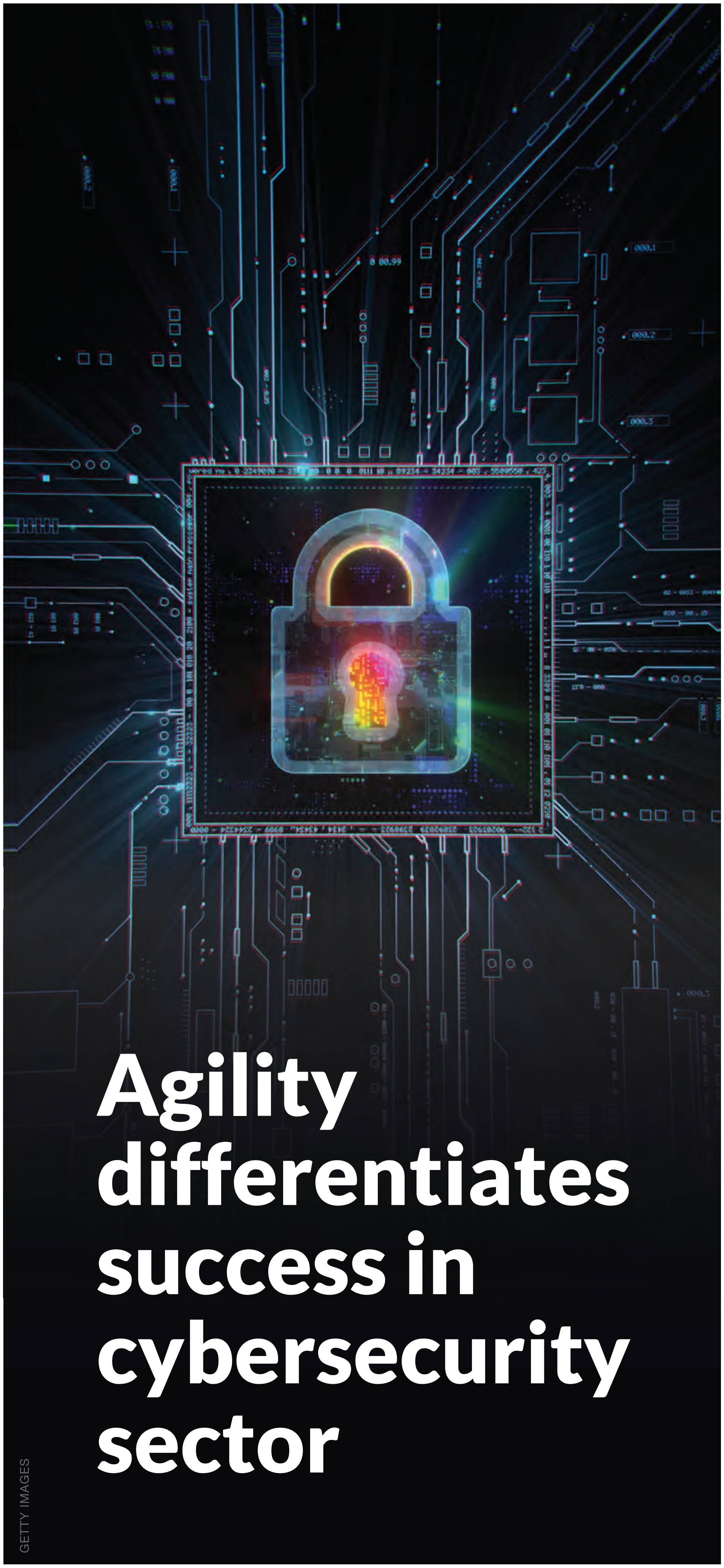

Agility differentiates success in cybersecurity sector

GETTY IMAGES

Cybersecurity impacts every aspect of daily living from basic online consumer activity to broad issues of national security. While innovative technology across domains continues to advance at breakneck speeds, so too do threats to cybersecurity that can have devastating effects. Companies need more than technical expertise to combat nefarious actors as well as to stay operational and competitive. Organizational agility — the ability to innovate, demonstrate situational flexibility, learn, and connect with nuanced environments — is the gold standard in differentiation within the cybersecurity space.

In connection with the GW College of Professional Studies' (GWUCPS) Center for Excellence in Public Leadership, the Washington Business Journal recently presented a roundtable discussion with local leaders in the cybersecurity industry and top administrators from the GWUCPS to discuss organizational agility as a multi-faceted business requirement within the swiftly expanding field of cybersecurity.

Participants included: Hart Rossman, vice president, Global Services Security, Amazon Web Services; Matt Hayden, vice president, Cyber Client Engagement, GDIT; Debbie Sallis, executive director, The Cyber Guild; Mike Baker, vice president, chief information security officer (CISO), DXC Technology; Amanda Sawicz, vice president of growth, Aretec Inc.; Liesl Riddle, dean, GWUCPS; Jim Robinson, executive director, GWUCPS, Center for Excellence for Public Leadership; Kafuti Talahumbu, associate director of corporate relations, GWU; David Walker, vice president, sales, Washington Business Journal.

Following are excerpts from the discussion, edited for publication.

What comes to mind when you think about organizational agility from a leadership perspective?

MATT HAYDEN: To us, it's the ability to stay ahead in receiving and implementing new technology that comes out. That means bringing in new experts on a regular basis. There's a constant growth cycle that we have to adapt to so we can rapidly meet the evolving goals and missions of the government.

It also means making sure we're built to support the employees we have. That includes upskilling employees and making sure that as these new technologies come in, we're reinvesting in them. That's part of that cycle. It isn't just to say we need new people. It's to take the individuals who have great strengths and to build on them.

