ST. LOUIS BUSINESS JOURNAL

TABLE OF EXPERTS

IS CYBERSECURITY A PRIORITY IN YOUR BUSINESS?

PRESENTED BY

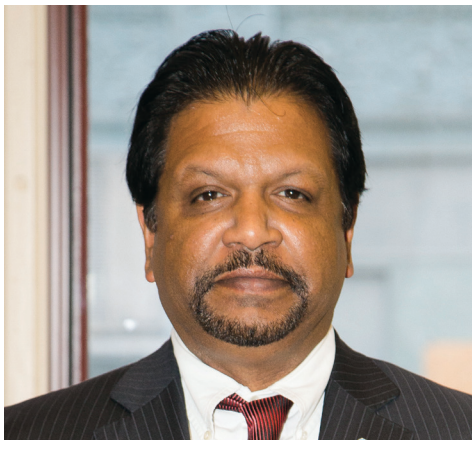
C3dge

UHY LLP Certified Public Accountants

AVATARA
IT'S TIME TO RETHINK I.T.

SpencerFane®

Meet the experts



SEKHAR PRABHAKAR

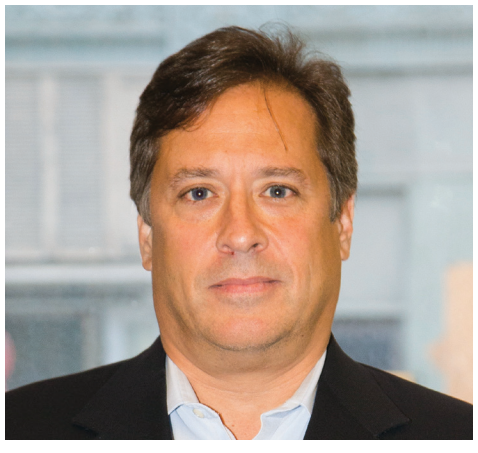
Sekhar Prabhakar is one of the founders of C-Edge Software Consultants. Prabhakar started his career as a software engineer at Arms Inc. working on a subcontract with Booz Allen Hamilton. He was one of the key members of the supply chain management system development team for Continental Baking Co. (Wonder Bread). Prabhakar then joined Sybase Open Solutions Group and supported several Wall Street customers, including Merrill Lynch, Goldman Sachs, Shared Medical System and other financial, health care and government organizations.

At Sun Microsystems, he was instrumental in maintaining and migrating the Sun Globe System that was used by senior management to look at sales of the products across the company. He was also part of the quality and financial team, which was responsible for implementing the IRQI (information resources quality index) that was used to govern the Corporate Services Vision for the entire company.

DAVE HARTLEY

David Hartley is a principal with UHY LLP in St. Louis delivering "Virtual CIO" technology guidance to primarily private businesses in the middle market. Hartley assists companies with everything from digital transformation and IT strategy to assessing cyber risks and implementing cybersecurity programs. Hartley has experience in technology, consulting, audit and C-suite business leadership roles.

Prior to joining UHY in 2015, Hartley was vice president and chief information officer at Arch Coal Inc., responsible for overseeing technology at the company from 2009 to 2015. He started his career as a CPA in Big 4 public accounting firms, including Ernst & Young, Arthur Andersen and Protiviti. Hartley's diverse skillset and decades of experience both as a CPA and a technology executive have made him a sought-after business adviser.

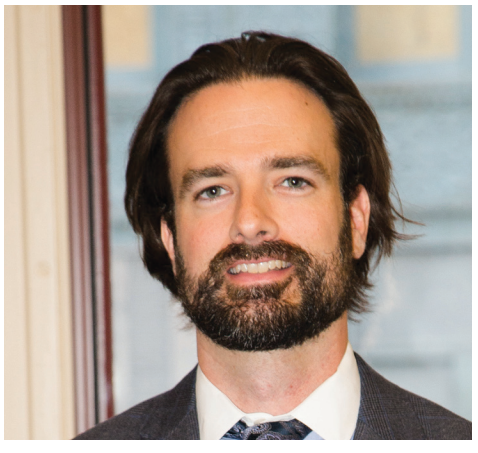


ROB MCCORMICK

Rob McCormick founded Avatara in 2005 with the goal of bringing enterprise level IT solutions to midsized businesses nationwide through CompleteCloud. CompleteCloud is the most secure private cloud environment on the market that leverages virtual desktops to help companies centralize data, increase performance, and rethink the way they pay for, access, and support their IT needs.

Prior to forming Avatara, McCormick was chairman and CEO of Savvis Communications, where he led the company from its initial IPO (as it evolved from Bridge Information Systems in 2000) to its development and growth as a service provider with more than 1 million square feet in data center space, a global network and almost $1 billion in annual revenue. Additionally, Savvis was honored in 2005 with Gartner's Magic Quadrant Award for Managed Hosting, ahead of companies like IBM and AT&T.

Prior to Savvis, McCormick was COO of Bridge Information Systems.



THOMAS HAYDE

As a privacy professional at Spencer Fane, Thomas Hayde aids clients in developing comprehensive strategies to address information practices and data breach risks, avoid potential claims and liabilities, and ensure compliance with all relevant legal requirements. Hayde also helps clients develop and implement protocols surrounding how to respond when a data breach occurs and defends clients against potential claims and lawsuits regarding data breaches. He has experience defending against and resolving civil claims and enforcement actions under specific information privacy laws, such as FCRA, GLBA, HIPAA and RFPA.

In addition to his privacy and data security practice, Hayde is a litigator. He has successfully represented Fortune 50 and Fortune 250 companies in a wide range of other complex civil litigation matters in state and federal trial and appellate courts.

