TABLE OF EXPERTS

ADVERTISING SUPPLEMENT

ST. LOUIS BUSINESS JOURNAL

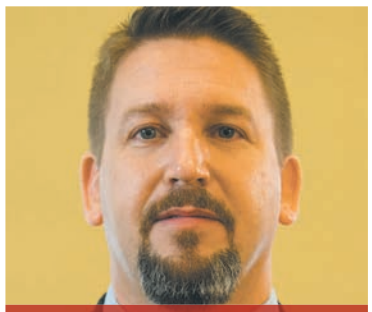
THE EXPERTS

DUSTIN LOEFFLER

Loeffler is assistant professor of cybersecurity and MBA program director with the John E. Simon School of Business at Maryville University. Loeffler comes to academia after 12 years of experience working for leading information security companies, such as IBM and Boeing, and continues to consult and present on information security issues. Dustin is a Certified Ethical Hacker (CEH), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM) and a Certified Information Systems Security Professional (CISSP).

TONY MUNNS

Munns, a partner in the Brown Smith Wallace Advisory Services practice, leads the firm's IT audit and security teams. Major projects include IT audit, security, HIPAA and PCI implementation services and technology attest reviews such as AICPA SSAE16 SOC1 and SOC2 reviews. He helps companies manage the risks associated with the use of technology. Munns is certified as a Chartered IT Professional (CITP) and Certified Information Systems Auditor (CISA).



JASON WOOD

Wood is director of operations for SpearTip with over 25 years of experience in security management and intelligence operations, and is a recognized Subject Matter Expert (SME) providing senior level counsel and advice on counterintelligence (CI) specific operations, doctrine, concepts, methodologies, analysis and training. He continues his efforts in protecting corporations from collection efforts of the Chinese, Russians, and other foreign or domestic entities targeting domestic clients.

BRYAN ARD

Ard has more than 20 years in consulting with 16 of that in solutions consulting. He has primarily worked in and around the financial services, health care and telephony verticals, providing leadership in the deployment of infrastructure and improvement of IT operations. Bryan has worked in the Information Security space for the majority of his career, helping to equip the business risk management function with a pragmatic approach to Information Security. He currently serves as the Information Security Officer for CenturyLink Technology Solutions.

AUDREY KATCHER

Katcher is a business advisory services partner at RubinBrown. Katcher has more than 20 years of public accounting experience covering Cloud Security, Internal and IT Audit. She is an author of the AICPA SOC2 guide and national leader for SOC1/SSAE16/ISAE3402. Katcher is a Certified Information Systems Auditor (CISA),and a Certified Public Accountant (CPA).

CYBER SECURITY

Security in an unsecure world

PHOTOS BY
DILIP VISHWANAT | SLBJ

▸ HOW SHOULD CYBER SECURITY BE ADDRESSED IN EDUCATION?

Audrey Katcher: Education of cyber risk and security needs to continue to focus on technical knowledge, while also having a path for developing communication skills. Companies need highly technical team members who can bridge the communication gap with business.

Dustin Loeffler: At Maryville University, we recognized there was a gap between employer needs and the available talent pool within the cyber security field. To close that gap, we created a new bachelors of cyber security major, which is enrollable as of fall 2014 and has different tracks. The unique part of our curriculum is that coursework covers and prepares students for information security certifications. Also, our tracks allow students to specialize in areas such as computer forensics. The key is to get our students on Day One to be practitioners with their employers.

▸ WHAT ARE THE GREATEST CYBER CHALLENGES?

Audrey Katcher: The leading cause of data breaches is actions of people, or a lack of action by people. Companies need to heighten awareness and skill sets among their employees, contractors and vendors. A health check of the people and process and technology supporting a strong cyber security environment can lead to proactive awareness sessions,

enhanced hiring/contracting plan for technical support, improved contracting with third parties and initiation of cyber resilience planning. Our "wrapper" of cyber controls services help before, during and after the incident. Also, IT is no longer within the traditional boundaries of a company. The boundaries have spread with mobile devices, third parties/vendors and data movement. It's critically important to ensure the security of mobile, vendors and information movement through independent assessments and then to manage that risk through mitigation as well as, potentially, insurance. A key security report to request of third parties/vendors is the Service Organization Control 2 (SOC2) reports, which assess the entities' security to help you understand the security over the information they house for your business.

