UNDERSTANDING THE TALENT MANAGEMENT INTRICACIES OF REMOTE CYBERSECURITY TEAMS IN COVID-19 INDUCED TELEWORK ORGANIZATIONAL ECOSYSTEMS

Darrell Norman BURRELL
The Florida Institute of Technology, Melbourne, Florida, USA
dburrell2@thechicagoschool.edu

ABSTRACT

The unanticipated disruption triggered by Coronavirus, also known as COVID-19, has accelerated the shift to virtual workplace ecosystems for employees in the government, business, and the military. The accelerated move to whole organization telework has also created new complex challenges around managing cybersecurity risks. Complex business and governmental organizational ecosystems have several significant and critical job tasks around cybersecurity. These roles have the involved responsibility of functioning as effective teams to handle incident responses, intrusion evaluations, crisis management, crisis communications, forensic data examinations, malware analyzations, firewall assessments, penetration testing, disaster recovery, emergency response planning, risk management, human factor analyzation, training assessment, and active network monitoring. This qualitative research study explores the nuances of employee engagement, organizational development, and the management of virtual and remote cybersecurity teams in ways that enhance complex business and organizational ecosystems in the world of professional practice.

KEYWORDS: cybersecurity, organizational behavior, remote teams, team management, virtual work groups, COVID 19, telework

1. Introduction

The disruption triggered by Coronavirus, also known as COVID-19, has accelerated the shift to virtual remote business workplace ecosystems for all employees. The move to telework has also created new organizational challenges around managing cybersecurity risks. As a result of the changing nature of work, many organizational managers lack the expertise and experience in effectively managing remote teams. Business organizational ecosystems with a competitive advantage successfully leverage both current technology and human resources to enhance their ability to engage in effective risk management and information security (Larrimore, 2018). As a result, many organizations are using virtual teams as a cost-effective way to access and distribute knowledge expertise across the organization (Agbi, 2018).

DOI: 10.2478/raft-2020-0028

2. Research Methodology

The focus of the research is on cybersecurity and information technology job roles. The approach used a content analysis review of current and very recent literature around virtual teams, cybersecurity teams, and team success. The databases and their hosts (shown in parentheses) included ABI Inform Complete (ProQuest), Baidu Scholar, CNKI Scholar, Semantic Scholar, Polska Bibliografia Naukowa**,** Academia.edu, Research Gate, Academic Search Premier (EBSCO), Business Source Premier (EBSCO), ERIC (EBSCO), and Google Scholar. Usage of these databases allowed a degree of assurance about the authority of the data retrieved and that the research went through rigid, meticulous, and controlled evaluation systems, which are the brands of scholarly research and writing. Historical data located through Internet searches was consequently confirmed through explorations using academic databases. The study employed the use of qualitative focus group methodology was used to collect, analyze, explore data, and provide results with a goal of influencing the world of business in organizational practice.

This research used a critical and analytical review of the academic and professional literature, to establish a conceptual framework for utilizing technology to improve communication, trust, and relationship building for virtual cybersecurity teams. By exploring the complex nature of teams, especially virtual teams, an organization can improve the high failure rates that are typically associated with virtual teams.

3. Background

According to 2017, Cybersecurity Trends report organizations are increasing their spending on cybersecurity on average by 21% (National Center for Midmarket, 2017). Consider the business adage that a team is only as strong as its weakest link. When it comes to your cybersecurity team, especially those that most work virtually, this adage has tremendous organizational repercussions. Effective cybersecurity teams must respond to a variety of threats. As a result, building collaborative teams has never been more critical to the effective prevention of cyber threats (Edwards, 2018). Business organizational ecosystems that are effective in cybersecurity prevention requires team collaboration between network and cybersecurity teams (Edwards, 2018). Dysfunction between team members represents some significant dangers and risks to organizations around data security (Sousane, 2018). Effective collaborative cybersecurity teams are critical to developing an effective and holistic cybersecurity culture (Sousane, 2018). The critical organizational need for more knowledgeable employees in cybersecurity and more cohesive workplace relations has become more critical with the on-set of COVID 19.

A comprehensive cybersecurity organizational culture is one where processes, operations, computer networks, computer software applications, training, communications, and employees are focused on furthering cybersecurity and data security within organizations (Sousane, 2018). It also includes the actions, behaviors, values, norms, assumptions, perceptions, and beliefs associated with information and cybersecurity (Sousane, 2018).

