An Assessment of AT&T's Information Security Policies and Enforcement

Key Contributors:
Michael Garcia
Daniel Garza
Abdul Alqarni

UNIVERSITY OF THE
INCARNATE WORD®

28 November 2022

Table of Contents

Executive Summary

AT&T created a Chief Security Office (CSO) to handle the creation and enforcement of security policy within the company and its subsidiaries. The CSO developed a document called AT&T Security Policy and Requirements (ASPR) that outlines secure information handling. This document closely resembles ISO/IEC 27001 and is closely monitored for possible updates. AT&T monitors this through the Global Technology Operations Center which operates 24/7 to provide near-real time data regarding the state of the company's operations. With regards to its public facing domains, AT&T encourages outside assistance through the use of the bug bounty program. This program utilizes the HackerOne platform and is very meticulous when determining how critical a bug discovered is. The company incentivizes bounty hunters by providing rewards up to $2000 dollars for critical demonstrable vulnerabilities.

While the company has a commendable cybersecurity infrastructure, it still suffers from its fair share of data breaches. They have suffered from two confirmed major breaches, one taking place in 2010 and the other discovered in 2015 (occurred in 2013 & 2014). The first breach exposed the email addresses of 114,000 3G iPad customers, while the second one resulted in the names and social security numbers of 290,000 customers leaked to third-parties. There is currently a third speculated breach of about 70 million customer records, which are being sold on the dark web. AT&T has denied the data belongs to them, but refused to elaborate on a potential source. From each of these breaches, AT&T has modified their policy (most notably from their 2015 breach) to prevent future incidents of a similar nature.

In this report, we examine how AT&T adheres to their information security policy as stated in their public-facing website, in conjunction with an outline of their modified information security management procedures as a result of major data breaches throughout the company's history. Additionally, we audit AT&T's compliance in laws and ethics in contrast with the established norms of the information technology industry, and how they have evolved to conform to rising threats.

Report Overview

Milestones:

1. Establish a separation of duties and create deadlines.
2. Conduct research about AT&T’s public-facing security policies.
3. Investigate reported issues they’ve had with data breaches.
4. Analyze and outline AT&T’s compliance with laws and ethics.
5. Evaluate the completeness and quality of the report before delivery.

Deliverables:

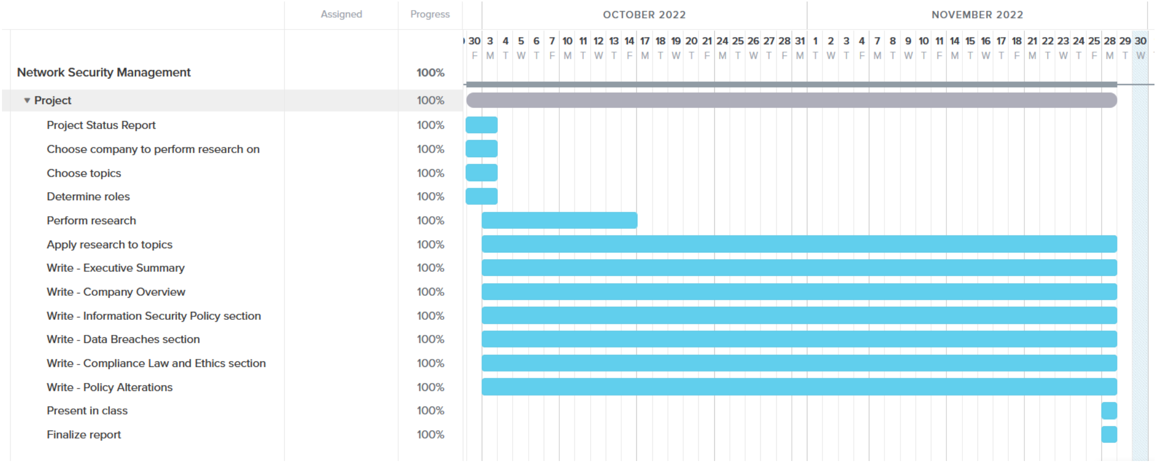
1. Status Report
2. Finalized Report
3. Presentation

Professional Accomplishments:

1. Learned about best practices regarding data security within an organization.
2. Proved the importance of strict compliance to policies and regulations for companies that handle PII.
3. Observed how companies respond to breaches via policy modification.

