**Glasworks Inc.**

**Security Ambassador Program**

**ISE 5300**

**Building Security Awareness**

[This document is not a complete security awareness plan document. It only covers the sections required by the ISE 5300 course offered as part of the SANS Technology Institute’s Master of Science in Information Security Engineering as of February 2021.]

|  |  |
| --- | --- |
| **Prepared By** | Jon Glas |
| **Date Revised** | 07/01/21 |
| **Version Number** | 1.0 |

# README

The business I have chosen is a fictitious company called Glasworks Inc. Glasworks Inc is a representation of my current employer to keep their details anonymous. Glasworks Inc is a company with a strong base in security with numerous awareness programs already in effect. The topic chosen for the Security awareness plan is to implement a Security ambassador program. This program will build upon the existing security foundation by building a community of advocates to help promote security across the company.

Table of Contents

[README 2](#_Toc78316660)

[1.0 Executive Summary 4](#_Toc78316661)

[2.0 Engagement Strategy 5](#_Toc78316662)

[2.1 Organizational Culture 5](#_Toc78316663)

[2.2 Communication and Modalities 5](#_Toc78316664)

[2.3 Reinforcement 6](#_Toc78316665)

[2.4 Branding 6](#_Toc78316666)

[3.0 Metrics 8](#_Toc78316667)

[3.1 Ambassador engagement scores 8](#_Toc78316668)

[3.2 Employee impact scores 8](#_Toc78316669)

[3.3 Ambassador Phishing Click Rate 9](#_Toc78316670)

[4.0 Appendices 10](#_Toc78316671)

[4.1 Learning Objectives 10](#_Toc78316672)

# Executive Summary

Glasworks Inc’s mission is to enable prosperity around the world. We accomplish this mission with a solid passion for solving customer problems with delightful and innovative software solutions. We have a customer obsession that drives us to achieve quick results. These values give us the strength to deliver for our customers. However, for us to truly delight them, we must also protect them.

Glasworks Inc is in the tax software industry, and for us to operate, our customers must trust us with their most sensitive data. As stewards of that data, our workforce must understand the risks we face every day. Many of these risks are technological, where malicious users exploit computer and application vulnerabilities to access systems and data. We have security scans to find and fix application vulnerabilities and strategies to rebuild systems to terminate unauthorized access. These controls mitigate and lower the technological risks we face. However, there is a human element to the dangers we face.

Humans are imperfect creatures and are very capable of making mistakes. The 2020 Verizon DBIR report shows accidental errors caused 22% of breaches. These errors include misconfigurations of computer systems, failure to patch application and server vulnerabilities, and accidentally sending data to the wrong recipients. Another 22% of breaches involved social engineering attacks. These attacks are psychological and are designed to trick targets into exposing sensitive information or facilitating the theft of data or money. In the end, the analysis shows that human risk contributed to over 60% of breaches. This data indicates that humans are the primary attack vector attackers are targeting today.

The security ambassador program is a security awareness plan that will empower a passionate and diverse group of employees to champion security throughout the company. The program goals are to provide training and resources to the ambassadors, build a security-minded community, and act as an advisory board to the security team.

Our success depends on our ability to deliver our services securely and at speed. The data we deal with requires us to comply with numerous regulatory constraints such as GDPR, PCI, and DOD STIGS. In a breach or data exposure, these regulatory rules require quick responses and time-consuming actions to resolve and notify affected customers. Time spent dealing with these incidents is time lost providing customer benefit. The damage to our brand can be catastrophic and put our business at risk.

The security ambassador program is a cost-effective and efficient tool to address human risk. The program allows us to scale our security program at a low cost. Security best practices will likely have a higher adoption rate as each business unit is more likely to listen to its peers. Security-related questions will be answered quickly through the ambassador community to help improve productivity and avoid delays trying to find time to speak with a security team member. The ambassadors will also advise and educate the security team to better understand the business’s needs.

This program will have a measurable result. Metrics collected will show the impact of the strategies taken, show where we need to adjust our tactics, and ensure we gain the best return on our investment. This way, we can ensure our customer data is protected and empower prosperity around the world.

# Engagement Strategy

The ambassador program’s objective is to build up the security knowledge of a group of passionate employees and enable them to guide and advise their peers to identify, respond, and reduce security risks. To achieve this goal, we will create a security ambassador role. This volunteer role will have a 2-4 hour monthly commitment to participate in training and seminars and build our security community and culture. This role will be publicized within the company and have exposure with senior leadership to help market the position to employees with interest in the role.

