TABLE OF EXPERTS

CYBERSECURITY

SPONSORED BY

Offit | Kurman
Attorneys At Law

SC&H GROUP

UMUC
University of Maryland
University College

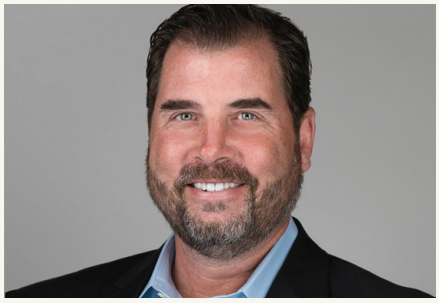
MEET THE EXPERTS

The Baltimore Business Journal held a round-table discussion on November 3, 2017, featuring a panel of three cybersecurity advisors who discussed the importance of adequate cybersecurity measures, and the top cyber risks that companies face.

DR. EMMA GARRISON-ALEXANDER, D.M.

Vice Dean,
Cybersecurity Graduate Program
University of Maryland University College

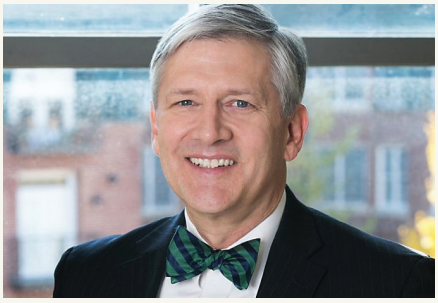
Prior to joining UMUC, Garrison-Alexander served as the assistant administrator for Information Technology (IT) and chief information officer (CIO) for the Transportation Security Administration (TSA) under the Department of Homeland Security (DHS). There, she led TSA's IT organization with an annual budget responsibility of $450 million and supported 60,000 employees. Before joining TSA, Garrison-Alexander served for 25 years with the National Security Agency where she was part of the Defense Intelligence Senior Executive Service. She holds a BS in Electrical Engineering, an MS in Telecommunications Management and a Doctor of Management in Technology and Information Systems.



JEFF BATHURST

Director Technology Advisory Services,
SC&H Group

Jeff Bathurst directs SC&H's Technology Advisory Services practice, helping clients strengthen their technology strategy and execution, specifically in the areas of technology leadership, enterprise applications, cybersecurity and infrastructure and cloud. Bathurst is a firm believer that if organizations want to be successful, they must leverage technology in the most opportunistic way. It starts with having a conversation about business value and goals, and then determining how technology fits into each organization's critical path to success. With more than 25 years of technology experience, his clients have included middle- and large-market clients from various industries. A long-time senior technology executive, Bathurst specializes in partnering with business leaders to define a company's current and future technology needs, understand security implications, evaluate technology options, and develop and implement enterprise-wide strategic solutions.



DAVID GREBER

Principal
Offit Kurman
Attorneys at Law

David S. Greber, Esq., practices with the law firm of Offit Kurman, P.A., which has offices in Baltimore and 3 other locations in Maryland. Mr. Greber is a member of the International Association of Privacy Professionals (IAPP), the largest and most comprehensive global information privacy community. The IAPP developed and launched the only globally-recognized credentialing programs in information privacy. Mr. Greber holds the CIPP/US certification (Certified Information Privacy Professional / US concentration). He advises clients on how to comply with federal and state privacy laws governing the collection, use, retention, disclosure, and destruction of personal information from customers.

With recent breaches by Yahoo and Equifax all over the news, why are adequate cybersecurity measures not more of a priority among companies?

Jeff: I think they are a priority. The more you see this in the media, the more it becomes top of mind for many firms. One of the biggest issues organizations are facing is that they THOUGHT they were addressing it. They are seeing the latest levels of breaches occurring on routine basis, and rethinking their effort and contemplating, "Are we as prepared as we thought we were?" They're having to revise their cybersecurity strategies and operations.

Many companies are at this point of self-reflection, determining if they are doing everything necessary to appropriately protect their important assets. In the past, organizations treated cybersecurity as a "one and done" type of activity. In reality, it must be woven into the corporate culture involving every employee. I think that's how we will see meaningful progress made with organizations.