Dustin Loeffler: Having 12 years of experience at both Boeing and IBM, I learned first hand as a hiring manager what hiring requirements I needed, and I'm translating those requirements into a curriculum that supports those requirements within academia. The Bureau of Labor statistics reports that cyber security will grow by 22% from 2012–2022 and includes a median pay of $86,000. So it's a field with a very low unemployment rate and it is compensated very well. These are a few of the strategic factors we looked at when introducing this new major.

Jason Wood: Working with Global 200 and Fortune 500 clients, I'll tell you, it's their awareness of the cyber threats that they face today and also their failure to recognize and embrace that cyber security best practices is actually a business decision.

Tony Munns: The lack of resources focused on IT and IT security specifically is one of the biggest constraints. The awareness at the executive management and the board level is one of the biggest obstacles, in terms of recognizing this as a significant risk for the continued viability of the company. A major incident has a devastating effect, and these incidents are starting to get that message through.

Jason Wood: A simple breach will cause absolute harm to a corporation's reputation or brand reputation. And obviously harm to their potential profits down the road, and we've seen that. So we talk to the C-suite and tell them they have to take responsibility. They're held liable for the actions that happen within that corporation.

Bryan Ard: There's a global shortage

of talent. Talent doesn't equal training. Training is Step Zero, and then a very small percentage of people that are trained will actually grow to be true talent. And that talent is in global demand. So you're seeing a lot of industry start to look at partners to provide those higher services because even if they attract the talent, they can't retain the talent because they can't pay the wages that are required to compete globally with everybody else, or the work just isn't interesting enough.

"You just may not be exactly what they're targeting. They want to use one of your systems to target somebody else."

JASON WOOD,
SpearTip

When we start talking about how the information security function partners with the business, increasingly, you're seeing a shift away from what I used to call ivory tower mentality and associated best practices. They were completely disconnected from the traditional risk management function, so the business wasn't involved. You had information security mandating things that would inhibit a business' ability to execute, so the business would become resentful and sometimes would actually defund the function or simply ignore it. If you don't add value to the business, you're not helping drive revenue. So what is your value brought to the business? Practitioners need to continue to learn how to sell the importance of the services are that they provide to the business and the associated value to the end customer.