Report Schedule Management

Gantt Chart:



	Assigned	Progress
Network Security Management		100%
▾ Project		100%
Project Status Report		100%
Choose company to perform research on		100%
Choose topics		100%
Determine roles		100%
Perform research		100%
Apply research to topics		100%
Write - Executive Summary		100%
Write - Company Overview		100%
Write - Information Security Policy section		100%
Write - Data Breaches section		100%
Write - Compliance Law and Ethics section		100%
Write - Policy Alterations		100%
Present in class		100%
Finalize report		100%

Management Board:
https://trello.com/invite/nsmgarzaf22/019b1dcc9651e502c9cae8d493e21cf0

Github Repository:
https://github.com/dsgarza/NSM-GARZA-F22

Company Overview

Mission

“Our culture means more to us than our job titles. Together we share in something greater, do incredible things and live out our values”

Purpose

“Connecting people to greater possibility - with expertise, simplicity, and inspiration”

Values

Live true. Think big. Pursue excellence. Be there. Stand for equality. Make a difference.

C-Suite Officers

Chief Executive Officer - John Stankey
Chief Strategy and Development Officer - Thaddeus Arroyo
Senior Executive Vice President, Chief Financial Officer - Pascal Desroches
Senior Executive Vice President, External Affairs - Ed Gillespie
Senior Executive Vice President, Chief Compliance Officer - David S. Huntley
Chief Marketing and Growth Officer - Kellyn Smith Kenny
Chief Executive Officer AT&T Latin America, Global Marketing Officer - Lori Lee
Chief Technology Officer - Jeremy Legg
Senior Executive Vice President - David R. McAtee II
Chief Operating Officer - Jeff McElfresh
Senior Executive Vice President, Human Resources - Angela Santone

Company Origins

Originally founded in the late nineteenth century as Bell Telephone Company, AT&T has been in some form of business for over one hundred years. The company gained its current name following a monopoly breakup in 1982. It was then bought by SBC in 2005, which retained the largely recognized name of AT&T. This has laid the foundations for AT&T as the world knows it today (“History of AT&T Brands”,2022).

Information Security Policy

Chief Security Office

As one of the world's most trusted communications providers for over 140 years, American Telephone and Telegraph (AT&T) treats information security with the utmost importance. AT&T's Chief Security Office (CSO) handles the creation, enforcement, and distribution of information security policy within the company.

Security Standards

AT&T uses a document called the AT&T Security Policy and Requirements (ASPR) as a foundation for ensuring that security is considered in every aspect of business. The format of ASPR is inspired by that of ISO/IEC 27001. Thus the document is focused on providing the basis of security innovation within the company. Additionally, the company is compliant with National Institute of Standards and Technology (NIST) Cybersecurity Framework and NIST 800-53 and the European Union's General Data Protection Regulation (GDPR), Criminal Justice Information Services (CJIS) Security Policy, and California Consumer Privacy Act (CCPA). The company completes annual audits including the Payment Card Industry (PCI) Data Security Standard, the Sarbanes-Oxley Act (SOX), SSAE 18/ISAE 3402 (SOC) and the Quality Management Standard (ISO 9001).

Strategy

The CSO created AT&T Security Center for Innovation in order to address growing concerns regarding employee and customer cyber security. Employees within this department focus on researching new threat areas as they arise. Such threat areas include "mobility and cellular/5G, cloud computing, networking, virtualization, Internet of Things, blockchain and artificial intelligence/deep learning/machine learning" ("AT&T Issue Brief", 2022). The findings of these studies influence additions to AT&T's security standards and enforcement.

The Security Center for Innovation also manages a blog on AT&T's website called "Cyber Aware". This space serves to provide an area for employees and customers alike to find answers to their most common surrounding cyber security. Some of their most popular articles include titles such as "eSIM: Coming Soon to a Phone Near You" and "Who Are You? A Brief Guide to Online Authentication". Additionally, there is a continuously updated security quiz called the "Cyber Aware Quiz". This quiz mainly covers authentication security, but has some questions covering the handling of smishing messages and email security. For those less initiated in the cyber world, the blog also hosts a vocabulary quiz of sorts under the "Understanding Terms and Technology" article. This quiz provides an introduction to the jargon used across the website, a quiz to determine one's knowledge, and a list of definitions put in "simple terms" to ensure that security awareness is accessible to anyone.

