1. Introduction & Motivation

Video conferencing platforms (VCPs) are platforms that enable audio and visual communication via the internet. Since the Covid-19 pandemic and subsequent lockdowns in place, there has been an enormous growth in the use of VCPs in all kinds of organizations. VCPs are now the main mode of communication for many organizations as members are isolated in different locations under the default Work-From-Home setting. For example, at the National University of Singapore, students and professors use Zoom (from Zoom Video Communications, Inc) or Microsoft Teams daily for lectures and examination proctoring. Furthermore, a lot of companies believe that "permanent remote work is the future of work—pandemic or not" (Courtney), including big tech companies such as Apple, Amazon, and Adobe. According to *The Business Research Company*, the global market for VCPs grew to 7.78 Billion USD in 2020 and is expected to be 8.67 Billion USD by 2025 (The Business Research Company). This signifies the vast number of users of VCPs globally. Since all kinds of organizations use VCPs, the data handled over their networks varies from user's personal data to highly confidential national data. Like most internet systems, VCPs are not unassailable, its communication protocols and data storage procedures require sophisticated security design and measures, otherwise, without proper security implementations, it would lead to catastrophic consequences from data leaks to theft of trade/state secrets. For instance, in April 2020, there were 500,000 Zoom passwords being hacked and up for sale. Hackers used credential stuffing attacks to steal the passwords and even users' meeting links from Zoom's database (Winder).

Hence, it is crucial to understand the information security management practices employed by VCPs to ensure the security of consumers' sensitive data and their systems. This research report will focus on the prominent VCP companies, namely, Microsoft Teams, Zoom, Cisco Webex, and Google Meets. (*Table 1.2*). The research will first discuss how VCP corporations manage information security within their organization, analyzing how they minimize risks and the approach they take towards information security. Moreover, since organizations require VCPs for remote meetings and conferences, it is important to maintain their own security and compliance while using these VCPs, which will also be tackled by the research. The research is guided by the Cyber security Trifecta of People, Processes, and Technology (*Fig 1.1*), wherein Technology, the focus is on the information security delivered by the VCPs themselves. In People and Processes, the focus is on how consumers of the technology itself, i.e. organizations, implement cybersecurity processes and processes to ensure their member persons are compliant.

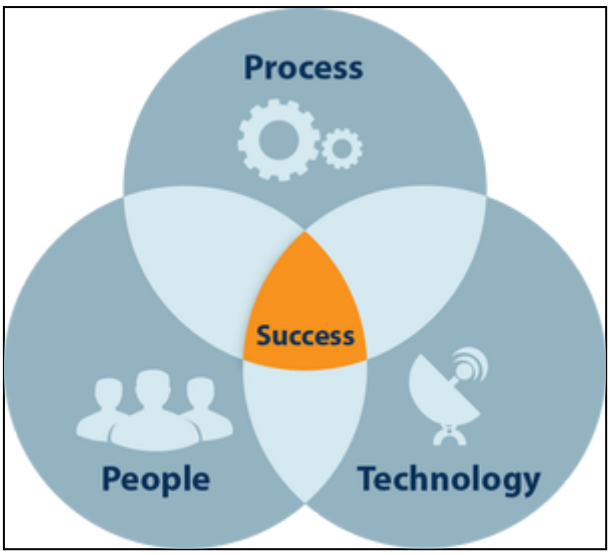

Fig 1.1 - Cybersecurity Trifecta of People, Process, and Technology.

Platform Name	Zoom	Teams	Meets	Webex
Company	Zoom Video Communications, Inc	Microsoft Corporation	Google LLC	Webex By Cisco

Table 1.2 - Table of platforms and respective companies analyzed in the report.

2. Information Security Management within VCPs

It is essential to analyze the security management of the VCPs themselves as service providers. How a service provider manages their information security internally and how they handle threats will form the basis of secure cybersecurity frameworks for consumers. This will also give a sense of the importance of maintaining cybersecurity to the respective service provider company.

2.1 Comparison of Placement of Cybersecurity Team in Company

Our analysis will start with looking at the structure and management of the information security team within the VCP organization to understand the role and importance of security within the organization.

Service Provider	Has a CISO? (Y/N)	Position Name	Level of CISO
Zoom Inc	Y	(Chief Information Security Officer)	Reports to CEO (N-1)
Microsoft Corporation	Y	(Chief Information Security Officer)	Reports to CTO, AI & Research (N-2)
Google LLC	Y	VP, Chief Information Security Officer, Google Cloud	Reports to CEO (N-1)
Cisco	Y	(Vice President, Chief Information Security Officer, EVP, Security & Collaboration)	Reports to CEO (N-1)

Fig 2.1.1 - Table of the placement of the security officer in the VCPs corporate structure. CIO refers to Chief Information Officer. CISO refers to the Chief Information Security Officer.

Based on the table above, all four VCP companies have their CISO in place. *The National CIO Review* states that a CISO's ability to sustain defenses against current and future cyber-attacks requires a high level of collaboration. Concerning the level of CISO, Zoom Inc, Google LLC, and Cisco's CISO all directly report to the CEO (N-1), which encourages effective and efficient information security development. Microsoft Corporation's CISO needs to report to the Chief Technology Office first. Such information might suggest that Microsoft is less efficient than the other three VCPs in high-level security management cooperation, but cannot be confirmed as other factors such as the large company size and its internal communication efficiency might alleviate this. In particular, Google has employed a full-time information security team of more than 250 security experts. It highlights the substantial importance that Google places on ensuring Google Meets is a secure service.

2.2 Comparison of Cybersecurity Practices within VCPs

Safe data transference, authentication, and access control are essential for both VCPs and users. This section will discuss the specific security measures and protocols implemented by each leading VCP and analyze the comparisons between the measurements.