Traditional employee teams are those that work at the same location and traditionally communicate and meet in person or face to face (Perkins, 2018). Virtual teams, on the other hand, engage each other using technology in ways beyond the limitations of having to be in the same physical location (Ng Lane, 2018). The utilization of virtual teams allows business organizational ecosystems to harness intellectual capital, subject matter expertise, and a diverse pool of talent and service based on specific situations or company goals without the restriction of geography

(Ng Lane, 2018). For example, an organization located in Claremont, California, could potentially leverage the human capital expertise and professionalism of an employee in Toronto, Canada, or Washington, DC, to be part of a virtual or remote cybersecurity team. The ability to leverage virtual or remote teams and opportunities becomes a vital recruiting tool for organizations looking to find expertise in cybersecurity job roles that often face shortages of cybersecurity talent.

The workforce development need is expected to increase by 18% for cybersecurity and Information security (Morgan, 2016). The potential risks of not being able to fill the jobs with cybersecurity teams that can work collaboratively together are significant, with the costs of cybersecurity breaches currently reaching $2.1 trillion around the world (Morgan, 2016).

New technologies have made it easier for professionals in different geographic locations to collaborate and communicate, which has enabled more meaningful use of virtual teams in organizations (Hagy, 2018). The formation and growth of virtual teams in organizational ecosystems indicate significant shifts in how work is accomplished and, more importantly, how members collaborate to perform and manage the work (Gelston, 2018).

Functioning as a virtual team is conceptualized on a continuum in which the more dispersed a team is, the more virtual it is (Martin, 2018; Quisenberry, 2018). The concept of a virtual team acknowledges that there will be some variation in how members interact, e.g., members may be geographically dispersed and communicate only through e-mail, voicemail or other communication technologies, they may be co-located and meet face-to-face, or they may be a combination of these (Martin, 2018; Quisenberry, 2018). In contrast to traditional face-to-face teams, working virtually has some challenges, including those around control and coordination, knowledge development and transfer, team effectiveness, and trust (Hagy, 2018).

Quisenberry (2018) stated that several types of virtual teams exist in business organizational ecosystems. They have permeated many functions, departments, and industries in various forms (e.g., cross-functional teams, project teams, account teams, product development teams, global teams, management teams, networked teams, etc.). As business organizational ecosystems become, more global and agile virtual teams are becoming just as critical traditional teams (Gelston, 2018). As a result, a virtual team can only be as effective as its ability of its team to collaborate, leverage each member's expertise, and tap into each member's experience to accomplish tasks (Gelston, 2018).

The significant benefit of the utilization of virtual teams is that talent, experience, and expertise can be leveraged and harnessed quickly from anywhere in the world based on need rather than location and without the added costs or time associated with relocation or travel (Agbi, 2018; Martin, 2018; Perkins, 2018).

Additionally, according to Martin (2018), as virtual team members span several time zones and geographies, the added benefit of virtual teams is having resources available nearly twenty-four hours a day. While viewed as an advantage to the organization, the notion of twenty-hour, round-the-clock access may be a disadvantage to the individual members (impacting work-life balance).

With the growth of global virtual cybersecurity teams, remote jobs, and telework the approach to managing and engaging employees has changed dramatically in ways that require new approaches to meetings, communications, relationship building and trust in the workplace as jobs move from face to face office locations to virtual ones (Gelston, 2018).

Corporations must now continually adapt their organizational structures and processes to meet the rapid pace of change

and complexity of a competitive global marketplace (Al Amour, 2018; Gelston, 2018). Corporations recognize technology as an essential enabler of meeting its goals through increasing organizational efficiency and reducing costs as much as possible to address the scope of change (Al Amour, 2018; Gelston, 2018). There are organizational pressures to obtain workers in locations that can supply the right types of skills at the correct cost (Al Amour, 2018; Gelston, 2018). Corporate leaders want to take advantage of pockets of expertise in various locations across the world by connecting them through utilizing communication technology (Al Amour, 2018; Gelston, 2018). As more and more corporations begin to use this strategy for organizing and communicating, the virtual team has now become a standard feature in global corporations (Al Amour, 2018; Gelston, 2018).

