Southern New Hampshire University
Capstone

2024

Cybersecurity Capstone

Alexander J. Hankes
Southern New Hampshire University

Hankes, A. J. (2024). Cybersecurity Capstone (Southern New Hampshire University).

Cybersecurity Capstone

Alexander J. Hankes

Southern New Hampshire University

ISE – 690 – 10918 – M01

Instructor Bryan Bechard

September 29th, 2024

Table of Contents

Consulting Problem One: Memo of Recommendation

TO: Sarah Tashima, *Chief Information Officer*

FROM: Alexander Hankes, *Security Consultant*

DATE: September 29th, 2024

SUBJECT: The Sonya Project

Intelligent virtual assistants (IVA) offer personalized and digitally enhanced customer service experience to streamline the evolving requirements of our business clients by leveraging generative artificial intelligence. As a leading global provider of outsourced customer service, Callego has commenced an assessment of the merits and security considerations of IVA technology with the Sonya Project.

Summary of IVA Technology

IVA technology depends on machine learning and natural language processing to simulate human conversations with customer inquiries. Conventional uses of IVA include web-based chatbots and digitalized voice assistants. Leveraging an autonomous interpretation of human words, messages, and even specific phrases, IVAs deliver a personalized answer to a customer's request effectively without supervision by a customer service specialist (Teet & Kesrarat, 2023). The primary advantages that IVA technology provides for customer service operations are to improve accuracy, boost operational response rates, and provide a personalized experience for our client's customers (Sieja & Wach, 2023).

Furthermore, IVA technology can help provide accurate natural language options for inquiries made by non-English speakers when translation services and or resources are not immediately available to assist (Chowdury et al., 2018). In addition, all customer inquiries can

be automatically recorded and analyzed for data-driven actionable insights to ensure that Callego maintains a competitive advantage with the implementation of the Sonya Project (Sieja & Wach, 2023).

Understanding how IVAs work

As a simulated customer service agent, IVAs rely on modular-based system architecture to detect and determine how to respond to a customer's inquiries (Atasoy & Kocyigit, 2021). When a customer interacts with an IVA, multiple modules record, swiftly interpret, and accurately generate a response in a natural language to assist the customer's needs. In advanced inquiries, an IVA can quickly route the customer to a human customer service agent for swift remediation. However, there are several security and compliance considerations when evaluating the adoption of emerging technologies and innovations. These include data security, privacy risks, and upcoming regulatory requirements such as the European Union's recently adopted Artificial Intelligence Act (*The AI Act Explorer | EU Artificial Intelligence Act*, 2024).

When assessing all necessary governance, risk, and compliance considerations involving the upcoming Sonya Project, Callego leadership must evaluate both the potential benefits and drawbacks. Customers and call center operations staff may struggle to embrace generative AI technology because the human brain is hardwired to resist unfamiliar concepts and changes. This psychological response, known as AI-related technostress, may arise particularly if the adoption and training period is unnecessarily rushed (Choudrie et al., 2023). Furthermore, all data resources, communications, and system architecture hardware and software integrations adopted face their own unique challenges when implementing adequate security controls with emerging technology. Additionally, Callego leadership must review all necessary controls to

provide proper storage, encryption, and monitoring to protect against known and emerging threat vectors arising from the adoption of IVA technology (Chung et al., 2017).

Security Considerations

As part of an IVA's primary functionality, its use of natural language processing additionally presents security challenges such as being susceptible to algorithmic bias. Algorithmic bias involves human, systemic, and computational bias that accidentally may generate misleading responses based on the customer's inquiry in relation to data about the customer in comparison to unrelated records such as data ingested from our business clients (Fifelski, 2023). After consumer complaints in 2019, Apple and Goldman Sachs Bank were investigated by the State of New York for leveraging algorithmic bias in their artificial intelligence systems for calculating risk of new Apple Card applicants by gender (Vigdor, 2019). While the investigation concluded in 2021 that no regulatory violations were found, it highlights the legal risks of deploying technology that relies on natural language processing (*DFS Issues Findings on the Apple Card and Its Underwriter Goldman Sachs Bank,* 2021).

In addition to the risks of algorithmic bias with native language processing, Callego must be mindful of the regulatory compliance standards of our business clients are met with the implementation of the Sonya Project. Privacy of sensitive data such as protected health information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA) for our United States-based clients in the healthcare industry establishes data privacy standards for patient healthcare information (Evans, 2023). Our financial clients also have their own unique regulatory requirements depending on where they operate in the global economy, which must be scrutinized to avoid compliance violations. NLP in the scope of human-machine interactions and the data ingested that occurs because of leveraging an IVA must be carefully evaluated against

our client's own regulatory and compliance requirements to avoid any unexpected loss of clientele. Furthermore, the current lack of industrial security standards for both AI and IVAs being properly enforced may present a security risk arising from a lack of historical insight into emerging vulnerabilities and exploits (Blasch et al., 2019).

Common Attack Vectors with IVA technology

The prevalence of IVAs for both consumer households and enterprise environments has grown in the past decade to over 8.4 billion units by the end of this year per industry forecast (McKee & Noever, 2023). Like other targeted platforms, a higher population of units historically has attracted adversaries to explore exploiting for profit. When exploring both current and historical adversarial attack methods targeting IVAs, it is important to understand that human – machine interactions are not exclusive when exploring potential threats.

Voice-recognition functionality in popular IVAs products such as Apple's Siri and Amazon's Alexa products have been found to be vulnerable to subliminal commands that human ears are unable to detect (Smith, 2018). This type of attack technique is known as content injection where an adversary may compromise an IVA to gain initial access for further harm (*Content Injection, Technique T1659 - Enterprise | MITRE ATT&CK®*, n.d.). In relation to the Sonya Project, this form of attack could be leveraged by adversaries attempting to exploit the human-machine communication trust inherent in modern IVAs relying on acoustic-based interactions which could disrupt data integrity, availability, and confidentiality (Zhang et al., 2023).

For chat-based IVA integrations where all interactions take place digitally such as on a website, it is important to understand the potential attack vectors that arise from limitations of modern generative AI functionality. While chatbots are not a new concept and have existed for

decades, adaptive IVA for chat-based communications allow customers to communicate with an IVA using natural language in real-time (Qammer et al., 2023). The primary risk with IVA-based chatbots is when an adversary uses what is known as a prompt-injection attack. In late 2023, a Chevrolet car dealership deployed an IVA chatbot to its website that relied on Chat-GPT's deep learning models, and one individual was able to secure a new truck for $1.00 (Sherry, 2023). Social engineering and focusing on exploitation of the human – machine communication trust can allow adversaries a method to compromise the integrity of data ingested for an IVA.

IVA Security Controls

Security controls allow us to reduce the attack surface for our people, processes, and technology from current and emerging threats. Any actions, processes, techniques, hardware, or other security measures that reduce the attack surface are examples of security controls for Callego (Gutierrez et al., 2006). With the adoption of emerging technology for an enterprise, it is important to acknowledge that security experts may not have had sufficient time to clearly document all potential threat vectors. However, with IVAs like the Sonya Project, adversaries are primarily targeting present weaknesses arising from human-machine trust using injection techniques.

Ultimately, computers and system architecture have been designed to trust human-based inputs as a source of absolute truth. Revisiting the previous analysis of common attack vectors for IVA technology, the Information Security team can uncover potential vulnerabilities that may impact the Sonya Project and offer beneficial countermeasures. In the first example, acoustic injection exploits arise from a failure to establish systemic controls and scope for what sounds an IVA should consider as human speech. With the rise of 'deepfakes' which synthetically generate

human speech to spoof a targeted victim, it is important to explore security safeguards that detect vocal inconsistencies and authentication technologies (Somers, 2020).

In the second example, we reviewed a chat-based injection attack that allowed an adversary to leverage the human-machine trust to purchase a vehicle from a dealership with unauthorized terms. This exploit arose from a failure to properly scope and establish controls to limit the chatbot's abilities to what was necessary for its functions and impose the objective of least trust to complete its designed purpose (Sherry, 2023). With both examples, a targeted security risk assessment process should have been leveraged to review any threats, vulnerabilities, or attack vectors before implementation. In addition, proactive monitoring, vulnerability scanning, real-time detection and response tools can help safeguard the Sonya project and Callego's people, processes, and technology from emerging threats (Finlay, 2024).

Next Steps

With consideration of Callego's commitment to ensuring its operations rely on effective tools to provide quality customer service for our clients and their customers, several security initiatives should be reviewed. By limiting scope and functionality of an IVA using least trust methodology, Callego leadership should review and consider implementation of the following security recommendations provided on the next page (*Figure 1 – 1: Proposed Security Initiatives*).

#	Proposed Security Initiatives	
1	**Security Control:**	Implement End – to – End Encryption using modern network standards and security methodologies.
	Ease of Implementation:	Medium Effort
	Reason:	When end – to – end encryption is enforced, the ability of a third party such as an attacker to intervene or listen in is not feasible.
2	**Security Control**	Implement identity proofing technical controls or operational procedures to automatically validate a customer's identity.
	Ease of Implementation	Low Effort
	Reason:	It is imperative that processes and procedures are in place to perform verification automatically or through being routed to a live customer service agent to verify the customer's information and/or confirm the individual is authorized to have access.
3	**Security Control**	Adopt a security training and awareness program for all employees.
	Ease of Implementation	Low Effort
	Reason:	To reduce risk of AI – technostress and bolster our incident response and reporting processes for the Sonya Project, it is important that security awareness training occurs for both the owners of the project, and those impacted by its implementation.
4	**Security Control**	Ensure that the Sonya Project's architecture and functionality is scoped using least trust methodology.
	Ease of Implementation	High Effort
	Reason:	To help ensure that the Sonya Project is not susceptible to an injection attack that exploits unused features or permissions, it is vital that only the functionality that is activated is the minimum the IVA needs to function without impact
5	**Security Control**	Review and adopt compliance requirements with the EU's Artificial Intelligence (AI) Act
	Ease of Implementation	High Effort
	Reason:	Starting in 2027, the European Union is expected to start enforcement of all requirements of the AI Act for our European business clients.

Figure 1 – 1: Proposed Security Initiatives

Consulting Problem Two: GDPR Compliance: A Revised Privacy Statement

When conducting business across geopolitical entities, it becomes necessary to understand the spectrum of requirements for handling and protecting data. Organizations desiring to do business with European partners and consumers must comply with the General Data Protection Regulation (GDPR) enacted by the European Union (EU) (Torre et al., 2020). Recently, the Chief Executive Officer (CEO) of Callego announced a strategic alliance with Spatzchen, a customer-service outsourcing agency headquartered in Berlin, Germany (*Southern New Hampshire University*, 2024). As part of Callego's Information Security team, it is essential that a review of our current privacy statement and associated documentation is conducted to ensure any potential compliance requirements associated with GDPR are effectively addressed.

To aid in revising our present privacy policy, the United States Department of Commerce in coordination with the European Commission enacted the EU – U.S. Data Privacy Framework program (*Data Privacy Framework*, 2024). As a replacement to the EU – US Privacy Shield and the United States Safe Harbor Program, the EU – U.S. Data Privacy Framework (EU-U.S. DPF) was enacted after an agreement for transatlantic data protections was reached in 2022 (Determann et al., 2023). The Data Privacy Framework established a self – certifying process and guidance for domestic organizations handling any data flow from citizens of the EU (*Joint Statement on Trans-Atlantic Data Privacy Framework*, 2022). Additionally, the EU-U.S. DPF provides necessary guidance to meet GDPR data privacy and disclosure requirements across seven industry standard privacy principles and 16 legally binding supplemental principles to enhance all European and associated transatlantic privacy considerations (*Data Privacy Framework*, 2024).

