



# CIO Perspectives: Managing Data Risk While Remaining Productive in a Remote Workforce



# FOREWORD

As work has become more distributed and global events led to even more remote work for companies of all sizes, it is increasingly important for teams and tools to work together to get more done. Company cultures have had to make shifts to accommodate the demands laid on businesses stemming from offices being closed - and remaining closed for extended periods of time.

Unfortunately, too many companies were not able to make these pivots and either went out of business or scaled back massively. On the other hand, at Egnyte, we have seen companies grow and thrive during these trying times with intentional IT strategies to support remote work. There are numerous examples of successful businesses that adapted quickly to the new remote reality and maintained continuity. To do this, they implemented intentional strategies to keep employees productive and collaborative, while keeping their critical business content secure.

In this Mighty Guide, we are pleased to share some of these stories of IT leaders who led change during the COVID pandemic. We appreciate their candid insights of their struggles, successes and lessons learned. We hope you find them valuable to your practice as an IT leader.



**Kris Lahiri,**  
Chief Security Officer, Egnyte



In a content critical age, Egnyte fuels business growth by enabling content-rich business processes, while also providing organizations with visibility and control over their content assets. Egnyte's cloud-native platform leverages the industry's leading content intelligence engine to deliver a simple, secure, and vendor-neutral foundation for managing enterprise content across business applications and storage repositories. More than 16,000 companies trust Egnyte to enhance employee productivity, automate data management, and reduce file-sharing cost and complexity. Investors include Google Ventures, Kleiner Perkins, Caufield & Byers, and Goldman Sachs. For more information, visit [www.egnyte.com](http://www.egnyte.com)

# TABLE OF CONTENTS

## CHAPTER 1

Effective Collaboration and Communication 6

## CHAPTER 2

Managing Content Risk in a Distributed Workforce 14

## CHAPTER 3

Keep Remote Work Groups Productive 24

## CHAPTER 4

Creating a Work Culture in a Distributed Workforce 32

## CHAPTER 5

Building a Secure IT Infrastructure for a Remote Workforce 40



EGN<sup>Y</sup>TE

# There's No “Going Back,” Only **Forward.**

Secure and manage all your content across distributed teams, devices, and apps.

# MEET OUR EXPERTS



AARON YOUNG  
Summit Healthcare Regional  
Medical Center  
VP-Chief Information Officer



GARY SORRENTINO  
Zoom Video Communications  
Global Deputy Chief  
Information Officer



JAMIE GIANNA  
Partners Behavioral Health  
Management  
Chief Information Officer



KEVIN B. BOYD  
University of Chicago  
Chief Information Officer



MICHAEL MARSCHEAN  
SubCom  
Chief Information Officer



ROBERT SHEESLEY  
Wrench Group  
Chief Information Officer



TRACY HOCKENBERRY  
Salisbury Management, Inc.  
Director of IT Business Systems  
& Enterprise PMO

## CHAPTER 1

# EFFECTIVE COLLABORATION AND COMMUNICATION

Working effectively with distributed work groups requires the right combination of technology and collaboration capabilities. Some businesses have strategically built their ability to work remotely, while others have been forced into a quick transition. Regardless of how you get there, what produces effective remote collaboration and facilitates employee productivity? To find out, we asked the experts the following question:

“What are the biggest challenges to effective meetings and collaboration in remote work groups? What advice can you offer in this area?”





Gary Sorrentino, Global Deputy CIO,  
Zoom Video Communications

Gary Sorrentino is the global deputy CIO for Zoom Video Communications. He has held several IT leadership positions across the financial services industry, including global head of client cyber awareness and education at JPMorgan Chase, head of global infrastructure technology efficiencies at Citi Private Bank, global technology CFO at Credit Suisse, and North America IT controller at UBS.



“Successful companies are not just blasting out technology. They are teaching people how to use the technology to work in a new way.”

We were in the collaboration business when COVID-19 hit. We realized that we were not only sending all our employees home, we were sending all our clients home, too. I’ve seen many companies make this transition, and they typically take one of three approaches:

- They fight it. They try to muddle through with phones and email and people working independently. That’s not a successful way to move forward.
- They mimic what they did in the office but using technology. This short-term fix quickly turns into video fatigue, middle managers who don’t know how to manage a virtual staff, confusion, and inefficiencies.
- They decide to rethink how they do things. These companies think through how they are going to keep collaboration and productivity up and how they are going to keep the company’s employees working together. They are the companies who will succeed in the future.

Successful companies are not just blasting out technology. They are teaching people how to use the technology and work in a new way. Meetings do not have run for the default one hour. Not everyone has to be at every meeting. Meetings can be purpose built; then, when the purpose has been achieved, the meeting ends. ■



Jamie Gianna, Chief Information Officer, Partners Behavioral Health Management

Jamie Gianna is answering the call of technology evolution in business: He is an executive who simultaneously steers operations, workforce, and technology to better achieve customer/client satisfaction. He blends a unique set of executive competencies that focus on the organizational mission, vision, and values, challenging the “we have always done it this way” mentality.



“Secure collaboration became a hot topic, especially to ensure HIPAA compliance in our communications with providers.”

Our organization, which serves a specific population of members and a network of health care providers, has been making this transition to remote work for several years. When the COVID-19 pandemic struck, that transition was not too difficult for us. Everybody had the necessary equipment, we had collaboration tools, and we had policies and procedures in place. The biggest challenge initially came with the use of video collaboration, which affected our workers and our network of health care providers.

Many of the providers had not used video as a meeting or collaboration platform, either with members or with us. Secure collaboration became a hot topic, especially to ensure Health Insurance Portability and Accountability Act (HIPAA) compliance in our communications with providers. We had to spend time and money subsidizing tools for our providers and helping them understand how to use the technology in a secure fashion. We educated them to use passwords, on all the policies and procedures for such collaboration, to share and set up groups, and on the etiquette of effective video conferencing.

We also had the logistical challenges of lining up meeting times with people working around their families. In a generationally diverse population such as ours, there were and still are some people who do not like to use video. ■





Kevin B. Boyd, CIO, University of Chicago

Kevin B. Boyd is CIO at the University of Chicago. In 2020, he was honored with the 2020 Chicago CIO of the Year ORBIE Award for not-for-profit organizations. His prior experience includes positions at Tribune Company, CNA Financial, United Airlines, Bank One, and Grainger. He was also an adjunct professor at Northwestern University for nine years. Kevin holds a master's degree from Northwestern University and bachelor's degree from Marquette University.

