USTELECOM | THE BROADBAND ASSOCIATION

2023 USTELECOM CYBERSECURITY CULTURE REPORT

The State of Small and Medium-Sized Critical Infrastructure Enterprises

Table of Contents

This report compiles the findings of a survey administered to small and medium-sized enterprises (SMEs).

Executive Summary

As we see an increasing number of cybersecurity threats to critical infrastructure around the world, staying vigilant to prevent attacks is a key priority for enterprises, both large and small. Data[1] show that smaller enterprises will soon be just as likely to experience a cyberattack as larger enterprises. Thus, cybersecurity culture is a mission-critical component of modern organizational culture. It is grounded in the beliefs and attitudes employees at all levels possess toward the cybersecurity practices of their enterprise, and it manifests in the ownership they take in doing their part to remain vigilant in defense of their enterprise.

Cybersecurity culture is believed to be an accurate predictor of an enterprise's ability to prepare for and respond with confidence to a cyberattack. To take a closer look, USTelecom surveyed more than 300 small and medium-sized enterprises (SMEs) engaged in critical infrastructure work to gauge their cybersecurity culture and which factors—from IT budgets to specific company practices—have the strongest correlation to mature cybersecurity culture.

Key Findings

Culture Varies Widely By Sector And Company Size

Cybersecurity culture and practices vary widely by infrastructure sector. The IT and Communications (Comms) sectors stood out as having the strongest cybersecurity cultures, with the Comms sector scoring most consistently high across the five dimensions.

The IT, Comms, and Financial Services sectors were the most likely to perform important cybersecurity culture practices including performance appraisals, rewards for proactive behavior, training initiatives, and routine communications with internal stakeholders.

Cybersecurity culture and practices vary widely with company size. More than 9 out of 10 companies with 501-1,000 employees agreed their companies were improving cybersecurity culture, different departments could work together, and employees speak their mind to help improve cybersecurity. Less than 2 out of 3 companies with 1-50 employees agreed with these statements with regard to their own ventures.

Companies with 501-1,000 employees were also more likely to utilize several cybersecurity culture practices, including performance appraisals, rewards for proactive behavior, learning and training initiatives, and routine communications with internal stakeholders.

Revenue Doesn’t Predict Culture But Culture Predicts Preparedness

Annual revenue is not a reliable predictor of cybersecurity culture. An enterprise’s cybersecurity culture is not contingent on its annual revenue. In fact, enterprises with between $1 million and $5 million in annual revenue had nearly as many Mature cybersecurity cultures as enterprises with top annual revenues of more than $50 million. This is an important finding that suggests smaller revenue streams do not necessarily hinder small and medium-sized enterprises from achieving a strong cybersecurity culture.

Cybersecurity culture is a reliable predictor of confidence and preparedness. The data and supplemental analyses indicate that cybersecurity culture is a driving force in defending against cyberattacks. As strength and maturity of cybersecurity culture increases, so does preparedness.

Of note, the frequency of cybersecurity-related communication is significantly higher among respondents with a Mature cybersecurity culture. This insight reinforces the notion that increased communication related to cybersecurity will foster confidence, transparency and truth telling, which leads to a stronger and more mature cybersecurity culture. Higher confidence directly translates to employees knowing what to do when faced with a cyberattack and departments being capable of working together.

IT Budgets Do Not Predict Culture But Multi-Faceted Approaches Do

Size of cybersecurity and IT budgets do not significantly impact cybersecurity culture. The size of an enterprise's cybersecurity and IT budget on its own does not have a significant impact on cybersecurity culture. Additionally, enterprises in the Growing cybersecurity culture segment often spend more on cybersecurity, but these increases—largely focused on capacity building, dissipate as the enterprise graduates into a Mature cybersecurity culture.

More complex, multi-faceted budgets drive cybersecurity culture. Companies with Mature cybersecurity cultures consider a greater number of factors for their cybersecurity spending. Protecting customer data, business continuity, preventing fraud/theft, and protecting staff are the factors that most strongly influenced cybersecurity spending within organizations with a Mature cybersecurity culture.

