Issues in Information Systems
Volume 24, Issue 4, pp. 51-65, 2023

DOI: https://doi.org/10.48009/4_iis_2023_105

Factors influencing the development of a successful cybersecurity culture

Queen, E. Booker, *Metropolitan State University, queen.booker@metrostate.edu*
Carl M. Rebman, Jr., *University of San Diego, carlr@sandiego.edu*

Abstract

All organizations are susceptible to the risks of cyberattacks. Protecting an organization's data and technology is crucial as such systems are frequent targets of attacks from those seeking to gain personal benefit or destroy the organization. Specifically, these external actors either hold an organization's data for ransom or they disrupt the organization's system by either shutting it down or changing the way the system runs. Literature has indicated that organizations can address and minimize threats and attacks is to develop a cybersecurity culture through implementation of intentional factors designed specifically to build such a culture. This paper examines the results of 276 cybersecurity leaders who participated in a survey to determine the number of cultural intentional factors implemented by the organization and number of cyberattacks experience during 2022. The results suggest that organizations can minimize cyberattacks by employing specific factors such as top management engagement, champions, communication, knowledge, security awareness, security training, motivation, and trust.

Keywords: cyberattacks, cybersecurity, culture, security awareness, security training, security education, security champions

Introduction

According to Everard (2023), cybersecurity culture refers to the attitudes, knowledge, assumptions, norms, and values of the workforce of an organization with respect to cybersecurity that are shaped by the goals, structure, policies, processes, and leadership of the organization. Everard (2023) suggests that creating an effective cybersecurity culture is best accomplished by recognizing that people, not technology, make an organization secure as people are both the best response to cyber-attacks and the weakest link in cybersecurity chains. Da Veiga et al. (2020) proposes that cybersecurity culture is "contextualized to the behavior of humans in an organizational context to protect information processed by the organization through compliance with the information security policy and an understanding of how to implement requirements in a cautious and attentive manner as embedded through regular communication, awareness, training and education initiatives."

Alshaikh (2020) found a consensus in the literature that establishing a cybersecurity was gaining significant focus as companies as a means for protecting information assets. Thus, it is important to foster an environment where employees are equipped to be the first line of defense in protecting an organization from cybersecurity threats. The rest of this manuscript is as follows. First, is a literature review of cybersecurity culture factors which is then followed by the research methodology, results, discussion, conclusion, and next steps.

Literature Review

Prior research has established the importance and significance of establishing a specific cybersecurity culture as part of the organizational culture due to the need for specific security education, training and awareness (SETA) (Da Veiga et al., 2020*;* Nel and Drevin, 2019*;* Parsons et al., 2015*).* SETA has been established as essential to creating and maintaining an effective cybersecurity culture in organizations to reduce cyberattacks from employee-related security incidents. This perception is supported by ISO/IEC standard which stresses the need for SETA programs as part of an overall management system of information security within the organization. The standard also recommends that organizations should provide an adequate level of education, training and awareness in security procedures and correct use of information systems for all employees. (ISO/IEC, 2013*).*

The factors that support a strong security culture has been researched for many years. Notably, there is no "silver bullet" to ensure against human behavior. However, there is general agreement among information security professionals that it is an absolute and necessary task for organizations to develop a culture around cybersecurity to protect the organization. (Alshaikh, 2020; Chia et al., 2002; Da Veiga and Eloff, 2010*;* Ruighaver et al., 2007*;* Shedden et al., 2016*;* Uchendu et al., 2021).

The process of establishing a cybersecurity culture has been studied in for many years with early work establishing definitions and later works connecting the work to both organizational behavior and organizational cultural lens. (AlHogail, 2015; Alshaikh, 2020; Da Veiga and Eloff, 2010; Da Veiga et al., 2020; Furnell and Thomson, 2009*;* Martins and Elofe, 2002*;* Nel and Drevin, 2019; Schlienger and Teufel, 2002*;* Van Niekerk and Von Solms, 2010; Uchendu et al., 2021). These studies suggest that traditional factors impacting organizational culture are similarly important for establishing a cybersecurity culture, just with an emphasis on cybersecurity. Uchendu et al. (2021) summarized the top factors studied and considered to be important to cybersecurity culture in the literature. The relevant factors are shown in Table 1.

