The Consulting Collection

ISE 690 Cybersecurity Graduate Program Capstone Project

Brett Logan

Southern New Hampshire University:
Global Campus
INSTRUCTOR: DR. TREBOR Z. EVANS

Table of Contents

Framing Statement

Welcome.

This document represents the culmination of learning and experience gained throughout an in-depth consulting project spanning three key parts. In union, these parts effectively illustrate the achievement of the six major outcomes of a cybersecurity graduate program. The outcomes reflect a deep preparedness and the creation of a highly valuable asset in the form of a candidate with a now proven ability to:

1. Assess the effectiveness of information security governance policies and strategies for planning, preparing, and responding to critical threats within diverse organizational contexts and situations in a manner aligned with cybersecurity standards and frameworks.
2. Develop risk management plans for conducting risk assessment and managing identified risk to align with the needs of internal and external controls, governing bodies, and vested stakeholders.
3. Develop strategic information security plans and strategies for establishing policies to guide internal and external influences that are aligned with national and international standards and practices.
4. Develop information security incident management and business continuity plans aligned with legal, regulatory, and international standards for appropriately responding to incidents in consideration of diverse demographics.
5. Employee leadership strategies for ethical behavior, tech standards, and emerging trends for advancing an organization’s strategic goals in diverse and multifunctional cybersecurity teams.

6. Enhance collaboration and communication by employing interpersonal communication skills and establishing communication plans and processes aligned to the needs of internal and external audiences.

To showcase the successful achievement of these outcomes, the following consulting collection consists of three parts: a memo of recommendation on intelligent virtual assistants, a revised privacy statement and recommendation of technical controls to meet the European Union's General Data Protection Regulation (GDPR) standards, and facilitation instructions for an incident management simulation tabletop training exercise. All three parts of the project represent this author's work as a cybersecurity consultant for a fictional company called Callego, with each section addressing all six major outcomes stated above from different angles and perspectives.

Consulting Problem One: Memo of Recommendation on intelligent virtual assistants (IVAs).

This scenario was based upon Callego's implementation of a new intelligent virtual assistant named Sonya. The consulting task was to analyze potential security risks of such technology and address security via design configurations, policies, procedures, and other methods. In addressing the prompt and completing a memo of recommendation, each numbered corresponding program outcome was achieved in the following ways:

(1) Assessment of risks of IVA and underlying technology including threat recognition.

(2) Recommendations for mitigation and management of risks of IVAs after evaluating potential security risks.

(3) Drawing on emerging industry practices for addressing risks of IVAs and/or artificial intelligence by recognizing emerging strategies among experts in identifying such risks.

(4) Explaining IVA development as a vital organizational strategy whilst balancing security risks and control measures with organizational mission, operations, and constraints.

(5) Recommending control measures after conducting research in multidisciplinary contexts to advance organizational strategy.

(6) Supporting organizational leadership through written recommendations via drafting an essential memo regarding IVAs and security.

Consulting Problem Two: Privacy Policy Revision to Meet GDPR Requirements and the Recommendation of Technical Controls to Meet the GDPR Standard of Due Care.

In this piece the company Callego has made the decision to form a partnership with the German company Spatzchen. Prior to this, Callego's business operations existed in the United States and Asia, making the introduction of European customers and data an extremely important consideration due to regional regulations related to privacy such as the GDPR. It was necessary to research, analyze, and assess GDPR policy and principles through the lens of organizational practices related to security while also recommending technical controls that meet the standard of due care. Each program outcome was addressed within this portion of the consulting collection in the following ways:

(1) The research, assessment, and creation of an annotated list of GDPR compliant policies that address organizational security while ensuring legal, ethical, and cultural compliance.

(2) The alignment of organizational risk management policies with GDPR.

(3) Identification and operationalization of GDPR privacy and data principles as related to organizational privacy statements and technical control measures.

(4) Analyzing and adapting organizational operations, policies, and procedures to align with the GDPR while balancing security risks and control measures with the corporate mission, operations, and constraints.

(5) Supporting and advancing organizational strategy while ensuring regulatory compliance via public discourse such as the revised privacy policy.

(6) Development of a public-facing privacy statement that establishes a public face for the organization and reflects the commitment to data protection and privacy principles.

Consulting Problem Three: Incident Management Tabletop Training Exercise

The final piece in the consulting collection was the creation of facilitation instructions for a tabletop training exercise involving key individuals that would test incident response procedures, mitigation tactics, data protection principles, employee readiness, and overall security preparedness. Like many modern-day organizations, Callego made impactful decisions in a rapidly evolving environment. Choices like implementing artificial intelligence and IVAs, and entering into business operations in Europe, introduced new security considerations that could be effectively tested via a tabletop exercise. This type of exercise is integral for organizations, and the experience gained by creating one addresses the six course outcomes by:

(1) Identifying and testing policy and procedure via the creation of a realistic threat scenario.

(2) Assessing risks while building risk management capability and increasing security culture via the tabletop training exercise.

(3) Developing and testing organizational data protection capabilities while analyzing alignment with industry regulations such as GDPR.

(4) Building business continuity capability and resilience during a critical incident by testing response strategies, attitudes, and choices.

(5) Encouraging ethical and prepared leadership via structuring a tabletop exercise to focus on and instill reflective decision making in incident management and response.

(6) Communicating and testing security principles through an immersive exercise that captures lessons learned from incident response.

It was the great philosopher Socrates that once said, “education is the kindling of flame, not the filling of a vessel”, a deeply meaningful observance that this capstone project so effectively reflects. Throughout the process of responding to the three scenarios, that flame of knowledge was steadily fueled in the form of new insights, analysis, and challenge by way of critical thinking and conceptualization turned tangible in the form of key work.

Stepping into the role of a consultant and responding to relevant cybersecurity concerns from a multitude of perspectives and objectives has created a graduate prepared by uniquely valuable experience. Ultimately, the progression through the three scenarios reflects a wide variety of contemporary cybersecurity considerations: from technical controls and attack/mitigation tactics, to legal, ethical, cultural, and global concerns. The reader is invited to consider the great depth of learning that occurred to produce this document, the commitment, dedication, and passion for cybersecurity in all its iterations that is on full display throughout the following pages.