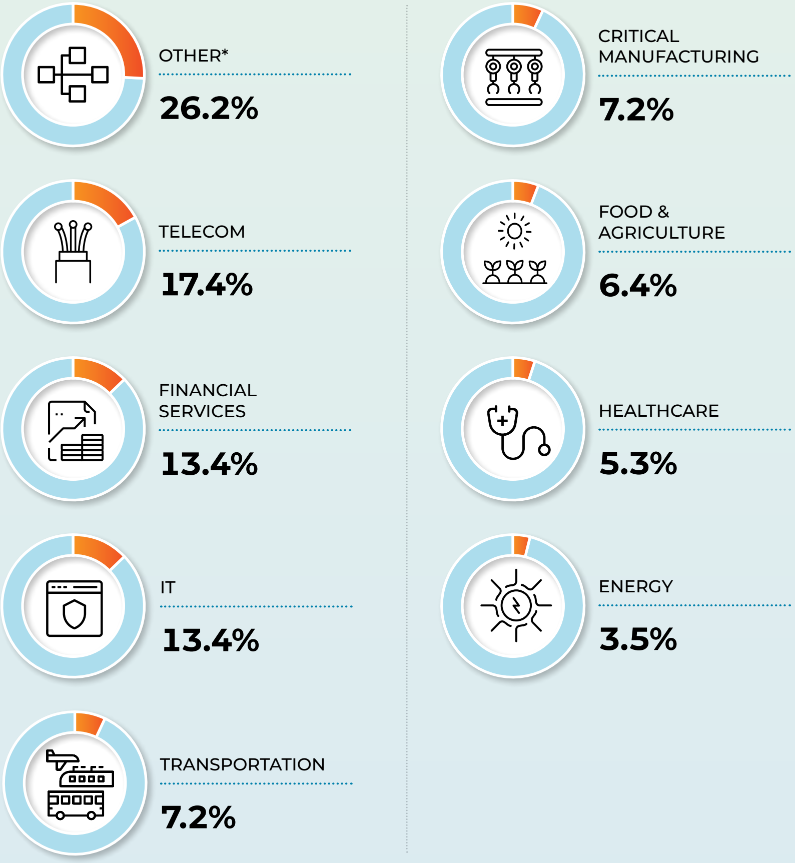
Methodology and Analytical Framework

Some 374 respondents from small and medium-sized enterprises assessed 27 statements exploring five dimensions of their organization's cybersecurity culture: *employee*, *management*, *organization*, *company* and *training*. See *Appendix A* for full survey.

Researchers used the responses to create average scores for each dimension and an overall composite score. Segmentation analysis then produced a cybersecurity culture index divided into four segments: *Mature*, *Growing*, *Emerging* and *Weak*. See *Appendix B* for details.

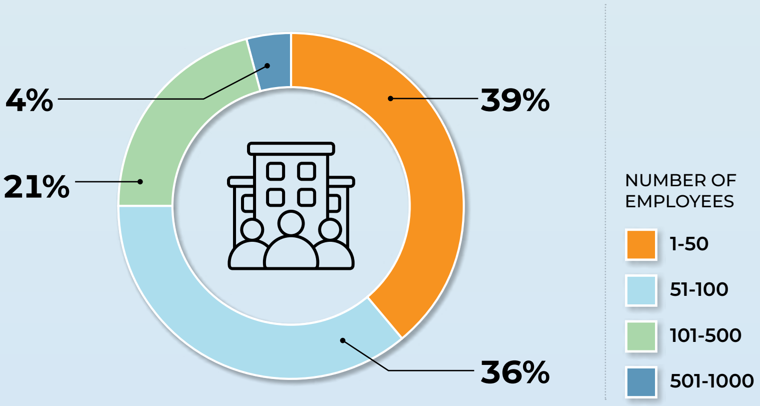
SAMPLE BREAKDOWN

Percentage of Respondents by Critical Infrastructure Sector

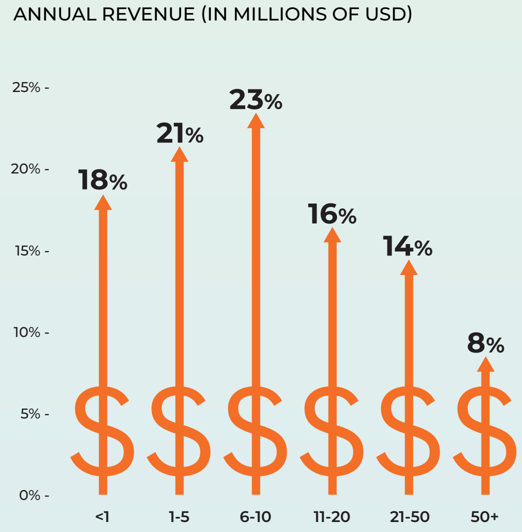


* *"Other" means a critical infrastructure sector that did not align explicitly with the 16 sectors established under Presidential Policy Directive 21 (PPD-21).*

