
# Measuring Stakeholders' Perceptions of Cybersecurity for Renewable Energy Systems

Stuart Madnick, Mohammad S. Jalali,
Michael Siegel, Yang Lee,
Diane Strong, Richard Wang,
Wee Horng Ang, Vicki Deng,
Dinsha Mistree

**Working Paper CISL# 2016-08**

**August 2016**

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

# Measuring Stakeholders' Perceptions of Cybersecurity for Renewable Energy Systems

**Stuart Madnick[1], Mohammad S. Jalali[1], Michael Siegel[1], Yang Lee[2], Diane Strong[3], Richard Wang[1], Wee Horng Ang[1], Vicki Deng[1], Dinsha Mistree[1]**

[1] Massachusetts Institute of Technology
[2] Northeastern University
[3] Worcester Polytechnic Institute

## Abstract

Renewable energy systems need to be able to make frequent and rapid adjustments to address shifting solar and wind production. This requires increasingly sophisticated industrial control systems (ICS). But, that also increases the potential risks from cyber-attacks. Despite increasing attention to technical aspects (i.e., software and hardware) of cybersecurity, many professionals and scholars pay little or no attention to its organizational aspects, particularly to stakeholders' perceptions of the status of cybersecurity within organizations. Given that cybersecurity decisions and policies are mainly made based on stakeholders' perceived needs and security views, it is critical to measure such perceptions. In this paper, we introduce a methodology for analyzing differences in perceptions of cybersecurity among organizational stakeholders. To measure these perceptions, we first designed House of Security (HoS) as a framework that includes eight constructs of security: confidentiality, integrity, availability, technology resources, financial resources, business strategy, policy and procedures, and culture. We then developed a survey instrument to analyze stakeholders' perceptions based on these eight constructs. In a pilot study, we used the survey with people in various functional areas and levels of management in two energy and ICS organizations, and conducted a gap analysis to uncover differences in cybersecurity perceptions. This paper introduces the HoS and describes the survey instrument, as well as some of the preliminary findings.

## Introduction

Rising demand for renewable energy resources has led to a noticeable focus on undertaking technological innovations to expand the green energy industry and respond to demand. As a result, cybersecurity has emerged as a critical issue as the green energy sector faces growing cyber risks. For example, smart grids—which are meant to provide reliable and efficient power network systems to distribute renewable energy resources—open up more direct and indirect connections to the Internet and more connections among the nodes in the networks. Smart grids also require advanced computing and communication technologies [1]. Adding new sources of renewable energy to grids also requires an increase in the frequency and speed of technological adjustments. Consequently, while enhanced features and functionalities are introduced, the networked systems become increasingly vulnerable [2, 3]. Other complications and vulnerabilities are also added with the Internet of Things (IoT), where intelligent devices are getting connected, as sensors and/or controllers, within energy networks. In fact, not only are vulnerabilities on the rise, but they also have the potential of becoming very sophisticated, given the unknown characteristics of new technologies. Because a great deal of attention is being focused on technological innovations in renewable energy systems, the cybersecurity research community has also focused mostly on the technical aspects. Overall, a similar trend is observed in energy companies as they face the challenges of the high cost of developing new technologies in a context of limitation of available resources. As a result, it is not surprising that the organizational aspects of cybersecurity have become a blind spot for both industry and academia.

Cybersecurity is an increasingly crucial and complex management issue. Many organizations have developed cybersecurity policies to protect their business information and operational systems. Although these policies are important, they are often not fully adopted, the reasons being that organizations are limited by the resources they can devote to cybersecurity, and they often misunderstand the status of their cybersecurity. An organization's goal should be to develop the best possible, most cost-effective approach to cybersecurity, which is further complicated by the different priorities of organizational stakeholders. Stakeholders' perceptions of cybersecurity play a critical role in achieving this goal, since they are the main source of decision-making. Moreover, as organizations evolve into extended enterprises, which includes ties with suppliers, customers, and other partners, there is a significant increase in the number of stakeholders, and a wider range of security complications and requirements.

The current cybersecurity literature does not adequately address these issues. Many professionals and scholars have approached the study of cybersecurity by focusing specifically on the technical (e.g., hardware and software) and detailed elements of the security systems themselves, such as encryption

[4-6], firewall technologies [7-9], and antiviruses [10, 11], or have measured specific events, such as mean-time-to-failure. Although these efforts are necessary, they often do not look at cybersecurity holistically and commonly neglect to consider its organizational aspects. They especially neglect to consider the perceived needs and security views of organizational stakeholders.

