BIRMINGHAM BUSINESS JOURNAL

TABLE of EXPERTS Series

Insights into CYBER SECURITY

Sponsored by:

AUBURN UNIVERSITY

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

TEKLINKS

UAB THE UNIVERSITY OF ALABAMA AT BIRMINGHAM

Warren Averett CPAs AND ADVISORS

The Experts

Ronald L. Burgess, Jr.
Auburn University

Lieutenant General Ronald L. Burgess, Jr. (Ret.) was commissioned in Military Intelligence through the Auburn University ROTC Program in 1974. Burgess earned a Master of Science degree in Education from the University of Southern California in 1980, and a Master of Military Arts and Science from the U.S. Army Command and General Staff College in 1986.
In 2012, Burgess retired from the US Army, as the 17th Director of the Defense Intelligence Agency, and joined Auburn University as Senior Counsel for National Security Programs, Cyber Programs and Military Affairs.
As head of the Defense Intelligence Agency and Acting Principal Deputy Director of National Intelligence, Burgess served as a key player within the national security arena, called upon by the President, the Secretary of Defense, the Director of National Intelligence, the Chairman of the Joint Chiefs of Staff, and Congressional leaders for his opinions, advice and expertise.

Ragib Hasan
UAB

Dr. Ragib Hasan is Assistant Professor in the UAB Department of Computer and Information Sciences, founder of the UAB Secure and Trustworthy Computing Lab, and a faculty affiliate of the Center for Information Assurance and Joint Forensics Research. Dr. Hasan's research interests are computer security, cloud computing security, and digital forensics. He created the notion of "digital data waste" which has been covered by various media outlets including MIT Technology Review and cNET, and his research has been funded by a National Science Foundation CAREER Award; the Department of Homeland Security; Office of Naval Research; Google; and Amazon. He received the 2013 Google RISE Award; the 2014 Best of Blogs and Online Activism Award for Innovation from Deutsche Welle; and the 2013 Information Society Innovation Fund Award for his Shikkhok.com online education platform used by children in South Asia.

David Powell
TekLinks

David Powell is a 17 year veteran of the IT industry, the last 12 spent in Managed and Cloud Services. Named one of the Top 250 People in Managed Services by MSPMentor for four consecutive years, David has worked for three of the top 100 Managed Services Providers. Since coming to TekLinks, he has helped the company become the nationally recognized Managed and Cloud Services practice it is today. David was recognized in 2011 by the Birmingham Business Journal as one of the Top
40 under 40. In 2013, he was recognized by the Birmingham Business Journal in their first ever ranking of the #40toFollow in Birmingham, recognizing David as one of the top 40 people to follow on Twitter.

John Thomas Malatesta, III
Maynard, Cooper and Gale PC

J.T. Malatesta is the chair of the firm's Cybersecurity Practice Group. In an advisory role, Mr. Malatesta counsels organizations on how to prepare for, and respond to, data breaches. This takes many forms, including the development and implementation of incident response plans, the assessment of vendor relationships, and cyber insurance. He also defends companies in regulatory investigations, enforcement actions, and civil litigations stemming from data breaches. Mr. Malatesta has handled a number of data breach investigations and civil actions, particularly in the financial services, health care, and insurance industries. He is a frequent speaker on emerging issues in data breach. He is a member of Infragard, a public-private partnership between the FBI and the business community on cybersecurity, and is a committee member of the Sedona Conference Working Group 11 on Data Security and Privacy Liability, a leading national think-tank on cybersecurity issues.

Cindy Wyatt
Warren Averett, LLC

Cindy Wyatt is a Member of the Firm and the Division Leader of the Firm's Risk Management, Internal Controls & Business Process Consulting Practice. She has over 22 years of operational and consulting experience and has worked with Warren Averett since 2000. During her tenure at Warren Averett, Cindy has assisted clients with cyber security, risk management, internal controls, fraud investigations, workflow and operational assessments, as well as a variety of other business advisory services. Cindy's prior experience includes serving as a division controller for a large thrift institution, as a financial and information systems auditor and consultant with an international accounting firm, and in an executive management position with a credit union.

The Discussion

Q: What are the key ingredients for a cyber-security strategy?

David Powell: When discussing IT strategies with customers, we often look for a good analogy to explain what they should consider, so with cyber security we compare it to securing their house. First, you have to determine what your valuable information is, and who has access to it. That's kind of like asking who has access to your family heirloom or the gun cabinet. Then you should think about the persistent monitoring, or what we equate to your neighborhood watch. You may have an alarm that's going to go off when someone breaks in, but you really need to be more active than that. Paying attention to kids jiggling the door handles on their way home from school, or noticing that unfamiliar van parked across the street. Then you consider the trusted user as a potential risk. Who are you giving access to your home? Who are you letting inside your perimeter? We used to be worried about the guy trying to kick in your door, and now we're a little more concerned about who you're giving trusted rights to. Then you need to train the users, which is like calling the family meeting where everybody sits around the table and talks about what each person needs to be concerned with so that everybody is on the same page. And finally, you've got to report and take action, which is to alert the neighborhood. If your house is broken into, you need to tell all your neighbors.

