CISPA
HELMHOLTZ CENTER FOR
INFORMATION SECURITY

Quantifying Security Training in Organizations Through the Analysis of U.S. SEC 10-K Filings

Jonas Hielscher and Maximilian Golla | CISPA, Germany | ACM CCS '25

Motivation

How Are We Doing in Cybersecurity?

Cybersecurity Is Hard to Measure [1,2]

Cybersecurity Vendors Have Other Incentives [3,4]

SAT Is Not Evidence-Based [5]

[1] Anderson et al.: **Measuring the Changing Cost of Cybercrime**. WEIS '19.
[2] Herley and Pieters: **"If you were attacked, you'd be sorry": Counterfactuals as Security Arguments**. ACM NSPW '15.
[3] Anderson and Moore: **The Economics of Information Security**. Science '06.
[4] Hielscher et al.: **Selling Satisfaction: A Qualitative Analysis of Cybersecurity Awareness Vendors' Promises**. ACM CCS '24.
[5] Lain et al.: **Phishing in Organizations: Findings from a Large-Scale and Long-Term Study.** IEEE S&P '22.

 SAT = Security Awareness and Training

From Where Can Reliable Data* on Organizations' Cybersecurity Strategies Be Obtained?

* That Tell the Factual Truth.

U.S. SEC 10-K Filings

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 10-K

☒ ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934
For the fiscal year ended September 28, 2024
or
☐ TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934
For the transition period from ______ to ______.
Commission File Number: **001-36743**

Apple Inc.
(Exact name of Registrant as specified in its charter)

- *Yearly Financial Report*
- *Factual Data*
- *Unstructured Text*
- *Lower Bound*

Source: https://www.sec.gov/Archives/edgar/data/320193/000032019324000123/aapl-20240928.htm

U.S. SEC 10-K Filings

Item 1C *Cybersecurity*

Cybersecurity Risk Management and Strategy

We have developed and implemented a cybersecurity risk management program intended to protect the confidentiality, integrity, and availability of our critical systems and information, including guest and colleague information.

Key elements of our cybersecurity risk management program include:

- Training of our employees in cybersecurity awareness and payment card compliance and additional training for cybersecurity personnel, software developers, and senior management in cybersecurity-related topics including, but not limited to, incident response, secure software development, and training commensurate with job responsibilities;

- *Yearly Financial Report*
- *Factual Data*
- *Unstructured Text*
- *Lower Bound*
- ***New: Item 1C Cybersecurity***

Source: https://www.sec.gov/Archives/edgar/data/1468174/000146817425000009/h-20241231.htm

Research Questions

Research Questions

RQ1: Prevalence

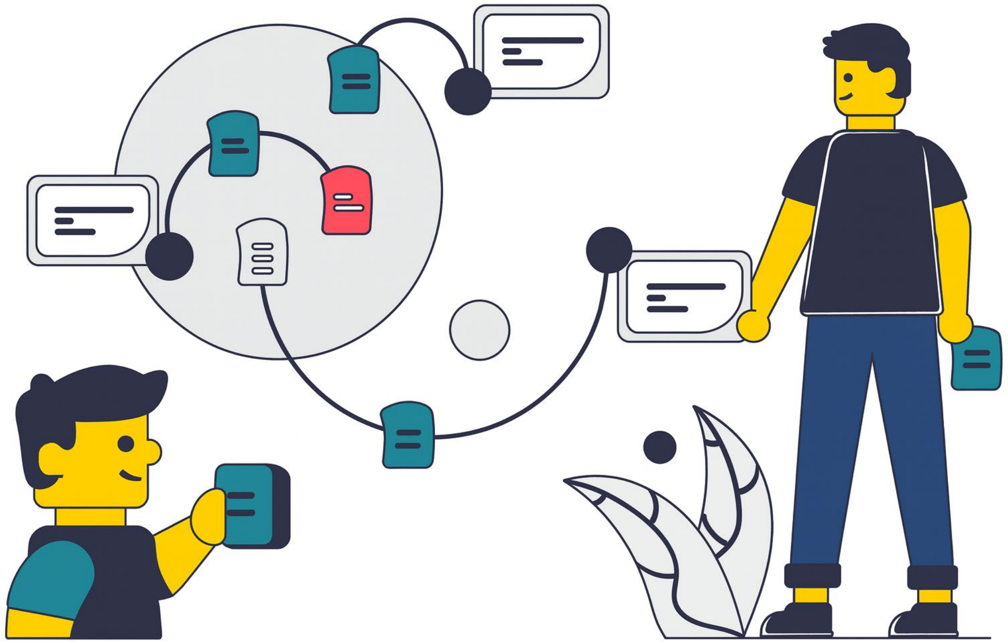
What is the **prevalence of SAT deployment** across organizations of various sizes and industries?