3.1. Virtual Teams and Collaborative Team Learning

Under Team Learning Conditions, Dechant, Marsick, and Kasl (1993) pinpoint three dimensions: Appreciation of Teamwork, Individual Expression, and Operating Principles. They believe that these conditions set the environment in which the team learning processes can effectively work with teams. Communication was seen in the literature as something important in ensuring that team members can express themselves to share their viewpoints. Based on Dechant, Marsick's, Kasl's (1993) definition of "Appreciation of Teamwork," communication appears to associate best with this dimension of Dechant, Marsick, and Kasl's (1993) model, which stresses the importance of team members needing to communicate, collaborate, and share ideas, experience, and expertise consistently. Collaborative problem solving and communication approaches between team members as a facilitator of the metacognition process (Dechant, Marsick, & Kasl, 1993). The ability to communicate and collaborate is even more critical in a virtual environment (Al Amour, 2018; Quisenberry, 2018).

3.2. Trust, Relationship Building, and Communication

The main reasons that diverse virtual teams fail are a lack of trust, lack of collaboration, and a lack of knowledge sharing (Hagy, 2018). According to Hagy (2018), trust is the main factor required to succeed in virtual teams because it is critical to team cohesiveness, communication, knowledge sharing, and engagement. Several researchers confirmed the importance of trust and communication in the leading and membership with virtual teams (Perkins, 2018; Ng Lane, 2018; Gelston, 2018; Al Amour, 2018; Agbi, 2018). Virtual teams cannot be managed the same way face-to-face teams were in the past (Colfax et al., 2009; Al Amour, 2018; Agbi, 2018). To succeed, virtual team leaders must shift paradigms and train managers to engage and communicate differently with interactions and behaviors focused on fostering collaborative communication and trust (Al Amour, 2018; Agbi, 2018). A critical element of trust is building a team culture that embodies psychological safety (Quisenberry, 2018). For team members to feel comfortable expressing their objections, the team must feel safe in its environment with no fear of retribution (Quisenberry, 2018; Edmondson, 1999). This need was represented in the literature by the work of Edmondson (1999) and termed as psychological safety or establishment of a level of university trust. In the organizational team, cultural context items such as discussing thoughts and feelings; getting to know each other; balance task accomplishment and relationship building it; and team members able to express their views appear to align with the concepts of trust, and psychological safety

(Edmondson, 1999; Quisenberry, 2018) and these elements are critical to team cohesion (Al Amour, 2018; Agbi, 2018; Quisenberry, 2018).

3.3. Data Collection

This study utilized qualitative focus group research of a collection of cybersecurity professionals that have work experience as part of a virtual team for more than two years and had at least two years of cybersecurity work experience. There were three focus groups of 6 people or a total of 18 participants. Three separate groups were used to help address issues around reliability and the validity of the results. All 18 participants were men. Fourteen of the participants were Caucasian American, and four were African-American. As a common practice in exploratory and participatory qualitative research, participant responses in direct quotes are used to elaborate and provide more context to the developed themes and research responses (Creswell, 2019).

The following represent the questions that were asked of the participants of the three focus groups.

1. What do you see as the benefits of using virtual teams for cybersecurity or information security operations in organizations?

The benefits of using virtual teams for cybersecurity or information security operations in organizations are the abilities to:

- The ability to find employee talent with the expertise and not be crippled by using just the talent around you.
- The advantage to gain a diverse set of information and ideas from people from different geographical locations, perspectives, and experiences, especially those from different countries.
- The option of deploying people from different sections of the country in case of an emergency (e.g., 911, fires, earthquakes, tornadoes) in an area.
- Virtual teams can work around the clock (according to time-zone of course), thereby maximizing time on target (pass work onto the next individual/team), internal office costs will be lower, higher employee satisfaction and work productivity, different viewpoints from people from different areas, etc.
- Participant 1 said, "You could create cybersecurity teams that could function like 24-hour seven days a week network and data security guards that could work in various areas of the country and around the world".

2. What do you see are the most critical elements of an effective virtual or remote cybersecurity team?

- Business continuity planning advantages that ensure that all critical resources of employee talent and expertise are not located in one geographical location.
- Cybersecurity expertise in a variety of critical areas.
- Risk management skills.
- Communications skills.
- Collaboration skills.
- Critical thinking skills.
- Adaptability to change skills.
- Leadership skills.
- Conflict management skills.

