CompTIA

WHITE PAPER

Embedding Cybersecurity Into Your Culture

Is your culture inadvertently undermining your security? Or does it encourage a "security first" mindset? This paper, written by CompTIA volunteers from across the globe from all sizes and types of businesses in the IT services industry, presents a path to embed cybersecurity into your culture by leaning into your culture. Recognizing the role of "people" in the people-processes-technology triangle is the key to unlocking a "security first" mindset within your culture.

Table of Contents:

Introduction

Every strong cybersecurity program incorporates people, process and technology (PPT). Organizations largely focus on the technology and the process, but despite ongoing security awareness training, many find their people are not changing their behaviors and embracing their role in security. If behavior is to change at the organizational level, then the culture of the people needs to be addressed. But how?

That's the wrong question. The first question to answer is "why?"

When we talk about a culture of cybersecurity we are talking about people having complete buy-in that they are doing what is right for the right reasons. They know the consequences of actions that are easy vs. correct. Have we trained and ingrained our culture with the muscle memory that the "right thing" is undertaken without thought? Some might say that your brain isn't exactly a muscle, but it is great at recognizing and following established patterns. Your culture should support a pattern of doing things the right way and not necessarily the easy way.

While there are core best practices inherent within cybersecurity, those practices can be deployed within any culture. This paper will help you identify your values and strengths, provide recommendations on how to leverage those strengths to improve your cybersecurity posture, including tabletop exercises and real examples of how cybersecurity fits into different values, and ultimately, how to think "security first" within the context of your business. This is all about leveraging cyber security for business advantage, the ultimate goal of any company.

Your greatest chance of success in embedding cybersecurity into your culture is to lean into your core values.

Executive Buy-in

Determining the Why

When looking at an organization's mission statement, the word "secure" or "security" is often missing. In today's modern threat landscape, protecting intellectual property (IP) and personally identifiable information (PII) is a necessary part of doing business – like paying corporate taxes each year. But building out a "why" for an organization can go above and beyond a compliance mandate or fear of losing IP or PII – the "why" can be a larger and more compelling mission: "We're not going to let our adversaries win; we are doing our part for the U.S. economy." Or "We're not having our livelihood stolen out from under us; we're going to protect our data and be more competitive with our security."

Incorporating security culture into the mission statement means that leadership (top down) is committed to support and resources for organizational behavior change. For that buy-in, you must start with the "why", and it must come from leadership. How the "why" is answered will reflect the organization's values as well as its shared understanding of what security means.

Once leadership comes to incorporate the language of security within the company mission and values, employees receive this differently than they do with IT- or cyber-related training and messages from the information security team. "Do as I do, and not just as I say," carries weight and fosters behavioral change. But it must be led with executive buy-in.

Using Your Culture to Embed Cybersecurity

Using culture to embed cybersecurity creates a strong foundation for security to be embraced successfully across an organization. Recommended security practices can be integrated in to your values, processes and behaviors rather then being viewed as disjointed add-ons As we talk about security and culture, we must figure out what a security mindset is.

One definition is: “A cybersecurity mindset involves understanding the goals and assets of an organization, understanding the risks and impact of attacks on those assets, and prioritizing resources to maximize protection.” Or it can be as straight forward as the common sentiment: “If you see something say something.”

In truth, we have to take the stigma away from reporting that you or a colleague did something incorrectly. How often have we said something like, “It is fine this time… but in the future, we don’t want to do that.” Opting for convenience in the interest of saving time is never the best way to address cybersecurity.

Another common mistake from information security leadership is to respond to anyone shining a light on potential cybersecurity issues by responding with “stay in your own lane” or simply pointing to others who should be told, while they concern oneself with their own role. Supporting discussion and openness is important. The information security team should work to leverage corporate values and culture to encourage employees to participate with security in their day-to-day conversations, no matter their role in the organization.

Ultimately, being able to deliver on the values of the company in a secure manner is the desired outcome.

Understanding Your Culture

What are your organization's values? What are its strengths? How does the organization sell itself? Consider an organization that positions its security services as best-in-class. Is that reflected within its own walls? Are training dollars and sensible security controls in place? Or was the margin on security services too tempting to pass on?

Take an organization committed to sustainability that creates security flyers or posters for information security awareness purposes. Being misaligned from corporate values may have a negative impact on how the message is received.