RQ2: Types

What **types of SAT** programs are most commonly implemented, and how are they integrated with other **employee-facing cyber-security** measures?

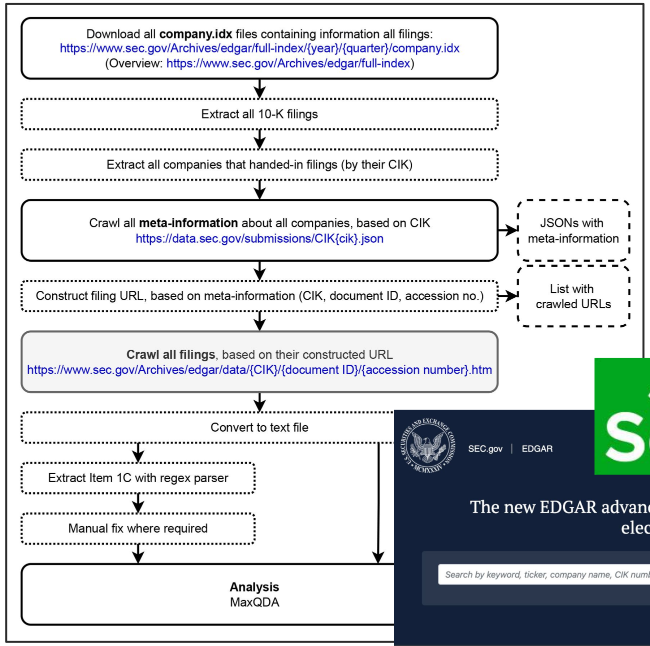
RQ3: Item 1C

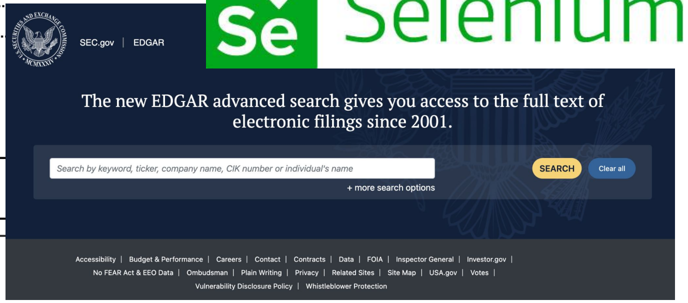
How did **Item 1C's** introduction **change** the **disclosure of human factors**-related cybersecurity risks and SAT strategies?