Consulting Problem One: Memo of Recommendation on IVAs

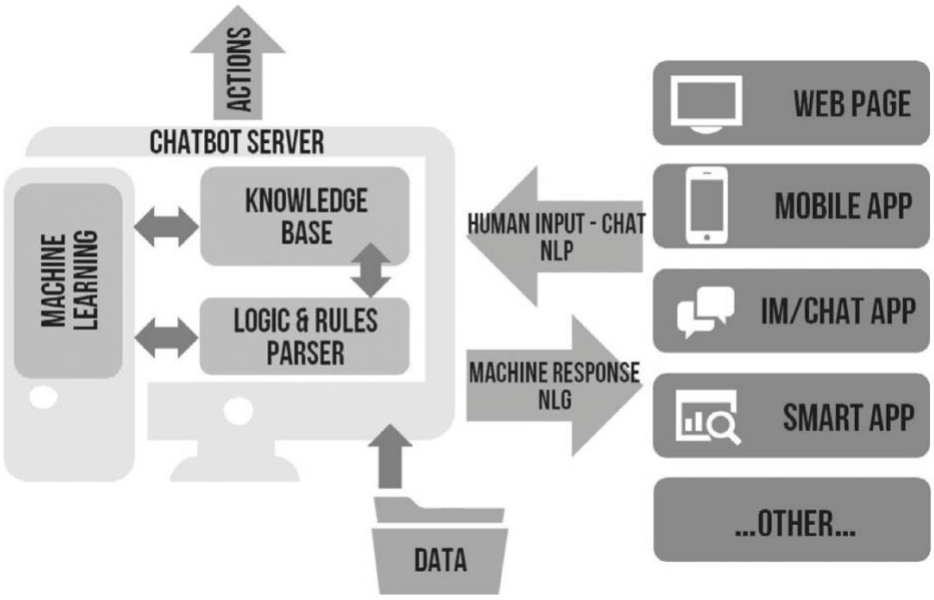
Introduction

As Callego proceeds with the development of Sonya, an intelligent virtual assistant (IVA) designed to interact with customers via phone and chat, it is important to recognize the security risks and corresponding control measures associated with this type of technology. This memo has been drafted to communicate these risks and provide recommendations for controlling them, ensuring a successful implementation and future success for the Sonya project.

Summary of Intelligent Virtual Assistants

As Callego continues the "We Are With You" marketing campaign aimed at becoming an industry leader in handling the most difficult and complex customer issues, the benefits of creating an IVA for use in Callego's customer service operations are numerous. Chiefly among these benefits is an increase in accuracy and consistency in responding to customer questions/requests, with the added benefit of routing the most difficult issues to human agents, saving time and resources while better servicing customers. An effective IVA will handle the vast majority of customer inquiries while routing the most serious and complex issues to a human agent. This creates the opportunity for more specialized and capable customer service personnel that can focus on the most serious requests, furthering the goal of "solving any problem a customer may present" and strengthening the Callego brand. Additionally, the implementation of IVA technology will create improved and consistent performance across all Callego's outsourced customer service clients, benefiting the organization's reputation while reducing training costs and human errors. Advances in natural language processing (NLP) have

created increasingly effective AI that can recognize a user's input and determine the most appropriate response. This process can be illustrated as follows:



(Abdulla et al. 2021)

Underlying Technology With Security Implications

Natural language processing, "a theoretically motivated range of computational techniques for analyzing and representing naturally occurring texts at one or more levels of linguistic analysis for the purpose of achieving human-like language processing for a range of tasks or applications" is the underlying technology that makes Sonya "smart"(Liddy 2001). This technology makes it possible for Sonya to interpret customer's spoken and written inquires, compare them to a cloud-based database of questions, answers, and customer information, and use artificial intelligence to select the most appropriate response/action. Each interaction will add to this database, broadening Sonya's resource pool and increasing the rate of successful interactions and ability to address more complex requests.

The two key parts to NLP are data preprocessing and algorithm development: "data preprocessing involves preparing and "cleaning" text data for machines to be able to analyze it.

preprocessing puts data in workable form and highlights features in the text that an algorithm can work with...once the data has been preprocessed, an algorithm is developed to process it. There are many different natural language processing algorithms" (Burns and Lutkevich 2021). Sonya uses a machine-learning based algorithm that hones rules, becoming more effective through repeated processing and learning. The security of collected and created data is of prime importance when using this type of technology, as is the security of the machine learning algorithm itself. This includes potential threats against physical infrastructure that houses the servers. Additionally, the ability of the AI to learn and grow independently necessitates a degree of risk involving its unknown future development.

Security Risks of Natural Language Processing

The use of natural language processing is not without risks. As adaptive machines like Sonya become increasingly complex and adept at lifelike conversation, it could inadvertently lead to the sharing of unnecessary information by users. Likewise, an intelligent enough machine could at some point begin to draw its own conclusions about the user via inferences based on unrelated input. In these scenarios, Callego could find itself in possession of unwarranted personal identifiable information (PII) such as social security numbers or birth dates. Additionally, if a user volunteers unsolicited information, it will still be processed by the algorithm and interact with the database. The transmission and storage of such information is protected by regulations such as the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR). The potential for the Sonya IVA to access PII thus creates extra challenges regarding privacy, compliance, and maintaining security of this information.

Once data has been created, NLP uses it to learn, oftentimes repeating and reusing words, phrases, and extracts of conversations from other users. Unfortunately, this cannot occur with

encrypted data, necessitating the need for stored communications and user data to be unencrypted and vulnerable: “communication is extremely valuable and many companies store past communication. Data can be encrypted on servers, but the ML algorithm cannot be taught on encrypted data. The result would not make sense; moreover, NLP tools are not prepared to learn on encrypted data. This is one of the moments when communication is revealed and can be read” (Abdulla et al. 2021).

A final security risk worth mentioning involves the potential for the artificial intelligence that underpins this technology to develop in unpredicted, unexpected, or even dangerous directions. This could be influenced by threat actors tampering with the controlling algorithm via vulnerabilities in the NLP application architecture, such as malicious inputs.

Adversarial Attack Examples

1: Data Confidentiality is a priority for Callego, especially when regional and industry regulations require strict adherence to avoid harsh fines and/or penalties. The Sonya IVA is vulnerable to an attack against customer data confidentiality due to the need for large amounts of data needing to be transmitted to, and stored in the cloud for processing: “many chatbots operating on a website use only Hypertext transfer protocol secure (HTTPS), which transfers data through an encrypted connection by a Secure Sockets Layer (SSL) or Transport Layer Security (TSL). HTTPS is ‘point-to-point’ encryption as opposed to ‘end-to-end’ encryption. HTTPS is secure on the user’s connection to a load balancer, but then the data are decrypted back to plain text. This makes the data open to attack all services after the load balancer” (Abdulla et al. 2021). The availability of such unencrypted data could be an enticing target for a malicious insider that already has access to the system, this could be an engineer involved with Sonya’s NLP algorithm or an employee of the cloud-hosting service.

2: System Availability may be compromised by a threat actor launching a denial-of-service attack against Sonja. This could be accomplished via the introduction of inconsistent or malicious data via the chatbot or phone agent: "ML algorithms usually consider input data in a defined format to make their predictions. Thus, a denial of service could be caused by input data whose format is inappropriate. It may also happen that a malicious user of the model constructs an input data (a sponge example) specifically designed to increase the computation time of the model and thus potentially cause a denial of service" (Adamczyk et al. 2021). This type of attack highlights the vulnerability of chatbot functions, which by design accept and processes whatever the user inputs, potentially resulting in intentional application failure. Novel adaptations of this type of attack can also be used to corrupt the entire system, for example the recently discovered zero-day vulnerability involving Log4j: "the Log4j tool is turning strings meant for logging into executable code. If a server uses Log4j to parse any user-entered text anywhere, that text can be formatted to contain a command that is then executed on the remote machine, which in turn effectively can gain the user remote code execution on the host system with full system-level privileges" (Killian 2021). Such an attack against the Sonya IVA could result in the threat actor gaining access to customer data, allowing for corruption or exfiltration of the data, as well as access to the NLP algorithm and database enabling a wide variety of malicious activity.

