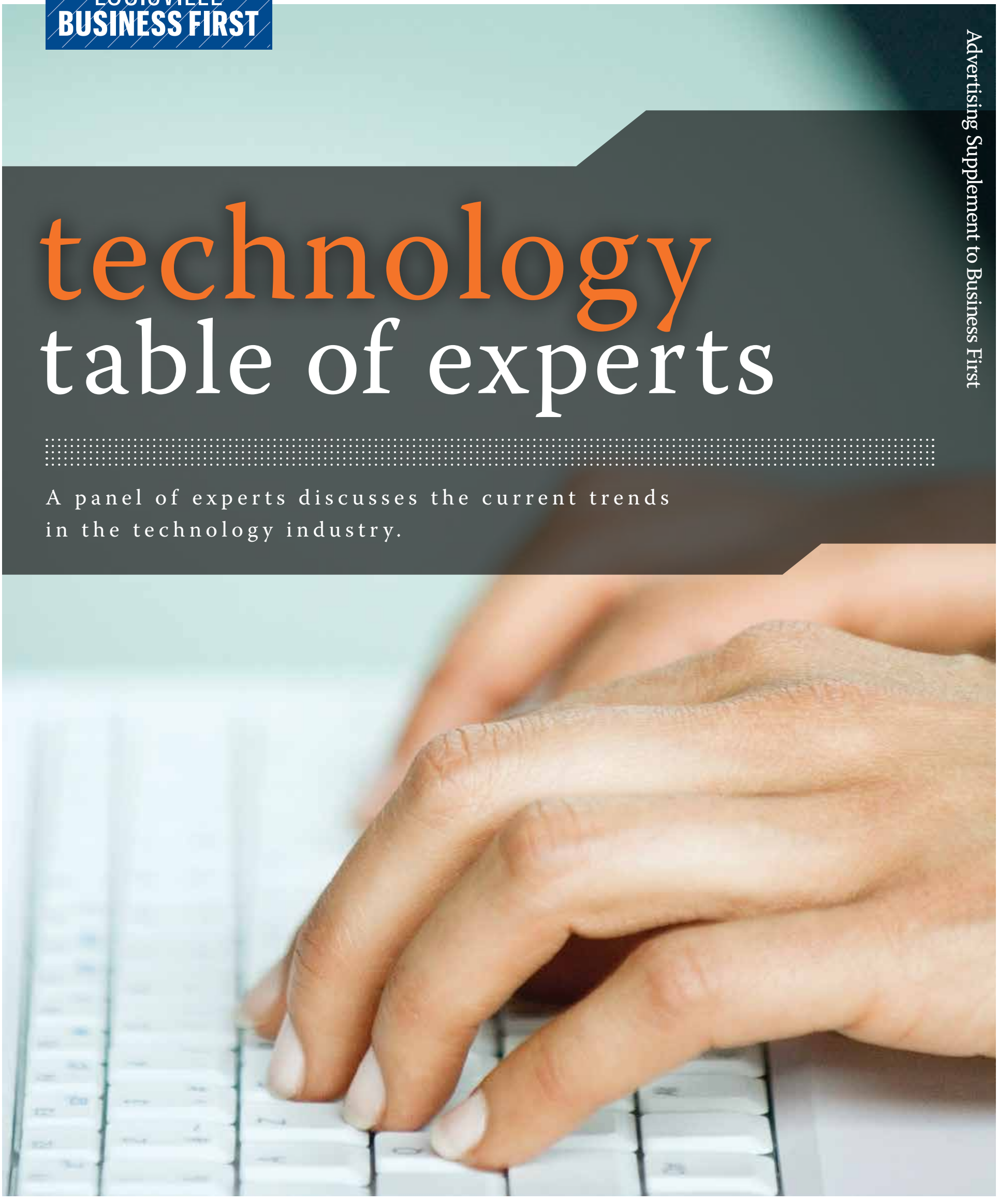
Advertising Supplement to Business First

technology table of experts

A panel of experts discusses the current trends in the technology industry.



sponsored by

data strategy

TECHNOLOGY CONSULTING DEANDORTON

Park community credit union

THE UNDERWRITERS GROUP

message from the publisher

GARY TYLER

Louisville Business First gathered several business leaders to give us their insights on the challenges, trends and opportunities in technology facing companies and individuals today. A few topics of discussion included the challenges and costs of keeping up with almost constant change in every industry, new technologies on the horizon and of course, cyber security. I believe you will find this discussion informative and useful no matter your technical sophistication or knowledge base of the tech sector and how your business is impacted by these changes.

The discussion in this section has been edited for space purposes. I want to thank Tom Monahan for stepping out of retirement to moderate and edit with this roundtable. Finally, I want to thank the sponsoring companies for their support and for the panelists who gave up their time to participate. They were **Steve Clark,** Chief Strategy Officer with Data Strategy, **Jason Miller,** Director of Business and Technology Consulting at Dean Dorton Allen Ford, **Jim Spradlin,** President and CEO of Park Community Credit Union, and **Deana Hauck,** CIC, Account Executive with The Underwriters Group. The sponsoring companies paid for the advertising in this section and for a seat on the panel.