Percentage of Respondents by Organizational Size



Percentage of Respondents by Revenue



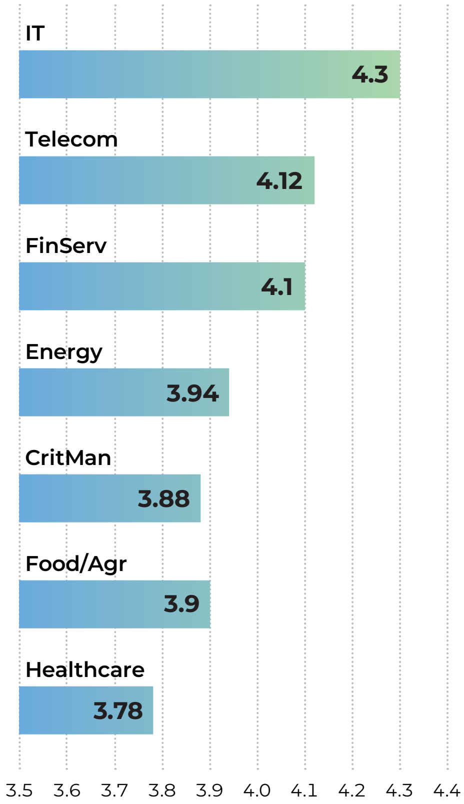
Cybersecurity culture refers to the attitudes and beliefs of people within an enterprise regarding cybersecurity and how these attitudes and beliefs manifest themselves in the behavior of employees. Cybersecurity culture is an important component of an enterprise's organizational culture, as it creates a sense of accountability in employees at all levels to ensure their enterprise is secure.

As small and medium-sized enterprises (SMEs) continue to experience increasing numbers of cyber incidents and breaches, it is crucial that these enterprises develop and strengthen their cybersecurity culture. Employing adaptable and repeatable cybersecurity practices and procedures like training and education initiatives, frequent cybersecurity related communications, and rewards for proactive behavior, are just a few of the many practices that have shown success in creating a stronger cybersecurity culture.

Cybersecurity culture is also believed to directly affect the confidence employees have when defending against a cyberattack and the overall preparedness of an enterprise. The 2021 Verizon Breach report[2] found that 82% of breaches involved the Human Element, including social attacks, errors and misuse. With cybersecurity culture playing a significant role in strengthening the human layer of security in an enterprise, building and strengthening cybersecurity culture has the potential to be the most critical success factor for small and medium-sized enterprises.

SECTION 1:
Cybersecurity Culture by Critical Infrastructure Sector

FIGURE 1:
Cybersecurity Culture by Critical Infrastructure Sector



In the first section of our findings, we look at how the critical infrastructure sector an organization belongs to can affect cybersecurity culture and practices. Respondents were asked to provide the critical infrastructure that best described the company where they worked.

The three largest infrastructure sectors within the sample are communications (Comms/Telecom) (17%), information technology (IT) (13%), and financial services (13%).

THERE ARE SIGNIFICANT DIFFERENCES IN CYBERSECURITY CULTURE AND PRACTICES BASED ON INFRASTRUCTURE SECTOR.

Within the survey, respondents provided their level of agreement (strongly agree—strongly disagree) with statements pertaining to the five cybersecurity culture dimensions: employee, management, organization, company, and training. Leveraging survey responses, average scores were created for each of the dimensions of culture within each critical infrastructure sector. Scores on each dimension range from 1 (Weak) to 5 (Strong).

The data is clear; there are significant differences in cybersecurity culture based on infrastructure sector at an overall level, composite scores across culture dimensions, and within each dimension of culture. *Figure 1* shows the composite score of each sector after averaging the dimension scores together. There are significant differences within sectors across dimensions of cybersecurity culture and that culture wanes significantly through different infrastructure sectors.