Penetration Testing

AT&T regularly tests their security to ensure proper compliance and standards. This process includes security status checks that involve determining general system security settings, proper resource allotment, and proper division of authority between administrators and users. To ensure confidential information stays within the company, additional vulnerability testing is only performed by internal personnel. These scans include commonplace scanning tools as well as proprietary AT&T developed tools to determine any risk of unauthorized access. Vulnerabilities found in these investigations are then ordered in terms of severity and analyzed to determine who they impact and how they can be remediated

The company also operates the AT&T Global Technology Operations Center. This department provides 24/7 monitoring of AT&T's network. This monitoring includes analysis and hunting of the anomaly ("AT&T Issue Brief", 2022).

Figure 1.1 - *A look inside AT&T's Global Technology Operations Center.*

AT&T allows help from its customers through the AT&T Bug Bounty program utilizing the HackerOne platform. Each bug found by the hunters must meet the following qualifications:

- Directly or indirectly affect the confidentiality or integrity of user data or privacy
- Compromise the integrity of the system
- Enable unauthorized access to significant data or resources
- Enable the running of unauthorized code
- Increase privileges or access beyond that which is intended
- Interfere with or bypass security controls or mechanisms
- Are exploitable (i.e. not purely theoretical)
- Can be launched remotely

- Could cause damage to a user's system

Reported bugs must not fall into any of the following categories:

- Attacks against AT&T infrastructure
- Social engineering and physical attacks
- Distributed Denial of Service attacks that require large volumes of data
- 0-day vulnerabilities less than 30/60/90 days from patch release are ineligible for bounty
- Provisioning and/or usability issues
- Violations of licenses or other restrictions applicable to any vendor's product
- Security vulnerabilities in third-party products or websites that are not under AT&T’s direct control
- Duplicate reports of security issues, including security issues that have already been identified internally
- Tenant/cloud systems executing in an Internet Data Center (IDC), where AT&T is simply acting as the site host

Should the reported bugs meet all of the requirements listed above, bounty hunters may receive rewards up to $2000 for their efforts (“AT&T Bug Bounty”, 2022).

Data Breaches

AT&T's Documentation

According to AT&T's own site documentation regarding data breaches from 2017, it identifies an upward trend of third-party sources revealing information to a company and leading to the discovery of a breach, rather than a company's own internal IT systems detecting one. A survey taken from global executives for one of AT&T's Cybersecurity Insights reports concerning breach notifications revealed that when it comes to who detects a data breach first, the breakdown was as follows (Cooper, 2017):

Employees: 50%
Law enforcement: 25%
Customers: 21%
Service providers: 19%

Currently, in AT&T's 2022 Cybersecurity Insights Report, it identifies ransomware as a major threat regarding data breaches. A survey was conducted where respondents were asked, "In your opinion, how likely are the following attack vectors?" with a list of options to choose from different industries, in which ransomware scored the highest overall ("AT&T Cybersecurity Insights Report", 2022). As seen in the next section, AT&T's previous data breaches were the result of data mishandling and operational vulnerabilities, not ransomware.