2.2.1 Cybersecurity Practices within Zoom

According to the *Zoom Security White Paper*, Zoom uses a distributed network of multimedia routers (MMR) to connect the host and all participants' devices; the connection is dynamically routed between endpoints. During a meeting establishment, the Zoom application will use HTTPS to connect the Zoom server to get the necessary information to establish a meeting and meanwhile analyze the network environment to determine the MMRs and port to use, then it will automatically connect to the TCP port or UDP port of the device. If enterprise SSL proxies and higher compatibility are supported, Zoom Client can also connect via HTTPS. During the meeting, Zoom will encode all media data being transferred (shared screen, video, audio) using the Advanced Encryption Standard (AES) protocol at the application layer. For all other data (chat messages), Zoom will also encrypt those content using TLS encryption standards. Zoom implements an end-to-end encryption protocol for all data transmissions, which protects the encryption keys to be safely stored on the users' devices. No other third parties, including Zoom itself, have the accessibility to the keys. For chat messages within a meeting, Zoom claims that the secure message is only visible to the intended recipient. Zoom also provides Zoom Meeting Connector to allow users to deploy MMRs and host meetings within the user's internal network, which brings up more security and is preferred to use by corporations.

For authentication methods, Zoom uses role-based authentication, which requires a user name and a password; it also supports two-factor authentication for general users and SSO (single sign-on) for organizational users when signing in. Zoom's SSO interface is compatible with both OAuth and SAML. Moreover, Zoom allows the meeting host to choose who can join the meeting and who cannot. For instance, the host can select a particular list of email addresses and automatically disallow any incoming connections that are not in the list. When authenticating a connection request, a unique token is generated for each user and each session.

> "*Each session has a unique set of session parameters that are generated by Zoom. Each authenticated participant must have access to these session parameters in conjunction with the unique session token in order to successfully join the meeting.*"
>
> *-- Zoom Security White Paper*

2.2.2 Cybersecurity Practices within Microsoft Teams

Microsoft Teams also implemented many security encryptions. Because Microsoft is a giant tech company with a large number of products, it has its own security compliance levels: A, B, C, and D. Microsoft classifies each product into one of these four categories. In this case, Teams is in the C category, which means it is managed under a number of standards of security measurements, including HIPAA, ISO 27018, and ISO 27001 (Jones). Teams use end-to-end encryption and are

highly configurable. Moreover, it encrypts all data in transit and at rest and uses multiple encryption layers. All of its traffic takes place over the TLS/HTTPS encryption layer, as well as other Microsoft Office components. Teams also use MTLS for server-to-server communications and a combination of Secure Real-time Transport Protocol (SRTP) and TLS to encode client-side messages like video/audio sharing. Additionally, it allows users to encrypt messages with the user's custom key on top of service encryption. Other than the encryption protocols, Teams has also implemented endpoint protection and Advanced Threat Protection (ATP) to help secure all devices connected to your organization's network and detect malicious links or attachments (Laura). The same protection is also integrated with other Microsoft products.

Microsoft Teams supports Modern Authentication, a Microsoft implementation of OAuth 2.0, and it is highly configurable as well. It enforces organization-wide and team-wide 2FA and offers SSO through Microsoft Active Directory, which stores all policy assignments and user directory information (Tracy). Administrators can configure the authentication settings through Active Directory. Teams also support the configuration of Enhanced Key Usage (EKU) for server authentication (Tracy).

2.2.3 Cybersecurity Practices within Google Meet

Google Meet deploys a variety of security measures similar to Microsoft's approach. As stated in *Google Meet Security & Privacy for Users*, users generally do not need to configure the security settings much because most security controls are already turned on. Meet's infrastructure also ensures that all user data will be encoded in transit and at rest during any meetings by default. Google Meet uses SRTP to encrypt real-time media information and messages. Moreover, according to the online article *How Google Meet Keeps Video Conferences Secure,* it has implemented the Datagram Transport Layer Security (DTLS) protocol within the IETF standards instead of TLS to provide better security. For every meeting, a unique encryption key is generated by Meet, and it dies as soon as the meeting is over. The encryption key is transmitted via a secured and encoded RPC (remote procedure call) while establishing a meeting, and it is never stored on the disks. Additionally, Google has employed an information security team in charge of regulating and maintaining Google's defense systems and building customized security infrastructure to provide security measures to prevent dial-ins and video meetings from getting its control flow hijacked (*Google's Approach to IT Security*). For compliance purposes, Meet and other Google products are compliant with ISO 27001, ISO 27017/18, FedRAMP, SOC, and HITRUST (*How Google Meet Keeps Video Conferences Secure*).

Google Meet, as expected, supports multiple two-step verification options to securely sign in accounts, including "hardware and phone-based security keys and Google prompt." Anonymous users are not permitted to join a Google Meet meeting, and users must have a valid Google account with valid access permission to enter a meeting. Furthermore, users and organizational users of Google

Meet can configure their accounts to enroll in Advanced Protection Program (APP) which the user can get Google's most robust protections to avoid account hijacking and phishing attacks. As stated in *How Google Meet Keeps Video Conferences Secure,* Google also provides Access Transparency for organizations and educational institutions, which saves the logs of all read/write requests to the recordings preserved in Google Drive. Administrators can even require the accessors to provide a reason for the access.

2.2.4 Cybersecurity Practices within Cisco Webex

Cisco Webex implements a multilayer security model consisting of a data-center security layer and an application security layer. According to *Cisco Webex Meetings Security White Paper*, Cisco has an organizational structure of security management: a Product Security Incident Response Team, an Information Security Cloud Team, and a manner of Shared Security Responsibility in order to manage security processes throughout the organization. The Webex group has also been doing internal and external penetration tests regularly. For encryption measures of Webex, it uses TLS 1.2 protocol as the encrypted communication channel. After a meeting session is established, the connection is transmitted over TCP, UDP, or TLS. The media content is encrypted using ciphers based on either AES 256 or AES 128. Webex supports end-to-end encryption as well and uses SRTP between devices and services. No third party can get the encryption keys. For certification compliance, Cisco Webex is compliant with ISO 27001, SOC 2, SOC 3, CSTAR, and FedRAMP.

Webex's access control implements role-based access, and users are classified into five groups: Host, Cohost, Presenter, Panelist, Attendee, and Site administrator. As expected, Webex supports two-factor authentication, SSO, OAuth 2.0 based standardized authorization. Additionally, Webex supports risk-based authentication to "stop the risk at the point of access or adapt to the changing user authentication environment" (*Cisco Webex Meetings Security White Paper*).