Best regards,

Gary Tyler,
Market President & Publisher

the panelists

STEVE CLARK

Chief Strategy Officer - Data Strategy

As Chief Strategy Officer, Steve Clark leads Data Strategy's Infrastructure as a Service initiatives, establishes and reviews key priorities, and translates them into strategic plans. Tasked with forging new working relationships with partners and ensuring that all initiatives are in line with the company's standards and objectives, Steve is responsible for the creation and identification of new growth opportunities for the continuing success of Data Strategy.

data strategy

JASON MILLER

Director of Business and Technology Consulting - Dean Dorton Allen Ford

Jason leads Dean Dorton's Business and Technology Consulting and is responsible for overseeing the evaluation, design, implementation, and support of business networks. He and the Dean Dorton Technology team provide and support accounting solutions and automation through leveraging technology. Jason also specializes in IT audit engagements, SOC reporting engagements, internal IT audit outsourcing, cybersecurity assessment and training, and PCI compliance matters.

TECHNOLOGY CONSULTING DEANDORTON

JIM SPRADLIN

President & CEO - Park Community Credit Union

Jim Spradlin has been with Park Community since 1995. He began his career with the credit union as the Loan Department Manager. From 2005 through 2008, Jim oversaw the mortgage department serving as the Vice President of Mortgage Lending before joining the Executive Team as a Senior Vice President in 2009. In this role, he oversaw Lending, Finance, and Information Technology. In 2010, Jim was promoted to Executive Vice President and was named President and CEO the following year.

park community credit union

DEANA HAUCK, CIC

Account Executive - The Underwriters Group

Deana is an Account Executive with The Underwriters Group. She has over 25 years experience in Insurance and Risk Management. Deana works with companies of varying industries helping them identify their specific risks. Once identified, she works closely with them on a strategic plan to mitigate those risks helping her clients build a stronger bottom line. She has extensive knowledge with the risks facing Financial Institutions. In addition to her knowledge in Property and Casualty Insurance, she has expertise in the evolving world of Cyber Liability.

THE UNDERWRITERS GROUP

the discussion

MODERATOR: What are some of the biggest trends or technology challenges that you're seeing in your particular businesses?

SPRADLIN: We're in financial services, so there is a huge movement toward mobile technology. Consumers today want it now, they want it at their fingertips. You have to be able to give them access to their data, to their accounts, even right down to applying for a mortgage. The challenge is making sure that you're giving it to them in a secure way and you're protecting their information. So that is our biggest challenge. That creates a huge financial investment, a huge time investment, and then an ongoing investment for security after that.

MILLER: One of the things we've started to notice is technology is changing faster than we can keep up. I've seen a study that says, we, as humans, can only keep up with so much change, and we've crossed the axis of how fast technology is changing versus what we can really keep up with. And as a business, you are constantly trying to determine where do you invest your dollars. How do you stay secure? How do you meet the needs of your business users? How do you meet the needs of your customers? And as Jim mentioned, there is the expectation that you're constantly giving them more mobility, more tools. I think that's the thing we struggle with the most – where to focus your strategy and where do you focus your resources.

SPRADLIN: Change is a big factor. Sometimes you have to draw the line and say this is the upgrade I'm going to do, this is the product I'm going to do, and just acknowledge in six months there is going to be something better, but you just can't continually be changing.

MAIN POINT

"We've crossed the axis of how fast technology is changing versus what we can really keep up with."

HAUCK: We are in the insurance business. Clients want to talk about cyber insurance now. It used to be the word they didn't want to mention. Many more are buying Insurance. A new trend specific to manufacturers is they're being forced into more automation just because they don't have the work force to run their productions machines.

CLARK: We support a lot of businesses like yourselves and the asks that we're receiving are mainly around a couple of different areas. One of them is the security aspect, which is kind of a global concern with all of our customers. Customers ask; How can we secure the information we have? How can we make sure that what is entrusted to us is actually protected and the overall course of trying to make sure that you're doing the right thing? The security aspect keeps everything in line. Along with that is the automation of IT to make sure that you have the proper manpower and the ability to absorb different changes within the environment. Organizations want to do more with less, but they don't want to reduce their staff. The challenge is the skill set of the staff that they have right now, and introduce automation into that framework, and allow them to do more productive things within the business. And I think the last thing is that we're seeing a lot of customers want help gaining some financial controls around what they're doing within their IT spend so that they understand that when they put a dollar in, what does it do to the overall mix of what the service is delivered back to the end user of the organization. So I think those are the really three areas that we're seeing the most differences in 2018.

