Building Cyberresilience From Collaborative Culture

Também disponível em português
www.isaca.org/currentissue

Despite growing investment in cyberprotection measures, the incidence of data breaches and cyberattacks continues to rise. Global cybercrime costs are expected to grow by 15 percent per year over the coming years, reaching US$10.5 trillion by 2025, up from US$3 trillion in 2015.[1] In 2021, the US Federal Bureau of Investigation (FBI) reported that there were 847,376 complaints of suspected Internet crime—a 7 percent increase from 2020—and losses exceeding US$6.9 billion.[2]

Cybercriminals are continually exploiting human weaknesses and loopholes in technology, and new attack methods constantly challenge existing solutions. For this reason, traditional cybersecurity approaches to protecting enterprises from cyberattacks have become ineffective.[3,4] To detect and withstand a cyberattack, businesses and technology leaders are continuously developing security strategies to protect the high-risk IT environment, keep data protected and maintain service delivery.[5,6,7,8]

In essence, they need to be cyberresilient. The US National Institute of Standards and Technology (NIST) defines cyberresilience as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."[9] Enterprises must have a comprehensive approach that involves establishing both robust security measures to prevent attacks, and plans and procedures to respond to and recover from attacks.[10] This includes incident response planning, business continuity planning (BCP) and disaster recovery planning (DRP). It also involves testing and updating these plans regularly to ensure that they are effective and relevant, establishing cybersecurity awareness and training programs for employees, and regularly testing the entire enterprise's preparedness.

An Agile approach is a great way to develop incident response plans. It allows for quick and efficient development of plans that can be adapted to rapidly changing conditions in a collaborative effort. When cyberattacks occur, incident response teams need to gather the relevant stakeholders around the table—IT security professionals, risk analysts, senior executives, legal professionals, the audit and compliance unit, human resources (HR) and communication professionals—to produce a robust and integrated response. In this dynamic situation, collaboration is the most critical element of a cooperative and effective response. It allows teams to be more flexible when developing plans and can ensure that the plans are able to handle any unforeseen incidents. Therefore, having a culture of collaboration in the workplace that values the idea that collective intelligence drives the most creative solutions is crucial to cyberresilience. Sharing threat intelligence and incident information with other enterprises in the same industry can uncover common threats and vulnerabilities, and collaboration with government and law enforcement agencies can lead to a better understanding of the threat landscape and assistance in responding to cyberattacks. Overall, collaboration allows enterprises to better understand the threat landscape, effectively deploy resources to deter threats, respond to attacks more effectively and recover more quickly.

The Agile Approach to Resilience

Because the threat landscape is constantly changing, enterprises must become more dynamic in their handling of cyberthreats and cyberincidents and use an Agile approach to improve their cyberresilience.[11]

JOSEPH CHENG | CISA, CRISC, CPA, MACS CP

Is an internal audit manager at the department of communities and justice in New South Wales, Australia. He has more than 20 years of experience in IT, IS audit, cybersecurity and governance. Cheng is also a member of the Australian Computer Society.

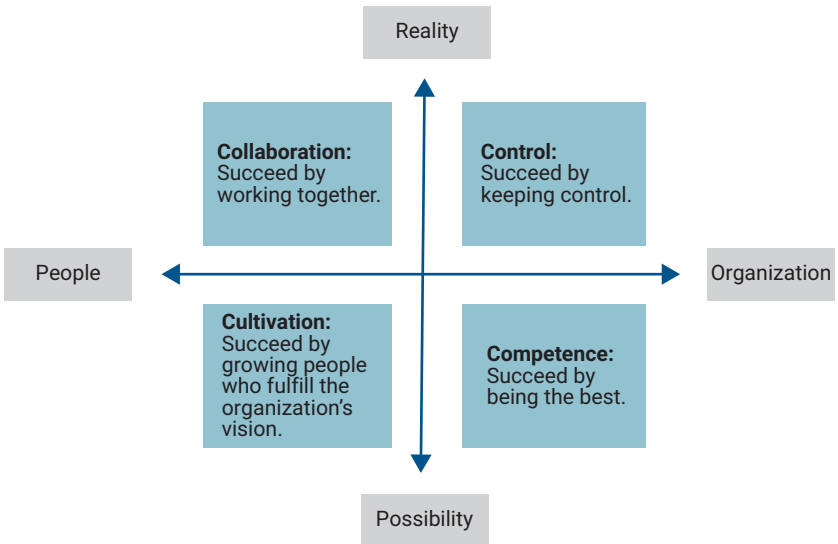
Collaboration allows enterprises to better understand the threat landscape, effectively deploy resources to deter threats, respond to attacks more effectively and recover more quickly.