2.3 Process in Place for Safe Storage of User Data

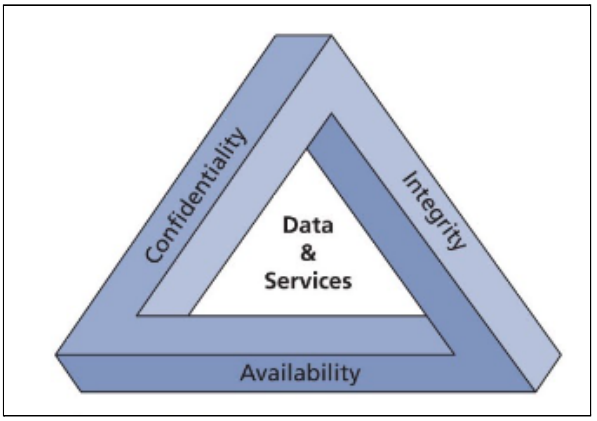

Fig 2.3.1 - The C.I.A. Triad

For data storage, VCP companies must follow adequate and rigorous security measures to ensure the safety of data servers and their data confidentiality, integrity, and availability of a C.I.A. Triad (Fig 2.3.1).

Zoom Inc claims to use worldwide distributed SSAE 16 SOC 2 Type 2 certified tier-1 colocation and commercial cloud data centers to process all real-time meeting data. Zoom provides a recording feature and the recorded video can be saved locally or on cloud servers. Locally saved recording files can be encrypted by the user; cloud-kept recording files, including shared files, chatbox messages, and text transcripts, are encrypted and password-protected or only be available to a specific domain of viewers. Moreover, the file owner can share, download, and delete his/her recordings (*Zoom Security White Paper*).

Microsoft Teams' solution is that any data which the user submits via Teams is kept and backed up in Microsoft Azure data centers, whether it's an instant message or a file. Azure is supplied in 54 worldwide regions, allowing users to preserve their data according to the area of their enterprise. Such processes imply that every piece of user data is preserved under the data protection legislation in effect in the location in which each company operates (Jones). The data stored in the data centers can be encrypted at rest as well. Moreover, Teams allows users/organizations to store data with a third-party storage provider, which means that organizations can choose to store their files in their own database (MicrosoftHeidi). Besides, to secure the C.I.A. of user's data, Teams is integrated with Data Loss Prevention (DLS) policy to ensure users don't send sensitive data with the wrong people (Laura).

Google Meet's recording files are preserved in Google Drive and are encoded at rest automatically. It complies with industry data protection standards and other data protection laws. Google has claimed that all data stored in the cloud will not be used for advertising or marketing purposes, and they do not store videos, audio, messages unless the user initiates a recording. Google's data center location is transparent; additionally, users can choose a specific region where they want their meeting recordings to be stored by using *data regions functionality* (*How Google Meet Keeps Video Conferences Secure*).

Cisco Webex utilizes switching equipment in multiple data centers across the globe. The majority of Webex Cloud services data is stored in Cisco's own data centers; for additional services, it can be delivered by private cloud instances such as SOC2 and ISO-compliant Microsoft Azure data centers and Amazon Web Services. Webex's data network also supports backbone connections, internet peering, caching, and global site backup. Data centers of Webex have deployed video surveillance and enforced 2FA, and it also implemented badge readers and biometric control for internal access control. Additionally, Webex data servers are classified into "trust zones" based on infrastructure sensitivity (*Cisco Webex Meetings Security White Paper*).

Section/VCP	Zoom	Microsoft Teams	Google Meet	Cisco Webex
Penetration Testing Frequency	Semi-annually	Semi-annually	Semi-annually	Semi-annually
Standards and Certifications	CSA STAR certification (based on IS027001), PCI DSS Certification, SOC2 Type 2 Privacy Shield TRUSTe,	ISO27001, ISO27018 Compliant, HIPAA Business (Jones)	ISO 27001, ISO 27017/18. HITRUST, FedRAMP, SOC	ISO 27001, SOC 2, SOC 3, CSTAR, FedRAMP.
E2E Encryption	AES (real-time media data), TLS (other data)	TLS, MTLS, SRTP, Endpoint protection and ATP, Custom key encryption	SRTP (real-time media data and messages), IETF, Unique one-time use encryption key	TLS 1,2, AES, SRTP,
User Authentication	Role-based Authentication, SSO with SAML or OAuth, 2FA available	MS' Modern Authentication, 2FA, SSO, Enhanced Key Usage	2FA, Google's APP available, Google's Access Transparency for organizations	2FA, SSO, OAuth 2.0, Risk-based authentication

Fig 2.2.1 - Comparison of cybersecurity practices within the VCPs

2.4 Process in Place for Handling and Reporting Attacks / Data Breach

No software is designed flawlessly. Even though the VCP companies have implemented many security measures to minimize the risks, there are always attacks that happen from time to time. When an attack or data breach occurs, it is important to see how immediately the company finds out the problem and reports the problem and how immediately the company solves the problem to minimize the damage.

2.4.1 Processes for Handling & Reporting Attacks in Zoom

Zoom does not provide an official document of how they process an attack. Still, they have a “Security Bulletin” web page that shows all the bugs/vulnerabilities of Zoom that existed before since 2018, with corresponding severity levels and detailed information. We can also find out the steps that Zoom took to handle an attack from actual cases. According to a recent article posted by Paul Wagenseil, a recent case is that on April 8, 2021, two analysts at the Pwn2Own contest demonstrated that they were able to hijack other users’ computers remotely by using vulnerabilities of the Zoom desktop application. Then, on August 13, 2021, Zoom fixed this flaw, and the software patches were available on September 30, 2021. It took nearly five months for Zoom to fix the vulnerabilities. Later, Zoom announced a new policy that "customers will be required to update their Zoom software to ensure it is no more than nine months behind the current version at any given time." (Wagenseil). Zoom has faced and performed rather poorly in terms of responding to data breaches with the speed and effectiveness of other VCPs. This might be because the company may not have had enough time and resource to prepare for the unexpected explosive growth in Zoom usage since early 2019. It is, however, now expanding, with a focus in R&D (Ang), so this indicates the possibility of improving security.

