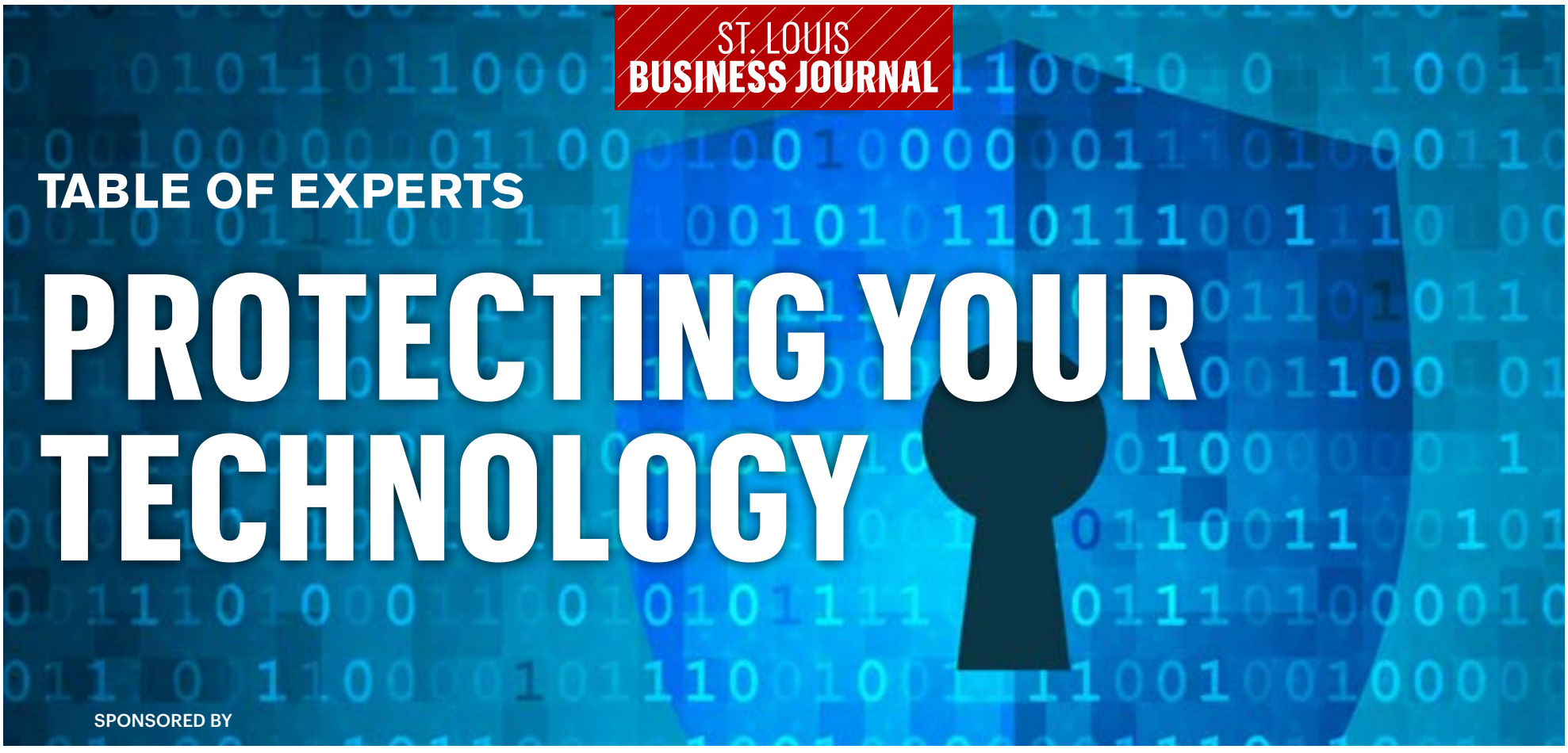


ST. LOUIS BUSINESS JOURNAL

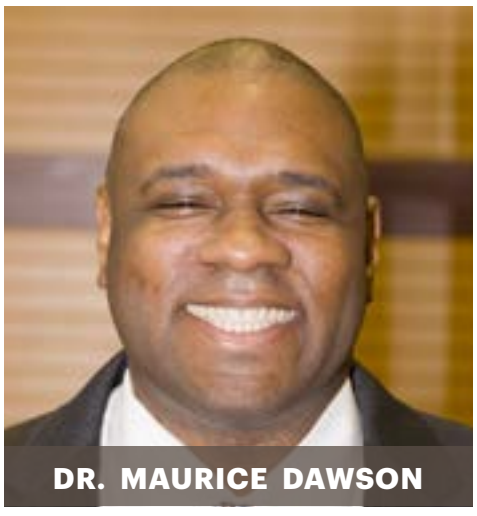
TABLE OF EXPERTS

PROTECTING YOUR TECHNOLOGY

SPONSORED BY

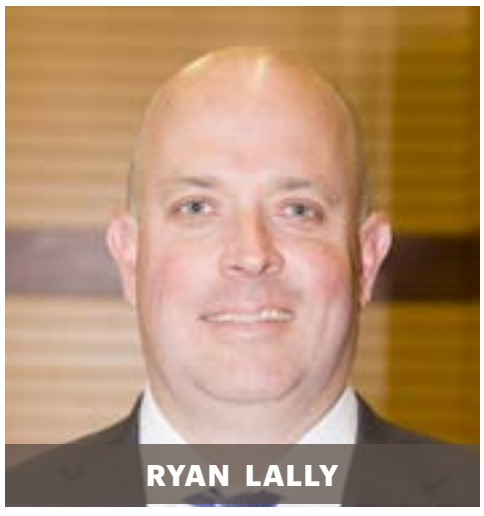
Armstrong Teasdale | Netelligent. | CliftonLarsonAllen | UMSL Business

TABLE OF EXPERTS



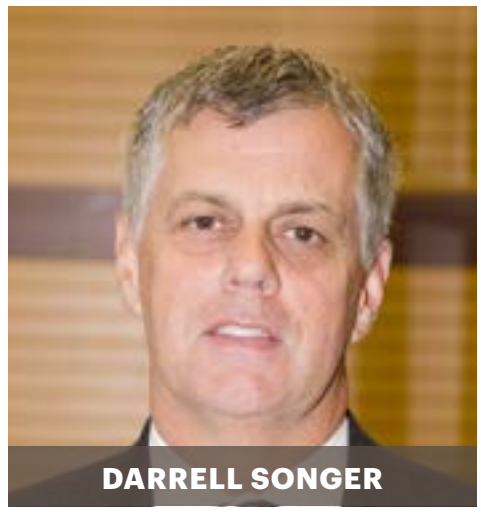
DR. MAURICE DAWSON

Dr. Maurice Dawson serves as an assistant professor of information systems at the University of Missouri - St. Louis, which is the only National Security Agency Center of Academic Excellence in the St. Louis metropolitan region. Dawson was a former visiting assistant professor (honorary) of industrial and systems engineering at The University of Tennessee Space Institute, and Fulbright Scholar to Chelyabinsk, Russia. He is the founding editor-in-chief of the International Journal of Hyperconnectivity and the Internet of Things, and co-editor of the book "New Threats and Countermeasures in Digital Crime and Cyber Terrorism." Dawson comes to academia with more than 10 years of experience from the defense and aerospace industry. Dawson holds terminal degrees in computer science and cybersecurity.



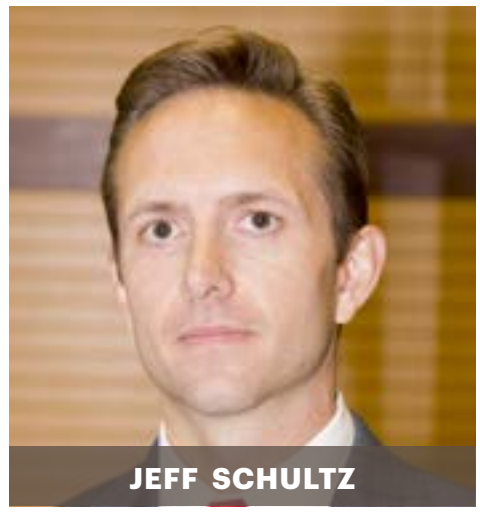
RYAN LALLY

As director of business development for the security practice, Ryan Lally provides strategic direction of security product, consulting and managed services for Netelligent's Security Solutions Portfolio. With more than 18 years of security experience in sales, consulting and executive management and roots in the local security community beginning in the late 1990's, Lally has experienced the rapid development of security technology markets, compliance standards, and dynamic cybersecurity threats with clients of every size and vertical. Through this myriad of experience, Lally shares a unique perspective in the practical aspects of security architecture, policy enforcement and security program development.



DARRELL SONGER

Darrell Songer is a principal at CliftonLarsonAllen in the St. Louis office, specializing in assurance and tax services for technology and emerging industries and leads the regional information system security group. Songer leads a team of technology and industry professionals that provide security services for the St. Louis region. The team is knowledgeable in the integration of business operations in relation to the overall framework of IT security thus ensuring business considerations are accomplished in a secure structure.



JEFF SCHULTZ

Jeffrey Schultz, partner at Armstrong Teasdale, is an experienced business litigator who has extensive knowledge about the field of data security and privacy. This background led him to be named co-chair of the firm's data security and privacy practice group and the former chair of The Missouri Bar's Technology and Computer Law Committee. Schultz is a certified information privacy professional (CIPP/US) through the International Association of Privacy Professionals. Schultz represents clients in complex commercial disputes, including those involving the misappropriation of trade secrets, computer tampering, nondisclosure and noncompete agreements, commercial contracts, shareholder disputes and social networking law. He has co-authored a number of articles concerning trade secrets, data protection and privacy, including "Trade Secret Litigation — an Updated Overview," which won The Missouri Bar Foundation's 2016 W. Oliver Rasch Award that recognizes outstanding substantive articles appearing in the Journal of the Missouri Bar.