Agility is the ability to respond to change. It is an effective way of dealing with an uncertain and turbulent environment. Agility represents an adaptive response to change. It helps people make sense of the current environment, identify uncertainties and adapt to them.[12]

Agility requires high levels of collaboration and flexibility. Teams must develop an Agile mindset—a thought process that involves understanding, collaborating, learning and staying flexible.[13] This approach sets up a strong framework for managing any adverse situation.

For example, sophisticated cybercriminals target staff through rapidly changing attack vectors, including social engineering. Therefore, security awareness programs and security protection measures must be threat focused and capable of quick adjustment to handle the ever-changing nature of cyberthreats and become more resilient over time.

FIGURE 1
Schneider Culture Model



Agility must be an enterprisewide goal for it to be effective.[14, 15] It requires employees to support change rather than resist it. An enterprise needs to encourage positive group dynamics and an enterprise culture in which employees can trust one another, enabling them to make collective decisions and be held accountable for the outcomes.

To become Agile, an enterprise must:

- Have a collaborative culture that enables the team to work together on a common goal, with members each doing their own part to collectively create a single product or solution.
- Have a strong management team to lead the effort and take the initiative.
- Set up a clear communication strategy for the response team and define the roles and responsibilities of each member.
- Establish a team structure that enables rapid decision-making, including the allocation of resources during an incident.
- Provide employees with the appropriate technology and security training to minimize risk and prevent vulnerability.[16]

Organizational Culture

Organizational culture is another critical component of cyberresilience. It is a collection of norms, values, expectations and standards that guide the behavior and actions of employees. The shared values and beliefs created by management shape employees' behaviors and perceptions.[17] According to the Schneider Culture Model (**figure 1**), there are four types of organizational culture: collaboration, control, competence and cultivation.[18, 19]

Collaboration culture is about building positive and trusting relationships among employees. This culture values teamwork and partnership to maximize employee knowledge and capabilities. It creates opportunities for teams to work toward common goals and fosters innovation, creativity, productivity and motivation.

Control culture is about order and stability, and decisions are made by top management. This culture values reacting to problems without wasting time on consensus-building activities. The atmosphere is hierarchical and serious, and the approach is directive.

Competence culture is about being the best. It values competition, and enterprises with this culture pursue excellence and create competitive and harsh atmospheres.

Cultivation culture is about learning and growing with a sense of purpose. Unlike collaboration, which emphasizes actuality, cultivation focuses on growth potential and possibilities. This culture is very personal and emotional in nature.

Collaboration and Cyberresilience

Enterprises with collaborative cultures encourage team members to work together by using their individual knowledge and capabilities to achieve common goals. When employees work together efficiently, job satisfaction, productivity and creativity improve. Therefore, embedding collaboration in the organizational culture is critical for cyber resilience.[20]

Collaboration involves open communication, shared decision-making and a willingness to consider and incorporate the ideas and perspectives of others. Collaboration often leads to more effective solutions and better outcomes than working alone. When employees are unwilling to collaborate, it can manifest as poor communication, resistance to the ideas of others and a focus on individual goals rather than collective ones. This can lead to inefficiencies, delays and suboptimal outcomes.