2.4.2 Processes for Handling & Reporting Attacks in Teams

On the other hand, Teams is doing well on the preparations. Microsoft has a Detection and Response Team (DART) that is in charge of responding to compromises and researching the latest attack methods, and Microsoft keeps doing attack simulation training regularly.

In order to handle potential attacks, Microsoft Trustworthy Computing Security Development Lifecycle (SDL) was used to build and develop Teams so that Teams can do well on handling common security attacks, including Eavesdropping, Compromised-key attacks, Man-in-the-middle attacks, Network DOS attacks, IP address spoofing, Spim, and RTP replay attacks (Tracy). A real case is that in early 2021, CyberArk, an access management vendor, found a vulnerability within Teams which allows potential attackers to get control of user accounts by using a malicious GIF file. After CyberArk published this vulnerability, Microsoft immediately patched it before any real attacker could utilize the bug (Jones).

2.4.3 Processes for Handling & Reporting Attacks in Google Meet

Google Meet has paid great attention to handling attacks, from incident prevention, incident detection to incident response. For preventing an attack or data breach, Meet has implemented automated network and system logs analysis which can identify malicious or suspicious activities. Google has a vulnerability reward program in which external security researchers can report potential

vulnerabilities to Google. In order to detect and handle an attack, Google has deployed multiple layers of machine learning mechanics to detect anomalous user activities across platforms. There is a dedicated subject matter team of experts employed to handle and report any type of data breach or attack (*Google Meet Security & Privacy for Users*).

2.4.4 Processes for Handling & Reporting Attacks in Cisco Webex

Cisco Webex has conducted penetration testing periodically based on internal assessors, and they also invite third-party vendors to conduct external penetration tests to detect vulnerabilities and get recommendation feedback. Once an attack or vulnerability is found, Cisco's dedicated Product Security Incident Response Team will be in charge of managing public disclosure of the vulnerability; meanwhile, the Cisco Emergency Response team will investigate the vulnerability comprehensively and try to prevent the threats. Everything about reporting and fixing is transparent (*Security Advantage for Webex White Paper*).

3. Information Security Management of Usage of VCPs Within Consumer Bodies

By evaluating each product based on the above-mentioned security practices, product design, and the product's individual security, security managers have the task of choosing the best VC solution that will best fit into their business and security requirements.

Due to the vast difference in the type of services provided, this research will adopt the concept of the Critical Information Infrastructure (CII) from Singapore's Cybersecurity Act 2018 and discuss the group of businesses that are considered CII and non-CII separately, focusing on how each VCP solution will fit into their business' security requirement. CIIs generally are required to have higher security standards due to the vitality and criticality of their data. Considering within the same category (CII or non-CII), different companies from various sectors will have additional requirements on how VCPs will aid their business and the types of security risks VCPs will expose them to. For example, a sales company might prefer a VCP which is user-friendly to connect people quickly. On the other hand, a production company might adopt VCP with stricter access control to better control who can attend their meetings.

Therefore, this section will focus on how different categories (CII or Non-CII) adopt different approaches when choosing and using VCP to ensure security and compliance data protection and privacy laws such as Personal Data Protection Act (PDPA), General Data Protection Regulation (GDPR) and the California Consumer Protection Act (CCPA), depending on their region. (Fig 3.1.1)

CII	Non-CII
Government, Infocomm, Energy Sector, Transport sectors (Aviation, Maritime and Land), Healthcare, Banking and Finance, Water, Security and Emergency, and Media.	Educational institutes, Retail business organizations, Entertainment industry (e.g. recreation)

Fig 3.1.1 - 2 general group of users - CII and Non-CII

3.1 VCP Usage Risks

Before discussing the appropriate guidelines and tools for users of VCPs to adopt, one needs to understand the risks that are related to user oversight.

For example, 'Zoom-bombing' was a common occurrence where attackers could join any ongoing meeting just by knowing the meeting number or meeting link and play highly inappropriate content during the meeting (Wagenseil). This was due to a lack of access control set by the creator of the meetings, such as passwords, so anyone was able to attend the ongoing meeting.

One other risk was the myriad of phishing scams. Due to the popularity of Zoom, many attackers aim to steal user credentials by sending phishing emails. Users were "informed" that they had their accounts suspended and had to reactivate through clicking a link and typing their login credentials (O'Donnell). Classic social engineering attacks take advantage of users' hurry or lack of attention to detail (Schoeman, Ahb & Irwin, Barry).

Cisco Webex also has security vulnerabilities relating to phishing. An open redirect attack could have been executed by an unauthenticated remote attacker to lure a user to their own malicious sites (Cisco Webex Meetings).

In addition to security vulnerabilities discovered, the Federal Trade Commission (FTC) has announced how Zoom's version of end-to-end encryption was deceiving since they still kept cryptographic keys generated for meetings which meant that Zoom was able to have access to all meeting contents (*FTC Requires Zoom to Enhance its Security Practices as Part of Settlement*).

Such security and privacy flaws are largely brought about when VCP users are not aware of how to use the VCPs properly. With secure usage practices in place, many organizations ensure that they minimize their usage risk as much as possible. Some of the actions taken below are discussed below.

3.2 Tools Used to Ensure Security

This section analyses the tools different CIIs and non-CIIs use to ensure their data is protected while using VCPs. The tools used by non-CIIs are usually a basis for the tools used by CII, where

CII's usage is more enhanced. eg. Customised rules for different user segments/ needs and training on securing meeting settings.

3.2.1 Tools Used to Ensure Security within Non-CII

Educational institutes often have existing relationships with VCP providers so the platform provided is already customized to the institute's needs ("Zoom for Education"), including restricting how and under what circumstances the company can collect and share student data. The platform may also come with preset settings, such as auto-muting new entrants and password access required and enabling end-to-end encryption provided by the platform (Lieberman). This makes it easier for non-technical organisations to take full advantage of the security solutions provided by the VCP. Often states have their own list of vetted VCP providers that educational institutes can use as a guide when selecting their VCP.

The entertainment industry also has similar requirements to educational institutes where they would want to broadcast performances for a "live" audience (Melendez). Thus they would be looking for VCP which will allow the performer or the technical staff to be able to control the meeting and prevent viewers from interrupting the performance, for example by unmuting themselves.