Table 1: Factors regarded as important to cybersecurity culture Reprinted from Uchendu et al

Factor	Definition
Accountability and responsibility	Accountability refers to an employee owning the outcome of an action/behavior, while responsibility refers to the employee's obligation to carry out a task that may pertain to security
Change management	The process that guides and supports employees towards the change necessary to develop a security culture within an organization.
Commitment	Employees within an organization understand the need for security and support practices to ensure security policies are adhered to and a security culture fostered.
Communication	The means utilized to share information between the organization and its employees, for instance means through which employees find out about security policies, procedures, and practices and what is expected of them.
Compliance	The process of ensuring employees and the organization adhere to standards and regulations on security.
Establishing a network of champions	Champions are members of an organization who support activities in raising security awareness and act as a point of contact. Champions within different sections, departments or offices of an organization create a network.
Ethical conduct	Behavior and decision making within an organization follow a moral code of right and wrong. Such code can impact how people adopt or engage with a security culture (especially if that culture is perceived as unethical or harmful).
Knowledge	Employee understanding of security hygiene practices as well as an organization's policies and procedures.

Factor	Definition
Motivation	Incentives provided to encourage employee adherence to security policies, practices, procedures, and advice.
National culture	This relates to the norms, values, beliefs and customs of the nation or region that an organization or employee is based in; these can influence an organization's security culture.
Regulations	The legal provisions/directives in relation to safeguarding information technology and computer systems, which organizations and their employees need to abide by.
Rewards and sanctions	Utilizing an approach of rewarding employee behavior which is security compliant, or penalising non-compliance which may result in a potential compromise (or compromise) of the organization.
Security awareness	The understanding that employees of an organization possess regarding security generally.
Security policy	A set of guidelines and processes which are defined by an organization in relation to security.
Security risk	This factor refers to the security threats and vulnerabilities that an organization (and its employees) is exposed to which can lead to intentional or unintentional impacts.
Security training	The provision of security education materials to and general upskilling of employees that would make them cognizant of security threats and the organization's respective policies and procedures.
Top management support, leadership, or involvement	The support and engagement of C-suite executives, senior managers, department managers, in creating, practicing, and maintaining a security culture.
Trust	Employees and the organization need to have confidence in each other both generally and as it relates to security activities. This confidence is two-way and can relate to any activities within or about the organization (e.g., trust in the organization generally, trust that its policies are well considered,
User management	The procedures that are in place to manage and monitor employee behavior and compliance.

Several studies support SETA or some part of it. For example, in the top factors found by Uchendu et al in their systematic literature review included both security awareness and training. Further studies indicate that awareness and training as part of a cybersecurity culture can improve employees' security behavior *(*Zakaria et al., 2007) as well as prevent security breaches caused by employees' noncompliance security policies and procedures (AlHogail, 2015; Dojkovski et al., 2010*;*).

Prior research also shows support for a comprehensive approach to developing a cybersecurity culture beyond SETA. Specifically, Da Veiga et al., (2020*)* and Fennelly and Perry (2020*)* state that security is "everyone's responsibility." They further contend that by developing a comprehensive approach to cybersecurity culture the default action (or the norm) by members of the institution will be to protect the organization. This in turn reinforces the need for a comprehensive framework and guidelines to assist organizations to build cybersecurity culture. Additional research has expounded on the importance of factors other than SETA such as the importance of leadership support security monitoring, security policies, user management, and security communications (Da Veiga et al., 2020*;* Greene and D'Arcy, 2010, Knapp et al., 2006).