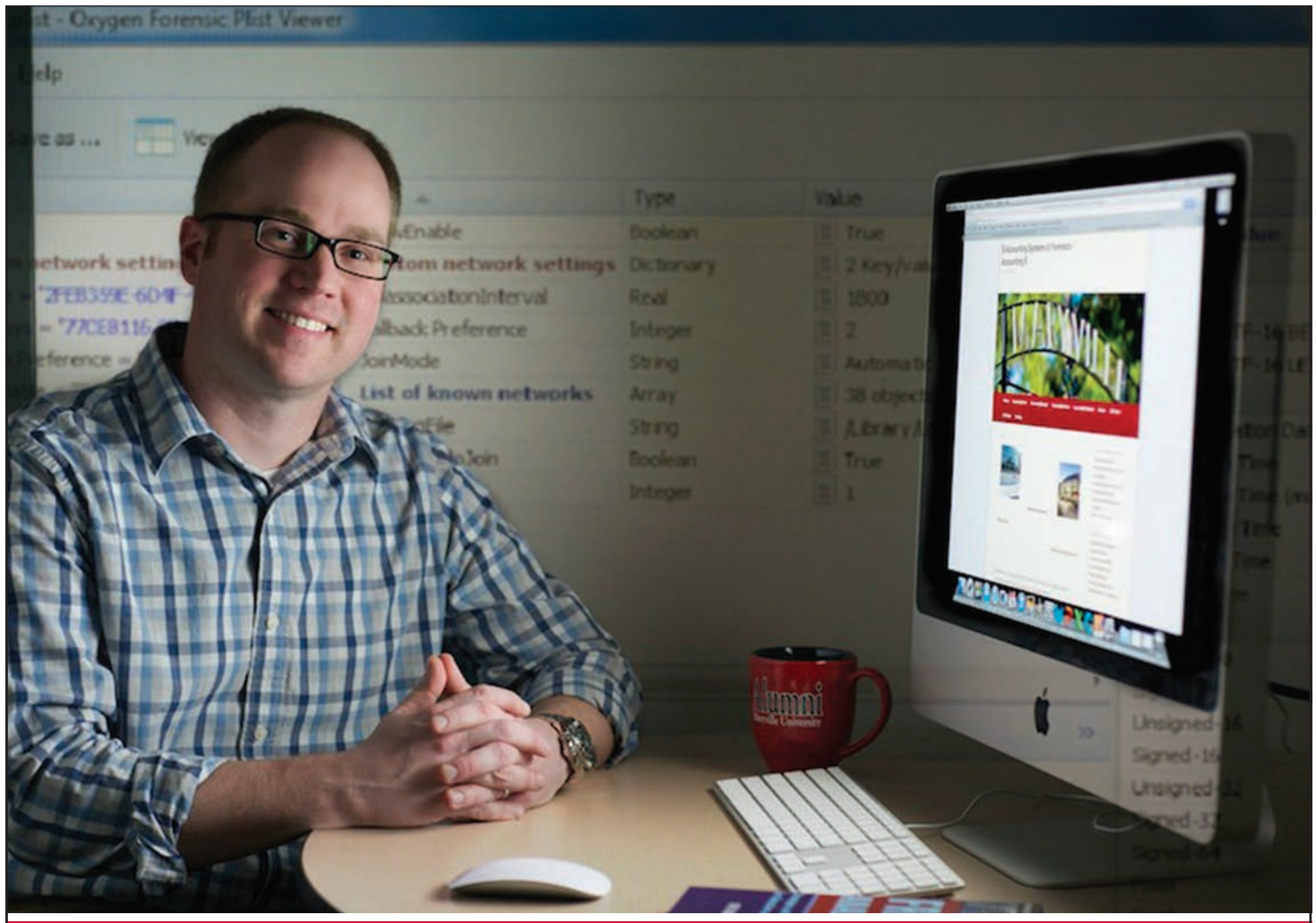
Tony Munns: To a great extent, organizations below the highly technical typically have security as a part of, for example, network administration. So it doesn't reach a status that you can apply the appropriate risk management steps within the organization. When we ask companies if they have done a security risk assessment, for example, that looks at where is all your data, what are all of your systems, what are the appropriate steps to ensure that you don't have a break-in? And then, what can you do when you get a break-in, how can you minimize or remove the threat in terms of managing the data within the organization to ensure that there's appropriate security fences, segmentation, encryption and other tools within the organization? And even given that, what are you doing to prevent data getting out of the organization? We're very good at making sure we have firewalls to protect our exterior, but as we know from a lot of the incidents, people can come in via a lot of different pathways. So what are you doing to ensure you know what data is leaving your organization? What are you doing in terms of having an appropriate incident response approach? Do you know what to do in those circumstances, like bringing in specialists such as SpearTip to enable you to contain, minimize and mitigate the threat that's faced.

Bryan Ard: And I would argue that we, as an industry, are pretty good at the network side of security.

Tony Munns: Exactly, because that's where security traditionally sits.

Bryan Ard: : But very poor at securing the end point. So if you look at sources like VERIS, an amalgam of reported breaches globally, it tells us the majority of the threat actually comes from inside of our network, not necessarily bad actors that we employ, but end points that are compromised. So what that means is, that laptop right there may or may not have a standard build on it, some level of hardening, and it's considered a trusted asset within the environment. But if that

CONTINUED ON NEXT PAGE



CONTINUED FROM PREVIOUS PAGE

asset travels and it connects to other networks or it's allowed to download software or allowed to pretty much go wherever it wants to on the Internet, then it becomes – even if it's fully patched – a risk due to activities of organized crime and nation states. Nation states, such as China, are very good at compromising end points, taking advantage of either known vulnerabilities or yet to be published vulnerabilities.

Tony Munns: Ponemon, the nationally recognized research organization that partners with Symantec to do an annual data breach study, found that malicious attacks caused 41 percent of data breaches, but human error caused 33 percent, and employee negligence caused 26 percent.

Jason Wood: And you put peer-to-peer file sharing on that laptop, you can download and listen to music. Now you just exposed that laptop to 1,200 other people who can access your laptop. And because that laptop is traveling, we ask corporations all the time, "What are you doing to secure your traveling laptop?" "What do you do when they come back?" "How do you verify that somebody hasn't taken advantage of it?" I used to travel with a Department of Defense organization. I will tell you that without a doubt, that organization was targeted, regardless of the country we went to. And if somebody left a laptop in their hotel room when they went out to dinner or something like that, we absolutely assumed it was compromised.