The Comms and IT sectors emerged as having the strongest cybersecurity cultures across each dimension of cybersecurity culture. The Comms sector is most consistent across the cybersecurity culture dimensions.

The data also provided detailed perspectives on nuances in cybersecurity by infrastructure sector, namely the Comms, IT, and Financial Services sectors.

COMMS SECTOR respondents agreed that:

- Their company has a strong cybersecurity culture (**98%**),
- Different departments communicate openly about cybersecurity **(93%)**,
- Employees understand the critical need to secure the organization against cyberattacks (**91%**),
- Employees in the organization know why cybersecurity is important to the business (**82%**), and
- Different departments are capable of working together to ensure cybersecurity (**81%**).

IT SECTOR respondents agreed that:

- Their company is taking actions to improve cybersecurity (**92%**),
- Their company has a strong cybersecurity culture (**90%**),
- Employees help other people comply with cybersecurity policies (**86%**),
- Employees in the organization help decrease incidents where computers are abused (**84%**), and
- Management at their organization knows their cybersecurity vulnerabilities (**82%**).

FINANCIAL SERVICES SECTOR respondents agreed that:

- Employees understand the critical need to secure the organization against cyberattacks (**84%**),
- Employees in the organization know why cybersecurity is important to the business (**84%**),
- Their company has a strong cybersecurity culture (**82%**),
- Different departments communicate openly about cybersecurity (**80%**), and
- Different departments are capable of working together to ensure cybersecurity (**80%**).

SECTION 2:
Cybersecurity Culture by Organizational Size

In this section, we look at the respondents according to their company size to gain insights on how the number of employees can affect cybersecurity culture and practices. Respondents fell into one of four groups, enterprises with 1-50, 51-100, 101-500, or 501-1000 employees. Respondents were asked to respond to statements about their enterprise using a Likert scale (strongly agree, agree, neutral/unsure, disagree, strongly disagree). Significant differences in cybersecurity culture and practices were shown when comparing enterprises based on organizational size. The results are shown in *Figure 2*.

THERE ARE SIGNIFICANT DIFFERENCES IN CYBERSECURITY CULTURE AND PRACTICES BASED ON ORGANIZATIONAL SIZE.

For example, more than 90% of respondents with 501-1000 employees agreed (both strongly agree and agree) with the following statements:

- Employees in my organization speak their mind to help improve our cybersecurity (**100%**),
- My company is improving our culture on matters of cybersecurity (**93%**), and
- Different departments within my organization are capable of working together to ensure cybersecurity (**93%**).

Respondents with less than 100 employees agreed to a lesser degree with the statements above. Nonetheless, a significant majority of respondents across all sizes agreed with the questions asked.

For example, enterprises with less than 100 employees agreed (both strongly agree and agree) with the following statements.

- Employees in my organization believe their actions are important contributions to the organization's cybersecurity (**83%**),
- Employees in my organization help other employees comply with matters of cybersecurity (**81%**), and
- Employees in my organization know why cybersecurity is important to our business (**80%**).

When asked about specific cybersecurity practices, **companies with more employees are more likely to formally assess compliance in performance appraisals, communicate with internal stakeholders, reward employees for proactive behaviors, and utilize training to build cybersecurity culture.** The full breakdown by organizational size is shown in *Figure 3*. Respondents simply agreed or disagreed (answered yes or no) to whether their enterprise performs these practices. These practices contribute to a stronger cybersecurity culture, which drives a higher level of preparedness.

FIGURE 2: Cybersecurity Culture by Organizational Size

PERCENTAGE OF RESPONDENTS WHO AGREE

	1-50	51-100	101-500	501-1000
My company is improving our culture on matters of cybersecurity.	59%	76%	83%	93%
Different departments within my organization are capable of working together to ensure cybersecurity.	60%	73%	81%	93%
Management at my organization believes cybersecurity is a priority.	73%	76%	84%	100%
Management at my organization knows our cybersecurity vulnerabilities.	67%	77%	75%	93%
Employees in my organization help other employees comply with matters of cybersecurity.	70%	81%	81%	94%
Employees in my organization help decrease incidents where computers are abused.	66%	75%	78%	93%
Employees in my organization speak their mind to help improve our cybersecurity.	62%	75%	76%	100%
Employees in my organization believe their actions are important contributions to the organization's cybersecurity.	68%	83%	74%	80%
Employees in my organization know what to do in order to ensure the organization remains cybersecure.	67%	74%	77%	93%
Employees in my organization know why cybersecurity is important to our business.	73%	80%	89%	93%