The sales industry might have different criteria as compared to the previous 2. Instead of broadcasting to hundreds of people at once, there is a need for more personal interaction from the sales agent to the potential customer. Importantly, the VCP chosen must also enable end-to-end encryption, not allowing any third party to be able to collect and share details of the meeting and client's data.

Zoom has a tool called "Security Button" that puts in place measures to ensure that access controls of meeting attendants are limited ("Securing Our Meetings - CIT - Wiki.Nus"). These include - locking the meeting once all the participants are in, limiting sharing of the screen only to the hosts, preventing participants from chatting, renaming themselves, unmuting themselves, and starting their videos. Google Meet and Microsoft Teams are able to grant teachers and staff members meeting creation rights and allow meeting creators to individually approve requests made by external participants before allowing them into the meeting. These restrictive access control tools are meant to ensure that "Zoom-Bombing" or similar threats are greatly minimized (Castelo).

3.2.2 Tools Used to Ensure Security within CII

Although CIIs require a higher level of security, government organizations are required to work across many other, possible external organizations. These organizations may not have the same access to the VCPs that CIIs do and can make standardizing communication difficult. Hence, a CII, for example, UK government organizations (gov.uk), have at least one type of VCP route that is open by default. This means that the platform can be opened for other organisations to access. To minimize

the risk of this, CIIs create a safe procedure that allows users to open access and communicate across organizations. This includes making sure tools are configured properly, testing them on end-user devices, and complete Know Your Customer (KYC). Hence the tools used will be similar to those implemented by Non-CII companies but are different through the implementation with stricter procedures.

3.3 How Employee Interactions Are Managed to Ensure Information Security

A chain is only as strong as its weakest link and for information security, it is no different. Having sophisticated technology might still be unable to catch any human errors due to the unpredictability of humans (Staff). Thus there is a need for proper procedures, instructions, and training for employees to minimize information security risk.

3.3.1 Minimizing the Risk of Using VCPs Through Training

Many organizations, both CII and non-CII, ensure that their employees are sufficiently trained to improve their security awareness so that they can fully utilize the appropriate meeting tools and practice safe cyber usage. This is usually done by having a comprehensive security awareness training program to instill a culture of security ("The Components of Top Security Awareness Programs [Updated 2019]"). For example, the Singapore government mandates that all organizations that operate CIIs put in place a cybersecurity awareness for their employees. For private organizations, the Cyber Security Agency (CSA) of Singapore also has resources that they can use to train their employees but this is not compulsory, as compared to for CIIs (Sagar et al.). Creating a set of guidelines is also essential for employees as it establishes good cyber practices and procedures to follow. Some standard practices and guidelines for VCP include (Ferbrache):

1. Creating a password for the meeting
2. Ensuring the 'waiting room' feature in VCPs is enabled by the host so that the host can choose who to allow into the meeting
3. Enabling only authenticated users to join the meeting so that the meeting cannot be accessed by anonymous users and locking the meeting after all expected participants have joined
4. Restricting screen sharing to the host only
5. Disable file sharing unless necessary

To balance usability with security, default settings are set based on the company's own guidelines wherever possible. These settings provide a quick way for employees to set up any meeting without needing to worry about their security settings, only requiring them to update their meeting settings for a certain feature that they might want to allow during that meeting (Assure Technical).

3.3.2 How Employee Interactions Are Managed to Ensure Information Security

For Non-CII industries such as educational Institutes such as the National University of Singapore, which uses both Teams and Zoom as their main VCP published an online guideline that educated users about Zoom and Teams, and the practices that can help them ensure their data is safe ("Securing Our Meetings - CIT - Wiki.Nus"). Some of these practices include: ensuring the 'waiting room' feature in Zoom is enabled by the host so that the host can choose who to allow into the meeting, enabling only authenticated users to join the meeting so that meeting cannot be accessed by anonymous users, and using the security button.

For CII industries, in addition to ensuring their users are well trained with the knowledge of properly using VCP during their work, these industries have to also ensure that their contractors and other third-party vendors are trained in the same way through their security awareness programs (Cybersecurity Act). One such example is the healthcare industry. VCPs can aid healthcare professionals in delivering consultations services with patients remotely. The Ministry of Health has come up with a guideline for telemedicine. This set of guidelines recommends healthcare professionals to verify their patient's identities again even after letting them into the meeting and to ensure that the VCP of choice allows for an end-to-end secure design to guarantee confidentiality and integrity of the session (*National Telemedicine Guidelines*).

3.4 Ensuring compliance while using VCP

Another aspect that companies have to consider is how to be compliant with data protection and privacy laws like GDPR, CCPA or PDPA, whilst using VCPs. However, during a VCP-based meeting, the VCP, usually a cloud-based service, is considered the data processor for the meeting. Thus as a consumer, to ensure that the company is still compliant with the above data protection and privacy regulations, the VCP has to be compliant with the regulation themselves.

3.4.1 VCPs compliance

Zoom's contractual commitments to GDPR and CCPA allow for its users their rights to access, erase, object to processing, rectification and restrict processing. Zoom has also promised to meet specific requirements from GDPR and CCPA (*Global Data Processing Addendum Agreement Zoom*).

Cisco Webex has committed itself to data protection and privacy by integrating these requirements into their product design in addition to the above rights to request access, correction, deletion, opt-out of sales, and non-discrimination (Cisco). Cisco Webex is also certified by Privacy Shield Principles for personal data based on GDPR and CCPA (Cisco, "Cisco Online Privacy Statement").

Google Meets has a comprehensive data protection and privacy commitment to many different regulations. Google commits itself to GDPR compliance in processing all customer data in all their contracts (Google Cloud). They ensure that they are specifically CCPA compliant by providing tools and offering specific products to address CCPA requirements for consumer rights (Google Cloud *The California Consumer Privacy Act & The California Privacy Rights Act Whitepaper*). Additionally, Google Cloud has taken specific actions as a Data intermediary to collect and use personal data limited to their stated purpose, be accountable to the consumer to access and correct their personal data. And to ensure that personal data is accurate, protected, and has a retention and transfer limitation (Google Cloud *Singapore's Personal Data Protection Act Whitepaper*).