Tony Munns: And a lot of organizations, because of their lack of investment, haven't taken advantage of advances that have been made. A simple step such as ensuring that all your laptops are encrypted is not carried out. When Windows 7 came out, encryption was delivered with the appliance. We go to many organizations and IT has not implemented this.

Bryan Ard: Can I say one last thing on the threat? We don't sell security enough to our organizations. There has to be continuous messaging so that people understand that they are the most important part of the every organization's security program.

"There has to be ongoing, constant, continual messaging so that people understand that they are the most important part of the security program."

BRYAN ARD,
CenturyLink

▸ SO HOW DO YOU MANAGE THESE REALITIES?

Audrey Katcher: We help clients prioritize and improve the cyber security process. The diligence of the monitoring with the right skill sets cannot be under estimated. This is not a "one and done" activity. An assessment performed months ago provides limited comfort today without ongoing monitoring. New threats are always emerging. It's important to ensure your organization has the right blend of people/process/technology in place that fits the culture of your business to support the protection of the business.

Jason Wood: We get phone calls, and people say, "Hey, we just had this

happen," and it would be maybe an organization we'd just gone and talked to." And we say, "Look, it's not a matter of if, it's a matter of when the breach is going to take place." And we tell them this, and they say, "Well, it's not going to happen to us. Why would they target us? " Well, you just may not be exactly what they're targeting. They want to use one of your systems to target somebody else.

Jason Wood: And you say, "Well, pull out your incident response plan and tell me what's on it. And we'll walk you through how to implement it." And they say, "What are you talking about? Why would we need one of those?" And then they say, "OK, help us out."

Tony Munns: And this is what we do, too. It's blocking and tackling.

Jason Wood: You have to partner with the company, not second-guess them, but bring them into the larger folds of understanding, what the true issues are, and then work with their general counsel, work with their C-suite folks and develop a plan to go forward. But being quiet about it isn't going to help.

Bryan Ard: Generally there's four legs to that stool: people, process, products, and partners. And if you don't have all four in place, you're going to struggle.

▸ WHAT DOES AN INCIDENT RESPONSE PLAN LOOK LIKE?

Tony Munns: Regulation is forcing it to be put in place in many organizations. But even those organizations struggle with putting it together despite there being a lot of help out there. NIST, for example, from the Department of Commerce, publishes a very good tool to enable companies to put together the plan. What the plan does it give you a mechanism to, one, recognize you have an incident; two, escalate it to the appropriate level of management and decision-making – and this is not just containing it within IT – it's escalating it to management, to PR and to legal so that you've got the appropriate people making the right decisions to bring in the appropriate parties to manage, understand the extent of the breach, and to be able to mitigate the impact of any potential loss of data, to remediate, to ensure that you've got the appropriate fixes applied to security, to systems, and then the notification communications that are required to all of the stakeholders. And I use the word "stakeholder" carefully because it's not just the people that are subject to the breach; it's not just the organization, but there are also a lot of regulatory requirements in terms of notification. Most states now have laws requiring that if there are more than 500 or 1,000 affected, depending on the state law, they must notify typically the attorney generals. And then obviously, if you're in a regulated industry, you're required to notify maybe the Securities and Exchange Commission (SEC), the Health & Human Services (HHS), or another government entity.

Dustin Loeffler: Illinois has that mandatory reporting to the attorney general, as does Missouri.

Jason Wood: The very first time corporate leadership sees a plan, shouldn't be immediately after a breach. Plan to initiate methodologies and practice that with the corporation to get approval from, again, top-down driven, to exercise that incident response plan prior to an actual breach taking place.

Bryan Ard: Too many organizations

CONTINUED ON NEXT PAGE

CONTINUED FROM PREVIOUS PAGE

don't have appropriate reviewers and approvers. The reviewer should be whoever's responsible for the risk management function. The approver is often your chief counsel. But the plan has to be socialized, reviewed, and approved on at least an annual basis, and it needs to be tested at least on an annual basis.