Research Goal/Purpose

The goal of this study was to draw upon previous cybersecurity studies to provide insight as to how many organizations were implementing factors to establish a culture that could have an impact on the protection of the organization's information systems and assets. This study was interest examining the number of factors implemented and which one or combination might be more effective. Lastly, this study sought to

survey a representation of different industries to determine consistency of successful factors.

Research Methodology

This study attempts to compare the number of factors implemented as well as type of factors implemented, and the impact on the number of successful cyberattacks on the organization. The study used a survey designed from the factors identified in the systematic literature review conducted by Uchendu et al. (2021). The survey consisted of the factor along with the definition and simply asked respondents to indicate to the degree the organization had implemented each factor, using a Likert-scale of 0 (don't know what this is/not sure), 1 (not at all), 2 (under consideration), 3 (in process), 4 (implemented in 2022), 5 (implemented prior to 2022).

Respondents were also asked the number of employees in the organization, the primary industry, and the number of successful cybersecurity attacks in 2022. No information about location was collected to protect the identity of organizations. A convenience sample of twenty security professionals previewed the survey and the list of factors. National culture and regulations were deemed "external factors" by the previewers and were removed from the final instrument.

Study participants were attendees of a 2023 webinar on creating a cybersecurity culture which included a presentation on academic literature of factors found to support positive cybersecurity cultures, and methods for implementation and assessment of the culture. The webinar had 302 participants of which 276 completed the survey in its entirety prior to the webinar. Participants were informed that the survey would be used to customize the webinar but would also be used as part of an academic study on cybersecurity culture implementation comparisons. The survey was released a month before the webinar and closed one week prior to the webinar. The survey was created using Qualtrics. Each factor was given a unique code as shown in Table 2.

Table 2: Factor Code Association

Num	Factor
F1	Accountability and responsibility
F2	Change management
F3	Commitment
F4	Communication
F5	Compliance
F6	Establishing a network of champions
F7	Ethical conduct
F8	Knowledge
F9	Motivation
F10	Rewards and sanctions
F11	Security awareness
F12	Security policy
F13	Security risk
F14	Security training
F15	Top management support, leadership, or involvement
F16	Trust
F17	User management

Data Analysis

Although the organizational location was not tracked through the survey, participants in the webinar were located from across the United States distributed as shown in Figure 1.

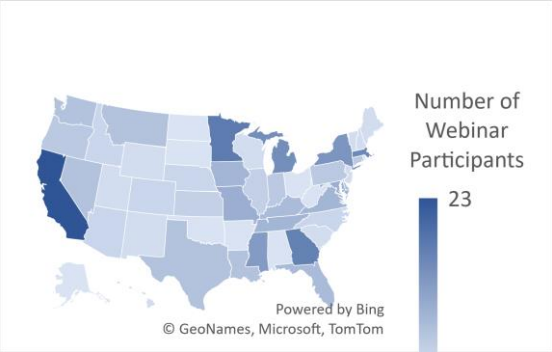

Figure 1: Location of Webinar Participants

The participants also represented a wide range of industries. The industries were grouped into 5 categories. The percent of respondents by industry is shown in Figure 2. The majority of the participants were from the retail industry, followed by finance and the hospitality industry which included hotels, food services and other entertainment organizations. Education included the range from day care to higher education. Other included a wide range of industries that did not fit the other four such as farming (11), manufacturing (13), construction (7) and government (9).