Dr. Emma: Having sat in that executive seat or senior executive seat with responsibilities within the cybersecurity domain, I have a perspective to share. Part of the issue regarding cyber is that executives have competing priorities. There are many areas that need to be addressed from a business perspective, however many executives have not made the connection between cybersecurity and their organization's bottom line. And in some cases, these competing priorities come down to a lack of funding. If you spend money on cybersecurity, then those funds aren't available to develop a new product or service.

Coming up with cybersecurity solutions for a government or industry or nonprofit organization is very complex because the core infrastructure where cyber takes place is within the information technology (IT) domain. And we rely heavily on technologies, such as computer software, applications, and mobile devices. As these technologies converge, the problem becomes extremely complex.

David: I think the smaller the company, the more the factors that Jeff and Dr. Emma mentioned come into play. I think it comes down to education, dread, and resources. Education in the sense that many companies are aware that there is hacking going on in the marketplace and that they might have an obligation to do something about it. But the topic is overwhelming, and money and resources have to be committed to analyze it, so dread takes over. Rather than take steps to do what they can do to address the risks, they sort of take an ostrich approach and hope that it will all go away.

Resources, of course are an important factor. Many companies are struggling just to do the basic operations of business and anything that doesn't bring revenue directly into the company becomes less of a priority because they're trying to survive and keep the lights on, so for small companies it becomes a real problem. But every company can and has to try to do something reasonable to address the problem.

What are the first steps a business should take to establish a cybersecurity program?

Jeff: There are three basic components: technology, training and the definition of "valuable" information. A business has to define

what assets need to be protected. In many cases, organizations take this we're going to have to secure everything approach. Instead, identify the valuable information and establish the protection of that information as the core of their cybersecurity actions. Cybersecurity education, as Dave pointed out, is a continuous process. It has to be indoctrinated into employee on boarding, ongoing employee training and operational processes. It is something that needs to be ingrained as part of every employee's professional development. A cybersecurity program was/is seen as a technology thing. Even though that's where a lot of it resides, it's a business operations thing.

Dr. Emma: Businesses can start with an organizational risk management strategy. The National Institutes of Standards and Technology (NIST) put together what they call the "Risk Management Framework" that has to be implemented across the federal government. But that framework has value to the private sector, too, because businesses can't prevent every cyber attack from happening. At some point in time a business will have a breach and will have to manage risk, and that's what the NIST framework does.

The NIST framework provides a process for managing risk that includes: categorization of information systems, selection of security controls, implementation of security controls, assessment of security controls, authorization of information systems, and monitoring of security controls. A business can use–and then assess–those controls to determine whether they are working as expected. Then the business can authorize its systems to operate because they've been put through this process.

Then, we're not only going to do continuous monitoring, but we're also going to perform diagnostics to look for problem areas and put in security controls on the fly to mitigate some of problems that are occurring in the network.

CYBERSECURITY

The Baltimore-Washington region is among the top cybersecurity hubs in the US. The skilled technical workforce in the region ranks among the most concentrated in the country and nationally-ranked local colleges and universities continue to stock a talented pipeline of cybersecurity talent.

- Maryland is home to over 10,000 cybersecurity contractors
- The Federal Government expects to spend over $40 billion on non-military IT in 2013
- 8 Greater Baltimore colleges and universities are recognized as NSA Information Assurance Centers of Excellence
- Maryland has over 19,000 job openings in cybersecurity, more than anywhere else in the country
- Baltimore-Washington is #1 in the US for percent of the population with bachelor's or master's degrees
- Baltimore-Washington is home to over 200,000 Cybersecurity professionals, with over 75,000 in Greater Baltimore/Central Maryland

David: I think the first step that businesses should take is to designate someone in the business who is responsible for data security and privacy-related questions, and identify a team within the business who represent the constituencies within the business that need to be around the table to discuss what should be done. Second is the education piece to find a path forward for an analysis of what should be done. I completely agree with Dr. Emma's reference to the NIST framework, which was the result of an extensive effort and study to identify business best practices for the benefit of those who are facing these daunting challenges. The NIST Cybersecurity Framework is available at www.nist.gov/framework.