MODERATOR: Let's talk about cyber security. What's the most important thing that companies should be doing to assure the safety of their data?

the discussion

MILLER: I would say the thing we see the most need for is awareness. And I have two prongs on that. One, awareness and buy-in from top executives, and knowing that it's not just an IT matter anymore, but that this is something that top executives and boards need to be concerned with. And the second one is just user awareness. We can put in the most sophisticated tools and protections, but that doesn't do any good if our users leave the doors open and allow the threats to come in. And so we've put a lot of investment in user-awareness training programs, continual monitoring, continual updates of new threats coming out and testing them, and then applying changes to our training and communications based on the results of the testing that we're doing of them.

SPRADLIN: We've tried to create a culture of security. So that's kind of been a shift. We speak a lot to the employees. We're offering a lot of training, whether it's video training, book training, or even classroom training, just about the importance of security. The end user is usually the most vulnerable, whether it's their clicking on spam e-mail that they shouldn't, whether it's the customer, using unsecured passwords, or handing out their passwords. There are so many vulnerabilities that it's really just communication and education, we think. Just to keep in front of everybody. Let them know how important it is and that 1234 is not a good password. And if they tell you to go six digits, 123456 is no better.

HAUCK: We deal with a wide range of businesses. I believe a lot of organizations want to tuck their IT people to the side because the C-Suites don't understand and they don't want to have those conversations. I would suggest looking at the services you're provided by your cyber-insurance policy. Many times they are free. Sometimes a company may think they are too sophisticated for those services but that's a mistake. Often the insurers will offer discounts through their preferred vendors that are very beneficial. I would also digress to say that there are Business First readers who don't understand cyber risks and are getting a late start at this. Maybe they mistakenly thought they could rely on an outsourced provider for protection. For those in this camp, to get started just ask yourself some basic questions: What do we do? We send e-mails. What are the content of the emails? Do we take credit cards? Do we have healthcare information? Are we using laptops? Just get your arms around that you have and what you're doing. Then look at where you're storing the information and go from there. I think it's important to talk to cyber-specialists from the insurance industry. By all means, complete a cyber application. Whether you buy insurance or not, it's going to be a tool for you to examine the weak areas of your program. You now have a goal as weaknesses have been identified and can start to enhance your security.

CLARK: I believe that one of the important things to understand is cyber security is not handled by a tool. We have a lot of customers come to us and say, "Hey, could you fix our cyber security? We want to buy a tool." Well, it's really a people process, then a technology conversation. You have to have all three legs of this stool working in unison to make sure that you actually have a cyber-defense. When addressing the topic of security within any organization, make sure you understand this is a layered approach. So you almost have to look at it as an onion. You have peels of different layers of security throughout your organization to protect yourself because at the end of the day, if someone really wants to take an offensive posture toward an organization, there are always vulnerabilities that can be exploited to gain access, both technological and procedural. You just don't want any intruders to come in too far. So you've got to have the ability from a tooling standpoint, to protect yourself from a process, making sure people aren't clicking on those rogue e-mails, and from a personal standpoint, they have to understand what's involved every time that they'd have an action involving anything that is on the public Internet Understanding what risk and exposure could be if something goes wrong, and the awareness aspect, and a lot of companies just don't know.

MODERATOR: What's the best way for a CEO and board members to really understand their technology needs and challenges so they can make wise decisions on expenditures and IT personnel?

SPRADLIN: You need to be close to your IT department. They need to trust them. So you have to be willing to go to them and ask questions and not worry about if the question sounds stupid because that's what they're there for. We're very fortunate. We actually have board members who are IT security experts. So we've got it from the board level. We've got it from the IT level. We'll just ask a ton of questions, and we'll go to the IT department, and there may be a new program, and the question a lot of times is: Do you feel safe with this program? What do you think is vulnerable? What's the worst thing that could go wrong? And ask them those questions. They either know the answer, or they're going to want to go out and find it and come back with the best recommendation that's out there. One of the things we always tell everybody is you don't have to be the smartest person at the table. So the first thing is to admit you're not the IT expert and be willing to take the advice from other people.

MILLER: I would say it would be important that they continue to participate in any kind of risk assessment. So any good cyber-program has an ongoing risk assessment in participating with the full management team and understanding what those risks are, understanding where you need to be focused in your attention. A lot of good stuff comes out of that. In 2017, the American Institute of Public Accounts came out with a product that you can engage a third party to come in and assess your cyber-risk management program. So there is a set of standards by which a CPA can assess an organization's cyber-risk. And prior to that, there was really no set of standards that you could assess risk management for cyber security. And so we're finding that organizations can use those to have a third party come in and ask the questions they don't know to ask, and the recipient of the report is management, the board so that you know that you're hitting all the areas that you may not know to ask the right questions of.

SPRADLIN: In any type of bank or credit union, you just feel like there is always auditors in doing something, and it used to be it was always the financial auditors. Now, we have just as many IT auditors, and we're doing vulnerability testing at least once a year. We're having cyber security audits all the time. We constantly have people come in and test the system to make sure that everything is right. And it helps having the board knowledge that we have because when we go to them and say, "We need to spend X amount of dollars to have this done," we'll get the buy-in from them.