Ronald L. Burgess, Jr.: You need to look at it holistically in terms of the ways you're going to do it, the means you're going to use to accomplish it and the end state that you're trying to accomplish. We call it the ways-means-and-end discussion. So there has to be a recognition within an organization that whatever you're going to have, cyber security is a 24 by 7 by 365 holistic approach. And it involves every member in the organization, from the CEO on down to the lowest person who has access to any piece and part of your organization. It's everybody's concern. Whatever policies and practices you're going to put in place, they have to be understood and usable and practical. And at the end of the day, they have to be enforced and reinforced across the spectrum of the whole thing. Most organizations will put it off to the people who are responsible for cyber security, but it's really the responsibility of everyone inside that organization. So at some point in time, the strategy has to recognize that it's not a matter of if an event is going to occur, it's when the event is going to occur, and how are you going to address that and be as transparent as you can be? Because in some cases, the industry doesn't want their consumers to know. But you still have to deal with it, and the better informed people are, they better you can deal with it.

Cindy Wyatt: The key ingredient to a cyber-security strategy is to look at what you are trying to protect, how you are protecting it, and who is involved in that protection. People typically do not focus on the "what". You don't need to necessarily protect everything. Focus on what you're trying to protect first and then you can then look at what kind of internal controls you need to put in place, and how are you going to respond on the risk. The best approach to do this is to have a security risk assessment performed to identify your sensitive data as well as potential gaps in your company's data security.

John Thomas ("J.T.") Malatesta, III: The fact that you're even talking about a strategy means you're ahead of the curve, because a lot of companies don't, or only think of it narrowly as an IT issue. I think there's still very much an "ostrich-in-the-sand" mentality when you look at this across a lot of industries. Now with Target, Home Depot and some of the other more noteworthy data breaches that have been reported over the last year highlighting the risk, this issue is now getting escalated within organizations. Companies are asking themselves if they are doing enough. And what would we do if we were hit? So you're getting a lot more dialogue now at the C-suite level about what you need to do to protect your assets. As for a strategy, you need to be mindful of where that personal information resides. And what are we talking about when we say we're protecting assets or information? You can expand the dialogue to look at it more broadly than what the statutes cover. Are we just worried about private, personal information, or are we worried about intellectual property too? C-suite, top-down involvement is critical. You have to have corporate buy-in and make it part of your culture. You have to emphasize this issue, not only in the form of a policy but in terms of implementation. And employee awareness and training are critical factors so that this is something that remains at the forefront of everybody's mind within the organization. For example, when an employee goes into the field, is he or she first asking, "Should I be storing this information locally on my laptop instead of the company server?" That decision exposes the company to heightened risk. If you have training and awareness built into the process, it mitigates the risk of this issue to your company.

Ragib Hasan: There are two major ingredients to a cyber-security strategy. The first one is to be prepared, to anticipate that there will be a problem in the future. And also to educate the employees as well as the customers. Because sometimes businesses prepare the employees well, but the customers are not well informed about the basic ways they can protect themselves. For example, two-factor authentication can easily prevent many of the background hacks that have happened recently. So each business should take a considerable amount of time to prepare and educate the employees about basic security, and educate the customers to some extent. And companies have to accept the fact that security breaches will happen sooner or later, so they have to be prepared. They can start by looking at what assets they have, what vulnerabilities are in their system, and what are the potential entry points into their system that hackers can use. Attacks can come from both outsiders and insiders, so each business should have a communication plan about the known vulnerabilities. But there can be some unknown vulnerabilities that they have not anticipated, so they should have a damage-control plan for handling these things. At the same time, they should also have a public-relations plan. When something bad happens, how are they going to tell their customers?

Q: What are some things businesses often overlook when developing a plan to protect their sensitive data?

Burgess: One of the first things is, when an employee leaves, what kind of access do they still have? Do they still have credentials? And folks who are not part of your organization – contractors or whatever – what access do they have to your system? That's becoming more and more of an issue now in terms of all the different things that are out there on your system. A lot of updates are done remotely, and sometimes you'll have your person pick up the phone and talk to someone who says, "I am now taking control of your computer." Do you know where that person is, and what are all the linkages in between and how secure are those? That's often not thought about. And the other thing is, as you look at your holistic holdings, there is some part that you have identified as the crown jewels. All information is not the same, so what are you doing different to the information that you have determined to be important and strategic?

Wyatt: One of the big things we see is businesses protecting sensitive data they shouldn't even have at all. When you look at the Target breach, they had credit card data that should not have even been in their system. So the first thing is actually identifying the sensitive information and making sure it is something you have to have. We always say to ask

about five times, and if you get to the fifth time and the answer is still that you have to have it, then you probably do. But for the most part – I'd say at least 50 percent of the time – companies can sanitize the data somehow, to get what you absolutely have to protect down to a more manageable level. The other thing is, not just knowing what you have to protect, but where it is. We have a large company we're working with now, and they wanted us to perform a security-risk assessment. We asked, "Over what?" and they said, "We don't know." Well, we started looking at their data, and it's everywhere. It's going out to vendors, it's coming in unsecure. So we had to get our hands around the "what" are we trying to protect, who has access to it, where it resides, how it's being transmitted and who is it being transmitted to? The other big gotcha is people always focus on external risks. They think the bad guy is always outside of their company. But in a lot of cases, the perpetrator is inside. They're not focusing on the internal risks. You can look for personal behaviors, but the best thing is to just limit access. Only give access to people on a need-to-have basis. I walk into some companies and people say, "Oh, we trust everyone." Well, trust is a bad thing on anything cyber. The other thing is you shouldn't look at cyber security as just an IT plan. If executive management is not involved and IT is living on an island, a company is never going to have as effective of a policy. Also, the cyber strategy needs to be updated at least annually. Most people put these plans in place, and they don't update them for several years. Winston Churchill said, "However beautiful a strategy, you occasionally need to look at the results." It's like cleaning out your closet. You need to clean out your closet at least once a year, and you need to really look at your security policy at least once a year.