There are some data security control measures out there that can be a beginning checklist for businesses to consider as they evaluate cybersecurity. The Center for Internet Security, which is a nonprofit organization, has published a series of 20 data security controls, which are in order of priority and are public. They can be found at www.cisecurity.org.

From a legal standpoint, the standards take into account the extent of resources a company has. A small company doing the best it can with minimal financial resources is not going to be treated the same way as a large company that can devote extensive resources to those same issues. But no company can think that they can sit and do nothing and comply with legal standards.

What are the top cyber risks that companies face?

Jeff: It normally starts at data protection. Depending on the industry, there could be personal health related information (PHI), personal identity information (PII) and/or intellectual property. Outside of data, there is the potential reputational/headline risk caused by a security breach. Lastly, there are operational risks within IT as well as other business activity. Within IT operations, they must be sound processes and procedures to collect

Left to right: Jeff Bathurst, Dr. Emma Garrison-Alexander, David Greber

BY DANIELLE FRATER

cybersecurity information and update all potentially affected systems. Within business activities, procedures are required to ensure monetary resources and sensitive information are not shared/released without proper authorization and validation

Dr. Emma: Certainly, a data breach that exposes critical business or government information is a big risk, but denial-of-service attacks are possible also. And one risk that sometimes gets overlooked by the public is the insider threat. For example, an individual with access to information and the right knowledge, who might have an employment issue, can do a lot of damage in terms of taking a system down or exposing and organization to malware (malicious software).

Complacency is another threat. Many of the incidents that have taken place recently resulted from a lack of patch management, which is a basic function of cybersecurity. The US Computer Emergency Readiness Team (CERT) under the Department of Homeland Security regularly publishes summaries of high-impact security incidents on its open website and has patch management information available for businesses and government to use. But patch management for an organization isn't free and can require a substantial amount of resources.

David: In addition to what Jeff and Dr. Emma have mentioned, I think one of the greatest risks for companies is in the nature of what's called social engineering. Phishing

emails that contain attachments that include malware that will give someone a gateway into an organization. These phishing attacks can be launched on multiple people within the same organization and you only need one of them to take the bait. The way to address that vulnerability is through internal education and administrative controls.

Jeff: One final point I want to make is that everything centers around people. People are one of the biggest risks to any organization because that's the wildcard. You can put the best control frameworks in place, you can put the best technology in place, but if people don't follow their training, that's really the biggest concern for a lot of companies.

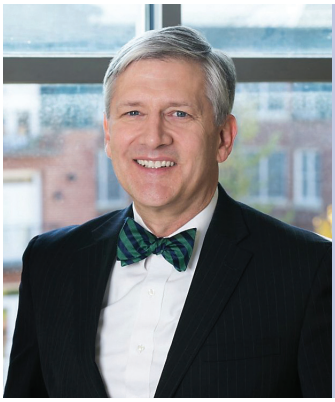
Are companies legally required to take cybersecurity measures?

Jeff: Yes, in a lot of cases it's becoming much more so. The most recent requirement is for companies doing business with the Department of Defense (DoD) where there's now a security framework and measures that they must implement by the end of this year – otherwise, they won't be doing business with the DoD. There is the well-established SOX compliance for all publicly-traded firms, FINRA compliance and SEC compliance. At this point, most of the industries have a cyber requirement. I expect more legal cybersecurity requirements as we move forward.

Dr. Emma: The laws on the books require certain actions regarding cybersecurity. For example, laws dictate that federal agencies follow certain rules. They must follow the Federal Information Security Management Act (FISMA), the NIST risk management framework as well as educational standards that are put forth by the National Initiative on Cyber Education, also known as NICE.

The TSA already had been following a number of cybersecurity best practices before they were passed as government-wide regulations over the past few years. For example, all of the TSA's applicable contracts contained a clause dealing with cybersecurity or IT security that companies had to meet. So, organizations are legally bound in different ways, and it's not always because of a specific law but can be a part of contractual agreements.