“Any digital tools that encourage people to be active and present in a positive way can help keep them engaged.”

Video conferencing and collaboration tools certainly facilitate remote meetings, but there can be real challenges, particularly during group collaboration. For example, the classic brainstorming session in which different people step up to a whiteboard and build on an idea can be more difficult in a virtual meeting. This can affect participation levels and productivity.

Collaboration tools and document sharing applications exist that allow many people to work on the same document simultaneously. This helps improve the productivity of brainstorming in a remote environment. We've used a tool that provides a shared space similar to a wall. Anyone in the meeting can post to that space and organize the content. It's more like re-creating the physical wall you would have in a meeting room. If you're running a brainstorming session, you can have multiple people doing something, and everyone can see and react to the results in real time. It's truly interactive. That's different from the whiteboard space in many tools, which is often one person sharing his or her screen and participants annotating it.

Another challenge in remote collaboration is that it's easier for people to be distracted and to do something else during meetings. Any digital tools that encourage people to be active and present in a positive way can help keep them engaged. Digital tools that encourage participation help remote work groups and can also facilitate hybrid learning environments. ■



Michael Marschean, Chief  
Information Officer, SubCom

Mike Marschean is a CIO with a passion for transforming technology organizations into business-focused teams. He delivers IT strategies and solutions to achieve the company's financial and strategic goals. Mike also develops teams that focus on deliverables and return on investment, using technology to achieve productivity, growth, and cost objectives to make the business more competitive.



“Sometimes, remote workers adopt tools for convenience, and IT cannot vet everything. We need to make sure that the enterprise solutions are workable and drive people back to them.”

When it comes to effective meetings and collaboration in remote work groups, the biggest technology problems are actually people problems. The technology works pretty well: The challenge is getting people to use the technology to work together effectively and maintain productivity.

Organization is important, too. Meetings are less effective when there's no real agenda, the materials haven't been distributed ahead of time, or materials have been distributed ahead of time but no one looks at them.

The information technology (IT) organization needs to do its due diligence behind the scenes to make sure that the technology is working for everyone. Executive teams, sales teams, and other groups use different solutions. Sometimes, remote workers adopt tools for convenience, and IT cannot vet everything. We need to make sure the enterprise solutions are workable and drive people back to them.

Securing the remote and collaborative work is an important part of that work. It's about making information sharing secure not just for employees but also for third parties and customers. Doing so requires data classification, access management, device management, multifactor authentication for users, and encryption. It's also auditing those systems regularly to make sure that the people who still have access really need it. Projects start and stop, and people come and go from project teams. ■



Robert Sheesley, Chief Information Officer, Wrench Group

Robert Sheesley is currently the CIO of Wrench Group, a national leader in home repair, serving over 550,000 customers annually. Robert is responsible for the information, technology and computer systems enabling and supporting Wrench Group's enterprise goals, including driving efficiencies achieved by harmonizing business applications, infrastructure, business processes, and technology support processes.



"A major challenge . . . is ensuring that we have all the tools in place to enable not only the secure exchange of ideas through a video conference but also the secure exchange of documents and content."

A major challenge with respect to secure collaboration is ensuring that we have all the right tools in place to enable not only the secure exchange of ideas through a video conference but also the secure exchange of documents. You can provide such security controls and monitoring yourself or through the support of a service provider.

Some controls protect people against doing things that come naturally—things that may carry potential risks. For instance, in our environment, if I want to share something I received in an email with someone I'm chatting with through our collaboration platform, I can copy that content into the chat box of our collaboration tool. If I try to copy the same content into a text message on my personal phone, however, the system will not allow me to do that.

You also have to think about how remote workers could introduce vulnerabilities they may not even think about. For example, if someone is using a personal desktop from home to access the corporate network through a virtual private network, there's a risk that someone else in the family could use that desktop to go to other sites, making that machine vulnerable to infection with malware.

To have an openly collaborative environment, you need good security controls and heightened user awareness. ■



Tracy Hockenberry, CDirector of IT  
Business Systems & Enterprise PMO,  
Salisbury Management, Inc.

Tracy Hockenberry is a technology and business leader with more than 15 years of experience leading cross-functional teams in technology and business strategy, systems implementation, business process innovations, and enterprise project management. Tracy is an energetic leader with a demonstrated ability to motivate teams.



“Using tools that allow file sharing and immediate chatting and collaboration . . . these capabilities can absolutely take you to the next level in terms of successfully working remotely.”

The greatest challenges to running effective collaboration and building consensus among remote work groups are having the right technology and being organized.

Being organized means creating meeting agendas and sharing them before meetings. This way, all participants can prepare by knowing why they are coming to a meeting and what they are expected to talk about. If you can't keep control of your meeting, you will have an ineffective meeting and lose the respect of your participants.

Executing an effective meeting strategy depends on underlying technology. Using tools that allow file sharing and immediate chatting and collaboration, being able to ping a team member during the meeting to ask a quick question—these capabilities can absolutely take you to the next level in terms of successfully working remotely. We have moved our technology infrastructure into the cloud over the past two years, and we can set up individual teams for various work efforts. No matter where people are physically located, they have a team and access to files, project stakeholders, and other team members. They have easy access, easy sharing, and collaboration tools for quick alignment. Even having basic equipment such as double monitors and headsets can make all the difference in productivity for remote workers. ■



## Key Points

- 1 An effective meeting strategy depends on using tools that enable file sharing, chat and collaboration, and the ability to ping your team member during a meeting to ask a quick question.
- 2 Any digital tools that encourage someone to be active and present in a positive way can help keep people engaged. Digital tools that encourage participation help remote work groups and empower hybrid learning environments.
- 3 The foundation of remote and collaborative work is making information sharing secure not just for employees but also for third parties and customers. Such an environment requires data classification, access management, device management, multifactor authentication for users, and encryption.
- 4 Sometimes, remote workers adopt tools for convenience, and the information technology team cannot vet everything. We need to make sure that enterprise solutions are workable and drive people back to them.