Burgess: I would highlight the annual piece. NIST (the National Institute of Standards and Technology) has come out with a cyber-framework that lays out a pretty good operating plan for companies to look at, and it recommends an annual review.

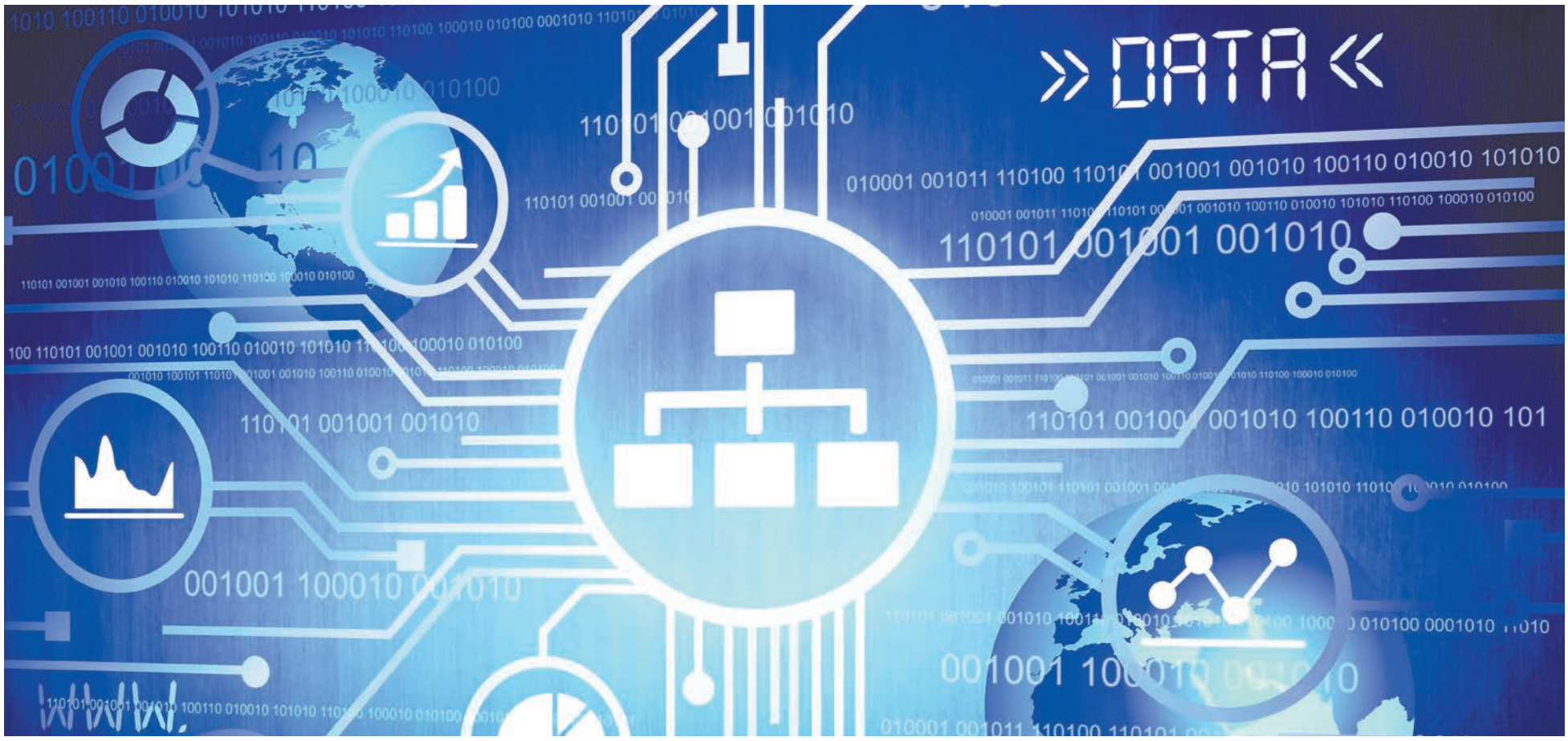
Malatesta: In terms of what things often get overlooked, the thing that came immediately to mind for me was vendors. I think a lot of companies do a good job of making internal assessments. What is our internal risk? How do we control problems within the four corners of our bricks and mortar? Vendors are being used with increasing frequency. From my perspective as a lawyer, companies also need to think through what happens if the breach isn't on their watch. What happens if it's a cloud-based storage company, or a service provider used for processing payment-card information? What obligations are we going to assume if there is a breach at a vendor, and how do we allocate that responsibility between ourselves and the vendor? For example, who carries out the notification obligation? Do our contractual provisions provide protection for us as a company in the event that there is a data breach at our vendor? A lot of times you have traditional language in these form contracts that cover these relationships, but cyber risks now introduce a new set of risks that may not have been squarely addressed with traditional language. You have to make modifications to the contract language to address this particular situation. So don't look only at your own house. You also have to look at what vendors you're using for your business.