MIKE BAKER: Organizational agility is an imperative for any company. It's the ability to adapt to change and who you are hiring, training, and mentoring to be able to meet that change head-on. In tech companies, I think there is a premium on that ability considering how fast it's evolving.

The problem that we have sometimes in the tech world is a lack of focus on soft skills development. People are naturally scared of change. Everything won't stay the same, so as leaders, when you think of organizational agility, you've got to think on your feet and lean into change and lead your team during change. You've got to be able to meet customer or threats where they are. I think that starts with the human being and making sure they have the tools, skills, emotional support, and soft skills to deal with and embrace change in general.

DEBBIE SALLIS: With my HR background, my first reaction is always from the employee end and how an organization needs to think about where people are at in order to help them get to where you need them to be. Agility is a scary word for most people because it means transformation to them, another word for redundancy. Reskilling is another word for who's going to lose their job. Trying to think about language and how you talk to people about what you're trying to do is a big challenge.

JIM ROBINSON: A major challenge when it comes to agility is that many leaders are used to top-down driven change. They have a challenge with empowerment and what it means to empower at the lower level. That's a real reorientation for many leaders.

What leadership traits or attributes make someone in cybersecurity successful?

AMANDA SAWICZ: In the realm of cyber leadership, the significance of empathy cannot be overstated. Empathy serves as a catalyst for unifying team members, fostering motivation, and steering collective efforts towards achieving favorable business outcomes. Acknowledging that technology relies fundamentally on human engagement, cyber leaders must prioritize the well-being and development of their team members. By nurturing a supportive environment, leaders empower their teams to drive successful results within the dynamic landscape of cybersecurity. At the end of the day, technology doesn't do anything without people. You have to take care of the people on your team, and the people are going to take care of the results.

HART ROSSMAN: One of the things that really helps security leaders to be successful in an environment where they're encouraged to focus on risk or what can go wrong is being optimistic and understanding, and being able to act on signals of success. Double down where things are working and scale that out so that everybody can benefit.

Likewise, when you learn from a mistake, you've got to be able to very quickly adapt, overcome, and then, again, scale out whatever that course correction is so that everybody benefits. If you encourage your people to be high-velocity decision makers, they're equipped to make a decision that they can deeply own end-to-end. They understand what the need is, they understand what they have to do, they can take the action, and then they can own that success. If they make a mistake, they have an opportunity to learn from it and then do another iteration.

MIKE: My number one value is leading with trust in our interactions. If you don't lead with trust and assume positive intent, it can create an adversarial relationship and impact agility.

Where does cybersecurity belong in the organizational structure? Do CEOs need to be security experts?

DEBBIE: Cybersecurity is an integral part of the business. It's a fundamental risk to technology, client data, shareholder value, and maybe national security. To me, cybersecurity is becoming as big as the financial numbers in terms of some underpinning risk to the organization.

As an investor and shareholder, I expect the CEO to be able to have the bandwidth and the capacity to have foresight and understanding.

MIKE: While a CEO may not be a cybersecurity expert, they are ultimately accountable to shareholders and new rules are requiring disclosure of significant cybersecurity incidents. So, I think the role of the CEOs and cyber is rapidly evolving with regulatory change and require them to be closer to managing and explaining cyber risk.

HART: At AWS, we talk about this idea that security is the top priority right up there with operations and some other important things. The way we expose that, for example, is through this weekly security meeting where our CEO is meeting with top leaders that are driving our security culture and our security outcomes. They're doing it in the same way that they meet with finance or HR.

My experience in other organizations is that security is not treated as an operation or as a fundamental part of the business. It's treated as a series of projects and programs under a leader.

I think that that's a very different mental model about the value of security to your customers and to your employees and your business than if it's a routine part of business operations. Having security leaders is critical. It's important that the business treats it as a fundamental aspect of operating the business.

How are industry and academic institutions working together to develop talent and create opportunities for employment, whether it's entry level, upskilling, or career changes?

MATT: We are constantly building partnerships with high schools, community colleges, universities and other organizations across the country to expand the cyber talent pipeline. For example, we engage with the Community College of Baltimore County, which has an amazing cyber program that's very specialized. At the same time, we're working with organizations such as GWU to help educate the institution on what skills a graduate needs in order to be able to jump in and get their feet wet. Having people that can hit the ground running is just as important as their diploma.

LIESL: At the GW College of Professional Studies, we have created a culture of market-responsive innovation to foster agile academic program development. Our faculty — most of whom work in industry and government like you — are thought leaders, who are anticipating what the cybersecurity workforce needs today and tomorrow.

Informed by conversations like the one we are having here today, we offer an end-to-end educational solution in cybersecurity. Our comprehensive curriculum — including bootcamps, bachelor and masters degrees, and continuing and executive education — allows working professionals to upskill and reskill in evening and weekend program formats.

Our learners will engage in online learning circles, in the evening at our classrooms in DC and Northern Virginia, and onsite at our industry and government partners, such as yours.

One of the things I've learned from conversations like these is the importance of fostering a cybersecurity workforce that is not only responsive, innovative, and technically excellent but also have strong soft-skills as well. Leadership, teams, managing change and human capital are critical too.

MIKE: We're looking for people who can integrate with the team not just technically but with the company values. Can they work successfully in the room? Do they possess similar organizational values? Do they seem to lead with trust? We've had so much success finding people who are curious about security and putting them in a position to grow into the role. Maybe they're coming out of the military or government service or hold a different role or in the organization.

It's an awesome opportunity to bring them in, leverage their unique experience, their worldview, their perspective, inject that into the culture, to help us think.

The George Washington University College of Professional Studies is an accelerator for career transformation in cybersecurity.
To learn more, go to: **https://cps.gwu.edu/cybersecurity.**