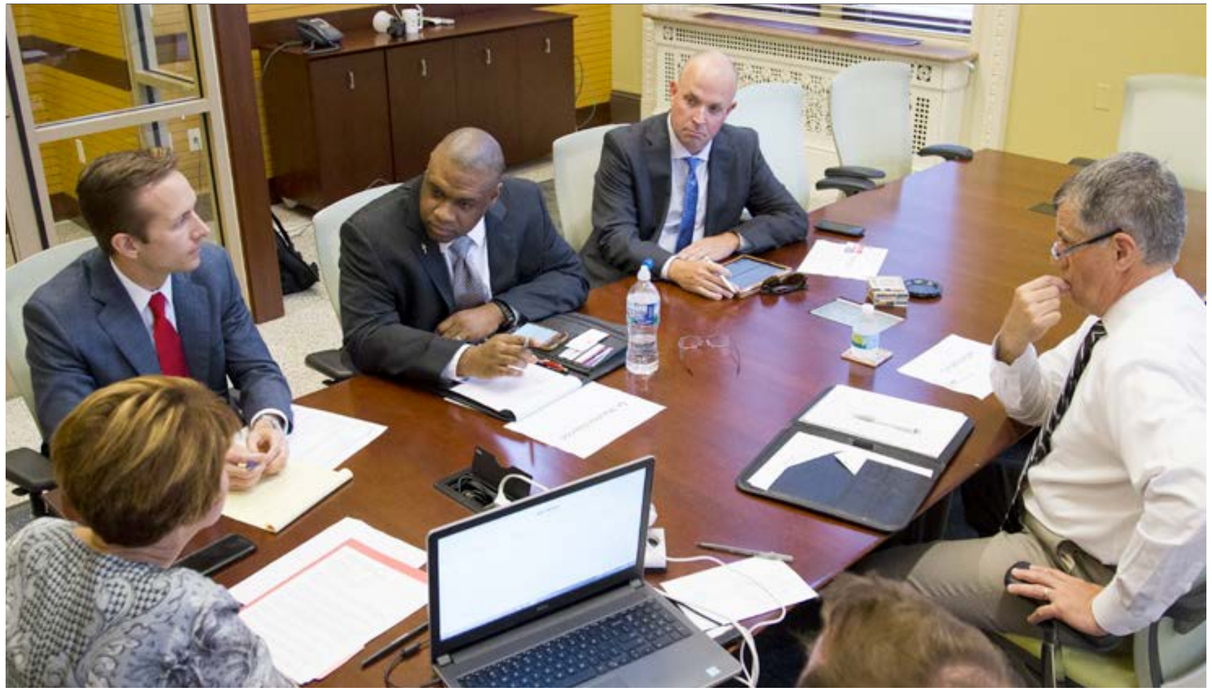


TABLE OF EXPERTS

PROTECTING YOUR TECHNOLOGY

Bad actors are getting around security controls in the networks and new security technology is being released all the time. Is there any technology that fixes the problem?

Ryan Lally: Not 100 percent of the time. There are emerging technologies that do a better job. Some of the new technologies are really a paradigm shift in how they approach security, and companies have to be willing to make that leap to do things better.

Maurice Dawson: From the Department of Defense standpoint, you don't release new technologies until they've been tested out in a test bed or virtual environment. And, in the meantime, there's STIGs, Security Technical Implementation Guides, and then every year the technology protocols go through a review. On the commercial side, you don't have that. They say the latest and greatest, and maybe they have a new intrusion protection device or prevention system, but those haven't been vetted out. So that's one of the disparities. Also, in the commercial sector, a lot of times they're not using the NIST Special Publications, which are for computer security for hardening and stuff like that. Those are some of the differences between how things operate in commercial and defense.

Jeff Schultz: In my experience, when we're dealing with breach situations, even if our clients have state-of-the-art security in place, bad actors are really good at finding ways to get around it. I think it will continue to be a problem, especially since you have to have a connection to the internet. You have to be able to communicate outside of your organization. As long as you have those portals out there, somebody is going to find a way in.

Is there a common theme across companies and industries when it comes to cybersecurity initiatives? Are companies ignoring it? Are they budgeting for it?

Maurice Dawson: I don't think companies are ignoring it. I do think companies are struggling to find talent. That's why the NSA has the Center of Academic Excellence to attract and train talent.

Jeff Schultz: I agree there's more awareness of the issues, and companies are starting to pay more attention to it. I think that companies have been struggling to get money into their budgets to take the steps that are necessary, especially when they have boards that have different priorities and don't recognize the seriousness of the threat that they're facing. It's very difficult to get that money allocated into their budgets so they can hire the security experts and lawyers to create an incident response plan. Fortunately, though, awareness is increasing. We read about newer and bigger breaches every day. That's really starting to get people's attention.