HAUCK: Jim, I agree with all the things you've said about the importance of IT people having a seat at the table. And the other thing I would say from observation is I sometimes see the IT department reporting to HR. The security of your information is paramount and should have oversight accordingly.

SPRADLIN: I would agree. We currently have IT as one of our top executives.

CLARK: I think the big challenge we run across is cultural. It's also not exactly the executive's role to understand everything that's going on in the room. It's really the team that the executive has supporting him or her that is really in charge with distilling down the information to facts. What in your business is core and how do you take that information and make the decisions that need to be made. It is not necessary to know the widgets you're using, but you need to know the overarching vision and the overarching spend control that you're putting out there with your acquisitions to know the true amount of dollars being saved or spent.

the discussion

MODERATOR: In your particular areas, is it difficult to find the type of employees you need to execute the technology side of your businesses?

SPRADLIN: It definitely can be because many times you're looking for a specific skill that's out there. In our case, we've got to have people that have got the knowledge to work the mobile products, the web products. I think we have 10 people right now in our IT department. Four of them are probably programmers, a couple of network people, so we've got to have that mixture out there. So we've learned to be very patient to make sure that we're making the right hire, not just any hire to fill the spot, but it can be challenging at times to find the right person.

MILLER: I think even at the height of the unemployment, IT was still a difficult area to find resources in, and it's becoming even more difficult with unemployment continuing to drop, and there are lots of opportunities out there for people. So it's important if you have good resources to invest in them, to try to keep them. I think that's more important than trying to find new ones. Just trying to keep the ones that you got. Because of that challenge, I think we see a lot of people starting to do co-sourcing and outsourcing. So outsourcing is on the rise in all areas, not just IT, but we're finding more and more businesses looking to go outside to a trusted third party to bring in the resources that they need, because they can't find them or retain them.

HAUCK: I agree. That's what we're seeing – a lot of outsourcing. And we're seeing IT is getting more and more specific as I mentioned with the manufacturers.

CLARK: Our challenge is really finding the right profile of individual. We work at the forefront of technology, and there isn't a marketplace to find most of the skill sets that we demand. We actually have to have the type of person that we can drop into a situation with training and bring them up to speed relatively quickly. In doing so, we do have some challenges finding some very finite skills, but we've put programs in place to foster skill acquisition internal to the company. Today an engineer might be on a help desk, then they might elevate themselves to the day-two support organization, then they may go into professional services or into an IT level, or another position within the organization. It's really giving a career path for an individual and building an individual. It's costly to do that, but in our marketplace, we can't find the people that we need, so we have to do that as a necessity.

MODERATOR: Is there anything that the community or the school systems could do to better develop the type of technology-trained workers that growing companies need?

MILLER: I think one of the challenges education has always had is they trail behind a little bit. By the time you realize what technology you need to be training on, technology is changing before they can get curriculum built. I think we're going to see more focus on the technical schools. So the Kentucky Community and Technical College System is going to be critical over the next few years to continue to turn out the specific niche industry skill sets we're going to need to see. So I think four-year degree requirements may continue to shrink as we see specific areas come out from a two-year degree program. I think adjusting our expectations with that will be helpful.

SPRADLIN: I would agree. I think it all comes down to the educational programs that are actually being offered and emphasized. I think as a society, we've gone through a period where everybody had to have their MBA, everybody had to have their law degree, but to your point, we're lagging a little bit behind to now really IT is where everybody needs to realize the opportunities are.

HAUCK: Yes. I agree.

CLARK: Well, I think it really comes down to the local companies' involvement in the school curriculums. I've heard of a large automotive organi-

zation needing to have engineers. So they actually infused talent into the local schools all the way from K-12 through higher ed. So industry involvement is a huge thing that I see as the different pockets of the country need to have different, finite skill sets. I'm starting to see in different areas up in the Midwest, data scientists were required by a pretty large pharmaceutical organization. So they actually teamed up with higher ed in the Indiana area and developed curriculum to meet the need. So industry involvement into the education, I think, is very important. The educational system is not going to keep up with the demand that they don't know about.

MODERATOR: It was mentioned a little bit earlier about companies outsourcing some of their IT services. When they do, what's the best way for company executives to manage these outside services to make sure they're getting what they contracted for?

MILLER: As we're doing compliance audits on a regular basis in all areas – HIPAA, the Health Information Portability Act, the Payment Card Industry – we're seeing the General Data Protection Regulation come down from the European Union. Strong vendor management programs are becoming a more and more critical component of this because there are so many places that are outsourcing services. So having a program in place by which the company continues to not only vet vendors on the front end, but have a way to manage their actions and hold them accountable to the companies' internal policies and requirements and compliance requirements that they may be open to is a huge component. Asking for third-party assessments to be done by those vendors, especially those holding critical data or sensitive data for you, getting systems and organization control reports or SOC reports are a good way to be able to get a third party to check to see that those vendors are maintaining the required level of due diligence and compliance.

