# Critical Security Controls White Paper

Name

Institutional Affiliation

Instructor

Course

Date

**Critical Security Controls White Paper**

Since data and file sharing are increasingly common in today's culture, organizations must consider the expense of computer networking. After all, networking consumption is visible on a worldwide basis. Most businesses struggle to adequately analyze digital security threats, resulting in discrepancies across safety policies. The SANS Institution has identified the top 20 key safety measures for comprehensive cybersecurity protection, which have grown to be critical for all sorts of businesses' security control procedures. These are the initial steps for every organization, corporation, or firm aiming to strengthen its information security, and they are considered must-dos. Businesses can avert the majority of cyber-attacks by implementing these management techniques. These twenty security measures specialize and concentrate on a few smaller tasks. It is via the deployment of security procedures, irrespective of the scale of the business, that the risk of large-scale cyber-attacks is reduced.

The SANS best 20 measures are intended to enhance and address the endangered network security risk state, as well as to assist individuals with their data sensitivity education. Apparently even networking security experts depend on the 20 controls since they offer excellent electronic security defensive advice. Computer-based information Science, which is currently known as Crucial Security Controls, was granted the best 20 security measures listed by SANS (Ahmed & Al-Shaer, 2019). This company is another well-known non-profit information cybersecurity company with a long history of data protection (Ahmed & Al-Shaer, 2019). They're perhaps most recognized for their publicized best-practice security guidelines and standards for operational systems (Ahmed & Al-Shaer, 2019). Therefore, if the company was granted the top 20 SANS' security measures then it means that these measures are up to standard and feasible.

Efficient networking authenticity and protection mechanisms have hit the 20 essential security controls procedures which means organizations may avoid around 80 % of assaults by employing simply the initial five measures; implementing all 20 controls could assist avert up to 98 % of cyber-attacks (Center for Internet Security, 2019). However, how these control procedures are implemented is determined by the corporation's approach and instruments. Businesses might find it challenging to execute it on their own. They need to work with their cybersecurity providers and adhere to their recommendations for diverse security control methods (Center for Internet Security, 2019).

## CSC Awareness

Owing to the COVID-19 pandemic that has transformed/crippled the planet's economic state, most firms have chosen to allow their workers to remain at their houses and operate from there since the culmination of 2019 until currently 2021. Cyber Attackers are targeting those who do not understand information security, from web pages to deception in the context of worker communications, and even posing as officials of the Centers for Infection Management and Preventative measures or the Ministry of Health. Individuals who steal confidential information show that the institution's vigilance has failed. When workers use a home device to operate remotely, the machine lacks security safeguards and is easily manipulated. According to the 2020 Status of Data and Security Management Study, 28 percent of workers lack expertise in detecting a malicious email, demonstrating the importance of an information security schooling program (Newhouse et al., 2017).

My recommendation is that cybersecurity sensitivity education is required to allow workers to operate remotely or in the workplace and that the training cannot be one-time. Each week, the firm should guarantee that workers attend the training sessions. The more

knowledgeable the operator, the lower the likelihood of cybersecurity incidents. The purpose of the firm's security sensitivity education is to safeguard the data of its personnel, and the many types of breaches. Workers should always be aware of the attacking tactics in order to avoid readily leaking corporate secrets. Information security is everybody's duty, not just the firm's therefore, in addition to using the encryption software given, workers should raise their security knowledge (Newhouse et al., 2017).

## CSC Benefits

The advantage of Critical Security Control (CSC) is that it prioritizes network security technologies designed effectively in identifying, preventing, or coordinating network assaults (Dutta & Al-Shaer, 2019). When recipients use the CSC strategy, a primary advantage of the measures is that they emphasize and concentrate on a tiny set of operations that effectively reduce cybersecurity incidents. CSC firsts investigate the cause of the potential danger. Only in conformance, CSC can be implemented based on the prerequisites and the safe operation structure. The greatest approach to inspire security executives to implement essential security measures is to have the backing of the company's management. Though CSC is not a required strategy for businesses, if the firm can manage to apply the framework for every control check, it may save a lot of money on system modifications in the future (Dutta & Al-Shaer, 2019). Since there are many types of cyber-attacks, a firm's adoption of essential security procedures is equal to possessing the best armor. Attackers conduct illegal system activities depending on system weaknesses, which pertains to illegal entry to computer data and resources (Dutta & Al-Shaer, 2019).