Table 1: Adversarial Attack Threat Analysis

Threat No.	Asset at Risk	Threat	Threat Community	Threat Action
1	The Confidentiality of Sonya IVA and Cloud-Storage Database	Loss of Customer Data Confidentiality	Internal	Malicious insider accesses unencrypted data used in NLP, resulting in data breach.

2	Sonya IVA Application	Impaired System Availability	Advanced Persistent Threat	Malicious data input in chatbot requires excessive computation and overloads system.

Control Measure Explanation

Control measures are necessary to address the types of attacks outlined above. The first example can be mitigated with the implementation of *end-to-end encryption*, rendering sensitive data unreadable while stored. In the second example, malicious inputs can be mitigated by engaging in *adversarial training*: "the NLP models can be trained on datasets comprising information about adversarial activities. Once it is done, the NLP model will be able to detect adversarial activities and can respond by not modifying its behaviour in response to adversarial activity. However, to make it happen, datasets on adversarial activities are required" (Bhatti et al. 2021).

Various other control measures will be important to the overall success of the Sonya Project by reducing risks associated with IVAs. Examples of these controls are as follows:

- Develop policies and procedures as related to data access and storage.
- Regular and ongoing review of the Sonya NLP algorithm.
- Make safeguarding user privacy a priority (via policies/procedures).
- Create a user awareness policy to be accepted prior to interaction with Sonya
    - To include language and information sharing concerns, i.e., what not to share:
        - Full Name
        - Email Address
        - Physical Address
        - Credit Card Information

    - Social Security Number
    - Vacation Plans

- Penetration Testing
    - To include testing for SSL issues and third-party components
- Load Testing
    - The Sonya IVA will need to be robust enough to handle user traffic from multiple Caleggo customers at the same time, preventing latency and system availability issues.
- Customer Training

Control Measure Evaluation

Evaluation of these control measures has been conducted based on cost and efficacy, resulting in three suggested implementation phases. This ensures immediate attention is given to severe security vulnerabilities, as well as ongoing protection of the Sonya project and all customers involved.

Implementation Phases

A	Immediate Deployment
B	Within 3-6 Months of Project Launch
C	May Be Deployed Over Time/Ongoing

Control Measure Cost/Efficacy Analysis

Control Measure	Cost	Efficacy	Recommended Phase
End-to-End Encryption	Medium	High	A
User Awareness Policy	Low	High	A
Org. Data Security Procedures	Low	High	A
User Privacy Policy	Low	Medium	A
Load Testing	Medium	High	A
Adversarial Training	High	Medium	B
Penetration Testing	High	Medium	C
IVA customer B2B training	Low	Low	C
Algorithm Review	Medium	Medium	C

Ideally, optimum security for the Sonya IVA will be achieved once all control measures are effectively implemented. The recommended measures included in Phase A for immediate deployment are all indicative of cost-effective, high efficacy actions that will ensure a successful launch and help minimize the chances of unforeseen issues. Thereafter, adopting the measures in Phases B and C will ensure ongoing attention to security vulnerabilities and continuous improvement to the IVA processes, helped by the incorporation of feedback from customer use and user experience.

Summary

The preceding identification of security risks and recommended control measures have been carefully researched and selected to provide Callego with the greatest return on investment during the initial implementation of the Sonya intelligent virtual assistant. The consideration and adoption of these control measures will ensure a safe, secure, and successful launch of this exciting new technology, paving the way for Callego's continued growth and prosperity as the world's premier customer service expert.

Consulting Problem Two: Privacy Policy Revision to Meet GDPR Requirements and the Recommendation of Technical Controls to Meet the GDPR Standard of Due Care.

Part A: Revised Privacy Statement

Introduction

The recent announcement of Callego's newly formed partnership with the German firm Spatzchen signifies an exciting new chapter for the organization. Having already established itself as a top-tier customer service provider in the U.S. and across Asia, this partnership will allow for the establishment of a European presence as well. While exciting, this presence will involve interaction with the data of European clients, necessitating close attention to regional data privacy regulations. The General Data Protection Regulation (GDPR) contains stipulations and policies that Callego must now adhere to in order to remain compliant, avoiding costly fines and reputational damage. Part of this process involves a revised organizational privacy statement that will reflect GDPR principles and foster trust, security, and prosperity in this new venture.

Revised Privacy Statement

Please see following page.

-this area left blank intentionally-

Callego Privacy Statement

Callego is dedicated to maintaining the highest privacy standards for our customers while delivering world-class customer service. This document was last updated March 2022.

Data We Collect

In order to conduct our business and provide valuable services, we collect personal and non-personal data about our customers. This includes personal identification information such as:

- Name
- Email Address
- Telephone Number
- Purchase Records
- Payment Information
- Social Media Profile Information

How We Collect Data

We collect data directly from our customers in the course of ordinary business such as:

- When a customer submits a request
- When a survey is completed
- Via cookies when our website is visited
- When a customer interacts with the Sonya virtual assistant

We also acquire customer data from third-party sources, which include partners and affiliates such as Spatzchen.

How We Use Data

We may use customer data to develop new services, personalize existing services, or for other purposes such as research and business development. The amount of personal data collected is limited to the amount necessary to fulfill the specific business purpose for collecting said data (data minimization).

Data collected and used is done so under a lawful basis, the *legitimate interest* of customers, insofar that it is used for the purposes that customers would expect or otherwise deem reasonable. This includes customer data used in the machine learning functions of Callego's intelligent virtual assistant and other data analytics processes.

How We Store Data

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. This stored data will only be kept for as long as necessary for the purposes it was processed, as described above. Wherever possible, stored data is encrypted and/or anonymized.

Sharing and Transfer of Data

Callego is a global company with presence in the U.S., Asia, and Europe. Data may be transferred between Callego and partners for the express purpose of improving customer service capabilities and addressing customer needs. European customer data may be sent to a cloud-

hosted database in the U.S. for the purpose of data analytics and improving the intelligent virtual assistant algorithms.

Marketing

Callego would like to contact customers for marketing and promotional purposes. If customers have agreed to marketing, they may opt out at a later time, and may opt out of the sharing of their data between Callego partners.

What Are Your Data Protection Rights?

Every Callego customer is entitled to the following rights:

- The right to access their data: copies of stored data may be requested (for a small fee).
- The right to rectification: any inaccurate information may be corrected and/or completed.
- The right to erasure
- The right to restrict processing
- The right to object to data processing
- The right to data portability

Callego reserves a one-month duration for which to respond to customer exercising of these rights.

Our Cookie Policy

Cookies are text files placed on your computer to collect standard internet log information and visitor behavior information. When you visit our website, we may collect information from you automatically through cookies.

Contact

Customers may contact Callego to exercise their rights as indicated via the following:
Email: customerconnect@callego.com
Telephone: 555.555.5555

Callego will occasionally update this Privacy Policy. When changes to this Privacy Policy are posted, the date at the top of this Privacy Policy will be revised. We recommend checking the website from time to time to inform yourself of any changes to this Privacy Policy or any of other policies.