## CHAPTER 2

# MANAGING CONTENT RISK IN A DISTRIBUTED WORKFORCE

Content risk and data governance are ever-present concerns, regardless of whether people work remotely or in an office. As the number of remote workers grows, however, the opportunities for lost or stolen data also rise. How do organizations manage content risk for remote employees? To find out, we asked the experts the following question:

“What are the biggest challenges to managing content risk in remote work groups? What advice can you offer in this area?”





Aaron Young, VP-CIO, Summit  
Healthcare Regional Medical Center

Aaron Young is a seasoned IT executive who relentlessly pursues excellence. He has extensive experience in IT strategy, infrastructure, integration, system development, and process improvement. As a result, he has developed the ability to navigate complex challenges and lead organizational change.



“We try to drive remote users to a virtualization platform rather than giving them virtual private network access and allowing them to install the application on their local machine.”

One of the biggest risks is retained data that is left behind because a person either inadvertently downloads something or puts it on a personal device. With policies, procedures, and education, you can train people to be more aware of their environment and the device they're using. You can educate them to clean up potential residual data.

You can also use technical controls to limit this risk. For instance, we use as many technical controls as we can to limit what people are allowed to print or share. For remote workers, if someone's work requires that he or she print something as a part of day-to-day activities, controls force that user to go through a more strenuous request process with the director to determine whether it is appropriate to do that kind of work at home.

Also, we try to drive remote users to a virtualization platform rather than giving them virtual private network access and allowing them to install the application on their local machine. Mobile devices have changed the way people work. We have mobile device management tools that allow us to remotely wipe mobile devices, if necessary. We can also use data-minimization strategies that limit data access to what is needed for the immediate tasks, and then wipe that data when the tasks are complete. ■



Gary Sorrentino, Global Deputy CIO,  
Zoom Video Communications

Gary Sorrentino is the global deputy CIO for Zoom Video Communications. He has held several IT leadership positions across the financial services industry, including global head of client cyber awareness and education at JPMorgan Chase, head of global infrastructure technology efficiencies at Citi Private Bank, global technology CFO at Credit Suisse, and North America IT controller at UBS.



“Employers and employees alike have proven that they can conduct business from alternate locations, but doing so requires redefining how we work securely.”

COVID-19 has turned out to be the greatest business continuity test of all time. Employers and employees alike have proven that they can conduct business from alternate locations, but doing so requires redefining how we work securely. It’s a process of holding the business rules up to the light and figuring out how to apply them going forward.

The technology can work with you and against you. It gives you the ability to limit what people can do depending on how they are connected and what they are looking at. It provides the ability to allow or restrict printing of certain kinds of documents at home. The question then becomes, What then? Are people throwing those printed documents in the garbage? At the office, everything goes into a shredder at the end of the day. Do employees have shredders at home?

COVID-19 has forced a transition that was already under way for many companies. These businesses have to recognize, however, that this is not a snow day. The change in how we work is here to stay. Eventually, the pandemic will recede, and we will move to a new hybrid way of working. Nothing will be the same as before the pandemic, which is why we have to look at those security rules we implemented and tested when we were in the office. We have to learn how to apply them now. We must change our frame of mind to recognize that these are long-term changes. ■



Jamie Gianna, Chief Information Officer, Partners Behavioral Health Management

Jamie Gianna is answering the call of technology evolution in business: He is an executive who simultaneously steers operations, workforce, and technology to better achieve customer/client satisfaction. He blends a unique set of executive competencies that focus on the organizational mission, vision, and values, challenging the “we have always done it this way” mentality.



“We have tools for data loss prevention, and we have controls within our Microsoft Office 365 environment that enable us to manage how documents are shared.”

For those suddenly forced to work remotely because of the pandemic, content risk has been a challenge. In our case, we had good content governance in place because we were already a distributed workforce and had already migrated to the cloud.

We have tools for data loss prevention, and we have controls within our Microsoft Office 365 environment that enable us to manage how documents are shared. Our email solution scans outgoing document attachments for personal health information and sensitive information, such as Social Security and credit card numbers. If any such information is found, the system blocks the email.

One challenge is that people working at home will become careless with sensitive information. It’s not logistically feasible to inspect everyone’s homes. Auditors have advised us to have strong training for handling sensitive information. We have a program of education, training, and awareness that was an annual process, but we have changed that to quarterly training. If people print documents at home, they must be able to shred it or put it in a HIPAA-compliant secure bag (one that zips up and has a lock). For compliance accreditation, you must demonstrate that you have processes, policies, and procedures in place and that you are taking steps to enforce them. ■



Kevin B. Boyd, CIO, University of Chicago

Kevin B. Boyd is CIO at the University of Chicago. In 2020, he was honored with the 2020 Chicago CIO of the Year ORBIE Award for not-for-profit organizations. His prior experience includes positions at Tribune Company, CNA Financial, United Airlines, Bank One, and Grainger. He was also an adjunct professor at Northwestern University for nine years. Kevin holds a master's degree from Northwestern University and bachelor's degree from Marquette University.

“As we think about remote work, we have to decide whether it is more likely that people, now that they’re working from home, will download sensitive data to home and personal computers.”

Data governance is always a challenge. It involves understanding who has access to what data, the appropriate uses of that data, where that data should live, and where it should be stored.

We don’t find that data governance in the remote world is all that different from in the physical world. Perhaps that’s because as an educational institution, we exist in a distributed environment, even in a non-pandemic world. We have a campus with many buildings and departments and we have people who are traveling all around the world.

As we think about remote work, we have to decide whether it is more likely that people, now that they’re working from home, will download sensitive data to home computers. Is there a greater likelihood that other people in the household will use those home computers? How do we make sure that data is protected? These are some of the same questions we’ve always asked, but the magnitude of risk has increased.

We have to consider the need for greater focus on securing endpoints, reminding users about good data hygiene, and increasing encryption of endpoint devices. One positive of the pandemic is that fewer laptops are being lost or stolen during travel. ■



Michael Marschean, Chief  
Information Officer, SubCom

Mike Marschean is a CIO with a passion for transforming technology organizations into business-focused teams. He delivers IT strategies and solutions to achieve the company's financial and strategic goals. Mike also develops teams that focus on deliverables and return on investment, using technology to achieve productivity, growth, and cost objectives to make the business more competitive.