In this paper, we introduce the MIT House of Security (HoS) framework and present a survey instrument to measure stakeholders' perceptions of cybersecurity. We seek to identify similarities and differences, both within and between different organizations. This research has three major objectives:

- To identify how perceptions both shape, and should potentially shape, decisions about investments in security systems, with a particular focus on identifying the areas most in need of cybersecurity, as perceived by the individuals in the organization.
- To identify perceived differences between importance and assessment of the HoS constructs among stakeholders. These differences are further compared among individuals with different organizational roles and functional areas; e.g., comparing the views of mid-level managers to those of senior management, or the views of information technology (IT) or operational technology (OT) workers with those of other members in the organization.
- To identify differences between the importance and assessment of the HoS constructs among different organizations (e.g., comparing two different organizations).

## MIT's House of Security

Through a comprehensive literature review and several surveys, researchers at MIT have divided cybersecurity issues primarily into eight metagroupings (i.e., constructs). Good security protects the "confidentiality" and "integrity" of data while providing "availability" of the data, networks, and systems to appropriate and authorized users, Confidentiality, integrity, and availability, also known as CIA, are often used as the only critical information characteristics [12]. Good security practices also go beyond just technical solutions and are driven by a "business strategy," with associated "policies and procedures" for security, and are implemented in a "culture of security." Moreover, these practices are supported by "technology resources" and "financial resources" dedicated to security. These eight constructs form the proposed House of Security and are shown in Fig 1.

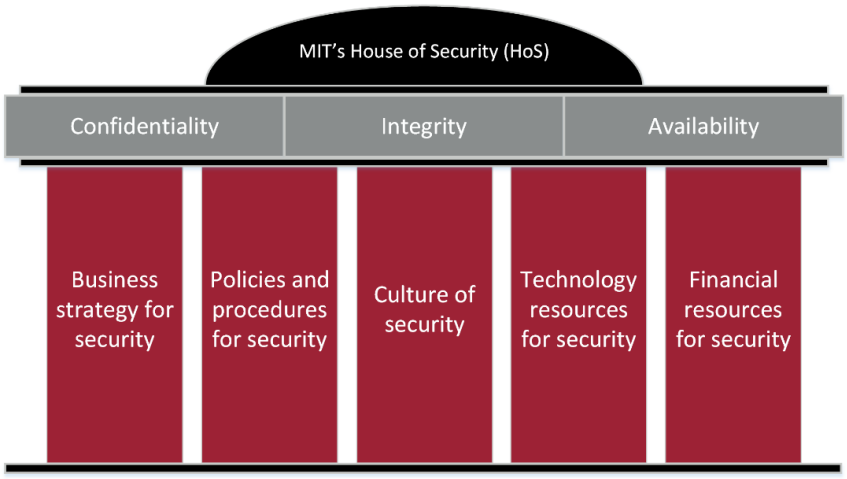


**Fig 1.** The eight constructs of the House of Security

## Survey Instrument

The survey includes three questions related to each construct of HoS (a total of 24 questions). In each question, respondents are asked to specify their perception of both the level of "assessment" and "importance." For example, they first respond to a question (e.g., "are people in the organization aware of good security practices?"), then identify the importance of that aspect. All questions are on a seven-point scale; "1" represents the smallest extent and "7" the largest extent.

The survey questions do not explicitly identify the construct being measured, but relate to aspects of the construct. Furthermore, there are multiple questions for each construct that are ordered randomly. The individuals are not aware of the categorization of the questions across the eight constructs.

A key part of this study involves gap analysis: how much does the perception of the current state of a cybersecurity aspect differ from the perception of its importance. Such gaps help identify potential opportunities for improvement within and across the extended enterprise. Differences in gaps among organizational stakeholders may represent different levels of understanding of security and help identify differences in local knowledge and needs.

We evaluated the quality of the survey instrument by measuring the statistical significance of the questions and the constructs and the reliability of the constructs by computing Cronbach's alpha [13]. While a key goal of our survey is to measure perceptions of the different constructs of security, we also plan to study the causes of these perception variations in our future research.

## Preliminary Results of the Pilot Study

For this pilot study, we distributed the survey broadly to members of two energy and ICS organizations, which we will refer to as organizations A and B. Respondents ranged from employees to top-level managers and across all major functional areas. This diversity was important in order to identify variations in perceptions of cybersecurity. Here we briefly discuss some examples of the results based on: individual questions; constructs (i.e., a group of questions about an HoS construct); and construct gaps (i.e., the gap between assessment and importance of a construct).