SPRADLIN: We do pretty extensive vendor management. Most of the people we use we're familiar with, or they're familiar with our core processing, so we've got an extra layer of vendor management there. We know that our core processor is okay with them. We will generally assign a project manager that works with them, that keeps in contact with them, to make sure that progress is going to meet our standards. There's a lot of communication.

CLARK: Organizations that do outsourcing still need to have some portion of visibility on a day-to-day basis. Maintaining the project management, maintaining a vendor control layer in there is critical to the successes of an outsourcing arrangement. Just wholeheartedly giving a program or a whole division to an outsourcer inevitably leads to a lot of challenges. So having the oversight and governance of vendor control all in place is a critical aspect, and don't trust the outsource or verify the outsourcer.

MILLER: When we provide services, we prefer co-sourced, and that would go along with what Steve said is you've still got to have somebody within the company involved and engaged with the outside resources so that you're working as a team to deliver on that. And we find that's a good model to use.

MODERATOR: Jim mentioned earlier how customers expect connectivity via their mobile devices. So what kind of challenges does that present in developing these kind of user-friendly apps?

SPRADLIN: Well, it changes so fast that it's hard to keep up with it, and so many of the companies that are doing it are relatively new. So your vendor management becomes a huge challenge to make sure that they can actually provide what you need. They're capable of doing it, but sometimes you get to a situation where they bit off more than they can chew, or they got too many going at one time. So vendor management becomes very key in that and just making sure they have the expertise to do what you need.

MILLER: I would agree with what Jim said. We help clients select tools, and software, and vendors all the time, and you're finding fewer and fewer of the tried-and-true people who have been around for 20, 30 years. You see a lot more very niche focus. Developers, or solution developers, pop up and they've maybe been around one to five years. Are they going to be around tomorrow? Are they going to get gobbled up by someone bigger and better? And so there's constant change. You aren't really able to have an expectation that you're going to have that software for 10, 20, 30 years anymore. You've got to be prepared to be nimble in your solutions and be able to move quickly and adapt to those changes.

CLARK: I totally agree with what everyone is saying with the nuances of the mobile and phone-based applications. Everything seems to be so dynamic in this world. You look back four, five years ago, this is just kind of a burgeoning technology. Now it's a booming technology. I think it's really important for organizations to take a look at the value you spend on developing the applications. Are you actually getting the return on that investment? And if you are, picking one of the niche players is a very daunting task to actually vet them out to see which one of the players are really going to provide you with the outcome that you're looking for. There are some really high-name app developers in the web and mobile space that come with a big ticket because they work with the Facebooks and the Groupons of the world, but they do a really good job. But you're going to pay a lot for those type of resources. So you just have to know what outcome you're looking for, what's the value to the organization, and then decide what's the price point for that development and outcome you're willing to pay for.

SPRADLIN: I think it's interesting that had this discussion been two years or three years ago, it wouldn't have been mobile. That's how fast it's changed. It would have been your website. Your website has got to be up to date. And while the website is still important, the emphasis is mobile, and that's how fast it's changed.

MILLER: And I think the other challenge we have or the thing that you have to focus on as you're evaluating providers and solutions is interoperability. So it's not the days of going to a single provider and them giving you all the functionality you need under one roof, especially in banking. We see this all the time. You've got 10, 20, 30 different software providers for all your different niche areas and making sure all those work together cohesively, give your users a good experience , is oftentimes a very difficult thing to balance with all the options that are out there.

SPRADLIN: I know in our case, it's got to integrate with the core. That's where all the data is at. So it's got to be able to go pull that out onto it, but then you've got to make sure that it can go to IOS, to Apple, you've got to make sure it can go to Android. It's got to work on your iPad, it's got to work on your tablet. It's got to work on the website, and it's got to look right. So there is a lot of research to make sure that there is a consistent feel across everything.

MODERATOR: Every business has to deal with some form of government regulations. Are government regulations keeping up with technology and do some of them need to change in order to make doing business easier?

MILLER: I think the biggest challenge we see in compliance is that there is not a fundamental federal standard. So each individual state is left up to their own rules. So if you're a national organization and have clients in all 50 states, you've got, I think right now, 48 different data breach and privacy requirement laws that are all changing. It's a full-time job having somebody keep up with those. If you're in niche areas like banking, you have the Gramm-Leach-Bliley Act that you have to contend with. If you're in health care, you've got HIPAA requirements. We're now seeing an international touch with the European Union and the general data protection regulation coming in May. Even if you're not operating in the EU, if you have data on citizens of the EU, now you've got new stringent requirements that you're going to have to contend with. And so it can be exhausting. Jim mentioned the fact that there is always an IT auditor in now, and it's because of all these different requirements and regulations that you have to keep up with. And so the thing we try to do is come up with a good, solid standard program at the top that goes to the most intricate and comprehensive requirements and then work your way down from them, making sure you've ticked all the boxes in all the different areas that you have to comply with.