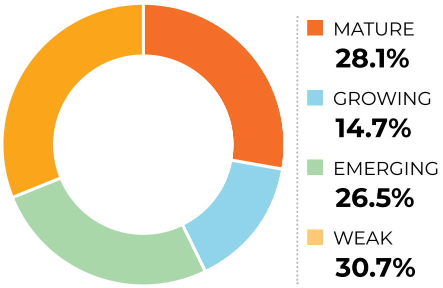
FIGURE 3: Cybersecurity Culture Practices by Organizational Size

PERCENTAGE OF RESPONDENTS WHO AGREE

"MY ENTERPRISE…"	1-50	51-100	101-500	501-1000
Assesses compliance in performance appraisals	53%	81%	70%	93%
Rewards employees for proactive behaviors	42%	59%	63%	87%
Promotes learning initiatives to build culture	57%	72%	75%	80%
Utilizes training initiatives to build cybersecurity culture	57%	65%	79%	87%
Routinely communicates with internal stakeholders	52%	61%	69%	93%

SECTION 3:
Segmentation Analysis of Cybersecurity Culture

FIGURE 4:
Cybersecurity Culture Segments



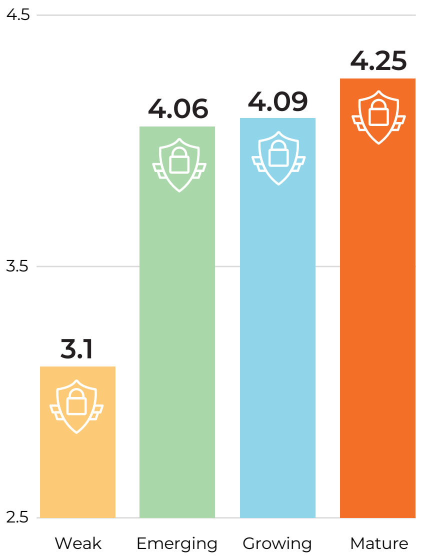
In this section, we discuss the findings gathered following the segmentation analysis of cybersecurity culture. Based on the answers provided by respondents when asked a series of questions for each of the cybersecurity culture dimension, composite-scores were created for each dimension that could range from 1 (Weak) to 5 (Strong).

From these responses, the researchers identified the **four unique categories** of Mature, Growing, Emerging, and Weak cybersecurity culture. *Figure 4* provides the size of each segment within our sample.

In *Figure 4*, we can see that enterprises in the Mature, Growing, and Emerging cybersecurity culture segments made up about 70% of the data. This means that most of the enterprises we surveyed are taking steps to strengthen their cybersecurity culture. Strengthening cybersecurity culture requires identifying an enterprise's limitations and barriers and then taking the necessary steps to overcome identified obstacles.

FIGURE 5:
Cybersecurity Culture Segment by Confidence

AVERAGE CONFIDENCE DEFENDING AGAINST ATTACKS



CULTURE IS CONFIDENCE IN CYBERSECURITY.

Confidence defending against cyberattacks increases significantly and proportionately with cybersecurity culture. **Confidence is an important indicator of how an organization will fare when faced with a cyberattack.** The more confident employees and management are, the more likely they will be able to adequately prepare for and respond to a cyberattack.

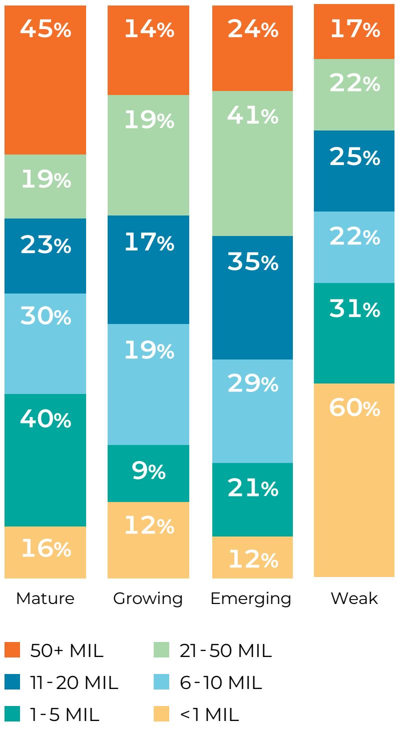
As shown in *Figure 5*, there was a dramatic increase in the average confidence level between Weak cybersecurity cultured and Emerging cybersecurity cultured enterprises. As cybersecurity culture levels continue to increase, so do employee levels of confidence. This finding suggests that organizations can see a significant growth in employee confidence as soon as they reach an Emerging level of cybersecurity culture.