On the following section, both the original and revised subsections of Callego's privacy statement will be provided as well as any required in consideration of GDPR security principles. For each subsection, an explanation for any modifications will be provided as well as any necessary justifications under GDPR requirements. Furthermore, an evaluation of potential impacts and organizational – focused considerations will be further examined from the proposed revision of Callego's privacy statement against the current strategic mission, operations, and workplace culture.

Revised Privacy Statement

A. About this Policy

Original:

[Not present or missing]

Revised:

As a global leader providing quality customer service operations, Callego (hereby referred to the "Company", "We", "Us") is committed to protecting the privacy of our partners, clients, and those who we assist on behalf of our clients. We conform with the EU-U.S. Data Privacy Framework as determined by the United States Department of Commerce in accordance with the European Commission and the EU's General Data Protection Regulation (GDPR) requirements for personal data and sensitive information.

For further information about the EU-U.S. Data Privacy Framework and to review Callego's certification status with the U.S. Department of Commerce's International Trade Administration (ITA), please visit: https://www.dataprivacyframework.com.

Explanation of approach:

When revising or developing legal documentation that will be provided to the public, it is vital that a scope and purpose is clearly defined. This section, which was not present with the original privacy statement, establishes common terminology such as defining the company affiliated with the statement and a summary of intent to meet any applicable privacy requirements.

Justification under GDPR:

Callego is a business entity which falls within the scope of a data controller as defined by the GDPR (Beems, 2021). As a data controller, Callego is required to provide all data subjects with the purpose of their activities when processing personal data, their privacy protections, as well as other requirements further provided in this privacy statement as outlined in *Article 13 – Information to Be Provided Where Personal Data Collected from The Data Subject* of the GDPR. This purpose of the privacy statement specifies a scope, the controller, resources, and a summary of any applicable or necessary compliance frameworks.

Potential Impacts:

By including the purpose of the privacy statement, Callego offers a legal disclosure to the public of its responsibilities and applicable regulatory scope for how it handles data. This focus of transparency can help applicable data subjects understand that they may have rights and control when it comes to their personal data. However, by specifically recognizing a specific framework or scope focusing only on the GDPR, in the future there may be legal implications for specific jurisdictions where consumer rights may fall under a stricter requirement.

B. **Data we Collect**

Original:

In order to conduct our business and provide valuable services, we collect personal and non-personal data about our customers.

Revised:

To properly conduct our business and provide valuable services, Callego may collect personally identifiable information (PII) to verify customers' identities and provide helpful information in accordance with any current or prospective client / partner service agreements. All personally identifiable information means that the data or information references an identifiable individual or data subject such as a living person. Examples of the information and data we collect may include personal details such as:

- Name
- Location information (Address, telephone numbers, email addresses)
- Sensitive personal identifiers (Your date of birth, medical record number, government identification number, provider information)
- Demographic information

Connection information (such as network connection latency, IP addressing, mobile phone, and/or carrier data)

Explanation of approach:

It was also important to consider the merits arising from the original statement that disclosed usage of non-personal data. Callego defined that its operations handled non-personal data in the original policy. However, non-personal data is not a requirement when approaching

GDPR compliance which is why it was removed from the original privacy statement (Torre et al., 2020).

Justification under GDPR:

When evaluating how the revised policy exhibits standards of due care under GDPR, it is important to note that GDPR data protection requirements for personal data only applies to sensitive, personally identifying information (PII) and not any anonymous data collections (Bernadini, 2023). Any data or information which relies on pseudonymization, which involves replacing personal data identifiers with generic, unidentifiable information, should be treated as personal information (Zerdick, 2021). PII may include any data or information that if used, could reveal or be linked to a specific individual using identifiers such as the following information classifiers:

- Name (full name, last names, maiden names, etc.)
- Contact information (email, physical addresses, mailing addresses, telephone numbers, location data)
- Physical characteristics (Race, Gender, Nationality, date of birth / age, photographs, etc.)
- Device or access (cookie IDs, device details, IP addresses, MAC addressing)
- Health information (Medical record numbers, diagnoses, disabilities, medical records)
- Financial data (credit card information, banking or account information) (*Principles of the GDPR*, 2024)

Potential Impacts:

While the original privacy statement generally covered both personal and non-personal data, it may be beneficial to disclose data that undergoes through pseudonyms to ensure legal accountability and transparency.

C. **How We Collect Data**

Original:

We collect data directly from our customers in the course of ordinary business. We also acquire customer data from third-party sources.

Revised:

All data we collect comes directly from our clients, partners, and their customers in accordance with any recent, prospective, or actively on-going service agreements or associated inquiries.

Third party sources of information may include data resources from any clients, partners or affiliated customers as defined by a service level agreement which may include systems and technologies with access not managed or maintained by Callego.

Explanation of approach:

With the original privacy notice, the vagueness can help from a liability reduction strategy for any legal concerns or proceedings against Callego. However, when relying on both the EU / US Privacy Framework and the GDPR, it is vital that context is provided for any partnerships or third parties and what data is processed by such external entities.

Justification under GDPR:

Article 13 of the GDPR specifically provides what information should be provided to by the data controller to the respective data subject. Furthermore, *Article 14* and *29* of the GDPR

requires that the data controller disclose if any PII is transferred to an external entity such as a partner or in cases where data is transferred to Callego by a client.

Potential Impacts:

Client data systems may provide data connections for the purpose of allowing Callego to act on behalf of a client for customer service operations. In this type of instance, Callego acts under the authority of the client to process PII often on instructions by the client's contractual obligations. From the focus of organizational impacts, the revised privacy statement focuses on disclosing that there may be contractual obligations which allow or grant the organization to collect PII from external entities. This could come under potential scrutiny by clients as well as in legal challenges such as being too narrow in scope.

D. **How We Use Data**

Original:

We may use customer data to develop new services, personalize existing services, or for other purposes such as research and business development.

Revised:

Callego limits the use of personally identifiable data collected to only what relevant data is necessary to complete a request in accordance with any recent, prospective, or actively on-going service agreements or associated inquiries.

All data collected may be acquired for the purpose of validating a customer's identity to provide personalized information, satisfy sensitive requests such as medical or financial account information, diagnostic summaries, or providing accurate information when requested. By using any of our services and/or products, you provide consent to the collection of any relevant information deemed necessary to complete a request.

Explanation of approach:

Originally, I sought to combine both how data was used and the following subsection on storage of data to allow an oversimplification of the topics. However, after reviewing the articles and principles of the GDPR, I found that this could become unfavorable for the organization's considerations towards reduction of risk and legal liability. One of the primary considerations I wanted to explore was the importance of implied consent by the data subject should they not exercise their rights to their PII.

Justification under GDPR:

When exploring the use of implied consent with the GDPR, it is important to understand what justifies any data processing first having the interactive consent of the data subject. GDPR defines that any processing can be considered lawful so long as the processing meet at minimum one of six activities (*Art. 6 GDPR – Lawfulness of Processing - General Data Protection Regulation (GDPR)*, 2023). Furthermore, should there be a purpose which falls outside the activities defined in Article Six of the GDPR, we shall ensure that the reasons for processing data coincides with the reasonable expectation of what is considered expected considering the nature of the data collected.

Potential Impacts:

One of the most significant changes from the original privacy statement and the revised version exploring how the organization uses any data it collects is the focus on purpose and limiting the use of data to what would be reasonable. This focus could allow a cultural adoption of being mindful of what data is used in the production environment. By embracing the privacy

of PII, Callego can demonstrate its commitment against competitors for embracing a privacy-centric approach.

E. **How We Store Data**

Original:

Callego customer data is stored at our corporate offices, on our networks and computing systems, and at the offices, networks, and computing systems of third-party partners, affiliates, suppliers, and vendors. .

Revised:

Callego maintains datacenters around the world, however we apply a standard of protection described in this privacy statement regardless of jurisdictional requirements. Some of the data we process may be completed outside of the country where you reside. We may retain any data we collect for longer periods of time for legitimate business and legal purposes such as for security and financial recordkeeping activities.

We use encryption to keep your data private while it is in transit and when stored. All personally identifiable information is stored and maintained in accordance with EU-U.S. Data Privacy Framework by Callego with appropriate security controls to protect all stored data from loss, misuse, and unauthorized access. Any personal data collected and retained is automatically anonymized after a period of time.

Third – Party providers such as partners, affiliates managed systems are required to meet or be complaint with industry-specific regulatory requirements described in this privacy statement.

Explanation of approach:

One of the challenges when disclosing where data may be stored or located is generalizing any specific details to honor the principles of transparency and technology neutrality arising from the GDPR. Thus, it was important to fall back on the privacy framework which the organization was leveraging to ensure compliance with the GDPR.

Justification under GDPR:

When any data is collected from a data subject, you must ensure that any explanation of how data is processed, stored, or transmitted is concise and easily understood as part of the upholding the principles of transparency and communications to advise the public of their rights when applicable (Wolford, 2023).

Potential Impacts:

F. **Marketing**

Original:

We may contact our customers for marketing and promotional purposes

Revised:

We may contact our customers for marketing and promotional purposes. This data does not include any sensitive or personally identifiable information except for the following information:

- A customer's contact preferences
- Location information (such as telephone, address, and email address information)
- Name

Any data for the purpose of marketing research undergoes anonymization to ensure that any personally identifiable information is sanitized.

Explanation of approach:

Marketing and advertising activities often fall within scrutiny of any consumer protection laws and privacy-driven security frameworks. While Callego operates across the world in multiple call center operations for their product and services, it is important to approach the use of a data subject's information carefully to ensure that any language is clear and concise to avoid the risk of any legal implications or regulatory violations.

Justification:

The GDPR provides clarification regarding data processing for marketing activities such as providing the data subject having a right to object to direct marketing within *Recital 70* (GDPR.eu, 2019). However, it requests that any disclosure to the public should be segmented within a subsection that focuses only on all data protection rights. Legal considerations arising from GDPR enforcement, should consider the outcome of the Italian Supervisory Authority's judgement against Eni Gas e Luce where marketing data was used despite the data subject opting out (Koch, 2023).

Potential Impacts:

Disclosing the use of marketing practices with data collection and use can often confuse consumers who do not understand or are in favor of keeping all of their PII private. However, it is vital that by providing this information, Callego shows that it is willing to be transparent and uphold the principles found within the GDPR.

G. **Your Data Protection Rights**

Original:

[Not present or missing]

Revised:

In accordance with ensuring that clients and their customers understand that they may opt out of any marketing information or need access to their personal information, we offer our clients and their customers the following in accordance with all respective regulations data security frameworks:

- Request a copy of all information we may have collected that is personally identifiable along with access records. When applicable, we may provide pertinent details of how the information or data is stored, retained, and/or destroyed.
- Correct any information or data that is personally identifiable to the requestor that was inaccurate or out of date.
- Deletion of any personal information for lawful purposes or is no longer required for business purposes.
- Opt-out of any marketing or promotional usage of personally identifiable information.
- Restrict access to a set party or parties to personally identifiable information.