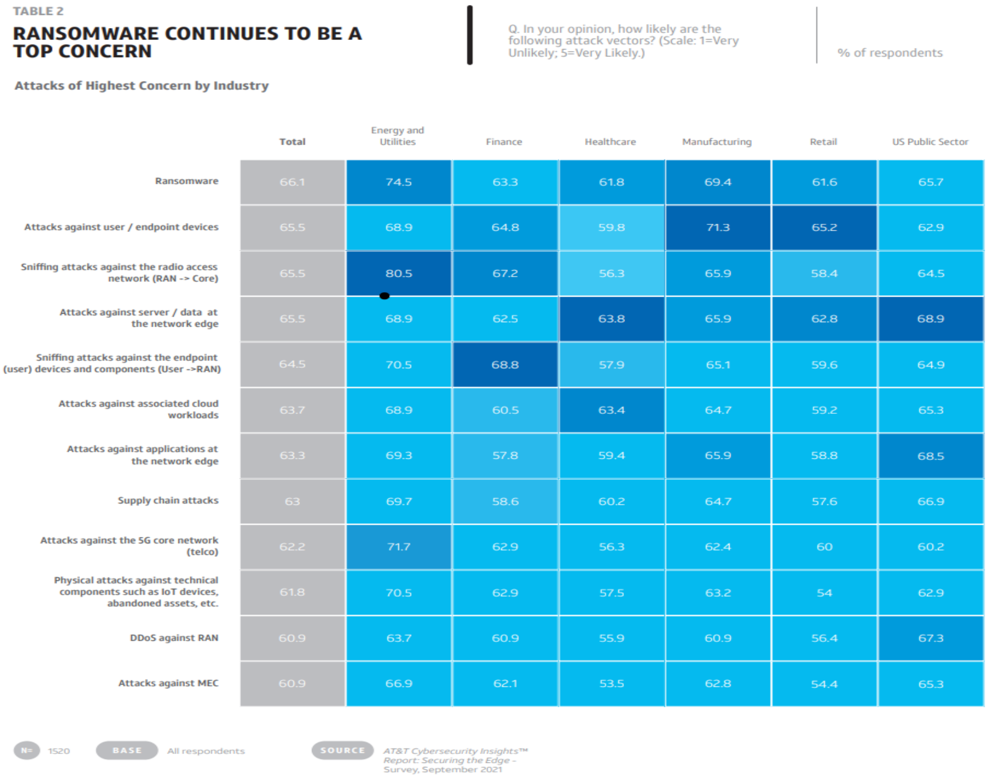


TABLE 2

RANSOMWARE CONTINUES TO BE A TOP CONCERN

Q. In your opinion, how likely are the following attack vectors? (Scale: 1=Very Unlikely; 5=Very Likely.)

% of respondents

Attacks of Highest Concern by Industry

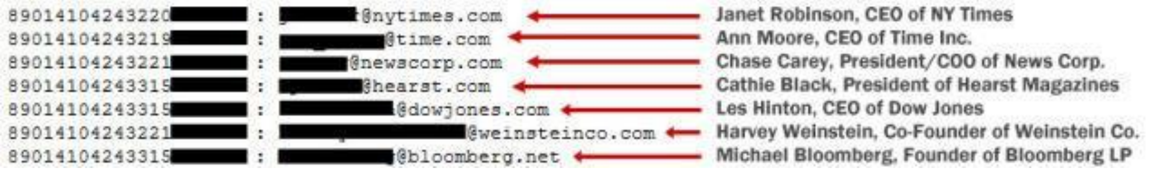
	Total	Energy and Utilities	Finance	Healthcare	Manufacturing	Retail	US Public Sector
Ransomware	66.1	74.5	63.3	61.8	69.4	61.6	65.7
Attacks against user / endpoint devices	65.5	68.9	64.8	59.8	71.3	65.2	62.9
Sniffing attacks against the radio access network (RAN -> Core)	65.5	80.5	67.2	56.3	65.9	58.4	64.5
Attacks against server / data at the network edge	65.5	68.9	62.5	63.8	65.9	62.8	68.9
Sniffing attacks against the endpoint (user) devices and components (User ->RAN)	64.5	70.5	68.8	57.9	65.1	59.6	64.9
Attacks against associated cloud workloads	63.7	68.9	60.5	63.4	64.7	59.2	65.3
Attacks against applications at the network edge	63.3	69.3	57.8	59.4	65.9	58.8	68.5
Supply chain attacks	63	69.7	58.6	60.2	64.7	57.6	66.9
Attacks against the 5G core network (telco)	62.2	71.7	62.9	56.3	62.4	60	60.2
Physical attacks against technical components such as IoT devices, abandoned assets, etc.	61.8	70.5	62.9	57.5	63.2	54	62.9
DDoS against RAN	60.9	63.7	60.9	55.9	60.9	56.4	67.3
Attacks against MEC	60.9	66.9	62.1	53.5	62.8	54.4	65.3

N= 1520 BASE All respondents SOURCE *AT&T Cybersecurity Insights™ Report: Securing the Edge – Survey, September 2021*