"The biggest data-governance challenge is complexity."

The biggest data-governance challenge is complexity. Many of the companies I worked for build and install products that last for years, even decades. Those companies need to maintain all the documentation around those products for internal support as well as compliance reasons. During that time, many people become involved, and there are many dimensions to consider. The documents themselves can have different security and data classifications. You have to have strong user ID authentication to determine who has access, what they can access and the type of access. Now we are also authenticating the devices that can and cannot have access to the data to provide even more security from remote attacks and hackers.

Complexity exists not only internally to our company but in how everything works among our customers, partners, and suppliers. Not many companies in this industry do what we do. We may lose a bid, and then become a subcontractor to the company that won. Because we collaborate with many of the same companies we compete with, we have to pay close attention to system security and information access over time, it's not just one and done. We have to ensure our security and access is continually updated to match the changes in these long term working relationships with multiple companies and organizations. Many documentation requirements are built into these projects. Depending on

the product, different governments will have regulations about information we have to provide them.

We have to provide thousands of pages of documentation to the customer, including documentation on the installation and ongoing information, such as performance certifications. These products last twenty years, so we have to maintain the documentation in case we have to repair a system we installed two decades ago. In addition to the documentation provided to the customer, we provide thousands more pages to various government entities and environmental regulators.

Securing this information is critical, and different applications provide different kinds of security controls, which adds to the complexity. One way to reduce complexity is to pick one platform that allows you to control everything in a specific domain, but there are multiple security domains that must be managed. These include, document, application, file system, network, and web security domains. No one security solution exists to encompass them all. ■





Robert Sheesley, Chief Information Officer, Wrench Group

Robert Sheesley is currently the CIO of Wrench Group, a national leader in home repair, serving over 550,000 customers annually. Robert is responsible for the information, technology and computer systems enabling and supporting Wrench Group's enterprise goals, including driving efficiencies achieved by harmonizing business applications, infrastructure, business processes, and technology support processes.



“[Data protections means] having all the tools and capabilities in place to protect the data in your network as well as your data in partners’ networks.”

Clearly, data protection is key, which means having all the tools and capabilities in place to protect the data in your network as well as your data in partners’ networks. We routinely talk with our software and SaaS vendors about what they’ve been experiencing and measures they take to improve and harden their networks and computing platforms.

As an organization, we’ve been able to adapt quickly to having a remote workforce, particularly from a content governance perspective. We consist of twelve brands across the Southeast and Southwest United States and California. If everyone were working in an office, we would be operating out of eighteen locations. Before the pandemic, we had already moved a lot of our infrastructure to the cloud. Our managed service provider oversees our security.

So, we proactively used the cloud network to address some of the risks and vulnerabilities associated with remote work groups. We have also taken advantage of automation to address gaps and vulnerabilities we see in the environment. Finally, we have applied machine learning to analyze language in emails so that we can intercept suspect emails before they reach recipients. ■



“Companies must quickly adapt corporate policies and procedures to the download and storage of data.”

Tracy Hockenberry, CDirector of IT  
Business Systems & Enterprise PMO,  
Salisbury Management, Inc.

Tracy Hockenberry is a technology and business leader with more than 15 years of experience leading cross-functional teams in technology and business strategy, systems implementation, business process innovations, and enterprise project management. Tracy is an energetic leader with a demonstrated ability to motivate teams.



In this year of the pandemic, many companies have incurred significant risk from having to move workers into their homes on short notice without sufficient time to plan that transition. When a company moves people into remote spaces so rapidly, it must secure its network, computers, files, personnel information, and client information. Such a challenge opens an organization to risk. In some cases, employees may have to set up their laptop at home so that it can access key applications and data for work. In other cases, employees may have to remove all the computer equipment from their office and set it up at home. Even these steps may not be enough, however.

In our case, most of our software solutions are software as a service, so the sites people sign in to are protected. In that kind of environment, companies must quickly adapt corporate policies and procedures to the download and storage of data. Companies must put policies and controls in place to prevent employees from storing data on personal devices or leaving paper files of sensitive data, such as protected health information, lying around their house. Companies must take steps to ensure that the data employees access when they are working at home is protected. In the case of regulated data, companies must ensure that employees handle data in compliance with relevant regulations. ■



## Key Points

- 1 The biggest data governance challenge is complexity. One way to reduce complexity is to pick one platform that allows you to control everything. The choice of tool is difficult, however, because each platform has its strengths.
- 2 Use technology controls to limit what people can do with the content they access, such as limiting the ability to print to certain locations or the ability to copy text from a document into a messaging app.
- 3 COVID-19 has forced a transition that was already under way for many companies. Businesses have to recognize that this change is here to stay. They need to look at the security rules they implemented when people were in the office and figure out how to apply them to a remote workforce.

## CHAPTER 3

# KEEP REMOTE WORK GROUPS PRODUCTIVE

As more employees work remotely, managers often have less direct interaction with the people who report to them. How does a company use collaborative technologies and management techniques to assure that the right work is getting done and that employees are engaged? To find out, we asked the experts the following question:

“What are the biggest challenges to keeping remote work groups productive? What advice can you offer in this area?”



Aaron Young, VP-CIO, Summit  
Healthcare Regional Medical Center

Aaron Young is a seasoned IT executive who relentlessly pursues excellence. He has extensive experience in IT strategy, infrastructure, integration, system development, and process improvement. As a result, he has developed the ability to navigate complex challenges and lead organizational change.



“Teams sometimes don’t see technology the same way and may not think of what they can do with the tools available to them.”

Keeping your remote work groups productive is partly a leadership challenge and partly how workers use the technology to collaborate more effectively.

Business leaders often feel that if they allow employees to work from home, those employees are not going to be as productive. In fact, people who work remotely end up being more productive and more conscientious about their work. So, this is really a leadership issue, and leaders need to focus on outcomes.

On the employee side, some teams transplanted to their home environment really struggle with the lack of interaction with their peers, while others do much better. In part, the outcome depends on the culture of the department. Some are used to picking up the phone and having three or four people working together. Others do more direct in-person interaction and may not think of what they can do with the collaboration tools available to them.