Explanation of approach:

One of the primary considerations that the GDPR focused on was establishing clear expectations of the controller to educate the public about their privacy and protection rights when data was collected or processed. In the original policy, this section was missing which meant that any disclosure in consideration of allowing Callego to be committed to meeting all regulatory and legal requirements.

Justification:

In properly adhere to GDPR, an organization that must collect or process data from any individuals or entities must communicate to the data subject the rights they have to their own personal information (Wolford, 2023).

Potential Impacts:

For competitors, the use and language of disclosing that the data subject has rights over their own data by Callego demonstrates that they are likely to conduct business within the scope of GDPR operating requirements. From an organizational perspective, disclosing rights to those who have their data must also be ingrained on operations and employees for when a consumer decides to leverage their privacy rights. This may include new operation procedures, communication guidelines, and processes for communicating and remediation of protected rights.

H. **Privacy Statement of other websites and partners**

Original:

[Not present or missing]

Revised:

This Privacy Policy does not extend to any websites or business entities such as clients and partners and pertains only to Callego and its subsidiaries.

Explanation of approach:

When exploring the potential impacts of a revised privacy statement with consideration to the partnership with Spatzchen, it may be worth noting that having an EU partner may create the opportunity to have the partner assume ownership of any data protected by GDPR as a responsible entity and controller. A responsible entity acting as the controller for EU citizens

and associated data may alleviate or limit liability for Callego for any risk of violations from mishandled data from vendors and unmanaged third parties. However, it is important to clarify this issue with Spatzchen as the partnership may meet the scope of joint controllers.

Justification:

Upon review of the GDPR, it is important to provide guidance for ensuring that any scope defined within the statement only applies to Callego from a legal focus. Furthermore, additional considerations arising from the partnership may meet the scope of joint controllers and that our policies would need to be unified to ensure compliance (Wolford, 2023).

Potential Impacts:

As noted, the primary impacts may fall against legal obligations and the need for a clearly defined scope.

I. **Changes to this Policy**

Original:

[Not present or missing]

Revised:

Callego reserves the right to modify or change this Privacy Policy at any time for any reason. When updated, we will post the updated privacy policy and reach out via contact preferences to our clients, partners, and their customers.

The last revision to this policy was made on September 29th, 2024.

Explanation of approach:

When approaching GDPR compliance requirements using the US / EU Privacy framework, one of the primary focus is providing additional details for when the policy was last updated and a brief summary of how and when the policy is updated and communicated.

Justification under GDPR:

The GDPR focuses on establishing communication requirements along with providing citizens of the EU more controls over their personal data (Wolford, 2023). The purpose of this section, which was not present or missing in the original privacy statement, is to inform any applicable data subjects that when there is any modification to the privacy statement it follows a communication process.

Potential Impacts:

Providing when a policy was last revised that is available to the general public is vital for when regulatory or compliance frameworks are updated, and the privacy statement may not reflect recent changes or laws. Furthermore, by providing notice that any modification to this statement will be communicated demonstrates that Callego is willing to ensure that its data processing activities are transparent, and privacy focused.

J. **How to Contact Us**

Original:

[Not present or missing]

Revised:

For any requests, questions, comments pertaining to this policy or to exercise your rights in regard to your personally identifiable information, please contact us by one of the following methods:

By e-mail: privacy@callego.com

By writing to us at:

Callego

Attn: Privacy Office

123 Main Street

Dallas, TX 75201

Explanation of approach:

Missing in the original privacy statement, it is vital that when a data subject or member of the public is concerned or wants to exercise their legally protected rights to have contact information with the proper parties able to handle their requests.

Justification under GDPR:

Article 12 of the GDPR focuses on the rights of the data subject to being provided transparent information on their rights to their personal data and having a proper understanding of how to exercise their rights. The data controller is responsible for ensuring that any request by a data subject is addressed within a reasonable timeframe (Wolford, 2023).

Potential Impacts:

By providing this information, you allow any parties concerned as well as regulators have a way to contact the organization that does not relay on publicly available channels. Furthermore, this contact method points to the stakeholders responsible within the organization who are qualified and prepared to address any privacy, regulatory, or legal request within a reasonable timeframe.

Consulting Problem Two: Top – Three Policy List

In 2023, approximately 55% of businesses reported that they incorporated organization policies to help bolster the security of their production systems (Elad, 2024). Security policies within an organization are developed to ensure the confidentiality, integrity, and availability of managed devices, identities, and data resources. Recently, the chief executive officer of Callego announced during the latest all-hands townhall that a strategic alliance was formed with Spatzchen based in Berlin, Germany. When evaluating the effectiveness of a business' ability to respond to critical threats, it is imperative to establish organizational policies which align with both jurisdictional and industry best practices.

Introduction

Jurisdictional boundaries represent one of the main challenges for multinational business organizations. Legal, regulatory, and relevant compliance requirements must be thoroughly understood by organizational leadership in consideration of expanding operations into new regions, countries, or industry sectors. Since its adoption in 2018, the European Union's (EU) General Data Protection Regulation (GDPR) applies to all businesses who compile and retain data stemming from EU citizens as part of their day-to-day operations, including those residing outside of EU jurisdictional boundaries (Blind et al., 2023). The primary focus of the GDPR is to ensure that businesses are transparent with how they collect, store, process, and use personally identifiable data (Kulkarni et al., 2023).

Organizational policies empower leadership by defining the foundation which all other procedures, processes, standards and guidelines acquire their authority (Andress & Leary, 2016). In consideration of achieving GDPR compliance, the EU / US Privacy Framework was developed to empower commercial operations conducting business within the United States meet

all necessary requirements when required to adhere to the GDPR (*Data Privacy Framework*, 2024). In respect to the recent partnership between Spatzchen and Callego, there is a need to triage and revise three critical policies to ensure that our people, processes, and technology are prepared for managing personal data from EU citizens. From an information security perspective, the following organizational policies must be reviewed, created, or revised:

- Data Protection Policy
- Incident Response Policy
- Access Control Policy

Data Protection Policy

The purpose of a data protection policy is to outline how Callego manages, retains, and secures data from both personally identifiable information (PII), and non-PII sources. When reviewing all data protection requirements from the GDPR, it is important to approach any focus of data security and protection areas with reliance on the regulation's seven core principles (Han & Park, 2022). All personal data must be processed, stored, and maintained in a manner that ensures its confidentiality, integrity, and availability up to and including from unauthorized use, loss, destruction, or damage through both technical and administrative controls (*Art. 32 GDPR – Security of Processing - General Data Protection Regulation (GDPR)*, 2016). Furthermore, in order to have the policy comply with the GDPR, a data protection policy must clearly define and implement technical controls such as applying encryption standards along with maintaining records of all data processing activities (*Art. 30 GDPR – Records of Processing Activities - General Data Protection Regulation (GDPR)*, 2018).

When approaching the creation or revision of a Data Protection Policy, with consideration to the legal and regulatory requirements arising from the GDPR, it is important to

rely on a document standard for all organizational policy documentation. A purpose and goal should be defined along with a general scope, documentation, and any legal or security frameworks identified. Applicable technical and administrative controls and countermeasures should refer to any applicable regulatory or legal requirements. A list of any applicable regulatory articles should be potentially included for which the organization must certify as part of its compliance with the EU / US Privacy Framework (*Data Privacy Framework*, 2024). In conclusion, it is also important that there is a classification taxonomy used for identifying policies as well as a document version control for tracking any necessary changes (Gobeo et al., 2020).

It is crucial to understand the importance of establishing a defined balance between the organization's needs and mission against security risks and controls. When companies prioritize fostering a culture of safe data practices, their people, processes, and technologies are effectively able to harness the value of their data assets and ensure its protected from misuse (Helemski, 2024). A policy which establishes a standard of data protection requirements must focus on data governance and access management with considerations to the organization its applied to. However, if the security controls it adopts are too robust, there can be impacts to operations and productivity.

Alternatively, when an organization fails to provide adequate safeguards for their data assets, the consequences arising from a data breach can lead to financial , reputational, and legal damages as well as a loss of consumer trust (Helemski, 2024). In consideration with the GDPR, a failure to adopt adequate data protection standards can result in fines and regulatory penalties. Article 84(4) of the GDPR authorizes fines of up to 10 million euros or in cases of undertaking

up to 2% of an organization's global operational turnover from the preceding fiscal year (*Fines / Penalties - General Data Protection Regulation (GDPR)*, 2021).

Data Protection Policy
Last updated: 09/20/2024

Policy No. INFOSEC-DPP-1020.0924
Effective: 10/05/2020
Policy Owner: Information Security

PURPOSE
Callego implements and maintains reasonable security and data protections to ensure the confidentiality, integrity, and availability of data processed in accordance with the following security frameworks:

- National Institute of Standards and Technology (NIST) Special Publication 800-53
- EU / US Privacy Framework

SCOPE:
All organizational managed technology, endpoint devices, data, and identities

POLICY:

1. All data processed in any form in the scope defined are the property of Callego.

2. All systems, network technology, and data transmitted on behalf of Callego must be encrypted using modern encryption standards to ensure applicable data protections.

3. Callego and any affiliated entities covered within the scope of this policy are responsible for ensuring the privacy and security of all confidential information. This includes administration, storage, and destruction or sanitizing of all data sources.

4. Any destruction or disposal of data will be done in accordance with jurisdictional laws and regulatory guidelines using the Callego Data Preservation Schedule and following organizational disposal procedures.

5. All data within the scope of this policy shall be accessed in accordance with organizational roles and scope of work.

6. Any suspected violations such as misuse, accidental loss, malicious destruction, and unauthorized access must be reported to Information Security.

7. Callego employees and any affiliated entity may not intimidate, threaten, coerce, or take any retaliatory action against an individual reporting a suspected violation.

Figure 2 - 1 – Proposed Data Protection Policy

Incident Response Policy

The purpose of an incident response policy (IRP) is to provide a high-level focus for the organization on how it prepares and responds to a security event (CISA, 2021). This policy is best developed prior to the organization responding to a major security incident. Upon review of all policies and procedures obtained from Callego leadership, it is important to note that while there are standard operating procedures for information security staff, an IRP has not been created. The expectations when developing a written IRP are to provide the following:

- Identification of key stakeholders
- Roles and responsibilities
- Incident Reporting process for employees
- Communication planning
- Relevant security frameworks and compliance requirements

The GDPR's regulatory requirements when it comes to handling data as a controller, there are several considerations that may impact an IRP policy. Upon becoming aware of a data breach or respective security incident, the GDPR specifies that a breach notification according to Article 33(1) must be within 72 hours to the supervisory authority. A critical characteristic of the GDPR's breach notification requirements is ensuring that any notification requires an adequate scope, consequences, impact, and all measures taken to remediate or lessen the damage from a security incident (Wolford, 2023). Thus, it becomes crucial that an incident response plan incorporates a communication standard for when a security incident is suspected. Timely reporting allows incident response teams to properly scope and develop a containment strategy to limit further compromise or impact.

Outside of the GDPR's breach reporting requirements, an IRP can help Callego establish a clear communication channel for its employees and concerned parties, such as customers, to report any reasonable security concerns to be evaluated by an internal information security team or through the use of a managed security service provider (MSSP). Additionally, documentation and technical review of any reported security concerns must be considered to ensure that each security incident maintains forensic evidence, scope, and cause meets organizational procedures for responding to an incident. An IRP policy develops an organizational baseline or standard that must be met for any incident response which can aid in timely reporting to regulatory bodies.