David: There's a patchwork of laws throughout the United States that apply to this. Not only the federal laws, but also state laws. The laws sometimes focus on individual sectors and sometimes not. For example, the Federal Trade Commission, which is one of the leading enforcers of cybersecurity and privacy law, enforces Section 5 of the Federal Trade Commission Act, which says that companies are prohibited from engaging in unfair or deceptive trade practices. It's a very



"Greater legal obligations and higher risks of cybersecurity intrusion create a greater exposure to economic and reputational liability."

DAVID GREBER
Principal
Offit Kurman Attorneys at Law

old law that they have used to enforce these measures. Taking adequate data security precautions is one of those things that is required.

With respect to state law, Maryland has a specific commercial law statute obligating companies to take reasonable security measures with respect to their data.

Rather than try and ascertain whether somehow a company fits in some narrow exception where they may be exempt from explicitly being required to comply with data privacy or data security laws, a company should assume that the answer to the question is yes, it is required to take cybersecurity measures.

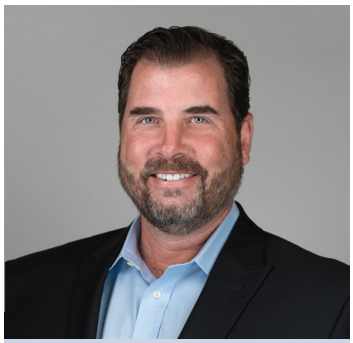
How has the Internet of Things (IOT) changed the cybersecurity landscape?

Jeff: It has created a whole new host of attack vectors. IOT is essentially digitizing analog objects; machinery, living spaces, clothing, furniture, etc. The Internet of Things is based on the ability to perform one of following measurements – temperature, proximity, pressure, water quality, chemical/smoke/gas presence, level and infrared using sensor technology and embedding these sensors into products.

If an object is digitized, meaning it operates on 0s and 1s – it can be compromised. That is creating a lot of consternation for technologists. This current technology wave is similar to when mobile technology hit the market. Before mobile technology, everyone came to work, they did their work on the computers, and they went home. With mobile technology, people were given the ability to access corporate information anytime, anywhere from a mobile, thus greatly expanding the amount of possible points of compromise and unauthorized data access.

IoT is a very promising technology and it has many potential use cases. It can monitor personal health, improve safety for the elderly, measure environments, automate data collection in manufacturing environments, and so on. The fundament concern is if it has an ability to collect data and transmit that information, then it has the potential to be compromised.

With this many access points into a company's technology infrastructure, it's nearly impossible to try and secure every device. These devices ultimately send data to a central repository and that's where I think organizations need to start... protecting the data repository. Many technologists debate whether to focus a cybersecurity program based on outside looking in, starting at the end points, or at the center where the data resides and looking outward.



"Cybersecurity isn't one-and-done. It must be woven into the corporate culture."

JEFF BATHURST
Director Technology Advisory Services, SC&H Group

Dr. Emma: The Internet of Things basically penetrates every domain out there. Anything that has an IP address can in some way get on the Internet, and IoT devices really were not designed to be secure. In some cases, it's very difficult to apply our current security approaches to IoT environments because our approaches were not designed for them. For instance, some devices are low power, low speed, so you can't run encryption on them. If you do, the device either will be unusable or too expensive.

When it comes to IoT, we need to revisit how some of our security controls and approaches apply. And that conversation needs to be about what exactly we want–or need– to protect. Right now, we see a tug of war between convenience and capabilities. How do we balance those two things? At home, consumers use their devices freely, and they want that same freedom when they enter the workplace. Trying to separate the two is very difficult for companies. How do we come up with a security framework that will be appropriate for the IoT environment? That's the challenge!

David: I have a privacy concern also about the way in which the Internet of Things is causing data to be gathered about individuals, without them really fully appreciating that the data is being gathered, used, and potentially disclosed to third parties. This summer I heard a story that illustrates that point. I just want to read two sentences out of this news report about Roomba vacuum cleaners: "Over the past couple of years, Roombas haven't just been picking up dust and chauffeuring cats around, they've also been mapping the layout of your home. Now Colin Angle, the chief executive officer of Roomba, maker of iRobot®, has said he wants to share the data from these maps in order to improve the future of smart home technology."