Ryan Lally: The security industry is focused on companies that have more robust compliance needs. There's a whole lot of government compliance, private industry compliance and vendor compliance that drives security initiatives and security spending. As a rule of thumb, if there's a fine or there's some sort of public disclosure that has to be done, then companies seem to be more willing to spend money on technology and resources. I think what's happened over the past two or three years is that a larger number of CEOs have now decided to try and define what their cybersecurity risk is, what information they're trying to protect and why. In many cases incidents really drive spending. It's not uncommon for me to be sitting in a room with a CEO post-breach trying to figure out how it happened, and how we can make sure it doesn't happen again.

Darrell Songer: I would first divide the entities into two different segments. The Fortune 500 base is active and diligent in the protection of systems and technology. Over 90 percent of the companies in the U.S. are considered small business or closely held. That is the sector we serve. Right now, just as Jeff mentioned, there's more information out about cyber crime and breaches than ever. But I think the smaller companies, particularly, are becoming immune to the "noise" because they've heard it so many times. It's like the weather forecast for snow in St. Louis that never comes. One of the questions we immediately ask is "What is your budget for cybersecurity?" We usually receive a blank stare, meaning there is none. Cybersecurity is not even a consideration. We have a difficult time getting the attention of the C-level individuals if they have not had an actual attack at a level that the company was noticeably impacted. Actually, we have numerous incidents with our client base where the breach was essentially ignored by management with respect to prevention of future nefarious acts. We find resistance to invest funds in the cybersecurity consulting world if it hasn't directly impacted a peer. And, if there's ever been imminent threat to an enterprise, particularly small business, it's from catastrophic damages from cyber-related crime.

Maurice Dawson: Defense has had security since the mid-'80s, but it's been very disjointed. Now they have common criteria, which focuses on international product certification across a number of countries. We also had something called DIACAP, which focuses on certification and accreditation. And, you also have an individual who is in charge of making sure systems meet particular requirements. These individuals are known as the Designated Approving Authority.

Darrell Songer: The Department of Defense has very sophisticated systems, and they're cutting edge. We are not seeing that sophistication trickling down to our clients.

Ryan Lally: I spent about 15 years working in global companies, and there are a lot of folks who have come out of the Air Force or the Department of Defense who have a lot of experience with advanced technologies and programs who have trickled down to the large enterprise. In St. Louis, those folks are in many cases very collaborative and manage robust security teams and budgets. In small to medium businesses, you're correct, if there's not a level of compliance or a reason to spend money from a business perspective, then we don't see a significant investment in cybersecurity programs.

Maurice Dawson: The commercial sector does not have requirements that can be determined by mission, information classification and system type unless your system requires compliant to regulations for Personal Identifiable Information, Protected Health Information, and etc. However, commercial organizations can take advantage of the National Institute for Standards and Technology Special Publications from the Computer Security Devision to create baselines that allow to set a minimal standard for cybersecurity security measurement.

Why has the commercial sector been such a late adopter to secure computing as the U.S. Government Rainbow Series documents are dated in the 1980s?

Maurice Dawson: So the Rainbow Series was the initial documentation for security, and the Rainbow Series were 20-plus different documents focusing on trusting system development, database development, covert channel analysis and more. The problem with that guidance is it was vast. But the issue was actually having commercial tech companies build products that meet this, because they weren't getting a lot of resale on these products. Later they came out with ISO 15408 Common Criteria, so they're working in NATO environments so they can share products across countries. In the past DIACAP was the leading systems certification and accreditation framework, which has been replaced by the NIST risk management framework. Previously you had DCID, which is the Director of Central Intelligence Directives. Now they have the ICD, the Intelligence Community Directives. The Department of Defense community has a method to further derive mandates, but the commercial sector doesn't have really a driving requirement. There's no one checking for compliance in comparison to the government. A lot of the Department of Defense organizations check yearly at a minimum. They have to make sure they're up to date. They have an independent third party come in and scan their system to see what they have done, searching for vulnerabilities, reviewing false positives, conducting penetration tests, and checking system documentation. So you have a pretty stringent requirement process to maintain certification or accreditation. But in the commercial sector you just don't have that at all, and it needs to happen. The problem, again, would be manpower. A significant number of companies are simply in reactive mode rather than a proactive one.

> *If you're a human resources manager or you work in HR, you need to create a job requisition to hire somebody that states that individuals must have graduated from NSACA school or they need to have a particular type of certification to weed down all of these people who are going to be applying for the job.*
>
> **MAURICE DAWSON,** UMSL

Jeff Schultz: I think the lag on the commercial side is attributable to something that we talked about earlier, which is the difficulty in getting the C-suite buy-in. The C-suite has to allocate funds. They may have to hire new people. They may have to buy new hardware and invest in new technologies. And I think there's been a general lack of awareness or a belief that these types of security incidents aren't going to affect their company. So a lot of small- and mid-sized businesses question why anybody from the outside would ever want any of their information or why they would be a target of attack? And a lot of times, they don't think about the vulnerabilities that are sitting in their own office, like their own employees. But, we're seeing a lot more from the commercial sector in terms of adopting and implementing cybersecurity controls and measures as it becomes more prevalent in the news and the government taking more action against companies that fail to secure their networks. That's been a big driver for the activity that we've seen recently.