SPRADLIN: In our case, there are multiple regulators that we have to answer to, and they might all have something different they're looking for. But I think they have the same challenge we have in finding qualified people that can come in, and actually do the exam, and actually look at what you're doing. We see a lot of different faces every time they come in, whereas the financial people might be the same ones for 20 years, those IT guys are turning over, and everybody has got a different viewpoint as to how they do it. From the legislative side, when they pass a law, does that congressman or senator understand or have somebody on staff who understands what they're actually getting ready to pass? So there are some challenges there. It's important to talk to those people, and talk to those offices, and tell them how it's going to impact you or maybe you don't need to look at that area, why don't you shift over here? This is where the real vulnerability is.

HAUCK: Jason, I agree with what you were talking about with the different state laws. It's so challenging. Alabama and South Dakota have no state notification laws regarding data breaches. All other states have their own unique laws. The state attorney generals have fines and penalties to attach to people who do not notify their residences properly, in the timely manner that they have set forth in their specific laws. It presents a nice revenue stream to those states. This is one of the things that a cyber insurance carrier will help you with and regulatory fines and penalties are covered in the policy. Also, we see there is a 2018 SEC Guideline that was just released in February and it's giving recommendations to the disclosure obligations for the publicly-traded companies. Then as Jason mentioned the EU and their GDPR coming out in May. One of the particular things that I noticed about the new GDPR specifies that the controller of personal data that has been the subject of a breach must notify authorities of that within 72 hours of the discovery of the breach. That's pretty stringent. Certainly, that paragraph has caveats but bottom line; we're a global society and what we see happening in Europe from a regulatory standpoint, will eventually be here. Think about a private school that at first glance seems to need a vanilla cyber insurance policy. But then there are 50 international students. The exposure changes. They need a policy that will respond to an international breach, with notification provisions outside the U.S. Cyber policies are responding to the needs of their policyholders. We're seeing the insurers are now including theft of money in the policy. Previously, it was only theft of information with a separate crime policy handing the money exposure. In banking, perpetrators hack the business or personal depositor's passwords, the account is hacked and the money out of the country before you know it. Cyber insurance is always evolving to respond to the threats policyholders face.

CLARK: We're seeing a number of new members to the C-suites of organizations starting to address this problem. Ten years ago, did we have chief security officers? It was a very rare title. We see it all the time now. We see chief governance officers now. And we're seeing more and more organizations on the smaller end of the spectrum actually have someone who has the chief security, chief governance, or chief compliance title within the organization. So organizations

are starting to take a look at and take a hold of what they can do. Teaming up with organizations to take a look at what the ever-changing dynamics of the regulatory environment they work within, it is critical because unless you're an organization of a critical mass that has the capability of keeping up with every legislative vote that goes on in every legislature across the United States, you're never going to keep up. So you actually have to have a third party help you out with the velocity of change. From a technology standpoint, we're seeing a lot of organizations start to tackle some of this governance at the perimeter by bringing in tools like called access security gateways that look at what comes in and outside of an organization. And they've got rules that are built into them to pick off the high-level offending policies that the government has already put into place or certain industries have already put into place. So it can flank some of the technology, some of the issues with technology, but a lot of this comes back to people in the process.

MILLER: We're so far behind as a society with GDPR. There are so many more requirements, not just on what you do if you have a breach, but what you have to do on the front end and also the fact that you have to acknowledge to the end consumer that you're going to keep their information and tell them what you're going to do with it. They have the right to tell you to delete it, to purge it, or the right to ask you to give them a copy of it. And I would say less than 5 percent of the organizations in the U.S. are prepared to have their systems do that because we consume information quickly. It goes throughout the organization, and being able to make that information readily available and portable to an end consumer who asks for it is something I don't think many organizations in the U.S. are prepared for. So there is a trend coming with more and more focus on that then we've ever had to do. Right now, most states are just asking or mandating what you do if you have a breach. They're not necessarily providing requirements on what you do on the front end for protecting and securing it. So there is still a lot of work to be done in that area, but it'll be a lot of ground to make up. yet, you're going to have to deal with it when it happens. So that's another challenge that we all run into.