Departments that use data as their driving indicators and daily metrics may adapt more quickly to a remote work environment than those whose work depends more on direct interaction with peers. These challenges can be overcome, however, if people creatively use the collaboration tools at their disposal. ■



Gary Sorrentino, Global Deputy CIO,  
Zoom Video Communications

Gary Sorrentino is the global deputy CIO for Zoom Video Communications. He has held several IT leadership positions across the financial services industry, including global head of client cyber awareness and education at JPMorgan Chase, head of global infrastructure technology efficiencies at Citi Private Bank, global technology CFO at Credit Suisse, and North America IT controller at UBS.



“Traditionally, companies show people how to do their jobs. They don’t teach them how to work.”

The biggest challenge is teaching people how to work in a new way. Traditionally, companies show people how to do their jobs. They don’t teach them how to work.

Similarly, companies don’t teach people how to collaborate. They don’t say that chat is a good medium for certain communications. They don’t show people how to use their calendar as a time-management tool. For example, my approach is to have my team open in the corner of my monitor all day. They’re all on mute, but if they need something, they can touch the screen and ask.

We need to teach people how to use the technologies in ways that make them productive in this remote working environment. ■





Jamie Gianna, Chief Information Officer, Partners Behavioral Health Management

Jamie Gianna is answering the call of technology evolution in business: He is an executive who simultaneously steers operations, workforce, and technology to better achieve customer/client satisfaction. He blends a unique set of executive competencies that focus on the organizational mission, vision, and values, challenging the “we have always done it this way” mentality.



“When working with remote work groups, where and when people do their work and how many hours they are spending are immaterial. What matters are outcomes.”

When working with remote work groups, where and when people do their work and how many hours they are spending are immaterial. What matters are outcomes. Are you getting the outcomes and deliverables you are looking for? That is a perspective that becomes important in a distributed organization.

It’s also important to keep teams and people connected. I have regular one-on-one meetings with my staff to see how they are doing. I also have weekly team video meetings with all my direct reports. Each meeting includes a ten-slide Microsoft PowerPoint presentation that provides information about work that is in process. We rotate through the team and take turns. We also take turns delivering three-slide presentations on topics unrelated to work. Some of those are totally hilarious, and it keeps people engaged.

Having two-monitor setups is almost a must when sharing documents. On one monitor, you can see documents and content; on the other, you can see everyone in the meeting in real time. ■



Michael Marschean, Chief  
Information Officer, SubCom

Mike Marschean is a CIO with a passion for transforming technology organizations into business-focused teams. He delivers IT strategies and solutions to achieve the company's financial and strategic goals. Mike also develops teams that focus on deliverables and return on investment, using technology to achieve productivity, growth, and cost objectives to make the business more competitive.



“Managers must manage by measuring output, by what people deliver every day.”

The biggest challenge is not a technological one but rather a people-management one.

Fortunately, we built and implemented a new infrastructure to better support remote work a month before the pandemic hit. We transitioned to work from home with no impact to the business. Minor issues arose, such as people connecting to the virtual private network. Those involved providing a bit more training and support.

Before the pandemic moved staff to working from their homes, we held a 15-minute meeting in my office every day just to talk about the challenges everyone faced. If there were open issues, we put them up on a whiteboard and kept coming back to them. The process really is not that different now, except that it's done in remote meetings.

Managers must learn how to manage their people and not rely on IT to tell them how many bits and bytes were going back and forth between a person's computer and the office. Managers must manage by measuring output, by what people deliver every day. Managers must talk to their direct reports every day and ask about what's going on and what their issues are to help them maximize their productivity. ■



Robert Sheesley, Chief Information Officer, Wrench Group

Robert Sheesley is currently the CIO of Wrench Group, a national leader in home repair, serving over 550,000 customers annually. Robert is responsible for the information, technology and computer systems enabling and supporting Wrench Group's enterprise goals, including driving efficiencies achieved by harmonizing business applications, infrastructure, business processes, and technology support processes.



"We approach this issue by working with employees to establish well-defined goals. We have tiers of time-based goals. . . . That's important, especially in a remote work environment."

It is important to engage people in the work they are doing. You don't want productivity to suffer because employees working from home may feel somewhat disconnected.

We approach this issue by working with employees to establish well-defined goals. We have tiers of time-based goals, with longer-term goals typically being more than three months out, short-term goals that focus on the upcoming week, and medium-term goals that land somewhere in between. In team meetings, we talk about how people feel about their progress toward the next milestone. We make sure that there are moments of celebration, too. That's important, especially in a remote work environment.

We have also been doing a lot more with our stakeholders. I encourage our information technology (IT) team to reach out more frequently to the business units we support. We have conversations not just about what we need from them or what we provided them in terms of a deliverable but how the business units feel about where we're at in any particular project. That purposeful communication as a habit helps strengthen the human element in what's going on in the organization. ■



Tracy Hockenberry, CDirector of IT  
Business Systems & Enterprise PMO,  
Salisbury Management, Inc.

Tracy Hockenberry is a technology and business leader with more than 15 years of experience leading cross-functional teams in technology and business strategy, systems implementation, business process innovations, and enterprise project management. Tracy is an energetic leader with a demonstrated ability to motivate teams.



“Employers have to make sure that information is readily available to their employees at any time and in any place. . . . Employees require access to those resources to do their jobs.”

Managers face two major challenges in keeping their distributed teams and remote workers productive. One is trusting that their remote employees are doing the work. The other is having the tools that give employees the flexibility they need to do their work.

Some collaboration tools enable you to track who is signed in to project resources, when, and for how long. With remote workers, however, the most important measurement is outcome, not hours worked. It's that high-quality outcome that matters to managers and the business. The COVID-19 experience has shown that employees working from home are working longer hours than when they were in the office—in part because they have more flexibility to adjust work around the demands of home life. Also, the tools of work are right there when they need them. If employees have an idea, they can immediately be in their office. In our teams, we see employees online at all hours of the day and evening.

For this to work, employers have to make sure that information is readily available to their employees at any time and in any place. If an employee needs data to complete his or her job and if in the past that data was available only in the office, now the employer has to quickly make those resources available through a document-sharing solution or collaborative workspace. Employees require access to those resources to do their jobs. ■



## Key Points

- 1 Companies show people how to do their jobs. They don't teach people how to collaborate. They don't teach them when to use chat versus video or how to use their calendar to manage their time. We need to teach people how to use tools in ways that make them more effective remote employees.
- 2 Departments that use data as their daily driving indicators may adapt more quickly to a remote workforce environment than those whose work depends more on direct interaction with peers.
- 3 Managers need to measure output, what people deliver every day. Managers need to talk to their direct reports every day.

