Informational Report

Informational Report on Genres within a Tech-Based Security Firm

Anderson Lake

Executive Summary

On [omitted] Dr. [omitted] asked for proposals for informational reports on potential post-college careers. The project was to examine the genres used in the field of our choosing. I choose to focus on the genres used by those in the tech-based security field. The proposal for the project was accepted on [omitted]. Work and research began on [omitted].

The following document is the final deliverable for the requested project.

The document first describes the purpose of doing the informational report. The purpose of the document is to give readers a comprehensive look at the genres used at a tech-based security firm. I then detail the methods of obtaining the genres for the report. I first researched local (within a 2-hour drive) tech-based security firms. I found [omitted], a security firm, located in [omitted]. I contacted [omitted] within the company. Mr. [omitted] emailed me 25 documents used in his field; each fell within the category of five genres.

The five genres analyzed were: Acceptable Use Policies, Evaluations, Notifications, Disaster Recovery, and Document Writing. The document then details the analysis of each genre. Each analysis shows the purpose of the document, how the style fulfills the purpose, and how the style is used by its audience. Each analysis comes with a bulleted list of what techniques are used in the documents.

The next section of the document is the results from my research of the genres. I detail how the documents fulfill their purpose, and reach their target audience. I determined that the documents allow the security company to grab the attention of their client, while at the same time making the client feel like the security company is part of the business, and not outsourced help.

The document then concludes with how well these documents work in serving their purpose. This section takes the information and results and determines whether or not these genres are effective tools for communication in the tech-based security field.

A list of references to the documents used, and an appendix that provides example documents, is provided at the end of the document. [Section omitted for security purposes]

Purpose of the Report

The purpose of this project is to be an informational report on a technical writing position for a tech-based security firm. This informational report is important for anyone interested in knowing more about working for a tech-based security firm, and anyone interested in analyzing the genres used in an expanding job market. This report will examine the genres used in the field of tech-based security writing. These genres include: Acceptable Use Policies, Sector Risk Profiles, the NIST's security for small and mid-sized businesses policy, as well as the NIST's Confidentiality Statement for vendors, a Security Briefing for an emerging threat, and a How-to-Write a Forensics Report instructional.

I conducted this report to examine a field that I was personally interested in. Examining the genres used allow me to get a unique glimpse into the kind of writing used in the field, and test my skills in analyzing and utilizing writing styles. This report will also allow any other readers to examine the genres used in tech security, to help make an informed decision as to whether or not they'd be interested in the field. Using the documents obtained from an actual tech-based security company, we can gain a unique glimpse into the field of tech-based security writing. The three main purposes for these genres are to inform on policies, threats, and to instruct. These documents are the primary documents used by a writer for a tech-based security firm.

Methods of Gathered Information

My secondary research began with a cursory search on Google for tech-based security firms within a two-hour driving radius from the York College campus. This was primarily done for practical purposes on the pretense that I would establish an interview with someone at the

firm. I found [omitted], based in a town outside of [omitted], which deals with the tech security of companies around the area. They deal with large clients such as government agencies, private schools, and local businesses. I then examined its list of employees and found [omitted], whose description included “avid writer.” His position in the company, and apparent interest in writing, told me that he would be the perfect contact for the informational report.

For primary research, I contacted [omitted] on [omitted] to establish an interview date, and also requested documents from the field of tech-based security writing. While the interview was conducted via phone at a later date, I was sent the documents on [omitted]. I received seven acceptable use guidelines, a business sector risk profile, an emerging threat security update, five NIST documents, and a link to a how to manual for writing an informational report.

Genre Analysis

Rules and Regulations

These documents are used to inform companies and users what they are allowed to do while using their system.

Acceptable Use Policies

The first set of documents is called “acceptable use policies.” These documents are created to define what users and systems are permitted to do, and what they are prohibited from doing, on their networks. These documents allow the client to have clear guidelines on what is and isn’t acceptable to do on their systems ([omitted] Interview).

These documents range in size depending on the complexity of the company and the system. For example an acceptable use policy for a municipal utilities company (Appendix 1.a) is only 2 pages, but the acceptable use policy for a University (Appendix 1.b) is 21 pages.

Despite the varying lengths, these documents all use similar design elements. These elements help the document easier to read and navigate, because the companies and people who would read these documents would more than likely be reading a specific section of the document when they have a question, and not front to back.

Some of these design elements are:

- Bold and Underlined Headings
- Bold sub-headings
- A table of contents or organizational chart (for longer policies)
- Page Numbers in this format: 4 of 22
- A running header that gives the documents title
- Links (in some cases) for references to organizations and examples of acceptable uses

Risk Profiles

These documents are used by the firm to either evaluate a threat to a company, or to notify companies of possible threats. These documents also examine how these companies can prevent, or repair, these threats.

