Josh Hatfield

INFO-I 330 (Section 9663)

Professor Abbott

13 October 2022

Capital Compass Consulting - Bring Your Own Device (BYOD) Policy

Overview

Capital Compass Consulting, originating from San Diego, is a mid-cap management consulting firm with 750 full-time individuals that has recently allocated part of its spending budget toward subsidiary office spaces in cities such as Houston, Tampa, Indianapolis, and New York City over the past year as a result of increased commerce. Given these circumstances, however, the firm does not intend to expand its services internationally until it can augment a more steady clientele to be able to raise capital using equity financing. The firm primarily serves small to mid-cap clients who may, for example, have strong business models in place but necessitate a more systemized coordination of their management overhead so that they can prioritize proliferating their businesses into new markets. With the increased use of Bring Your Own Device (BYOD) due to COVID-19 for facilitating transactions, communication, and confidential assets with clients, the following security policy highlights comprehensive stipulations that Capital Compass Consulting should follow pertaining to BYOD so that employees can safeguard the firm's reputation as well as uphold confidentiality (NDA) agreements procured for clients. Note: Any reference to the term "device" in the policy below refers to BYOD.

Policy

For better readability, this policy is sectionalized based on categories that stipulations should fall under so that similar stipulations may be grouped together:

On-Site Business Functions

1. Objective: To ensure device access for on-site business functions, employees should verify devices that would be denoted as BYOD. Host networks need to be able to confirm the addresses of devices in correspondence to the authentication provided, generate logs for documentation of device activity from packet headers, and block connections to destination addresses that are not specified in the allow list for firewall configurations.

    a. Requirement: All level 1 employee devices must be registered onto a site's host network using their provided employee credentials and accept the PKI certificate based on network configurations. Acceptable devices for level 1 employees include: laptops with macOS, Windows, or Linux operating systems installed; pre-approved Apple and Android devices; and pre-approved smartwatches.

    b. Requirement: All level 2+ (administrative) employee devices follow level 1 requirements, but level 2 employees must also provide an access code to login to the administrative network for elevated network access.

    c. Requirement: Outside of the designated intranet VPN tunneled through a site router, where encrypted communication is required with a subsidiary location, no employee is permitted to activate a VPN while on-site. Host networks must be able to generate logs for transmitted packets on all devices, and any internal address outside of the host may be considered malicious until audited by an administrator for verification.

2. Objective: To facilitate an allow list for firewall configurations, employees will conduct their on-site work through devices on the company intranet. This intranet guarantees that policies can and will be reconfigured since configurations will need to be flexible based on the conditions specified by the client.

    a. Requirement: Communication, file sharing, and any other functions relevant to the employee type must be conducted through the intranet, though pre-approved browsers are permitted for use outside of the intranet. Browsing privileges include low-risk browsing like industry research, but social media platforms and other non-work sites like streaming services should be blocked on the browser.

    b. Requirement: Although most sites outside of ones specified on the allow list will be accessible, all employees must receive approval for any site not using the HTTPS protocol or without an updated SSL certificate. If an employee is using an approved HTTP site, the site firewall should still indicate that all information on that site is transmitted through an unencrypted channel.

3. Objective: Confidential client data must not be disseminated outside of approved employees based on on-site employee functions, regardless if disseminated online or in-person using a device.

    a. Requirement: Approved employees are not permitted to take pictures of confidential client data. If any sensitive file or information is displayed on a device, employees may not have their mobile device visible in the vicinity of the device unless explicitly consulting the client to discuss this information.

    b. Requirement: Only devices given permission to view access for confidential data of a particular client should be able to access the associated files. It should be implied that employees using a device will not disseminate this information to other employees, regardless of locality, if they are not approved by the client.

Off-Site Business Functions

1. Objective: While employees work off-site, the extranet company VPN will ensure that communication is encrypted via tunneling to the site's host network, preserving confidentiality of client documents transmitted and stored on the intranet. Off-site functions for devices replicate on-site functions and policies due the physical linkage to the intranet using the extranet VPN.

    a. Requirement: Employees are required to always launch the extranet company VPN from their device when working remotely outside of the site host's network. After providing their credentials, employees can access documentation on the intranet remotely, where the same parameters apply for internal document permissions but can be handled externally.