Equifax announced a cybersecurity breach last month. Last week, Whole Foods and Sonic announced cyber breaches. This week, Yahoo revealed the scope of its breach was actually 3 billion people, not 1 billion as previously disclosed. Why are companies still not addressing their cyber risk appropriately?

Rob McCormick: The problem you have in the current age of computing is people are used to convenient access to data and oftentimes offline access to data, and there's a real lack of policies preventing them from doing the things they like to do on the internet. In order to really address these things, you have to change not just the technology, you have to change employee behavior. And when those employees are large performers on the revenue-generation side, for example, especially in the mid-business space, employers are really reluctant to do that. They say, "Well, then I have to tell so-and-so to not use Dropbox," or I have to say, "You have to use multifactor authentication to get in," or "You have to change your password occasionally." Those are things they don't really want to tell their employees because the employees get aggravated. We tell people, "You just don't have a choice. You have to deal with it." The challenge is cultural not just technical.

Sekhar Prabhakar: Everything starts with leadership having the buy-in for cyber risks vitally important. Leadership has to definitely consider that cybersecurity is not just an IT problem; it is a business imperative. If sensitive data is not protected, then basically you lose your customers' trust. So, you have to engage in assessing that risk, and what is the level of security you must attain. By inserting controls, then constantly monitoring risk, and continuously improving upon it, you will minimize the risk. In the past, companies used to say, "Oh, everything is secure." So you wouldn't know unless you're hacked. By following this process, just like how you lock your door and check your windows, this is basic housekeeping that executives have to do, and they should look at it as mostly a business imperative and not just a technology problem.

Thomas Hayde: And in the space of privacy professionals, there's this concept that's referred to as privacy by design. And there are some business leaders out there who are trying to incorporate this ideal into their core mission statement. That you protect your consumers' sensitive information, and that the confidentiality, integrity and accessibility of that information is protected at the highest possible level. So every department, every unit, every initiative, it starts with what's called a privacy assessment of how is this business initiative going to comply with that mission statement? But that's just not in the cultural zeitgeist of business, especially in the U.S.; we do not include the ideal of privacy by design or security by design. At a visceral level, all I can say is, especially among the smaller to mid-sized businesses I often am advising that it's just the culture or the attention isn't paid as much to this until they suffer a serious or possibly serious incident. Then it hits them that "This is real" and "It can happen to me, and it could potentially disrupt my business to a degree of catastrophe."

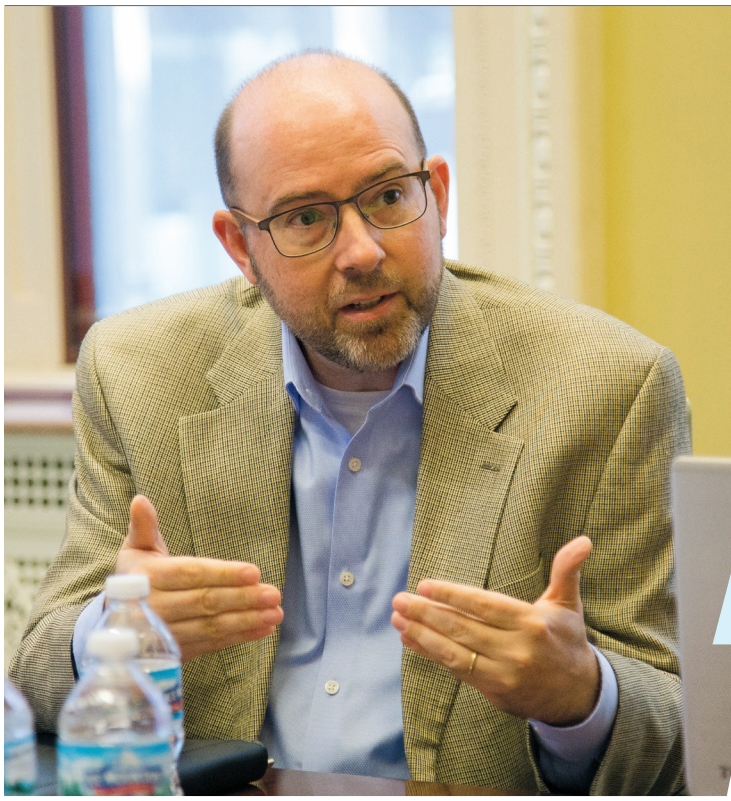
Dave Hartley: Going back to the original question, there's two things that pop up in my mind. The first thing is, this is really difficult work. It's complex when you look at how organizations have grown over decades. They didn't grow with security in mind. They grew with ease of use, they grew pre-internet, and now we're at a stage where we're trying to deal with that. One example of that is Equifax, because if you believe the CEO, it was one employee who missed one vulnerability, and it was combined with the fact that it was missed by a vulnerability scan. Look at all the business processes and technologies Equifax has in place, and it still happened to them. Same thing with Yahoo. They proclaimed a breach and said it was a billion accounts affected. And it was only after Verizon acquired Yahoo they realized the number was actually 3 billion accounts. Equifax has hundreds of cybersecurity employees, and it still happened. So, the cyber response is not necessarily appropriate or commensurate with the risk right now. And cyber risk continues to escalate. I think there is a lot of denial in terms of, "It's going to happen to somebody else, but it's not going to happen to me." And I think there's a lot of that thinking still out there. When you look at how they got in Yahoo, they did a targeted phishing attack on a single Yahoo employee. The bad guys only have to succeed once where we have to succeed every single time, which is why it's almost impossible to do.