Participant 1 said, "The ability to tap into diverse knowledge, expertise, education, and ability of all team members are the elements of an effective virtual cybersecurity team."

Participant 2 said, "An effective virtual cybersecurity team needs, ingenuity, creativity, and innovation which includes developing new insights into situations; questions conventional approaches; encourages new ideas and innovations; designs and implements new and effective approaches."

Participant 3 said, "An effective virtual cybersecurity team must have team members that understand and keeps up-to-date on local, national, and international policies and trends that affect the organization's ability to be most secure."

Participant 4 said, "An effective virtual cybersecurity team needs to be buoyant and resilient in the way it handles pressure and is persistent even when there are challenges and impediments."

Participant 6 said, "These teams must have the ability to effectively set goals and priorities around the risks and interests of the company."

Participant 7 said, "An effective virtual cybersecurity team should be very results-oriented in ways that accountable for measurable high-quality, timely, and cost-effective results."

Participant 8 said, "An effective virtual cybersecurity team can make educated, effective, and timely decisions, even when data are limited."

Participant 9 said, "An effective virtual cybersecurity team can rapidly uncover and investigates problems in ways that generate multiple viable solutions and recommendations."

Participant 10 said, "An effective virtual cybersecurity team keeps abreast of technological developments and advances in ways that use of technology to achieve results."

3. What are the best ways to use technology to help make virtual and remote cybersecurity teams more effective?

●Communication tools can assist with meetings and sharing ideas, especially those with cameras or videos that allow participants to see each other during meetings.

●Project plans and update dashboards can be used so that all members of a team understand the critical priorities and progress on projects.

●The ability to use virtual labs and technology-driven scenario-based training to allow teams to practice working collaboratively.

●The ability to use show and tell demonstrations via a secure visual and audible software is necessary for virtual teams.

Participant 1 said, "Any technology tools that allow virtual teams to communicate and collaborate more effectively are critical to helping the cybersecurity teamwork effectively. These tools could be those like ZOOM that allow participants to have meetings where they can see each other and view documents."

4. What role do you see that communication plays in effective virtual cybersecurity team success?

●Communication is needed to have effective virtual cybersecurity team success because teams need well thought through methods to work through concerns and conflict.

●There needs to be a documented process to hand off information and make sure that all risks, methods, and approaches are understood and covered.

Participant 1 said, "Communication is vital...without, there are just a bunch of rogue employees working online in different areas and time-zones. Collaboration is critical to ensure that our areas of risk are covered and addressed".

5. What role do you think that management plays in virtual or remote cybersecurity team success?

●Managers must be supportive from the top-down as well as the bottom up.

●Management needs to understand the knowledge and skills of its team members.

●Management must maintain current business continuity plans.

●Management needs to clear any organizational barriers that would hamper the team's effectiveness.

Participant 1 said, "Management should make sure that the team has right members on it with the right talent, expertise, education, and experience required to complete the project or to work on the virtual team."

Participant 2 said, "Management can play a significant by understanding that virtual teams don't have the formal opportunities to connect. This includes the

meetings in the hallway or the ability to meet for coffee or lunch when you work in the same physical location. As a result, management can host virtual events like birthday parties using ZOOM or Go-To-Meeting conferencing technology tools. Management can schedule virtual coffee breaks using Zoom or Go-To-Meeting conferencing technology tools. Make "check-in calls" that do not have a work-related agenda to connect with team members on a personal level".

Participant 2 said, "Management needs to trust the knowledge and expertise of employees and give them autonomy by allowing them to determine the best way to organize their work. Building a culture of trust is critical to team success, and management plays a significant role in creating a culture of trust and empowerment".

Participant 3 said, "Management should create a culture of accountability for the remote team. Virtual team members need to take more individual responsibility to meet deadlines, so it is critical for someone to hold them accountable. However, virtual managers have fewer opportunities to observe their employees. This includes developing metrics that focus on results, not the number of hours worked. Still, these metrics should be developed in a collaborative or participatory manner between management and the team members to make the theme realistic and feasible".