Explanation of Work Process

The work process undertaken consisted of investigating where the former privacy statement falls short of expected GDPR principles. This warranted research into key components as outlined on the European Commission's website, which was then used to compare, contrast, and apply to this particular organization. As opposed to the former Callego privacy policy, the revised policy contains necessary information aimed providing customers with greater detail and more information. This type of disclosure is important in maintaining compliance, and thus the following new sections were added to the policy:

- List of data protection rights
- More specific disclosures surrounding data (types, use, etc.)
- How customer data is collected, protected, transferred, used, stored, and destroyed.
- Sharing and Transfer of Data
- Cookies information
- Contact information

Additionally, the GDPR stipulates that there must be an identified lawful basis for processing customer data, which is identified in the "*How We Use Data"* section. Care has been taken to compose a reader-friendly statement that did not become too detailed or delve into becoming a checklist, as this would then increase the likelihood of only those items on the list being attended to at the possible expense of overlooking additional areas of concern.

Justification Under GDPR

Looking at the revised statement in greater detail reveals that it meets standards of reasonableness and due care aligned with the principles of GDPR and EU conceptions of privacy. To confirm this, the following principles of GDPR were examined and applied:

- What data can we process and under what conditions
    - See "*Data We Collect*" and "*How We Collect Data*"
- For how long is data kept and is it necessary to update it?
    - See "*How We Store Data*"
- Purpose of data processing.
    - See "*How We Use Data*"
- What information must be given to individuals whose data is collected?
    - See "*Marketing*", "*What Are Your Data Protection Rights*", "*Cookies*", "*Contact*"
- How much data can be collected?
    - See "*How We Use Data*"

Of key importance for any organization seeking to expand operations into other areas of the globe is the variation in cultural norms and expectations. As it applies to Callego's new partnership and thus access to European customer data, the European conception of privacy is an important consideration that must be acknowledged as part of a broader successful expansion: "the European Union was an institution founded on a balance of intergovernmental and supranational policies, and, in this case, its approach to data privacy is supranational. The United States, conversely, continues to emphasise [sic] states' rights in its governing, and, its bottom-up approach to data privacy is conducive to that emphasis" (McCoy 2021). This is indicative of privacy expectations in Europe, wherein the average person likely has higher expectations due to widespread agreement and the blanket adoption of rights/regulations, vs. the state-by-state considerations in the U.S. Some examples that reflect Europe's greater privacy concerns, and specifically Germany where Callego's partner Spatzchen is located, are as follows:

- In Europe, Facebook's facial recognition software is banned.
- Google must first alert Europeans in advance when sending out "street view" cars, and in some places (i.e., Germany) citizens may request for their homes to be blurred.
- "A German court ruled against Google and on behalf of a German businessman who argued that the search engine's autocomplete function which associated him with "scientology" and "fraud" constituted a privacy violation" (Wittmeyer 2013).

This difference in privacy conceptions has been incorporated into the revised statement with the addition of more specifics, greater detail, enhanced (two-way) communication, and the affirmation of user rights.

Discussion of Impacts on Organization

When a company such as Callego puts forth a statement of any kind, including privacy, it is a direct reflection of the core mission, operations, and culture of the organization. This means that revising the privacy statement is indicative of a deeper shift at Callego impacting all of these areas. For instance, the organizational mission at Callego centers around the ability to provide clients expert customer service representation despite difficulty or complexity, leveraging years of experience with sensitive information. The adoption of more stringent policies will essentially raise the bar when it comes to working with sensitive information, adding strain to operations during implementation, but further bolstering Callego's commitment to, and experience with, such data. This shift in degree of attention will undoubtably affect the organizational culture by emphasizing privacy, security, and the flexibility needed to assimilate new or foreign concepts. Embracing GDPR compliance will serve Callego by demonstrating to the world, both customers and competitors alike, how seriously and personally the organization takes people's rights to privacy. As a customer service company, this highly visible commitment to people will only

further enhance positive perceptions and help Callego stand out from other companies. While this shift entails significant upfront costs to implement technical controls and compliance auditing, the resulting cultural and reputational impacts, alongside access to an entire continent of potential customers, will more than account for this initial expense.

Annotated Top-Three List of Documents to Revise Under the GDPR

- Data Retention Policy

Prior to entering the partnership agreement with German customer-service outsourcing firm Spatzchen and thus falling under GDPR compliance obligations, Callego did not have a well-documented policy for organization-wide data retention. In fact, disparities existed between departments and divisions that make the revision and implementation of this document at the organizational level a priority. The revised contents which will align with GDPR include:

- The types of information covered in the policy.
- The length of time Callego is entitled to keep data.
- What is done with data that is no longer needed.
- What is done with data held past the retention period. This section is important as it has implications for data used with Callego's Sonya IVA learning algorithms. It is suggested that all data retained in Sonya's server database be anonymized to maintain GDPR compliance.

From a mission and operational standpoint, the revision of this document and implementation of its contents will help save money by reducing the storage of unnecessary data and applicable issues surrounding storage, i.e., security. Additionally, the document will prepare Callego for future regulation in the U.S. that contains overlapping requirements with the GDPR: "a little

noticed provision of new consumer privacy laws in California and Virginia, effective January 2023, is the need for detailed data retention schedules and defensible destruction programs... by 2023, alongside the GDPR's data minimization requirements, U.S. data privacy legislation will require specific disclosures regarding data retention periods" (Squire et al. 2021). In essence, revision of the data retention policy document could give Callego an edge against competitors in the U.S. region by making the organization "pre-compliant" and lessening resource allocation to this issue in 2023.

- Incident Response Procedures

Callego's documented incident response procedures are an integral component of GDPR compliance: "developing a proven, consistent, and repeatable incident response plan is critical for complying with the GDPR. This plan should include all steps that are needed in the event of a data breach and should be tested frequently to identify gaps" (Redmon 2018). Prior to interacting with European Union customer data, Callego was not bound by certain necessities in terms of incident response procedures, creating the need for review and revision to meet updated standards and avoid regulatory violations and penalties. Items to be revised/added to the current incident response procedures include the release of the following information in the event of a breach:

  - Specific data breach details (number and type of data records and subjects).
  - Contact details for Callego's Data Protection Officer.
  - Likely consequences of the data breach.
  - Actions taken to address the breach.

Additionally, there is now a 72-hour window to notify supervisory authorities that a breach has occurred, making it necessary to incorporate contact and timeline information into the updated procedures (as suggested in tabletop exercise projected lessons learned).

As a customer service company, Callego relies heavily on reputation and delivering on the marketing campaign promise of "we are with you" which seeks to reassure customers of the organization's commitment and capability in handling complex issues. With data breach statistics showing a steadily increasing likelihood of occurrence at some point in time, Callego must consider the effect this will have on customers: "according to the 2021 Annual Data Breach Report, the overall number of data compromises (1,862) is up more than 68 percent compared to 2020" (Achten 2022). Revising the incident response procedures to meet GDPR standards will also help the organization retain customer confidence during a breach, which does count as a "complex issue", due to honest communication, increased reaction speed, and a demonstrated commitment to resolving issues affecting customers in a professional and expedient manner.