Jason Wood: And get third party validation – somebody who has experience in doing an incident response comes and looks at your plan and fixes those holes that are going to be in it. We can't take one off the Internet, copy it and say, "Hey, it's applicable to my organization." It has to be written specifically for the information that you have.

Bryan Ard: HIPAA attestations are critical now since last September with the new regulations in force. After an incident, if you are negligent, you could be fined very large sums.

Dustin Loeffler: It is cases such as this where businesses should really rely on their external audit firms. I think those firms are the perfect subject matter experts to help organizations ensure that they are in compliance with regulatory requirements. In fact, we will be educating our students at Maryville University to become well versed in security requirements such as PCI DSS for those organizations accepting credit cards.

Tony Munns: We have a large HIPAA practice that helps all levels of health care and associated industries ensure they're in compliance.

Bryan Ard: When I do execute industry standards of care, that is the first thing I throw, "Hey, I have an attestation. I did my due diligence. My fiduciary responsibility was met." That's huge when you get to litigation.

Tony Munns: If you look at the HHS web site, you can see all the reported incidents with millions of records that have been compromised. And usually the very first thing they state in their notes is they have not completed a security risk assessment. They have not implemented an appropriate HIPAA regimentation program. They do not have incident management.

Jason Wood: I will tell you that from the advisory standpoint, it comes down to educating the board of advisors, the C-suite, exactly what the threats are, how they need to be open to the fact that, yes, they are a target. And then they need to start looking at some type of plan that they can implement to, again, test the security of their network. Gartner or Forrester, they always recommend that somebody get a threat intelligence service. And, you know, we get a lot of information back from corporations that say that when they go and ask for a threat intelligence service, they don't know what to do with the information.

Jason Wood: At SpearTip, we try to bring all that together for them. It's part of the overall program. Because people don't know how to put it together, how to analyze the information, how to validate the information, how to provide that information to a user so it's relevant. And that's really what we miss in the industry.

Tony Munns: Which brings us back to the point that what the organization hasn't done is to look at the whole organization and choose an appropriate framework or methodology to approach security within their organization. And it's one of the areas I think that the academic community can help tremendously. I've worked with many of the educational institutions in the area. And when I've looked at their curriculum, one of the things that's lacking is, their students coming out with an understanding of what ISO is or what ITIL is.

Dustin Loeffler: Typically when we say ISO, we mean ISO 27001, which is a particular international standard for information security which is integrated into our curriculum at Maryville.

Tony Munns: Right, which enables an organization to manage the whole of the security requirement, not just at the network level, but all of the components of it and ensure that they have the pieces together.

Bryan Ard: I'm becoming increasingly convinced that trying to mitigate up front is a losing battle. And 'm not saying that we shouldn't, but we have to be honest with ourselves that no matter what we do, we're going to be breached.

Tony Munns: I understand, but that doesn't mean that we don't put the appropriate resources into the blocking and tackling, get our patches up to date, update our software, encrypt our data and do those other blocking and tackling issues that minimize. It's a risk management question.

Bryan Ard: Agreed. What I see is that people think that that's enough, but they have no situational awareness, right? When we're doing business in countries like China, situational awareness is critical because I can't keep out a nation state actors. If they want in, they're going to come in. So what I need, because I can't outspend them to stop them from coming in, but what I can do is have enough instrumentation and telemetry, so that when they come in, I see that they're in and then I can act on it.

Tony Munns: But the danger of focusing on nation level actors is that 95 percent of the businesses in St. Louis, for example, turn around and say, "We don't do any business in China. We don't do any business in Russia. Doesn't affect us." But you're moving focus of risk to something they don't recognize.

▸ HOW DO YOU BALANCE THE NEEDS FOR CUSTOMER CLIENT ACCESS WITH SECURITY REQUIREMENTS?

Audrey Katcher: The prudent approach is to consider the level of risk worth accepting and then look to mitigate any additional risk through the implementation of preventative and detective controls.

"I like for businesses to rely on their external audit firms. I think they are the perfect people to help ensure that you're in compliance with regulatory."