Evaluations

This is a general Business Sector Risk profile. It's a general overview of the security risk for a specific business sector. This document provides a full evaluation of the potential risks to a

client’s business or organization. It details specific threats and security concerns that the security firm has for their new client. This document is essential for the security company to give to a new client ([omitted] Interview).

These documents are relatively short averaging around 4-5 pages. These evaluations are kept short because they need to be accessible to the client, and a document that is too long would likely keep the client from reading the entire document, despite the need to do so.

Certain styles are used to further the readability of the document. Bold and underlined headings help introduce the client to new sections. Sub headings are a smaller font than the headings, but are larger than the main text, and are neither in bold nor are underlined. Bulleted lists are used to emphasize certain points in the document like specific risks to a system and a list of policies that might aid the company.

Some of these design elements are:

- Bold and Underlined Headings
- Medium font for subheadings
- Bulleted lists for emphasis
- Paragraph breaks to give readers a break

Security Briefing

The next set of documents used in Risk Profiles is a security briefing. These documents, often sent by email, are alerts sent to customers to warn them about emerging threats. These emerging threats range in nature from malicious viruses to hardware malfunctions. These

documents provide detailed information on what the threat is, how the threat works, how to prevent the threat, how to begin recovery if the threat is already present, and a brief overview of what the threat can do to the client ([omitted] Interview).

These documents are sent via email, but are relatively short, fitting on about 2 pages. This length is necessary because the document needs to be concise, so that clients can act immediately to the threat with all the information they need. If the document was too long the client might not be able to react to the threat quickly enough, and if the document was too short the client would likely not have all the information needed to be informed about the threat (Appendix 2.a).

Bold headings are used to highlight important sections. A list of preventive measures and affected systems are often provided. Contact information is given so that a client can easily get in touch with the security company. Graphics are a very large part of these documents. These images allow the client to see exactly what they'd see, rather than the text just describing it to them.

Some of these design elements are:

- Summary, preventative measures, solutions, and an overview of the threat
- Bold headings
- Bulleted lists
- Emailed document that translates to 2-3 pages
- Graphics to illustrate visual cues detailed in the email
- Links for more information and contact information

Instructional

These documents serve to educate clients or those within the security firm. They can teach a company how to prevent or recover from a threat.

Disaster Recovery

The first set of documents in the Instructional category is Disaster Recovery instructions. These documents detail how to recover a certain program or system after disaster. This is often to solve a problem caused by a virus or system shutdown ([omitted] Interview).

These documents range in size from 20 to 30 pages. The reason for this size is because of the comprehensive information included inside the document. The documents first summarize what the threat was, what it did to a system, and then provides step-by-step instructions for how to recover from the disaster.

Despite the length of the document, it provides a lot of information for the client. This document is only needed if the client suffers a disaster, at which point the client would then need a detailed list of what to do to recover. Making the document shorter would ultimately be detrimental to the client.

Some of these design elements are:

- Title Page, Brief overview of threat, and detailed list for recover
- Lists are often in a I, A, I, a, II, A, ii, a, format
- A table of contents or organizational chart
- Bulleted lists for detailed information, and easy to follow instructions

- A running header that gives the documents title
- Links to documents with specific details about parts and systems not needed for recovery

Results of Research

The result of my research shows that professionalism and organization are the two main factors that go into every genre written in the field. Every document is organized in separate lists and often used bulleted lists to draw the attention of the intended audience. Section headings are bold to help readers identify key sections, or sections that they are interested most in reading. This style of writing lends itself to the corporate structure, and shows that even though the tech-security firm is an outside organization, it still acts like a part of the companies it works for. This synergy is due, in part, that the firm must work as an entity within the organization to protect its data and files.

By examining these documents, determining the operations and techniques of the organization are easy. The firm works with many different clients, but must treat every client as though it were the only client the firm works for. This inter-organizational writing style assures the client that the firm is working for them, and is there to serve that client's needs. This also allows the security firm to persuade the client into reading every document sent by the firm, because they establish themselves as a necessary part of the organization.

Conclusions

These documents show the importance of a security firm to a company. The Security firm is essential in helping the company run smoothly, and recovering from disasters. The Security firm must notify the client, and must do so in a manner that does not waste the client's time, but

also give them comprehensive information. These documents allow the client to think that the security firm works for them to improve their life and well-being. The genres used in the security firm need to be comprehensive, yet concise. This is done by proper formatting, and only after analyzing the audience of the document. While a lot of the documents are similar in design and style, subtle differences show how each documents was written with a specific audience in mind. Audience is the main focus of a tech-based security firm's genres, and each document shows this.

[References and Appendices removed for security purposes]