Hasan: A big mistake is to have an absolute trust on any part of technology security. For example, businesses often assume that anything sent over SSL (Secure Sockets Layer) is secure, but then the Heartbleed bug came out and businesses learned that they are exposed to a lot of data breaches and data losses. So businesses cannot really depend on any part of technology as a 100 percent guarantee against any hacks. They have to think about a very diverse approach to security. The other thing they overlook is that security is not a technical problem, it's a human problem. We had security problems 2,000 years ago, and we'll still have them 2,000 years from now. So we have to consider people and their behavior. Outsiders and insiders. Do you trust your employees? Do you trust a low-paid operator whose job is to deal with sensitive data? The WikiLeaks case shows that you can't really completely trust everyone. There might be someone in the loop who is either malicious or negligent enough to leak sensitive information. And finally, you also have to consider that these days, information travels a lot. Information is no longer static. You can have a really secure file system, but then if your information is partly stored in a cloud, it has to go through the Internet. And also, a lot of employees bring mobile devices to work and use them to access the company's network, and that might be an entry point. It can expose the company to malicious software, and it's something many people haven't considered. So you have to consider what new developments are out there that can change your whole scenario about protecting sensitive data. You have to consider where your data goes and how it's stored all the time.

Powell: When you fire somebody, it's very likely that you will take their keys and revoke other levels of access. But suppose you fire somebody on a Friday afternoon, but the IT guy had already left earlier to go to Dragon Con, and he can't take the user out of the system until Monday. That's a problem. What we also see as a problem is what they call shadow IT, which is what happens when IT decisions are made by people not in IT. So when the marketing department turns up a WordPress site for something, but you fail to patch or update it regularly, it's a security problem. Or when the sales department has a report they want to make available to everyone, and they ask everyone to install Dropbox on their iPads so they can push all their sales reports to Dropbox. So the two easy ones are: what happens when you fire somebody, and the other is this idea around people who are not in IT making decisions about IT. Because it used to be that the IT department were the people who knew tech. And now a lot of decisions that impact the technology footprint of the company are being made outside of the IT department. There needs to be some reining in. We make a lot of deference to usability instead of acceptable use within the organization.

Q: What are some of the top preventative measures a company can take to reduce the potential of a security breach?

Wyatt: Since we're in football season, it comes back to good old-fashioned blocking and tackling. You need to have good IT policies. Having acceptable-use policies, telling users what they can do. Having user trainer and awareness, letting them know everything that's going on and why they need to be concerned. Anti-virus. When you think of how many breaches come through because of inadequate anti-virus controls, it's crazy. We just had a breach with a company that did not have the anti-virus installed correctly. They had it installed on an individual workstation level instead of a server level. The breach came through the server, attached a key-tracking device, captured banking information, and then the perpetrator was able to enter wire transactions. All because the anti-virus was installed wrong. The other area is your firewall. So many people just set up a firewall and don't restrict it. A firewall is what you make it. Only open up the ports on your firewall that you need. Don't give everyone access to everything. I know that's frustrating to the users, but it's a lot more secure for the company. I'm going to keep stressing, this is not an IT issue. This is a management issue. At the more secure companies, it's a culture. Management is involved, the board knows, people are asking questions. It's not just us dealing with the IT guy. If IT doesn't get support, you're going to have more breaches. So I stress that management has to be involved.



Malatesta: You want to minimize the number of locations where you have this information stored. In addition, encryption is a relatively low-cost measure to enhance the protection of data. Multi-factor authentication is another example of a good security measure. And then employee awareness, employee awareness, employee awareness.

Hasan: One of the issues that hasn't been discussed is the importance of having strong passwords. Because in most cases, companies will leave the default passwords on their routers. These days, even if you have an eight-character password with uppercase and lowercase letters, that's easy to beat. The hackers have become sophisticated. They use new techniques for launching a brute-force attack. They have dictionary-based attacks. And also they are sometimes using the cloud to make attacks faster. So it's really important to have a strong and secure password, with different combinations of things to make it hard to guess. Upper and lower case, symbols, and no dictionary words. You shouldn't have the word "password" or something that's easy to guess.

Malatesta: You'd be shocked at how many people use that as their password.

Hasan: A lot of people have passwords that are 123456, or abcdef. So you have to make the employees aware that they have to use strong passwords. The recommendation these days is to change your password every 90 days, and maybe more often for critical systems. Also, you should never use the same password in multiple sites. Especially, you should never reuse your bank or other financial institution passwords in any other sites.

Burgess: Right now I have four pages of different passwords. Yes, I go to the extreme. There are password generators that you can plug in your password and it will tell you whether it's weak, moderate or strong. The strong is probably anywhere from 15 to 18 characters and runs the whole gamut. How often do you change them? Do you use the same password for your system at work as your banking account? We're human. We use derivatives. We might change a letter here and there. You have to think about that. And where do you store those passwords? I have mine on one thumb drive that stays with me. I keep it locked up. Look at how you do this to protect yourself.

Hasan: You also need to consider where your data flows. Are you using a cloud, either directly or indirectly? The recent iCloud hack showed that when people are taking pictures on their iPhones, behind the scenes the iPhone was making backups of everything on the phone in the cloud. So even though you might not think your data is going outside your company, it might be because of some design flaw. So think about where your data is actually going, and is there any way that someone can access that data outside your company?

Powell: What you see sometimes is a company's compliance department wielding this big stick trying to club the user community into submission to do it a certain way so they can check a box on the audit framework, rather than making acceptable use a part of the culture and convincing the user community that this is a good idea, that it's something you should want to do. It's like a budget. You can either live by a budget, or you can fabricate all this documentation to convince the accountant that you live by a budget. You're much better off to have it permeate the culture and be something that you prescribe to daily, and then it yields those results, instead of something that people are forced into complying to so that the auditor can check a box. You have to have this culture that wants to drive towards that, where everyone's pulling in that same direction and understands what it means to the organization and what the inherent risk is – as opposed to "I have to do this, otherwise I get reamed out by the compliance department." So the culture piece is what I'd really stress.