- Bring Your Own Devise (BYOD) Acceptable Use Policy

While BYOD has become more common and convenient for many organizations, it does pose particular risks to GDPR compliance and especially the required principle of accountability: "this principle is defined in GDPR Art.5.2, stipulating that: The controller shall be responsible for, and be able to demonstrate compliance with [other data protection principles] and crucially with the principles of security and confidentiality introduced in Art.5.1.f)" (Sotiriou 2021). It is recommended that when employees do use personal devices, they do so via virtual private network to meet the GDPR stipulation that data must remain within the controller's sphere of control. Revised contents of the policy should include:

- Allowed apps and tools to be used on employee devices.
- Process for accessing data using employee devices.
- Approved device models and versions of operating systems.
- Password security requirements.
- Policy emphasizing the viewing of data rather than storage.
- Procedures for transferring data from one device to another.
- Reporting procedure for security concerns.
- Data storage policy (should be as little as possible).
- Regular auditing period.
- Enforcement and accountability provisions for non-compliance.
- Mandated technical measures to be used on employee devices such as data encryption and anti-malware software.

Implementation of a policy with these components will better align Callego practices with GDPR by increasing data security and oversight. Principle 7 of the GDPR concerns security, and the updated policy addresses those security risks that arise when employees use their own devices. The benefits of BYOD are well known and at an operational level can increase employee productivity while reducing organizational hardware cost. Callego's track record of working with sensitive data has engrained data security into its organizational culture, raising employee security awareness and education. While BYOD has risks in terms of security that could threaten GDPR compliance, if any company is prepared to address these risks and reap the benefits of more a more content and productive workforce while maintaining compliance, its Callego.

Summary

Competition in the customer service market has been steadily increasing over time, making it essential that successful organizations evolve and adapt to maintain market share. A key part of this is the transition to a more digitized, interconnected world, one which offers many new and exciting opportunities, such as improving customer service via the use of artificial intelligence. This evolution also results in interaction with ever-increasing amounts of customer data at a time when individuals and institutions are taking privacy more seriously than ever. Adapting Callego's privacy policy to meet GDPR principles not only helps address these concerns, but it also allows this organization to continue its record as the world's most capable customer service expert while accessing an entire new continent of potential customers.

Part B: Technical Recommendations

Introduction

As Callego proceeds with an accelerated timetable concerning the Spatzchen partnership, responsive actions are required to quickly meet GDPR principles and compliance. The following memo outlines practical and effective control measures based upon cost effectiveness and deployment timeframes which will meet the necessary requirements for this exciting new era.

Identification and Description of Recommended Control Measures

Adoption of the following three control measures is recommended to help align Callego with privacy expectations of the GDPR and the newly revised privacy statement:

<u>Encryption</u>

Encryption is a mathematical function which uses a key (secret value) to encode data and ensure that only users with access to that specific key can access the data. Specifically, application-layer encryption is recommended in which encryption and decryption is performed at the end application, ensuring data remains encrypted in transit through Callego's network until it reaches the specific destination application containing the decryption key. Adopting this control will help maintain the confidentiality and integrity of user data that Callego and its partner organizations collect.

Identity and Access Management (IAM)

IAM is based on defining specific roles and access privileges of users and devices to both cloud and on-premises applications. Properly implemented, it will ensure that assets (i.e., data) are only able to be accessed when granted, and in a given context. As a software solution at the application level, IAM will ensure that confidential and protected information is only accessed when authorized and appropriate, while simultaneously bolstering the security of other network locations such as hosts. Other components of a robust IAM system include multi-factor authentication, user behavior analytics, and change management such as de-provisioning of digital identities.

Intrusion Prevention System (IPS)

An IPS is a security tool that will continuously monitor Callego's network for any malicious activity and take actions to prevent it when detected. Functioning at the network level, the system will monitor traffic flows to detect and prevent any vulnerability exploits. Typically placed directly behind the firewall, "the IPS is placed inline (in the direct communication path

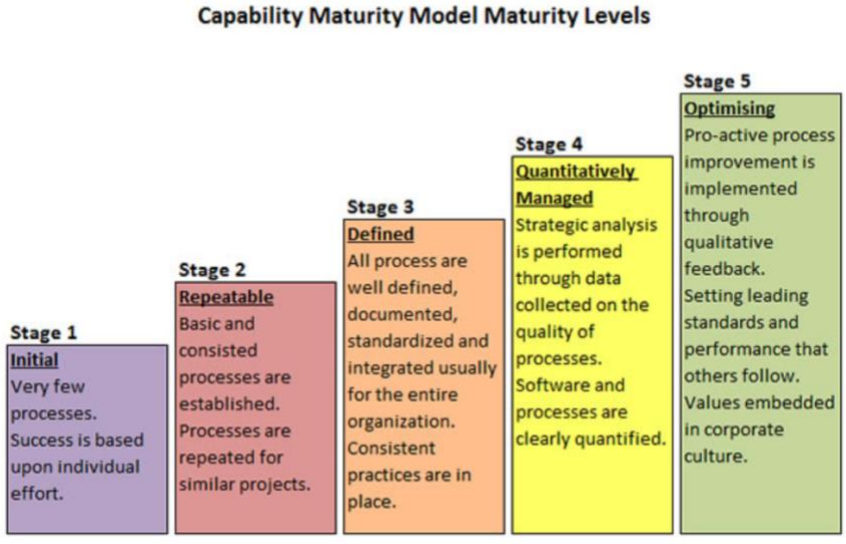
between source and destination), actively analyzing and taking automated actions on all traffic flows that enter the network. Specifically, these actions include:

- Sending an alarm to the administrator (as would be seen in an IDS)
- Dropping the malicious packets
- Blocking traffic from the source address
- Resetting the connection" (PaloAlto 2022)

A properly implements IPS will help safeguard sensitive data and overall business operations by ensuring constant vigilance and rapid reaction to potential threats.

Present and Future State Description

When evaluating the three selected controls, it is helpful to compare them against existing controls already in place. The Capability Maturity Model effectively illustrates how these changes increase Callego's security posture by showing a change in current level. The five maturity levels of this model are the initial, repeatable, defined, managed, and optimizing levels.



(Humphrey 2011)

Control: Encryption

Current State: This control is currently only used by select individuals using public/private keys to sign emails, meaning it is at the Initial level. This reflects that success relies upon individual effort and the control is not widely adopted.

Future State: Defined. Once encryption is implemented for all data traversing or residing in Callego's network, this control will advance two stages. This accounts for improved consistency and standardization.

Control: Identity and Access Management (IAM)

Current State: Based upon current policies and procedures such as password management and physical access controls, this control is at the Repeatable stage.

Future State: Implementation of robust IAM will result in an upgrade to stage four, Quantitatively Managed. The ability to manage access and perform strategic analysis on collected data will help Callego improve security and identify potential insider threats before vulnerabilities are exploited.

Control: Intrusion Prevention System (IPS)

Current State: Callego currently relies upon firewalls to prevent unauthorized access to the network. Due to basic and consistent use, this reflects a positioning at the Repeatable stage.

Future State: Implementing an IPS would also take this control to the Quantitatively Managed level, wherein "an organization monitors and controls its own processes through data collection and analysis." (NAS 2007). The system will be able to mature as new vulnerabilities and exploits are discovered, allowing for improved defense and proactive response.

Overall Appraisal: As a simple measure, adding the numerical value of the current vs. future maturity stages shows an overall increase from 5 to 11, indicative of the effective increase to security.