Figure 1.2 - *Table showing AT&T's survey results from the report.*

Past Breaches

In 2010, there was a small breach that resulted in about 114,000 email addresses of AT&T iPad owners to be leaked. A hacker group originating from 4chan exploited a security flaw in one of AT&T's customer-identification scripts, which involved organizing a brute-force attack on an entry field for SIM card ICC-ID numbers. These ICC-ID numbers were linked to the private email addresses of said iPad owners, which when entered into the field as part of an HTTP request, then populated with a corresponding email address if the number was valid. By entering semi random ICC-ID numbers using a PHP script, they were able to obtain these email addresses, involving people from Michael Bloomberg to a Mr. Eldredge, who was command for a fleet of B-1 bombers. The hacker group notified AT&T shortly after executing this attack, but not in time for a few third parties who also exploited this vulnerability. While most of these emails may have already been public information, the most sensitive ones are internal email addresses that, if accessed, could leak potentially sensitive information for a company or government organization. AT&T quickly took action and shut down the script behind the feature that produced the email addresses, and sought to inform customers whose information may have been obtained (Tate, 2010) (Coldewey, 2010).



```
89014104243220[redacted] : [redacted]@nytimes.com
89014104243219[redacted] : [redacted]@time.com
89014104243221[redacted] : [redacted]@newscorp.com
89014104243315[redacted] : [redacted]@hearst.com
89014104243315[redacted] : [redacted]@dowjones.com
89014104243221[redacted] : [redacted]@weinsteinco.com
89014104243315[redacted] : [redacted]@bloomberg.net
```

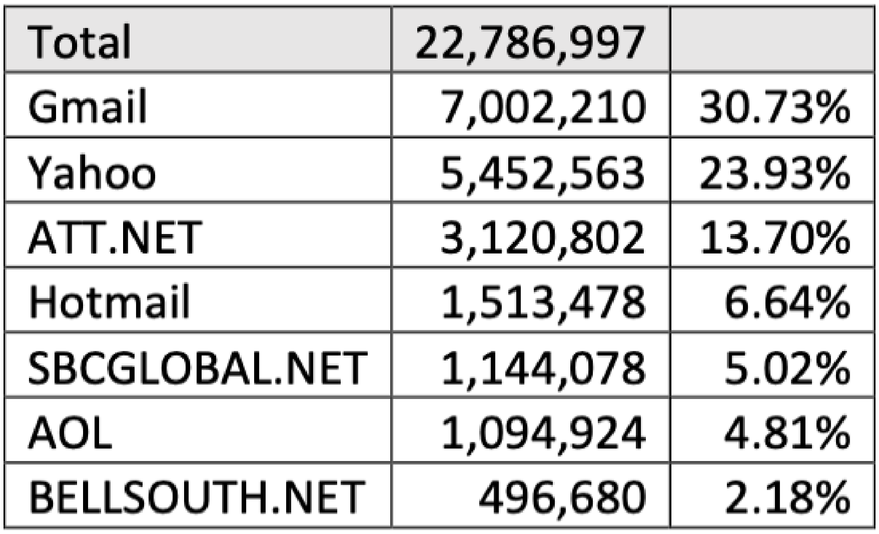
Janet Robinson, CEO of NY Times
Ann Moore, CEO of Time Inc.
Chase Carey, President/COO of News Corp.
Cathie Black, President of Hearst Magazines
Les Hinton, CEO of Dow Jones
Harvey Weinstein, Co-Founder of Weinstein Co.
Michael Bloomberg, Founder of Bloomberg LP

Figure 1.3 - *ICC-ID numbers with identified emails from the breach.*

In 2013 and 2014, two data breaches occurred within AT&T that resulted in about 290,000 customers' names and full or partial social security numbers being exposed. As a result, AT&T paid a $25 million civil penalty to settle an investigation by the Federal Communications Commision in 2015 (Nayak, 2015). The breach originated from call centers based in Mexico, Colombia, and the Philippines. In Mexico, three employees accessed more than 68,000 accounts without proper authorization to submit more than 290,000 AT&T phone unlock requests through the company's online portal, which a third party used to traffic stolen phones from the carrier. It was later in the investigation that the breaches in Colombia and the Philippines, where it was discovered approximately 40 employees had accessed almost 211,000 customer accounts to repeat the same process. As a result of these attacks, AT&T sent out a breach notification to notify all affected customers whose accounts were accessed and provided complimentary credit monitoring services for said customers. They also publicized that they have agreed to improve their security practices and are regularly filing compliance reports to the FCC. Modifications were made to their security policies, and AT&T is selectively terminating a few vendor sites "as appropriate". In a statement, a spokesman for AT&T said, "Protecting customer privacy is critical to us. We hold ourselves and our vendors to a high standard" (Rosenfeld, 2015).