Burgess: I know of some very large companies in this nation that set the tone at their board meeting every quarter. The first briefing given is the cyber brief by the IT folks. It sets a tone for where they're going in terms of that. I come from a community where we had the biggest secrets in the United States. And as I would look my people in the eye, I believe in trust. My people had a lot of stuff they had to undergo. Polygraphs, background checks. But I also come from the community that says trust but verify. So there's nothing wrong with putting a keystroke logger on your system. Where are your people going? Why are they plugging a thumb drive into their operating system? Do you have rules on that? As for the background checks, I don't think you have to go real deep, but what do you really know about your people? What is their basic financial situation? Whatever you put into place can't be pencil-whipped. You really have to have a culture where you're executing this stuff. How often do you bring in an external third-party to come in and take a look at your company? Everybody is in the room together and they see the same things and they're comfortable with it. You have to have that disenfranchised eye look at you once in a while to see what you might have missed. At the end of the day it starts at the top. Set a culture that you're serious about this, and then go with it.

"So even though you might not think your data is going outside your company, it might be because of some design flaw."

- Ragib Hasan

Malatesta: There are some good public materials out there to give you some guidance on how to think through this issue. For example, the FTC has issued a guide for businesses on ways they can mitigate these risks. FACTA, the Fair and Accurate Credit Transactions Act, identifies 26 red flags that companies need to be thinking about. It's something an unregulated company also can look to as persuasive guidance to make sure they're thinking through these issues correctly.

Q: Are the majority of breaches external or internal? What are the percentages?

Burgess: I would probably put it around 75 percent external, including the vendors, and 25 percent internal. But insider concern – especially with intellectual property and hard data – is a big deal. And 25 may be lowballing it.

Malatesta: I think the insider threat is higher. I think it's more like 60-40.

Hasan: According to CERT (Computer Emergency Response Teams), internal breaches are not only very common, but they found 67 percent of the surveyed respondents think they are much costlier than an external breach.

Powell: I've read that the top two risks are physical security – people just coming in and walking off with something – and number two is trusted user.

Wyatt: With regulated industries like the health-care industry, about one-half of the breaches come from vendors. Think about that.

Powell: That's because there is a hole in the EMR (Electronic Medical Record), or something to that effect.

Wyatt: There's a hole somewhere in it, or with the way they got access.

Burgess: If you look at the Target breach and the one that just hit Home Depot, it was an external vendor who actually opened the door and let someone do something. I can give you any number that you want to hear, but I'm not sure the numbers are really good here. The bottom line is it's an issue and it's an area that a lot of businesses don't pay as much attention to. Because everybody reads that it's the criminal gangs that are trying to hack them.

Malatesta: A lot of people think of this narrowly, as a cyber threat by a computer hacker. But a lot of the exposure is simple things, like an employee losing a laptop.

Q: What options are available for companies looking to prevent data breaches and ensure the security of their information?

Hasan: It's really important to have an external audit of your system. Because when you are designing a security system it's easy to overlook an obvious vulnerability. The thumb drive example is a good one. Some researchers conducted an experiment where they left thumb drives containing malware near a company's parking lot and they checked how many employees picked one up and then plugged it into their company network. And they found that a lot of people actually do that. So you have to think about the whole security process, and it's important to have a third party come in and take a look at your system.

Powell: I think we're going to have to move past passwords to the widespread adoption of two-factor authentication. We work with RSA, which is a token generator. It generates a random number, and there's an algorithm on the other side measuring against that. It is a really effective way to drive security while still maintaining usability. It uses a key fob that goes on your key chain – with the reasoning that most people have their keys with them at all times, or close to that. There are some measures like that you can take. Ultimately we need to have a better way of doing it now, while recognizing that

we're still humans and we're not going to jump through massive hoops. We can try to make it a little bit easier for users, but I think you're going to see a strong trajectory toward two-factor authentication in the next couple of years as we realize that passwords are inherently flawed. And some of the security questions that come behind them if you don't remember your passwords are just as bad. I think in some of the breaches recently involving the celebrities, the hackers were able to get on iCloud and answer the security questions based on what they found on the celebrity's Wikipedia page. So you can certainly bypass those types of security measures. That's an area where there's going to be an opportunity for careful policy-making to make a huge impact. And the technology is available now, it's just not yet widely adopted.

Burgess: Some people believe that in two to three years, we won't even be using passwords. We'll be moving to biometrics, whether it be a retinal or whatever. Where it's going or how fast is hard to say. Change in this country is evolutionary as opposed to revolutionary. It will take some massive event before people really wake up to some things. So we'll see where it moves. Going back to the phones, we have them coming out our ears now. Just the android malware since 2011 has increased by over 500 percent. It's everywhere. So what in a company doesn't need to be connected? If it doesn't need to be connected, then don't connect it. Because everything doesn't need to be connected. What is the critical information? I'll use the old intel-community term, need-to-know. Does everybody in the company need to have access to everything, and how do you minimize access to some of the information? Not just intellectual property, but does everybody really need all the banking information and everything else, just because they can?

Wyatt: The best place to start is to perform a security risk assessment. That's the most efficient approach. A risk assessment demystifies a company's cyber-security response. It helps identify threats and evaluate the current internal control environment. Then you can come up with actionable items for the vulnerabilities you need to work on immediately. Because without that, you're kind of just throwing darts at the dart board. We definitely recommend having an independent party look at it. The problem is you can't see yourself independently. It's why Tiger Woods pays somebody just to watch him swing, and then adjusts from that. All the great baseball players do the same thing. IT people who design a system are not the best for auditing the system. You truly do need an independent review. It's going to bring a fresh perspective.