Microsoft Teams incorporates privacy by design in all engineering and business functions alongside similar GDPR requirements for all personal data (Microsoft). Moreover, they are CCPA compliant due to their rigorous implementation to meet GDPR (Microsoft, "California Consumer Privacy Act (CCPA) FAQ").

3.4.2 Consumer compliance

Understanding that all of these VCPs are compliant with data protection and privacy laws as data processors, the organization the host of the meeting belongs to will assume the role of the data controller. Hence, it is important employees know how to set up their meetings to ensure that they have security settings that will comply with data protection and privacy regulations.

To ensure the principle of data minimization, default settings with minimal features should be set for all employees. This will allow users to only enable the features which they will be using during the meeting only if they need them. Features such as recording or other logging functions, if used during the meeting, must be acknowledged by all participants and participants should know where and how the recorded video will be stored and used (John and Wellmann 46).

4. Recommendations to Consumers of VCPs

As seen above, there are many factors in ensuring the safe and secure usage of VCPs. In this section, we provide a non-exhaustive set of recommendations for VCP consumers to consider after taking into account their security, compliance, and business needs. Moreover, as we have previously discussed how all VCPs are currently compliant with data protection and privacy regulations (Section 3.4.1), we believe that recommendations will focus on an organization's security and business requirements.

In general, organizations should thoroughly research their VCP to ensure it employs good standards and practices. They can check the certifications received by the VCP, such as a FedRAMP certification, especially for those based in the United States. This is especially better for CIIs as it has

requirements that are much higher than the typical baseline for industries (Recovery Point). Organizations that deal with citizens in the EU; gather data from EU customers should use VCPs that are GDPR compliant. Another measure of a VCP's implicit strength of cybersecurity is the placement of a cybersecurity officer in its organizational chart. Such nuances can help consumers decide which VCPs to use based on how they value data security.

Apart from choosing a VCP, organizations need to ensure their own usage of VCPs is secure, through the use of tools and staff training. As mentioned in Section 3, there are several different methods that organizations can employ to ensure the secure usage of VCPs, from tools common across VCPs to some VCP-specific options, such as Teams allowing users to choose 3rd-party storage providers to store the meeting data. Additionally, it is strongly recommended that organizations, even non-CIIs, provide employees with cybersecurity training because alert employees make up the last layer of security against attacks and breaches. Most governments put out informative resources that are pertinent to their country's cyber landscape and organizations can use these to set up their training program, because different jurisdictions may have different laws regarding cybersecurity so organizations must ensure they are complying with these specific laws, such as the CCPA or GDPR. These free-of-charge government resources are useful for SMEs to use when they do not have a dedicated IT team or resources to hire trainers.

4.1 Recommendations for Non - CII industries

For non-CIIs, the leading VCPs discussed in this paper are all suitable for general work usage. They each provide an acceptable level of security, with an organization chart that has considerations for cybersecurity. From our analysis, Google Meets boasts very secure features (Section 4.2). However, this may not be feasible in some circumstances, such as if the company already has in place an infrastructure with other email services. For many industries, governments also may be working together with VCPs to make it easier for businesses in that industry to integrate them into their practice. For example, many districts in the USA have existing contracts with VCPs (Lieberman, Mark), which ensures the VCP is complying with education privacy laws and district schools can use them easily. If no such recommendations are available, organizations should conduct a risk assessment to identify their information assets that are exposed when using VCPs and how vulnerable they are. For example, for IT consultancy companies, even though they are not dealing with critical information assets, they exist in a highly competitive field and may be more prone to attempts of data breaches from competing consultancy firms, who may be attempting to gather useful data about their competitors. Consultancy firms also need to communicate very frequently with external clients, which exposes their data to external networks. Hence, in this case, they would want to use a more robust VCP.

For the entertainment industry, we believe that Zoom is the best choice as they provide an all-in-one solution under the ZoomEvents platform. This can best benefit smaller to medium artists, those without a large team to help manage their upcoming virtual concerts. The capabilities of Zoom Events to manage ticketing, registration, and even analyze the statistics produced all together might be very attractive to these artists (Zoom). Standard security controls such as password authentication or disabling screen-sharing by participants are also present (*Zoom Video Webinar: FAQ*).

4.2 Recommendations for CII industries

For most CII industries, we believe that a highly secured VCP is more relevant to their industry needs. For industries that value secure information transfer such as government agencies, banking, and finance or other security and Infocomm industries, they might prefer to choose Google Meets which uses the more secure IETF instead of TLS (as in Teams, Zoom, and Webex) to transport its data as discussed in section 2.2.3. Moreover, Google has a large cybersecurity team which compared to the rest of the VCP, shows their larger commitment towards making Google Meets a secure service (Section 2.1). It also provides the option of enrolling into its Advanced Protection Programme, which provides an even higher level of user security.

However, as discussed in Section 3.2.2, a CII might still require a VCP which is much more accessible. We believe that Zoom, based on the additional meeting features, simple user interface, and experience. This can be seen in how the Healthcare Industry still uses Zoom for remote consultation purposes. For example, the Khoo Teck Puat Hospital in Singapore has a teleconsultation program built on Zoom. This is more beneficial than Google Meets as firstly, patients need not have Google account to make it easier for less tech-savvy patients to join a remote consultation meeting, and secondly, Zoom provides functionalities such as remote control, on-screen annotations, and consultation recordings (KTPH *Teleconsultation at Specialist Outpatient Clinics (TeleSOC)*).

4.3 Additional Considerations

The above recommendations for each industry are based on purely technical and high-level business perspectives. However, we understand that there are much more considerations to take into account such as current business deals which the organization already has. One such example would be an organization that is currently using Microsoft 365 Suite. Although Microsoft Teams can be used as a standalone VCP, as long as one has a Microsoft account, using it as a complete suite package allows better utilization of features. These include native collaboration on Microsoft's renowned productive tools like Powerpoint and Excel. Other integrations within Teams such as Outlook and OneDrive can improve the user experience using Teams as compared to other VCPs due to the simplicity and user-friendliness that benefits from the Microsoft 365 Suite (French). We believe that

organizations already under the GSuite package would similarly best benefit from using Google Meets considering their extensive cloud services and other integrated products.