SPRADLIN: This may or may not be the right way to say this, but I'm going to say it anyway. Part of what we're running into with the dangers of a breach or the dangers of information getting stolen is I can somewhat control if you're using my ATMs or my ITMs, or you're going into my branches, but we've got debit cards in 50 states and Europe. I can't control every bank in the world and what security they've got on their machines when you go to use it. So there is always that vulnerability that it's not your shortcoming that's going to cause the problem, and, tal technology changes coming that are going to interrupt a number of different industries, and I speak just from the accounting industry. We're seeing things like block chain and how that's going to impact how businesses work together and eventually will impact how we perform an audit organization. Machine learning, artificial intelligence are huge things that the industry is watching on how it's going to change how we do accounting and how we do audits. I think that's just some small examples of technology disrupting multiples of years of the fill out an application right there on your phone, you can scan the VIN number in, and then, bam, off you go. So you've got to be aware of all these changes that are out there that literally happen daily. But you've got to balance that with not being too reactionary throughout and try and buy the next greatest thing. So it's a real balancing act for those disruptive forces that are out there. And at our size, we kind of like to take a little bit of a wait-and-see and then see if it's really going to catch on before we do it.

MODERATOR: How do you think companies are dealing with disruptive technologies, and what role do these technologies play in reshaping our society?

MILLER: I think it goes back to what I mentioned early on, which is that changes are happening so quickly and we're struggling to keep up with them. But there are some fundamen- way we've done certain things, and the changes will continue to happen faster than we've seen historically.

CLARK: We see very similar things across the board with the customers we're dealing with. We have customers that actually work in the retail space, and they're quaking right now because of the whole shakeup that's going on with the mass Internet consumption that's affecting things like Toys-R-Us going out of business and Blockbuster getting killed by a streaming service. Those are the things that help customers involve their technology teams to get a better value from technology so they can drive new areas of exploration for revenue streams because right now, our marketplace is changing so fast with the different market streams being disrupted. Brick and motor, in 10 years, is going to look vastly different than it does today. And how, as a society, are we going to actually adapt to those changes? Are we going to expect all of our retail being out of certain small hubs within the United States? Are we going to still have the general store in each one of our home towns? So that's one of the things that we see the changes really disrupting is that the communication and acquisition of goods and services is really going through a moment of change right now that needs to be addressed from pretty much every consumer and every technology company out there.

SPRADLIN: There are so many things in our industry. There is, for example, a national mortgage company that advertises very heavily that they can give you an approval in four minutes on your phone. That changed the way we all had to think about it because now you're competing against that. There is geo-coding out there, where if you've got the app, it knows if you're on a car lot, and it can prompt you to

SPRADLIN: We refer to that as the "thanks, Amazon" effect. Everybody loves Amazon. Amazon just changed the expectation in the marketplace. We want it now.

MILLER: It makes it really hard for our small customers and partners to keep up because they have set that bar so high. They have large budgets. And so for your small local retailer to offer the same website functionality and immediate gratification is really difficult. They want to keep up, but you look at it and, say, you don't have the budget to deliver at the same rate and pace that they are. So we find that to be very much a challenge for clients.

MODERATOR: We've talked a lot about how businesses have had to change and adopt new technologies. What about your customers? How have their understanding of technology and their expectations changed in the last five or 10 years?

MILLER: I think they have become more educated and more demanding for technology. I think five, 10 years ago, it was a challenge to convince people you need to invest in technology. It was more of an expense. I think more are seeing it as a strategic investment today, and so it's changed the conversation in what they're willing to do. I've had a conversation just recently that we would put together a solution for somebody and take it to them, and you would just cringe because you would think they were just going to kick about the price of it, and now you take them a cloud solution that's probably even more expensive if you extrapolate it out, and they don't blink an eye at it. They're more open to that concept, realizing that it's going to change the way they can do business rather than something that might have been historically on premise or locked in that they will use for a period of time and then replace in the future. So I think we have started to see a shift in people embracing it versus resisting it.

SPRADLIN: They are much more trusting. I don't want to use the phrase they blindly trust technology, but it's close to that because they figure you wouldn't put it out there if it didn't work, you wouldn't put it out there if it wasn't safe. They'll download that app and go right along with it, whereas I would say even five years ago, you had to convince a lot of people it was okay to use the app. It was okay to use the website. Even if it was secure, they were always s keptical. But I think some of that skepticism has gone away, for better or for worse.

MILLER: I think that was true for something like cloud accounting solutions before. It used to be I've got to have it here so I can protect it.

MODERATOR: The whole concept of storing it out there was foreign.

MILLER: Now everybody has accepted that that's the way of the business model. I think people are seeing that it allows you to adapt faster versus the system that you would buy, and install, and use it for 10 or years. If you want to keep up, people are embracing that a lot more and have become more trusting of the technology.

MODERATOR: How about your customers, Deana?

HAUCK: My customers are more visionary with technology – looking to the future and what they can do to compete and attract customers.

CLARK: I see the industry being very cyclical in nature. So in the 70's and 80's, everyone who had a computer and a development staff. Take a look at the 90's and early 2000s, a lot of people bought shrink-wrapped software packages. Now, we're back in 2010 and getting into 2020s, and we're starting to see the wave back again of internal development. Even in cloud service providers, you have to develop the application most of the time to work properly with the function within your business. So it's almost a wave coming back of organizations developing custom software to meet the needs of their demands. So that's the changes I see, and the trends and technology is coming back to we need to develop something custom for us. We can't use what everyone else is using.