Rob McCormick: People ask, "Why is it that all of these hacks are of large companies?" Well, because their problem is really hard to solve because they're distributed enterprises. They probably acquired the technology over time, and they can never just start over, right? If you're a mid-sized company, you actually can start over. We tell people, "The only way to really solve this problem is start from scratch with a security-first view of it," and that's technology, employee behavior and then the monitoring of that. The larger you are, the harder that is to do and its really expensive.

What question should business executives be asking their IT leaders?

Dave Hartley: Having led a technology function at Arch Coal, I would like the executives and my clients to ask, "What do you need?" "How can I help?" "What is it that keeps you awake at night?" I think getting those answers is important for you to understand what's really

CONTINUED ON NEXT PAGE ▶



> *The risk continues to escalate. And I think there is a lot of denial in terms of, 'It's going to happen to somebody else, but it's not going to happen to me.'*
>
> **DAVE HARTLEY,** UHY LLP

► *CONTINUED FROM PREVIOUS PAGE*

happening. But the flip side of that is, it's not just an IT conversation. You need cross-functional teams working on it, because when you look at the damage to Equifax or anybody that suffered a breach, it's not just IT that suffered. You look at all the other things. And that's where you need to have people across the entire business looking at this problem comprehensively from the beginning rather than just being brought in once a cyber breach has happened.

Sekhar Prabhakar: You have to have an overall risk management assessment for the company. Do we have a risk management framework? Are you putting the right controls in place? So, if a threat happens, what is the timeframe that the top executive is going to be informed? How does he need to deal with it? Is there a good communication process that is established? Have you tried these kinds of cases by simulating similar attacks? Are you storing your sensitive information in a place that is isolated from your regular data? You should plan a lot of levels of security based on your aptitude to deal with risk. These challenges are not only in commercial, but in the Department of Defense too. I attend a lot of conferences, and this is the main thing they're talking about that the leadership has to take notice and make sure this entire posture is really there so you can minimize the risk of being hacked.

Rob McCormick: I think it's important to understand that if you ask the IT guys, a lot of times the answer they're going to give you is, "It's a long timeframe, a lot of money, and complicated," And so I try not to ask open-ended questions. To me, the first thing you want to know is, what risky behaviors are going on right now with our employees and our data that are easily corrected? You may hear, "We've got our entire database on laptops that are out wandering around the world." That should be a red flag.

Dave Hartley: And those laptops are not encrypted.

Rob McCormick: Right. Or they're using public cloud services because it is easy in the short term? I always say, "Let's not leave the keys in the car." Look for simple things to change like password policies or eliminate the use of external or public storage,

Thomas Hayde: As a lawyer, we love these written policies and procedures, and that's a starting point. What do we have in terms of written policies and procedures? Do they fit what's actually going on in the business? If not, what do we need to change or add to in the policies and procedures? Or what do we need to change as far as our business behavior and our setup? Even industries that aren't financial institutions or health care-covered entities that are required by law to have written policies and procedures, generally the approach of having a written document that sets out privacy and security policies gives you somewhere to start with. And then on the back end, when an incident does occur, whether you have specific regulators in the health care financial spaces, or if it's just the possibility of state attorney generals or the Federal Trade Commission, the fact that you've, from a compliance and risk mitigating standpoint, you're going to look a lot better to have had policies and procedures that you adopt that you review, and then importantly, that you then perform to those policies and procedures.

Rob McCormick: Have a password policy. A lot of people still don't. So if you have a problem and a regulator comes in and says, "You didn't expire passwords?" They're going to throw you out the window really fast. Even those things aggravate employees that aren't used to it, and it's not just their computers, it's all their devices. So again, the business executives need to understand that they just have to get past that.

Sekhar Prabhakar: That is a cultural shift that has to happen. The leadership has to really set that policy, and it has to be a written policy. Then you need to ask, "Do we have an insurance policy to cover in case things were to happen?" That kind of mitigation of risks from the business community perspective is very important. By spending some money, I protect a big loss for business.

What are the top cyber risks that you see companies struggle with?

Sekhar Prabhakar: The biggest risk that I see is that security in most companies is an afterthought and not part of system lifecycle development. Code scans are run after the application development is complete and remediation is undertaken after the fact. Security should be an integral part of application development, especially given the rapid changes in technologies that bring a new set of problems of threats. For example, the growing use of web services that are not secured properly or cloud computing without adequate security controls bring new challenges.

Rob McCormick: It seems to me that the biggest risk going on today for the executive is that it's become very easy to turn a well-architected secure system into a vulnerable system because data is now easy to store all over the place. AWS makes it really easy. Just get on the web, buy yourself a server with some storage, and put some stuff up there. You used to have to go to the IT guys, and they would have to buy a server, and there was a process and integration, and now you can have data repositories anywhere you want, easy right? So how do you, as the business executive, deal with that? Because to me, the biggest risk is not knowing where your data is. In the old mainframe days, you knew where your data was and had very few ways to get to it. Today we use private cloud environments to help people achieve this piece of mind utilizing the same old principles: centralization, standardization, and minimize ways in and out of your core systems, or otherwise minimize the surface area of attack. So if you know where your data is, like the old mainframe I keep going back to, "All my stuff is centralized. It's in a secure data center. I've got firewalls around it." Then you have to focus on keeping people out. The minute that data just starts showing upon laptops or in Dropbox you have lost control, and breaches tend to start happening. The fact that it's so easy to put data on external repositories where you have no control whatsoever is a really big problem. The multiplication of that availability has really driven a problem that's very hard to solve from a business perspective.