Systematic Functionality Explanation

All three control measures work in tandem to systematically bolster security at Callego. In a layered defensive model in which data is the threat actor's target, the first line of defense is a combination of internal/external protection offered by IAM and IPS. If the attacker is internal, a properly implemented IAM will prevent or greatly interfere with inappropriate data access from the outset by disallowing unauthorized access while simultaneously discouraging attempts via user activity monitoring. At the same time, the IPS will alert to unusual or suspicions activity, even taking preemptive measures such as disconnection if necessary. If the attacker is attempting to infiltrate the network from an external source, the IPS is designed to detect and act immediately with actions such as dropping malicious packets and blocking traffic from the source address. If these lines of defense are breached nonetheless, the additional security layer of encryption will ensure that the threat actor still does not have access to readable data. In this way, all three control measures will function systematically to protect Callego's network and increase security.

Information Security Principle Explanation

The recommended control measures meet several principles for information security. As outlined in the previous section, the controls effectively contribute to a layered security model by working in tandem to protect data, with redundancy in case of failure. In addition, the following principles are met:

- Least Privilege: “The principle of least privilege recommends that users, systems, and processes only have access to resources (networks, systems, and files) that are absolutely necessary to perform their assigned function. By governing the level of access for each user, system, and process, the principle of least privilege limits the potential damage posed via unsanctioned activities, whether intentional or unintentional” (CIS 2022). This principle is met when IAM is implemented because it involves assigning users (and devices) a unique digital ID that will restrict/authorize access to information and network locations based upon the specific role and use, which can be programmed in alignment with the concept of least privilege.
- Defense in Depth: Augmenting layering, this principle ensures that risks are controlled for using multiple fashions such as physical, technical, and administrative. The recommended implementation of encryption alongside an Intrusion Prevention System illustrate the concept of defense in depth by impeding/slowing a successful attacker first by identifying and taking actions to prevent access, and then by rendering targeted data unreadable, thus less appealing.

Justification

With the accelerated timetable moving the Spatzchen partnership forward to early next month, implementing these control measures is now more important than ever. Determining practicality, cost effectiveness, and expedience will reveal optimal timing and effects to the organization.

- Encryption

Implementing widescale data encryption is feasible within the accelerated timeframe, and is worth the upfront cost in order to comply with GDPR due diligence requirements and set the

tone for an overall increase in organizational security culture. In terms of value, Callego must consider not only the cost of leaked/stolen data, but also the potential fines for GDPR violations: "less severe infringements could result in a fine of up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher" (Wolford 2022). All variables considered, implementing encryption can and should occur prior to the partnership launch date and its value is highly justifiable.

- Identity and Access Management (IAM)

Taking longer to implement, yet with wide-reaching and lasting impact, IAM will require more upfront investment from Callego. This investment will result in a substantial increase in security, while positioning the organization for continued growth. The ability to automate portions of IAM means that workflows, access rights, processes, and applications remain GDPR compliant and are able to be consistently tracked and adapted. Internal costs of this control include preparation costs, implementation costs, and ongoing operational costs: "The total costs (license fees and internal and external implementation costs) of an average project for a company with 20.000 users, and 4 system types supported by an Identity and Access Management System (e.g. Windows, Unix, Mainframe and SAP) usually exceed 1 million Euros" (Kern 2022). This falls far short of the GDPR fine of €10 million, making the investment cost effective and recommended. The implementation phase can begin immediately with the selection of systems and which aspects of the organization are to be included, including potential new hires as necessary (technical employees).

- Intrusion Prevention System (IPS)

Implementing an IPS is a practical and valuable addition to Callego's operations. The wide array of information gathering, detection, and reactive abilities will help ensure GDPR compliance, especially with regard to minimizing the time taken to detect new threats. Additionally, GDPR requires exhibited due diligence with regard to efforts made in safeguarding user data, which can be addressed with a robust and adaptive network security architecture. At an operational level, a properly implemented IPS can also alleviate time-consuming actions typically performed by employees such as a network administrator by automating many tasks such as packet inspection and hardware inventory, both increasing efficiency and reducing labor costs, helping to offset the cost of implementing the IPS.

Summary

While the accelerated timeframe surrounding the Spatzchen partnership poses challenges related to GDPR compliance, the recommended technical controls will address this. It is recommended that encryption be implemented immediately, followed by an Intrusion Prevention System, and finally Identity and Access Management. The initial phases of assessment and pre-positioning of resources for the latter two controls can begin immediately, with the goal of a fully functional IPS within three months, and organization wide IAM by six months. During the period leading up to complete implementation, aspects of these controls will already be increasing security at Callego and contributing to overall GDPR compliance.

Consulting Problem Three: Incident Management Tabletop Training Exercise

Introduction

As Callego concludes an eventful quarter highlighted by the implementation of the Sonya intelligent virtual assistant and the Spatzchen partnership, it is important to be reminded that both of these advancements present new security concerns. Cyber threats are constantly evolving and any potential weakness within an organization creates the risk of exploitation. The following tabletop exercise has been designed to bring awareness to certain security issues related specifically to the Sonya project, but with implications for GDPR compliance as well. The relevant issues explored are as follows:

- Unintentional Insider Threats
- Employee Security Awareness/Training
- Malware Intrusion Detection
- Data Breach/Compromise

As the exercise unfolds, participants will have the opportunity to suggest actions related to unfolding events, ask questions or seek clarification, and offer input from their relative area of expertise.

Objectives

While there are numerous benefits and advantages to conducting a tabletop simulation exercise, the specific objectives of this particular scenario are as follows:

- Identify strengths/weaknesses in organizational processes and procedures.
- Identify potential weaknesses in staff response.
- Increase familiarity with Callego's incident response plan.
- Familiarize staff with current threat environment.

- Highlight areas of significant security concern.
- Increase communication between different departments/roles.
- Encourage critical thinking at all times.
- Increase reaction speed during a suspected incident.
- Prevent exploitation by identifying and mitigating vulnerabilities.

Team Roles and Responsibilities

The following roles, as members of the incident management team, will participate in the exercise:

- Lead Facilitator: "The primary host of the exercise, this individual is responsible for setting the stage, presenting the exercise scenario, introducing injects and discussion questions, and facilitating conversation between exercise participants. The Lead Facilitator should have experience with exercises or the subject matter area being discussed—though this does not necessitate that the individual be an expert in cybersecurity" (Constantini and Raffety 2021).
- Information Technology Management: decision-making participant.
- Security Operations Management: decision-making participant.
- Lead Network Security Analyst/Engineer: information resource and participant.
- Lead System Administrator: information resource and participant.
- Documentation Lead: responsible for record keeping and documentation of all aspects of exercise including decisions made, responsible parties, and lessons learned.
- Suggested Cross-Departmental Spectators
    - Human Resources
    - Legal

- Public Relations

Elements To Be Tested

The following four elements will be tested and/or potentially exploited in this exercise:

- Security Principle: Defense in Depth: “defense-in-depth is an information assurance strategy that provides multiple, redundant defensive measures in case a security control fails or a vulnerability is exploited” (Imperva 2021). This principle is reflected in the exercise by a combination of administrative and technical control measures aimed at preventing access to the Sonya IVA database. Administrative controls include employee security awareness training with an emphasis on phishing education, while technical controls include Callego’s new IDPS system.
- Security Policy: Employee Email. Current Callego policy forbids employees from clicking on unknown links, however the scenario takes advantage of confusion caused by the recent introduction of the Sonya IVA and a sense of urgency in problem solving a potential customer issue.
- Technical Control Measure: While the IDPS is capable of identifying and responding to malicious traffic such as would be detected upon malware infestation or data exfiltration, the exercise takes advantage of the fact that a new IDPS system takes time to be trained and establish a baseline. During this time the system as a whole is weaker, and the potential for vulnerability exploitation is higher as determined by employee reactions.
- Incident Response Countermeasure: Containment. “Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early in the course of handling each incident. Containment provides time for developing a tailored remediation strategy. An essential

part of containment is decision-making (e.g., shut down a system, disconnect it from a network, disable certain functions)" (NIST 2012). The scenario will test whether Callego employees make the appropriate containment decisions or if the situation degrades further.