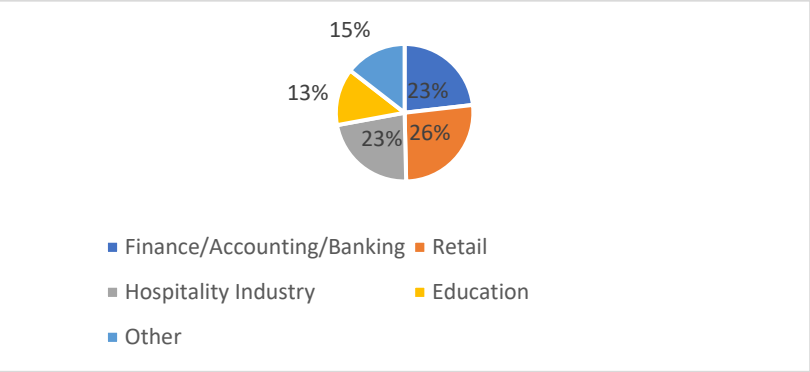

Figure 2: Breakdown of Respondent Industries

The number of employees by range are shown in Table 3 and The number of successful attacks for respondents ranged from 0 to 9, with the majority of the successful attempts at 0. The number reported is listed in Table 4.

Table 3: Number of Employees

Range of Employees	Count
less than 250	55
between 250 and 500	76
between 501 and 750	73
greater than 750	72
Total	**276**

Table 4: Number of Attacks (General)

Number of Successful Attacks in 2022	Count	Percent
0	81	29.3%
1	64	23.2%
2	31	11.2%
3	22	8.0%
4	13	4.7%
5	21	7.8%
6	25	9.1%
7	9	3.3%
8	5	1.8%
9	5	1.8%
Total	**276**	**100%**

Table 5 shows the crosstab of employee count and the number of successful attacks. As shown in the table, most organizations had 3 or fewer successful attacks with 0 as the most frequently reported for all employee group sizes except for those greater than 750 which reported the count of 1 as the most frequently reported number of successful attacks.

Table 5: Cross tab of employee count and successful attacks

Number of Successful Attacks/Employee Count	less than 250	between 250 and 500	between 501 and 750	greater than 750	Total
0	17	27	20	17	81
1	16	16	13	19	64
2	4	9	8	10	31
3	3	7	8	4	22
4	2	4	4	3	13
5	6	2	7	6	21
6	2	6	8	9	25
7	3	2	2	2	9
8	1	2	2	0	5
9	1	1	1	2	5
Total	**55**	**76**	**73**	**72**	**276**

Table 6 shows the crosstab of the number of successful attacks by primary industry. All industries had a range of successful attacks. Hospitality had the most successful cyberattacks during 2022, followed by finance and related industries and then retail. When separating and counting the number of successful attacks at five or more, Hospitality had the highest number of successful attacks, with 20 attacks, closely followed by Finance and related industries with 19. Retail had the highest number of no reported attacks.

Table 6: Cross tab of successful attacks by primary industry

Number of Successful Attacks	Primary Industry					
	Finance/ Accounting/ Banking	Retail	Hospitality	Education	Other	Total
0	17	30	13	11	10	81
1	17	17	13	9	8	64
2	1	11	6	3	10	31
3	4	4	7	4	3	22
4	6	1	3	1	2	13
5	4	5	6	1	5	21
6	8	3	8	5	1	25
7	2	2	3	1	1	9
8	2	0	2	1	0	5
9	3	0	1	1	0	5
Total	**64**	**73**	**62**	**37**	**40**	**276**

We started by analyzing those companies who had zero or no cybersecurity attacks in 2022 as our baseline of what factors might constitute best practices in creating a cybersecurity culture. Table 8 presents a breakdown of the 81 companies who reported having zero (0) successful cyberattacks along with their report response on the Likert scale questionnaire. Recall that each factor was rated by each respondent using a Likert-scale of 0 (don't know what this is/not sure), 1 (not at all), 2 (under consideration), 3 (in process), 4 (implemented in 2022), 5 (implemented prior to 2022).

For those with no successful cyberattacks in 2022 (Table 7), 81 of the 276 companies had implemented 9 out of the 17 cybersecurity culture factors prior to 2022. The specific factors were change management programs, commitment, communication, compliance infrastructure, champions, security awareness practices, security training and top management engagement and are highlighted in Table 8. In addition, all 81 of these organization were either in the process of or had implemented the remaining factors in 2022 except rewards and sanctions (F10), trust (F16) and user management (F17). Rewards and sanctions (F10) and trust (F16) are the only two factors where there can be a range of implementation statuses.