Potential Current Breach

As of 2022, an established threat actor group known as ShinyHunters has made claims that it holds over 70 million customer records from AT&T and has posted the database for sale. This claim comes just days after the group sold data pertaining to T-Mobile customers, which was verified by the company to have been a legitimate data breach. This hacker group is known for attacking a multitude of organizations, which includes Microsoft back in May 2020, where 500GB of data was stolen from private developer GitHub repositories (Moore, 2020). A Milwaukee-based cybersecurity consultancy named Hold Security was able to intercept a 1.6GB compressed file from this breach ”on a popular dark web file-sharing site”. In this data set, patterns were observed that suggest the data relates to AT&T customers, such as email addresses ending in “att.net”, and AT&T subsidiaries such as “SBCGlobal.net” and “Bellsouth.net” (Holden, 2022).



Total	22,786,997	
Gmail	7,002,210	30.73%
Yahoo	5,452,563	23.93%
ATT.NET	3,120,802	13.70%
Hotmail	1,513,478	6.64%
SBCGLOBAL.NET	1,144,078	5.02%
AOL	1,094,924	4.81%
BELLSOUTH.NET	496,680	2.18%

Figure 1.4 - *Result of parsed data and how much of each domain was found.*

AT&T has denied the claims that the data came from their systems and has suggested that the source is either not authentic or from another company. The company said in a written statement that, “This information does not appear to have come from our systems. It may be tied to a previous data incident at another company. It is unfortunate that data can continue to surface over several years on the dark web. However, customers often receive notices after such incidents and advice for ID theft is consistent and can be found online” (Lapienyte, 2022). AT&T refused to elaborate on what they meant by “a previous data incident at another company”.

Compliance - Law & Ethics

Security Policy & Ethic

AT&T takes security very seriously. After it has come across the airlink, your data enters the AT&T network, where we take great care to ensure that data confidentiality and integrity are protected.

To secure data both in transit across the network and stored in the network, AT&T has implemented a comprehensive security program that focuses on 13 major areas. The areas are derived from ISO 17799, COBIT, and other industry best practices.

Human Factors as Part of Security Policy

Taking human factors into account is an important part of the successful deployment and adoption of a wireless security architecture. Security policies can either drive or impede adoption, depending on the circumstance. The more intrusive a security policy is on users, the more they will attempt to circumvent it, which makes policy enforcement even more important.

Chief Security Officer of AT&T

When we want to mention ethic and policies in AT&T, we must start first, by talking about **William O'Hern** the Chief Security Officer, "The AT&T Chief Security Office (CSO) establishes policy and requirements, as well as comprehensive programs, to ensure security is incorporated into every facet of AT&T's computing and networking environments. Our technical personnel work in partnership with other AT&T Business Units and Divisions to evaluate threats, determine protective measures, create response capabilities, and ensure compliance with best security practices."

Chief security officer (CSO) has a big role to play in any organization and here are some of the (CSO) **responsibilities.**

Chief Security Officer Responsibilities:

- Building a comprehensive security program that includes physical safety and cybersecurity policies.
- Reviewing existing security measures and updating protocols as needed.

- Overseeing the daily operations of the company to identify potential security risks and room for improvements.
- Managing, evaluating, and resolving any physical or digital security incidents or breaches.
- Ensuring that the company's security policies comply with federal laws and legislations.
- Presenting risk assessments and improved security policies to management team members.
- Working with management to develop and implement an appropriate budget for security programs.

Training and Compliance in AT&T

The AT&T CSO is charged with directing and coordinating security awareness and education.

"The group maintains an internal security awareness website and newsletter, employee- and department-specific bulletins and communications, job aids, technology conferences, and employee security awareness events to deliver general and targeted security awareness initiatives within AT&T. The program uses subject matter experts from various security groups and disciplines across the business for content development and to deliver webcasts and video productions."

The AT&T internal security awareness program takes an innovative engage-while-learning approach.

"Our program enforces personal responsibility from every person who touches the network – from office workers and server administrators to those in the field and more. Using a series of animated characters to share learnings about security, the storylines ask employees to imagine real-life scenarios that could involve them, such as opening a dangerous link or sending data unencrypted. Our lead animated character – which has become an iconic internal brand – learns awareness lessons on behalf of the employee."