Participant 4 said, "Management should have a project dashboard that has up to date action plans with the entire team so that everyone is aware of the status of a project at any given time. Management needs to give employees tools and the ability to access the documents they need remotely securely. Using cloud-based file-sharing software that can help everyone easily share documents and stay organized".

Participant 5 said, "Management should include all team members in the work planning stages and should clearly outline the roles and responsibilities of everyone on the team".

Participant 6 said, "Supervisors of remote teams should schedule check-ins at key milestones with individual team members to assess progress, provide feedback and coaching, and make required course corrections".

Participant 6 said, "Management sets the tone for the team...he/she needs to anticipate and be readily available for all types of project management concerns...the team will follow suit of the management team".

Participant 7 said, "Management should understand the nature of unique challenges around insolation that can diminish a remote employee's motivation. The insolation that virtual team members experience can create a climate or feelings where remote employees can lose sight of the value and significance of their contributions. Remote team members can face a lot of distractions. As a result, regular, consistent, constructive, and positive feedback is critical to keeping remote employees engaged. This can occure using video conferencing for face to face interactions".

Participant 9 said, "Management should ensure that everyone is properly trained on the tools that are used to collaborate or communicate virtually".

Participant 10 said, "Management needs to encourage a culture of open, honest, and collaborative communication. Communication is the most important part of effective virtual teams. As a result, management must set expectations; everyone should be aware of the expected time frame for responding to e-mails and voicemails. Management should consider ways to reduce unnecessary e-mails whenever possible; quick chats or instant messages are more effective. Management should ensure that virtual meetings are as effective as possible. Unnecessary and ineffective virtual meetings are a significant issue on teams. Managers of virtual teams need always to consider if a meeting is

required, and if so, set clear objectives for what needs to be accomplished".

6. How can management foster trust in a virtual or remote cybersecurity team?

●Managers must communicate with and get to know the strengths, talents, and abilities of every team member.

●Managers should provide positive accolades when possible and convey the information sincerely.

Participant 4 said, "Management needs to respect the expertise of the team, listen to their recommendations, and empower them to be part of the strategic decision-making process around cybersecurity".

7. In what ways can management foster a healthy relationship building or cohesiveness in a virtual or remote cybersecurity team?

●The manager can hold meetings to engage all team members.

●Remote team members should be given roles in meetings that are as meaningful as the roles of on-site team members.

●Managers should not make negative comments about people working remotely.

●When possible, the manager should meet with remote team members.

Participant 5 said, "Management must establish a presence by being available for any question asked, and give the teams tasks they can accomplish as a team versus just solo...allow the team to come up with ways to address any issue – this established buy-in from all participants".

8. In what ways does management have to manage a virtual cybersecurity team differently than one working in the same physical location?

●Ensure that communication is often and consistent.

●Verify that information conveyed is clear by asking questions.

●Use virtual tools to communicate (Skype, Go-to-meeting, telephone, mobile phone, VTC, etc.).

Participant 6 said, "Online teams need direction and expectations laid out for them – perhaps a little more than people in the workplace. Everyone must be productive; otherwise, the virtual team as productive. Management must also effectively manage conflict because there can be misunderstandings around communication where members on the team are using e-mail and other non-face to face communication approaches. Misunderstandings need to be managed".

9. What do you see are the most critical skills that are required to be effective working in a virtual cybersecurity team?

●Flexibility and availability. Both of which are critical because participants are in different locations and time zones.

●Effective Communication around listening and giving information.

●Expertise in the most critical areas of cybersecurity.

●Effective writing skills to document processes.

Participant 7 says, "Online teams need direction and expectations laid out for them – perhaps a little more than people in the workplace. Everyone must be productive. Otherwise, the virtual team may not be as productive as possible".

Participant 8 says, "Skills in communication, project management, technical application, self-motivation, problem management, the ability to self-learn new skills, patience, and a host of other adaptive/social skills".

10. What are the additional risks and areas of concern concerning cybersecurity because of telework and COVID -19?

Hackers are not taking off from attacks because of COVID 19, and there could even be more vulnerabilities in organizations because of the use of employee's home Internet providers and their personal computers. As a result of these new risks, organizations and cybersecurity management teams must manage these new risks while helping all remote employees with telework cybersecurity recommendations that include:

●Implement Mobile Device Management (MDM) and Mobile Application Management (MAM). These solutions can help manage and secure mobile devices and applications. These tools can also allow organizations to remotely implement several security measures, including data encryption, malware scans, and wiping data on stolen devices.