Exercise Timeline

Initial Attack Vector

The initial attack vector is email, in the form of a malicious link that downloads malware onto an employee workstation. Taking advantage of the relative newness of the Sonya intelligent virtual assistant implementation and likely growing pains, the threat actor has crafted a believable email to customer service describing troubles with the chatbot and attaching a file said to contain visual proof of the problem. Under pressure to quickly remedy the issue and save Sonya's reputation, the employee seeks to fix the problem immediately and clicks the link to investigate what exactly is going wrong.

Initial Response Frame

The initial attack will test employee security awareness and protocol adherence. The decision made is whether to click the link or to notify IT/Security due to the attachment. At this point the facilitator should prompt a group discussion on phishing techniques (pressure, social engineering, etc.) as well as policy review.

Branching Scenarios

Assuming the employee clicked the malicious link, the exercise shifts to further repercussions. The employee is now having issues with their workstation (slow processing, freezing, strange pop-ups, etc.), and contacts IT for assistance. After briefly describing the

situation, the IT specialist must decide what actions to take. This will test isolation techniques, network segmentation, and containment strategies.

Moving further along, the IT worker did not catch the warning signs and instead of acting, simply filed a request for new equipment to replace the employee's malfunctioning workstation. At this point, the IDPS is sending a large amount of notifications to security personnel, which can either be viewed as an emergency or a glitch due to the new system. The final decisions made with regard to these alerts will have great impact on how much customer data is stolen, what type of GDPR violations occur, Sonya/website operability, etc. There is a very real possibility of continued degradation, systems taken offline, and a severe data breach involving the protected information of scores of Callego customers.

Potential Injects

A) Unknown to IT, the threat actor has already established command and control (C2) and the infected workstation is regularly pinging (checking-in with) another IP address. When IT takes the workstation offline, this ping does not get sent, firing the attacker's failsafe, and causing customer data to be encrypted.

B) Suppose the attachment contained a different form of malware, aimed at taking Callego's entire system offline and undermining the ability to operate effectively. The website becomes unavailable the Sonya IVA (both chat and voice features) is suddenly offline.

C) The email is blocked, but somehow the malware still it's made its way into the network. Management overhears employees discussing unusual drone activity over the campus courtyard during lunch hour; later, an infected USB is found atop the trash near a now malfunctioning workstation.

Inject Response Frames

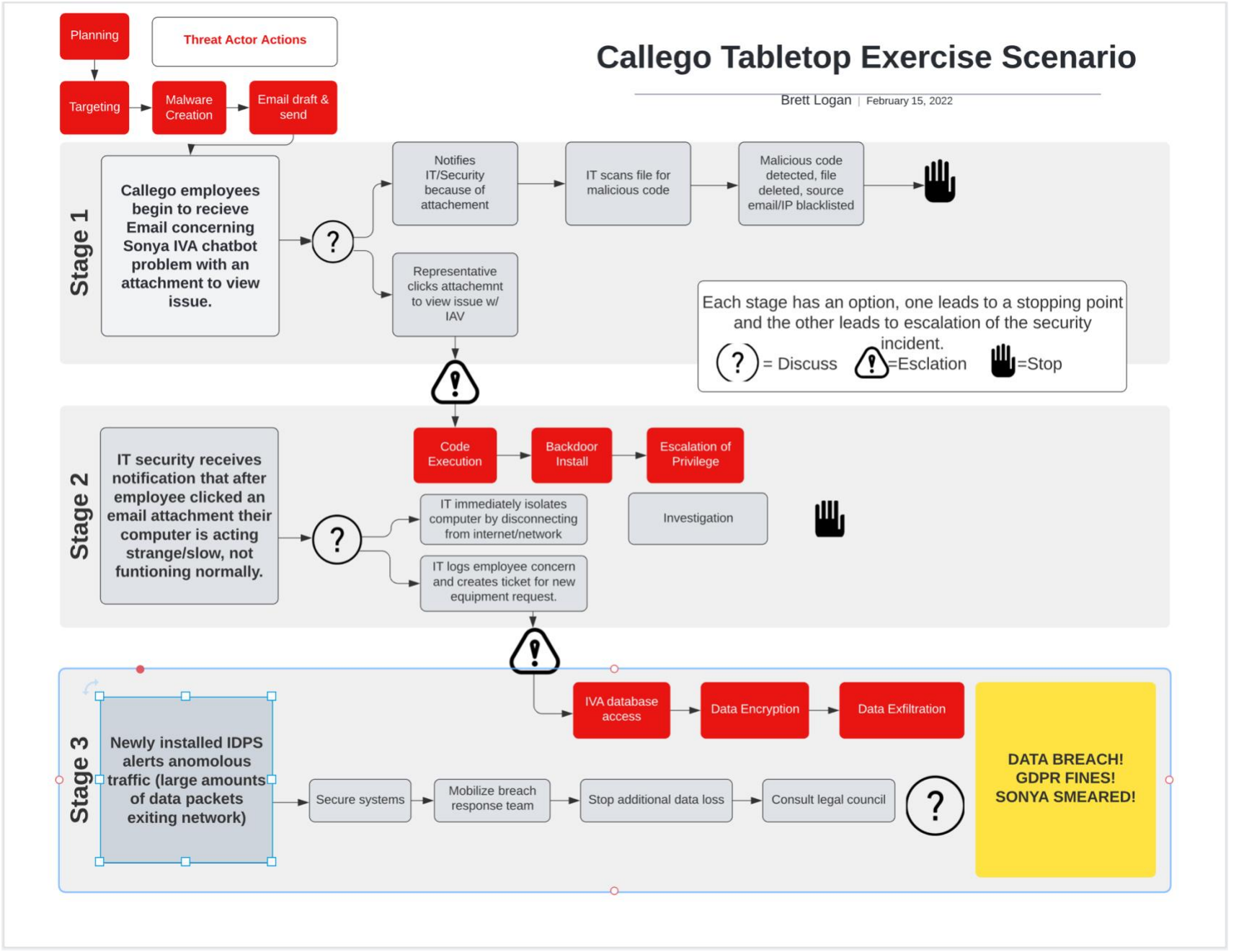
A) This inject will test procedure following data encryption. Facilitator should prompt group discussion based on countermeasures and actions. Suggested questions include:
    - Can the data be unencrypted?
    - What is the organizational policy on ransomware?
    - How will we know the extent of affected data?
    - How long do we have to notify affected customers?

B) This inject will test procedures and controls. Facilitator should prompt group discussion on policy and procedure as it relates to a DDoS attack.
    - How is the organization affected?
    - What happens to data that was in queue w/ IVA prior to outage?
    - What procedures are in place to restore access?
    - What countermeasures currently exist to prevent this from happening?

