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.

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.
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 good at finding ways to get around it. I think it will continue to be a problem, especially once you have to connect 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.

Darrell Songer: That's 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 fire 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 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.

Maurice Dawson: The commercial security sector because of companies adopting as the U.S. Government Rainbow Series documents are dated in the 1980s.

Maurice Dawson: The commercial side of things can be determined by mission, information classification and system type, so your system requires compliant to regulatory bodies. For example, healthcare organizations, Personal Identifiable Information, Protected Health Information, and etc. However, commercial organizations can take advantage of the National Institute for Standards and Technology (NIST) and Cyber Security Division to create baselines that apply to your cybersecurity measurement.

Ryan Lally: Why has the commercial sector fallen behind the defense sector in terms of 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 a 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 there have been 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.

Darrell Songer: The Department of Defense has the most sophisticated systems, and they're cutting-edge. We're not seeing that sophistication trickling down to the commercial sector.

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 industry. Louis那些 information is in many cases very collaborative and brings together a lot of big security teams and budgets. In small to medium businesses, it's a lot of folks who have technology or a reason to spend money from a business perspective, and they don't see a significant investment in cybersecurity programs.

Maurice Dawson: The commercial sector because of companies adopting as the U.S. Government Rainbow Series documents are dated in the 1980s.

Maurice Dawson: So the Rainbow Series was the initial documentation for the Department of Defense. It's a 20-plus different documents focuses on national security, system development, database development, fusion channel and analysis. More the problem with that data, they have not had an actual attack at a level that the company was actually impacted. Actually, we have numerous clients with our base which the breach was essentially ignored by management with respect to prevention of future situations. We find resistance to invest funds in the cybersecurity control-world of 100% directly impacted a deal. And, if ever there is immense threat to an enterprise, particularly small business, it's from catastrophic damages from cyber-related crimes.

Maurice Dawson: Defense has had security since the mid-40s, but it's a thin line. We now have common criteria, which focuses on international product certification across a number of countries. We also have something called EKACP, which focuses on certification and accreditation. And, you also have an individual which in charge of making sure systems meet particular requirements. These individuals are known as the Industry Guiding Authority.

Darrell Songer: The Department of Defense has the most sophisticated systems, and they're cutting-edge. We're not seeing that sophistication trickling down to the commercial sector.

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 industry. Louis那些信息 is in many cases very collaborative and brings together a lot of big security teams and budgets. In small to medium businesses, it's a lot of folks who have technology or a reason to spend money from a business perspective, and they don't see a significant investment in cybersecurity programs.

Maurice Dawson: The commercial sector because of companies adopting as the U.S. Government Rainbow Series documents are dated in the 1980s.

Maurice Dawson: So the Rainbow Series was the initial documentation for the Department of Defense. It's a 20-plus different documents focuses on national security, system development, database development, fusion channel and analysis. More the problem with that data, they have not had an actual attack at a level that the company was actually impacted. Actually, we have numerous clients with our base which the breach was essentially ignored by management with respect to prevention of future situations. We find resistance to invest funds in the cybersecurity control-world of 100% directly impacted a deal. And, if ever there is immense threat to an enterprise, particularly small business, it's from catastrophic damages from cyber-related crimes.

Maurice Dawson: Defense has had security since the mid-40s, but it's a thin line. We now have common criteria, which focuses on international product certification across a number of countries. We also have something called EKACP, which focuses on certification and accreditation. And, you also have an individual which in charge of making sure systems meet particular requirements. These individuals are known as the Industry Guiding Authority.

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

Maurice Dawson: The ability to predict behaviors and dis- cover norms of their target.

Jeff Schultz: From a legal perspective, Internet of Things is changing the landscape. As Maurice mentioned, there's a lot of devices these are collecting information about the user. And from a law suit standpoint in discovery, if you’re seeing somewhere what was somebody was doing at a particular time, what they were doing, whether or were they 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 fascinating developing field because it has created many new sources of information. Also, we've heard rumblings recently about product liability cases against manufacturers of those 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 device. 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 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 name of whomever is living next door. There's no security, and you can see who's on 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 use. So, there's good with these social media apps because of the relationship with somebody in the neighbor hood.
It's no secret that our government uses
is one of them. Their fear is that it will
ment of Defense agencies listed the six
real verification. It's really open.
be just a general lack of awareness. For
also old-fashioned training: Make sure
also old-fashioned, physical
the vulnerabilities are. I like to believe
of the amount
borhood. But in the terms of the amount
from disclosure to the outside world?
ne from disclosure to the outside world.

Darrell Songer: One of the Depart-
nments 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 – abduc-
tion of children, kidnapping and such.
It's no secret that our government uses
similar technology to track people in for-
exterior countries.

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

Jeff Schulte: We've been talked about
some of the technical safeguards. Mak-
ing 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, lock-
ing file cabinets and that sort of thing.