Method

Crawling Pipeline

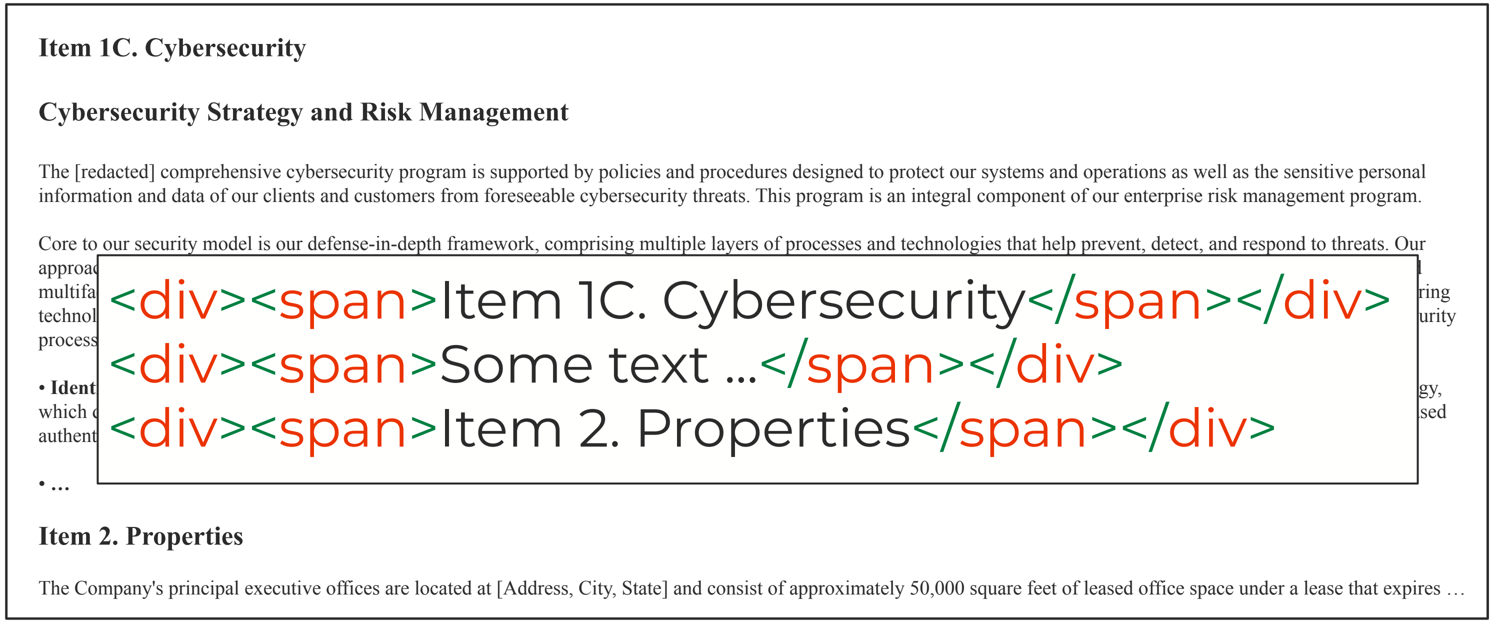




Crawling SEC DB

6,719 Filings

Extracting “Item 1C”



Item 1C. Cybersecurity

Cybersecurity Strategy and Risk Management

The [redacted] comprehensive cybersecurity program is supported by policies and procedures designed to protect our systems and operations as well as the sensitive personal information and data of our clients and customers from foreseeable cybersecurity threats. This program is an integral component of our enterprise risk management program.

Core to our security model is our defense-in-depth framework, comprising multiple layers of processes and technologies that help prevent, detect, and respond to threats. Our approac … multifa … ring technol … urity process …

