FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE

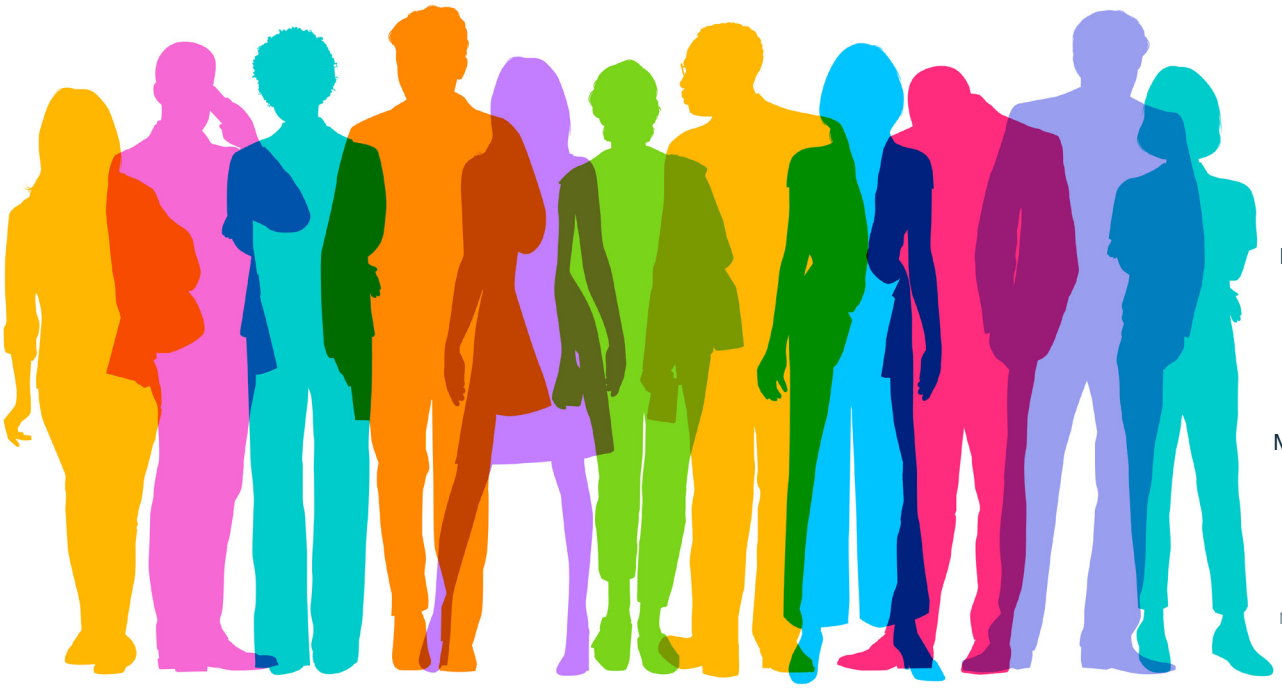
MARCH 2019

HOTTEST CISO TRENDS OF 2019

KLOGIXSECURITY.COM
617.731.2314

K logix

TABLE OF CONTENTS



Magazine Contributors:

Kevin West
CEO, K logix

Katie Haug
Director of Marketing, K logix

Kevin Pouche
COO, K logix

Marcela Lima
Marketing Coordinator, K logix

Contact Us:

marketing@klogixsecurity.com

617.731.2314

LETTER FROM

KEVIN WEST

CEO

KICKING OFF THE YEAR WITH TRENDS

We kicked off the year by collecting strategic trends from our CISO community. On a consistent basis we collect trends throughout the year, but during the RSA conference each year, we sit down with CISOs in back-to-back interviews to ask them the same set of questions in order to collect trends, publish them in this magazine, and impact our service offerings.

This year at the RSA conference, we sat down with almost 20 security leaders, including CISOs, CIOs, cyber lawyers, security researchers, and many others to gain a wide range of opinions on a variety of crucial cyber security topics.

WHY WE DO THIS

There are two reasons we collect trends on a regular basis. First, the goal of starting our magazine was to provide a platform to CISOs and other security leaders to share their stories. When we started the magazine five years ago, CISOs were rarely interviewed or profiled. We felt we needed to hear from these security leaders to help others in our industry who were looking for insight into their goals and challenges. Since we couldn't find this data in the market, we decided to fill this gap by reaching out to these security leaders to feature them in Feats of Strength.