However, forensic reports arising from incident response procedures may have an impact on the organization's legal liability. Forensic reports arising from incident handling involving a data breach are often the target by plaintiffs in any cyber-related litigation events (Koskey & White, 2021). However, to address concerns of discovery activities arising from an IRP child processes and procedures, for major security incidents, an external forensic entity should be leveraged to shield internal documentation and provide an unbiased report for any potential legal proceedings. Additionally, access to any internal incident documentation should be restricted from access by roles who are not involved in incident response activities (Koskey & White, 2021).

Incident Response Policy
Last updated: 09/20/2024

Policy No. INFOSEC-IRP-0924.0
Effective: 09/29/2024
Policy Owner: Information Security

PURPOSE
Callego's incident response plan provides necessary guidelines when a security event occurs. A security event may include when there is a reasonable suspicion of malicious activities or indications of compromise that need to be remediated. The goal of this policy is to ensure that any security events are properly investigated with consideration of ensuring business continuity of Callego's enterprise operations.

SCOPE:
All organizational managed technology, endpoint devices, data, and identities

POLICY:

1. Callego recognizes that malicious activities may include both internal and external threats. These may include compromised systems, loss, corruption, and unauthorized activities and other actions which impede upon confidentiality, integrity, and availability of data and managed information systems.

2. Callego and all entities identified in the scope of this policy are responsible for safeguarding and protecting sensitive information arising from malicious activities.

3. All suspected security incidents must be reported to the Information Security Department immediately by the following contact methods:
    a. By phone: 1-800-450-1234 ext. 1
    b. By email: infosecurity@callego.com

4. Any security breach of personally identifiable information must be reported to the Chief Information Security Office immediately. The Chief Information Security Officer is responsible for reporting any breach notifications to applicable legal, regulatory, or Callego executive entities within 72 hours.

Figure 2 - 2 – Proposed Incident Response Policy

Access Control Policy

An access control policy (ACP) provides the requirements for how access is managed and for which considerations in which access is appropriate (Hu et al., 2017). The purpose of an ACP is to further ensure the confidentiality, integrity, and availability of data against accidental or malicious destruction, errors, unauthorized access, and loss. Additionally, ACP from a high-level focus defines all necessary rules and guidelines that define how digital identities meet any conditions to be granted specific information or technology resources (Shan et al., 2024). *Article 32* of the GDPR establishes the considerations and requirements for addressing the security and access controls surrounding the security of data processing.

When exploring the importance of an ACP against the GDPR's primary objective of ensuring appropriate and transparent privacy rights for EU citizens as data subjects, a policy focused on access control is vital to limit the risk of misuse. Article 25(2) of the GDPR specifies that a data controller "shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed".

By employing the principle of least trust, Callego can leverage a ACP to enforce that any data processing and access is only performed by authorized employees with a focus on limiting access to only what is needed for a role's business activities. Furthermore, enforcing auditing and logging requirements for all user identities as well as enforcing identity access controls such as requiring multi-factor authentication can ensure that when access is leveraged, an identity can validated for access authorization and their activities monitored.

In consideration of Callego’s core values, and strategic focus towards meeting GDPR compliance to protect its recently announced partnership with Spatzchen, the enforcement of an

access control policy can demonstrate the organization's commitment to meeting any security requirements across the world. Furthermore, it will allow the organization to establish automated monitoring and actions for when unusual behavior access occurs to its information systems.

Access Control Policy
Last updated: 09/29/2024

Policy No. INFOSEC-ACP-0924.0
Effective: 09/29/2024
Policy Owner: Information Security

PURPOSE
Callego access control policy ensures that all identity access management controls are implemented with consideration of technology security policies, standards, and procedures, and regulatory compliance requirements.

SCOPE:
All organizational managed technology, endpoint devices, data, and identities

POLICY:

1. It is the responsibility of the IT Department in conjunction with the Information Security team to establish and monitor access conditions and roles for all employees, guests, customers, and vendor identities within the following activities:

    a. Establish a procedure for the creation, modification, of any changes impacting or restricting access for user identities.

    b. Review access for the purpose of ensuring compliance and enforcing account access requirements on a re-occurring basis no less than once every 12 months

    c. Ensure that Callego's managed systems have a process to automatically disable inactive accounts and restrict access based on risk assessments.

    d. Ensure that all managed systems automatically audit and log account modifications, including enabling, disabling, and removal actions with timely notification to Information Security.

    e. Enforce that any non-security functions or activities rely on a non-privileged identity as deemed appropriate and segment any roles needing access to security functions to having a separate account for any privilege access.

2. Information Security and the IT Department shall employ the principle of least trust, allowing access in accordance with only the minimum requirements for users to complete their daily business functions.

3. Information Security shall enforce a limit and lock out period for a series of unsuccessful logon attempts within a specified timeframe in accordance to NIST Cybersecurity framework.

Figure 2 - 3 – Proposed Access Control Policy

Consulting Problem Two: Technical Controls Recommendation

Effective July 2023, the European Commission approved the use of the EU – U.S. Data Privacy Framework (Bryant, 2023). This decision acknowledged that the EU – U.S. Data Privacy framework demonstrated satisfactory protection requirements in alignment with European Union's adoption of the General Data Protection Regulation (GDPR) for cross – border data transfers (Manfredi, 2024). With the recent announcement of Callego's partnership with Spatzchen is expected to proceed starting October 30th, 2024, it becomes vital to effectively prepare for self-certification leveraging the EU – U.S. Data Privacy Framework by exploring additional technical controls to ensure compliance with GDPR.

Introduction

To further support compliance with GDPR requirements, Callego's Information Security Department has been tasked to adopt technical controls in accordance with Article IV of the EU – U.S. Data Privacy framework which requires organizations to "reasonable and appropriate measures to protect" personal data. A technical control involves a hardware or software component used to ensure the confidentiality, integrity, and availability of organizational systems, network resources, and endpoint hosts managed within the enterprise (*Technical Controls*, 2024). Additionally, due to the leadership's latest initiative to officially begin our partnership in a month's time, it becomes vital to recommend technical controls that effectively align Callego's people, processes, and technology and our revised privacy policy.

Control I: Implement a Security Information and Event Management (SIEM)

Technical Control: Implement a Security Information and Event Management (SIEM)			
Description	**Scope of functions**		
A SIEM is an automated tool to support real-time analysis of an event using a centralized log management system and storage of all system event and access logs in near real – time.	Network Components	Host Devices	Applications
	X	**X**	**X**

Figure 2 – 4 Identification and function scope of SIEM implementation

When evaluating the potential focus for ensuring compliance to GDPR, ensuring adequate security controls meet all regulatory and data handling considerations is paramount. A SIEM provides log management from a centralized management system and aids in the detection of potential security events and log retention of all systems within the organization's infrastructure (Johnson et al., 2019). Furthermore, a SIEM covers a variety of hardware, network resources, and application monitoring to ensure that continuous monitoring and alerting for effective incident response occurs when there is a security event detected. As part of the security domains, a SIEM provides benefits for organizational security operations.

Capability Maturity Model States (Present and post-implementation)						
Level 1 (Initial)	Level 2 (Repeatable)	Level 3 (Defined)	Level 4 (Managed)	Level 5 (Optimized)	Present State	Future State
Implement-ation is needed, not yet explored. Non-existant	Implemented, but lacks defined processes	Processes defined, systematic improvements in progress	Systematic improvements deployed, functionality may need further tuning or advanced modifications	Tuning and functionality workload focused on maintenance and updates to functionality	Level 1	Level 3

Figure 2 – 5 CMM Considerations for SIEM Implementation

Using the capability maturity model (CMM) for further exploration of implementation improvements, current enterprise architecture lacks a centralized log management system or modules to help ensure that security operations actively monitor all managed systems and user

identities appropriately. Using best practices, it is important to note that post deployment, there is a reasonable expectation for an improved future state over time. Level 5 (Optimized) state is likely within the next 12 to 24 months.

At present, Callego does not rely on a SIEM solution and is at the initial stage leveraging the capability maturity model (*Capability Maturity Model (CMM)*, n.d.). However, it is crucial that impacts which may arise from deployment, such as fiscal considerations, ease of implementation, and any potential impacts to be considered from existing infrastructure hardware and application components when exploring this technical control. SIEMs can be managed internally or through a third party such as a managed security service provider (MSSP) for monitoring system logs and security events. On average, a SIEM may cost on average 50,000 USD to over 10 million annually due in part to licensing considerations, organizational size, and data ingestion and storage costs (Logpoint, 2024).

Control II: Deploy a User and Entity Behavioral Analytics (UEBA) solution

Technical Control:	Deploy a User and Entity Behavioral Analytics (UEBA) solution		
Description	**Scope of functions**		
UEBA solutions rely on user-based risk detections, entity activity tracking, and user profiling and calculation scores to determine insider risk (Khaliq et al., 2020	Network Components	Host Devices	Applications
		X	**X**

Figure 2 - 6 Identification and function scope of UEBA solution implementation

To further enhance our security controls, the use of a user and entity behavioral analytics (UEBA) solution can help ensure that identities managed by Callego are properly scrutinized and monitored. UEBA solutions rely on user-based risk detections, entity activity tracking, and user profiling and calculation scores to determine insider risk (Khaliq et al., 2020). The primary device scope of a UEBA includes managed identities and endpoint devices.

Capability Maturity Model States (Present and post-implementation)						
Level 1 (Initial)	Level 2 (Repeatable)	Level 3 (Defined)	Level 4 (Managed)	Level 5 (Optimized)	Present State	Future State
Implement-ation is needed, not yet explored. Non-existant	Implemented, but lacks defined processes	Processes defined, systematic improvements in progress	Systematic improvements deployed, functionality may need further tuning or advanced modifications	Tuning and functionality workload focused on maintenance and updates to functionality	Level 2	Level 4

Figure 2 – 7 CMM Considerations of UEBA Solution Implementation

When exploring the CMM for present and post – implementation states, it is vital to understand that Callego presently has functionality of a UEBA through its license considerations with our cloud infrastructure, however usage and tuning of systemic processes is needed to improve upon its maturity as a technical control in the enterprise. Within the next 30 days, there is a potential for further configuration and systemic improvements to arise to a Level 4 future maturity state. Furthermore, continuous monitoring upon implementation of this technical

control allows for the long-term focus of optimization and continuous monitoring of this control by incident response personnel to meet qualifications of meeting level 5 optimization within the next six months. (*Capability Maturity Model (CMM),* n.d.). As Callego already relies on E5 licensing from Microsoft 365, the implementation of Defender for Identity sensors on critical systems such as domain controllers can ensure that this technical control is met without additional cost considerations. However, training and risk analysis by incident responders must be considered as a potential fiscal impact as well as administrative activities such as tuning to limit alert fatigue (Khaliq et al., 2020).