## CHAPTER 4

# CREATING A WORK CULTURE IN A DISTRIBUTED WORKFORCE

Many companies that support a remote workforce struggle to maintain corporate values and employee morale. What technologies and management strategies have companies adopted to successfully overcome these challenges? To find out, we asked the experts the following question:

“What are the biggest challenges to maintaining a work culture and employee engagement within remote work groups? What advice can you offer in this area?”





Aaron Young, VP-CIO, Summit  
Healthcare Regional Medical Center

Aaron Young is a seasoned IT executive who relentlessly pursues excellence. He has extensive experience in IT strategy, infrastructure, integration, system development, and process improvement. As a result, he has developed the ability to navigate complex challenges and lead organizational change.



“Developing competency and remote work etiquette is an important part of developing a remote work culture.”

It really comes down to the chief executive officer (CEO) or the leader of the organization. Some CEOs need to have people in the room. Instead, they should give permission to their managers to create a culture in which it's OK to work remotely. Allowing people to work from home can have a significant bottom-line impact on the business. It's really a cultural thing that I feel is driven from the top down.

The other aspect of a remote work culture is getting people up to speed on the technology they will use. It can be frustrating for everyone in a meeting if someone constantly struggles with the technology. In addition, it's often the same people who struggle, who never figure out how to mute their microphone. Developing competency and remote work etiquette is an important part of developing a remote work culture. ■



Gary Sorrentino, Global Deputy CIO,  
Zoom Video Communications

Gary Sorrentino is the global deputy CIO for Zoom Video Communications. He has held several IT leadership positions across the financial services industry, including global head of client cyber awareness and education at JPMorgan Chase, head of global infrastructure technology efficiencies at Citi Private Bank, global technology CFO at Credit Suisse, and North America IT controller at UBS.



"Maintaining culture is also about keeping people informed. It's important that companies not stop doing that even when offices begin to reopen because I think we are going to continue to move to a more hybrid state in which remote work becomes the normal state."

Companies need to make a conscious decision about how they support their remote employees. How they do that depends on corporate leadership and company culture, but here's an example.

I know one chief executive officer (CEO) who scheduled a 90-minute all-hands video conference. All 5,000 employees were required to attend. The meeting started, and when the CEO joined the call, he said, "There's no meeting. For the next 90 minutes, I forbid work. I want everybody to go outside, go for a walk, go hug your kids, do whatever you want for the next 90 minutes." He was sending a clear message that the company cares about its people and doesn't want workaholics.

If part of the company culture is to support employees working from home, that will involve teaching them how to use the tools and work effectively in a virtual environment. It also means giving employees the right equipment and making sure that they have the right kind of chair and desk so they don't injure themselves and the right kind of lighting.

Maintaining culture is also about keeping people informed. It's important that companies not stop doing that even when offices begin to reopen because I think we are going to continue to move to a more hybrid state in which remote work becomes the normal state. ■



Jamie Gianna, Chief Information Officer, Partners Behavioral Health Management

Jamie Gianna is answering the call of technology evolution in business: He is an executive who simultaneously steers operations, workforce, and technology to better achieve customer/client satisfaction. He blends a unique set of executive competencies that focus on the organizational mission, vision, and values, challenging the “we have always done it this way” mentality.



“You really have to prepare for working as a distributed organization and think about how you will maintain that sense of connectedness and belonging to a team.”

You really have to prepare for working as a distributed organization and think about how you will maintain that sense of connectedness and belonging to a team.

We have always had a monthly all-employee meeting in which every employee would come to a huge auditorium on campus, and then leadership would get on stage and talk about everything that was happening. Even before we hit that tipping point a few years ago where most people worked from home, they knew they had to come in for that meeting. It kept everybody connected and in the know. The pandemic forced us to turn that meeting into a virtual forum. At first, a lot of people tuned out. When we made it a requirement, it continued as before. We have been able to reestablish our corporate culture and keep that momentum going.

A significant challenge has been connectivity. Many of our employees live in remote areas with poor broadband access. The pandemic has exacerbated that because now, instead of one person working from home, the entire family is there drawing on limited connectivity. We have not found a viable solution to solve everybody’s internet woes. ■



Michael Marschean, Chief  
Information Officer, SubCom

Mike Marschean is a CIO with a passion for transforming technology organizations into business-focused teams. He delivers IT strategies and solutions to achieve the company's financial and strategic goals. Mike also develops teams that focus on deliverables and return on investment, using technology to achieve productivity, growth, and cost objectives to make the business more competitive.



“There is a potential disparity in corporate cultures between those who are fluent with the technologies they use to engage and collaborate and those who struggle with those tools.”

Maintaining a work culture among remote workers is a major challenge. The days of interdepartmental sports teams and after-work happy hours have fallen by the wayside for many companies. In fact, the relationships between companies and their employees have changed. So much more is based on mathematical assessments and measured outcomes. With fewer workers on premises, hanging motivational posters on the walls no longer works. Whereas extroverted employees may have shined in an office setting, in a more virtual world the introverts could have an advantage.

Corporate leadership must become more savvy about how they communicate with their employees. When in-person relationships are not possible, leadership must use tools such as social media and virtual town halls to set the tone and expectations. They must educate employees to be effective with the technologies they are using. There is a potential disparity in corporate cultures between those who are fluent with the technologies they use to engage and collaborate and those who struggle with those tools. ■



Robert Sheesley, Chief Information Officer, Wrench Group

Robert Sheesley is currently the CIO of Wrench Group, a national leader in home repair, serving over 550,000 customers annually. Robert is responsible for the information, technology and computer systems enabling and supporting Wrench Group's enterprise goals, including driving efficiencies achieved by harmonizing business applications, infrastructure, business processes, and technology support processes.



“We’ve taken several steps to address this. One is to move our initiatives tracking towards alignment with our strategic objectives.”