The ambassador role will be a one-year commitment and will have the following responsibilities:

* Act as a point-of-contact for security for their team.
* Attend monthly security all-hands meetings to get updates on the latest security incidents, news, programs, events, and also interact with other Ambassadors.
* Present a topic in the all-hands meeting and coordinate lunch-n-learn training sessions.
* Develop and refresh Computer Based Training videos for the business.
* Build a security community by collaborating and sharing ideas, concerns, and stories.
* Participate in security awareness campaigns, events, and polls.

## Organizational Culture

As a company in the technology industry, Glasworks Inc’s culture is very outgoing. The business supports fun activities and events. Foosball tables and ping pong tables are frequently in use throughout the day. The on-premise workout gym hosts sand volleyball tournaments that promote teamwork and competition. This friendly and fun personal culture reflects the business’s mission as well, where we go out and find ways to compete and enable prosperity worldwide.

The majority of our offices reside in the United States, but we have a presence in Europe, Asia, and Australia. The regional diversity will create challenges in localizing training materials and seminars. Communications and workshops will need to consider the time zone differences in these overseas sites and ensure they are engaged and supported in the ambassador program. Partnership with the communication team and having localized leadership support in these work sites is critical for the program’s success.

Marketing is another requirement for this program. Glasworks Inc has a strong value to support the work/life balance for its employees. Content for this program aims to help our ambassadors’ work and home life. Using the marketing model of AIDA, we will draw in our employee’s attention by selecting topics that work for both work and home life by showing why threats like phishing and malware are dangerous to both our company and our families.

The outgoing culture will drive for more fun and interactive modalities. Games and contests will allow teams to participate and collaborate to solve for learning objectives as a community. The program’s goal is to drive engagement and interest by factoring our culture into our training modalities.

## Communication and Modalities

**Ambassador All-Hands Meeting**

Educating and training the ambassadors is facilitated through a monthly ambassador all-hands meeting. These meetings are available for live and virtual attendance by ambassadors. The sessions will cover current security topics through instructor lead training or presentations. Ambassadors will be called upon to present topics of interest and suggest topics for future meetings. Educational games and competitions will help drive interest and engagement.

**CBT Training Videos**

The ambassador program will help promote and drive learning objectives through new computer-based training (CBT) videos. The CBT videos will be less than three-minute shorts and focused on security topics identified by the ambassador community to reinforce the required behaviors our employees need to adopt. The videos will also help drive performance improvements. Employees with questions and concerns can reference these training videos rather than reaching out to the security team. The repository of quick answer videos will help unblock teams quickly by removing bottlenecks.

**Tech Talks**

Each month the ambassador community can host a tech-talk for the company to cover current topics in security. Tech Talks will focus each month on a trending topic in cybersecurity. These lunch-n-learn type presentations are tailored with the same work/life balance model to show why these topics are important and how these presentations can help the business and your home life. Each tech talk will focus on a learning objective to help with positive behavioral changes.

## Reinforcement

Glasworks Inc has a security awareness foundations program already implemented. The learning objectives and goals of that program will be inputs into the topics touched on by the ambassador program and will serve as reinforcement training for the ambassadors. Those lessons will flow through into the CBT shorts, and tech talks the ambassador program will produce to help keep the peers up to speed on security.

## Branding

Glasworks Inc has a central security team called Cybercraft and its logo. This brand and logo carry a strong security theme with it and will serve as a foundational brand for the ambassador program. The existing logo will allow the ambassador program to leverage existing marketing materials and networks already set up for the Cybercraft brand to promote the events the program is driving.

The ambassador program will introduce two brand-building characters for use in its meetings, videos, and tech talks:

**Firewally**



Firewally is a security expert that takes the form of a cartoon firewall. Firewally will serve as the protagonist in the stories and examples meant to demonstrate positive behaviors the ambassador program develops. He will be a family-friendly character and will have a fun and humorous personality to help engage employees and their families in our outgoing culture.

**DarkHat’er**

Logo

Description automatically generated

DarkHat’er (pronounced dark-hat-er) is a cybercriminal that takes the form of a dark-colored hat with a sinister face. DarkHat’er takes on the role of the antagonist and is Firewally’s nemesis. He will act as an adversary to Firewally in the training stories and examples. DarkHat’er will highlight the risks that the business and our home lives face and demonstrate the painful consequences of leaving those risks unchecked.