Control III: Implement a Data Loss Prevention (DLP) Solution

Technical Control:	Implement a Data Loss Prevention (DLP) Solution		
Description	**Scope of functions**		
Relies on trainable data classifiers to identify and automatically label and enforce encryption on sensitive data managed by the organization to prevent unauthorized data loss.	Network Components	Host Devices	Applications
		X	**X**

Figure 2 – 8 Identification and function scope of DLP solution implementation

Data Loss Prevention (DLP) is a necessary control for not only preventing data loss, but automatically classify all sensitive and personal data entering and departing the organizational infrastructure. Data loss prevention solutions allow for limiting loss of sensitive data from departing users and generative alerts for risky data activities arising from insider threats or security events (Liu & Kuhn, 2010). Furthermore, from a cost considerations perspective, DLP tools may become expensive to upwards of $385,000 for 10,000 users within the first year of deployment (*Data Loss Prevention Software Cost*, n.d.). However, it is vital to understand that DLP tools can not only alert and limit data loss but enforce modern encryption of any data leaving the environment through unauthorized activities such as a compromised user.

Capability Maturity Model States (Present and post-implementation)						
Level 1 (Initial)	Level 2 (Repeatable)	Level 3 (Defined)	Level 4 (Managed)	Level 5 (Optimized)	Present State	Future State
Implement-ation is needed, not yet explored. Non-existant	Implemented, but lacks defined processes	Processes defined, systematic improvements in progress	Systematic improvements deployed, functionality may need further tuning or advanced modifications	Tuning and functionality workload focused on maintenance and updates to functionality	Level 1	Level 2

Figure 2 – 9 CMM Considerations for DLP Solution Implementation

As an initial implementation using CMM, there may be delays in proper implementation due in part to training and initial deployment due to the requirements to tuning of alerts and initial

classifications. Presently, no implementation has been deployed within our infrastructure, however like UEBA, it may be necessary to rely on cloud infrastructure components such as Microsoft Purview for data loss prevention controls and automatic deployment of trainable sensitive data classifiers and auto-labeling. Further tuning of classifiers and DLP policy considerations would be limited to a future state of level 2 based on the time constraints explored.

Considerations

GDPR prioritizes the handling of personal data which all three technical controls provide a layered approach focused primarily on data privacy protection for managed identities, devices, and network systems. With a focus by all three identified controls against the focus of data privacy monitoring and protections, it is vital to understand how each technical control has a complementary component to one another. All identified technical controls offer further benefits for supporting compliance with GDPR and the certification process outlined within the EU – U.S. Data Privacy Framework. Additionally, deployment of a SIEM can aid Callego information security teams to monitor continuously all managed identities, devices, applications, and connected networking solutions to provide a complete view of all activities and transmissions occurring across the enterprise and any connected resources.

Furthermore, the adoption of UEBA allows for identity monitoring with automatic risk assessments based on what is considered normal for the identified entity against what may be abnormal. This implemented control can allow Callego incident handlers the ability to not only track risky activities such as data access and discovery, but feed into the SIEM as another information vector to evaluate data usage and lay the groundwork for exploring an insider risk program in the future. This provides another functionality from our current security initiatives

to ensure that we meet all GDPR requirements regarding personal data access and monitoring data systems for misuse.

Building atop the other recommended technical controls, the implementation of a DLP solution, such as Microsoft Purview, can complement both proposed controls and existing implementations. DLP solutions can not only track compliance management and assess whether our controls meet any necessary regulatory requirements but allow the enforcement of encryption standards as defined by GDPR to protect personal data from loss, misuse, and unauthorized access (*Data Privacy Framework*, 2024). Future more, DLP solutions can enforce that any data that is moved to temporary storage or transmitted outside of our managed infrastructure is properly encrypted to avoid an adversary in the middle or access by an unauthorized entity. DLP tools build on both SIEM and UEBA to enhance monitoring of abnormal access, but also provide depth and further context for evaluating insider risk or associated behaviors.

Further evaluation of the benefits of implementation of the explored controls includes how all three technical controls allow for the continuous monitoring of data within Callego's infrastructure to ensure a focus least trust methodology. GDPR prioritizes the handling of personal data which all three technical controls provide a layered approach focused primarily on data privacy protection for managed identities, devices, and network systems. By leveraging the principle of least trust across the monitoring functionalities of all three technical controls proposed, we are able to enhance existing domains such as governance, risk, and compliance, security operations, as well as identity access management solutions.

Regarding practicality and justification, it is important to focus on the merits of each proposed technical control and their ability post 30 days to ensure that we provide the necessary security mechanisms to protect personal data. Maturity of all proposed controls can allow us to

improve our security posture in alignment with focusing on protection and monitoring of sensitive data. Ultimately, the average cost of a data breach and all regulatory considerations when approaching fines from any possible violations in 2024 is around 4.88 million dollars (USD) which exceeds the likely initial costs of implementation of all three technical controls from a single, hypothetical security infraction (*Cost of a Data Breach 2024 | IBM*, 2024

Consulting Problem Three: Incident Management Simulation Exercise

When evaluating the effectiveness of an incident response plan, it is vital that hypothetical exercises are conducted involving the people, processes, and technology without risk of impact to business continuity. The use of tabletop exercises can help business leaders understand how their communication, incident coordination roles, and procedures behave when responding to a security incident under simulated incident testing (*7 Reasons Tabletop Exercises Are a Must*, 2018). In addition, tabletop exercises can help identify potential deficiencies with current incident response planning as well as explore emerging security risks posed by recent technology innovations and evolving attack vectors. Thus, this paper will explore and provide facilitation instructions for an incident management simulated exercise focused on an intelligent virtual assistant (IVA) in development relying on tabletop game mechanics by Callego, an imaginary business organization.

Purpose

As a recognized leader in managed call center outsourcing provider, Callego has been actively developing an IVA in its Sonya Project to enhance the overall customer experience in its product offerings (*Southern New Hampshire University*, 2024). IVA technology consists of generative artificial intelligence (GAI) using machine learning and natural language processing (NLP) which is used to simulate a human customer service agent autonomously (Teet & Kesrarat, 2023). However, as a developing technological innovation, GAI poses a unique challenge for organizations wishing to implement adequate security controls against threat vectors that have not been methodically documented by security researchers. Furthermore, several concerns arise from the nature and limitations facilitated by the trusting relationship within human – machine communications such as socially engineered threats, fraudulent data

collection using injection techniques, and known exploits designed to manipulate IVA and related GAI technologies' data integrity using both human and malicious artificial intelligence (Somers, 2020).

Objectives of the Exercise

To ensure that Callego's people, processes, and technology can effectively identify that its present incident response protocols are effective, this tabletop exercise will focus on a simulated series of security incidents based on emerging threat vectors against the Sonya Project and its use of GAI – based technology. An incident includes any identified security events that could feasibly evolve into a multistage attack impacting the confidentiality, integrity, and availability of the tools and technology integrated with the Sonya Project and cause a loss of control of any interconnected systems and data repositories (National Cyber Exercise Program, 2022). Additionally, this tabletop exercise will focus on the following exercise objectives:

1) Identify the and evaluate the effectiveness of all incident response procedures and communications between the incident response team, key stakeholders, and system owners.
2) Examine specific areas for improvement throughout the incident response lifecycle, applicable controls, systems, and organizational resilience to limit potential detriments to business continuity to production infrastructure in future incidents.

I. Incident Management Roles & Responsibilities

For this tabletop exercise, it is vital that all roles and responsibilities of each player are identified. The following table represents what players, at least, would be needed to carry out the scenario event for the purposes of preparing to respond and remediate an incident from a

collaborative standpoint. Key participants may include relevant stakeholders, leadership, or even delegation from system teams and owners.

The primary role for incident management, coordination, and recovery communications would be a Security Operations Manager. This role would carry all incident escalation responsibilities to ensure that any security event is triaged against all organizational criteria for incident declaration. In addition, the Security Operations Manager would oversee and lead incident triaging, containment requirements, and communicate to key information technology operations teams for any necessary resources or impacts. Post incident response, this role would be tasked with overseeing any modifications or revisions to present organizational security response procedures.

In addition to the Security Operations Manager, lead incident response analysts would be needed to facilitate detection, identification, and recovery of a security incident. Furthermore, the incident response analysts, who usually work from a security operations center (SOC), would be tasked with validating any alerts or notifications related to the event as well as evaluating the severity of any related security events. Ultimately, incident documentation and the establishment of a reputable timeline for the incident fall under the scope of any security analysts included in the tabletop exercise.

All post-containment and forensic collection activities such as chain of evidence collection, reviewing mitigation of any persistent threats, as well as reviewing any technical security controls for improvements are performed by Security Engineers. Security Engineers are another role that needs to be included to help with exploring a tabletop exercise for potential remediations, impact scopes, as well as performing verification of technical controls and ensuring that any persistent issues are adequately resolved. Furthermore, Security Engineers are

vital to help review applicable configuration management as well as any security tools are enforced.

From a key stakeholder perspective, it is important that IT Leadership along with the Chief Security Information Officer (CISO) are included to review that organizational disaster recovery and response processes behave in a simulated security incident to ensure that business productions and business continuity initiatives are satisfactory met. From their focus on the peoples, processes, and technologies required for the organization's mission, key stakeholders can help ensure that if there are any impacts from current operational procedures and systems in a simulated incident, that further strategic measures can be introduced to ensure that when a similar incident occurs, all incident response and security measures will limit or deter the risk of impacts.

Lastly, Governance, Risk and Compliance (GRC) Management should be included to ensure that all procedures and activities explored by the security team meet key organizational controls and practices. GRC has a focus on exploring risk reduction strategies such as ensuring that the best practices for patch management and vulnerability remediation are implemented as defined by key stakeholders.

Scope and Methodology

Throughout this and future tabletop exercise, one or more incidents may arise that prompt the incident response team to identify and contain a scenario problem. The explored scenario may focus on both adversary attack phases (Offensive) and incident responders' abilities to detect and rely on potential countermeasures to contain a simulated incident. Additionally, discussion prompts may be provided by the tabletop exercise facilitator designed to examine how current security controls, communication, and incident response procedures effectively respond

to a simulated security incident and/or series of uncorrelated events. Further decisions will be explored during the exercise that could potentially shift the attack vector, potential countermeasures, and supply appropriate consequences.

The primary focus of this exercise is against a known potential threat vector that may target the Sonya Project against the risk and potential impact of a denial-of-service attack (DoS). A significant portion of globally based DOS attacks in 2024 have been demonstrating a renewed focus by attackers to leverage internet of things (IoT) devices as well as generative AI platforms to incorporate them into a malicious botnet (*2024 DDoS Attack Trends | F5 Labs*, 2024). Common reasons may be for a variety of reasons; however, many can be motivated by cyber criminals desiring to propel a social, political, or ideological cause (IC3.gov, 2024). Chatbots and IVA systems, especially when incorporated into call center operations, may face an adversary targeting its resources to victimize another organization when its controls are not implemented effectively.

When combating or limiting the impact of a DoS or distributed DoS (DDoS), attention to minimizing the attack surface through defense-in-depth methodology is imperative. Common controls exist in firewall management systems using rule-based filtering to limit or block traffic based on specifically defined indicators. Additional considerations should be made to segment network zones to minimize the impact of a compromise to a specific zone or region of an organization's network and systems. Additionally, critical system resources which may be sensitive but required for the Sonya Project can rely on defense in depth and network segmentation to limit access to its systems in conjunction with firewall tools.

From an exploration towards Callego's security policies and procedures, the primary focus of this exercise is geared towards limiting impact to business continuity during the incident

response lifecycle. Communication of systemic impacts by both information security and other internal teams is vital when determining if there are grounds for escalating the call for a major security incident. Ensuring that the confidentiality, integrity, and availability of all production systems is maintained during an incident which has a high probability of loss of control is paramount to ensuring reputable business continuity during an incident or disaster. Furthermore, when a major component or implementation that provides a structural effectiveness fails or is the target for containment, downtime and potential impacts must be thoroughly explored to ensure that present processes and remediation procedures are communicated and implemented effectively.