The second reason we collect trends is to shape, validate, and influence our information security consulting services. We extract trends that directly impact our K logix methodologies and service offerings. This ensures what we offer to our customers is a direct reflection of the challenges and goals of CISOs. We're always absorbing these trends we collect to help validate, mature, and pivot our business to the place information security leaders are going; not where they've been.

2019 CISO TRENDS

In our Q&A article starting on page 6, we go deep into the responses from CISOs we interviewed at the RSA conference, and I wanted to share a few of the top trends and high-level findings from our analysis:

The clutter of technology is overwhelming. Across the board, CISOs believe there are no silver bullets, and the overwhelming amount of security companies add more work to their plates in order to filter through the noise.

We listened and our Project Advisory service helps clear the clutter by helping identify and prioritize business and technical outcomes that need to be achieved in order to remediate key risks and advance security programs. Our approach is not focused on market hype, but on our clients desired outcomes, security maturity, and operational capabilities. Our results save your team valuable time and provide a justified business decision.

Security is a business problem. Many CISOs believe they've finally made it to the boardroom in a meaningful way, have established strong alliances with other business leaders, and are respected within their organizations. However, many CISOs may be asking themselves 'now what?', because they are not armed with the right approach or knowledge to make the biggest impact.

As an organization, we strongly support CISOs engaging with business counterparts and the board, and all of our services enable this, especially our Actionable Risk Assessment. This holistic service helps CISOs understand their security baseline in business language that can be easily communicated to their executives. It also provides justification for decisions and makes the best use of your team's time and resources.

LEARN MORE

We would love to share all of our trends in more detail with you, our readers, through our Trends Presentation. This presentation covers 5+ years of CISO and security leader trends and correlates them to our service offerings. We are actively sharing the latest version with many CISOs, so please reach out to us if you would like to see our Trends Presentation.

If you want to reach me, you can email me at kwest@klogixsecurity.com, or check out more CISO profiles at www.klogixsecurity.com/feats-of-strength

KEVIN WEST is the founder and CEO of K logix, a leading information security company based in Brookline, MA. K logix helps create confident information security programs that align with business objectives.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JEREMY WALCZAK
CISO, CATHOLIC HEALTH

HEADQUARTERS: Buffalo, NY

EMPLOYEES: 9,000+

ANNUAL REVENUE: $1.1 Billion

Jeremy Walczak, currently the CISO of Catholic Health, exemplifies a security leader with a unique, business-oriented background. Walczak studied Marketing at the University of Buffalo, and through a recommendation from a friend, he also completed his Management in Information Systems degree.

When discussing his undergraduate degree background in Marketing and Management of Information Systems, Walczak says, "I find these degrees to be very valuable in the sense that it helps with communicating, relating, and selling IT and information security needs to others in the business."

After spending several years living and working in Dayton, Ohio for NCR Corporation where he obtained his M.B.A. from The University of Dayton, Walczak returned to Western New York and worked at Delaware North, a global food service and hospitality company, where he had his first exposure to working in information security. He says, "It was more of a compliance focus at the time in the sense that we were marching toward adhering to PCI guidelines. Those were our drivers, but that's how I first got into a formal information security role and started branching away from traditional IT. It is not because I necessarily chose this path, it was more making myself available and relying on the skillsets I had developed earlier on to point me in this direction."

After moving on to Independent Health, a health plan and services organization, Walczak spent the next eight years working his way up from Security Architect, to Director of Information Risk, to eventually becoming their Chief Information Security Officer. During his time at Independent Health, Walczak strategically established a link between the work his team did from an information security perspective to ensuring they comprehensively enabled customer trust. He comments, "That was our value proposition, to enable customer trust. It was the strategic angle about making our consumers feel comfortable working with us. And the moment we break that trust is when there are dire consequences or events that may potentially lead to more costly healthcare."