Ryan Lally: A notable trend in the last 12 months that has been unique out of all of the years that I've been in security has been ransomware, which in itself is not generally a security breach sort of incident, meaning data isn't typically stolen via ransomware, it's just encrypted. However, ransomware causes business outages, and it slows down productivity. I would imagine that every company of any size in the area has been affected by it, a lot of spending has come from it. It's loud and noisy. There might be data loss or data destruction, but it doesn't mean that it's being sold on the internet.

Maurice Dawson: Even worse, when you talk about ransomware: It takes a certain threshold to have the FBI involved.

How will Internet of Things and Internet of Everything change the landscape of cybersecurity?

Maurice Dawson: So you think about, in the simplest form, your own devices, smartwatches, smartglasses, Nest thermostats, Bluetooth, and these are all internet-enabled. A number of these devices may not be protected as much, right? Nest thermostats actually track when you're moving the temperature of the house. And you can take that data and easily dump it into a open source tool like RStudio and just run analytics and say well, this is the stats based upon this person's usage, to get how often they're in the house, how often they shop. And, when you think about data for images. You may have teenage kids who take pictures and post them on Instagram or Facebook. You know, those images have geotags, so you can actually take those pictures and start mapping them out on an actual heat map and say well, this person goes to this particular school because they're at this location; they shop here so often. You can correlate that with the refrigerator that's tracking perishable foods. Or say, is this person going to be away from their home, you could pull the data from the networked thermostat to look at temperature patterns, or movie history lists from a streaming device. This data gives the ability to predict behaviors and discover norms of their target.

Jeff Schultz: From a legal perspective, Internet of Things is definitely changing the landscape. As Maurice mentioned, a lot of these devices are collecting information about the users. And from a lawsuit standpoint in discovery, if you're wondering where somebody was at a particular time, what they were doing, or whether they were interacting with a specific device, you may be able to capture that information. And that information may be discoverable evidence that we can use. It's a very fascinating development because it has created many new sources of information. Also, we've heard rumblings recently about product liability cases against manufacturers of these devices who fail to put security controls in place or have certain vulnerabilities that result in some sort of harm or injury to the user of the devices. That's the cutting edge or the new frontier that we're seeing with these devices. It's definitely changing the landscape.

Ryan Lally: The fact is that everything on our smartphones are tracking everything that we do.

Maurice Dawson: There's a social media app called Nextdoor that gives the address and the first names of who is living next door. There's no security, and you can see who sent an invite to who, so you can establish relationships. You can see who attended what event. Basically, you can start running analytics on your neighbors on what they actually type and try to see the keywords they say. So, there's good with these social media apps in terms of you can start building a relationship with somebody in the neigh-

CONTINUED ON NEXT PAGE

CONTINUED FROM PREVIOUS PAGE

borhood. But in the terms of the amount of information that's given, it's just too much. And the site doesn't do any type of real verification. It's really open.

Darrell Songer: One of the Department of Defense agencies listed the six biggest cyber risks for 2016 – and the tracking mechanism you're referring to is one of them. Their fear is that it will be used for nefarious activity – abduction of children, kidnapping and such. It's no secret that our government uses similar technology to track people in foreign countries.

What steps can a business take to protect its proprietary technology from disclosure to the outside world?

Jeff Schultz: So we've talked about some of the technical safeguards. Making sure that all of your hardware and your software are up to date, making sure you have good IT and security personnel. There are also old-fashioned, physical safeguards like locking your doors, locking file cabinets and that sort of thing. But from a legal perspective, one of the things we encourage our clients to do is institute non-competes in appropriate circumstances; institute non-disclosure agreements if a non-compete isn't appropriate; or if a non-compete is appropriate, include a non-disclosure agreement in that non-compete agreement. And, companies should obtain invention assignments from their personnel so when their personnel are developing technologies on the company's dime or using the company's resources, they're obligated to turn that technology over to the company and to assist the company with getting intellectual property protection for that technology. Then there's also old-fashioned training: Make sure employees are aware of the risks associated with their activities on computers and on the internet so they know what the vulnerabilities are. I like to believe that most employees aren't out to sabotage their companies. They generally want to do the right thing, and there may be just a general lack of awareness. For example, we've recently seen a lot more victims of phishing scams. As a result, I know that there are a lot of companies now that are investing in training their employees to be aware of potential phishing emails. Ransomware also has been a big driver in employee training. I mentioned technical safeguards. Companies should consider limiting their employees to only those areas of their networks that the employees have a need to access and restrict access beyond those areas. Putting those sorts of limitations on employees' authority is also a really helpful safeguard to help protect technology and information from disclosure to the outside world. It's especially important when you're dealing with R&D folks.

If there's ever been imminent threat to an enterprise, particularly small business, right now a cyber breach is probably the largest possible damage they can have.