Dave Hartley: From my perspective, both in the public breaches that have

> *You have to have an overall assessment for the company. Do we have a risk management framework? Are you putting the right controls in place?*
>
> **SEKHAR PRABHAKAR,** C-Edge Software Consultants

been publicized in the media along with what I see throughout the UHY client base, is that companies are struggling with phishing. And if you're going to educate your employees and get them to do one thing — if you can get them to understand what phishing is, why it's so dangerous, and what they can do about it — you'll be substantially down the path. When you look at the Yahoo hack, how did that happen? That breach came through a single phishing attempt targeted at a specific employee. And you see that play out a lot. Why phishing has become so difficult is because it used to be there were very obvious things, that when you got a phishing email, that they misspelled words or phrases that didn't make sense. Those days are gone. Now phishing emails are getting really, really good, and it is very difficult to tell. That's why this culture of cybersecurity needs to happen, creating awareness so that your employees are an asset and not a liability, and that they're part of the solution, not the problem. That sense of cyber awareness, the educated employee, which we'll talk more about later, is paramount in my mind.

Rob McCormick: We've had a couple customers where there is an email that looks like it's from the executive to the CFO pursuing the movement of funds to a false account. It's really, really hard, even if you're educated to identify that the message was fake. There are really nice training programs now that automate phishing training where you can build fake attacks that really emphasize the learning while your employees are facing realistic attack scenarios. In a sense, they have gamified security training, it works well as you're constantly keeping them aware, because they know you're testing them all the time.

Sekhar Prabhakar: Oftentimes, we have this mindset that an attacker is always from the outside. However, the threat could originate from the inside. So employee training and awareness become very important. While most companies have mandatory security training that employees need to take, it would be good to make them more engaging and also offer incentives to complete the training.

Dave Hartley: And many nontechnical business executives unfortunately aren't comfortable having this conversation. What we have to do is to help them get to the point where they are comfortable having cyber conversations. And it flows both ways. They have to express an interest and try and make an effort to understand, but we, as technology, legal and other professionals, need to make sure that we eliminate the tech lingo and instead describe cyber risks in straight-forward terms. These conversations should be grounded in business risk management — not bits and bytes, not acronyms, not hardware. It's not any of those things. It's making sure that the person understands the business risk and recognizes what they need to do about those risks.

Sekhar Prabhakar: You have to have the process in place. When are you going to inform the concerned authority to minimize the risk? You wait for when 1 billion records were stolen, then you find out 3 billion were stolen. These kinds of things have to be addressed in a timely fashion to prevent further damage. And that is something you have to incorporate into the process depending on the level of risk that you can handle.

Dave Hartley: A small investment up front in cyber preparedness and incident response can save substantial costs on the back end when something does happen.

Rob McCormick: When you talk to the business guys, they don't really have a picture in their head like we do about how risky it is. We hear "Well, I just had that server up for five minutes." It doesn't take 30 seconds until something's compromised because it's electronic attacks, not people attacks. They will find an open door immediately. So I try to draw this picture. I say, "You got this castle with your wall around it. And picture the scene from 'Lord of the Rings' with the castle being sieged by a million orcs and you kill 10 and here come more, that's really what it's like." That many people and bots are trying to compromise your systems and your employees all the time. If you're not paying attention, they will. It's not just some guy decided to attack you. Most of this is electronically driven and random. They're trying to exploit everything that's out there. Just being in business and existing online, you are at risk. Which is why you want to make yourself look as uninteresting as you can electronically. But it's not just somebody had to know your company and go after it, it's just part of being on the network in the first place. It's really horrifying if you see those kinds of events.

Sekhar Prabhakar: Law enforcement is taking cyber crime more seriously. Cybersecurity breaches can wreck many individuals and families. The United States is doing good things, but this is not so in all other countries.

What should companies and individuals do to mitigate risk and protect themselves?

Dave Hartley: One of the services we deliver for our clients is cybersecurity employee awareness training. One of our lessons learned over the last couple of years is that if you have a training where you bang them over the head, "No, no, no. Don't do this, don't do this," they tune out. They don't listen. They don't care. We have an interesting opportunity right now that the Equifax breach has gotten to the point where the average employee is now concerned. One of the training sessions we do now is specifically

CONTINUED ON NEXT PAGE ▶

▶ *CONTINUED FROM PREVIOUS PAGE*

targeted around the Equifax breach. We start the training with some education about the top cyber risks — phishing, spyware, keyloggers and ransomware. Then we go into a seven-step action plan that people should follow specifically in response to the Equifax breach. We teach them during the class about the steps they should take to protect themselves. And I've never seen a group of cybersecurity training employees that have been more engaged. The participants are taking notes and come up to me afterwards and ask, "Can I share this training with my kids? My family? Will this session be recorded where I can have them watch it?" Because it is things that we should be doing, but a lot of us aren't. I did a presentation yesterday and asked the group, "How many of you are aware of and concerned about the Equifax breach?" Every hand in the room went up. My next question was, "How many of you have done something about the Equifax breach or have a plan for what you're going to do about it?" Two hands out of over 100 people. And that's where we have an opportunity to really connect with people on a level that they care about because now they're concerned and want the help. If we can teach people why phishing is so dangerous on a personal level, that benefits the employer too, and you now have a more educated and secure workforce, but it's also benefited them personally. So that's one of the strategies we use is to try to make our training sessions personal so that people actually care and they feel invested in what they're learning.

Sekhar Prabhakar: I always have subscribed to some of those LifeLock services, which are good at monitoring things. During the OPM hack, the government provided a free credit monitoring service to defense contractors and employees. This information was sent in letters and e-mails. However, not many people took the initiative to register for these services unless something happened to them. It is important that we are more proactive and protect ourselves by utilizing these types of services and not wait until something happens.

Rob McCormick: It really is a life skill now. From the time you're born to the time you die, you better understand, whether it be at work or at home, people are out looking to get at you in an electronic fashion.