DUSTIN LOEFFLER,
Maryville University

Jason Wood: Cyber security has to enhance and enable the business without a doubt. With that, you have to be realistic. You can't protect everything. You have to decide what's the most important, whether that's 10, 20 or 30 percent of your intellectual property or pre-patent technology, and apply more protections to that and understand that other information may just simply be out there, but it's not critical to your organization's growth and revenue. You may have to protect some information less and protect some critical information more. It's a simple process but companies really believe that they have to protect everything the same and you can't. Because that means when somebody breaches your network, they now have, access to a global network.

Tony Munns: I think what you're highlighting is that organizations need to do an assessment of where they are and what steps they need to do, including a mapping of, "Where is my data?" Have I done a data classification exercise so that I understand what is intellectual property, what is financial, what is potentially PHI, health care information, what is potentially competitive information such as price lists and formulas and those kinds of things.

Jason Wood: Excellent point. But over the years, it's been somebody within the

IT department who's been focused on that and trying to reach out to different departments in saying, What's critical to your department? And they get no response or they get limited response. And again, I go back to top-down driven.

▸ SHOULD IT BE UNDER THE CFO INSTEAD OF THE CIO?

Bryan Ard: It should be to the CEO. If you don't have a seat at the table, you're going to have a hard time because information gets filtered as it flows up through every organization.

Bryan Ard: If I'm the, CFO, I'm going to filter the information very differently to the CEO than if I'm the CIO. But at the end of the day, regardless of the structure, they need some seat at the table. There needs to be some opportunity to socialize these concepts and to get buy-in on the value to the business. That's absent in so many organizations.

▸ IN WHAT WAYS WILL MOBILITY AND THE CLOUD IMPACT YOUR OR YOUR CLIENT'S SECURITY POSTURE?

Audrey Katcher: Expansion of mobility and use of the cloud expands the necessary control points, the responsibility for contracting and monitoring third parties and new technologies and the discipline within the organization to enforce a reasonable level of control.

Dustin Loeffler: As a society, we are quickly moving into the age of the Internet of Things where we'll have connectivity of all aspects of our life to the Internet. For example, we are already seeing adjustments that can be made to our thermostat via our smart phone to sensors monitoring your activity and health level. All of these areas have a built in cyber security component that needs to be investigated or implemented to secure these devices from exploitation. In our program, we'll specifically be looking at the security issues of these embedded systems as well.

Bryan Ard: Historically security is the protective coating that we put on things, and it can no longer be that. Security has to be cooked into everything we build. And as an industry, we're beginning to learn how to do that. But in many areas, especially consumer electronics, we are still lagging. When we buy our home internet router from our low cost manufacturers, they are often ridden with software defects that present opportunity for compromise. The manufacturers have little financial motivation to make the investment to fix bugs and provide updates because there's no money in it. We need to figure out, how to motivate the consumer electronics providers to prioritize fixing security flaws in existing products and reduce the defect rate in newly released products.

Jason Wood: But that's the point. So if we go to the question, How does it affect your security posture, organizations, and I would argue that even shareholders, are going to have to figure out what they're going to allow systems access to. So, if you were walking around with an iPhone or an Android phone, can you access your, all your work email? Yes. Can you access pre-patent technology from home? Absolutely not. We're going to limit that function. When it comes to the cloud, they're going to have to make the same decisions.

CONTINUED ON NEXT PAGE

CONTINUED FROM PREVIOUS PAGE

Bryan Ard: What you're seeing now is an increasing trend toward businesses wanting to off-load risk and liability to their service providers. Businesses not only have to meet more complex privacy regulations, but they are also demanding increased limits for liability. This dramatically increases the complexity of contract negations. These forces are causing service providers to build much more security into their services. As service providers minimize their exposure to customer data through customer controlled encryption the risk will migrate back to the customer. Over time, you'll see the level of product security be more of a dial that can be turned up or down as the customer and the data dictate.

"IT infrastructure is the enabler of companies nowadays. There's no such thing as a non-IT company nowadays. It's fundamental to everything we do."

TONY MUNNS,
Brown Smith Wallace

Tony Munns: It is beholden on you as an organization to do the appropriate due diligence to assure yourself that, if you are going to take your company's data and put it out into a cloud entity, you ensure that you get some kind of assurance up front that they have the appropriate mechanisms to secure, to control and to manage that data. Part of the problem has been in the rush to move to lower cost computing, people have trusted vendor statements in terms of their capability and they've lost out on that trust. What can you do to assure yourself that the vendor you're trusting to host your systems, your data, your processes has the appropriate security and control mechanisms in place? There are tools. The SSAE16 or the SOC2 under the AICPA guidelines give you the assurance of an independent auditor's review of the adequacy of the system of internal controls of those organizations. So there are steps you can take to assure yourself that you're picking wisely.

