Sponsored Content

thought leadership roundtable

Technology/Cybersecurity

Technological advancements heighten cybersecurity challenges

Technology experts at Eleven Fifty Academy, LEAP Managed IT, Purdue Research Foundation, Resultant, and Trava discuss how organizations can minimize risk in today's cybersecurity environment.

JIM GOLDMAN
Co-Founder and CEO
Trava
jim.goldman@travasecurity.com

SEAN HENDRIX
NineTwelve
Sr. Technology Consultant
Purdue Research Foundation
sean@ninetwelve.us

MICHAEL THOMAS
Chief Operating Officer
LEAP Managed IT
michael@leapmanagedit.com

MIKE VANCE
Vice President of Technology Services
Resultant
mvance@resultant.com

DAVID WHITT
Senior Director of Cybersecurity
Eleven Fifty Academy
dwhitt@elevenfifty.org

Q: Let's start with a discussion of cybersecurity. Every day there seems to be news of a data breach. What are organizations doing wrong and how can they protect themselves?

JIM GOLDMAN: I think it's less about what organizations are doing wrong, and more about not doing enough. The current approach to cyberrisk management is broken, particularly for small- to medium-sized businesses. It's easy to get caught up in buying what appears to be the next big cybersecurity tool. But a random collection of security tools does not a cybersecurity program make. Today's cyberrisk management must involve a comprehensive integrated strategy that first includes understanding your risk with regular vulnerability assessments, then mitigating risk by repairing the most severe areas of vulnerability, and finally, transferring residual risk with cyber insurance. Most companies are not considering all three parts of the strategy. Companies can take some very manageable first steps to protect their data, but the most important first step is knowing where your systems are weak.

SEAN HENDRIX: The starting point is awareness. This is where the concept of "zero trust" comes into play. As a business community, we tend to default to a condition where we trust the networks we are using. If we, as business leaders, buy in to the idea of zero trust, we will drive awareness in our organizations and provide the leadership required to implement the cybersecurity measures necessary to protect our networks.

MICHAEL THOMAS: Unfortunately, cyberrisk is part of the landscape that business leaders have to navigate, and trends keep going in the wrong direction. Due to continual technology advancements and increased utilization of third-party platforms, achieving a 100% risk-free posture is not possible. What is possible is for organizations to develop a cybersecurity plan and to have the discipline to test, adjust and improve it as an ongoing business improvement process.

> *"The current approach to cyberrisk management is broken, particularly for small- to medium-sized businesses."*
> JIM GOLDMAN

One of the most overlooked, yet most critical, aspects of a cybersecurity plan is around training and testing employees. It is hands down the best investment an organization can make and if properly managed can cut in half the overall threat risk to an organization. Beyond training, we are seeing a big increase in enterprises adopting endpoint detection & response and multi-factor authentication services, both of which are extremely effective at reducing overall cyberrisk.

MIKE VANCE: Cybercrime is constantly evolving, so it should be no surprise that data breaches are happening with greater frequency and greater impact to organizations. If a system was put in place and hasn't been monitored or maintained, it should be immediately reviewed.

A solid cybersecurity foundation focuses on securing two major categories: accounts and data. To improve account security, implement multi-factor authentication with centralized account management through use of single sign-on. This approach can reduce the risk of social engineering attacks such as phishing, which has emerged as

Sponsored Content

the most predominant threat to an organization's accounts. Data is secured through access authorization and authentication as well as data-loss prevention policies incorporating governance and technical controls, mobile device management, and zero-trust methodologies. None of this reduces the need for ongoing monitoring of these controls. Implementing a regular maintenance and security review cycle to audit accounts and data and remediate any oddities or areas of concern is imperative to cybersecurity.

DAVID WHITT: Best practices to prevent a cybersecurity attack are not always well-understood throughout an organization. Also, hackers are getting better at what they do. For optimal protection, an organization must first acknowledge that they are potentially vulnerable. Second, it's important to have qualified personnel on staff or on contract who continually look for innovative ways to negate potential threats.

Q: How does 5G technology figure into cybersecurity concerns these days?

DAVID WHITT: According to the Brookings Institute, the 5G "race" is the focus for retooling how we secure the 21st century. 5G technology is moving toward a web of digital routers that denies inspection points. Inspection points are where protective measures have existed, thus creating opportunity for innovative cybersecurity solutions. The 5G shift also opens new avenues of attack and opportunity to protect from Internet of Things breaches.