## CSC Barriers

Although the CSC's 20 control mechanisms have highly effective countermeasures against attackers, they require time to deploy. The challenges that businesses will face are mostly caused by two variables: zero-interaction among workers and training difficulties. Small firms' security systems are not as comprehensive as those of major corporations which can afford to engage experienced IT security specialists and train personnel. 70 percent of small companies are underequipped to contend with a cyber-attack, and three out of four small companies claim they do have not enough staff to resolve IT safety, so I'm convinced that any linked system setup, patch maintenance, and entitlement control are severely lacking in IT professionals (Dutta & Al-Shaer, 2019).

Workers with no contact make it harder for the firm to deploy the CSC program. The company's management will be unable to assess whether control procedures are realistic, and the firm's strategy and outmoded technologies, along with restricted finances, will make execution difficult (Gros, 2021). My recommendation is to arrange a weekly staff meeting with the risk management committee as the starter and IT personnel to declare the firm's system weaknesses and decide which control strategies are practical.

## Company Adoption & Implementation

Prior to adopting important security measures, the firm chooses to create a comprehensive plan. The long-term task of connecting security control improvements with the data system's framework necessitates the firm inviting outsourced experts and expert technological employees to establish a plan for implementing control mechanisms. The seriousness of cyberattacks is increasing. Owing to the importance of the information companys hold and the networks to which this data links, all sectors confront overwhelming risk (Gros, 2021). Cyber criminals earn money by stealing, extorting, and selling this data. Medical care,

banking, postsecondary learning, and small companies are among the sectors most susceptible to cyber-attacks (Kobezak et al., 2018).

I agree with businesses that use these three sorts of regulations as protective countermeasures.

- Application of controls that are more sophisticated, such as antimalware, border defense, and data retrieval (Kobezak et al., 2018). The biggest developed aspects of cybersecurity include anti-virus software, firewalls, and contingency planning retrieval of operational processes. Even the retrieval feature in the Cloud system assists the firm in data protection.
- Implementation of standard security setup procedures which include managing administrator permissions, restricting channels, susceptibility analysis, inventories, and login surveillance (Kobezak et al., 2018). Controls indicate dangers and weaknesses; moreover, the firm assists workers in implementing control features with their own gadgets and unique services. The periodic assessments are ongoing to guarantee that the firm's systems are in good working order.
- Implementation of controls that are still in their infancy, such as log surveillance, intrusion detection, and prevention systems, vulnerability scanning, and information protection, which have low rates of complete acceptance and moderate levels of intermediate implementation (Kobezak et al., 2018). This is appropriate for businesses that do not have enough skilled people to apply security management metrics and do not have any experts for assessment.

## Measurement and Metrics

The firm is adopting essential security control procedures to enhance the system by evaluating, mending, and streamlining reporting obligations to satisfy metrics; hence, the firm's control procedures promote the pattern of risk reduction (Kobezak et al., 2018). To decrease the risk expense of CSC, the firm relates to institutional breaches, such as information disclosed, which would destroy the firm's brand. The Ministry of Healthcare and Social Services, for instance, penalized Idaho State School $400K for failing to notice firewall policy modifications that led to the possible disclosure of sensitive patient data for 17,500 patients. Although CSC is not required for every company to adopt, when the control procedures are engaged, the company needs to uphold the country's statutory regulations for key security controls (Kobezak et al., 2018).

## References

Ahmed, M., & Al-Shaer, E. (2019). Measures and metrics for the enforcement of critical security controls. Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security - HotSoS '19. https://doi.org/10.1145/3314058.3317730

Center for Internet Security. (2019). The 18 CIS controls. CIS. https://www.cisecurity.org/controls/cis-controls-list/

Dutta, A., & Al-Shaer, E. (2019). “What”, “Where”, and “Why” cybersecurity controls to enforce for optimal risk mitigation. 2019 IEEE Conference on Communications and Network Security (CNS). https://doi.org/10.1109/cns.2019.8802745

Gros, S. (2021). A critical view on CIS controls. 2021 16th International Conference on Telecommunications (ConTEL). https://doi.org/10.23919/contel52528.2021.9495982

Kobezak, P., Marchany, R., Raymond, D., & Tront, J. (2018). Host inventory controls and systems survey: Evaluating the CIS critical security control one in higher education networks. Proceedings of the 51st Hawaii International Conference on System Sciences. https://doi.org/10.24251/hicss.2018.597

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. https://doi.org/10.6028/nist.sp.800-181