A big challenge with that lack of physical closeness is creating a sense of belonging and shared values in the organization. We’ve taken several steps to address this. One is to move our initiatives tracking toward alignment with our strategic objectives. In this way, we enable everyone to see the business value of the work they are doing. It also enriches those stakeholder discussions we have with the business units that our IT organization supports.

Another informed adjustment we’ve made is when we acquire an organization and begin the planning to integrate that company’s IT operations into our own. In the past, I or a senior member of my team would have flown to the new location and spent a week or two engaging with the stakeholder community to familiarize them with our methodology for certain implementations. With no-travel policies in place, however, we are forced to plan and carry out implementations and integrations remotely. We now break the process down into smaller steps and slow the integration path. For instance, instead of a three-day in-person discovery process, with workshops that run for several hours, we break the process into a series of one-hour video meetings spread over several weeks. This change has forced us to be flexible about extracting the right topics in the right sequence and getting the right people in the meetings, and has presented some unique collaboration with our key SaaS partners relative to their approach to engaging with us to achieve the same exceptional results we have experienced in the past with them. ■



Tracy Hockenberry, CDirector of IT  
Business Systems & Enterprise PMO,  
Salisbury Management, Inc.

Tracy Hockenberry is a technology and business leader with more than 15 years of experience leading cross-functional teams in technology and business strategy, systems implementation, business process innovations, and enterprise project management. Tracy is an energetic leader with a demonstrated ability to motivate teams.



“Another important piece in keeping the work culture intact is making sure that the company sets up its remote workforce to be successful.”

Maintaining company culture and employee engagement with remote teams begins with effective communication from company leadership. This is especially true in times of transition, such as what many have experienced with COVID-19. Having much of the company work done by remote employees places a new demand on the executive team to provide an elevated level of communication. They have to put more thought into the timing and delivery of their messages.

Another important piece in keeping the work culture intact is making sure that the company sets up its remote workforce to be successful. This means providing employees with the equipment and collaborative IT infrastructure to make their jobs easier so that they can produce what the company expects from them. During the pandemic, employees who moved from their offices to their homes were already familiar with the corporate culture, their coworkers, the tools, and the processes. When companies add new people to a remote work group, they must convey all that information remotely.

It is absolutely imperative that the relevant people have all the files and resources necessary to onboard new employees and keep existing workers operating as close to normal as possible. Managers must be able to refer and give access to different content assets, policies, project materials, and department files. ■



## Key Points

- 1 An important facet of keeping the work culture intact is setting up the remote workforce to be successful. This means providing employees with the equipment and a collaborative technology infrastructure so that they can produce the work expected of them.
- 2 Maintaining institutional and cultural values requires consistent communication about those values, whether that happens with staff in multiple buildings or staff working remotely.
- 3 A big challenge with the lack of physical closeness is making sure employees have a sense of belonging and shared values. Aligning initiatives with strategic objectives enables everyone to see the business value of the work they are doing.



## CHAPTER 5

# BUILDING A SECURE IT INFRASTRUCTURE FOR A REMOTE WORKFORCE

Supporting distributed workgroups and remote employees requires an array of communication, collaboration, and security capabilities. What kind of decision-making goes into building the infrastructure necessary to support a remote workforce? To find out, we asked the experts the following question:

“What are the biggest challenges to building a secure IT infrastructure for work groups? What advice can you offer in this area?”



Aaron Young, VP-CIO, Summit  
Healthcare Regional Medical Center

Aaron Young is a seasoned IT executive who relentlessly pursues excellence. He has extensive experience in IT strategy, infrastructure, integration, system development, and process improvement. As a result, he has developed the ability to navigate complex challenges and lead organizational change.



“You have to be strategic and thoughtful about the possibilities so that you make acquisitions not just for what you need today but for what you might need tomorrow.”

If you don't put a strategy in place for which technology you purchase, then you're just buying a bunch of stuff and spending without anticipating future needs. When we look at a technology solution for the organization, we look at it from a long-term strategy perspective.

For example, if I'm looking at a system for collaboration, I would evaluate the standard lineup of collaboration tools. If I'm being strategic about it, however, I will think about what collaboration really means and what it can do to drive the business forward. I will take that consideration a step further and think about how I can use collaboration to bridge my video endpoints for our telemedicine systems because that's just a different kind of collaboration. By having a strategic viewpoint of what the enterprise needs, I can make an investment that solves multiple challenges.

You have to be strategic and thoughtful about the possibilities so that you make acquisitions not just for what you need today but for what you might need tomorrow. When COVID-19 hit, we were in a good position to support employees working from home. Because of the technology we deployed to enable video collaboration with patients, we were actually able to reduce the amount of personal protective equipment (PPE) our health care providers and physicians had to use in patients' rooms. We were able to donate some of our PPE to surrounding hospitals that had a shortage. ■



Gary Sorrentino, Global Deputy CIO,  
Zoom Video Communications

Gary Sorrentino is the global deputy CIO for Zoom Video Communications. He has held several IT leadership positions across the financial services industry, including global head of client cyber awareness and education at JPMorgan Chase, head of global infrastructure technology efficiencies at Citi Private Bank, global technology CFO at Credit Suisse, and North America IT controller at UBS.



“Technology that does not support continuous innovation will become irrelevant. Decision-makers must consider this fact when building an infrastructure to support a remote workforce.”

Technology decisions can be difficult because so much innovation is happening so fast. In addition, there is uncertainty about how job roles and processes are changing as more people work remotely.

Decision-makers need to look at applications that give them command and control over workflows and security. Usability is critical, as is training people how to use the technology effectively and securely.

Companies must also consider the future. In my view, we are already on the road to a hybrid work model that may affect job roles. If someone can effectively perform at a level the company expects, then it should not matter where that work is done. This approach can affect many things, including where companies find talent. Virtual work spaces also make it easier for companies to offer employees training and certifications that improve their qualifications.

Artificial intelligence (AI) is becoming increasingly important in collaboration tools. AI can deliver more frictionless functionality that makes users feel more immersed and collaborative. Technology that does not support continuous innovation will become irrelevant. Decision-makers must consider this fact when building an infrastructure to support a remote workforce.