●Train employees on how to ensure that sensitive information is encrypted and safeguarded at home.

●Implement and enforce two-factor or multi-factor authentication (MFA) were a texted code or a call for verification is sent to the phone of the employee before access to the organizational network is granted.

●Ensure all computers and mobile devices that are used to access work networks are updated security patches and virus protection. There are an increasing number of Coronavirus (COVID 19)-based social engineering and malicious emails that can prey on individuals interested in the most relevant information about COVID 19.

●Implement policies that do not allow the sharing of work computers. These policies reduce the risk of unauthorized or inadvertent access to protected company information.

●Offer employees the ability to use Virtual Private Networks (VPNs) to ensure that internet utilization is encrypted and that the employee user location when assessing the company network is private

●Implement policies that sensitive organizational information should never be downloaded or saved to employees' personal devices or cloud services, including employee computers, thumb drives, or cloud services such as their personal Google Drive or Dropbox accounts (Suciu, 2020).

●Implement policies that prohibit access to company information systems while on public Wi-Fi with the use of a VPN.

4. Conclusions

Conclusions from the study are in line with emerging trends from the literature. Due to the COVID-19 pandemic, many teams who enjoyed the benefits of working in the same physical space have become virtual teams overnight. Teams dealing with an unplanned transition to remote work need help, especially with accomplishing work that requires interdependent, coordinated effort (Bendaly, 2020). Managers need to continue to remind members of the team of adapting and changing roles and responsibilities. Coordinating and ensuring everyone on the team understands these changes is a crucial responsibility of team leaders (Bendaly, 2020). Managers need to ensure the team has regular communication about what is happening with critical stakeholders, such as customers, competitors, regulators, suppliers, the broader organization, or other factors that could affect their work. Make sure everyone on the team is aware of the latest information about the situation and how it may impact individual and team goals, priorities, and plans (Bendaly, 2020).

Given the magnitude and frequency of changes in our world today, teams need to consider whether their goals and priorities should change too proactively. Once goals and priorities are clear, managers must help the team identify and plan around newly emerged obstacles, such as resource constraints. As a result, managing remote teams and teleworkers require a recalibration of employee engagement on several levels (Bendaly, 2020).

4.1. Clarifying Core Work Coverage Hours for All Employees

Most teams have expectations about team members being present and available during work hours, even for remote employees (Suciu, 2020). Before the crisis, most remote workers had a dedicated workspace and reliable childcare in place, which allowed them to meet those

expectations. In the face of our new normal, teams should explicitly review expectations about what constitutes business hours and how much flexibility team members have around working staggered shifts (Bendaly, 2020).

4.2. Having More Regular Meeting

Although managers and team leaders should not have meetings for meeting sake, contact communication with colleagues and management helps to build a cohesive team and avoid employees having feelings of isolation (Bendaly, 2020).

4.3. Setting Communications Expectations

Teams usually have preferences about how quickly members need to respond and which modes of communication should be used (Bendaly, 2020).

The increase in the occurrences and costs of cyber breaches and technologically driven crime has created some very complex workforce shortages, and workforce expertise challenges that all organizations must develop effective strategies to address (Morgan, 2016). The emergence of COVID 19 has created new complexities around cybersecurity and information security risk management (Suciu, 2020). Given the impact of new cybersecurity risks, there forms a critical need to create a cybersecurity culture that includes effective teams and processes that can address the emerging treats (Sousane, 2018; Nobles, 2018). The traditional approach taken by many organizations in safeguarding their information assets has been primarily to rely on technical controls such as hardware and software (Zuhdi, 2018). However, in today's information-risk work environments, technical controls alone are not sufficient to combat cybersecurity risks (Nobles, 2018). Organizational cybersecurity culture can be broadly described as a union of people (employees), processes, procedures, symbols, technology, training, awareness, commitment, and direct actions focused on sustaining cybersecurity within organizations (Zuhdi, 2018; Nobles, 2018).