Q: What are some best practices to help monitor for and identify breaches?

Hasan: The first place to start is to look at the system and then monitor and log everything. Also, have an easy way to process the log. Because sometimes you have so much data coming in, it's difficult for humans to make sense of that. So it's important to have a good log-on tool that will monitor everything that's happening to your system and send out red flags to IT or other personnel whenever something happens. Then you also have to monitor the traffic. Where is it coming from? Some companies have a lot of traffic coming in from Europe or China, where they might not have good security. So you have to monitor the network and all the activity that your system has. You have to monitor the location of your data really well. Does the data live in your company or does it go inside to the cloud? Wherever your data is going, is that secure, and how do I identify any breaches? If somebody loses your data, are they going to tell you? You have to make sure that whatever vendor is using your data, they will tell you about any breaches that might happen. Because sometimes a lot of these cloud vendors lose data but they never tell the customer. So you have to worry about that. And then the employees' devices. It goes back to what we were saying about the need to know. In computer science we call it the principle of least privilege. Don't give anyone any privilege that they don't need to have. Also, the mobile device culture is everywhere. So we now have to think about whether you are going to allow people to bring in their personal devices and attach them to the company network, and allow them to transmit any data to their personal devices. Because that might be a big security hole when it comes to data breaches.

Powell: Large banks have the staff to perform those types of functions. UAB has the staff. But if you're an orthopedic surgery practice and you have HIPAA requirements, you don't have a robust IT staff to do all those things. What we recommend a lot is finding a security firm that can work with them. We work with a company called Alert Logic. One of the things in most compliance standards is capture-and-log review. There are a lot of people who capture their logs, but it's never at the top of anybody's priority to list to review the logs. So Alert Logic comes in, and we work with this security-operations team who will analyze your logs while proactively monitoring the hacker message boards. So when you're in that middle market and smaller, you really need to find a partner to perform that function. Because it's a lot to expect that the orthopedic practice with their one IT guy can do all those functions. So recognize that the scope is broad, and the compliance risk keeps moving downstream. It used to be that the small drycleaner didn't have compliance concerns, but now the drycleaner who has a point-of-sale system has some risk. They need to have vigilance around that, but they also need to recognize what they can't do themselves. That doesn't mean it doesn't get done. It means they need to find somebody to do that function for them.

Burgess: First of all is the recognition that you have to have a way to monitor whatever it is. The question is, where do you start paying attention to how you're going to monitor this? Do you do it at the firewall, which is where most people go, or do you kick it even farther out to the Internet rung? How far out can you go, and then work your way back in. Because the more opportunity you have to identify the threat, the better chance you have to either stop or mitigate it in a timely manner. The other thing is, inside a company, the IT folks have to be completely connected in terms of understanding the business from a grassroots level. Because as they are monitoring for the company, what you're really trying to pick up are anomalies. You're not picking up the normal stuff. You're trying to have either a system or people that can identify the one-off where you say, "What happened here? What's going on? Should I dig deeper?" Anomaly detection is a big deal in this.

Wyatt: Everybody is going to have a breach. I've read studies that say 100 percent of companies will

have a breach within the next five years.

Burgess: It's kind of become an accepted part of the lexicon. It's going to happen.

Hasan: It's not just companies but also individuals. Sooner or later your personal data will get breached. You think your personal data is in the phone, but in reality it's in the cloud. So as soon as the cloud gets breached, your personal data will get breached, too.

Wyatt: So yes, you need to work on preventing the breach, but I think companies have even more exposure by not monitoring it for early detection. Because more damage is going to occur the longer the breach goes on undetected. Like with Target, it was almost a month after the breach before they detected it. The smaller and mid-size companies definitely aren't doing enough. The larger companies ask, "What should we be monitoring?" We always say firewall activity, network traffic, anti-virus logs, user activity, and unusual file extensions. That can catch a lot. On your data base files, has anything changed beyond what you were expecting? Has anybody copied a large amount of data? Most companies do not look at these like they should, and those things are going to catch and limit the exposure of a breach. So while you can't get 100 percent preventative, you can detect early and stop and mitigate it.

Malatesta: What I do as a lawyer is advise companies on what their requirements are. Some companies are surprised to know that there is a regulatory framework out there that mandates that they undertake risk assessments, or intrusion detection, etc. So my role is more of making them aware of those types of obligations, and then flagging the types of practices that commonly results in some type of legal inquiry.

Q: We're hearing a lot about the cloud. How does that fit into security?

Powell: What we frequently see is customers going to the cloud because of security and not in spite of it. Fish swim in schools to protect themselves from sharks. So when you look at the SMB (small to medium business) space, the idea that they can secure themselves effectively against all the things we've talked about, that's very daunting. By going to the cloud and subscribing to compliance to a large degree, or by coming into our place, they can subscribe to a certain level of that. Granted, we still need them to enforce strong passwords on their user community and things like that. But there is a certain aspect of compliance that they can achieve by going to the cloud. If I walked down to the bank on the corner and said, "I'm here from IT. Can you show me where the server room is," they'd probably walk me right back there and not challenge me. So going to the cloud overcomes the physical piece. What's really reset the parameters of how people, and particularly larger companies, view the cloud is that the CIA just went with Amazon. It's a $600-million deal. Now, it's an Amazon-hosted private cloud in a CIA-owned facility. But the number of people who are going in that direction and the balance of risk – where you don't own all the risk and someone else is kind of owning the risk around that – that's very compelling for a lot of businesses. So even the enterprise space is very much embracing the cloud. It gives them capabilities and a subscription to a portion of compliance that would be very difficult for them to do themselves.