Table 7: Number of Successful Attacks=0 and number of responses on the Likert scale.

Factor/Number of Responses	0 – NS	1 Not al all	2 UC	3 IP	4 In 2022	5 Pre 2022
F1: Accountability and responsibility	0	0	0	23	22	36
F2: Change management	0	0	0	0	0	81
F3: Commitment	0	0	0	0	0	81
F4: Communication	0	0	0	0	0	81
F5: Compliance	0	0	0	0	0	81
F6: Establishing a network of champions	0	0	0	0	0	81
F7: Ethical conduct	0	0	0	21	40	20
F8: Knowledge	0	0	0	0	47	34
F9: Motivation	0	0	0	25	29	27
F10: Rewards and sanctions	17	17	11	19	17	0

Factor/Number of Responses	0 – NS	1 Not al all	2 UC	3 IP	4 In 2022	5 Pre 2022
F11: Security awareness	0	0	0	0	0	81
F12: Security policy	0	0	0	0	0	81
F13: Security risk	0	0	0	0	35	46
F14: Security training	0	0	0	0	0	81
F15: Top management support, leadership, or involvement	0	0	0	0	0	81
F16: Trust	10	22	18	19	12	0
F17: User management	0	0	22	11	21	27

The next step of the analysis was to determine if there was a relationship or impact between the factors and the number of successful attacks. Table 8 presents the summary of the number of attacks with reported company Likert response from the survey by each of the seventeen factors. For those with one successful cyberattack in 2022 most of 64 companies had implemented change management programs, commitment, communication, compliance infrastructure, champions, security awareness practices, security training and top management engagement prior to or during 2022. These companies also were either were in the process of implementing or had implemented the remaining factors in 2022 except rewards and sanctions (F10), trust (F16) and user management (F17).

Comparatively, the 31 organizations that had two or more successful attacks focused their efforts on monitoring users, establishing policies and security awareness. There was not as much engagement of top leadership and engagement as organizations with one or fewer successful attacks. It was found that companies that 7 or more successful attacks were just starting to implement cybersecurity culture factors. These companies seemed to just be implementing security awareness, security policies, communicating accountability and responsibility for actions, creating motivation, and working to obtain top management support.

Using the number of attacks as the grouping variable, ANOVA (shown in Table 9) was run to determine if there was significance of different for the responses for each factor. Each factor was significant at $p<.001$ indicating that there was significant difference between the number of attacks and the responses provided. This statistic supports prior research that shows engagement of top leadership, education, communication, champions and security policies are all critical to creating a successful cybersecurity culture whereas monitoring employees without those is not successful in creating a positive culture.

Table8: Number of Successful Attack and number of responses on the Likert scale Listed by Factor

FACTORS/ Number of Successful Attacks	0 Not Sure	1 Not at all	2 Under C	3 In Prog	4 Imp 22	5 Pre 22
F1: Accountability and responsibility						
Only 1 attack	0	9	16	14	8	17
2	0	10	4	10	4	3
3	7	2	2	3	5	3
4	1	2	3	2	5	0
5	6	4	5	2	3	1
6	2	8	4	5	3	3
7	1	2	2	0	1	3