Dave Hartley: I had the unfortunate pleasure of somebody filing my taxes for me three years ago. So I have been to the IRS office in Chesterfield more than I have ever wanted to. And then somebody hijacked my personal email account. Those two things, without causing a lot of damage, made me hypersensitive and hyper aware of personal cyber protection. A lot of people are living sort of in this fog and they don't clearly see the issue, and they haven't necessarily done what they need to do, whether that's from not having enough time or not making it a priority. We need to help people understand why beefing up their cyber protections needs to be a priority.

Thomas Hayde: From the macabre legal perspective, these incidents are going to be inevitable. There's no such thing as perfect security. So with that in mind, looking at our small to mid-sized client base, we are talking about cybersecurity insurance, and it's less common the smaller your company gets. But companies really need to be considering what the potential exposures are when an incident is going to occur. Cybersecurity insurance is still a product in its infancy, but it's certainly grown leaps and bounds. And I think the insurance industry is really figuring out how to price and service that sector. So it's going to become more accessible. It's going to become something like your general liability, your workers' comp something that needs to be a part of your portfolio. Other than that, I also recommend companies bring in experts, whether it's an outside counsel or forensic experts. With those type of vendors and consultants, you need to have an ongoing relationship with them and not wait until you have a problem. That way, someone doesn't have to first learn everything about your systems, everything about your business after something happens. They have a baseline understanding, so that when something does occur that needs to be investigated, potentially contained, remediated, they have a head start there, and you have a Rolodex of potential vendors that can help you out when you need it. Because what we see are a lot of our clients, again, waiting. Something happens and then that's the first time that they really want to have a conversation with me. They hadn't thought about this issue in a way where they're prepared to act as quickly as they could because some of these incidents, you're talking minutes are important. Hours are critical. Days can mean the difference between your business making it through the incident or not.

Rob McCormick: A speedy response is really, really important in almost every instance. And if you're prepared, you can move quickly.

Sekhar Prabhakar: I would like to have an attorney as a part of my cybersecurity defense, because I want to know exactly what I'm supposed to speak about and not supposed to speak about. What information should I be sharing at that moment and with which sources, and how should I communicate? It is very similar to registering a complaint with the police and hiring an attorney for what you experience in other situations, such as property damage or when you are injured. This approach will help deal with cyber crimes in a better way.

Dave Hartley: We co-hosted an event

a couple weeks back where the group was challenged to respond to cyber response scenarios. We said, "Here's the breach scenario. You all have to respond to this case study." So the discussion started with basic questions like, who is authorized to talk about the breach?" Trust me — when the house is on fire is not the time you want to be making these basic, critical decisions. Anything you can do to prepare in advance of a breach, like developing a written incident response plan, will prove extremely beneficial. During each of the scenarios we asked four or five fairly significant questions about decisions that have to be made quickly. I think there was a real a-ha moment for the business executives thinking, "Wow. I never really thought about that before. If that were to happen to my business, it would be incredibly damaging." So getting people to engage and really think through some of these decisions in advance of a breach is critically important. On a totally separate point, I was talking to an insurance sales representative for one of the major insurers last night. And he said, "We feel we've pretty well penetrated the public company world," but what they view as the next big market for cyber insurance is the middle market. I think the need for cyber insurance is, unfortunately, becoming more significant every day. So I think that in the next five years, you'll see a significant push from the insurers into the middle market.

Sekhar Prabhakar: You also want to make sure that the businesses that you're engaging with have a good cybersecurity policy. Are they going through the training? There is a possibility their systems could be compromised which can hurt your operations or services. These kind of checks have to be done. And one other thing I liked what you said about getting experts to come in and talk with your employees can help increase this awareness across businesses. So that you have neighborhood watch. There is a benefit to everyone being involved as this benefits the entire business community.

What kinds of tools and services do you recommend to ensure companies are prepared to minimize breaches?

Rob McCormick: I think it's really important for companies to understand that the days of passive security measures are long gone. It used to be, "Yeah, I bought a firewall. I put it on the Internet. We're good, right? And every once in a while, we'll check and see if anybody's trying to get in." But as we talked about before, it's significantly more likely that the attacks are going to come from the inside. It oftentimes is an employee that doesn't know they've been compromised. If you're not actively inside the wall looking for issues or threats, you're most likely going to miss it. Tools exist today that dynamically respond to the changing threat factors, whether it be the web-locking technology that do not allow your employees to go to sites with ransomware, or active internal intrusion detection looking for somebody's internal PC trying to break into the server. This is all inside where the firewall traditionally was; outside-in is not the only problem anymore. It is often an employee that got phished or somehow compromised, and now they're in. By the way, no light goes off saying "Somebody broke into one of your 400 desktops." They're going to hang out there for a long time quietly doing their thing, because they don't want you to catch them. The longer they go without getting detected, the more damage they can cause. If you're just watching your outside firewall and happily doing your business, you're going to get nailed eventually. The technologies that actively watch what's going on internally and prevent those kinds of behaviors inside the firewall are really important.