5. Future Trends

As the workplace globalizes even further, video conferencing will still be mainstream in several organizations despite offices reopening. With the increasing prevalence of cloud services, artificial intelligence, etc, data spreads faster and further than ever before. Along with rising security and data privacy concerns, new regulations, policies, and guidelines are being put in place to protect the huge amount of data generated. For an organization to be successful, there is a need to embrace proper information security management. Organizations, if they have not already, need to properly choose and implement VCPs using the recommendations suggested above in a robust manner, keeping up with any new security issues that arise.

6. Conclusion

In this paper, we analyzed 4 leading VCPs, Zoom, Microsoft Teams, Google Meets, and Cisco Webex through the lens of the cybersecurity trifecta. In terms of technology, we saw that all the VCPs have some level of security robustness, with all the companies having a CISO in their organizational structure, and all the VCPs are at least IS027001 compliant. However, some platforms, such as Meets and Webex seem to have an additional focus on cybersecurity due to the additional features in place, and also as evidenced by the lack of data breaches that have occurred in these two platforms. After this, looking at the process part of the cybersecurity trifecta, of using VCPs, we saw that many CIIs and non-CIIs employ the tools available through these platforms to ensure their data on VCPs is secure. CIIs need more robust tools as compared to non-CIIs whilst non-CIIs often also look at maintaining usability for their external clients as well, so as not to hinder business growth. Under the People aspect of cybersecurity, many organizations provide training to ensure their employees use the VCPs in a safe manner. In many countries, such as Singapore, it is in fact compulsory for CIIs to provide employee cybersecurity training. This is to prevent employees from accidentally exposing critical data to external risk. Non-CIIs can employ their IT teams, hire external vendors or even use government resources to conduct these training, which is highly recommended. Finally, through this analysis, general recommendations were provided that all organizations can use to manage their cybersecurity risk when using VCPs, following which, more specific recommendations were provided based on the industry and nature of the company. However, users of VCP need to understand that risk cannot be completely minimized, there is always risk present and users of VCPs need to be vigilant and set in motion contingency plans in the event of data breaches.

References:

"Cisco Webex Control Hub - Security Advantage for Webex White Paper." *Cisco*, Cisco, 25 Aug. 2021, https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/webex-room-series/white-paper-c11-743769.html?ccid=cc001100&oid=wprco021742.

"Cisco Webex Meetings - Cisco Webex Meetings Security White Paper." *Cisco*, Cisco, 23 Feb. 2021, https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html.

Courtney, Emily. "30 Companies Switching to Long-Term Remote Work: FlexJobs." *FlexJobs Job Search Tips and Blog*, FlexJobs.com, 26 Oct. 2021, https://www.flexjobs.com/blog/post/companies-switching-remote-work-long-term/.

"Google Meet Security & Privacy for Users." *Google Meet Help*, Google, https://support.google.com/meet/answer/9852160?hl=en#zippy=%2Cencryption%2Csafety-measures%2Csecure-deployment-access-controls%2Cprivacy-transparency.

Google's Approach to IT Security. https://static.googleusercontent.com/media/1.9.22.221/en//enterprise/pdf/whygoogle/google-common-security-whitepaper.pdf.

"How Google Meet Keeps Video Conferences Secure | Google Cloud Blog." *Google*, Google, https://cloud.google.com/blog/products/g-suite/how-google-meet-keeps-video-conferences-secure.

Jones, Caltlin. "Microsoft Teams Security: How Safe Is Teams for Your Business?" *Expert Insights*, 31 Aug. 2021, https://expertinsights.com/insights/microsoft-teams-security-how-safe-is-teams-for-your-business/.

"Teleconsultation at Specialist Outpatient Clinics (TeleSOC)." *Khoo Teck Puat Hospital*, https://www.ktph.com.sg/patients/teleconsultation.

LauraWi. "Overview of Security and Compliance - Microsoft Teams." *Overview of Security and Compliance - Microsoft Teams | Microsoft Docs*, https://docs.microsoft.com/en-us/microsoftteams/security-compliance-overview.

"Make Video Conferencing Tools Work across Government." *GOV.UK*, https://www.gov.uk/guidance/make-video-conferencing-tools-work-across-government.

"Market Research." *Giving Intelligence Teams an AI-Powered Advantage*, The Business Research Company, Mar. 2021, https://www.reportlinker.com/p06033664/Video-Conferencing-Global-Market-Report-COVID-19-Implications-And-Growth.html?utm_source=GNW.

"Meet Security and Privacy for Education." *Google Workspace Admin Help*, Google, https://support.google.com/a/answer/9822731?hl=en.

"Microsoft Detection and Response Team (DART)." *Microsoft Security Blog*, 23 Aug. 2019, https://www.microsoft.com/security/blog/microsoft-detection-and-response-team-dart-blog-series/.

MicrosoftHeidi. "Location of Data in Microsoft Teams - Microsoft Teams." *Microsoft Teams | Microsoft Docs*, https://docs.microsoft.com/en-us/microsoftteams/location-of-data-in-teams.

MSFTTracyP. "Security Guide for Microsoft Teams Overview - Microsoft Teams." *Security Guide for Microsoft Teams Overview - Microsoft Teams | Microsoft Docs*, https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide.

"Privacy." *Zoom*, 1 Nov. 2021, https://explore.zoom.us/en/privacy/.

Sagar, Mohit, et al. "Singapore Government Committed to Educating All Government Employees on Cybersecurity." OpenGov Asia, 6 Apr. 2019, https://opengovasia.com/singapore-government-committed-to-educating-all-government-employees-on-cybersecurity/.

"Security Bulletin." *Zoom*, 11 Oct. 2021, https://explore.zoom.us/en/trust/security/security-bulletin/.

Staff, TNCR. "The Organizational Importance of the Chief Information Security Officer." *The National CIO Review*, 26 Apr. 2021, https://nationalcioreview.com/featured/the-organizational-importance-of-the-chief-information-security-officer/.

Wagenseil, Paul. "Zoom Security Issues: Everything That's Gone Wrong (so Far)." *Tom's Guide*, Tom's Guide, 19 Oct. 2021, https://www.tomsguide.com/news/zoom-security-privacy-woes.