Document Retrieval, On-Site and Off-Site

1. Objective: Clients should have the assurance that only designated employees may have access to their confidential information based on the conditions of their confidentiality agreement. Parameters are set in place with the contingency to limit the retrieval procedures for employees on devices so that documents remain internal.

    a. Requirement: Approved employees are permitted to communicate and share files with other employees assigned to the same client through the intranet. However, for downloading or replicating files onto the devices' storage to complete offline work, employees must enter their credentials and assume document expiration, whereby the document eventually locks until pushed upstream to its intranet location to match with the hash value.

    b. Requirement: Logs store who downloaded documents and when, and only administrators can establish file permissions.

Other Personal Business Functions, On-Site and Off-Site

1. Objective: All communication pertaining to business functions should be conducted through an intranet employee registry or an email address connected with the company's domain name to ascertain authentication given the threat of spear phishing.

    a. Requirement: For any business function with or without communication with a client, employees using a device must use the company intranet and/or their professional email address so that logs can determine whether the communication associated with the address matches with the device previously verified on the host network.

2. Objective: Malicious activities executed by employees should be monitored and remediated promptly to prevent injury to other employees or clients.

    a. Requirement: Permissions should be analyzed and updated frequently to reflect approved employees for confidential documents. Terminated employees must be removed from permissions, with logs monitored through human oversight for irregular requests like file downloads prior to termination or resignation.

    b. Requirement: An intrusion detection system will flag irregular activity such as number of file requests or packet payload sizes committed by employees on the intranet. Flags must be monitored through human oversight for determining remediation if necessary.

Client Site Business Functions

1. Objective: While consulting at client sites, employees may be handling sensitive financial documents that should never be stored in an unencrypted state.

    a. Requirement: Since employees must be using the extranet company VPN, the VPN router will only allow inbound financial documents when employees upload the documents using a secure portal located in the intranet if permitted by clients.

    b. Requirement: Paper documentation, if requested for transmission by a client, must only be faxed to a secure machine at a site's location using the portal.

2. Objective: In instances where teams are working at competitor sites, client documents for a team should never be transmitted or exposed to others.

    a. Requirement: Client documents, contingent on employee authentication, should only be accessed by the verified devices associated with the employee. New devices must also be manually reviewed for this protection mechanism.

Data Deletion and Remediation

1. Objective: In the instance of intentional or unintentional deletion of documents on employee BYODs, backup documents for clients should be always stored on an encrypted server accessible through the intranet unless specified.

    a. Requirement: Whenever employees create or finish working on a client document within a session, they should upload a copy of the document to the encrypted server. The same permissions and configurations should apply to the copy file as with the original document.

    b. Requirement: Employees should notify clients of this backup procedure and determine whether they are receptive to these documents created by employees to be stored on the server.

2. Objective: Clients should be able to request removal of their documents from the intranet. This entails documents previously procured by the client or documents created by employees and uploaded to a location on the intranet.

    a. Requirement: If requested by a client, all documentation and backup files associated with the client must be removed from all devices as well as the company intranet. Employees who downloaded documents for offline work, logged by the system, will be required to send this documentation to an administrator and sanitize/remove the files from their devices.

Justification

Although most of the policies above entail stringent or forbidden practices given the nature of consulting, especially in instances where multiple contracts are made to clients that are competitors, these policies needed to carefully enumerated since management consulting firms may have access to wide ranges of sensitive data stored by clients and therefore need to prevent any malicious against client confidentiality within these documents. For this reason, to prevent wrongful repudiation against employees for wrongful conduct, many of the policies tabulate an overarching requirement for all devices under BYOD to be maintained on a site's host network so that the company can verify devices that should be permitted on the network and ascertain the trail of actions conducted through a device from an employee since the employee will have already been authenticated.