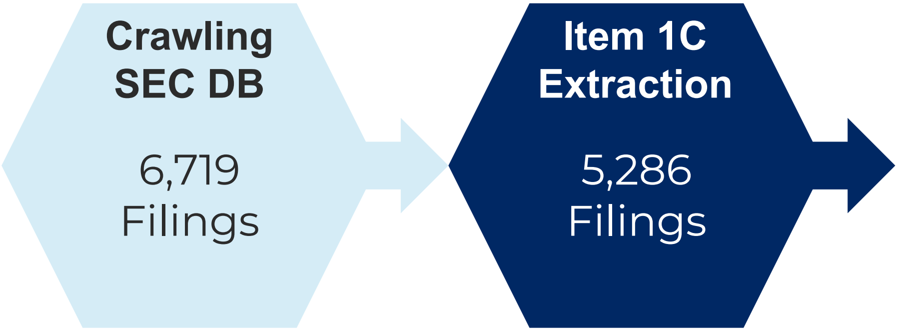
• **Ident** … gy, which … sed authent …

• …

Item 2. Properties

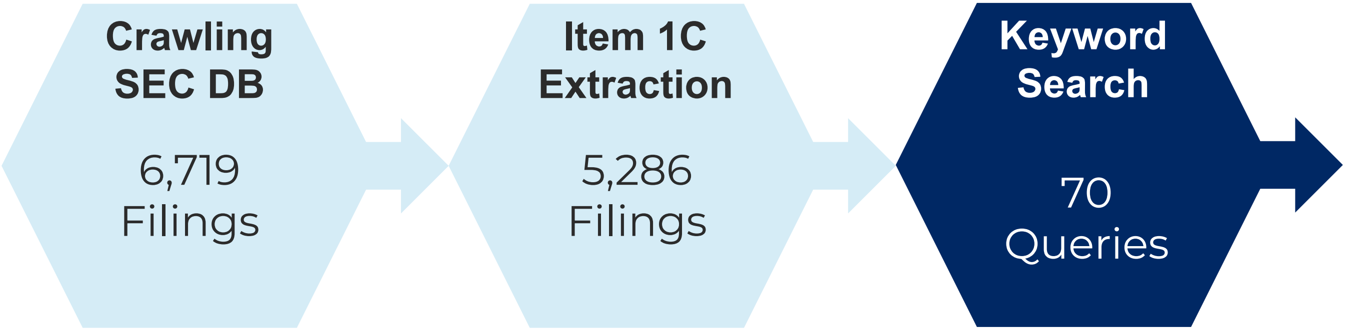
The Company's principal executive offices are located at [Address, City, State] and consist of approximately 50,000 square feet of leased office space under a lease that expires …

<div>Item 1C. Cybersecurity</div>
<div>Some text …</div>
<div>Item 2. Properties</div>



Identifying Keywords

(ALL communication
ANY training, awareness, education
NOT ANY board, executive, chief, committee, ciso, ‘corporate communication’, telecommunication)
WITHIN ONE SENTENCE



Identifying Keywords

Item 1C. CYBERSECURITY

Cybersecurity Strategy and Risk Management

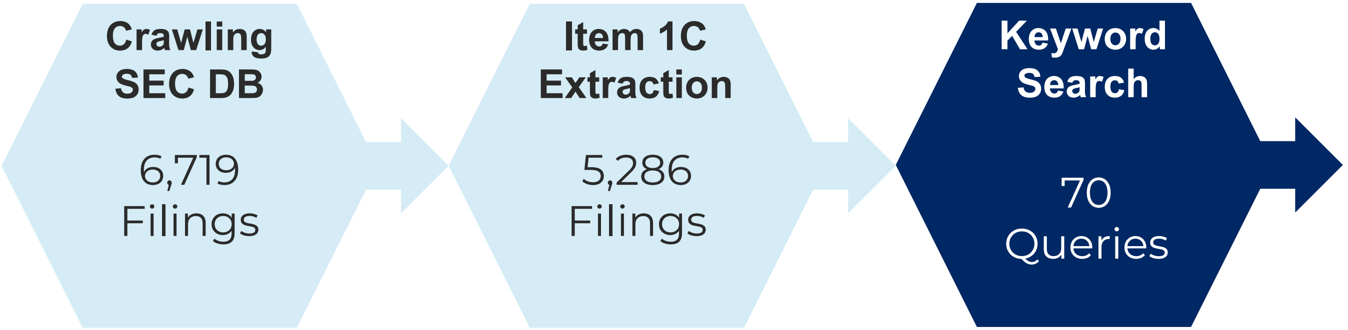
The [redacted] comprehensive cybersecurity program is supported by policies and procedures designed to protect our systems and operations as well as the sensitive personal information and data of our clients and customers from foreseeable cybersecurity threats. This program is an integral component of our enterprise risk management program.