DARRELL SONGER,
CliftonLarsonAllen

Are the non-competes enforceable?

Jeff Schultz: It's a common misconception that non-competes just simply aren't enforceable. In Missouri – and in most states – non-competes are enforceable if you have trade secrets that you're trying to protect – like how your technology operates, what your business processes are – or customer relationships. So, if you have one of those two protectable interests that you're trying to safeguard from misuse by an employee who is leaving and going to work for a competitor, you can enforce that non-compete. Now, there's a limitation on non-competes. They have to be reasonably limited in geographic scope. They also have to be reasonably limited in time. In Missouri, two years is about the limit. We've seen some five- and 10-year non-competes in the sale of business context. So, when somebody sells their business to another company they're made to sit on the sidelines for a little bit longer because they received a lot more money, and it would be unfair for them to go and take that goodwill back from the company that bought their business. For geographic scope, it's whatever is reasonably necessary to protect the employer. If an employer operates in a specific region and the information that you're trying to protect wouldn't be harmful if it was used outside of that region, maybe that's where you draw the line on geographic scope. Because a lot more businesses are national in scope or have a global scope, we're seeing much broader non-competes, and we're seeing enforcement of much broader non-competes. Nationwide non-competes aren't that uncommon anymore. And courts do have some hostility to worldwide non-competes, but you can still go beyond a national scope and get protection to the extent that it's reasonably necessary to protect your company and your business.

Maurice Dawson: While employed as a Senior Program Manager at Rockwell Collins we were directed not to sign non-competes as multiple Lead System Integrators would require use of our Common Avionics Architecture System for their airport. If we signed a non-compete or agreed to simply supply our system to one LSI we would limit our actual business and lose our position as top rated glass cockpit developer. Thus we signed Proprietary Information Exchange Agreements, and set up a Brewer-Nash Model which allowed us to work with multi-organization while protecting their Intellectual Property. Also, we would develop our systems to require few interfaces for our systems to integrate. Thus organizations could rethink their technical solutions for systems integration that do not expose any source code.

Jeff Schultz: That's definitely the way we see many relationships with independent contractors handled. Many won't sign a non-compete because they're just dealing with a small, specific part of the business. And because that particular independent contractor may be performing the same functions for lots of different businesses, it doesn't make sense for it to enter into a non-compete; doing so would prevent the independent contractor from obtaining other jobs. In those situations, a company should make sure it has non-disclosure agreements, confidentiality agreements and invention assignment agreements in place with its independent contractors so the company is able to then safeguard its information. In the event that the independent contractor discloses it to another entity, the company will have some legal recourse.

Are there any other legal protections available to protect technology?

Jeff Schultz: Most states have adopted the Uniform Trade Secret Act, Missouri being one of them. And, recently, the Federal Defend Trade Secret Act was adopted by the federal government. Both of those acts allow companies to safeguard their trade secret information from outsiders and misuse by outsiders. To qualify, the information has to be the subject of reasonable steps to maintain its secrecy. So, a company must have reasonable physical and technical safeguards in place. A company should consider putting into place policies and agreements to protect that information. And the other criteria for a trade secret is that it has to be of value to somebody who can actually put it to use. For example, if a competitor got its hands on the alleged trade secret information, would

CONTINUED ON NEXT PAGE

We're seeing a lot more from the commercial sector in terms of adopting and implementing cybersecurity controls and measures as it becomes more prevalent in the news.

JEFF SCHULTZ,
Armstrong Teasdale

CONTINUED FROM PREVIOUS PAGE

knowing that information be valuable to the competitor? Would it give the competitor a leg up? For a lot of proprietary technologies, especially when you have a company that has an active R&D department, it's with cutting-edge stuff into which the owner has invested a lot of time and money and which will have significant value to competitors. Competitors can get an unfair head start if the information were to fall into their hands because they can circumvent the time and expense that it would otherwise take to develop the information on their own. There are also computer tampering statutes, both state and federal. The computer tampering statute in Missouri is a fairly robust statute that we use frequently to get injunctions and to take recourse against folks who may steal data. A lot of times we use it in the departing employee context. And then, at the federal level, there's the Computer Fraud and Abuse Act. That's another computer tampering statute that provides some protection for a company's technologies. Those statutes were primarily developed with hackers in mind.

Are companies addressing cybersecurity in their coverage?

Maurice Dawson: In 2013, Lloyd's of London contacted me about how to insure organizations for cyber insurance like power plants and other facilities deemed important critical infrastructure. So what I came up with when I spoke with them was, measuring them against some type of baseline control. Do they have these controls in place, and then, based upon their compliance with these controls, setting the insurance rate appropriate for them. They're a bigger risk with the least amount of controls they have.