But from a legal perspective, one of the
things we encourage our clients to do is
to have non-competes in appropriate
circumstances, institute non-disclosure
agreements if a non-compete isn't appro-
 priate, or if a non-compete is appro-
 priate, include a non-disclosure agree-
ment in that non-compete agreement.
And, companies should obtain inven-
tion assignments from their personnel
so that 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 pro-
tection for that technology. Then there's
also old-fashioned training. Make sure
employees are aware of the risks associ-
ated with their activities on computer
and on the internet so they know what
the vulnerabilities are. I like to believe
that most employees aren't out to sub-
stitute 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,
know that there are a lot of compa-
nies now that are investing in training


Jeff Schulte: It's a common miscon-
ception that non-competes just simply
aren't enforceable. In Missouri – and in
most states – non-competes are unen-
able if you have trade secrets that you're
preserving. You have to have a non-
competitor and the company doesn't
operate in that non-compete agreement.
So, if you have one of those two protect-
tive interests that you're trying to safe-
guard from misuse by an employee who
is leaving and going to work for a compet-
itor, you can enforce that non-compete.
Now, there's a limitation on non-com-
petes. 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
someone sells their business to anoth-
er 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 com-
pany that bought their business. For geo-
graphic scope, it's whatever is reasona-
ble and 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
what 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-com-
petes, and we're seeing enforcement of
much broader non-competes. Nation-
wide non-competes aren't that uncom-
mon and they're something that's been
looked at in the South, because of the
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 Rock-
well Collins we were directed not to sign
non-competes as multiple Lead Sys-
tem Integrators would require use of our
Common Avionics Architecture System
for their airport. If we signed a non-com-
pete or agreed to sign non-compete ag-
 ment to one LSI we would limit our actual
business and lose our position as top rat-
ing glass cockpit developer. Thus we signed
Proprietary Information Exchange Agre-
ments, and set up a Brewer Nash Model
which allowed us to work with multi-
or single-locale proprietary informa-
tional Property. Also, we would develop
our systems to require fewer interfaces to
our systems to integrate. Thus organiza-
tions could refund their technical solu-
tions for systems integration that do not
expose any source code.

Jeff Schulte: That's definitely the way
we see many relationships with indepen-
dent contractors handled. Many won't

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: It's a common miscon-
ception that non-competes just simply
aren't enforceable. In Missouri – and in
most states – non-competes are unen-
able if you have trade secrets that you're
preserving. You have to have a non-
competitor and the company doesn't
operate in that non-compete agreement.
So, if you have one of those two protect-
tive interests that you're trying to safe-
guard from misuse by an employee who
is leaving and going to work for a compet-
itor, you can enforce that non-compete.
Now, there's a limitation on non-com-
petes. 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
someone sells their business to anoth-
er 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 com-
pany that bought their business. For geo-
graphic scope, it's whatever is reasona-
ble and 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
what 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-com-
petes, and we're seeing enforcement of
much broader non-competes. Nation-
wide non-competes aren't that uncom-
mon and they're something that's been
looked at in the South, because of the
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 Rock-
well Collins we were directed not to sign
non-competes as multiple Lead Sys-
tem Integrators would require use of our
Common Avionics Architecture System
for their airport. If we signed a non-com-
pete or agreed to sign non-compete ag-
ment to one LSI we would limit our actual
business and lose our position as top rat-
ing glass cockpit developer. Thus we signed
Proprietary Information Exchange Agre-
ments, and set up a Brewer Nash Model
which allowed us to work with multi-
or single-locale proprietary informa-
tional Property. Also, we would develop
our systems to require fewer interfaces to
our systems to integrate. Thus organiza-
tions could refund their technical solu-
tions for systems integration that do not
expose any source code.

Jeff Schulte: That's definitely the way
we see many relationships with indepen-
dent contractors handled. Many won't
We’re seeing a lot more from the commercial sector in terms of conducting and implementing cybersecurity controls and measures as it becomes more prevalent in the news.

JEFF SCHULTZ, Armstrong Teasdale

CONTINUED FROM PREVIOUS PAGE

The classic response from a C-suite individual would be “yes, we are covered.” We then ask if you 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 of business policy in general. 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 extremely 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 so, you’ve been following 12 mandatory regulatory considerations, and you’ve only done six of them, it’s difficult to ascertain 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 critical importance 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. Agencies 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. One of them was a company called SafeNet who studied 2,010 breaches around the world and looked at the amount of financial loss organizations 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 30 percent of your customers would stop doing business with you as a result of a breach down to 2 percent or 6 percent for a low-impact scenario. The highest level is the most frightening. If an organization receives suspicious activity while they were employed by our client, we conduct a forensic examination of the computer to determine if what’s called a cryptographic hash matches an individual machine and had access to this particular file. It’s a large percentage of customers that lose confidence and stop doing business with that vendor.

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

Maurice Dawson: In 2013, Lloyd’s of London published a white paper about how it insures organizations for cyber insurance like power plants and other facilities deemed important critical infrastructure. So what came up is, if you were a director, you would, in a legal sense, be measuring them against some type of baseline level. Do they have policies in place? Do they have controls in place? You then ask, based upon their compliance with those controls, setting the insurance rate appropriate for them. They’re a bigger risk with the least amount of coverage in place.

Jeff Schultz: 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. Agencies 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. One of them was a company called SafeNet who studied 2,010 breaches around the world and looked at the amount of financial loss organizations 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 30 percent of your customers would stop doing business with you as a result of a breach down to 2 percent or 6 percent for a low-impact scenario.

If a company has a sophisticated security model in place that differs 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 user interacts with the object, so this particular file hasn’t been used in a month. They lose access to that file. So, down the road, when they’re trying to get access to those files. Or, if you know they’re going to be putting in their two-week notice, then they immediately access is removed.

Ryan Lally: There’s so many applications that employees access every day that you can’t attach information to. With services like Box or Dropbox or Facebook, you’ve got your own personal e-mail accounts and instant messaging accounts. Well, not those are encrypted sessions, and so standard network technologies can see the destination of the site, what site you

CONTINUED ON NEXT 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 cybersecurity 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 contractors 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 businesses.

---

**CONNECT WITH OPPORTUNITIES**

Safeguarding your technology assets is a business issue, not a technical issue. Address the big picture with us.