Core to our security model is our defense-in-depth framework, comprising multiple layers of processes and technologies that help prevent, detect, and respond to threats. Our approach to safeguarding against external threats incorporates a suite of preventive technologies, including malicious email blocking, defenses against automated attacks and multifactor authentication. These strategies act to proactively intercept and neutralize cyber threats to help ensure data remains secure within our environment. Event monitoring technologies run continuously, detecting suspected intrusion attempts and alerting our Cybersecurity Incident Response team. [Redacted] undertakes a number of critical security processes to mitigate and protect against cybersecurity risks, which include but are not limited to:

- **Identity and Access Management**. Employees are provided with the minimum amount of access required to perform their jobs using role-based access control methodology, which defines access to our information systems based on job function. Privileged or elevated access to our systems is subject to supplemental approval requirements, increased authentication processes, and additional logging and monitoring.

- **Security Awareness and Training**. Events and education activities are hosted throughout the year, such as the Cybersecurity Awareness Month, expos, videos, training programs and frequent phishing simulations. [Redacted] continuously trains workforce members on the importance of preserving the confidentiality and integrity of customer data.
All new hires have mandatory information protection and privacy training as part of their onboarding, and all workforce members complete an annual cybersecurity refresh training.

- ...



Comparison with Old 10-K Filings

2024

Item 1C. CYBERSECURITY

Cybersecurity Strategy and Risk Management

The [redacted] comprehensive cybersecurity program is supported by policies and procedures designed to protect our systems and operations as well as the sensitive personal information and data of our clients and customers from foreseeable cybersecurity threats. This program is an integral component of our enterprise risk management program.

Core to our security model is our defense-in-depth framework, comprising multiple layers of processes and technologies that help prevent, detect, and respond to threats. Our approach to safeguarding against external threats incorporates a suite of preventive technologies, including malicious email blocking, defenses against automated attacks and multifactor authentication. These strategies act to proactively intercept and neutralize cyber threats to help ensure data remains secure within our environment. Event monitoring technologies run continuously, detecting suspected intrusion attempts and alerting our Cybersecurity Incident Response team. [Redacted] undertakes a number of critical security processes to mitigate and protect against cybersecurity risks, which include but are not limited to:

- **Identity and Access Management**. Employees are provided with the minimum amount of access required to perform their jobs using role-based access control methodology, which defines access to our information systems based on job function. Privileged or elevated access to our systems is subject to supplemental approval requirements, increased authentication processes, and additional logging and monitoring.
- **Security Awareness and Training**. Events and education activities are hosted throughout the year, such as the Cybersecurity Awareness Month, expos, videos, training programs and frequent phishing simulations. [Redacted] continuously trains workforce members on the importance of preserving the confidentiality and integrity of customer data.
All new hires have mandatory information protection and privacy training as part of their onboarding, and all workforce members complete an annual cybersecurity refresh training.
- ...

VS

2023

Item 1A. Risk Factors

Safety and Security Risks

Threats of cyber incidents, physical security, and terrorism could affect the [redacted] business. Technology failures, cyber attacks, privacy breaches or data breaches could disrupt our operations or reputation and negatively impact our business. We increasingly rely on information technology systems and third-party service providers, including through the internet, to process, transmit, and store electronic information.

Our information technology systems, and the systems of the parties we communicate and collaborate with, may be vulnerable to a variety of interruptions, as a result of many of our employees working remotely, updating our enterprise platform or due to events beyond our or their control, including, but not limited to, network or hardware failures, malicious or disruptive software, unintentional or malicious actions of employees or contractors, cyberattacks by common hackers, criminal groups or nation-state organizations or social-activist (hacktivist) organizations, geopolitical events, natural disasters, failures or impairments of telecommunications networks, or other catastrophic events.

Moreover, our computer systems have been, and will likely continue to be subjected to computer viruses, malware, ransomware or other malicious codes, social engineering attacks, unauthorized access attempts, password theft, physical breaches, employee or inside error, malfeasance and cyber- or phishing-attacks. Cyber threats are constantly evolving, are becoming more sophisticated and …

Crawling SEC DB
6,719 Filings

Item 1C Extraction
5,286 Filings

Keyword Search
70 Queries

Comparison with 2023
5,021 Filings

Comparison with Size and Sector

Item 1C. CYBERSECURITY

Cybersecurity Strategy and Risk Management

The [redacted] comprehensive cybersecurity program is supported by policies and procedures designed to protect our systems and operations as well as the sensitive personal information and data of our clients and customers from foreseeable cybersecurity threats. This program is an integral component of our enterprise risk management program.