*Individual questions*

An example of the results of a question for organizations A and B are shown in Fig 2. The figure presents the assessment of a user (my perceived assessment, marked as MA), the importance (my perceived level of importance, marked as MI), and the gap between MA and MI. This illustrates that people in different organization can have very different perceptions regarding their organization's cybersecurity. For example, for a question about well-defined and communicated cybersecurity strategy, there was a large gap (particularly in organization B), which implies that aspect falls far short of what is perceived to be needed among the respondents. Moreover, this example shows that organization A not only has a higher assessment about this question, but also they also have a higher expectation.

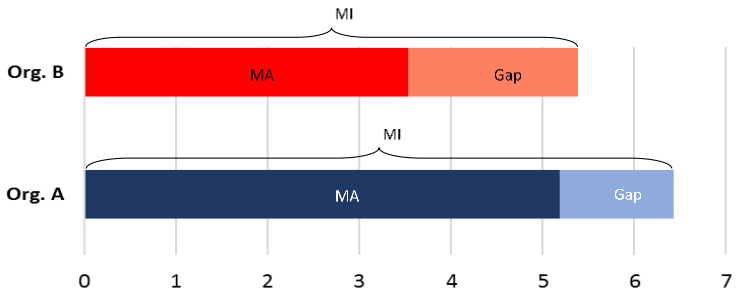


**Fig 2.** Responses to a question on a seven-point scale: "The organization has a well-defined and communicated cybersecurity strategy." MA: my perceived assessment, MI: my perceived level of importance, Gap=MI-MA

*Constructs*

Beyond the individual questions, the results of the constructs present a more holistic overview. Each HoS construct contains three related questions, and the results of the questions are aggregated to present the construct. We have found, so far, that for a given organization, the assessment levels are likely to differ across the eight constructs, while the importance levels are often similarly

high. Comparing organizations, one can observe and study both similarities and differences between the organizations.

The aggregated results of the eight constructs for organizations A and B are presented in Fig 3[1]. The two organizations are relatively similar in their perceptions of availability, but differ noticeably in their perceptions of the state of policies and procedures for security—see Fig 3. At this point, we are not focusing on the specifications of organizations A and B. Obviously, there are other factors that might be at work, such as private vs. public company, large vs. small company, etc. Although these other factors may make it challenging to compare the organizations, these diagrams do provide important insights into the differences in perceptions. We will pursue these issues further in our next stage research with a larger number of organizations.

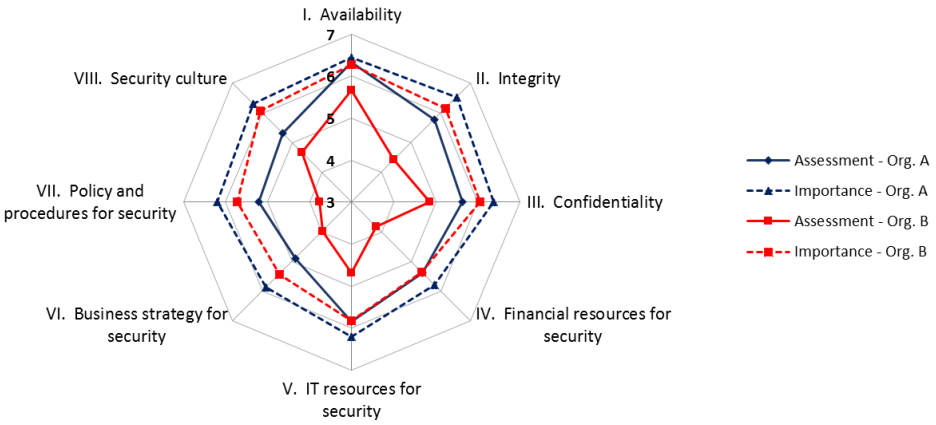


**Fig 3.** Assessment vs. importance in organizations A and B

*Construct gaps*

Although viewing the values of each of the constructs provides some quick insights, it is often more intuitive to examine the gaps between assessment and importance levels. The construct gaps in organizations A and B are presented in Fig 4[2]. As can be seen, in this case, organization B has significantly larger gaps than organization A, with Policy and Procedures for Security construct having the largest gap.

Gap analysis might show that one organization had an overall assessment of 5 in a construct, and if it viewed that construct as only having an importance value of 5, the gap would be zero and the organization might be content. If another organization had the same overall assessment of 5, but viewed

[1] Since assessment and importance values are usually above 4, we show the range 3 to 7 on the graph.