Timeline Considerations

This tabletop exercise is expected to last for a total of five hours, including necessary breaks and post-incident discussions. No live systems will be leveraged for the purposes of this exercise and should be conducted in a conference room with all incident responders and any relevant stakeholders as necessary. The exercise is set up with three phases to help explore Callego's ability to detect, identify, contain and remediate a multi-staged security event.

Initial warm-up questions should be used to introduce all responding players to the purpose of the exercises as well as provide general rules and guidelines for what is expected. The primary focus is to allow the incident response players to openly discuss between one – another how to approach the issue and develop a plan to address the potential remediation of the scenario event. It may be best to limit answers to up to two sentences to ensure that quick responses and further discussions highlight potential deficiencies within the policies, procedures, communication, and communications to impacted departments and stakeholders.

Warm – Up Activity

The following questions may help as a warm – up or icebreaker activity to get all players ready for the initial scenario and the following mechanisms used by this tabletop exercise:

1) Introduce yourself and what part you assist with within the incident response lifecycle.
2) What areas of concern do you see with Callego's current security controls, data, and systems?
3) What sources of information do you use to help identify a potential threat for organizational systems?
4) How are Sonya Project security concerns reported? Are there any concerns, exploits, or vulnerabilities you have with generative AI systems?

Stage I:
Detection of a Denial of Service, targeting external organization exploiting Sonya Project

Scenario:

This morning starting at 8:47AM, there has been a sudden uptick of customers calling our primary support lines as well as chat-bot services powered by Sonya on our website requesting a callback escalation for a human customer service agent. Usually, a human customer service agent can remediate a customer escalation issue with less than 5 minutes of waiting on hold after Sonya was implemented.

At approximately 10:15AM, Callego's regional office in Omaha, NE received a call from a concerned organization that they were receiving a large volume of calls from Callego human-based customer support agents that were impacting their telecommunication systems for several of their offices.

An initial investigation by the telecommunications team at the request of IT Operations uncovered several million calls continue to be escalated from Sonya's integration for inbound call flow requesting human intervention, creating unnecessary long waiting times for our client's customers and has overwhelmed our volume capacity to continue to take inbound calls at this time.

Initial Framing Questions:

1) What tools, notifications, and/or alerts allow for automated reporting of potential systemic impacts at Callego?
2) Who is responsible for reporting an incident?
3) What information, system owners, or resources would you use to validate the scope of this issue?
4) What actions would you take with the information presented at this point of the exercise?
5) Are there any countermeasures that could assist with the information you know at this time?

Figure 3 – 1 - Scenario Details for the Exercise and initial Framing Questions

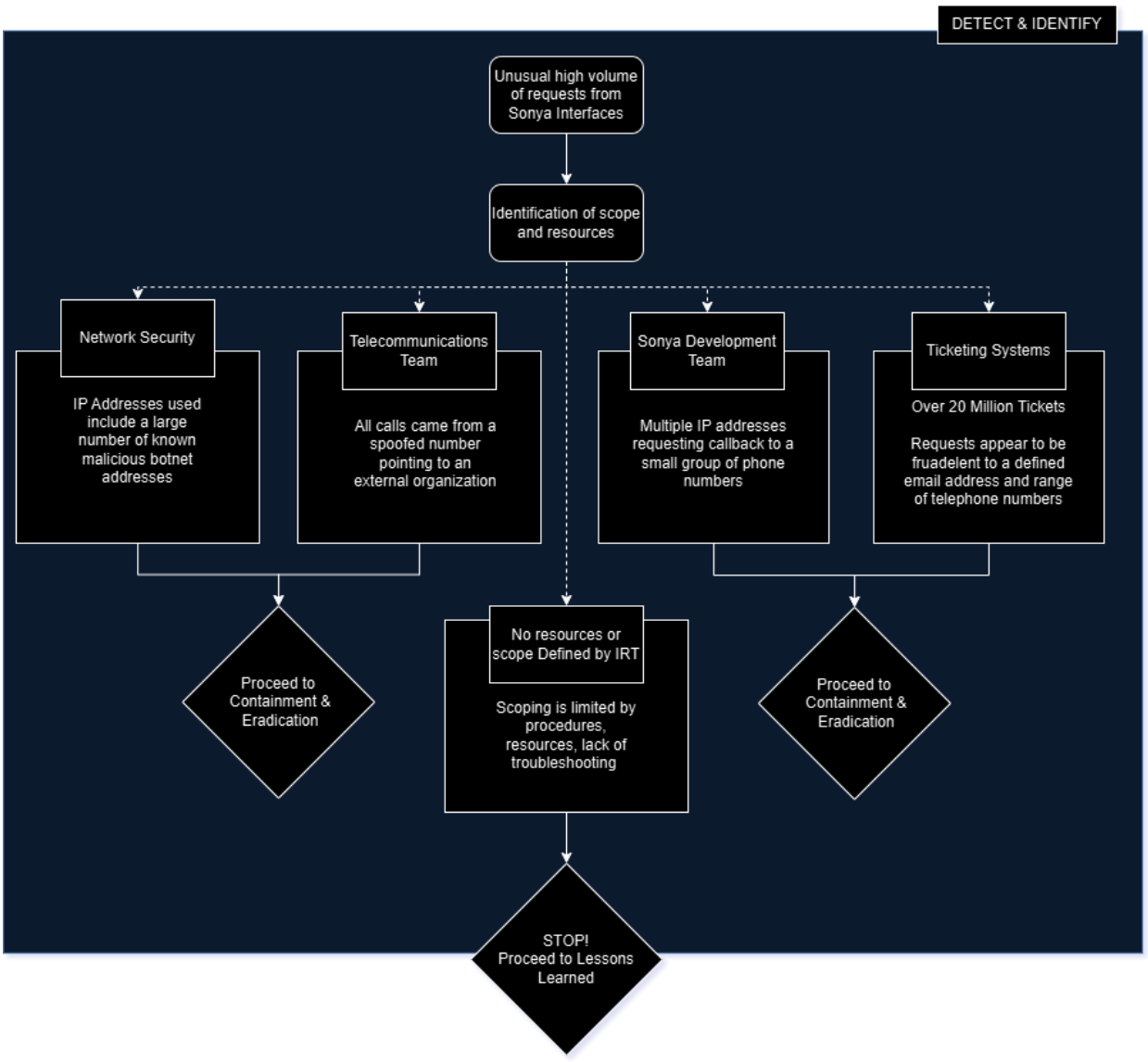

Figure 3-2 - Diagram of Detect and Identifying Cause by Incident Response Team

Potential Information for branching scenerios
Relay only if telecommunications team is brought up as a resource to scope the issue: Telecommunications and ticketing teams report that a large volume of these calls continue to request a call back to a small group of telephone numbers that all belong to a non-profit legal advocacy group, Lawbreakers, Inc, located in the United States that recently made the headlines for a conterversial project aimed to provide legal defense funds for hate groups and individuals accused of hate crimes across North America and Europe. Additionally, telecommunication teams suspect that all inbound calls requesting a callback maybe getting spoofed. **Relay only if there is any mention of the Sonya Development Team brought up as a resource to scope the issue:** The Sonya Project Team reports that the chatbot service appears to be getting a large volume of requests from a multiple IP addresses across the world requesting a callback to a series of telephone numbers. **Relay only if any mention of the Ticketing Systems Team brought up as a resource:** The Ticketing and/or IT Operations Team report that all telephone systems appear to be suffering from a denial of service. Ticketing systems are overwhelemed with over 20 million requests active in our system at this time. All caller information points to a small group of telephone numbers, but in each case the customer information is not found from its connections to client database systems. In addition, when prompted for an email address tied to an account, all requests made mention of the following email owned by the registry provider, GoDaddy: iana@registry.godaddy **Relay only if any mention of Network Security is brought up as a activity resource:** Network Security has found that the Sonya chatbot interface is getting hit by several known botnet IP addresses located across the world as well as what could be considered expected traffic activity. **Relay if actions explore contacting owner of telephone numbers:** After reaching out to Lawbreakers, Inc, they report that this is not the first time they have been targeted and have been impacted by Callego human customer service representatives calling excessively. They are in the proccess of placing a temporary block against Callego's owned telephone numbers used by its call centers and have requested that Callego prohibit calls towards their owned telephone system numbers. **Relay if actions explore contacting email address owner:** GoDaddy has not responded to our requests at this time.

Figure 3-3 - Table of Potential information for branching scenarios

Once the initial phase of detection and identification occurs, depending on the outcome of resources and scope of impact uncovered, it is important that if no scope or desired exploration to potential resources occurs, that the exercise skips to the lessons learned at the post incident discussion. Following identification and scope analysis of potential issues arising from the incident's scenario where additional new information is uncovered, it is important to prepare for the containment and erradication activities as a incident response team. Prior to completing any containment and/or erradication explorations, ensure that several discussions occur against the following questions:

1) What do you think is occurring at this point in regards to the incident? What is the cause? What is the threat vector?
2) What motivations may an adversary have when it comes to this type of attack?
3) What tools, alerts, and countermeasures can be helpful for detecting and identifying this type of attack?
4) Are there any tools or security controls that can limit this type of attack?
5) When communicating the findings and/or raising the incident, what information should be communicated? Who should this be communicated to?

Stage II: Containment and Erradication:

Potential Countermeasures and Containment activities may include the following during the containment and erradication phase:

- Place a block, known as a blacklist, against all numbers owned by Lawbreakerz, Inc from contacting Callego
- Explore security controls such as a blacklist against known IP addresses and/or numbers used by malicious threat actors.

- Temporary explore shutting off Sonya for containing the inicident from further harm
- Explore security controls for Sonya chatbot to limit automated callback to specific phone numbers or to instead supply a contact number.