SEAN HENDRIX: 5G offers a future where almost everything we work with becomes connected to the network. We see this already in our daily lives with the adoption of ring doorbells and video streaming services. Going forward, we will see this level of connectivity in our physical industries, such as manufacturing and agriculture. Unfortunately, this increase in the number of connected devices comes with an increased risk for cyberattacks.

MICHAEL THOMAS: The introduction and expansion of 5G technology is creating a revolution for a lot of industries and providing profound benefits to consumers as well. As with a lot of advancements, it also brings with it a lot of new and expanded risk. The proliferation of connected devices, super-charged data transfer speeds and decentralized routing paired with advancements in Artificial Intelligence give the bad actors potentially more opportunity to exploit networks and users.

MIKE VANCE: As a society, we are mobile. Thanks to advancements like 5G, work takes place anywhere and everywhere that we are. A cybersecurity plan developed to secure an area such as the office network—as opposed to your accounts, data, or devices—is missing the complexity of the modern workforce. Mobile device management, or MDM, is a requirement for organizations thinking about security in the context of how people work today. These systems allow organizations to manage the company data and accounts on the device, putting in place controls to ensure data stays within the organizationally approved locations and not directly on the phone, tablet, or other mobile devices. MDM allows controls that support elimination of data should the phone be lost or missing.

Q: Please explain how Zero Trust Architecture is meant to address these cybersecurity concerns? What are the pros and cons?

MIKE VANCE: Zero Trust Architecture is an ominous name for an approach to cybersecurity that acknowledges that people and their devices are working everywhere. It's built around the premise that there is no home base and no secure locations, meaning that the architecture of the cybersecurity program is designed to secure your organization's accounts and data regardless of where they are. This approach meets the needs of today's modern business with the flexibility needed to work securely anywhere.

DAVID WHITT: Zero Trust Architecture is an initiative that is in place to help prevent full data breaches by eliminating trust from an organization's network architecture. When you hire someone who specializes in zero trust, you get someone who can prevent breaches that are becoming more common from network architecture. The downside is that trust will take a moment longer because you're going from "always trust" to a "never trust, always verify" scenario. From a technical perspective, there are many ways of leveraging network segmentations, preventing lateral movement where an organization's network architecture has experienced breaches.

JIM GOLDMAN: Zero Trust is an underlying design assumption, a risk management philosophy. It is a framework built for large enterprise-scale companies that is based on a very strict identity verification process whereby only authenticated and authorized users and devices can access applications and data. It can be one very effective way to protect against cyberthreats, but it is a predesigned solution that is meant to be applied generally to any large-scale organization. In other words, boilerplate. And you are starting with a solution, rather than doing a risk assessment to identify the true areas of risk unique to your business. For small, even medium-sized businesses, Zero Trust is a bit of overkill. One important way to protect themselves is by implementing two-factor authentication as a form of identity verification.

SEAN HENDRIX: Implementing Zero Trust Architecture—when you are deploying a large population of connected IoT devices—will mitigate your risk of cyberattack by securing every layer of your communications stack: transport layer, control plane, and data plane.

Q: What can small- and medium-sized businesses do to protect themselves on a budget? How does cyber insurance figure into all of this?

MICHAEL THOMAS: It starts with having a plan and acknowledging the potential risks that are out there. Some organizations either avoid the conversation completely or assume that they have everything covered from a cyber standpoint. Definitely not the recommended approach.

There are a lot of state and federal resources out there to help small- and medium-sized companies. CISA.gov is a great place to get started. Investing in an outside expert to perform a cyberrisk assessment can help quickly identify the current risk profile and provide critical mitigation strategies. The cost is typically minimal given the benefits.

Cyber insurance will encourage an organization to put certain cybersecurity standards in place. The caveat is that an insurance policy is a two-way agreement. The organization must also agree to adopt and enforce standards included in the policy, such as multi-factor authentication. Make sure to take the time to ask questions about how a policy will help your organization sustain operations. Will it cover lost revenue, attorney fees, remediation, or potential claims?

MIKE VANCE: Small- and mid-sized businesses have the same security goals as enterprise organizations but fewer resources to accomplish them in an ever-changing environment. All organizations should start with the foundational goals of securing accounts and data and conducting ongoing monitoring. For small and mid-sized businesses, finding a credible partner will help alleviate the expense of ongoing monitoring and maintenance as well as ensure consistent attention on evolving threats.