Core to our security model is our defense-in-depth framework, comprising multiple layers of processes and technologies that help prevent, detect, and respond to threats. Our approach to safeguarding against external threats incorporates a suite of preventive technologies, including malicious email blocking, defenses against automated attacks and multifactor authentication. These strategies act to proactively intercept and neutralize cyber threats to help ensure data remains secure within our environment. Event monitoring technologies run continuously, detecting suspected intrusion attempts and alerting our Cybersecurity Incident Response team. [Redacted] undertakes a number of critical security processes to mitigate and protect against cybersecurity risks, which include but are not limited to:

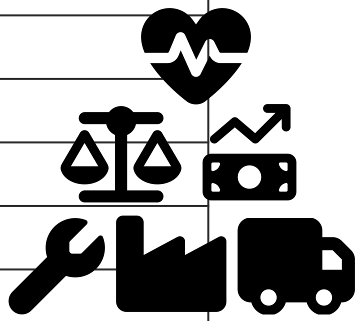
- **Identity and Access Management**. Employees are provided with the minimum amount of access required to perform their jobs using role-based access control methodology, which defines access to our information systems based on job function. Privileged or elevated access to our systems is subject to supplemental approval requirements, increased authentication processes, and additional logging and monitoring.

- **Security Awareness and Training**. Events and education activities are hosted throughout the year, such as the Cybersecurity Awareness Month, expos, videos, training programs and frequent phishing simulations. [Redacted] continuously trains workforce members on the importance of preserving the confidentiality and integrity of customer data.
All new hires have mandatory information protection and privacy training as part of their onboarding, and all workforce members complete an annual cybersecurity refresh training.

- ...

VS

Company Size	Total Assets (U.S. Dollar)
Micro	< 100 Million
Small	100 Million - 500 Million
Mid-	500 Million - 2 Billion
Mid+	2 Billion - 10 Billion
Large	10 Billion - 100 Billion
Mega	> 100 Billion