FACTORS/ Number of Successful Attacks	0 Not Sure	1 Not at all	2 Under C	3 In Prog	4 Imp 22	5 Pre 22
8	1	0	1	0	1	2
9 or more attacks	0	0	0	2	2	1
F2: Change management						
Only 1 attack	0	0	0	23	22	19
2	0	0	0	12	10	9
3	0	7	6	6	3	0
4	0	3	1	1	3	5
5	0	6	5	5	3	2
6	0	8	5	6	5	1
7	0	0	2	1	5	1
8	0	2	1	2	0	0
9 or more attacks	0	1	2	1	1	0
F3: Commitment						
Only 1 attack	0	0	0	0	33	31
2	0	0	0	0	19	12
3	0	0	0	13	9	0
4	0	0	0	9	4	0
5	0	0	0	10	11	0
6	0	0	0	13	12	0
7	0	0	0	7	2	0
8	0	0	0	0	5	0
9 or more attacks	0	0	0	1	4	0
F4: Communication						
Only 1 attack	0	0	0	0	30	34
2	0	0	0	0	14	17
3	0	0	10	5	7	0
4	0	0	6	7	0	0
5	0	0	4	9	8	0
6	0	0	12	5	8	0
7	0	0	3	3	3	0
8	0	0	2	0	3	0
9 or more attacks	0	0	2	1	2	0
F5: Compliance						
1	0	0	0	0	27	37
2	0	0	0	0	17	14
3	0	0	5	7	3	7
4	0	0	3	3	3	4
5	0	0	3	6	9	3
6	0	0	2	9	6	8
7	0	0	4	1	3	1

FACTORS/ Number of Successful Attacks	0 Not Sure	1 Not at all	2 Under C	3 In Prog	4 Imp 22	5 Pre 22
8	0	0	3	2	0	0
9	0	0	0	0	3	2
F6: Establishing a network of champions						
Only 1 attack	0	0	0	0	26	38
2	0	0	0	0	17	14
3	0	0	4	10	5	3
4	0	0	2	5	2	4
5	0	0	9	4	5	3
6	0	0	3	11	5	6
7	0	0	5	1	2	1
8	0	0	1	3	1	0
9 or more attacks	0	0	2	2	1	0
F7: Ethical conduct						
Only 1 attack	0	0	0	19	22	23
2	0	0	0	8	15	8
3	0	0	4	7	4	7
4	0	0	5	3	4	1
5	0	0	10	4	2	5
6	0	0	5	7	8	5
7	0	0	3	0	2	4
8	0	0	0	2	2	1
9 or more attacks	0	0	1	0	2	2
F8: Knowledge						
Only 1 attack	0	0	10	16	17	21
2	0	0	7	7	10	7
3	0	0	5	6	3	8
4	0	0	4	7	0	2
5	0	0	5	6	6	4
6	0	0	8	3	5	9
7	0	0	2	3	3	1
8	0	0	0	2	3	0
9 or more attacks	0	0	1	1	3	0
F9: Motivation						
Only 1 attack	0	0	16	21	16	11
2	0	0	8	5	10	8
3	0	0	8	4	8	2
4	0	0	4	1	5	3
5	0	0	6	7	3	5
6	0	0	4	5	8	8
7	0	0	1	0	5	3

FACTORS/ Number of Successful Attacks	0 Not Sure	1 Not at all	2 Under C	3 In Prog	4 Imp 22	5 Pre 22
8	0	0	1	3	0	1
9 or more attacks	0	0	0	2	1	2
F10: Rewards and sanctions						
Only 1 attack	11	15	11	13	14	0
2	6	6	6	4	9	0
3	0	0	1	8	5	8
4	0	0	1	7	3	2
5	0	0	6	2	7	6
6	0	0	7	5	4	9
7	0	0	4	1	1	3
8	0	0	0	3	2	0
9 or more attacks	0	0	1	1	1	2
F11: Security awareness						
Only 1 attack	0	0	0	0	30	34
2	0	0	0	0	20	11
3	0	0	4	7	7	4
4	0	0	2	4	2	5
5	0	0	3	5	7	6
6	0	0	4	8	9	4
7	0	0	1	3	2	3
8	0	0	0	1	2	2
9 or more attacks	0	0	2	2	0	1
F12: Security policy						
Only 1 attack	0	0	0	0	0	64
2	0	0	0	0	0	31
3	0	0	3	5	8	6
4	0	0	4	2	4	3
5	0	0	6	7	6	2
6	0	0	8	6	5	6
7	0	0	1	1	4	3
8	0	0	2	1	1	1
9 or more attacks	0	0	1	2	1	1
F13: Security risk						
Only 1 attack	0	0	0	20	24	20
2	0	0	0	13	10	8
3	0	0	5	6	7	4
4	0	0	1	3	5	4
5	0	0	4	3	5	9
6	0	0	7	6	5	7
7	0	0	0	1	3	5