Providing cybersecurity training for employees is also vital. As cybercriminals develop new methods to gain access to your organization's data, your employees continue to stand as the final defense against them. A well-trained user base will save an organization from a breach time and time again.

See page 24

Continued from page 23

Sponsored Content

Without proper security protocols, systems, and controls in place, cyber insurance won't be an option. Regardless of an organization's size or insurance status, a strong cybersecurity posture is recommended.

DAVID WHITT: Cyber insurance should be figured into any business that stores information such as Social Security numbers, credit card numbers, account numbers, driver's license numbers or health records. The insurance will cover you if you have data breaches and will depend on the size and amount you need covered. Most states do require a company to notify customers of a data breach, which could be extremely extensive and expensive without coverage. This insurance protection should be a line-item on your business budget, regardless of being a small, medium, or large company.

And, if possible, all businesses should hire a team that can actively monitor and be kept up to date on any active or "zero-day" threats. Zero-day refers to the fact that the developer has only just learned of the flaw and has "zero days" to fix it. Another good option would be hiring a pentesting (penetration testing) company to find and exploit any vulnerabilities. This is a best practice that should be secured on a regular basis. All businesses should also train their personnel on the latest security practices, along with ensuring their software is updated, as well as their computers. These measures will limit their potential for a breach.

JIM GOLDMAN: Every company is different and has a different level of cyberrisk. You must start with a risk assessment to understand where you are vulnerable and how to prioritize your action items for mitigation. And it can't just be one time. There are affordable solutions that allow businesses to run regular vulnerability risk assessments, so you can lay the groundwork for a comprehensive integrated strategy, whether you are doing it in-house or through your managed service provider.

Implementing two-factor authentication is another good start. And providing regular security awareness and training to your employees is very important. Make sure it includes interactive exercises to identify phishing emails. Phishing is one of the most common ways that cybercriminals enter your company. Make sure your data is backed up and accessible. That way, if there is a breach and your data is being held hostage by ransomware, you can reinstall the backup and minimize your business interruption.

Cyber insurance policies are becoming a requirement for doing business, but insurance companies are proving to be more risk averse. Companies with a comprehensive cyberrisk management program in place have a better chance of getting a policy and attaining better rates. But they must do their part. Cybercriminals are getting smarter, they're getting more aggressive, and insurance companies are no longer willing to absorb that kind of risk if a company does not have protective measures in place.

SEAN HENDRIX: Moving to secure cloud services will allow small- and medium- sized businesses to leverage the security capabilities of the IT industry. Implementation of virtual private networks and similar connectivity provide layered security methods, especially when working in remote- or tele-work environments. Taking care to bring these principles and a zero-trust approach to manufacturing and other IoT-heavy environments is also important as more devices continue to be connected to business networks.

Cyber insurance is an interesting topic. One perspective is that cyber insurance helps after the cyberattack has happened and the damage has been done. Monetary loss may not be the only effect of a cyberattack; time and intellectual property can also be casualties. Insurance can be useful, and each business needs to make its own value determination. However, industry best practices promote a proactive approach where cyberattacks are prevented or mitigated from the beginning.

Q: What do you think the cybersecurity landscape will look like five years from now?

SEAN HENDRIX: The cybersecurity landscape is only going to get more complex over the next five years. With the massive increase in the number of connected devices and the ubiquitous nature of connectivity, this presents a large increase in available attack points. The silver lining is that industry is aware and racing to deploy solutions. It is a race and it's not clear yet whether attacker or defender will end up on top.

MIKE VANCE: There's no doubt that cybercrime is going to continue to evolve and intensify. There is too much investment in the crime itself for us to believe that a cybersecurity defense that works today will be relevant five years from now. Organizations need to be prepared today and continue to stay current with cybersecurity programs.

DAVID WHITT: Cybersecurity will have its place within every organization, similar to a must-have HR component, and will be something that is taught in schools at earlier stages. With the rate that technology innovates, advancing a cyber team is a good tactic to keep the company covered from new vulnerabilities and ensure personnel are up to date.

JIM GOLDMAN: Given the current trends of frequency and the gravity of today's cyberattacks, if businesses are unwilling or unable to put measures in place to stem the tide then it will have to be mandated by government. Ransomware has become its own economy. That has to change. If these trends continue, cyber insurance will be unattainable, either because insurance companies will stop covering cyberrisk or it will simply be too expensive. Every company from small to enterprise scale will proactively put comprehensive cyberrisk management strategies in place. Or it will be legislated. And/or, new and existing customers will stop doing business with you because they are not confident that their data is being protected.