Values show up in daily business and minute-to-minute activity. Naturally, culture and security in a 3–5-person business can and will look different from a 50-person business. And it's important to note that truthfully identifying what values are showing up where can be a difficult task.

The people tasked with responsibility for security are often technical people, and many already understand the technical and regulatory reasons for a security measure but are inadequately skilled in communicating this in a way that is personal to the staff. This becomes a challenge when it comes to changing behavior. We'll explore the idea of a security "champion" later in this paper.

When trying to identify how your values can act as an insertion point for a culture of cybersecurity, examine them to find what are you doing that is already living in that cybersecurity mindset.

You don't have to rewrite your culture. Use your culture to implement cybersecurity. One mantra to consider is: "You have to know what makes your employees tick, and what ticks them off." Not every employee or team member learns or comprehends the same and each person's style of being a champion for a particular effort is different. Recognizing this is important.

By leveraging your existing values, you can intertwine your culture and cybersecurity. If you have a healthy culture (supportive, inclusive, diverse, allows for mistakes) then you should be able to have a cybersecurity-first mindset. Establishing trust within the relationships among executives, employees, clients and vendors will make cyber efforts easier.

For instance, one value could be "technical excellence." This value defines an ability to deliver technology with specific outcomes. A willingness to dive into problems to find the root cause, not just fix whatever bug was reported, is a form of technical excellence, which fosters a more stable user environment. This also represents a security mindset.

Other examples of how a value can be a vector for cybersecurity include:

Listening to our clients and employees is a value which reflects open communication. Therefore, communicating misconfigurations, indicators of compromise or just something that doesn't feel right, etc. becomes a way to embed cybersecurity with an existing value. Training and ongoing learning is a value, which shows up in automated processes and innovative solutions for customers. Adding cybersecurity training would naturally augment automation with a secure testing method and review of impacted assets prior to release, leveraging training as a value to build a more secure culture.

Defining Your Values

If you have not conducted an exercise to identify your values, this section will help you. It's important to note that the maturity of the organization comes into play here. Not just how old or large it is, but how smoothly do processes and procedures play out, as well. Think about how convenience and speed may enable or conflict following the procedures in place. Or being able to explain to the client why a process/procedure is in place that makes sense to the client – this last part is a sign of a more mature, cyber-first mindset managed services provider (MSP).

An example to help illustrate:

> "The CEO's daughter calls in and says that her father is in the hospital, and she needs his email password."
>
> There are a lot of ways to handle this. The simple and most expedited way to handle this is to provide the person with the password. A more mature approach would be to verify this person is who she says she is and get more details on why this is needed.
>
> In making this decision, our dispatch team reached out to the CTO, and said, "Hey, this sounded funny to us; what do you think?" Not having a whole lot of interaction with the daughter before, the CTO got on a call with her and had her relay the situation. Upon consideration, he asked if someone else could authorize this request from her. The COO of the client company confirmed the CEO was in the hospital and that she was indeed his daughter. They came up with a plan to deal with the CEO's email situation while he was in the hospital, which included her having access to his accounts.
>
> The CEO's daughter and the client COO both thanked us separately, expressing appreciation for the extra diligence in confirming that they were who they said they were and working with them to deal with the situation with the least amount of risk. The moral of the story is that providing good security is also providing great customer support, which may be one of your very own values. Not taking the easy way, even though it sounds urgent and scary, reflects your organization's values and provides for a learning opportunity with the client.

Defining organizational values are essential for cybersecurity because it creates a common language for awareness and behavior aligned with an organizations security, risk, and business goals. A good recommendation for defining values is word mapping. Typically, a small team puts together a word map and circulates for input from staff identifying words that ring true. Challenges will differ from a 5-person shop vs a 70-person shop.

For example, is the organization present in more than one country? This may mean that cultural differences need to be considered when communicating, creating new processes or making any big changes in the organization.

Similarly, is there more than one language spoken within the organization? The more we tailor communications, the more relevant it will be to employees and other third parties and the more likely it is that we can achieve a positive cultural change. Even if there is an official language in an organization, it is not uncommon that the official language is not spoken by all roles and departments.

Speaking of communication and company language, many companies just throw technology at the problem. Simply implement a security awareness training program and that box is checked, for example. It's not just about technology, it's about the employees, who are people. Just like with establishing a company brand, we must humanize the cybersecurity culture building. Create a diverse culture program that meets the needs of everyone. Just as people learn in different ways, people also support in different ways. Make it positive and collaborative. A great first step is to assign a "champion" to lead the charge.