Based off the questions asked in this survey, confidence translates directly to employees knowing what to do to ensure their enterprise's cybersecurity, and departments being capable of working together to ensure cybersecurity.

REVENUE ALONE DOES NOT ENSURE A STRONG CYBERSECURITY CULTURE.

Our segmentation analysis shows that the emergence of Mature cybersecurity culture is not contingent on annual enterprise revenue. Smaller organizations may not need to significantly grow their revenues to reach a Mature cybersecurity culture. As seen in *Figure 6*, while 45% of organizations that fall in the Mature cybersecurity culture segment have annual revenues exceeding $50 million, the second largest group within this segment are companies with annual revenues between $1 to $5 million at 40%. **This finding suggests that revenue size of an organization does not hinder its ability to establish a strong cybersecurity culture.**

FIGURE 6:
Cybersecurity Culture Segment by Revenue

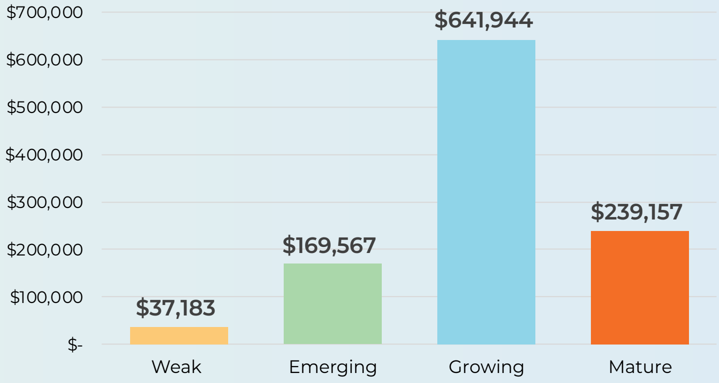


SIZE OF ANNUAL CYBERSECURITY AND IT BUDGETS DO NOT SIGNIFICANTLY IMPACT CYBERSECURITY CULTURE.

Organizations with weaker cybersecurity cultures direct less of their overall budget to IT and cybersecurity. Those in the Growing cybersecurity culture segment spend significantly more on maintaining cybersecurity, compared to other segments. However, as seen in *Figure 7*, this seems to be a temporary increase as budget allocations drop by about $400,000 as companies graduate from Growing to Mature cybersecurity cultures. The increase in budget between the Emerging and Growing cybersecurity culture segments could be attributed to necessary investments for capacity building.

FIGURE 7:
Cybersecurity Culture Segment by Budget*

TOTAL BUDGET MAINTAINING CYBERSECURITY



**75% of the respondents have less than 100 employees*

STRONG CYBERSECURITY CULTURE MEANS MORE COMPLEX, MULTI-FACETED BUDGETS.

The final key finding relating to the budgets of cybersecurity culture in the four segments of our analysis are the number of factors that influence an enterprise's cybersecurity spending. **Respondents from organizations in the Mature cybersecurity culture segment are significantly more likely to indicate that more factors influence their cybersecurity spending.**