FACTORS/ Number of Successful Attacks	0 Not Sure	1 Not at all	2 Under C	3 In Prog	4 Imp 22	5 Pre 22
8	0	0	3	0	0	2
9 or more attacks	0	0	1	1	1	2
F14: Security training	0	0	0	20	24	20
Only 1 attack	0	0	0	23	21	20
2	0	0	0	8	15	8
3	0	0	5	5	11	1
4	0	0	2	1	5	5
5	0	0	11	3	3	4
6	0	0	5	10	2	8
7	0	0	4	3	1	1
8	0	0	2	0	2	1
9 or more attacks	0	0	1	0	3	1
F15: Top management support, leadership, or involvement						
Only 1 attack	0	0	0	28	18	18
2	0	0	0	9	8	14
3	0	0	6	2	8	6
4	0	0	5	2	3	3
5	0	0	6	3	5	7
6	0	0	6	6	7	6
7	0	0	1	4	3	1
8	0	0	1	2	2	0
9 or more attacks	0	0	2	1	1	1
F17: Trust						
Only 1 attack	10	24	12	7	11	0
2	2	5	5	9	10	0
3	0	0	9	2	7	4
4	0	0	3	4	2	4
5	0	0	4	5	9	3
6	0	0	8	3	4	10
7	0	0	1	2	3	3
8	0	0	2	1	0	2
9 or more attacks	0	0	2	2	0	1
F18: User management						
Only 1 attack	0	0	14	10	17	23
2	0	0	5	9	9	8
3	0	0	0	0	12	10
4	0	0	0	0	7	6
5	0	0	0	0	14	7
6	0	0	0	0	11	14

FACTORS/ Number of Successful Attacks	0 Not Sure	1 Not at all	2 Under C	3 In Prog	4 Imp 22	5 Pre 22
7	0	0	0	0	6	3
8	0	0	0	0	4	1
9 or more attacks	0	0	0	0	1	4

Table 9: ANOVA Results

ANOVA

	Sum of Squares	df	Mean Square	F	Sig.
Accountability and responsibility	174.922	9	19.436	10.352	<.001
Change management	280.785	9	31.198	39.448	<.001
Commitment	113.475	9	12.608	74.101	<.001
Communication	227.078	9	25.231	75.55	<.001
Compliance	112.051	9	12.45	26.654	<.001
Establishing a network of champions	153.449	9	17.05	36.986	<.001
Ethical conduct	28.419	9	3.158	3.798	<.001
Knowledge	48.777	9	5.42	5.824	<.001
Motivation	28.694	9	3.188	3.132	0.001
Rewards and sanctions	161.376	9	17.931	9.75	<.001
Security awareness	93.054	9	10.339	22.315	<.001
Security policy	154.197	9	17.133	40.657	<.001
Security risk	45.159	9	5.018	6.73	<.001
Security training	128.874	9	14.319	22.007	<.001
Top management support, leadership, or i	108.045	9	12.005	16.675	<.001
Trust	157.576	9	17.508	11.03	<.001
User management	38.692	9	4.299	4.432	<.001

Discussion

Based on the results, organizations that minimize successful cyberattacks engage and embrace the following factors first: security awareness, security policy, security training, top management support, leadership, or involvement, change management, commitment, communication, compliance, and establishing a network of champions. The two factors that appear to have no impact on thwarting successful attacks are rewards and sanctions, and trust. Organizations with the most successful attacks (2 or more) appear to focus more on monitoring users (user management) than organizations that had fewer successful attacks. This suggests that monitoring user activity has less of an impact than training and communicating with users, especially if the practice appears to not have engagement of leadership.