Darrell Songer: The classic response from a C-suite individual would be "yes, we are covered." We then ask if we can review the policy, and typically we find they do not have sufficient or the correct coverage. Typically appropriate coverage will be covered in a separate rider and not an embedded line item of their general policy. Maurice mentioned some of the baseline requirements that you would want your company to have before you can insure them. The larger insurance companies have developed applications that are extensive and technical in nature. A key step in the process is to review the application for cyber insurance. What we often find is that answers to the questions in the application are not technically correct. Often, the answers in the applications are simply wrong and misleading. The danger is certain of those "wrong answers" could void the coverage. If you claim you've been following 12 mandatory technology considerations, and you've only done six of them, it's difficult to protect yourself and have an insured claim. One example is the question on the application regarding external penetration testing. The applications often ask if an outside company has performed penetration testing, and almost every company says yes, but rarely have they had the actual service performed.

Jeff Schultz: I've seen a number of cyber policies, and what's striking to me is the variation in terms of coverage. It's critically important for consumers of cyber insurance to read and understand what their policy covers and make sure that it's actually covering what's necessary for your specific business.

Darrell Songer: In our discussions with agents and carriers, it appears the cyber insurance arena has not sufficiently matured as a risk or product line. The cyber insurance world is just too new and too difficult to predict at this point. Actuaries haven't been able to put numbers together to make informed predictions. We see wide ranges of policy costs, and again, it goes back to the application.

Ryan Lally: There have been a lot of studies, and we reference them occasionally in presentations. One of them was a company called SafeNet who studied 2,000 breaches around the world and looked at the amount of financial loss that an organization would take on after a breach. They had data points regarding high impact events that create financial loss for customers, to low impact events like having to make informational disclosures to clients speculating about a breach. It ranged from something like 35 percent of your customers would stop doing business with you as a result of a high impact breach, down to 5 percent or 6 percent for a low impact scenario. The bottom number is the most frightening. If a customer receives something in the mail that said "Your information was lost, we have no reason to believe that anybody has done anything with it, however, it was stolen." There would be a large percentage of customers that lose confidence and cease to do business with that vendor.

What legal strategies or avenues are available to a business when it experiences a theft of its technology?

Gartner is stating that by 2017 that 50 percent of companies are going be outsourcing some part of their network security program.

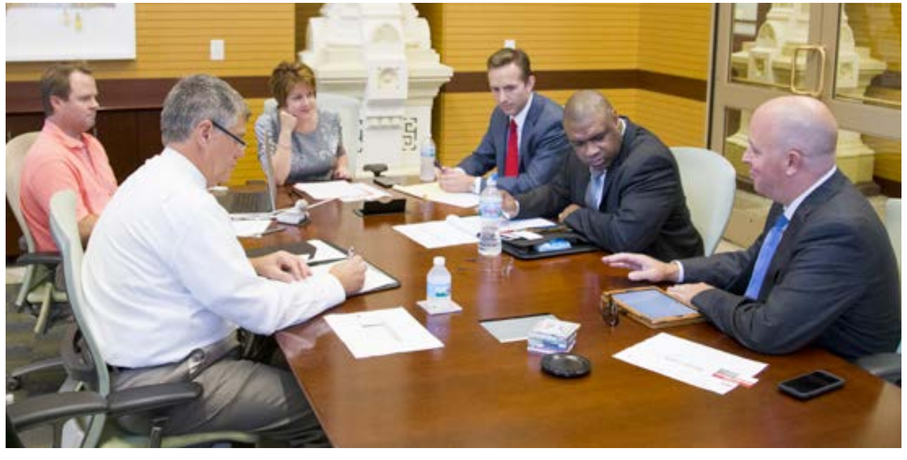
RYAN LALLY,
Netelligent

Jeff Schultz: You find out about the theft, and if the information is in a competitor's or would-be competitor's hands, and you know that the competitor is going to use the information immediately to compete unfairly, you can go into court with that immediate threat of irreparable harm and ask the court to enter what's called a temporary restraining order. That's an emergency injunction that stops the thief from using the stolen information – it essentially locks them up. And if the thief violate that injunction, the violation is potentially punishable by the court's contempt power. If the situation isn't that urgent, you can try sending a cease and desist letter to see if you can engage in a dialogue about the theft. A lot of times, if the information has been taken by a departing employee, the new employer may not want anything to do with the information that's being brought from the old employer. Most businesses that I've dealt with – especially in our region – want to do the right thing. Most businesses hold themselves to high ethical standards. You can see if you can engage in a discussion by sending out that cease and desist letter. If the cease-and-desist letter doesn't work, but it's not an immediate threat of irreparable harm and you have some time, you can file an action and seek what's called a preliminary injunction. This injunction is issued after more evidence is presented during a bench trial. Those trials can last anywhere from a half day to three days or more. The injunction will stay in effect until the end of the case. And then, at the end of the case, you make your request to the court for a permanent injunction.

Maurice Dawson: From a technical standpoint you can use things like audit logs that show that this person has been on this machine and had access to this information. So audit logs would be a great from a legal standpoint to show that the individual did take that information. To go a step further one could compare crytographic hashes to show file integrity while reviewing other file properties.