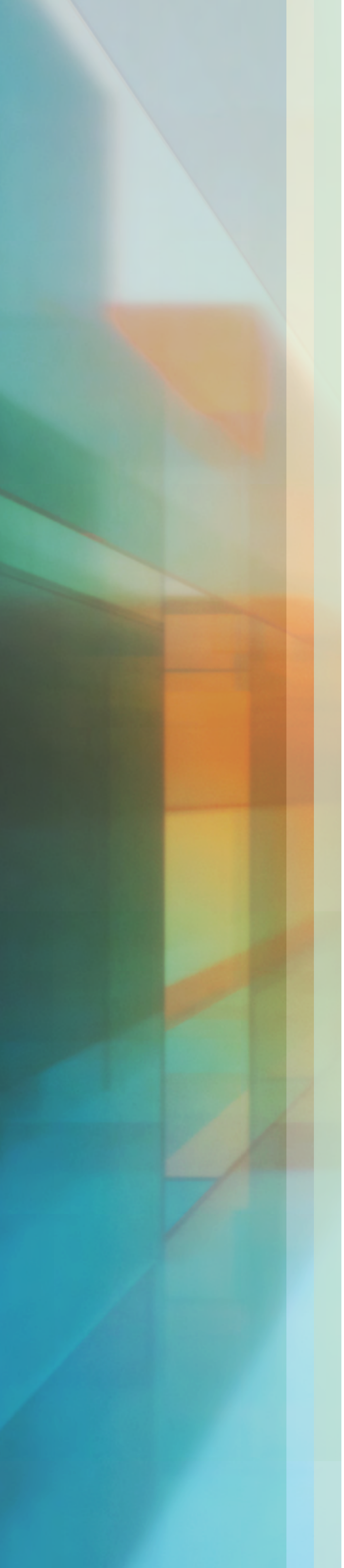
Notice in *Figure 8* the degree to which the factors that influence cybersecurity spending decreases demonstrably through the lower levels of cybersecurity culture. On average, only 17% of respondents within the Weak cybersecurity culture segment strongly agreed that any of the below factors influenced their cybersecurity culture spending.

Given that these differences are statistically significant we can confidently conclude that these differences are driven by the groups included in the analysis. The trend of the Mature segment being statistically and significantly different from all other segments persisted across virtually all metrics within the survey.

FIGURE 8: Cybersecurity Culture Segment by Spending Factors

SPENDING FACTORS	MATURE	GROWING	EMERGING	WEAK
Protecting customer data	**73%**	**49%**	30%	18%
Business continuity	**62%**	31%	30%	18%
Preventing fraud/theft	**62%**	42%	27%	24%
Protecting staff	**61%**	30%	29%	15%
Customer requirements	**59%**	**31%**	15%	10%
Protecting IP	**58%**	**42%**	32%	20%
Legal compliance	**58%**	**35%**	37%	18%
Competitive advantage	**58%**	27%	27%	12%
Protecting brand	**55%**	26%	21%	22%

Bold Text – *Denotes Statistical Significance*



Conclusion

The findings in this report demonstrate the importance of cybersecurity culture in small and medium-sized enterprises. After analyzing several variables, we were able to see which factors have the largest influence on the strength of an enterprise's cybersecurity culture. Both the critical infrastructure sector an enterprise belongs to, as well as the organizational size of an enterprise, were shown to have a significant impact on the strength of a cybersecurity culture.

A clear relationship between employee confidence and cybersecurity culture was also shown in our findings. Enterprises with a Mature cybersecurity culture benefit from a higher level of confidence among their employees. Higher confidence directly translates to employees knowing what to do when faced with a cyberattack and departments being capable of working together.

The size of an enterprise's cybersecurity and IT budget did not have a significant impact on cybersecurity culture, though enterprises with Mature cybersecurity cultures did indicate that they considered a greater number of spending factors than weaker enterprises. Top cybersecurity spending factors included protecting customer data, maintaining business continuity, preventing fraud or theft, and protecting staff.

It was also clear that strength of cybersecurity culture did not rely on an organization's annual revenue. In fact, enterprises within the second smallest revenue category had nearly as many enterprises in the Mature cybersecurity segment as enterprises with top annual revenues of more than $50 million. This finding challenges the long-held belief that enterprises need significant revenue streams to achieve a robust cybersecurity architecture.

From our survey and analysis, we can say with confidence that cybersecurity culture within small and medium-sized enterprises is an important factor in the growth and maintenance of a robust cybersecurity posture, especially in the face of growing cyber threats. Enterprises can best achieve a Mature cybersecurity culture by promoting cybersecurity practices like education and training initiatives and increasing the frequency of cybersecurity communications across all levels of their enterprise. Executive level engagement is a critical success factor as employees take their cues from the top.

Appendix A

EMPLOYEE

- Employees in my organization comply with formal organizational security policies.
- Employees in my organization help decrease incidents where computers are abused.
- Employees in my organization work to avoid violating cybersecurity policies.
- Employees in my organization understand the critical need to secure our organization against cyber-attacks.
- Employees in my organization help other employees comply with matters of cybersecurity.
- Employees in my organization speak their mind to help improve our cybersecurity.
- Employees in my organization believe their actions are important contributions to the organization's cybersecurity.
- Employees in my organization know what to do in order to ensure the organization remains cybersecure.
- When it comes to cybersecurity, employees in my organization know the difference between right and wrong.
- Employees in my organization know why cybersecurity is important to our business.