How it Works

Security Champions

Ensuring the champion has a deep understanding of the culture, as well as possess emotional intelligence and strong communication skills is a factor in success.

To help galvanize the organization, identify a "champion" to communicate the vision as well as communicate back to the security team what they hear from the various teams or users. Depending on the size and complexity of the organization, a network of champions may be required. This is sometimes referred to as a security ambassador program, where employees are tagged from each business unit to help corporate security find the best way to incorporate the training and hands-on experience for different security topics. We elaborate a bit more on this in the culture section.

Having the right contacts and conversations will also help. Speaking with other departments or individuals tasked with those roles regularly will give the champion a wide overview of the biggest risks or weakest points in the organization. In a smaller company, a single person may be responsible for more than one of these areas. In those cases, focus on the risk management intent of the information being shared. For example:

Forensic analysis, incident response and security monitoring departments (in the case of larger organizations) can provide information about current threats and attack vectors in companies. They may also suggest information security campaigns based on root causes for different incidents and observed threats within the organization.

Key departments/groups of employees (leadership, executive assistants, finance departments, IT, procurement, HR, etc.) are often considered a higher risk due to the type of information that they handle, being an attractive target for attackers, being more exposed to potential attacks, etc. It is important to understand what kind of processes they follow and what specific risks they face in their day-to-day activities in order to protect them better with the relevant security controls and to train them properly.

Corporate communications and learning & development departments can help identify types of communications, materials, topics and tone that work better within the organization. Some organizations may successfully utilize a SharePoint intranet site for updates and tips pertaining to security. Others may leverage lunch and learns, and others may prefer a combination of video training and digital newsletters. Any delivery mechanism that resonates at the company level and at the business unit level should be explored.

This is not about being a security expert. As a matter of fact, marketing and communication roles can often communicate the cybersecurity awareness initiatives better than IT or cyber-security experts. The easier and more engaging you can make security to digest; the more behavior will change. It's about instilling a habit of watching those little things that suggest something "isn't right" and knowing they can get someone to dive into what they've noticed.

This brings us to what can be a sensitive topic around security; the impression that security imposes extensive restrictions on being able to work efficiently and is inconvenient. If security is used as an automatic roadblock to every new app or idea that comes from the user community, for reasons legitimate or otherwise, that creates shadow IT which is often riddled with security holes. Finding ways to integrate users into the process, address their concerns for new tools and finding ways to help, not just say no, are better approaches to balancing business efficiency needs with security needs.

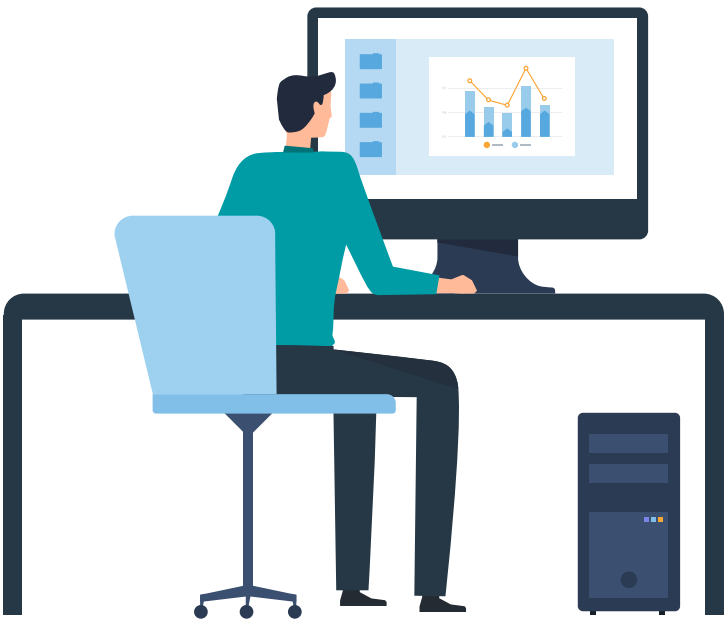
At the same time, educating those business units on the "why" will further the embedding of cybersecurity into your culture. Does our culture understand that when, not if, these events occur they have real consequences beyond 'you've violated a policy'? When, not if, something happens, it costs real time, real money, etc. "We do these things not because they are right, we do these things because we each play a real role in the outcome." Every employee embracing this understanding will bring security into your culture.