Conclusions, Limitations and Future Research

All organizations are susceptible to the risks of cyberattacks. Protecting an organization's data and technology is crucial as such systems are frequent targets of attacks from those seeking to gain personal benefit or destroy the organization. Prior research has established that a specific cybersecurity culture with

SETA and making it part of the organizational culture can significantly minimize or mitigate hacking attacks on the organization.

This study compared the implementation of factors that support the building of a positive cybersecurity culture as reported in the literature to the number of successful cybersecurity attacks in 2022 which included the components of SETA. Findings suggest that coinciding with SETA, it is also important to have support from top management. Otherwise, most of the efforts will not have the desired impact of stopping hacking attacks. Although the participants were from diverse industries and from across the United States, the sample size from each industry was not sufficient to effectively generalize the results. Further, although the ANOVA supports the differences between groups for the results, a deeper statistical analysis is necessary to better understand the interactions between size of organization, industry, number of successful attacks and factors implemented and when.

Future research for this study is to collect additional data to ensure the samples represent a larger voice from manufacturing and related firms and others that have customer data often sought by the dark web and hackers. This would include the engagement of more statistical analyses and intra-effects such as industry and size.

References

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavio*r, 49, 567-575.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98, 102003.

Center for Strategic and International Studies (CSIS). (2020). Significant Cyber Incidents https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents [accessed 4 June 2023]

Chia, P., Maynard, S., & Ruighaver, A. (2002) Understanding organizational security culture. Proceedings of PACIS2002, Japan

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196-207.

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, 92, 101713.

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2010). Enabling information security culture: influences and challenges for Australian SMEs.

Everard, T. (2023). What is Cyber Security Culture and why does it matter for your organisation? PA Consulting. https://www.paconsulting.com/insights/what-is-cyber-security-culture-and-why-does-it-matter-for-your-organisation [access 4 June 2023]

Fennelly, L. J., & Perry, M. A. (2020). Building a Sustainable Culture of Security. In The Professional Protection Officer (pp. 397-401). Butterworth-Heinemann.

Furnell, S., & Thomson, K. L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security*, 2009(2), 5-10.

Greene, G., & D'Arcy, J. (2010, June). Assessing the impact of security culture and the employee-organization relationship on IS security compliance. In *5th Annual Symposium on Information Assurance* (pp. 1-8).

Infosec Institute. (2018). Why an Effective Security Awareness Program Needs Security Champions in Your Organization. Retrieved from: https://resources.infosecinstitute.com/ why- an- effective- security- awareness - program- needs- security- champions- in- your-organization/ [Accessed 3 May 2021]

Knapp, K. J., Marshall, T. E., Kelly Rainer, R., & Nelson Ford, F. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security*, 14(1), 24-36.

Martins, A., & Elofe, J. (2002). Information security culture (pp. 203-214). Springer US.

Nel, F., & Drevin, L. (2019). Key elements of an information security culture in organisations. *Information & Computer Security*, 27(2), 146-164.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, 9(2), 117-129.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, 26(1), 56-62

Schlienger, T., & Teufel, S. (2002). Information security culture. *Security in the Information Society*, 86, 191-201.

Shedden, P., Ahmad, A., Smith, W., Tscherning, H., & Scheepers, R. (2016). Asset identification in information security risk assessment: A business practice approach. *Communications of the Association of Information Systems*, 39 (15),297-320

Tsoukas, H., & Chia, R. (2002). On organizational becoming: Rethinking organizational change. *Organization Science*, 13(5), 567-582.

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, 109, 102387.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, 29(4), 476-486.

Zakaria, O., Gani, A., Mohd Nor, M., & Badrul Anuar, N. (2007). Reengineering information security culture formulation through management perspective. *Proceedings of the International Conference on Electrical Engineering and Informatics*, Institut Teknologi Bandung, Indonesia.