Collaboration with external partners, such as other enterprises and government agencies, can be a critical means of sharing information and resources to improve cyberresilience.

In particular, collaboration among different departments within an enterprise is critical for effective incident response and BCP. For example, the IT department is responsible for identifying and containing a cyberattack, the communications department is responsible for informing stakeholders

and the media, and the operations department is responsible for restoring production and filling customers' orders. Therefore, collaboration among these departments is essential to ensure a coordinated and effective response.

Collaboration between enterprises is also important. Sharing threat intelligence and incident information with other entities in the same industry can expose common threats and vulnerabilities. Collaboration with government and law enforcement agencies can lead to better understanding of the threat landscape and more robust assistance in responding to cyberattacks. Overall, collaboration helps enterprises better understand the threat landscape, respond to attacks more effectively and recover more quickly.

Collaboration can support a defense-in-depth (DiD) approach by allowing multiple parties to share information and resources, which leads to a more comprehensive understanding of potential threats and vulnerabilities and the development of more effective security measures and incident response plans. In addition, collaboration can facilitate the sharing of best practices and the development of industrywide standards, which can improve the overall security posture of an enterprise or an entire industry. Enterprises can collaborate to develop and share threat intelligence that can be used to update cybersecurity strategy.

Effective collaboration can enhance an enterprise's ability to withstand and recover from a cyberattack. Collaboration among different departments, such as IT, legal and HR, can ensure that all aspects of a cyberincident are addressed. Collaboration with

external partners, such as other enterprises and government agencies, can be a critical means of sharing information and resources to improve cyberresilience. In addition, having an internal culture of collaboration can foster a sense of shared responsibility for cybersecurity, which can lead to better decision-making and more effective incident response. Therefore, combining the use of technology and collaboration can be extremely effective in improving cyberresilience.[21]

> Culture cannot be easily quantified, but a good collaborative culture produces behaviors that are trackable.

How to Develop a Collaborative Culture

An enterprise can take five simple steps to build a collaborative culture, enabling it to tackle any threat, cyber or not:[22]

1. **Lead from the top**—Business leaders must create an inclusive environment that energizes teams, stimulates creativity and promotes a work culture that is both productive and joyful. Collaborative leaders seek a range of opinions and ideas from teammates to build strategies and solve problems.[23] As a result, employees feel engaged and trusted, and they are more likely to take ownership of their work.
2. **Get the right people involved**—Collaboration is all about how people interact. The most essential ingredient of a successful collaborative culture is having the right individuals in place and setting up teams that are likely to collaborate effectively and efficiently to get the best possible outcomes.
3. **Create an environment of trust and transparency**—To foster and stimulate productive collaboration, enterprises need to provide a safe environment where employees can communicate openly and honestly, provide and receive constructive feedback, and form meaningful bonds with one another.
4. **Help employees develop friendships and bonds**—Having friendly relationships at work makes people more engaged, more open to sharing their ideas and more willing to take on new challenges as a team. Creating a sense of belonging among colleagues enhances the effectiveness of cross-functional collaborative teams, allowing them to handle crises and resolve issues more effectively and efficiently. This can have a positive impact on team dynamics and productivity as a whole.
5. **Encourage and recognize collaborative actions**—Recognizing and valuing employees' contributions can make them more engaged. Studies have demonstrated a positive correlation between employee recognition and their engagement and performance.[24]

How to Measure the Maturity of a Collaborative Culture

Culture cannot be easily quantified, but a good collaborative culture produces behaviors that are trackable. The main characteristics of a healthy collaborative culture are:

- A clear vision that is evident in every activity
- Trust
- Participation by everyone
- A commitment to shared decision-making and problem solving
- Direct communication

Measuring collaboration within an enterprise can be accomplished through a variety of methods including:

- **Surveys**—Asking employees how they perceive collaboration within the enterprise can provide valuable insights. Questions can focus on topics such as communication, trust and teamwork.
- **Interviews**—Conducting interviews with employees and managers can provide a more in-depth understanding of the enterprise's collaborative culture.
- **Observation**—Observing workplace interactions and communication can provide information about the level of collaboration and teamwork.
- **Performance metrics**—Measuring the performance of teams and projects can provide information about the effectiveness of collaboration, such as:
  - **Participation rate**—Measuring the percentage of employees who actively participate in collaborative activities or tasks
  - **Engagement rate**—Measuring the percentage of employees who are actively engaged in collaborative activities or tasks

LOOKING FOR MORE?

- Read *In Pursuit of Digital Trust. www.isaca.org/digital-trust*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

  - **Quality of collaboration**—Measuring the quality of the collaborative process and output
  - **Time savings**—Measuring the amount of time saved by employing a collaborative approach
  - **Innovation**—Measuring the level of innovative thinking and solutions generated by the collaborative process
- **Collaboration software analytics**—In enterprises that use collaboration software such as Microsoft Teams or Zoom, collaboration can be measured by analyzing the number of messages, files shared and meeting frequency.

It is important to use a combination of methods to get a comprehensive understanding of the enterprise's collaborative culture. In addition, it is important to remember that culture is complex and multifaceted, so enterprises should examine all aspects of culture rather than focusing on one element or one metric.

Conclusion

Cyberattacks can have an enormous impact on an enterprise. They affect not only IT, but also the business as a whole and its customers. Therefore, a multidisciplinary team approach that involves all relevant stakeholders—risk, IT, executive board, legal, compliance, communications, finance and HR—is required to develop an incident response strategy. With a strong cyberresilience strategy, an enterprise can detect and defend against cyberattacks, produce a robust and integrated response to crises, and recover from cyberincidents.[25]

To protect themselves from cyberthreats, enterprises should employ an Agile approach to cyberresilience. Cyberresilience should be an active process, and adjustments should be made when new cyberthreats are identified.

The best way to bring together an effective interdisciplinary team to manage the dynamic cyberthreat landscape is to foster a collaborative culture in the workplace; one that encourages employees to share their knowledge and work toward common goals.[26] Once employees develop a sense of belonging, collective intelligence from team members can deliver creative solutions to solve problems and deal with crises.

Once employees develop a sense of belonging, collective intelligence from team members can deliver creative solutions to solve problems and deal with crises.

Endnotes

1 Morgan, S.; "Cybercrime to Cost the World $10.5 Trillion Annually By 2025," *Cybercrime Magazine*, 13 November 2020, *https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/*

2 Federal Bureau of Investigation (FBI), *Internet Crime Report 2021*, USA, 2021, *https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf*

3 Maurer, T.; K. Taylor; T. Grossman; *Capacity-Building Tool Box for Cybersecurity and Financial Organizations*, Carnegie Endowment for International Peace, USA, 2019, *https://ceipfiles.s3.amazonaws.com/pdf/FinCyber/English/FinCyber+Full+Toolbox_final.pdf*

4 Roege, P. E. *et al.*; "Bridging the Gap From Cyber Security to Resilience," *Resilience and Risk*, Springer, UK, 2017, *https://link.springer.com/chapter/10.1007/978-94-024-1123-2_14*

5 Conklin, W. A.; A. Kohnke; "Cyber Resilience: An Essential New Paradigm for Ensuring National Survival," *Proceedings of the 13th International Conference on Cyber Warfare and Security (ICCWS)*, National Defense University, Washington DC, USA, 2018

6 Moura, J.; D. Hutchison; "Cyber-Physical Systems Resilience: State of the Art, Research Issues and Future Trends," 2019, *https://www.researchgate.net/publication/335173978_Cyber-Physical_Systems_Resilience_State_of_the_Art_Research_Issues_and_Future_Trends*