> *"It's been a very common thing where there have been vulnerabilities exploited across platforms that a lot of different merchants were using, and credit card information is getting stolen from that platform, from that little point in time from where they're putting it in on your web site to where it gets encrypted and sent to the processor."*
>
> **THOMAS HAYDE,** Spencer Fane

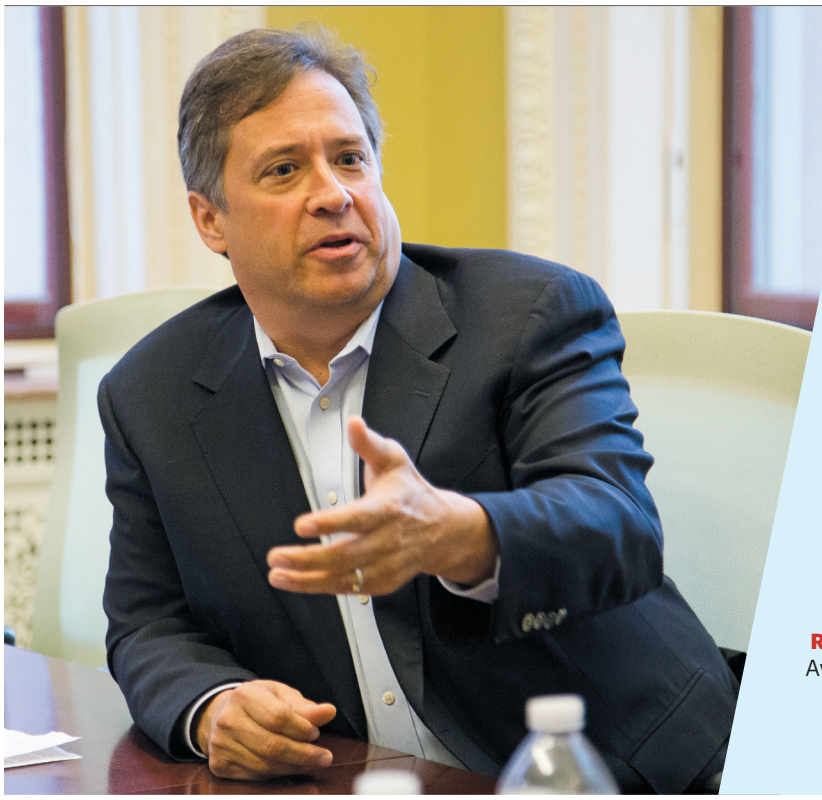
Sekhar Prabhakar: Mobile phones have become one of the key things where people use it for everything. So, when one of the firms asked us to build a mobile application, we send a list of questions. That includes "Do you give your mobile phone to your kids?" "Do you let them install any apps on them?" These are some of key things we want to know, because a lot of free apps collect information. On my phone, I don't download any apps, no free things. These are some precautions I take personally. Also, you may have the best tools and you may have the best people, but not having the whole risk assessment and the security framework that fits your needs for your industry and your customers is very important. CEdge has developed our own tools such as cyber edge and forensics edge. We start from assessing risk, analysis and penetration testing to help design a cyber posture. We are working on predictive analytic capabilities as well as post analysis in case a customer is hacked. This includes forensic evidence from logs. Sometimes people say, "Oh, we are using ArcSight or Solarwinds to protect our site." And these tools certainly do that. But if people are not alerted in a timely fashion and things are not taken care of, you may have the best tools but still you may have let go something that could have caused problems.

Rob McCormick: That's a good point. Quarterly scans or just making sure your PCs are all patched is just not enough anymore. Things change so dynamically, intra-day, intra-hour, intra-minute. Unless you're using third parties that are actively in the current threat space that know, "Today, something just came out five minutes ago," your going to be too late. Take the WannaCry ransomware that caused so much trouble. The people that were using services that understood how to quickly close down the vulnerability had no issues. Other people paid a huge price; you really need to leverage security experts. Your traditional IT support is not in the fight enough to know how to handle all the various attacks. We consider ourselves pretty good at what we do, and we still leverage industry leaders when it comes to security.

Thomas Hayde: Reviewing contracts with your vendors as well. They may sign up for e-commerce platform and the web development contract with a provider, and then they assume that that vendor's responsible for patches, when that's not set forth anywhere in the contract, that wasn't addressed, that's just an assumption. We've seen that happen a lot. And then a patch gets missed. And on the e-commerce platforms, it's been a very common thing where there have been vulnerabilities exploited across platforms that a lot of different merchants were using, and credit card information is getting stolen from that platform, from that little point in time from where they're putting it in on your web site to where it gets encrypted and sent to the processor. And if you go look, various states will keep a database available where you can look at all the data breach notifications that companies have had to give. California has one that may be the most comprehensive. You can go look through there if you're interested and see that a lot of the breaches over the last couple of years have involved credit card payment information. And a lot of them have been vulnerabilities from e-commerce platforms. And it gets down to the assumption of the businessperson that that vendor was going to be responsible for making sure everything was patched, and that wasn't addressed. So business people need to be aware of that, and bring in consultants, counsel, whoever it is, to help them review their contracts with those key service providers to know, "Who's responsible for making sure this aspect of security is going to be covered?" Because these patches are put out, and then it goes months for some of these companies that they didn't have their e-commerce platform patched. And it's an easy vulnerability for the hacker to exploit. And then for some companies, that ends up being all your customers in a six-month period now are going to be notified, and they're going to realize that their credit card information was exposed because of your company's failure to protect their credit card information that they thought was secure when they entered it on your web site to buy $100 of whatever widget you're selling. And so, are they going to come back and engage in e-commerce with your company again? It's a huge potential intangible cost to your business goodwill, and I think it goes back to the culture issue, again, that businessperson not realizing that was a point that needed to be addressed and just assuming, "Well, I've got these web site developers that are bringing in an e-commerce platform. They must be responsible for it, right?" And they're not.

Rob McCormick: We are the virtual CIO for most of our customers. We have had cases where the marketing person or the sales person wants to build a site for their customers, and they hired a web development company. These guys are usually artists that know how to make a site look pretty, but they don't understand the technology. And then they hire someone else to do the back

CONTINUED ON NEXT PAGE ▶



> *If it is more than just a brochure for your company, if it actually captures data or credit cards or anything like that, you need to really think that stuff through. Because most of those companies are not all that sophisticated about it.*
>
> **ROB MCCORMICK,** Avatara

► *CONTINUED FROM PREVIOUS PAGE*

end stuff. All done with little to no long-term accountability or concern around security. It's one thing, if it is a pretty brochure that sits off the network, but what if it is capturing credit cards or other consumer data. You really need to think this stuff through.