Clarifying Event

Snap decisions are often a golden opportunity to pause, review the decisions being made, understand security implications and come to an agreement on acceptable solutions. In the writing of this paper, we were collaborating with people from all around the world. At first this paper was written in MS Word and simply emailed as an attachment. After our first meeting we decided that we needed a more collaborative space to work on the document. We had someone make the comment: "Well I can just put that on my personal Google Drive." While there is nothing wrong with Google Drive, your personal Google Drive is very different than the Google Drive or SharePoint that is set up by your organization.

A simple conversation like this can act as a "clarifying event." If you dig in just a little bit, some conflicts begin to appear and questions surface; a learning opportunity not to be missed. In this case those questions include:

- What makes it so much harder to share from a corporate collaboration platform vs. a personal drive? It could be several things; all of which lead to a less secure system.
- Is my corporate collaboration platform so difficult to use with its more secure environment that a user would rather opt for convenience over security?
- How do we identify and control data leakage and sprawl onto personal cloud platforms? What is our policy on this and are our users aware of the proper procedures to share documents?
- Do our employees understand what type of information is considered proprietary, sensitive, confidential or public?



Tabletop Exercises

One way to bring clarifying events to light is through tabletop exercises. Making these tabletop exercises relevant and clear to top management ensures they understand the importance of information security; therefore, leadership should participate in the exercise and reflect on impact both during and after the simulation.

Many times, it's better to have a short but relevant tabletop exercise rather than an elaborate simulation that does not relate to them. Some aspects are essential for this type of exercise to be successful:

- The exercise should be performed in a safe environment to learn. The exercise should not be presented as a test and there cannot be any negative consequences for participants. It's recommended not to record the exercise unless there is already a positive culture in the organization, and it does not have an impact on the participants' performance.
- Providing the participants with all the information about the exercise (including what is expected from them before and during the exercise) and even a short test meeting will ensure that they feel more confident and have a more positive attitude towards the exercise.
- Face-to-face exercises are preferred but, if remote inclusion is required, the use of the camera is recommended to encourage participation.
- At the end of the exercise, it's important to reflect on points for improvement (lessons learned), but also on the positive outcomes (e.g., the team was very well organized, and decisions made were based on facts).
- Most tabletop exercises require a follow up remediation or process improvement plan as a result of the lessons learned with those involved. Including top management on the status of the improvements will provide more tangible visibility into challenges with resources or accountability. For example, if a document such as a crisis management plan is used during the exercise but is not efficient or includes contradictory information, the review and updating process may stall out from inattention; having top management included in the progress updates will likely reinforce prioritization.
- A second exercise after some time will demonstrate to participants the effectiveness of the first simulation (it tends to flow better, participants are more aware of the existing procedures, make better decisions, etc.).

- The tabletop exercise can be a great opportunity to invite key stakeholders from different departments (e.g., legal, IT, finance, corporate communications/marketing). In a normal incident they will most likely need to collaborate, and the simulation will make sure all the departments are aligned when dealing with a real situation.
- Manage participants' expectations. Although the scenario will be as realistic as possible, it's important to ask participants not to challenge the scenario during the simulation since many aspects would happen differently in an actual incident.

How do you know if an exercise produces a clarifying event? This example of a CIO at a manufacturer in the Defense Industrial Base running a tabletop exercise to test the physical security of their manufacturing area illustrates.

"They had spent nearly a year to improve employee awareness by adding training, signage, alarm systems, employee badges, visitor escorting policies and reporting mechanisms. They notified their staff that the physical security would be tested over the coming two weeks, so no one would be surprised. Despite their efforts, the CEO and CIO watched from afar as their perpetrator made their way into the warehouse area, chatted with a couple workers, nodded hello to others and navigated through the shelving units to the interior office.

In the debrief with the staff, the CIO shared that to many active participants it was eye-opening just how quickly they forgot to be on alert and even made the intruder feel welcome, without following procedure or training. He shared that the CEO was supportive of the importance of the exercise, didn't blame anyone for messing up and helped to facilitate the lessons learned. This provided an opportunity for all participants to agree on better training and controls, both technical and physical, to close the gaps. The group involvement in remediation ideas with the CEO and myself participating helped to move the warehouse security into 'a whole new realm' with follow-on exercise results greatly improved."