Early on in his career, Walczak was told by a former business mentor to find a way to get out of IT in order to leverage more of his business skills. In his role at Independent Health, he had the opportunity to interact with other business leaders to a greater extent because his role was not as heavily focused on the management of technology. He grew in terms of understanding how the business operated, what the business needs were, and then translating this back into technology or security solutions. The heavy focus was more on risk management, something Walczak regards as a formative transition in his career.

BUDGET, PRIORITIZATION, AND ALIGNMENT

Walczak has almost one year under his belt as the CISO of

Jeremy Walczak's Thoughts on IoT

"I think IoT is interesting. I look at medical devices as our IoT here, in the sense that we have our traditional server farm, we have our workstation, we have our WiFi, but then you've got this whole other area of connected wired and wireless medical devices that are out in our facilities, and it's something that you have to be very careful and deliberate when you go out and attempt to affect these devices from a security perspective. The last thing you want to do is interrupt operations or services at a critical point of care. That's a whole area of risk that can go well beyond traditional infosec risk as it also can have a significant operational risk. How do we manage that smoothly? It brings in a whole other subset of leaders within the organization, which is new for me when you compare it back to my time in manufacturing, travel & entertainment, or health insurance."

Catholic Health, a comprehensive healthcare system based in Buffalo, New York. Walczak viewed the role as an opportunity to join a larger organization with more responsibility. He explains, "Fortunately, I stepped into an area and to a company that had already accomplished a great deal in terms of the security program. However, there's certainly a lot left to do, whether it's standing up new capabilities and technologies or continuing to mature what we have in place today. So, I'm excited to do that. For me, it was time for that new opportunity."

Before joining Catholic Health, Walczak ensured he would receive sufficient budget, be aligned with the prioritization process, and have strong alignment to other leaders. To kick start the inherited program and maintain a strong security standing, he chose to focus on a few key, high-level priorities. He says, "What I found to be successful in the past, is coming into the year with three high priority things that I'm expecting to get done. I'll always have three, four, or five other scenarios or solutions thought through in my back pocket because what I've found is depending on what external events or circumstances unfold throughout the year, I may be presented with other opportunities to react with dollars that were not previously budgeted to solve an emerging threat."

THE KEYS TO BUSINESS ALIGNMENT

To ensure strong alignment with other executives, Walczak believes in finding ways to become indispensable to an organization. He does this through being willing to help business leaders solve challenges and offer a helping hand to those in need. He comments, "I try to find out how I can help. Something I picked up early on in my career is figuring out how to become indispensable by being willing to jump in and work to solve other people's issues. It might be working with the CIO on a key technical challenge, or it could be helping to push basic process improvements that have been waiting to be completed for some time." Walczak tackles challenges such as this by understanding if there are any security barriers inhibiting this, or if there is anything that can be done from a security perspective in order to overcome the other person's challenge.

By approaching board alignment in this same manner, Walczak believes CISOs may become more valuable through building strong trust, and focusing on continued engagement and communication. He explains, "There is a difference between management and oversight. I truly believe that executive leadership has a responsibility and accountability to manage day-to-day operations. However, you must find the right level and the right type of detail to ensure your board is appropriately and reasonably informed of the issues you are managing. And you've got to find the right balance. You need to do your job as a manager, but then the board also has to do their job and ensure they've been properly informed and can validate the decisions that you have made. I try to do that through risk indicators, performance indicators, as well as the right type of dashboarding, so to speak."

MAPPING BACK TO STRATEGIC GOALS

Walczak leads his security program with the core strategic value of continuing to map and mature to their adopted framework and ensuring all information security objectives map back to Catholic Health's strategic goals. He believes everything his team does, no matter the project scope, must tie back and support the organization's end goals.

In order to continue to accomplish this goal, Walczak must overcome challenges related to funding, prioritization, and entrenched business processes. He discusses why prioritization and entrenched business processes pose unique challenges to his strategic goals and growth. He says, "Group think can be dangerous. It can maintain certain entrenched customs that may not add value and it's those customs that you're now competing with for dollars and resources. This is where a good risk management process can come into play to help bring visibility to an organization's evolving risks and lead to improved allocation of resources and funding. This is important because you can't boil the ocean."