Within the on-site business functions, the first primary objective is to tabulate devices through the sites' networks, as mentioned, so that the company can use multilayer authentication based on the PKI system that generates private keys for each device as well as

the credentials provided when an employee logs into the network. In turn, assuming that employees correspond to the device verification previously made, the company can log the actions made by employees on each device over the network, which may or may not be actively monitored but ensures that trails of logs were generated for any possibility of maliciousness committed; this oversight also coheres with the following policy where employees should not activate external VPNs outside of the ones designated for the company intranet and extranet so that the company knows every device that should be verified on their site networks. Moreover, as specified by the subsequent requirements, only devices pertinent to business functions should be accepted and verified onto the network since employees could abuse the confidentiality of clients when using devices like microphones or cameras. In consequence, we can see how these levels of assurance are easy to implement on the end of employees yet provide valuable insight into the behavior of the company when compartmentalized into individual device usage.

For many developing and larger firms that need to handle sensitive documentation, they may decide to utilize a company intranet so that the scope of the intranet limits the mechanisms by which employees can formulate malicious activities and increases the business intelligence in terms of security mechanisms such as, for example, employee permissions to sensitive documentation. Whenever an employee authenticates into the intranet, whether through the site's host network or with an extranet company VPN, all business functions will therefore be limited in scope to the intranet so that the company can limit the methods in which employees exfiltrate sensitive data onto their devices or through the internet for malicious intent. As a subsidiary permission in terms of browsing, there may be instances where employees need to easily access and compare publicized industry research for various sources, and due to the low-risk nature of exposure to this type of activity, employees are permitted to access these sources through browsers outside of the scope of the intranet for better readability and convenience. However, the firewall will still intend to obstruct access to most sites unless given approval by an administrator, which helps coalesce both convenience and safeguards against vulnerabilities like unencrypted data channels so that there is some level of freedom exercised yet protection mechanisms for devices in place.

As for confidentiality, consulting firms may need to sign NDAs based on an arbitrary set of conditions so that they have a legal obligation to maintain the confidentiality for a client when analyzing their documentation. For this reason, the company intends to prevent dissemination of any confidential documentation by forbidding the use of any camera whenever employees are on-site; furthermore, since many mobile devices have camera functionalities built in, employees should supplementarily not be allowed to have their mobile device visible or present in the vicinity of confidential information unless permitted by a client to communicate synchronously by phone or other means. While approved employees for confidential information may intentionally abuse this policy by taking pictures off-site, having the policy explicated for all parties and enforced for employees entitles clients legal reparation and/or action against the employee for violations to any stipulations substantiated within the NDA. Any dissemination otherwise, including physically showing another employee not approved to view confidential information, is likewise considered a violation of the NDA and will need to be monitored on-site for upholding this policy.

In terms of off-site functions, the requirement of an extranet company VPN replicates remote access to the internal environment so that all activities are similarly logged as with the on-site policies and employees are verified prior to access to confidential documentation (*Difference*, n.d.). With an intranet environment and association to the document retrieval policy, documentation cannot be exfiltrated to employees' device storage unless downloaded through

the portal on the intranet, and this importantly guarantees that employees cannot easily transfer files from the intranet to their personal devices unless an encryption wrapper is tagged to the file during the transfer. In essence, the premise of this policy allows employees to be able to download files to their devices if they necessitate work offline, but they can only access the files by providing their credentials, which confirms if they are actually permitted to access the file or not. By tagging expiries to files as well, employees are not permitted to access the file, for example, beyond the agreement with the client unless permitted, and this yields a salient practice to enforce renewal of the file expiration so that the system can log how long or in how many occurrences an employee sought to redownload a file onto a verified device.

Regarding personal business functions both on-site and off-site, which indicates any uncategorized functions that may relate to business yet does not necessarily need to fall under the scope of consultancy, it is important that the company can log where communication occurs so that all messages are accounted for if internal audits are required or the clients seek confirmation that an employee had not illegally disseminated information to unapproved employees, competitors, or individuals. Communication can easily be traced using an intranet employee registry so that logs generate who employees communicated to at specific times within the company and whether the employees should be communicating based on the confidentiality conditions archived for their clients. Employees are also free to use a professional email address for contact outside of the intranet, but including this policy means that they should remain tentative toward only communicating business functions through these channels rather than, for instance, personal email addresses or SMS applications.