Hasan: My main research area is on cloud computing and my lab (UAB SECRETLab) analyzes the security and privacy of clouds. One of the things companies should also remember is the cloud is not a silver bullet to solve all the problems. It will provide small and medium businesses with some protection. But clouds also come with other new traits that people might not have considered. A cloud is like a motel. You can get a room, but some other guys who you don't trust could get a room next to yours. Whenever you send your data to a cloud, you have to consider the threat that comes from co-tenancy. Because the cloud is a shared resource, a lot of people share the same computer storage systems. That comes with other risks of data breaches, or information being leaked through the cloud. But cloud is definitely the future in terms of the cost savings and other features. But you shouldn't think that just by sending off your data to a cloud that it's secure against everything. Even the most famous clouds like Amazon and Microsoft are not 100 percent secure. They provide a lot of security features, but you still have to look at other issues. Like availability, which is often the most overlooked part of security. If you outsource your data to a cloud, will your business be stable if the cloud goes down? So you have to think about the trade-offs when you are using the cloud.

Q: What are the key components to be included in a breach/incident response plan?

Powell: What you don't want is the "do-anything" response, where you just throw a whole bunch of stuff up and hope that it does something. Because then you have the law of unintended consequences. You're not documenting those changes, and you're not considering what's impacted over here or over there. When you find something that needs to be addressed, you have to run it through the whole process, so you don't create a hole over there because you patched this one over here, or so you don't decrease usability and the user community freaks out. You really have to look at the holistic context of how does this flow in the whole process. But you get the sense sometimes that when security breaches happen, that people think there's this room with a whole bunch of knobs and levers, and you just start switching them hoping that one will stem the tide. It really has to be much more prescriptive than that. You have to be cool under fire and run it through your process, and trust that the process you have in place will yield the results you want instead of a willy-nilly approach to things.

"Some people believe that in two to three years, we won't even be using passwords. We'll be moving to biometrics, whether it be a retinal or whatever."

– David Powell

Burgess: This is a company problem, not an IT problem. So whether it's your CIO or CISO or whoever, that person is part of the key management team, and it becomes a company problem. So you have to have a plan that you're going to put in place. But as we say in the military, no plan survives first contact. Once you come in contact with the enemy – or in this case, the problem – you're going to have to start adjusting on the fly. It's just the way it works, because nothing ever unrolls exactly like you think it will. Then you have to start preserving everything, because that's how you're going to go about your risk mitigations once you start looking at the root-cause analysis. You have to have a process that you go through to start closing the door. Then what are you going to do to reestablish what you had going on? One of the phone calls that needs to happen reasonably early is to law enforcement. You're not a singleton in this, and we have some capability inside our FBI and some local law enforcement. The sooner you bring someone in, the sooner you can start dealing with the situation. That makes some people very nervous, because you have stock holders and everything else. But this starts putting you at risk when other data is out there.

Malatesta: We do advise a number of companies on the preparation of an incident-response plan, and the first question we ask is, what's the regulatory framework in which you operate? What sector are you in? Bank, health care, education? You have to understand that backdrop, because there is a defined statutory framework that governs some of the obligations in the event of a reportable breach. The second thing is ascertaining what your incident-response plan addresses. What's the underlying information? Does the plan cover any company data, or is it more limited to just non-public personal information. So you have to define what type of breach triggers this internal response procedure. All of this is going to run through information security. Your employees need to know who they should call if they have a suspected breach. That's part of employee training, and it's really the only thing that about 95 percent of your company employees need to understand. Then there has to be a defined policy procedure for management to follow once that gets reported. Schools go through fire drills. They have a defined process to follow. Companies need to be prepared to do the same thing. But a lot of times it takes a scare before they get prepared.

The next issue is, what are your escalation principles? Who gets involved? We typically use the terminology "incident response team." You have to have a multi-disciplinary approach within the organization. So that's going to typically involve information security, risk management, legal and probably some level of compliance. When you suspect there may be a data breach, there is a defined set of questions that need to be answered. For example, do you notify your cyber insurance carrier? Who will perform the investigation? Do you have an affirmative obligation to notify your customers, and if not, should you anyway as a gesture of good will? What is the right message, and how are you going to get it out there? As you can see, there are a lot of tentacles to incident response, and that's why planning is so important. So you want to have that plan – I call it a playbook – that you can pull off the shelf, and you basically have your game plan to follow. So it's not an ad-hoc response. It's a disciplined, measured response, and everybody knows what their role is.

Hasan: Most states mandate what you have to do in case of a data breach, but Alabama does not.

Malatesta: There are 47 states that have data-breach notification laws, but Alabama is one of the three that doesn't. But it's the place of residency of the impacted consumer that triggers the law. Even if you're an Alabama business, if you have information on a Georgia resident, that Georgia law governs your obligations. So you need to be aware of your company's footprint.

Hasan: Many of these laws require that you notify the customer. You can't really hide the breach.

Wyatt: One of the key things when developing an incident response is deciding what a breach is. A lot of our clients will categorize breaches, say it's a level one breach, a level two, etc. That really helps with the escalation process. Communication is key. We had a situation where a breach happened, and the IT guy tried to manage it himself. They didn't have an incident-response policy. And talk about snowballing. It went bad real quick. It could have been better managed when he identified it, but several months went by before he communicated it. So make sure you have the right people involved. Make sure the board or the business owners are read into the situation.