Documentation and Processes

Aligning workflow processes with the proper tools will further enhance cybersecurity within your culture. Misalignment can have the opposite effect. For example, if employees are told not to share confidential information with third parties via email, but that is the procedure to follow when working with a vendor, a process and security conflict arise. Similarly, we cannot tell employees to make use of a password manager if we provide one that is very difficult to use or expect the employee to select and pay for one themselves. Leadership, front line managers and technical staff should all be involved in drafting processes and procedures when it comes to cybersecurity. Leadership inclusion allows for clear support of the new policies and initiatives, which will increase user awareness and demonstrate that everyone will be held to the standard. Meanwhile, when team members and individual contributors are included and involved with processes and procedures, it gives them the feeling of ownership, which leads to more comprehension and productivity. They are more likely to become a champion of the effort. The output of the documentation will be more realistic and reflective of how things work properly.

Keep in mind, this process does not really have an end. Regular reviews will help keep the processes working effectively. Use those reviews to identify and close any gaps that may have opened. Here are some considerations to help develop good documentation and processes:

- Have clear, delineated documentation and processes to use for everything from building a machine or a service to how the company operates. Management plans and polices are the blueprints for your organization.
- Baselines will identify irregularities. Identify them within your documentation.
- Make it OK to ask security questions (within staff and clientele). Encourage mature and open conversations with clients and support teams. For example, help clients understand why a desired app or piece of software must be security checked prior to implementation.
- As you document your processes, identify what value the process ties in to. If you identify your values in these operating procedures it helps people to understand what that value is and support the procedural initiative. For example, if a process is to confirm a request for an updated payment bank account or check address via a second means of communication (the request comes in via email but must be validated via phone), the value that is being reinforced could be authenticity, integrity or open communication.

There are many stages of maturity in documentation as an organization grows. The reliance on process will either allow an organization to scale quickly and efficiently or drown in unplanned project issues and unsatisfactory deliverables. The policies and processes will likely go through many iterations of improvements as technical and physical cybersecurity controls are added. Good governance encourages the right behavior, ie how people behave when no-one's looking. Culture is strengthened through well-communicated, right-sized and appropriate governance The most important rule of thumb is to ensure the procedures match the actual functionality needed of the business unit or role; establishing cyber-secure procedures that cause business disruption, job dissatisfaction or loss of efficiency will likely get kicked to the curb. Bring the stakeholders together to design the security improvements in the policies and procedures in a way that reinforces efficiency and company values at the same time.

Peer Reviews

Mistakes happen. Fostering the mindset of finding and remediating without fear of repercussion, looking dumb or getting written up will help to create loyalty and provide room for innovation. Referring to users as "the weakest link" or otherwise blaming people undermines their desire to report issues and ask for help.

Since most of us cannot see our own mistakes, controls as basic as a configuration guide or baseline document will benefit from a second person reviewing the work of the first one. And being able to review proposed changes will help the originator to learn and grow in their role. Quality control will also tie into multiple company values, another opportunity to embed cybersecurity into your culture.

Setting the tone of peer reviews is crucial. It is not a matter of not trusting the work being done, but ensuring all angles are examined. A peer review is also not considered "beneath me" type of work it is imperative work that ensures quality. This includes a thorough review with fresh eyes. A superficial review adds nothing more than if the individual who did the work reviewed it themselves. Have the discipline to think through the review process and commit the investment to have people double check the work of others. It's important to note that most frameworks include a peer review process control. If you or your clients have regulatory compliance goals or requirements, you will need a peer review process in place.

Positioning Cybersecurity with your Clients

Up to this point, this paper has focused on your culture and values. But as you are acutely aware, clients play a significant role in the efficacy of cybersecurity. Extending the "security first" mindset from the MSP into clients is how you can differentiate your business from competitors. A culture that embraces cybersecurity and communicates the why's and how's behind policy and procedure is more than an MSP offering tech solutions. Instead of being the enforcer of cantankerous cyber rules, you can bring immense value as a partner in solving your clients' security challenges. This can and will result in new business.

As the examples above show, your relationship with clients will deepen as you work with them to help create their cybersecurity culture. If not already, help them manage their culture. Don't just sell them cybersecurity awareness software, work with them to manage the process, reporting, incentives to their employees and teach them to celebrate meeting specific goals and the wins when the cybersecurity culture changes and improves. You can include reviews of the cybersecurity culture as part of client business reviews and even encourage clients to do the same with their own employees.