Winder, Davey. "Zoom Gets Stuffed: Here's How Hackers Got Hold of 500,000 Passwords." *Forbes*, Forbes Magazine, 29 June 2021, https://www.forbes.com/sites/daveywinder/2020/04/28/zoom-gets-stuffed-heres-how-hackers-got-hold-of-500000-passwords/?sh=659ad4055cdc.

Zoom Security White Paper. https://explore.zoom.us/docs/doc/Zoom-Security-White-Paper.pdf.

"Zoom for Education." *Zoom Video*, explore.zoom.us/docs/en-us/education.html. Accessed 9 Nov. 2021.
Lieberman, Mark. "The K-12 Educator's Guide to Safe and Effective Videoconferencing." *Education Week*, 10 Dec. 2020, www.edweek.org/technology/the-k-12-educators-guide-to-safe-and-effective-videoconferencing.
Melendez, Steven. "For Artists, the Show Must Go On—and Zoom Is Their Venue." *Fast Company*, 24 Mar. 2020, www.fastcompany.com/90478442/for-artists-the-show-must-go-on-and-zoom-is-their-venue.
"Securing Our Meetings - CIT - Wiki.Nus." *Securing Our Meetings*, wiki.nus.edu.sg/display/cit/Securing+Our+Meetings. Accessed 8 Nov. 2021.
Staff, Alert Logic. "Why Are Humans the Weakest Link in Cybersecurity?" *Alert Logic*, 10 Nov. 2021, www.alertlogic.com/blog/why-humans-weakest-link-cybersecurity.
Wagenseil, Paul. "Zoom-Bombing: How to Keep Trolls Out of Your Zoom Meetings." *Tom's Guide*, 24 Mar. 2020, www.tomsguide.com/news/stop-zoom-bombing.
O'Donnell, Lindsey. "Zoom Impersonation Attacks Aim to Steal Credentials." *Threatpost*, 1 Dec. 2020, threatpost.com/zoom-impersonation-attacks-credentials/161718.

Schoeman, Ahb & Irwin, Barry. (2012). Social Recruiting: a Next Generation Social Engineering Attack. Journal of Information Warfare. 11. 17-24.
Assure Technical. "Video Conferencing Security Tips." *Assure Technical*, 8 Nov. 2021, assuretechnical.com/video-conferencing-cyber-risks.
"Global Data Processing Addendum Agreement Zoom." *Global Data Processing Addendum* , Sept. 2021, explore.zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf.

Cisco. "GDPR." *Cisco*, 26 Jan. 2021, www.cisco.com/c/en/us/about/trust-center/gdpr.html#%7Etab-our-program.
Cisco. "Cisco Online Privacy Statement." *Cisco*, 28 June 2021, www.cisco.com/c/en/us/about/legal/privacy-full.html.
Google Cloud. "GDPR." *Google Cloud*, cloud.google.com/privacy/gdpr. Accessed 10 Nov. 2021.
"The California Consumer Privacy Act & The California Privacy Rights Act Whitepaper." Google Cloud, May 2021.
"Singapore's Personal Data Protection Act Whitepaper." Google Cloud, Nov. 2020.

Singapore Parliament. Cybersecurity Act. No. 9 2018, 5 Feb. 2018, https://sso.agc.gov.sg/Acts-Supp/9-2018/. Accessed 12 Nov. 2021.

"National Telemedicine Guidelines." National Telemedicine Advisory Committee (NTAC) Members, Jan. 2015.

John, Nicolas, and Maximilian Wellmann. "Data Security Management and Data Protection for Video Conferencing Software." *International Cybersecurity Law Review*, vol. 1, no. 1–2, 2020, pp. 39–50. *Crossref*, doi:10.1365/s43439-020-00013-4.

"The Components of Top Security Awareness Programs [Updated 2019]." *Infosec Resources*, 15 Oct. 2020, resources.infosecinstitute.com/topic/components-top-security-awareness-programs.

Ferbrache, David. "9 Security Tips for Video-Conferencing." *KPMG*, 14 Apr. 2020, home.kpmg/xx/en/home/insights/2020/04/covid-19-hygiene-for-conferencing.html.

Cisco Webex Meetings. "Cisco Webex Meetings Open Redirect Vulnerability CVE-2021-1310." *Cisco*, 9 June 2021, www.cisco.com/c/en/us/support/docs/csa/cisco-sa-webex-open-redirect-PWvBQ2q.html.

FTC Requires Zoom to Enhance Its Security Practices as Part of Settlement , 9 Nov. 2020, www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement. Accessed 12 Nov. 2021.

Microsoft. "California Consumer Privacy Act (CCPA) FAQ." *Microsoft Docs*, 23 Aug. 2021, docs.microsoft.com/en-us/compliance/regulatory/ccpa-faq?view=o365-worldwide.

"General Data Protection Regulation - Microsoft GDPR." *Microsoft Docs*, 1 Oct. 2021, docs.microsoft.com/en-us/compliance/regulatory/gdpr?view=o365-worldwide.

The Business Research Company. "Video Conferencing Global Market Report 2021: COVID-19 Implications and Growth." *Report Linker*, Mar. 2021, www.reportlinker.com/p06033664/Video-Conferencing-Global-Market-Report-COVID-19-Implications-And-Growth.html?utm_source=GNW.

Castelo, Micah. "Why Videoconferencing Security Is Essential to Remote Learning." *Technology Solutions That Drive Education*, 24 June 2020, edtechmagazine.com/k12/article/2020/04/why-videoconferencing-security-essential-remote-learning-perfcon.

Recovery Point. “Why a FedRAMP Certified CSP Is Your Best Bet.” *Recovery Point Systems, Inc*, 2 June 2020, www.recoverypoint.com/blog/fedramp-certified-csp.

French, Darcy. “Microsoft Teams Review.” *TechRadar*, 8 Nov. 2021, www.techradar.com/reviews/microsoft-teams.

Zoom. “Zoom Events - Virtual Events Platform | Zoom.” *Zoom Events*, events.zoom.us/?utm_source=web&utm_medium=digital&utm_campaign=&zcid=4694. Accessed 13 Nov. 2021.

“Zoom Video Webinar: FAQ .” Zoom, Apr. 2021.