Q: Considering the cost of cyber security, if everybody is going to be breached eventually then what is the catalyst for me to really do anything differently from what I'm currently doing?

Burgess: I've read that among Fortune 500

companies, anywhere from 30 to 80 percent of the company's net worth – their bottom line – is actually in their intellectual property. It's not in the infrastructure and other stuff. So if we lose anywhere from $250 billion to $1 trillion from hacking and stuff disappearing – that was the number that was put out in the Symantec Study – should that cause us concern as a nation from a security standpoint? Last year the GDP of the United States was about $15.4 trillion. So if one-fifteenth of our national wealth went out the side door, that's an issue for us as a nation and we better pay attention. Closer to home, the FBI tells us that in 2011 we lost $12.5 billion to cyber crime. In 2012 that number went up to $14 billion. And a lot of companies don't report, so the actual number is somewhere north of that. Those are not inconsequential numbers. So strictly from a threat standpoint, the real question is can you afford not to pay attention to it?

Wyatt: I have several clients who have said "If Target can't protect their system with all their resources, why should I even bother"? That's like saying if I can't protect my house from every single burglar, then why should I even lock my doors? There are basic preventative things you can do that do not get into high cost, like password security controls and firewalls. Not doing anything is going to be far more costly in the long run. With data security, the old adage "an ounce of prevention is worth a pound of cure" definitely holds true.

Malatesta: Some companies don't have a choice. If you're a financial institution or in the health care industry, you don't have to be a large-scale company to fall subject to the obligations of certain statutes. You have an affirmative obligation under the law to be prepared, even though it can be a somewhat expensive undertaking. But there are also a number of small fixes that you can make that significantly mitigate your risk levels. So we're not talking about tens of thousands of dollars. You can take some low-cost initiatives to reduce your exposure, and those are well worth it. All companies are in the business of establishing trust with their customers. Consumers nowadays have an expectation that if they turn over personal information, then you're going to take care of it. Once you have an incident, you have to restore that trust.

Hasan: With the Internet and everything being connected, the attack surface of any business has increased a lot. And also, there are many more attackers. Your computer system is connected to the whole world. In the past you'd have maybe 10 local criminals who would break into houses. Now there are millions of people all around the world trying to break into your system. So if you don't take the very basic counter measures, then you'll become a hot target that attracts all these people. By taking a few easy and cheap counter measures – a strong password, firewall, anti-virus updates – you can prevent more than 80 percent of these attacks.

Powell: Sometimes fear demotivates. Small incremental changes are ultimately what we need. And it has to start at the top with the business owner. You don't have to be an expert on security, just like you don't have to be an expert on the tax code. But you need to be aware of the things you should be concerned about. The business owner needs to talk to his IT staff and say, "I recognize this is important, I recognize that I'm not an expert, and I don't expect you to be one. But we need to create a plan to make us better." And then once you execute all those things, start over and do a new set of things to make you better. It's that continual process of improvement. The first place to start is to walk around the office, and if somebody has a password written on a sticky note, change that. Do you have an acceptable-use policy? How are people using mobile devices? There are little things that business owners can just kind of eyeball and see that they are risks. Just the awareness that it needs to be done, and then bring in the experts to help you advance the ball.

Q: Any final thoughts?

Burgess: We're doing this discussion on 9/11. I think it's appropriate to remember that. We have a lot of critical infrastructure in this country, and businesses play into that, whether it be banking, transportation, electrical, agriculture. There are some nation states that want to do harm to this country. There are criminal organizations, terrorist organizations. It is appropriate to remember in this cyber space we all exist in that bad things can happen if we don't do the right things.

Wyatt: Cyber security can be very daunting to small and mid-size companies. I want to stress the performance of a risk assessment. It is the easiest way to get a picture of all your key vulnerabilities. Then you can start working on a plan. It's the monsters in the dark that you can't see that are going to get you, not the ones you do see. So it helps to turn on the light so you can at least know what your exposure is. The knowledge that comes from a risk assessment is definitely powerful.

Malatesta: I think "daunting" is the right word. A lot of people have the approach that this is a tremendous obligation that they're being told they have to undertake. I don't necessarily think that's the case. You can get intimidated because there's a lot of tech talk involved. But there's a recognition that in this day and age, this is going to impact every single business. For decades, locking your doors when you went home at the end of the day was a part of doing business. Now you have to do the same thing in the electronic environment. There's a checklist of about 30 practices or so that you can look at and say, "Are we addressing these concerns?" That's going to eliminate the supermajority of the risks, and most are relatively inexpensive fixes.

Hasan: As I said earlier, security is not completely a technical problem, it's a human problem. When business owners are considering the security of their system, they have to consider humans in the loop. So any security plans should involve how the customers and the employees behave.

Powell: The business owner five years ago was probably intimidated by technology to a large degree. But in the last five years, it's gotten so good that it's taken a lot of the technology out of technology. When you buy an iPhone, it doesn't come with a manual. So business owners today use technology a lot more, and they may actually feel more comfortable. It's not necessarily a technological solution as much as it is a cultural process. The business owner should be able to get behind processing culture and getting with the experts and finding an answer to a problem more so than going back into the server room and letting the IT guy talk all kinds of jargon to him. Business owners just have to take that first step and start working towards getting better than they are today.