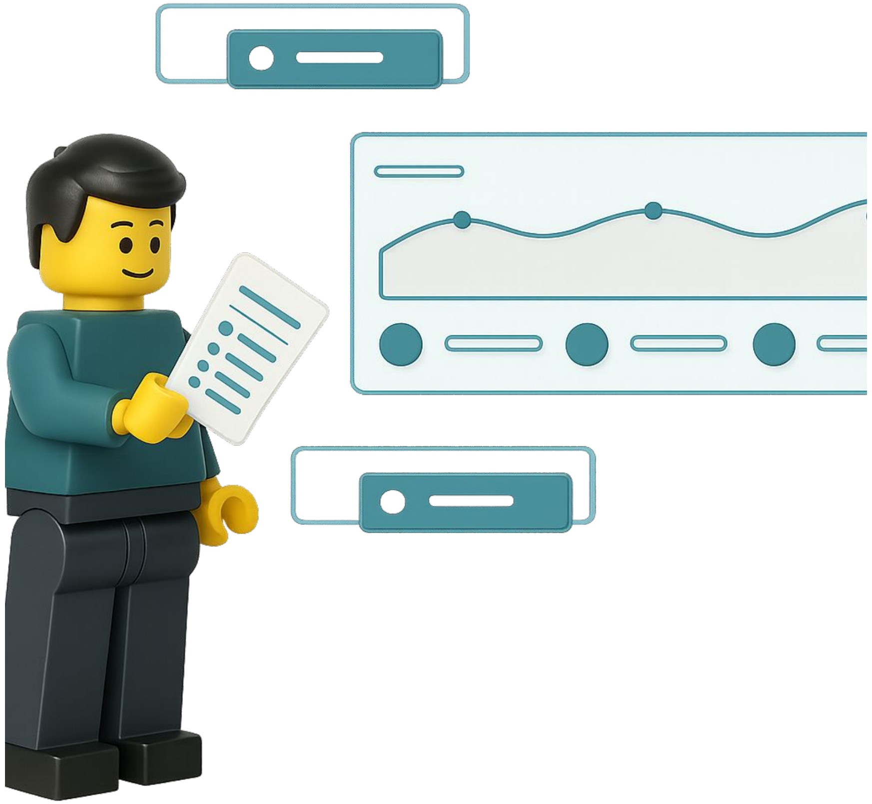
Crawling SEC DB
6,719 Filings

→ **Item 1C Extraction**
5,286 Filings

→ **Keyword Search**
70 Queries

→ **Comparison with 2023**
5,021 Filings

→ **Correlation** (Size, Sector)
8 Sectors
Micro to Mega



Results

A General Overview

Content	Item 1C Only									Full 10-K	
Year	2024[2]									2024	2023
	All (C_{24})	Energy & Transportation	Finance	Industry	Life Science	Manufacturing	Real Estate & Construction	Technology	Trade & Service	All (F_{24})	All (F_{23})
n	**5,286**	546	767	565	728	705	548	605	671	**5,286**	**5,021**
Awareness Training (SAT)	76.9%	80.6%	85.3%	73.6%	72.3%	78.0%	69.9%	78.8%	78.7%	78.3%	23.6%
Phishing Simulation	24.4%	22.3%	30.5%	22.8	19.0%	28.2%	27.0%	20.3%	24.1%	26.5%	1.6%
Annual SAT	23.2%	22.0%	32.7%	23.7%	12.4%	22.8%	23.5%	25.5%	22.2%	23.2%	2.4%
Mandatory SAT	12.1%	15.2%	15.6%	11.5%	7.6%	9.9%	13.9%	13.7%	11.6%	12.1%	1.1%
Onboarding	5.3%	2.2%	6.6%	6.0%	4.7%	3.3%	7.5%	6.0%	5.5%	5.3%	0.1%
Tabletop (Management)	21.1%	20.3%	26.1%	17.0%	10.9%	23.0%	19.7%	25.8%	25.5%	22.4%	0.6%
MFA	10.2%	11.9%	11.0%	10.4%	7.4%	11.9%	9.3%	9.1%	11.0%	11.0%	2.1%
Reporting Functions	7.9%	7.9%	9.4%	7.8%	8.0%	7.9%	7.1%	6.9%	7.3%	N/A[3]	N/A
Passwords	4.8%	5.3%	3.8%	5.5%	6.7%	3.8%	5.8%	4.1%	3.9%	12.6%	7.8%
Social Engineering	6.4%	4.0%	9.3%	6.0%	7.3%	6.7%	6.6%	5.1%	5.7%	32.8%	20.1%
Malware	15.2%	15.4%	13.7%	17.9%	13.2%	14.8%	19.3%	13.4%	14.0%	51.7%	30.2%
Cyber Insurance	24.7%	24.7%	24.3%	23.7%	27.7%	25.7%	22.4%	25.6%	27.7%	48.0%	32.4%
NIST CSF	39.9%	50.2%	43.7%	40.7%	25.7%	43.3%	36.7%	41.2%	41.3%	39.9%	2.0%
ISO 27001	7.9%	4.9%	5.6%	8.8%	2.3%	7.0%	4.0%	19.5%	11.8%	7.9%	1.5%

Results

1 **SAT Is Widespread**

78% Implement SAT

2 **Types of SAT**

Primarily Phishing Simulations

3 **Across Sectors**

Significant Differences
(Finance > Construction)

“All employees are required to pass a mandatory cybersecurity training on an annual basis and receive monthly phishing simulations to provide ‘experiential learning’ on how to recognize phishing attempts.”

 SAT = Security Awareness and Training

Results

"We employ a variety of measures, including password protection, frequent mandatory password change, multi-factor authentication, and internal phishing testing."