MODERATOR: Before we wrap up, I'd like to offer the opportunity for anybody to add anything they think Business First readers would like to know.

HAUCK: I would just add that we're hearing a lot about the ransom demands. "We've shut your system down and we require payment or you can't get the system back". The response that I've gotten from so many people is, "I have backups, so I'm not

going to worry about that". We most recently had a client that turned on their computer and discovered a ransom demand. (This isn't the first insured with this problem.) They went to their backup, which was also corrupted. This did happen to be after hours when it was discovered. We were on the phone with them, getting them to the insurance company and they in turn with an attorney, protecting the attorney-client privilege. The insurance company IT specialists in there to see if they really did have to pay this ransom. It was determined that, yes, there was no way to break this. The ransom was required in virtual currency. This takes time and the cyber policy handled this process as well. Once the payment was made, keys were given to unlock, the IT specialists were back to scrub the system. I believe this insured was down 3 ½ to 4 business days, which is pretty incredible.The cost of the process and the forensics were more than the ransom demand.

MODERATOR: We've seen TV shows and read stories about these cyber kidnappers. How common are ransom demands in the Louisville area?

MILLER: It happens more frequently than you would like to think it would. I do think more places are starting to get more aware of cyber security requirements. I think we're seeing some slow progression of people responding and trying to be more proactive, but there is still a big gap in that process. So I reiterate that the cyber-insurance programs are critical today. There was a period of time the insurers didn't really know what to do with this stuff, and most of the policies you would look at disclaimed out just about everything and didn't really deliver on what the consumer expected. But they've come a long way in the last three or four years. I would say the key to it is making sure you're proactive and fill out the policy application honestly because that could come back to bite you. If you say that you've got protections in place and they find that you didn't, they're not going to pay. We've seen where they will come back and say, "You didn't do what you said you were going to, so we're not really responsible for what happened to you." But it is reality. It does happen here, and it happens to people who expect it not to happen to them. One of the most challenging things I hear when I talk to somebody is, "Well, nobody would want my data."

SPRADLIN: Famous last words.

MILLER: They don't care what the data is. They just want to keep you from getting to your data, and there is money to be had by doing that. So anybody is a potential victim. I think that's the biggest message is anyone can be a victim.

MODERATOR: So in most of these cases, are companies paying ransoms, or are they finding ways to solve the blocks?

MILLER: I'd say the majority will go to backups, but we have seen a number, as Deana mentioned, that they did not have proper security around their backups, and so those become compromised as well. But the majority of our clients that have dealt with that, we will restore from backups. But there are instances where if you don't segregate your backup properly, it gets compromised the same as your main data, and then in that case, it's really about your only option is to pay the ransom. And then you've only got a certain amount of confidence that it'll actually restore after you pay the ransom. So that's always a risk, too.

HAUCK: And I would also add that you may become a target because of who you do business with. So you may feel like you have really nothing they want, when in fact, you really do.

MILLER: We've seen third parties become the conduit to bigger instances over the years.

MODERATOR: Being unable to access your data for even a few hours would be devastating for many businesses, much less being down three-and-a-half days like Underwriter's client was.

HAUCK: Running your company without your system and information is cumbersome if not impossible. I would also add the personally identifiable information of their employees was not breached.

CLARK: We're seeing it from a broader picture across the Midwest. I wouldn't say it's quite weekly yet, but it's getting pretty close to the time frequency of a week that we're hearing from a customer or getting contacted by a customer that has had some sort of a breach or encryption attack affecting their systems. So it's a real threat out there. And most of the customers contacting us are not Fortune 500s. They are the small and medium-sized business. These attacks are very detrimental to their outcome or the longevity of the organization. So it's kind of sad to see. We had a meat market that was one of them. You wouldn't think of that as being a high-value target, but they got the point-of-sale devices. So they couldn't conduct business anymore, and it was just a two-location meat market. So it's a scary endeavor, and it's a challenge for everyone who is facing it.

MILLER: We're even seeing nonprofits subject to it and vulnerable to it as well.

MODERATOR: Has law enforcement, on any level, made any progress in catching/prosecuting these hackers?

MILLER: I think there have been some cases of that, but typically, most of the ones we've dealt with locally aren't to the magnitude that you could even get active involvement from the FBI. There is so many of them, they don't have the resources. You can call them and log the statement, but they basically say unless it's a certain dollar amount, they can't even take action. So that's a challenge.

HAUCK: I would throw out that the Secret Service does have a lower dollar threshold for investigating a cyber breach. Even here in Louisville, they have agents assigned to cybercrime and doing the research. Many times businesses do not have that choice when they have a breach. The local law enforcement automatically calls the agency to investigate. I know of times when the FBI reviewed the information, which takes some time, and then declined investigation due to not meeting their threshold.

MODERATOR: All right. I appreciate everyone taking time out from their busy schedules to participate in this round table.