I have two kids who have Roombas in their apartments and I thought to myself, "What exactly have they been gathering out of this private space of my kids' apartments and how in the world can this company share this data with others?" The gathering in the first place is objectionable to me, but the sharing of it makes it even worse. The maker of Roomba has assured consumers that it will get consent in order to share this data, but I'm just concerned that that consent may be buried in a long privacy notice that nobody reads.

How do you see the security landscape changing over the next 12 months as it relates to your industry?

Dr. Emma: UMUC has been a leader in cybersecurity education for a while. We were one of the first institutions to offer full degree programs and certificates in cybersecurity starting back in 2010 when there were very few others out there. What we have seen over the years, and it continues to occur, is that more and more educational institutions are getting into the game and they have started to offer cybersecurity programs as well.

I think one part of all that activity is about meeting the needs of the student population that says, "I want to be part of the cyber fight. I want to help my company. I want to help my government, my nation from a security perspective."

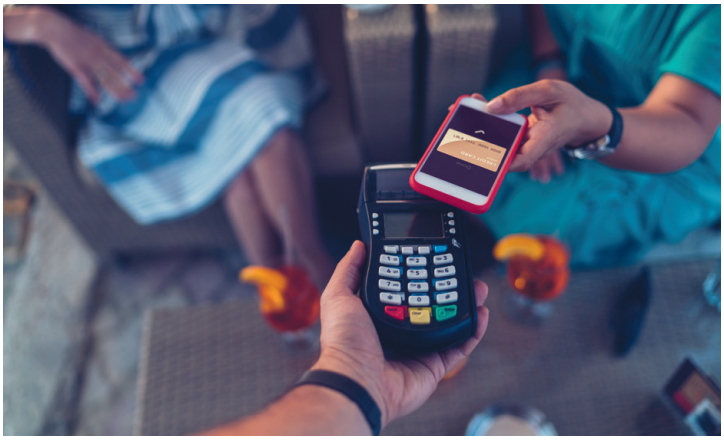
But I think the other part is that employers are looking for employees with the right skill set and knowledge base to help secure their companies. So, I expect the number of cybersecurity programs to increase as the need for a well-trained cyber workforce continues to grow.

David: Within the law industry, I think that in the next 12 months, and in the near future, there are going to be a growing number of security attacks and privacy breaches that will cause legislatures to adopt increasingly more stringent regulations on what cybersecurity steps businesses must take and what privacy-related steps businesses must take. I think as a result of that, there's going to be increasing pressure on businesses to do something to respond and that will put a premium on consultants like Jeff and educators like Dr. Emma and lawyers like me to help these businesses comply with the rising level of legal expectation.

Jeff: SC&H Group is a management consulting and CPA firm. Currently, we have cybersecurity requirements due to private and/or confidential client information as well as business operations. I think the cybersecurity and legal requirements as well as the security frameworks are going to become more stringent as we move forward.

In our technology advisory consultancy, one of the challenges that we regularly discuss with clients deals with cybersecurity and the lack of available talent to help organizations with cybersecurity needs. Our practice helps organizations establish their cybersecurity program, framework and to recommend technologies. However, they still need technically proficient individuals to support the cybersecurity program, its technologies and the results.

Unfortunately, I feel cybersecurity is going to be a never-ending treadmill. Threats will come and go as new technology comes to market. Continuing education and staying on top of things is really the message to send to organizations – don't go to sleep at the wheel.



GETTY IMAGES

Regularly communicate cyber-related information, train employees on a consistent basis and review internal procedures involving sensitive information. Everyone in the organization needs to be indoctrinated as part of a cyber-aware culture. Cybersecurity needs to be listed as a mission-critical organizational objective.

To what extent are emerging legal standards for data protection and increased regulation impacting the business community?

David: I think that greater legal obligations and higher risks of cybersecurity intrusion create a greater exposure to economic and reputational liability. I also think that there is a perception that the federal government is stepping back from regulation generally, which would potentially include privacy regulation. But the states will likely fill the regulatory void. What we're going to see is that state legislatures are going to consider giving consumers the right to sue directly for breaches of cybersecurity and privacy law standards, whereas, now there are only limited rights for consumers to sue.