Q: Moving on to questions about talent, what is the job outlook for people interested in cybersecurity careers, and how are those jobs being filled?

JIM GOLDMAN: In the past, if you wanted a career in infotech or info security, you became a software engineer. As cybersecurity and cyberrisk management have expanded as a discipline, there are a wide variety of roles much more specific to risk management, incident response, and compliance. There are now more jobs than talent in the field of cybersecurity and cyberrisk management.

SEAN HENDRIX: In short, the job outlook is very strong. As we discussed previously, the proliferation of networks (both wired and wireless) and the number of devices is increasing rapidly.

MICHAEL THOMAS: The market continues to be very strong for individuals in IT, development, and cybersecurity. At LEAP we have developed a two-year cybersecurity apprenticeship program to help individuals with limited experience learn the core infrastructure management skills and help them progress to a cybersecurity analyst role at the end of the program. Purdue University and Eleven Fifty Academy have both been great partners for us in helping supplement training for our team.

MIKE VANCE: Because of the evolving and growing threat, cybersecurity roles within internal IT teams and tech partners will only increase in demand and importance. The opportunities are plentiful for those beginning their careers as well as for experienced individuals looking to enter the field.

DAVID WHITT: Careers in cybersecurity are the hottest in the tech market and there is no sign of this slowing down. In fact, demand is increasing at an unprecedented rate. We at Eleven Fifty Academy are doing our part to fill these jobs through our accelerated Cybersecurity immersive program, which was recently named among the Top 10 cybersecurity courses in

Sponsored Content

the U.S. and best for certifications by intelligent.com. The expected growth rate for cyber jobs is 62% through 2022. Given the plethora of cyberthreats each week, a career in cybersecurity equates to job security.

Q: What are Indiana's strengths as it tries to retain/attract top tech talent when it comes to cybersecurity?

DAVID WHITT: Eleven Fifty Academy had the first cyber range in the state and was the first coding bootcamp in the U.S. to have world-class, globally recognized certifications available at an accelerated pace to launch into a career in cybersecurity. We are working to meet demand locally, with home-grown talent.

JIM GOLDMAN: Tech opportunities seem to be on the rise, particularly in Indianapolis. It's more affordable than the traditional tech hubs like Austin or San Francisco. And there are venture capitalists like High Alpha who are investing in Indiana tech startups, as well as organizations like TechPoint that sponsor tech events and awards programs. It's becoming a hotspot for IT and digital services.

"Doubling down on cybersecurity personnel will save a lot of money long-term."
DAVID WHITT

SEAN HENDRIX: We have a strong technology sector already in place and the adoption of connectivity and IoT for physical industries, such as manufacturing and agriculture, driven by the adoption of Industry 4.0 creates additional opportunities. These opportunities combined with Indiana's strong quality of life/quality of place puts Indiana in the pole position for job opportunities.

MICHAEL THOMAS: Indiana is such a great place to live and raise a family. I can attest to that myself after moving from Chicago 10 years ago. We have a lot of higher ed institutions focused on training cybersecurity skills, coupled with plenty of career advancement options. Graduates can look ahead and see that Indianapolis can easily support a 10-to-20-year career path. That's very enticing and hasn't always been the case for this industry locally.

MIKE VANCE: Indiana's strengths come in the sizable job landscape here, the breadth and depth of education options for students at many different career points, and the quality of life that Indiana residents enjoy. People can begin their careers within the field of cybersecurity or successfully transition to the field later in life.

Q: What are the biggest obstacles to talent retention and attraction?

MIKE VANCE: To retain our talented and curious technologists, Resultant has committed to developing and growing their skillsets to keep up with new technology and expand their opportunities technically and as leaders. We've also found that despite a desire to be able to work anywhere, our teams still desire to come together for collaboration and connection, whether it's for social purposes, ideation, learning, or something else. Enabling collaboration and connection within any work environment has allowed Resultant to attract, hire, and retain exceptional talent.

DAVID WHITT: Communities that are wonderful places to live, work, and play win over others that may struggle with one of these economic development pillars. Having quality educational options is also a key component. Companies need to skill up personnel via continuous education to stay up to date on the latest threats. Requiring updated certifications leads to a security mindset and better-prepared personnel.

SEAN HENDRIX: It's really numbers. There are an increasing number of positions and not enough talent to fill these positions. Continuing to fill the pipeline in the university system is important. However, increasingly re-skilling/up-skilling will play a role in filling these positions. We have the other ingredients of cost-of-living and quality of place.