Jeff Schultz: That's right. When you go in for a request for a temporary restraining order, you have to have affidavits that swear to the truth of the facts that you're aware of. In preparation, we'll often conduct a forensic examination of the computer that the would-be defendant used while they were employed by our client, and we'll look for web-based email activity, the USB activity and any other suspicious activity.

Ryan Lally: From a technology standpoint what we find when we're trying to prove or disprove how something nefarious has happened is that a lot of times customers don't have enough technology or visibility in their network to get an accurate picture of all of the things that could have happened. Advanced malware, for instance, is very good at erasing itself. So, those types of cyber threats are very hard to track if you don't have visibility in all of parts of your network and systems.



Jeff Schultz: We see varying levels of sophistication with our clients in terms of how they handle security and what capabilities they have. And, you're right, that some of the advanced malware does cover its tracks pretty well. If you have an individual who is particularly savvy when it comes to using computers, there's a lot they can do to make it more difficult to pick up the scent and follow their trail; but, usually, there's a way. It just means it's going to be a lot more difficult. If a company has a sophisticated security group and IT group, it makes it a lot easier when we're conducting investigations.

Maurice Dawson: You can have discretionary access controls, or role-based access controls. And, from there, put a security model in place that differs how the subject interacts with the object. So, this particular file hasn't been used in a month. Then they lose access to that file. So, down the road, when it's time to give them the boot, they don't have access to those files. Or, if you know they're going to be putting in their two-week notice, then immediate access is removed.

Ryan Lally: There's so many applications that employees access every day that you can attach information to. Web services like Box.com or Dropbox or Facebook. You've got your own personal e-mail accounts, Skype and Instant Messenger. Well, a lot of those are encrypted sessions, and so standard network technologies can see the destination of the site, what site you

CONTINUED ON NEXT PAGE

CONTINUED FROM PREVIOUS PAGE

attach it to, but they can't necessarily see what you did because of the encryption. So it's important that customers understand those risks and their blind spots.

What is the importance of attending an institution that has received the National Security Agency and Department of Homeland Security Center of Academic Excellence for cyber defense education?

Maurice Dawson: That particular program has been vetted by the National Security Agency and the Department of Homeland Security for research within the department, labs and mapping of curriculum to the NSA knowledge units. So, essentially you're having students who are abreast of the latest and greatest in terms of cybersecurity. Faculty are researching the latest cybersecurity issues, and the other university departments have cybersecurity concepts in their courses. For cyber programs, this is the one and only accreditation that's out there, and it's done by the federal government. This program requires a university to have an environment that promotes hands-on cyber security learning. For this, UMSL has a virtual and a physical lab. In both labs, our students can actually try these tools that we talked about, Kali Linux, Wireshark, Maltego and others and use them in the virtual sandbox environment.

Jeff Schultz: In the cybersecurity world, accreditation and credentials are becoming more and more important. As this area matures, individuals who at one time were able to get by and hold themselves out as being very knowledgeable about these areas may not be keeping up with certifications or may have never received them, and they may not be familiar with the new technologies that they're being asked to deal with. For our data security and privacy group at Armstrong Teasdale, we have made a conscious effort to make sure that our group members are certified. We have three certified information privacy professionals, two in the U.S. and one with the EU certification, and we have two certified ethical hackers. We want to make sure that we're up to speed and staying abreast of changes in the technology so that we can be conversant as we're conducting our investigation, and so that we can explain it to the court and the jury.

Maurice Dawson: So if you're a human resources manager or you work in HR you need to create a job requisition to hire somebody that states that individuals must have graduated from NSACA school or they need to have a particular type of professional security oriented certification to kind of weed down all of these people who are going to be applying for the job.

How difficult is to find good technical security people?

Ryan Lally: Gartner is stating that by 2017 that 50 percent of companies are going be outsourcing some part of their network security program. And, I think, that the continuity of resources, the new deployments of technology, the challenges and costs that are ensued with that have a lot of companies looking toward outsourcing, either via consulting or managed services, on some level.

Darrell Songer: It is difficult to find professional staff with the technical skills necessary to perform the level of security testing we perform. We use search firms and still struggle to come up with right candidates. Typically, the candidates we find don't match the qualifications that Maurice mentioned. With that said, there is definitely a talent pool out there and the compensation level for the right people is climbing.

Maurice Dawson: When I lived out in the Baltimore-D.C. area, where I was a product manager for cybersecurity and network architecture, we had the issue where individuals would come work for us, and then they would actually jump to NSA or DISA or some other government agencies, because they were competitive in terms of salary and offering stability. That was something we had never seen before. I saw the same thing in Huntsville, Alabama when I worked as a program manager for army aviation. So even some of the defense contractors are struggling to keep talent.

Ryan Lally: A lot of times executives don't really know what they need when they're hiring somebody. So it's not uncommon to have a person who has gotten a lot of certifications maybe to try to move into the cybersecurity area, but not having real experience. St. Louis has a very small community of people. So it's a bidding war, and the largest companies in town that have the ability to pay the most money begin to collect talent because it's available and they can pay for it. So there's a massive gap in the smaller business.