For other personal business functions, there is obviously the concern that terminated or resigned employees can execute malicious activities against clients, therefore necessitating that the company has the defensive means to monitor and remediate these activities as soon as possible so that clients remain protected. Systems, for example, can scan file permissions, updates to file permissions, and any other irregular activity in relation to permissions so that only approved employees have access to their clients' confidential information. It should be assumed that terminated employees should automatically be removed from all permissions and be monitored prior to termination for irregular requests so that they do not attempt to steal large amounts of internal documents. Lastly, the company can mitigate unwarranted threats by actively flagging irregular activity, which can be as granularly applied as packet payload sizes, so that humans can review whether the alert is due to legitimate malicious activity.

The rationale for data deletion and remediation remains two-pronged in that documentation should be able to be safely deleted if requested by a client, yet all documentation should be backed up in the event that any document accidentally deleted can be retrieved from an encrypted server. For this reason, whenever employees finish a document and receive confirmation by the client to store a back-up file, they can conveniently confirm the upload process, which copies files with the same configurations to the encrypted server for storage. If clients request removal of all their documents, including copies, administrators will be able to retrieve all stored and offline files (preventing individuals from continuing to work on offline versions), send these documents to the clients, remove permissions, and safely delete the documents from the intranet using overwrite methods.

Finally, employees may need to travel to client sites to conduct in-person business functions and require protective measures in place to be able to uphold stipulations of the contracts procured for their clients. Within consultancy, employees may also occasionally need to handle sensitive financial and tax documents, and if the proposal requires storage of these financial documents for further examination on the company intranet, then only the secure portal

located on the intranet (accessed by the extranet VPN) should allow inbound financial documents. It should be subsidiarily assumed that employees cannot download these documents onto their personal devices at the client site since they will have already been logged into the extranet VPN. In circumstances where the client requires only paper transmission of these documents, then employees can secure them by faxing them to a secure machine at a site's location specified by the intranet's secure portal on devices so that they are not faxed to a team working with a competitor or other unapproved employees.

Connection

Although we can see how most of the policy and justification in relation to BYOD are very specifically defined to account for important parameters within management consulting firms like client confidentiality, we can also observe how these nuanced objectives and requirements mold well with readings as well as other concepts illustrated within this course. For example, employees within consulting firms may have fluid roles since the interpretation, direction, and team composition for one project may be vastly different than another within turnover periods, and it can be precarious to amalgamate their roles between these projects since it may influence inadequate practices by employees in regards to security or privacy of both the company and clients. In the journal article by Palen and Dourish (2003) for the Module 2 Privacy reading, they define concept of the "identity boundary" as a psychological phenomenon where individuals may affiliate with a social group to rationalize their individual actions, and within consulting firms where team members in one consulting project may eventually diverge into teams consulting for competitors, we can envision how conflicts could arise if prior members attempt to assist each other based on the group identities that they internalized (pg. 132). By clearly elucidating functions in relation to BYOD, where individual work and coordination exists based on the explicit permissions elucidated for the function in mind, a policy can subconsciously address the problems relating the identity boundaries so that employees have a clear expectation, without the room for interpretability, of their actions in relation to the "technologically-mediated environments" through BYOD (Palen and Dourish, 2003, pg. 132).