Sekhar Prabhakar: Oftentimes, we also forget about the physical security. A lot of people in offices, they take it for granted. They're not in their seat and they don't even have a screen saver turned on in a few minutes if they're not really working at the desk. At Sun Microsystem, that was taken seriously and our CEO Scott McNealy often talked about this. You've got to have all those controls, including physical security. And also the point you bring up is a good thing with e-commerce. We have been doing e-commerce work for the last several years and have helped our clients achieve PCI compliance. While the statement of work may outline the scope related to the compliance, it gets tricky when it comes to whose responsibility it is to deal with certain things. For example, patch management at the operating system level is very important. When a security loophole is found, you have to put the patch in. In large enterprises it is hard to get those patch updates in place unless there is a clearly defined plan that considers all aspects of risks. A well-defined operational framework helps protect the company. This has to be monitored and continuously improved. it is very much necessary that the senior management allocates the necessary resources and make it a part of the mission.

Talk about the pros and cons of outsourcing.

Sekhar Prabhakar: Global companies keep outsourcing the work in different places, and then there's mergers, acquisitions, and then you go ahead and deal with those things as they come up. These companies look at any data residing in the U.S. and know that it's protected by the policies established by the government. The information has to be made available when our government demands. When you have offices around the world, there could be issues. I heard from one of the executives who went to another country to their office there, and he was under the impression that it would be well protected, and he was surprised that it was a very small room, and there were a bunch of people doing the entire IT operations from that room and not much security. So what is the level of physical security you have in those places? Have you done any assessment? Because our government says we are to protect our borders it does not mean protecting just physical boarders. You're having to protect virtual border, which means IT assets and data in other counties too. Is the government going to really ensure that people are taken to task if data or IT assets are lost? Do you want to put the data that you cannot even get by requesting a subpoena or whatever? All those things come into play, so it's always good to have companies rely on local companies to do business especially when it comes to sensitive data as risk could be better contained.

Rob McCormick: We've seen this swing from when I was really on mainframes, which are very secure — you knew they were in a room with locks and really hard to get into — to this now highly disaggregated environment with data everywhere and public cloud and really easy to get access. Now I think businesses are starting to get suspicious of that. Because I go back to, what should I know as the business owner? I should know where my data is and how can people get at it? And the only way to really know that is to make it a much smaller problem. We talk heavily about, you got to think about, how do I centralize everything? With our product, even your desktops are in the data center. What you see is like a movie of what is happening on your computer in the data center, kind of like the terminal to the old mainframe. And the only thing in and out of the data center is that picture, and even that's a highly authenticated and secure channel. There's no holes open into the data center because they don't have to be, and you know exactly where all your data resides. If you host with Microsoft or AWS, do you really know where your data is? Or if you use Google or Dropbox, do you know what they're doing? What happens when something goes wrong, can you call them up for help? Do you just trust that because they're big, they're smart and have your businesses best interest in mind? We build a private dedicated environment per customer. We use a subscription model, so it's got the economic benefit of cloud, which is you didn't have to buy all the hardware, but it's yours,it's built from scratch, and you know where it is. We give midsized businesses the ability to move to a new environment that was built with a security first mindset. Again, think mainframe, all your data in one place and very secure, meshed with the access and mobility of today's environment. Done right, you can have the best of both worlds.

Dave Hartley: So my firm sees outsourcing from a slightly different perspective. My firm provides traditional audit and tax servicess, in addition to other outsourcing and consulting services. We also perform SOC audits for companies, such as SOC 1, SOC 2, SOC for cybersecurity. We're seeing a real explosion in demand caused by the concerns about outsourcing that you guys have just raised. Companies are now saying, "I have to get a handle on my third-party cyber risks. I need to know what my partners are doing to protect me." We're seeing middle market companies bombarded with questionnaires from large public companies trying to get a handle on their third and fourth party cyber risks. Rob, you've probably filled out dozens or thousands of those types of questionnaires for your business. What the AICPA and others are driving towards is more clarity in the market regarding cyber risks. In addition to the usual SOC 1 and SOC 2 reports, we're seeing other forms of third-party cyber risk management evolve, such as shared assessments and the Cloud Security Alliance (CSA). We're starting to see this need for independent assurance really grow. The trend towards understanding, measuring, and managing the third-party risk in your technology supply chain is really growing. It's critically important, for the reasons that you guys have outlined, that you need to know what your partners are doing — or not doing. You can mitigate some of the risk from a legal perspective by including protective wording in your contracts and transfer some of the risk through cyber insurance. But managing third-party risk needs to be an active and intentional task you perform, not something that you get to only after something bad has happened.

Rob McCormick: That's 100 percent right. Our customers, Boeing subcontractors, Lockheed subcontractors, medical malpractice law firms that deal with Cigna, we have clinics and hospitals, and they're all getting pushed down security standards from larger customers or industry regulators, and you can't answer the questions that Boeing or Cigna asked you accurately if you can't actually inspect what's going on. So the concept of, "Well, I'm hosting my stuff with the big guy so it must be OK, does not work," bigger is not better anymore. As a matter of fact, bigger may be much worse, because you have no control over what they're actually doing. And they may say, "Well, you have to patch your own systems," but Amazon has systems underneath that are running all this stuff. How do you know what they're doing with those?