The use of information technology and virtual teams provides substantial benefits to individuals and organizations, but it also presents significant information technology security risks or, more specifically, cybersecurity risks (Zuhdi, 2018; Sousane, 2018; Larrimore, 2018). Approaching the elements of virtual teams from a holistic perspective contributes to a strategy and the ultimate result that is called the "Virtual Team Cycle of Success" (Quisenberry & Burrell, 2012). Once leaders embrace this cycle of success and institute processes and policies centered on the theory, they stand to reap a harvest of improved performance amongst virtual teams (Quisenberry & Burrell, 2012). As the marketplace continues to evolve, more organizations will be forced to turn to virtual teams to accomplish the task and operate efficiently (Quisenberry, 2018). The organizations that discover how to lead and utilize virtual cybersecurity teams accurately will ultimately create an extremely beneficial and potentially sustainable competitive advantage for themselves (Nobles, 2018).

4.4. Darrell Burrell Self Reflection Leadership Unplanned Circumstances Adaptability Assessment

Below is a self-assessment tool developed to managers that have been forced to manage remote teams because of COVID 19. The goal of this tool is the help managers identify their strengths and find managers that need additional developmental, and organizational support concerning adaptability in an environment of constant change.

Darrell Burrell Self Reflection Leadership Unplanned Circumstances Adaptability Assessment (2020).

5=Always 4=Very often 3=Sometimes 2= Not very often 1= Rarely, if ever.

With 5 being very high and 1 being very low, circle the number that best matches your true self-assessment of your leadership adaptability skills during an unexpected and urgent situation requiring you to lead change:
5=Always 4=Very often 3=Sometimes 2= Not very often 1= Rarely, if ever

The questions should be answered in the context of unplanned and urgent circumstances in need of attention.

1. I insistently pursue crucial data, evidence, and knowledge. 5 4 3 2 1

2. I use a variety of approaches to consistently and frequently communicate information, activities, and results to stakeholders on a variety of levels. 5 4 3 2 1

3. I am proactive and not reactive in ways that necessitate initiative during unexpected and urgent conditions. 5 4 3 2 1

4. I am a critical, strategic, and clear thinker in stressful conditions. 5 4 3 2 1

5. I display emotional intelligence, emotional self-regulation, and calm during unexpected and urgent situations. 5 4 3 2 1

6. When change is needed, I embrace it quickly and focus on creating paths that help others see how the required change can occur. 5 4 3 2 1

7. I am encouraging, optimistic, and in ways that attempt to find possibilities from solving problems. 5 4 3 2 1

8. I am resourceful, innovative, and creative when it comes to problem-solving. 5 4 3 2 1

9. I am mentally strong and recover quickly from setbacks. 5 4 3 2 1

10. I behave fearlessly and take calculated risks. 5 4 3 2 1

11. I make decisions and come to conclusions in a timely and decisive fashion. 5 4 3 2 1

12. I create a clear path and vision concerning problems and solutions. 5 4 3 2 1

13. I value expertise and knowledge and am committed to continuous learning and development 5 4 3 2 1

14. I think it is imperative to display respect, authentic concern, and empathy when I work with others on complex problems. 5 4 3 2 1

15. I attempt to identify each employee's strengths and try to find projects and opportunities for them to leverage and develop and display those strengths, competencies, and abilities. 5 4 3 2 1

Add up your responses from each of the questions and calculate your scores:

65-75: Highly competent Adapter – You have the qualities necessary to lead change and respond appropriately to unexpected problems, crises, urgent circumstances. You have the skills and abilities that could allow you to assist those less skilled through mentoring and collaboration.

64-51: Serviceable Adapter – You have the qualities necessary to lead change and respond appropriately to unexpected problems, crises, urgent circumstances, but you could strengthen some areas to be more productive. Note the areas where you scored less than a five and focus your attention on improving them.

51-38**:** Slight Adapter – While you have some strong leadership qualities, you still have plenty of room for improvement to successfully lead change and respond appropriately to unexpected problems, crises, urgent circumstances by focusing on any areas where you did not score a 5. You could probably benefit from having a highly competent adapter as a mentor.

37 or less: Apprentice Adapter – You need to focus your professional development activities on enhancing the skills and abilities to lead change and respond appropriately to unexpected problems, crises, urgent circumstances through a focus on any areas where you did not score a 5. You could probably benefit from having a highly competent adapter as a mentor.