7 Linkov, I.; A. Kott; "Fundamental Concepts of Cyber Resilience: Introduction and Overview," *Cyber Resilience of Systems and Networks, Springer International*, USA, 2018, *https://link.springer.com/chapter/10.1007/978-3-319-77492-3_1*

8 Yano, E.; W. de Abreu; P. Gustavsson; R. Åhlfeldt; "A Framework to Support the Development of Cyber Resiliency With Situational Awareness Capability," *Proceedings of the 20th International Command and Control Research and Technology Symposium*, Annapolis, Maryland, USA, 2015

9 Ross, R. *et al*.; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160, vol. 2, rev. 1. *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, USA, 2021, *https://doi.org/10.6028/NIST.SP.800-160v2r1*

10 Abraha, C.; R. R. Sims; "A Comprehensive Approach to Cyber Resilience," *MIT Sloan Management Review*, 16 March 2021, *https://sloanreview.mit.edu/article/a-comprehensive-approach-to-cyber-resilience/*

11 Hult, F.; G. Sivanesan; "What Good Cyber Resilience Looks Like," *Journal of Business Continuity and Emergency Planning*, vol. 7, iss. 2, 2014

12 Agile Alliance, "Agile 101," 2022, *https://www.agilealliance.org/agile101/*

13 *Op cit* Hult and Sivanesan

14 *Ibid*.

15 Van't Wout, C.; "Develop and Maintain a Cybersecurity Organisational Culture," *ICCWS 2019 14th International Conference on Cyber Warfare and Security*, 2019

16 Conklin, W. A.; D. Shoemaker; "Cyber-Resilience: Seven Steps for Institutional Survival," *EDPACS*, vol. 55, iss. 2, 2017, p. 14–22

17 Tohidi, H.; M. Jabbari; "Organizational Culture and Leadership," *Procedia—Social and Behavioral Sciences*, vol. 31, 2012, *https://doi.org/10.1016/j.sbspro.2011.12.156*

18 Schneider, W. E.; "Productivity Improvement Through Cultural Focus," *Consulting Psychology Journal: Practice and Research*, vol. 47, iss. 1, 1995, p. 3–27, *https://doi.org/10.1037/1061-4087.47.1.3*

19 Kropp, M.; A. Meier; R. Biddle; "Agile Practices, Collaboration and Experience," PROFES 2016: Product-Focused Software Process Improvement, Springer, Switzerland, 2016, *https://doi.org/10.1007/978-3-319-49094-6_28*

20 Harris, A.; "Exploring the Agile System Development Best Practices Cybersecurity Leaders Need to Establish a Cyber-Resilient System: A Phenomenological Study," Colorado Technical University, Colorado Springs, Colorado, USA, 2019

21 Brown, S.; J. Gommers; O. Serrano; "From Cyber Security Information Sharing to Threat Management," *Proceedings of the 2nd Association for Computing Machinery Workshop on Information Sharing and Collaborative Security*, Denver, Colorado, USA, 2015, *https://doi.org/10.1145/2808128.2808133*

22 Edmonson, S.; "Creating a Collaborative Culture," Annual Meeting of the National Council of Professors of Educational Administration, Austin, Texas, USA, 2001

23 Brunner, C. C.; "Exercising Power: Authoritarian and Collaborative Decision-Making," *School Administrator*, vol. 54, 1997, p. 6–9

24 Anitha, J.; "Determinants of Employee Engagement and Their Impact on Employee Performance," *International Journal of Productivity and Performance Management*, vol. 63, iss. 3, 2014, p. 308–323, *https://doi.org/10.1108/IJPPM-01-2013-0008*

25 Annarelli, A.; F. Nonino; G. Palombi; "Understanding the Management of Cyber Resilient Systems," *Computers and Industrial Engineering*, vol. 1, iss. 49, 2020

26 *Op cit* Brunner