We are at a stage of redefining work. Companies and employees must sit down and plan for the long term. ■



Kevin B. Boyd, CIO, University of Chicago

Kevin B. Boyd is CIO at the University of Chicago. In 2020, he was honored with the 2020 Chicago CIO of the Year ORBIE Award for not-for-profit organizations. His prior experience includes positions at Tribune Company, CNA Financial, United Airlines, Bank One, and Grainger. He was also an adjunct professor at Northwestern University for nine years. Kevin holds a master's degree from Northwestern University and bachelor's degree from Marquette University.

“Collaboration technologies must be user friendly. They must also be reliable and secure.”

Our greatest challenge is building a technology infrastructure that supports our diverse population of users. When we adopt collaboration solutions for the university, we thoroughly review them for a diverse and complex environment. That means that the tool must be user friendly, accessible, mobile friendly, scalable, secure, and able to meet the needs of our different populations.

We support the work of University faculty, students, and staff. We also operate a large laboratory school that includes kindergarten through grade 12—a broad population of users. They must also be reliable and secure from disruption and data loss. The tools may be used for research, instruction and administration.

When we adopt a solution that will be used across the university, we perform our due diligence to make sure the tool fulfills the needs of our diverse user population. ■



Michael Marschean, Chief  
Information Officer, SubCom

Mike Marschean is a CIO with a passion for transforming technology organizations into business-focused teams. He delivers IT strategies and solutions to achieve the company's financial and strategic goals. Mike also develops teams that focus on deliverables and return on investment, using technology to achieve productivity, growth, and cost objectives to make the business more competitive.



"If a tool is easy to use, people will use it. If it's hard to use, no one will. You must measure that ease of use to make the right choices."

Here are several of the key challenges we have in building an IT infrastructure to support our global activities, which involve working with people all over the world:

- Drive consensus on which tools ought to be in the organization. Different teams have different priorities, and some would prefer one tool over another.
- Once a tool has been rolled out, make sure that people are actually using it. How many people are using the new technology? The answer comes down to training and usability, which is an important consideration in adopting an application. For a remote workforce, having connectivity and video conferencing are table stakes. That is foundational. You also need an application design that makes it easy for people to communicate and collaborate. That's really the value. If a tool is easy to use, people will use it. If it's hard to use, no one will. You must measure that ease of use to make the right choices.
- Verify that the tool is delivering the expected return on investment. Companies often deploy new technology, transition to it, and then move on. Once the implementation is over, you have to verify that you are getting what you need from that technology. Many times the ROI can only be measured months after a go-live. It's very easy to move on to other priorities. You need to have the process

discipline to measure results 6 months or a year after implementation to determine the success of a project.

- Make sure it is secure. Security is a constant struggle. You can work to centralize security controls, but at the same time, users are trying to figure out ways to transfer information more easily. Often, they download their own tools to do that. You must constantly look for tools that enable users to work easily and securely. When you make it easier for people to work, they will be less likely to look for end-runs around your controls.

Part of the answer is simplifying the application stack so that you are managing and working with fewer applications. We have adopted collaboration technology that incorporates voice, video, large file sharing, and security. This technology has replaced four independent tools. ■



Robert Sheesley, Chief Information Officer, Wrench Group

Robert Sheesley is currently the CIO of Wrench Group, a national leader in home repair, serving over 550,000 customers annually. Robert is responsible for the information, technology and computer systems enabling and supporting Wrench Group's enterprise goals, including driving efficiencies achieved by harmonizing business applications, infrastructure, business processes, and technology support processes.



“When choosing tools, I want to make sure that we choose one that provides secure, flexible collaboration capabilities.”

One challenge is getting the organization to recognize the value that good collaboration tools can bring to an operation. It's not always apparent how much you can gain in terms of accelerated processes, the ability to produce deliverables, and the overall value to the organization until the collaborative capability is in place.

When choosing tools, I want to make sure that we choose ones that provides secure, flexible collaboration capabilities. When you think about integrating new acquisitions and onboarding new employees, it's all about communication, communication, communication. You must ensure that everyone understands how the project is structured; why it's structured the way it is; and how we will ensure that we stay on track, in scope, and on budget while enlisting input from all interested parties along the way. All of my IT leaders are aware of and trained in areas of stakeholder management. Setting expectations upfront and then delivering on the communication related to those expectations is a key component of our methods and approach. We need the means to support iterative formal and informal review of work and address any issues that arise in a timely fashion to ensure a high degree of confidence in our ability to lead our organizations through transition. This approach is dramatically more important now in the remote work environment than when we were all physically the same room together. ■





“You must pay close attention to security. Then, you must help your remote workers get past the frustrations of learning about new technology.”

Tracy Hockenberry, CDirector of IT  
Business Systems & Enterprise PMO,  
Salisbury Management, Inc.

Tracy Hockenberry is a technology and business leader with more than 15 years of experience leading cross-functional teams in technology and business strategy, systems implementation, business process innovations, and enterprise project management. Tracy is an energetic leader with a demonstrated ability to motivate teams.



To put together the tools needed to support remote teams, you must pay close attention to security. Then, you must help your remote workers get past the frustrations of learning about new technology.

Security is a big issue. Think about how to protect your organization and your data. To do that, you must understand how you are going to manage access to information resources, how you will secure remote communications, how you will protect email against phishing campaigns, whether you will support the use of personal devices, how you manage data encryption, and how you enforce corporate policies and procedures. Identify your high-risk areas, and put a mitigation plan in place. Companies that deal with sensitive or regulated data often begin with compliance requirements, a risk analysis, and measures they will need to take to mitigate risk factors.

Another important part of supporting the technical infrastructure for remote workers is simplifying the setup for them. If they are working from home, this may mean sending a tech person to their house to make sure they are set up. Or, it can be done through remote sign-in and screen sharing so that a tech person can walk through set up and explain what an employee needs to know to do his or her job. ■



## Key Points

- 1 Organizations must recognize the value that good collaboration tools can bring to an operation. The value of accelerating deliverables is not always apparent until the collaborative capability is in place.
- 2 You have to be strategic and thoughtful about the possibilities so that you make acquisitions not just for what you need today but for what you might need tomorrow.
- 3 Artificial intelligence (AI) is becoming increasingly important in collaboration tools. AI can deliver more frictionless functionality that makes users feel immersed and collaborative. Technology that does not continue to innovate will become irrelevant.

EGN<sup>Y</sup>TE

# The Office Has Changed. The Mission Hasn't.

Content Control When It Matters Most