[2] Since construct gaps are usually less than 2.0, we display gap values in multiples of 0.5 from 0 to 2.5.

that construct's importance as being 6, the gap of 1 might indicate an area for improvement.

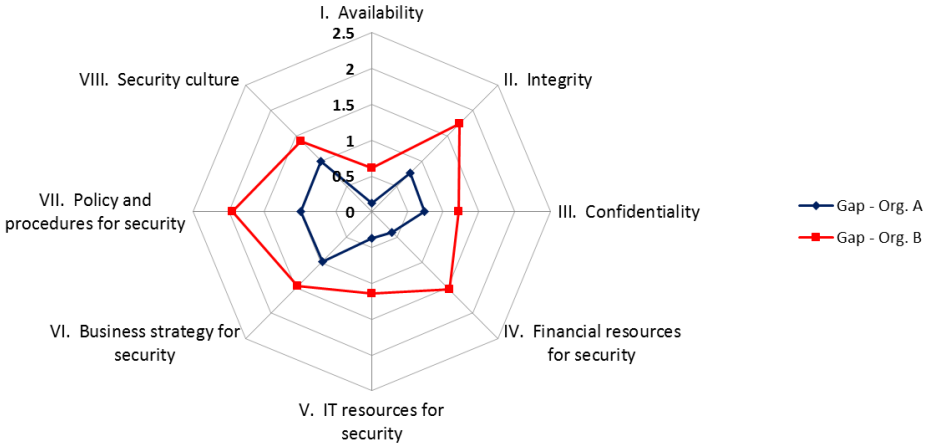


**Fig 4.** Gap analysis in organizations A and B (gap = importance – assessment)

For the rest of this paper, we discuss the results of stratified construct analysis along other dimensions, such as level within the organization or functional area within the organization.

## Construct Analysis

Fig 5-A shows the distribution of cybersecurity perceptions (i.e., construct assessment levels) based on the organizational level of the respondents: from executive level, to line managers, to professionals. Significant differences can be seen: Executives giving generally lower assessments, professions and middle managers in the middle, and "Others" with highest assessments.

Although ratings of assessment and importance are individually important, the size of the gaps can provide more insights (see Fig 5-B). The results show that top-level executives tend to have much higher gaps, across almost all constructs, than middle management and non-management personnel. This disparity in perceptions may imply that executives are more dissatisfied with the security situation in their organizations. Perhaps executives think situations are worse than they really are because they do not understand how and whether security measures are being correctly implemented. Or alternatively, executives might see problems that people in other roles do not see and, as a result, their perceptions of a security gap are higher

Overall, the sample sizes in this pilot study are small; hence, we use these findings to illustrate some of the issues that we expect will be significant

in our larger study. We are currently conducting a large-scale study to better compare the results across various organizational levels. Follow-up studies and case studies would also help further clarify the underlying causes of differences in perceptions.