REFERENCES

Agbi, R. O. (2018*). Leadership communications strategies for enhancing virtual team performance* (Order No. 10748206), available from ProQuest Central; ProQuest Dissertations & Theses Global. (2026711541).

Al Amour, M. (2018). *Leadership for virtual teams: Perspectives on communications, leader traits, and job satisfaction* (Order No. 10828994), available from ProQuest Central; ProQuest Dissertations & Theses Global. (2072579991).

Bendaly, N. (2020). Your Team Is Now Working Remotely 5 Ways to Strengthen Communication and Team Cohesion in the COVID-19 World. *Forbes.*

Colfax, R. S., Santos, A. T., & Diego, J. (2009). Virtual leadership: A green possibility in critical times, but can it work? *Journal of International Business Research, Vol. 8,* 133-139, available at: http://www.jibs.net/, accessed on 20 April 2020.

Creswell, J.W. (2019). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. London: Sage Publication Inc.

Dechant, K., Marsick, V. J., & Kasl, E. (1993). Towards a model of team learning. *Studies in Continuing Education, Vol. 15, Issue 1*, 1-14.

Edmondson, A. C. (1999). Psychological safety and learning behavior in work teams. *Administrative Science Quarterly, Vol. 44*, 350-383.

Edwards, M. M. (2018). *Identifying factors contributing towards information security maturity in an organization* (Order No. 10746212), available from ProQuest Central; ProQuest Dissertations & Theses Global. (2018859946).

Gelston, G. M. (2018). *Virtual leadership in complex multi-organizational research and development programs* (Order No. 10829139), available from ProQuest Dissertations & Theses Global. (2058035370).

Hagy, M. R. (2018). *Trust at no sight: Establishing trust in the process rather than in the individual members of a global virtual team* (Order No. 10813764), available from ProQuest Dissertations & Theses Global. (2099573117).

Larrimore, N. P. (2018). *Risk management strategies to prevent and mitigate emerging operational security threats* (Order No. 10747292), available from ProQuest Dissertations & Theses Global. (2023213918).

Martin, K. A. (2018*). Study of productivity rates for geographically distributed agile teams* (Order No. 10826315), available from ProQuest Dissertations & Theses Global. (2057566211).

Morgan, S. (2016). African Americans Underrepresented in the Cybersecurity Field. *Forbes*, available at: https://www.forbes.com/sites/stevemorgan/2016/04/07/african-americans-underrepresented-in-the-cybersecuritv-.field/#3c1ad72915c9, accessed on 20 April 2020.

National Center for Middle Market. (2017). *Cybersecurity and the middle market: The importance of cybersecurity and how middle market companies manage cyber risks*. National Center for Middle Market, available at: http://cybersecuritycenter.middlemarketcenter.org/Media/Documents/NCMM_Cybersecurity_Report_FINAL.pdf, accessed on 20 April 2020.

Ng Lane, J. (2018). *Teams and organizing in the digital age: How team networks form and why they perform* (Order No. 10817033), available from ProQuest Dissertations & Theses Global. (2070941894).

Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *Holistica-Journal of Business and Public Administration, Vol. 9,* 71-88.

Perkins, M. J. (2018). *Organizational leadership activities that positively influence virtual employee engagement* (Order No. 10785852), available from ProQuest Dissertations & Theses Global. (2031062890).

Quisenberry, W., Burrell, D. (2012). Review of Management Innovation & Creativity. *Winter, Vol. 5, Issue 16*, 97-116.

Quisenberry, W. (2018) Exploring how emotional intelligence contributes to virtual teams: Interpretive Analysis of a Phenomenological Study. *European Scientific Journal, Vol. 14, No 5*.

Sousane, R. (2018). *Understanding federal cybersecurity culture: An expert perspective on current and ideal state* (Order No. 10785377), available from ProQuest Central; ProQuest Dissertations & Theses Global. (2030526181).

Suciu, P. (2020). COVID-19 and Computer Security, Part 2: Shoring Up Systems for Remote Workers. *Tech News World*.

Zuhdi, B. (2018). *Information security risk analysis and advanced persistent threat: A multiple case study* (Order No. 10837747), available from ProQuest Central; ProQuest Dissertations & Theses Global. (2085189586).