Another important concept mentioned within the readings, from an organizational level, is the benefit of deploying a strong security system in mind that aligns with client incentives since security as an externality for clients based on the dependency on the system itself can help or hurt the reputation of the consulting firm that seeks to earn their confidence for negotiating contracts (Anderson and Moore, 2006). As Anderson and Moore (2006) accentuate in their journal article from the Week 2 Security reading, clients will be less inclined to endorse systems of companies that misalign their own interests with those of the clients, and if there is no transparency in ascertaining the liability of companies so that they cannot obfuscate their incentives from their clients, then they can lose the confidence of their clients, especially in the event that a security vulnerability causes a negative externality for these clients. Based on this reading in class, my policy attempted to be as transparent as possible in terms of the mechanisms, permissions, and remediations in place using BYOD so that the company's incentives align with its clients'; also, the policy ensures that clients have complete agency based on their own incentives so that they can specify which documents, employees, and functions should be applied for the services rendered, assuring that there is no ambiguity with the policy stipulations in mind. If the policy can reflect the benefit of security as an externality as the company's clientele continues to grow, then more businesses will be inclined to work with the company with confidence that it will value their incentives regarding privacy and security.

While completing the Module 5 Learning Activity for Privacy, one of the most puzzling and sometimes frustrating aspects of the experience when analyzing Facebook's privacy policy was how disorganized it felt when attempting to navigate to or index a certain topic (Abbott, 2022). Although my policy is not as extensive or far-reaching as Facebook's policy since I only focused on BYOD stipulations, I intuitively tried to categorize stipulations together, which were further indented for objectives and requirements, so that readers can narrow down searches based on both the categories and indentations made. Moreover, I sought to list the categories contingent on their association to one another so categories would reasonably lead to similar ones, and employees would not have to navigate the policy or scroll several times for comparison between categories that should be listed together. Ultimately, I was able to accomplish this using an iterative process, where I first specified the categories I thought would be relevant and then added or removed these as I continued to formulate my policy.

Finally, I thought that it was important to encapsulate a strong design structure of security and privacy for employees in a way that would not necessarily hinder their ability to perform business functions yet still enmesh these functions with this design structure so that they could be more aware of the consequences of their accountability for others. This ideology is exemplified in Cavoukian et al.'s (2010) journal article from the Module 7 Privacy reading, where they note, "The fact is that *Privacy by Design* and accountability go together like innovation and high productivity. You can have one without the other, but it is hard" (pg. 408). If there is any ambiguity regarding *Privacy by Design*, then the policy has failed to accomplish one of its overarching tasks, and the company cannot hold any one individual accountable for increasing literacy since the policy itself does not support the design structure. In a way, this accentuates to employees why security and privacy are so valued from a company perspective, and as highlighted in the first paragraph of this section, clients can see the explicit avenues in which security and privacy are entrenched in the design of the BYOD policy when handling their data. All parties should feel comfortable with the design structure in place for security and privacy, but they should not need to feel overwhelmed since the policy is sectionalized into clearly defined business functions for reference.

Conclusion

Overall, the components specified above attempts to compose a BYOD policy for a hypothetical management consulting firm, who intends to grow a strong client pool and hopes to do so by enumerating a policy that gives confidence toward a set of security and privacy practices. Categories range from device verification at on-site locations to document retrieval, which further define various objectives for these categories and requirements that can help assure that they are met. The justification and connection sections after the policy demonstrate how aspects of the policy were determined as well as try to give credence to why they relate to the materials we have discussed throughout this course.

References

Abbot, J. (2022). *What's in a Privacy Policy?* [Class handout]. Indiana University-Bloomington, INFO-I 330.

Anderson, R., & Moore, T. (2006). The Economics of Information Security. *Science*, *314*(5799), 610–613. https://doi.org/10.1126/science.1130992

Cavoukian, A., Taylor, S., & Abrams, M. E. (2010). Privacy by design: Essential for organizational accountability and strong business practices. *Identity in the Information Society*, *3*(2), 405–413. https://doi.org/10.1007/s12394-010-0053-z

Difference between Intranet VPN and Extranet VPN. RF Wireless World. (n.d.). Retrieved October 13, 2022, from https://www.rfwireless-world.com/Terminology/Intranet-VPN-vs-Extranet-VPN.html

Palen, L., & Dourish, P. (2003). Unpacking "Privacy" for a Networked World. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, *5*(1), 129-136. https://doi.org/10.1145/642611.642635