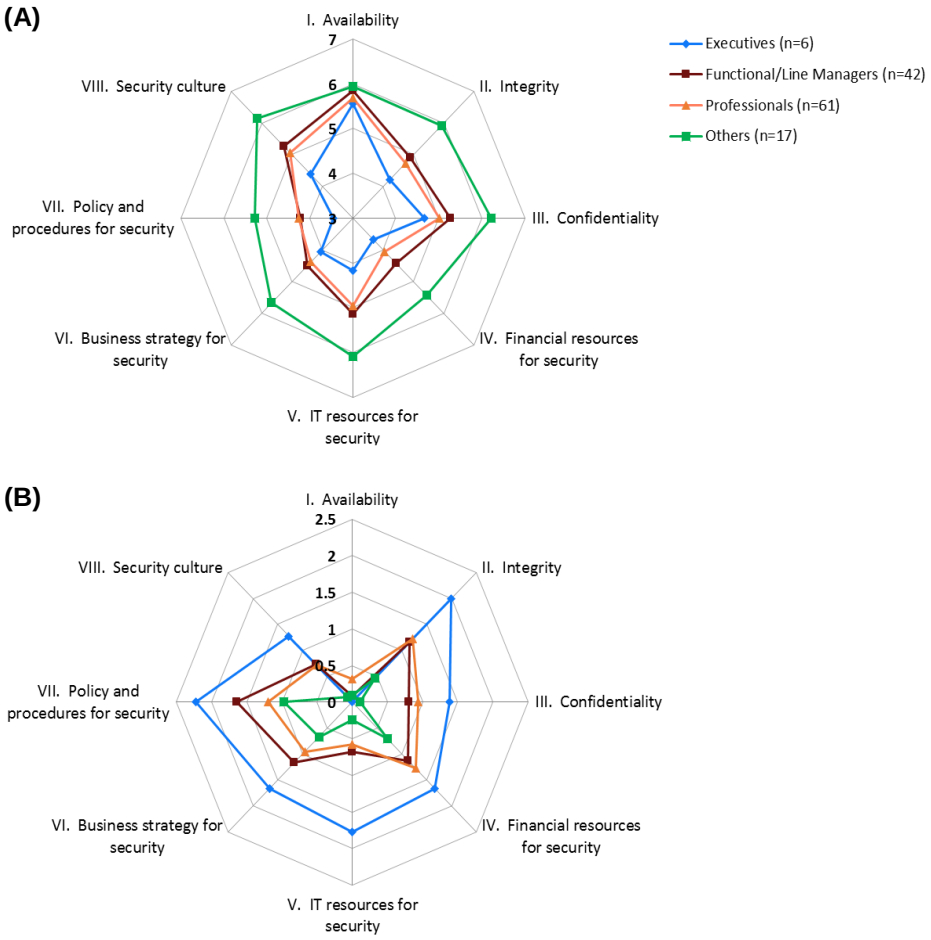


**Fig 5.** Assessment levels (A) and gaps (B) by organizational levels in organizations.

Fig 6 presents the gaps among IT, OT, and other areas in organization (such as Marketing, Finance, etc.) Interestingly, OT staff generally have higher gaps across the eight constructs. This is consistent with the frequent mention of IT/OT cultural gaps.

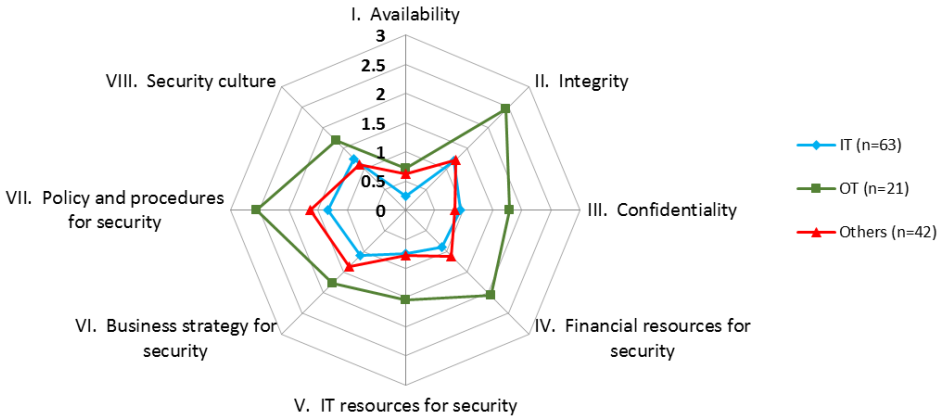


**Fig 6.** Gaps based on functional areas: information technology (IT), operational technology (OT), and other areas

## Conclusion

In order to identify security strategies and cross-organizational trends, we analyzed perceptions of importance and assessment for the eight security constructs of the House of Security. In addition to being a unique way to study organizational aspects of cybersecurity, this study sheds some light on perceptions, which are important, since they are the foundations of decision-making in an organization. We believe that the results of this pilot study and our follow-up large-scale study will have important implications in a number of areas, including assessment of an organization's cybersecurity needs, marketing of cybersecurity products, and development of an organization's cybersecurity technologies and policies, which is increasingly important in the renewable energy industry.

**Opportunity to participate in our large-scale research -** Using respondents from these two organizations, this research allowed us to conduct a pilot study using the survey instrument and analyze the constructs and gaps. In order to improve the comparisons, increase the generalizability of the findings, and study other dimensions, such as differences among industries, we are developing a larger dataset. We invite you and your organization to participate in our confidential organization benchmarking exercise, similar to organizations A and B in this paper. If you would like more information about this opportunity, please contact the corresponding author.

**Acknowledgement -** This research was conducted by the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, also known as MIT-(IC)$^3$. This material is based, in part, upon work supported by the Department of Energy under Award Number DE-OE0000780. We thank those who participated and provided the survey data. Early research was supported, in part, by Cisco Systems, Inc. through the MIT Center for Digital Business.