MANAGEMENT

- Management at my organization believes cybersecurity is a priority.
- Management at my organization personally invests in our cybersecurity.
- Management at my organization knows our cybersecurity vulnerabilities.
- Management at my organization understands our cybersecurity vulnerabilities.

ORGANIZATION

- My organization values the protection of our information and data.
- Different departments within my organization are on the same page about cybersecurity.
- Different departments within my organization communicate openly about cybersecurity.
- Different departments within my organization are capable of working together to ensure cybersecurity.

COMPANY

- My company has a strong cybersecurity culture.
- My company is improving our culture on matters of cybersecurity.
- My company is taking actions to strengthen our cybersecurity culture.

TRAINING

- My organization provides formal cybersecurity training/education to employees.
- My organization provides informal cybersecurity training/education to employees.
- My organization requires employees to participate in annual cybersecurity training/education.
- My organization offers cybersecurity training/education throughout the year.
- The cybersecurity training/education offered by my organization is of good quality.
- The cybersecurity training/education offer by my organization impacts employee behavior.

MATURE

The mature cybersecurity culture segment made up 28% of the sample. Mature is an appropriate term to describe the cybersecurity culture within this segment as the data indicated an established strength across each dimension of cybersecurity culture. Respondents fitting within this segment scored significantly higher on each dimension of cybersecurity culture compared to other segments. Respondents within the mature cybersecurity culture perceived the culture as being strong on each of these dimensions.

GROWING

The growing cybersecurity culture segment made up 15% of the sample. Growing is a fitting term for this segment as the data indicates there is strength across most dimensions of cybersecurity culture. Specifically, there is strength in the culture at the company, management, and department levels as well as in preparedness. There is a slight lag in the scores pertaining to employees and the training pertaining to cybersecurity culture.

EMERGING

The emerging cybersecurity culture segment made up of 27% of the sample. Emerging appropriately describes this segment as there is strength emerging within specific dimensions; however, there are also limitations or barriers preventing cybersecurity culture from growing and maturing within this segment.

WEAK

Finally, the weak cybersecurity culture segment made up 31% of the sample, the largest of the four segments. The term weak is a fitting description as scores across each dimension are significantly lower than all other segments and there is a wider range in scores across the cybersecurity culture dimensions suggesting there is a great deal of work to be done for organizations to shift from the weak to emerging segment.

Figure 9 at right outlines the composite-scores of each dimension for each of the four unique culture segments in our analysis.

FIGURE 9: Cybersecurity Culture Segment Characteristics

CHARACTERISTICS	MATURE	GROWING	EMERGING	WEAK
Preparedness – cyberattacks	4.6	4.3	4.1	3.4
Company	4.8	4.3	4.0	3.1
Management	4.6	4.3	4.1	3.4
Department	4.6	4.3	4.1	3.5
Employee	4.5	4.2	4.1	3.4
Personal	4.6	4.3	4.1	3.6
Training	4.5	4.1	3.9	3.1

Numbers represent composite-scores within each cybersecurity culture dimension; range from 5 (Strong) to 1 (Weak).

Acknowledgements

USTelecom

Robert H. Mayer
Senior Vice President,
Cybersecurity & Innovation

Contributors

Paul Eisler
Vice President, Cybersecurity

Brianna L. Bace
Intern

Survey Partner | CyberRx

Survey Lead

Dr. Dustin Williams
Research Psychologist

Contributor

Ola Sage
CEO

ENDNOTES

[1] Widup, S., Pinto, A., Hylender, D., Bassett, G. & Langlois, P. (2021). 2021 Verizon Data Breach Investigations Report. Verizon. https://www.verizon.com/business/resources/reports/dbir/

[2] Widup, S., Pinto, A., Hylender, D., Bassett, G. & Langlois, P. (2021). 2021 Verizon Data Breach Investigations Report. Verizon. https://www.verizon.com/business/resources/reports/dbir/

USTELECOM | THE BROADBAND ASSOCIATION

USTelecom.org