Dave Hartley: I take a little bit different view regarding the size issue. For example, Amazon Web Services (AWS) publishes an AWS risk and compliance whitepaper that outlines its approach to cloud security and how AWS integrates into all of the major control frameworks (NIST, FedRAMP, HIPAA, ISO, etc.) It begins with about 20 pages of its approach to complying with all of those control frameworks, including links to its SOC 1, SOC 2, SOC 3 reports audited by an independent CPA firm. It basically says, "Here's our approach to mitigating cyber risk and we have audits to prove this is what we do." They also include their responses to the Cloud Security Alliance's questionnaire in the next 50 pages. So there's a fair amount of information that the major cloud players are putting forward and they are having audits performed to prove those controls are in place. I agree with your statement though that the problem is that you have to read the information provided by the cloud provider and understand those controls, including figuring out where your infrastructure and applications end and where theirs begins. That overlap and interplay between the different environments is critically important, especially as you use more and more external partners and cloud providers. You have to really pay attention to this convergence of cyber worlds to make sure you don't get burned.

Rob McCormick: I'd make a relatively technical argument that the more generic the infrastructure, the less secure it is. Amazon does have all that documentation however, they're trying to provide a very flexible, very dynamic infrastructure that anybody can just go use. We think security by design is what's important. You need to think from the bottom up. "What does my business do?" "What do my systems

need?" And, "How do I, from the bottom up, make sure that it's secure for what I need to do?" The generic system can be as secure as they can make it, but it's still a generic system. In which case, they've got to have some openings in there that you wouldn't necessarily want to have. They have to have user-friendly portals that let you go turn things on and off, and create openings. We think, if you're really building an infrastructure for your company alone, there are ways to do that without buying into the big disaggregated companies.

Thomas Hayde: I'd say for a lot of the small, closely-held businesses we deal with, cloud solutions are pretty appealing. It makes it easier for someone to get that consistent security control across the whole system down to the network. But then from the legal perspective, I'm sure your master services agreement has a limitation of liability. They all do. And it's usually defined as a limit on how much you paid us for these services for the past quarter or six months. I think the longest I've seen is two years. And that can sound like a pretty big amount. But people don't realize the potential costs of responding when an incident occurs, and the potential liability to third parties. So you're talking about big first-party costs of bringing in forensics, folks to assess and contain, bringing in the legal services, bringing in notification services that can get pretty expensive. What I've seen is you get anywhere from five to 10,000 records in a population of consumers that are affected by a breach, and you're starting to get pretty sure that just the response costs, not third-party liability, but just your first-party costs are going to exceed six figures easily. So, again, having counsel that can review those contracts for you and determine your level of risk, and then help you go to your broker and figure out what you need in your insurance portfolio, because these are costs that could cripple a lot of these closely-held businesses. So that's another important thing I think for them to be cognizant of. As great of a security that you feel that you're getting through some of these products and doing it the right way, incidents are going to be inevitable. Human error is a factor. I think depending on what survey you look at, in two-thirds of incidents the primary factor is human error. So that's always going to be out there. And so you're going to have to deal with the contingency of, it's inevitable that you'll have to deal with some sort of data breach.

Rob McCormick: The insurance point is a really good one because you're correct in that service providers are not going to take on unlimited liabilities or the price for their service would be something no one could afford. Our typical customer will move their data from servers in a nice IT closet in an office building that may or may not have a janitor with a key to their server closet. We move them into a centralized audited secure physical facility with a lot of really good tools in place to protect their data. They are definitely decreasing their risk, but that does not relieve themof all potential liability. Its still a real good idea to get insurance.

Sekhar Prabhakar: So whenever we get a contract, especially with the DOD, we make sure what our liability limits are to ensure we are covered. I don't want to sign up for something where I have a provider, and he goes like, "OK. We'll pay you $20,000 for an incident," and our client is looking for a much higher coverage. So those kinds of things have to be assessed on a regular basis for every contract. And going back to your point about the insurance and covering those things, everything will be looked at. So if we take the scenario you suggested, that there are going to be increased costs when the breach happens, let's reverse it. Let's engage an attorney before. Let's engage an assessment firm. So that companies are at least aware of the costs and what you can go ahead and take care of in a structured way to minimize those problems and say that if things were to happen, you can at least use that assessment as a baseline to, "For 20 hours, I'm being charged this much." So you have to do the same from a business risk assessment perspective.

Rob McCormick: I like this topic, because I hear it all the time, "Well, you should just take on the liability." So you went from this really insecure thing, right, with huge risk, and I don't have a liability on that. You're going to pay me to improve your risk situation exponentially. And then on top of that, you also want me to move all of your potential liability to me, right? So it's not a rational thing to ask your service provider for. And people should understand that. That's kind of the way that works. Now your contract should have all of the nice SOAs and everything else, but uncapital liability if something ever goes wrong, I always say, "Do you have that today from your one outside IT guy in the closet?" Whatever it is, even if it's a really nice system and you got 10 IT guys. Are those guys liable if they mess up? Do you get to go and extract your $10 million from your five IT guys? And the answer is no, right? So outsourcing shouldn't mean always moving the liability if something bad goes on. You should recognize as partners that if something happens, then there has to be insurance or a plan to cover.

Sekhar Prabhakar: With large cloud providers taking over everything, there's so much data, and you are at a lot more risk. It may be better to go with other providers and spread out the risk. Certain things I may put on cloud provider like Amazon, but certain other things I may put on a local company like Avatara. This can minimize your risk. So in that way, I am going to a provider, I can hold them responsible for a certain SLA and cost associated with certain applications. Risk assessment posture can help with analyzing current and future needs to better plan the security posture and have proper insurance and process to protect yourself.

Rob McCormick: We often times move customers off of big shared email providers when we onboard them. We like the idea of keeping your server data, including mail inside the castle, where we can protect it and care for it. Our customers like calling people they know and trust if/when this ever occurs.