# Metrics

The ambassador program will influence and target both ambassadors and their peers with new information and training. Measurements are required to determine the program’s overall effectiveness in reducing risk to the business.

Glasworks Inc’s central security organization already tracks mandatory compliance data for the company. This data will be helpful to use year over year to determine company-wide impact, but more direct metrics will need to be tracked in higher frequency than currently done with compliance metrics for the scope of this program.

Listed below are the impact metrics we will be collecting.

## Ambassador engagement scores

**Metric**: Ambassador’s interest and participation levels abstracted into an engagement score.

**Why It is Measured**: Participation and interest are crucial for ambassadors to build a strong community and influence change in the organization. Lower scores will reveal stagnant ambassadors. Engagement scores over time will show overall effectiveness and areas to be improved.

**Collection Method**: Ambassadors and the program lead will complete surveys regarding their feedback, interest, and participation in the program. Survey results will calculate into an engagement score. The score will be from 0 to 100, with higher scores showing higher interest and participation.

**Collection Frequency**: The information will be collected quarterly and evaluated over time.

## Employee impact scores

**Metric**: Employee improvement levels abstracted into an impact score.

**Why It is Measured**: Program effectiveness is determined by workforce behavioral changes. Measuring factors that determine program impact will show if the program is effective or needs adjustments.

**Collection Method**: Employees will fill out quarterly surveys. Surveys will quiz employees on learning objectives from past training, productivity improvements or decreases, and employee feedback regarding ambassadors. Survey results will calculate into an engagement score. The score will be from 0 to 100, with higher scores showing higher interest and participation.

**Collection Frequency**: The information will be collected quarterly and evaluated over time.

## Ambassador Phishing Click Rate

**Metric**: Number of ambassadors who fall victim to phishing simulations by clicking on links or opening attachments.

**Why It is Measured:** Ambassadors are champions of security for their teams. Their security awareness needs to be tracked in more detail to determine if they adopt the required behavioral changes.

**Collection Method**: Glasworks Inc’s central security team hosts periodic phishing simulations and stores results. Ambassadors in the program will be added as a new tracking data point.

**Collection Frequency**: The phishing simulations are automated and done every month to subsets of the workforce.

# Appendices

## Learning Objectives

The security ambassador program will provide educational content for its ambassadors to learn from and take away to help spread those lessons to their peers. Much of the content will be informative, but when the program has content meant to drive a behavioral change, a learning objective will be associated. Learning objectives document desired behaviors and knowledge the recipients need to know. Objectives define specific capabilities learners should have after completing the training.

**Title**: Data Security

**Target Audience**: Security Ambassadors, all employees.

**Goal**: Data classification and handling is a company security policy at Glasworks Inc. Employees need to know the differences in public, restricted, sensitive, highly sensitive, and secret data classifications. Employees need to know secure access methods to handle, transmit, store, and destroy data based on its classification.

**Background**: Software developers, customer support agents, and security guards all have access to data. This data is critical to the companies mission, and there is a mandate to protect data from loss, left, or unauthorized alteration. Governmental regulations have strict controls on how data is accessed and handled, and our policies reflect these requirements. Failure to comply with these regulations can cause significant penalties and damage to the company brand.

**Applicable Human Risk**: All employees.

**Learning Objective 1**: Employees can identify the data classifications of Public, Restricted, Sensitive, Highly Sensitive, and Secret.

* *Individual Metric*: The ambassador program will offer certification on data classification to ambassadors and track individual certificates.
* *Organizational Metric*: Updates to the annual CBT security training will document each business unit and organization’s data classification quiz scores.

**Learning Objective 2**: Employees will know what Glasworks Inc approved tools are authorized to access data classified as sensitive or above.

* *Individual Metric*: Workstation and audit log scans will identify and document what tools are used to access company data stores.
* *Organizational Metric*: Percentage of authorized tool use vs. unauthorized tool use summarized by each organization.

**Learning Objective 3**: Employees will know to use multifactor authentication and ensure they do not share credentials.

* *Individual Metric*: Each employee’s onboard status to the corporate MFA and single sign-on framework will be tracked.
* *Organizational Metric*: Percentage of employees onboarded to the corporate MFA and single sign-on framework summarized by each organization.