## References

1. Gharavi, H., Ghafurian, R.: Smart grid: The electric energy system of the future. IEEE (2011)
2. Liu, J., Xiao, Y., Li, S., Liang, W., Chen, C.P.: Cyber security and privacy issues in smart grids. IEEE Communications Surveys & Tutorials 14, 981-997 (2012)
3. Pearson, I.L.: Smart grid cyber security for Europe. Energy Policy 39, 5211-5218 (2011)
4. Boneh, D., Franklin, M.: Identity Based Encryption From the Weil Pairing. Siam Journal of Computing 32, 586-615 (2003)
5. Dolev, D., Yao, A.: On the Security of Public Key Protocols. IEEE Transactions on Information Theory 29, 198-208 (1983)
6. Needham, R.M., Schroeder, M.D.: Using Encryption for Authentication in Large Networks for Computers. Communications 21, 993-999 (1978)
7. Cheswick, W.R., Bellovin, S.M., Rubin, A.D.: Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley (2003)
8. Oppliger, R.: Internet Security: Firewalls and Beyond. Association for Computing Machinery 40, 92-103 (1977)
9. Zwicky, E., Cooper, S., Chapman, D., Ru, D.: Building Internet Firewalls. O'Reilly & Associates (2000)
10. Furnell, S.: Cyber Threats: What Are the Issues and Who Sets the Agenda? In: SGIR Conference. (Year)
11. Kephart, J., Sorkin, G., Chess, D.W., S.: Fighting Computer Viruses. Scientific American November, (1997)
12. McCumber, J.: Assessing and Managing Security Risk in IT Systems. Auerbach Publications (2005)
13. Cronbach, L.J.: Coefficient alpha and the internal structure of tests. Psychometrika 16, 297-334 (1951)

## APPENDIX

A. In my organization, I am a/an:

- Executive (CEO, CFO, VP, etc.)
- Functional or Line Manager
- Professional (Consultant, Engineer, In-house Expert, etc.)
- Other organizational member

B. In my organization, I work in area of:

- Information Technology (IT) Security
- IT, but not Security
- Operational Technology (OT) Security
- OT, but not Security
- General / Physical Security
- Business Security Policy or Management
- Other, i.e., not in Security, IT, or OT (e.g., Marketing, Accounting, HR, etc.), Please specify: _____

Assessment Scale:

1= In my view, this security statement is true to a very SMALL extent in my organization.
7= In my view, this security statement is true to a very LARGE extent in my organization.

**Importance Scale:**

1= In my view, it is NOT at all Important that my organization address this security statement.
7= In my view, it is VERY Important that my organization address this security statement.

1. The organization's business strategy sets direction for its cybersecurity practices.
2. The organization has adequate safeguards against internal and external threats to its data and networks.
3. In the organization, cybersecurity funds are appropriately distributed.
4. In the organization, the IT group takes cybersecurity seriously.
5. The organization's data and networks are available to approved users.
6. The organization has adequate policies for when and how data can be shared.
7. The organization has adequate technology for supporting cybersecurity.
8. People in the organization carefully follow good cybersecurity practices.
9. The organization has a well-defined and communicated cybersecurity strategy.
10. Cybersecurity is a funding priority in the organization.
11. The organization uses its IT security resources effectively to improve cybersecurity.
12. The organization has adequate policies about user identifications, passwords, and access privileges.

**Assessment Scale:**

1= In my view, this security statement is true to a very SMALL extent in my organization.
7= In my view, this security statement is true to a very LARGE extent in my organization.

**Importance Scale:**

1= In my view, it is NOT at all Important that my organization address this security statement.
7= In my view, it is VERY Important that my organization address this security statement.

13. The organization adequately monitors its data and networks against possible attacks.
14. Cybersecurity is a business agenda item for top executives in the organization.
15. The organization has well-defined policies and procedures for cybersecurity.
16. People in the organization can be trusted to engage in ethical practices with data and networks.
17. The organization has procedures for detecting and punishing cybersecurity violations.
18. In the organization, business managers help set the cybersecurity strategy.

19. The organization makes good use of available funds for cybersecurity.
20. The organization provides good access to data and networks to legitimate users.
21. The organization has a rapid response team ready for action when cyber attacks occur.
22. The organization protects its confidential corporate data.
23. People in the organization are aware of good cybersecurity practices.
24. The organization's data and networks are usually available when needed.

C. What is the biggest concern that you have about cybersecurity? (need not be included in the questions above) _____

D. Any other comments or suggestions? _____

E. If you would like to receive a copy of our research results, please provide your email address:(optional) Email: _____

We thank you for your time spent taking this survey.