MICHAEL THOMAS: Tech talent in Indy is no longer a hidden gem. We all see it with more and more tech companies setting up operations in the area. Demand is way ahead of supply. At LEAP, we keep team members by focusing on our core goal: being the best place to work. We make sure team members are challenged and fulfilled. Based on results of our engagement surveys, we are focused on redesigning roles to help get team members closer to our clients, where they can see their hard work making a difference in real time.

Q: Thinking more broadly about technology, what should IT leaders be thinking about as they prepare their 2022 budgets?

MICHAEL THOMAS: We approach every budget planning session like the scene in Apollo 13 where the engineers throw everything on the table and see what they can use to solve the problem at hand. Often, we see that the first step is to talk about all the new hardware widgets and software a company needs. We recommend slowing down and answering the questions: what problems need to be solved, can current technology be used better, and what can be stopped/discontinued altogether?

MIKE VANCE: At a high level, IT leaders should be thinking about their budget with proactivity and integration in mind. When preparing budgets, we work with clients to think strategically about the business, considering what future pains may be and what goals are to be met across the organization, not only within IT. This approach builds partnership across the organization and better serves the business. In 2022, these considerations will likely include ensuring a secure environment—but cybersecurity shouldn't only be a line item on its own. It needs to a part of every solution under consideration. Second, IT should be thinking about how to best simplify and connect systems to support the organization, its people, and the information needed to make sound decisions.

DAVID WHITT: Budgets should incorporate the cost of updating outdated legacy equipment, when possible, and its associated software. Doubling down on cybersecurity personnel will save a lot of money long-term. We see examples to support this nearly every day in the news.

JIM GOLDMAN: Business leaders should not budget for or spend money on anything until they truly understand what needs to be fixed. Make regular vulnerability risk assessment a priority and put it in the context of overall business objectives. Also, consider your sales and marketing strategies and how risk assessment and cyberrisk management is imperative to getting and retaining customers.

SEAN HENDRIX: If technology leaders can understand the business challenges and translate those into technology requirements, IT budget needs will be quickly identified. The challenge for technology leaders is in keeping up to date with technology developments—5G, cybersecurity and other IT developments are accelerating the pace of change. The biggest question we get today is "how do I use 5G in my business?"

Q: "System interoperability" is a term we hear more often these days. How does it play into a successful business strategy?

SEAN HENDRIX: The fact is we have been and will continue to operate in an environment with multiple generations of network, application, and device technology. However, new tools and solutions are becoming available in the market to reduce the complexity and redundancy previously associated with interoperability. Business leaders need to continue to assert their need for a "common operating picture" and not accept high complexity or system/data redundancy as a prerequisite for a solution.

MIKE VANCE: It's far-fetched to think all organization needs can be

See page 26

Continued from page 25

served by a single system. As growth happens, systems are added to meet new or changing needs. The urgency of the need often outweighs taking the time to implement with connection of systems and data. Therefore, resulting disjointed records create challenges across the organization.

Interoperability matches people and records across systems within the organization so a holistic picture can be viewed. The result is better information to run the business as well as reduction of exposure to cybersecurity risks and attacks.

DAVID WHITT: System interoperability refers to the basic ability of different computerized products or systems to readily connect and exchange information with one another, in either implementation or access, without restriction. The implementation of system interoperability increases productivity and reduces costs and errors throughout connected systems like health care. It also defines why you need an IT/cybersecurity team.

Q: What essential skills/positions do IT teams need today to effectively serve their organizations?