Mostly, the current legal threat is through regulatory enforcement, such as through an FTC action.

Dr. Emma: I think that cybersecurity legislation, the congress' ability to pass legislation, will continue to be very difficult. President Trump issued an executive order back in May around cybersecurity, which to my mind reiterated things that we were already doing, which I think is a good thing. But it's been a very difficult place legally, congressionally, to be able to put out enforceable, binding, cybersecurity legislation.

Jeff: One of the things that we are spending a lot of time talking to companies about is cyber insurance. Cyber insurance issuers and consumers are having a hard time quantifying organizational risk. How much coverage and what type of coverage should we get? While it is a legal issue, it is also liability issue. Organizations need to incorporate cyber insurance as part of their overall insurance portfolio for their business operations – that's our recommendation.

There are local firms that are active in the cyber insurance space. It is quickly becoming a standard insurance product. To obtain cyber insurance, a company must be able to quantify their risk and that is a challenge for many companies. Companies need a clear understanding of their computing environment, the sensitive data that resides on it and their areas of vulnerability in order to obtain cyber insurance.

"It's been a very difficult place legally, congressionally, to be able to put out enforceable, binding, cybersecurity legislation."

DR. EMMA GARRISON-ALEXANDER, D.M.
Vice Dean, Cybersecurity Graduate Program University of Maryland University College

As security needs grow, the skills gap is becoming more of an issue in cybersecurity. What must be done to fill the gap?

Dr. Emma: Educate, educate, and educate some more. I think also, we need to look to institutions of higher education that can assist employers and employees in getting the skills and knowledge they need to go into the workforce and really make an impact. And it's important to look at the transferable skills that people have, so that with some additional education and training they can move into the cybersecurity field. That's part of how our programs are designed at UMUC – they help people move from one career field into the cybersecurity career field.

One thing we do at UMUC is view cybersecurity holistically. For example, we offer a cybersecurity management and policy program because we recognize that cybersecurity is not just a technology problem. Technology people don't get together and work on a problem in isolation and then hand it over to policy, then legal, and then human resources. They must come together as a group to work on the problem and iron out a solution.

So, we need to understand from an education and training perspective that everyone in an organization requires training, and not just the technical IT staff. Within the education domain, we must make sure that cybersecurity education is part of the HR degree, part of the accounting degree, because interdisciplinary and multi-disciplinary approaches are necessary to fill the skills gap and meet the workforce needs.

Jeff: For me, the education is going to happen in a multitude of ways – apprenticeships, partnerships and continuing education. Apprenticeship programs are big in other countries and there is a significant movement in our country. Apprenticeships would help get the needed professionals to market by partnering these programs with organizations – government and private – to invest in training individuals in cybersecurity disciplines.

There is also a continuing educational component. As I mentioned before, training your employees on a consistent basis, changing their computing behavior, and making these processes part of the overall daily operations of a firm is important – it builds the brain's "muscle memory".

Lastly, we should look to partnerships with service organizations. There are companies providing cybersecurity monitoring and technical services. These firms can help organizations – who can't acquire the required talent – select, implement and operate the necessary security tools and services.

David: I would add that what has to happen is the quality and availability of practical public information on cybersecurity and privacy needs to improve. There are already some excellent resources. The resources available at www.ftc.gov, the Federal Trade Commission's website, include a number of accessible, digestible videos and other information that can help a company to get up to speed. The NIST site (www.nist.gov) has the framework and other information available. But still, I think greater efforts need to be made to consolidate these resources into bodies of knowledge that can be accessed in one central location in a way that does not totally overwhelm companies, particularly small business owners, as they try and get up to speed in privacy and cybersecurity law.

Dr. Emma: I would just add the following to the sites that you mentioned, the Department of Homeland Security US-CERT and ICS-CERT, which have great information for businesses as well as the general public. Both provide instructions regarding patches and other cyber solutions once they become available. And because the Internet of Things continues to affect more and more areas of our lives, it's becoming more important to assess and update our security controls –even in our homes–if we really want to rid ourselves of all those vulnerabilities.

GETTY IMAGES