d.). *Data Backup Automation and why it matters*. Rubrik. https://www.rubrik.com/insights/how-to-automate-data-backup

Taieb, R. (2023, July 25). *What is access control management?*. LinkedIn. https://www.linkedin.com/pulse/what-access-control-management-ronen-taieb/

Tully, R. (2021, June 16). *Ten steps to an effective data protection program*. Spirion. https://www.spirion.com/blog/ten-steps-to-an-effective-data-protection-program/