Leverage the same techniques from the earlier portions of this paper to transfer this knowledge to clients. Expand tabletop exercises to include clients working with your techs. An example could be to allocate time on a monthly basis to go through the process of not only how to handle specific trouble tickets, but how to handle security related items. Whether it's dealing with client passwords, sharing passwords or simply communicating something seems odd. Work through how to communicate with each other in your organization, the client and vendors when it comes to security. Discuss ways to improve communication, processes and procedures, and cybersecurity awareness.
This example of how one MSP approaches the challenge of client cybersecurity illustrates how being a partner results in a better outcome for everyone:

"One of things we used to do when working with our clients to help improve their cybersecurity hygiene and improve the culture is whenever we found a computer unlocked, passwords written down or suspicious browser history, we would document the computer name and then issue a pink\red sticky note on the computer. We would tally these and at the end of the month, report it to our IT Liaison at the client. Whomever had the most sticky notes would have to buy lunch or coffee and donuts for their department. Of course, this was in collaboration with the client, and they communicated it to their employees. This created a positive challenge, somewhat of a game for them. If no one received any pink\red sticky notes, then we as the MSP would bring lunch, or coffee and donuts for everyone. All the employees at these clients were talking about it, holding each other accountable. It was successful and had a positive impact on the cybersecurity culture."

This example brings together culture, coaching and cybersecurity. It also shines a light on the diverse and large number of people that have a role in being responsible for cybersecurity. In fact, the sprawling of responsibility has even been recognized by a May 2022 Joint Cybersecurity Advisory co-authored by cybersecurity authorities of the United Kingdom (NCSC-UK), Australia (ACSC), Canada (CCCS), New Zealand (NCSC-NZ) and the United States (CISA, NSA, FBI) with recommendations on having transparent conversations with clients to define responsibilities on securing sensitive data.

Summary and Success

How do you know if your efforts to embed cybersecurity into your culture are working? As with any change, culture or otherwise, you'll want to establish measurable goals, rooted in your organization's values. From the examples of values addressed earlier, here are recommendations on how to evaluate success:

- Technical excellence means always looking for the right solution. Rather than simply fixing a symptom for something that looks suspicious, the value of technical expertise means running vulnerability scans and looking for indicators of compromise when a user reports that their keyboard is acting funny.
- Customer service means technicians remind clients when there is a behavior that is risky and reports that risk to the dispatch team who will frequently reach out to the client liaison and determine if the risk is acceptable. This allows faster recognition when clients are doing something wrong and report on it. Track these interactions through your client management tools.

- Communication can mean providing updates on critical infrastructure situations like when there is a known vulnerability in Windows. Especially when it is going to make a major news cycle. By reaching out in personalized emails and potentially phone calls on events that might worry an owner, cybersecurity is enhanced, the value is at the forefront, and the client is engaged. Clients then have a clear set of actions that need to be taken and the MSP is positioned as a partner in their cybersecurity.

There are communities out there to help you. This paper comes from one of many of CompTIA's work groups focused on helping the industry succeed in its role as the steward of protecting sensitive data. Membership with CompTIA includes the CompTIA Information Sharing and Analysis Organization (ISAO), which is where the May 2022 Joint Cybersecurity Advisory referenced above was received. Peer forums and real-time threat information pulled from multiple sources along with the tools to manage it all are at your fingertips. Having great information and a quality group of peers allows you to be the partner to your clients they need you to be.

A self-assessment of your culture, values and how security fits is always a great place to start. Work through the recommendations within this paper, keep talking and keep learning.

Special thanks to all of the contributors, reviewers, writers and work group volunteers coming from large and small MSPs, international corporations, and individuals from across the industry that helped create of this paper:

Dave Alton, CTO, Strategic Information Resources, Inc.
Joy Beland, VP Partner Strategy and Cyber Education, Summit 7
Bill Campbell, CEO, Balancelogic
Anu Khurmi, Managing Director, Global Services, Templar Executives Ltd.
Gema Perez Cortes, Global Cyber Risk & Compliance Lead, Capgemini
Jhovanny Rodriguez, Vice President & Co-Founder, Greenlink Networks
Natalie Suarez, Principal Solutions Advisor, Connectwise