4 Employee-Facing Security

Beyond MFA, rarely discussed

5 Employee Blaming

Described as Insider Threats

6 Usable Security Non-Existent

2/5286 Use PW Managers

 SAT = Security Awareness and Training

Comparison by Size

	n	Micro 1,340	Small 837	Mid- 1,002	Mid+ 1,098	Large 661	Mega 111
Awareness Training (SAT)	4,065	52.8%	80.0%	84.1%	88.5%	89.3%	88.3%
Phishing Simulation	1,292	11.5%	20.9%	27.5%	34.1%	33.3%	23.4%
Annual SAT	1,228	11.3%	19.5%	24.2%	33.9%	32.4%	38.7%
Mandatory SAT	642	5.3%	11.8%	13.4%	14.1%	17.5%	18.0%
Onboarding	281	3.3%	6.8%	4.8%	7.5%	5.6%	2.7%
Tabletop (Management)	1,113	5.1%	15.9%	25.6%	31.2%	35.1%	30.6%
MFA	539	9.1%	9.1%	11.5%	11.8%	7.9%	8.1%
Reporting Functions	417	5.7%	8.2%	8.2%	8.5%	10.0%	11.7%
Passwords	252	5.8%	4.5%	5.3%	3.6%	3.8%	3.6%
Social Engineering	216	4.0%	5.5%	7.7%	8.3%	6.5%	11.7%
Malware	802	14.3%	14.3%	16.1%	15.8%	15.0%	14.4%
Cyber Insurance	1,307	16.3%	24.5%	25.7%	31.1%	30.0%	25.2%
NIST CSF	2,111	16.6%	32.9%	44.1%	55.7%	60.1%	59.5%
ISO 27001	415	2.1%	6.3%	10.2%	11.1%	12.1%	10.8%

Results

7 **Company Size**

~ The bigger, the more SAT

8 **Cyber Insurance, and NIST**

Significant Correlation with SAT

9 **Item 1C**

Focus on Mitigations

"We have also purchased network security and cyber liability insurance in order to provide a level of financial protection, should a data breach occur."

SAT = Security Awareness and Training

Discussion

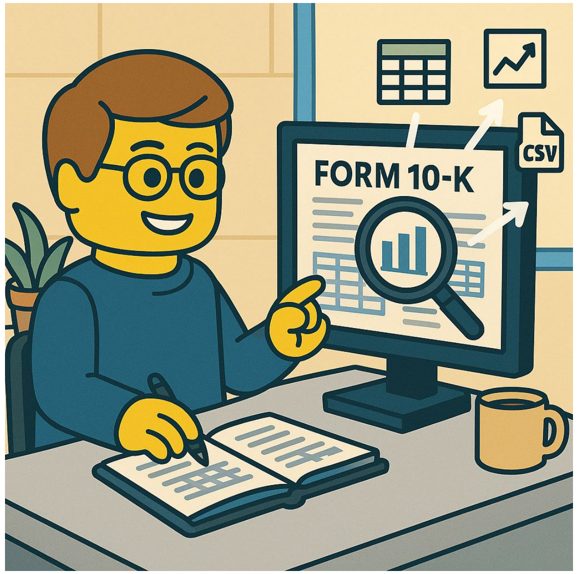
What Can We Learn?

Industry Best-Practices

Phishing Simulations Do Not Work! [1,2,3]

Employee Framing

"Threats" or "Valuable Assets"?



10-K Filings Are Rich

New Factual Dataset Available

[1] Lain et al.: **Phishing in Organizations: Findings from a Large-Scale and Long-Term Study**. IEEE S&P '22.
[2] Lain et al.: **Content, Nudges and Incentives: A Study on the Effectiveness and Perception of Embedded Phishing Training**. ACM CCS '24.
[3] Ho et al.: **Understanding the Efficacy of Phishing Training in Practice**. IEEE S&P '25.

Takeaway

SAT Is Everywhere

Phishing Simulations,
are Widespread

Significant Differences
Across Size & Sector

“Users Are the Enemy”

Usable Security
Is Not Present

Employees Are Blamed
and Depicted as Threat

Rep. Package

Crawling and Parsing
Pipeline & Scripts

Coded Data and Tables
Available

Jonas Hielscher

Maximilian Golla

Paper

Dataset