▸ IF I'M A VENDOR, WHAT BURDEN DOES THAT PUT ON ME IF YOU HAVE THOSE STEPS IN PLACE?

Tony Munns: As a vendor of those cloud services, you are then in the position where you need to get independent auditor attestation on the adequacy of your system of internal controls, and that those controls are in place and operating effectively to be able to give that assurance to your clients that you are a trusted organization.

▸ SO, I'M A SMALL BUSINESS AND I WANT TO DO BUSINESS WITH ONE OF THE LARGER FORTUNE 500S OR EVEN 100S IN TOWN. WHAT DO I HAVE TO DO TO BE COMPLIANT?

Tony Munns: You have to look at the type of processes or data or transactions that you will be handling on behalf of those companies and ensure that for those industries that you're covering, you have the appropriate compliance pieces in place and that you've got independent attestations. So that may be an attestation that you have implemented HIPAA fully in your organization. If you're handling credit card transactions, that you have implemented PCI DSS standards and have a report on controls that attests to the security of handling of credit card transactions. If you are an outsourcer of services or processes, then you have the SSAE 16 or the SOC 2.

Jason Wood: And keep in mind those organizations, you're talking about the big ones in town, may also have an internal mechanism of compliance and vendor audit that you have to pass.

Tony Munns: I think one of the opportunities that's been lost in this country is the fact that we never had that unifying privacy or security rule that most of the rest of the developed world adopted 20 to 30 years ago. And for better or for worse, on the adequacy of those rules, at least it gave a baseline that enabled industries and businesses to be able to meet at least that minimum standard and understand the architecture. And I think that's partly what the academic environment over here has suffered from because there is no standard baseline on which you build and awareness, an understanding and the appropriate tools.

Jason Wood: Absolutely. And I think most organizations, most educational institutions are. What you might see, though, if you were to go out there is somebody who's in a graduate program may be hearing the same thing that they're hearing in an undergraduate program, when they come back to school. Because there's constantly evolving technology.

Jason Wood: There is absolutely duplication out there. And I think it's, as you partner, if you're an undergrad and you're only doing undergrad, and then you have also have a partnership with a graduate degree program with Maryville University.

Dustin Loeffler: Maryville University actually has this undergraduate/graduate partnership newly in place with Washington University.

Jason Wood: And that's fantastic. And now what we have to develop are measurable steps from the undergrad program all the way through, and we have to know exactly what those criteria are. Because again, we can't afford to have somebody who's going back for their graduate program to not understand the strategic level thought processes that those guys are coming out of the undergrad program to implement. It just has to be measurable results throughout the entire program. And you have to be able to implement that the day that you go to work. We bring people on for 30, 60, 90 days at times just to see how well they're doing, and oftentimes, they don't make the cut because they're not ready to go from the classroom to the workforce. And that's what we have to make sure they can do. You addressed it earlier when you talked about how you're partnering with the industry and other security firms and education departments to make sure that it's relevant.

Jason Wood: So it's important that they constantly apply that within the education process. So the on-the-job training must map to the classroom training, not just lecture.

Dustin Loeffler: We focus on a model of experiential learning at Maryville. So for instance, in our pen test class, we are building virtual entities to where students will be conducting assessments against these virtual entities that represent a bank, a manufacturing facility, or pick your business. This will allow our students to become familiar with these architectures in the academic environment prior to seeing them as consultants. This drastically reduces their learning curve and increases their practical experience level.

Tony Munns: We tend to get very specialized people that understand components very well. And, one of the things that we lack is that ability to step back and understand a complete organization. You need to understand all aspects, because IT infrastructure is the enabler of companies nowadays. There's no such thing as a non-IT company nowadays. It's fundamental to everything we do. So our students need to have an ability to step back and understand the complexity of the organization, complexity of the systems, because if they remain focused in their single areas, then they're ineffective.

Audrey Katcher: Countries need to work together to build trust, cooperate and share information. As we monitor cyber security on The Hill with the AICPA, we see many of the same obstacles that exist for any international coordination.