C) This inject tests principles surrounding employee security awareness. Group discussion should be focused on alternative/creative attack vectors and how the average employee might respond.
    - Can this type of vector be eliminated?
    - Do current policies address this scenario?
    - How long would it take to determine what had happened?

Visual Representation

Please see following page.


Planning
Threat Actor Actions
Targeting
Malware Creation
Email draft & send
Callego Tabletop Exercise Scenario
Brett Logan | February 15, 2022
Stage 1
Callego employees begin to recieve Email concerning Sonya IVA chatbot problem with an attachment to view issue.
?
Notifies IT/Security because of attachement
IT scans file for malicious code
Malicious code detected, file deleted, source email/IP blacklisted
Representative clicks attachemnt to view issue w/ IAV
Each stage has an option, one leads to a stopping point and the other leads to escalation of the security incident.
?= Discuss
=Esclation
=Stop
Stage 2
IT security receives notification that after employee clicked an email attachment their computer is acting strange/slow, not funtioning normally.
?
Code Execution
Backdoor Install
Escalation of Privilege
IT immediately isolates computer by disconnecting from internet/network
Investigation
IT logs employee concern and creates ticket for new equipment request.
Stage 3
Newly installed IDPS alerts anomolous traffic (large amounts of data packets exiting network)
IVA database access
Data Encryption
Data Exfiltration
Secure systems
Mobilize breach response team
Stop additional data loss
Consult legal council
?
DATA BREACH!
GDPR FINES!
SONYA SMEARED!

Projection of Lessons Learned

In summary, the following takeaways can be derived from the exercise:

- A key area of vulnerability was uncovered relating to the implementation of new processes and services (the Sonya project and the IDPS). A well-researched threat actor could take advantage of the training period for both of these systems.
- Lack of employee security awareness needs to be addressed via updated policies, procedures, and training that includes phishing, social engineering, and external device usage.
- There is significant confusion surrounding GDPR reporting requirements. This necessitates clarification and the drafting of formal policy.
- More training is needed on IDPS alert response and communication chains. There is a tendency to rely heavily on automation at the expense of overall security. Further investigation is warranted into how best to utilize the human component in tandem with this new system.
- Current communication policy is resulting in slow reaction times and confusion under pressure.
- Callego's organizational security culture is not currently homogenous; different departments are approaching security from individual perspectives. A revamped security training program could address this and improve the overall security posture by ensuring more consistent and united threat response.

References

Abdulla, H., Hasal, M., Nowaková, J., Ogiela, L., Saghair, K., and Snášel, V. 2021. Chatbots: Security, Privacy, Data Protection, and Social Aspects. Concurrency Computat Pract Exper. 2021;33:e6426. https://onlinelibrary.wiley.com/doi/pdf/10.1002/cpe.6426

Achten, Alex. 2022. Identity Theft Resource Center. Identity Theft Resource Center's 20212 Annual Data Breach Report Sets New Record For Number of Compromises. https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/

Adamczyk, M., Agrafiotis, I., and Malatras, A. 2021. European Union Agency for Cybersecurity (ENISA). Securing Machine Learning Algorithms. https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms

Bhatti, B. M., Mubarak, S., & Nagalingam, S. 2021. Information security implications of using NLP in IT outsourcing: a Diffusion of Innovation theory perspective. *Automated Software Engineering*, *28*(2), 12. https://doi.org/10.1007/s10515-021-00286-x

Burns, E. and Lutkevich, B. 2021. TechTarget. A Guide to Artificial Intelligence in the Enterprise. Natural Language Processing (NLP). https://www.techtarget.com/searchenterpriseai/definition/natural-language-processing-NLP

Center for Internet Security (CIS). 2022. Election Security Spotlight- Principle of Least Privilege. https://www.cisecurity.org/insights/spotlight/ei-isac-cybersecurity-spotlight-principle-of-least-privilege

Constantini, L. and Raffety, A. 2021. National Association of Regulatory Utility Commissioners. Cybersecurity Tabletop Exercise Guide. https://pubs.naruc.org/pub/615A021F-155D-0A36-314F-0368978CC504

European Commission. 2022. Principles of the GDPR. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr_en

Humphrey, Watts. 2011. The Data Group. Management Theories Blog. Capability Maturity Model. https://www.data-group.com.au/1-38-capability-maturity-model-cmm/

Imperva, no author stated. 2021. Learning Center Blog. Defense-in-Depth. https://www.imperva.com/learn/application-security/defense-in-depth/

Jaycocks, A., Mann, S., Marcellino, W., Matthews, L., Pearsons, J., Schimer, P., and Schulker, D. 2021. Rand Corporation. Natural Language Processing. Security and Defense Related Lessons Learned. https://www.rand.org/pubs/perspectives/PEA926-1.html

Kern, Dr. Axel. 2022. BetaSystems. Measurable IAM Benefits Part 3- Cost Calculation. http://blog.betasystems-iam.com/iam-benefits-part-3-iam-cost-calculation/

Killian, Zak. 2021. Hot Hardware Blog. Serious Log4j Security Flaw Puts The Entire Internet At Risk- Even iCloud and Stream. https://hothardware.com/news/serious-log4j-security-flaw-puts-the-entire-internet-at-risk-even-icloud-and-steam

Liddy, E. 2021. Syracuse University School of Information Studies. Natural Language Processing. https://surface.syr.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/scholar?hl=en&as_sdt=0%2C38&as_vis=1&q=natural+language+processing&btnG=&httpsredir=1&article=1019&context=cnlp

McCoy, Owen. 2021. European Interactive Digital Advertising Alliance. A Legislative Comparison: US vs. EU on Data Privacy. https://edaa.eu/a-legislative-comparison-us-vs-eu-on-data-privacy/

National Institute of Standards and Technology (NIST). 2012. Special Publication 800-61. Computer Security Incident Handling Guide. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

No Author Stated (NAS). TechTarget. Capability Maturity Model (CMM). https://searchsoftwarequality.techtarget.com/definition/Capability-Maturity-Model

PaloAlto Networks, no author stated. 2022. Network Security. What is an Intrusion Prevention System? https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

Redmon, Gant. 2018. Security Intelligence. Incident Response Under GDPR: What to do Before, During, and After a Data breach. https://securityintelligence.com/incident-response-under-gdpr-what-to-do-before-during-and-after-a-data-breach/

Schneider, Gary. 2021. Ubiq Security. Why is Application-Layer Encryption So Important. https://www.ubiqsecurity.com/blog/what-is-application-layer-encryption/

Sotiriou, Athina. 2021. TechGDPR. Bring Your Own Devise And Data protection. https://techgdpr.com/blog/bring-your-own-device-and-data-protection/

Squire, Patton, Boggs LLP. 2021. United States: Robust Data Retention Programs Required By New Laws. https://www.mondaq.com/unitedstates/data-protection/1070526/robust-data-retention-programs-required-by-new-laws

Wittmeyer, Alicia. 2013. Foreign Policy Analysis. Do Europeans Really Care More About Privacy Than Americans? https://foreignpolicy.com/2013/06/11/do-europeans-really-care-more-about-privacy-than-americans/

Wolford, Ben. 2022. GDPR. What Are The GDPR Fines? https://gdpr.eu/fines/