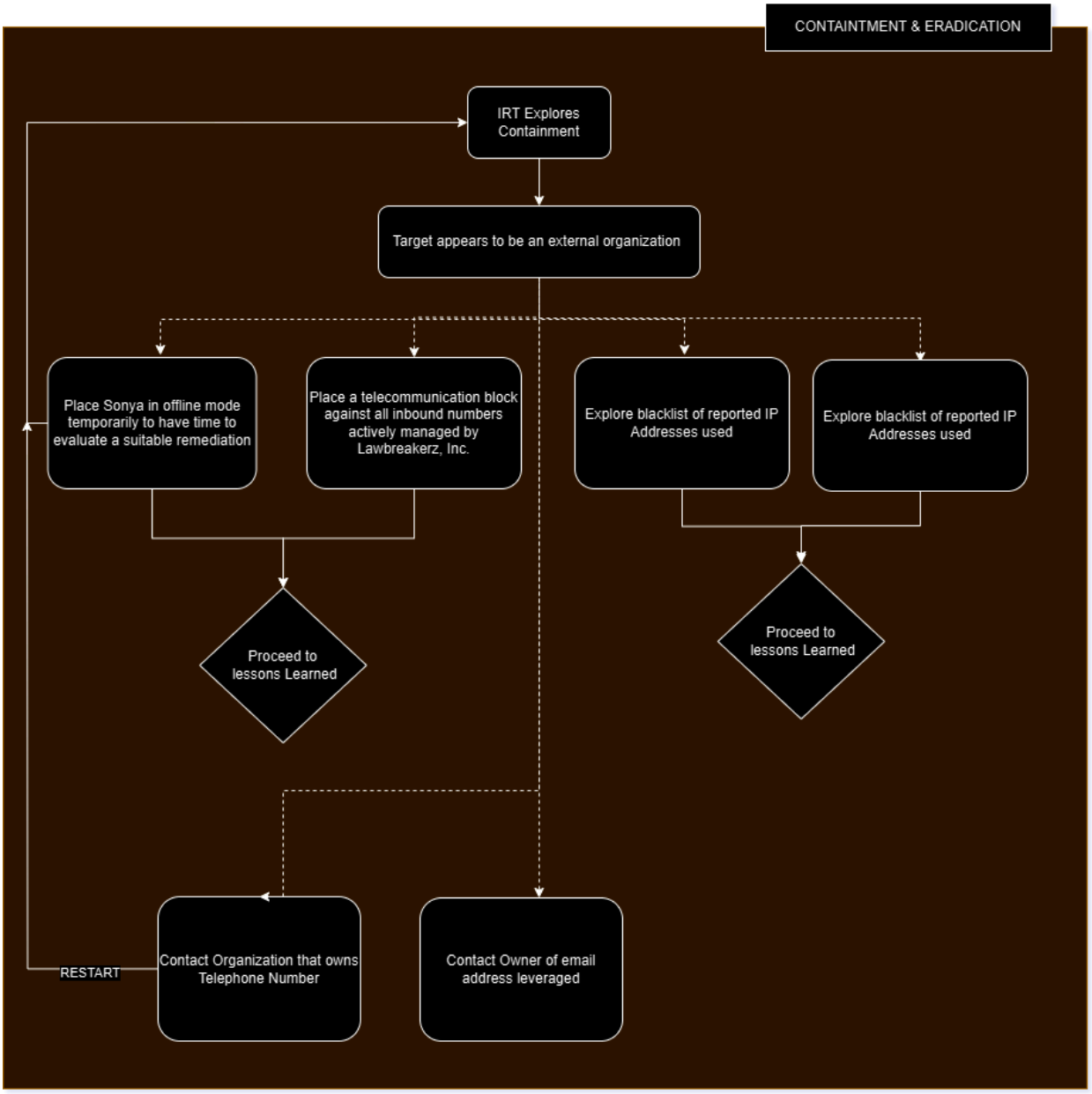

Figure 3-4 Containment and Eradication Activities by Incident Responders

Stage III: Post Incident Recovery & Lessons Learned

Upon conclusion of all stages depending on the response of the incident response team within the confines of the scenario, it becomes necessary to understand how all activities and actions taken may have encouraged or impacted the resilience of Callego's business operations during both simulated and real security incidents. When evaluating the effectiveness of security controls, processes and incident response procedures, it becomes necessary to review how an exercise or actual security incident arose and if the steps taken to detect, identify, contain, and eradicate the threat were effective to the needs of the organization.

Common questions which may arise during the post-incident review of this tabletop scenario include the following:

1. How effective were our present security controls or monitoring tools during the security incident?
2. Are there any security controls that need to be revisited? What concerns did the team uncover regarding our controls and tools?
3. Would adding any new security controls or tools be beneficial to minimize the impact of a similar incident?
4. How effective were our containment procedures?
5. How effective were our detection tools?
6. What issues or takeaways arose during the exercise that impacted incident communications?
7. Do any of our procedures need to be updated?
8. Are there any controls that could have stopped this type of attack prior to detection?

9. If this incident arises in the future, are there any compliance or regulatory concerns such as missing controls that could create liability for the organization?
10. How did the Sonya Project impact and/or contribute to the impact of this simulated exercise? Are there similar concerns that need to be reviewed by GRC and the development team?

From a supplementary approach of the post-incident process for this tabletop exercise, it may become necessary to explore the use of documenting any results of carrying out this tabletop exercise using a structured communication framework such as SBAR. SBAR stands for Situation, Background, Assessment, and Recommendation and is a popular healthcare industry communication process to share post-incident concerns and actions needing to be addressed (*Tool: SBAR | Agency for Healthcare Research and Quality*, n.d.). The SBAR can be effectively leveraged for incident response teams to report their concerns and findings for change management, system owners, and non-technical teams.

Additional Guidance

Additional explorations beyond this exercise scenario could include reviewing the National Institute of Standards and Technology (NIST)'s recently published profile exploring emerging risks against generative artificial Intelligence through NIST AI 600-1 (Roberts, 2024). Furthermore, on behalf of our European Union (EU) business partner, the EU offers its own security considerations and the first globally recognized security framework for AI released as the AI Act of 2024 (*AI Act*, 2024). The AI Act focused on a total of four levels of risk for AI systems for corporations and entities under regional jurisdiction of the EU.

Framing Statement

Cybersecurity involves safeguarding the confidentiality, integrity, and availability of infrastructure, systems, identities, and data for enterprise technology (*What Is Cybersecurity? | CISA*, 2021). Across the world, a typical data breach cost organizations $4.88 million dollars with business email compromise (BEC) accounting for over $2.9 billion dollars in losses annually (St John, 2024). With the adoption of interconnected systems and emerging technologies, the risks of a cyberattack impacting business continuity can leave lasting impacts for businesses and corporations from remediation activities, legal costs, regulatory fines, and reputational damages. For the purposes of this consulting collection capstone, three consulting problems are explored with a focus on human factors, legal considerations, and incident management targeting a fictional entity.

Introduction

As part of Southern New Hampshire University's requirements for achieving a Master of Science focused on the Cybersecurity field, ISE – 690 focuses on the pinnacle of our academic journey. The course requires both applied experience and leveraging prior coursework for the purpose of certifying students can demonstrate core competencies from the graduate program (*ISE 690 Syllabus - ISE-690-10918-M01 Cyber Security Capstone 2024 D-3 (Jul - Oct)*, n.d.). Through each of the consulting problems, we evaluated the efficacy of governance, risk, and compliance initiatives to address complex organizational requirements, regulatory bodies, and communicated our findings to key stakeholders. In addition, the challenges faced by each of the consulting problems represent the challenges that security practitioners face when navigating multi-disciplinary teams, enterprise architecture, and addressing difficulties arising from recent innovations and implementations that may not have been appropriately vetted.

Consulting Problem One

With consulting problem one, the objective is to explore the security concerns and assessment criteria from the adoption of an intelligent virtual assistant for Callego, an outsourcing customer service provider with multinational operations. For the first problem scenario, we are tasked with approaching the security considerations and emerging strategies to evaluate the risk of generative artificial intelligence. Our focus is to communicate effectively while understanding the critical balance between security controls and operational deployments. Using a memo template for the first piece, the role as a consultant is relied upon to support organizational leadership and internal stakeholders a written recommendation of control measures to address any concerns with implementation of an emerging technology.

Consulting Problem Two

Through consulting problem two, our focus shifts to the regulatory and legal challenges when Callego commits to a strategic partnership with a firm based in the European Union. For this reason, this consulting problem is broken down into a total of three pieces exploring GDPR requirements for a revised privacy statement, top three policies, and top three technical controls, revised. To best address the considerations presented by consulting problem two, we are tasked with triaging potential policy considerations that best align with the needs of the organization. Ultimately, we explore adapting organizational culture, operations, policies, controls, and procedures to effectively align with a international regulatory requirement.

Consulting Problem Three

Finally, with consulting problem three, incident management and response capabilities are explored through a simulated tabletop scenario to thoroughly examine the roles and responsibilities of incident responders and organizational stakeholders. For this problem, our

focus is to develop a structured tabletop exercise to explore how Callego's people, processes, and technology detect and respond to simulated events. The purpose of the exercise is to address potential impacts to business continuity, the organization's incident response policies, communication planning, and the effectiveness of the organization's risk management strategies.

Reflections on Learning

As part of this capstone, we confronted problems that arise commonly for companies across the world. Organizations face complex challenges when addressing the confidentiality, integrity, and availability of resources found within their people, processes, and technologies. Through each of the consulting problems, our use of applying deductive, inductive, abductive, or a hybrid of reasoning techniques to effectively strategize and recommend technical controls, policies, and security tools that synergize the needs of the organization against security frameworks. Our considerations when choosing a mode of reasoning can help us explore potential solutions from a focus on a specific event that may not be effectively correlated to a logical cause. Additionally, starting with a generalized concept such as a security framework, we can then drill down when establishing an appropriate scope. Lastly, we had to explore issues such as communicating complex technical information with consideration to the audience to limit the risk of disengagement.

References

7 reasons tabletop exercises are a must. (2018, December 13). CIS. https://www.cisecurity.org/insights/blog/7-reasons-tabletop-exercises-are-a-must

2024 DDoS attack trends | F5 Labs. (2024, July 16). F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/2024-ddos-attack-trends

AI Act. (2024, September 10). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Andress, J., & Leary, M. (2016). Why information security policies? In *Elsevier eBooks* (pp. 63–75). https://doi.org/10.1016/b978-0-12-802042-5.00005-6

Art. 30 GDPR – Records of processing activities - General Data Protection Regulation (GDPR). (2018, April 3). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-30-gdpr/

Art. 32 GDPR – Security of processing - General Data Protection Regulation (GDPR). (2016, August 30). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-32-gdpr/

Atasoy, M. E., & Kocyigit, A. (2021). An extensible software architecture for intelligent assistant. *2021 6th International Conference on Computer Science and Engineering (UBMK)*. https://doi.org/10.1109/ubmk52708.2021.9558940

Bernadini, K. (2023, January 20). *GDPR personal data – what information does this cover?* GDPR EU. https://www.gdpreu.org/the-regulation/key-concepts/personal-data/

Blasch, E., Sung, J., Nguyen, T., Daniel, C. P., & Mason, A. P. (2019). *Artificial Intelligence Strategies for National Security and Safety Standards*.

Blind, K., Niebel, C., & Rammer, C. (2024). The Impact of the EU General Data Protection Regulation on Product Innovation. *Industry and Innovation*, *31*(3), 311–351. https://doi.org/10.1080/13662716.2023.2271858

Bryant, J. (2023, July 10). European Commission adopts EU-US adequacy decision. *IAPP*. https://iapp.org/news/a/european-commission-adopts-eu-u-s-adequacy-decision/

Capability Maturity Model (CMM). (n.d.). https://www.itgovernance.asia/capability-maturity-model

Choudrie, J., Manandhar, N., Castro, C., & Obuekwe, C. (2023). Hey Siri, Google! Can you help me? A qualitative case study of smartphones AI functions in SMEs. *Technological Forecasting and Social Change, 189,* 122375. https://doi.org/10.1016/j.techfore.2023.122375

Chowdhury, S. S., Talukdar, A., Mahmud, A., & Rahman, T. (2018). Domain Specific Intelligent Personal Assistant with Bilingual Voice Command Processing. *TENCON 2018 - 2018 IEEE Region 10 Conference, Region 10 Conference, TENCON, 2018 - 2018 IEEE*, 0731–0734. https://doi-org.ezproxy.snhu.edu/10.1109/TENCON.2018.8650203

Chung, H., Iorga, M., Voas, J., & Lee, S. (2017). "Alexa, Can I Trust You?" *Computer*, *50*(9), 100–104. https://doi-org.ezproxy.snhu.edu/10.1109/MC.2017.3571053

CISA. (2021). Incident Response Plan (IRP) basics. In *CISA | DEFEND TODAY, SECURE TOMORROW* [Report]. https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

Cost of a data breach 2024 | IBM. (2024). https://www.ibm.com/reports/data-breach

Data Loss Prevention Software cost. (n.d.). https://www.strac.io/blog/data-loss-prevention-software-cost

Data Privacy Framework. (2024). https://www.dataprivacyframework.gov/

Determann, L., Baker McKenzie LLP, Nebel, M., Baker McKenzie, Schmidl, M., & Baker McKenzie. (2023). The EU–US data privacy framework and the impact on companies in the EEA and USA compared to other international data transfer mechanisms. In *Journal of Data Protection & Privacy* (Vol. 6, Issue 2, pp. 120–134) [Journal-article]. Henry Stewart Publications.