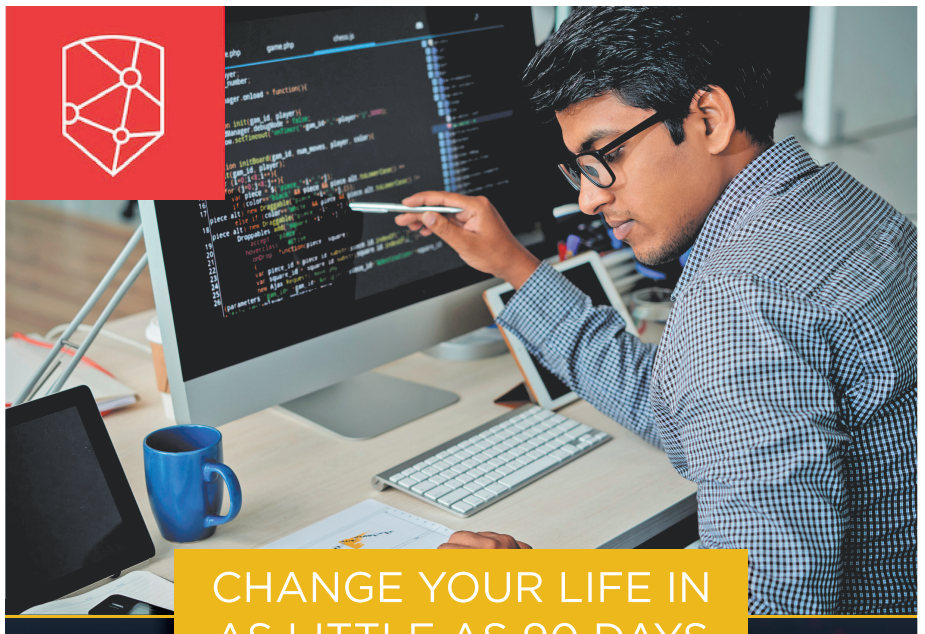
JIM GOLDMAN: Small businesses need to consider what essential skills/positions they need that are different than enterprise-scale organizations. They simply may not have the budget to accommodate a cybersecurity team or even an executive position. But that doesn't mean they have to do without. A virtual or fractional CISO (vCISO) allows small and medium-sized businesses to get high-level cybersecurity professional services on a part-time retainer or project basis.

SEAN HENDRIX: It is clear we are moving to a fully wireless network environment where a seamless, secure network environment is required. Network engineers need to continue to grow their skills to keep pace with these developments. The other skill set that is poised for explosive growth is OT, or operational technology. This is the process of taking traditional IT infrastructure and deploying it to the operations side of the business. The classic example of OT is connected IoT devices on the factory floor. As the digital transformation of our physical industries accelerates, OT skills will become increasingly important.

MICHAEL THOMAS: The project manager position is our fastest-growing position as we continue to be more client-centric and we continue to add PMs with foundational IT skills/knowledge in 2022 and beyond. Individuals who can lead, keep projects on track and advocate for the client/end user are a real difference maker.

MIKE VANCE: Today, essential skills always include cybersecurity expertise, whether that's accomplished in-house or through a partner. Today's high-functioning teams also need to include strategic expertise—an area where our Resultant team is often sought out for partnership. Without IT strategy, organizations get into a reactive cycle of responding to issues. Approaching technology proactively and strategically results in a team and environment better equipped to support the organization and employees.

DAVID WHITT: Communication skills cannot be overstated. Individuals who think outside the box, offer creative solutions, and are attentive to the needs of their organization as well as being good listeners are all essential for building an effective and successful IT team. At Eleven Fifty Academy, we incorporate essential skills training into our curriculum to benefit the individual and their employer. ●



Jim Goldman is the co-founder and CEO of Trava, a cyberrisk management company. He is a nationally published author, frequently requested speaker, and regular content contributor to Forbes on the topics of cybersecurity and cyber insurance.

TRAVA

Sean Hendrix is a senior technology consultant for Purdue Research Foundation specializing in new product introduction. He has 23 years of experience starting organizations that engineer, develop, and launch new products for production and is presently CTO of NineTwelve Institute and Managing Director of the Indiana 5G Zone.

5G ZONE
INDIANA | POWERED BY NINETWELVE

Michael Thomas is Chief Operating Officer of LEAP Managed IT. Prior to joining LEAP in 2014, he worked for more than a decade at a Fortune 200 firm where he was responsible for a nationwide team dedicated to consulting with large organizations on how to use technology to improve business results.

LEAP MANAGED IT

Mike Vance serves as Vice President of Technology Services, formerly KSM Consulting. In this role, he leads a team of over 120 technologists helping clients identify and execute a strategic IT vision that enhances business effectiveness. Mike brings over 25 years of experience leading enterprise technology teams, most recently as the CIO of Vera Bradley.

Resultant

David Whitt is Senior Director of Cybersecurity at Eleven Fifty Academy. He is a veteran of the U.S. Air Force, for which he served as a technical engineer on top-secret aircraft. He was drawn to Eleven Fifty Academy as a student to further explore his love of coding and has stayed on to lead Eleven Fifty's cybersecurity efforts.

Eleven Fifty Academy

Content paid for by Eleven Fifty Academy, LEAP Managed IT, Purdue Research Foundation, Resultant, and Trava.