Policy Alterations

The majority of policy modifications done by AT&T came as a result of a settlement of an investigation into the malpractice that occurred with the aforementioned 2015 data breach. Along with a $25 million dollar fine, they were tasked by the Federal Communications Commission to "develop and implement a compliance plan to ensure appropriate processes and procedures are incorporated into AT&T's business practices to protect consumers against similar data breaches in the future." In addition, there were also required to "improve its privacy and data security practices by appointing a senior compliance manager who is privacy certified, conducting a privacy risk assessment, implementing an information security program, preparing an appropriate compliance manual, and regularly training employees on the company's privacy policies and the applicable privacy legal authorities". The tasks were as follows:

- Must complete a risk assessment aimed at identifying internal risks
- Within 90 days, must create, implement, and enforce an information security program specifically geared towards protecting CPNI and Personal Information from unauthorized access
- Must monitor the effectiveness of a new information security program. If it is deemed ineffective, AT&T must implement a new program
- Within 90 days, must complete a Compliance Review
- Within 120 days, Chief Compliance Officer must draft and distribute Compliance Manual to all employees
- Must establish a compliance training program

AT&T was compelled to notify each individual affected by this breach and provide a toll free information hotline focused on questioning the impact of the incident ("AT&T to pay $25m to settle investigation", 2018).

References

AT&T Bug Bounty - Welcome. (n.d.). Retrieved November 28, 2022, from https://bugbounty.att.com/

AT&T Cyber Aware: Fraud Prevention & Cybersecurity Program. AT&T Cyber Aware | Fraud Prevention & Cybersecurity Program. (2019, March 11). Retrieved November 28, 2022, from https://about.att.com/pages/cyberaware

AT&T Cybersecurity insights report 2022. AT&T Business. (n.d.). Retrieved November 28, 2022, from https://www.business.att.com/categories/cybersecurity-insights-report.html

AT&T Issue Brief: Network & Data Security: AT&T Social Responsibility. AT&T News, Wireless and Network Information. (n.d.). Retrieved November 28, 2022, from https://about.att.com/csr/home/reporting/issue-brief/network-data-security.html

AT&T to pay $25m to settle investigation into three data breaches. Federal Communications Commission. (2018, October 10). Retrieved November 28, 2022, from https://www.fcc.gov/document/att-pay-25m-settle-investigation-three-data-breaches

Coldewey, D. (2010, June 10). *AT&T Security Breach Leaks Thousands of iPad owners' emails (but luckily, little else)*. TechCrunch. Retrieved November 28, 2022, from https://techcrunch.com/2010/06/09/att-security-breach-leaks-thousands-of-ipad-owners-emails-but-luckily-nothing-more/

Cooper, C. (2017, August 17). *How cyber attacks & data breaches are discovered*. AT&T Business. Retrieved November 28, 2022, from https://www.business.att.com/learn/research-reports/how-data-breaches-are-discovered.html

History of AT&T Brands: AT&T Intellectual Property. History of AT&T Brands | AT&T. (2016, October 5). Retrieved November 28, 2022, from https://about.att.com/innovation/ip/brands/history

Holden, A. (2022, August 11). *It might be our data, but it's not our breach*. Krebs on Security. Retrieved November 28, 2022, from https://krebsonsecurity.com/2022/08/it-might-be-our-data-but-its-not-our-breach/

Lapienyte, J. (2022, April 12). *AT&T database of 70 million users sold on Hacker Forum - Cybernews*. Cybernews. Retrieved November 28, 2022, from https://cybernews.com/news/att-database-of-70-million-users-sold-on-hacker-forum/

Moore, M. (2020, May 8). *Microsoft github account reportedly hit in huge cyberattack*. TechRadar. Retrieved November 28, 2022, from https://www.techradar.com/news/microsoft-github-account-reportedly-hit-in-huge-cyberattack

Nayak, M. (2015, April 8). *U.S. FCC imposes $25 million fine on AT&T over Customer Data Breach*. Reuters. Retrieved November 28, 2022, from https://www.reuters.com/article/us-at-t-settlement-dataprotection/u-s-fcc-imposes-25-million-fine-on-att-over-customer-data-breach-idUSKBN0MZ1XX20150408

Rosenfeld, E. (2015, April 8). *AT&T data breaches revealed: 280K US customers exposed*. CNBC. Retrieved November 28, 2022, from https://www.cnbc.com/2015/04/08/att-data-breaches-revealed-280k-us-customers-exposed.html

Tate, R. (2010, June 9). *Apple's worst security breach: 114,000 iPad owners exposed*. Gawker. Retrieved November 28, 2022, from https://www.gawker.com/5559346/apples-worst-security-breach-114000-ipad-owners-exposed