DFS issues findings on the Apple Card and its underwriter Goldman Sachs Bank. (2021, March 23). Department of Financial Services. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202103231

Elad, B. (2024, February 3). Cyber Security statistics 2024 Facts and trends that users need to know. *Enterprise Apps Today*. https://www.enterpriseappstoday.com/stats/cybersecurity-statistics.html

Evans, B. J. (2023). The HIPAA Privacy Rule at Age 25: Privacy for Equitable AI. *Florida State University Law Review*, *50*(Issue 4), 741–810.

Fifelski, B. A. (2023, September 26). UM expert testifies on the dangers of AI in banking. *Crain's Detroit Business*. https://www.crainsdetroit.com/banking-finance/artificial-intelligence-has-pros-and-cons-banking

Fines / penalties - General Data Protection Regulation (GDPR). (2021, October 22). General Data Protection Regulation (GDPR). https://gdpr-info.eu/issues/fines-penalties/

Finlay, S. (2024, June 14). *AI presents benefits, pitfalls for car dealers*. https://www.wardsauto.com/dealers/ai-presents-benefits-pitfalls-for-car-dealers

Gobeo, A., Fowler, C., & Buchanan, W. (2020). *GDPR and Cyber Security for Business Information Systems*. River Publishers.

Gruschka, N., Mavroeidis, V., Vishi, K., & Jensen, M. (2018). Privacy issues and data protection in big data: A case study analysis under GDPR. *2018 IEEE International Conference on Big Data (Big Data*. https://doi.org/10.1109/bigdata.2018.8622621

Gutierrez, C. M., Jeffrey, W., & Cita M. Furlani. (2006). FIPS PUB 200. In *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION*. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

Hamilton, C., Swart, W., & Stokes, G. M. (2021). Developing a Measure of Social, Ethical, and Legal Content for Intelligent Cognitive Assistants. *Online Submission*, *16*(3), 1–37.

Han, S., & Park, S. (2022). A Gap Between Blockchain and General Data Protection Regulation: A Systematic Review. *IEEE Access*, *10*, 21693536. https://doi.org/10.1109/access.2022.3210110

Helemski, G. (2024, August 6). Data access in the digital age: Building a secure and accessible environment. *The Fast Mode*. https://www.thefastmode.com/expert-opinion/36342-data-access-in-the-digital-age-building-a-secure-and-accessible-environment

IC3.gov. (2024, July 31). *DDOS attacks: Could hinder access to election information, would not prevent voting*. https://www.ic3.gov/Media/Y2024/PSA240731

ISE 690 Syllabus - ISE-690-10918-M01 Cyber Security Capstone 2024 D-3 (Jul - Oct). (n.d.). https://learn.snhu.edu/d2l/le/content/1678846/viewContent/34517211/View

Johnson, A., Dempsey, K., Ross, R., Gupta, S., & Bailey, D. (2019). *Guide for security-focused configuration management of information systems*. https://doi.org/10.6028/nist.sp.800-128

Kelley, A. (2024). CISA conducts AI-driven cyber tabletop exercise with government and industry. *Nextgov.Com*, N.PAG.

Khaliq, S., Tariq, Z. U. A., & Masood, A. (2020). Role of User and Entity Behavior Analytics in Detecting Insider Attacks. *Institute of Electrical and Electronics Engineers*. https://doi.org/10.1109/iccws48432.2020.9292394

Koskey, A., & White, M. (2021, June 30). Incident response considerations: Protecting the attorney-client privilege. Reuters. https://www.reuters.com/legal/legalindustry/incident-response-considerations-protecting-attorney-client-privilege-2021-06-24/

Kulkarni, M. S., Naik, H. L., & Bharathi, S. V. (2023). Textual Analysis of Privacy Policies to Understand the Effect of GDPR. *2023 2nd International Conference on Futuristic Technologies (INCOFT)*, 1–5. https://doi.org/10.1109/incoft60753.2023.10425479

Leach, E., & Weller, A. (2020, February 20). How to build a "culture of privacy." *IAPP*. https://iapp.org/news/a/how-to-build-a-culture-of-privacy

Liu, S., & Kuhn, R. (2010). Data loss Prevention. *IT Professional*, *12*(2), 10–13. https://doi.org/10.1109/mitp.2010.52

Logpoint. (2024, July 26). *The ultimate SIEM pricing guide*. Logpoint. https://www.logpoint.com/en/blog/the-ultimate-siem-pricing-guide/

Manfredi, R. (2024, April 8). *U.S. Cybersecurity and Data Privacy Review and Outlook – 2024*. Gibson Dunn. https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2024/#_Toc157161990

McKee, F., & Noever, D. (2023). *Acoustic Cybersecurity: Exploiting Voice-Activated Systems*.

Content injection, technique T1659 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/techniques/T1659/

Mirth, T., Jasper, T., Palus, T., & Tenorio, T. (2024). Systems and Methods for Artificial Intelligence-Based Security Policy Development (Patent No. edspap.20240028009). In *USPTO Patent Applications* (edspap.20240028009). U.S. Patent and Trademark Office.

Nadeau, M. (2024, April 4). *General Data Protection Regulation (GDPR): What you need to know to stay compliant*. CSO Online. https://www.csoonline.com/article/562107/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html

National Cyber Exercise Program. (2022). Joint Cyber Defense Collaborative Artificial Intelligence Cyber Tabletop Exercise. In *National Cyber Exercise Program* [Scenario document]. https://cisa.gov

Ottis, R. (2014). Light weight tabletop exercise for cybersecurity education. *Journal of Homeland Security and Emergency Management*, *11*(4), 579–592. https://doi.org/10.1515/jhsem-2014-0031

OWASP Top 10 for LLM & Generative AI Security. (n.d.). *LLMRISKS Archive - OWASP Top 10 for LLM & Generative AI Security*. https://genai.owasp.org/llm-top-10/

Principles of the GDPR. (2024). European Commission. https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr_en

Qammar, A., Wang, H., Ding, J., Naouri, A., Daneshmand, M., & Ning, H. (2023). *Chatbots to ChatGPT in a Cybersecurity Space: Evolution, Vulnerabilities, Attacks, Challenges, and Future Recommendations*.

Roberts, K. (2024). *Artificial Intelligence Risk Management Framework: Generative Artificial*

Intelligence Profile. https://doi.org/10.6028/nist.ai.600-1

Schmidt, J., Schutte, N. M., Buttigieg, S., Novillo-Ortiz, D., Sutherland, E., Anderson, M., De Witte, B., Peolsson, M., Unim, B., Pavlova, M., Stern, A. D., Mossialos, E., & Van Kessel, R. (2024). Mapping the regulatory landscape for artificial intelligence in health within the European Union. *Npj Digital Medicine*, *7*(1). https://doi.org/10.1038/s41746-024-01221-6

Science & Tech Spotlight: Combating Deepfakes. (2024, March 11). U.S. GAO. https://www.gao.gov/products/gao-24-107292

Shave, L. (2024). Cybersecurity in the Digital Age. *IQ: The RIM Quarterly*, *40*(2), 24–28.

Shan, F., Wang, Z., Liu, M., & Zhang, M. (2024). Automatic Generation of Attribute-Based Access Control Policies from Natural Language Documents. *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, *0*(0), 1–10. https://doi.org/10.32604/cmc.2024.055167

Sieja, M., & Wach, K. (2023). Revolutionary artificial intelligence or rogue technology? The promises and pitfalls of ChatGPT. *International Entrepreneurship Review*, *9*(4), 101–115. https://doi-org.ezproxy.snhu.edu/10.15678/IER.2023.0904.07

Smith, C. S. (2018, May 10). Alexa and Siri can hear this hidden command. You can't. *The New York Times*. https://www.nytimes.com/2018/05/10/technology/alexa-siri-hidden-command-audio-attacks.html

Somers, M. (2020, July 21). *Deepfakes, explained | MIT Sloan*. MIT Sloan. https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained

Southern New Hampshire University (2024). *Consulting Problem Two: GDPR Principles and Compliance* [Document]. https://learn.snhu.edu/content/enforced/1678846-ISE-690-10918.202457-1/course_documents/ISE%20690%20Callego%20Privacy%20Statement.pdf

Southern New Hampshire University. (2024). *ISE 690 Consulting Problem Three: Building Incident Management Capability with a Tabletop Simulation Exercise.* https://learn.snhu.edu/content/enforced/1678846-ISE-690-10918.202457-1/course_documents/ISE%20690%20Consulting%20Problem%20Three.pdf

St John, M. (2024, August 28). *Cybersecurity stats: facts and figures you should know*. Forbes Advisor. https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/

Technical controls. (2024). Resilient Energy Platform. https://resilient-energy.org/cybersecurity-resilience/building-blocks/technical-controls

Teet, T. P., & Kesrarat, D. (2023). User Experience Towards Chatbots in Myanmar. *2023 7th International Conference on Business and Information Management (ICBIM), Business and Information Management (ICBIM), 2023 7th International Conference On*, 31–36. https://doi-org.ezproxy.snhu.edu/10.1109/ICBIM59872.2023.10303181

The AI Act Explorer | EU Artificial Intelligence Act. (2024). EU Artificial Intelligence Act. https://artificialintelligenceact.eu/ai-act-explorer/

Tool: SBAR | Agency for Healthcare Research and Quality. (n.d.). https://www.ahrq.gov/teamstepps-program/curriculum/communication/tools/sbar.html

Torre, D., Abualhaija, S., Sabetzadeh, M., Briand, L., Baetens, K., Goes, P., & Forastier, S. (2020). An AI-assisted Approach for Checking the Completeness of Privacy Policies Against GDPR. *2020 IEEE 28th International Requirements Engineering Conference*. https://doi.org/10.1109/re48521.2020.00025

Vigdor, N. (2019, November 10). Apple Card investigated after gender discrimination complaints. *The New York Times*. https://www.nytimes.com/2019/11/10/business/Apple-credit-card-investigation.html

What is data protection? | Microsoft Security. (2024). https://www.microsoft.com/en-us/security/business/security-101/what-is-data-protection

Zhang, X., Lee, S. K., Kim, W., & Hahn, S. (2023). "Sorry, it was my fault": Repairing trust in human-robot interactions. *International Journal of Human-Computer Studies, 175*, 103031. https://doi.org/10.1016/j.ijhcs.2023.103031

Zerdick, T. (2021, December 21). *Pseudonymous data: processing personal data while mitigating risks*. European Data Protection Supervisor. https://www.edps.europa.eu/press-publications/press-news/blog/pseudonymous-data-processing-personal-data-while-mitigating_en