He continues, "For prioritization, that's where a couple of things can come into play. It is where your risk assessment process and mapping to a framework and then building out a maturity model are important. So, if I'm the lowest level on my maturity model and I know through whatever risk assessment I'm doing, it points out that "XYZ" is a significant issue, you can then begin to have a more data driven discussion around highest risk and prioritization of effort. It also comes down to what's tolerable from an organizational perspective. How much change can I inflict in one fell swoop or in one calendar year to move the needle for the organization."

TOP CISO TRENDS

We interviewed **16 CISOs and security leaders** to learn about their top goals, challenges, strategies, and so much more.

ANDREW BJERKEN,
Global CISO and Privacy Officer, Catalina

ROLAND CLOUTIER,
CSO, ADP

ALAN DAINES,
CISO, FactSet

ADAM FLETCHER,
CISO, Blackstone

SUMMER FOWLER,
CISO, Argo AI

EMILY HEATH,
CISO, United Airlines

THOMAS MURPHY,
CISO, Northwestern University

DR. MICHAEL MYLREA
Sr. Advisor, Cyber Security, Pacific Northwest National Laboratory

GOPAL PADINJARUVEETIL
CISO, Auto Club Group

CHRISTOPHER PAINTER,
Former Coordinator for Cyber Issues, US State Department

SHAWN RILEY,
CIO, State of North Dakota

ROB SLOAN,
Research Director WSJ Pro, Dow Jones

LANCE SPITZNER,
Director, SANS Institute

BRANDON SWAFFORD,
CISO, Webster Bank

EVAN WHEELER,
CISO, Financial Engines

BRANDEN WILLIAMS,
Director, LATAM/Canada BISO, Union Bank

This month, we interviewed, polled, and surveyed many CISOs and security leaders to better understand cyber security trends and the direction our industry is headed. The main focus of our research was done through interviews at the RSA conference in March, where we spoke with many CISOs attending the conference. We also surveyed seven members of our advisory board along with other CISOs who were not able to attend the conference, yet still wanted to help contribute to our trends.

A GLIMPSE INTO WHAT WE LEARNED:

- CISOs are exhausted by the inundation of security messaging from a cluttered and confusing security company marketspace. They have reached their breaking point in terms of seeing too many vendors on the conference expo floor and receiving countless emails and calls from companies touting similar messaging.
- CISOs are focusing on the human aspect of cyber security more than ever. 99.5% of breaches happen because of some aspect of 'touch' with a human, demonstrating how easy it is to hack a human.
- Most CISOs agreed that they are in a place where they have board access, executive visibility, and strong leadership roles, however many aren't sure they are making the most of their newfound roles.

There are countless more trends we learned, and in the next pages, we include the questions we asked followed by a variety of answers from our CISO interviews.

What are the top trends from the RSA conference this year?

ALAN DAINES: We're striving to finally recognize that nobody has a silver bullet. Instead we're coming to an understanding of what our biggest risks are, what are our most high value assets, and how we are focusing on those to buy down the risks we're accepting with our respective companies. Because for the first time at the conference, it felt like we are acknowledging the state of affairs. I don't know if I've ever felt that in past years. It's more honest. I used to come back frustrated from RSA, just more of the same, so many vendors promising to fix the world.

ANDREW BJERKEN: The California Consumer Privacy Act is a big trend I'm learning and hearing about.

Risk is another big trend I'm hearing about around how you set up a good risk program and profile. The last thing of interest is the CISO bootcamp. They go over how to build a program, it culminates with a tabletop exercise; every CISO should go through a tabletop before they have to go through the real deal.

BRANDON SWAFFORD: The trend here is that there seems to be more vendors than there are customers. There are vendors out there trying to capture customers, yet people don't understand the problem that is being solved. The large amount of new vendors creates a lot of confusion for customers as it becomes hard to choose and understand whether they have actual experience and are reliable.

I think authentication is probably the biggest wave, also consolidation. And then you have attack simulations and continuous risk assessment stuff. Those are the ones that I think have the most long term legs because they fill a known gap to reduce complexity, increase efficiency, and introduce new knowledge. I see malware, AI, and blockchain in my view as well.

CHRISTOPHER PAINTER: There is a huge amount of discussion around AI. AI has become such a buzz word that I don't think any two people you talk to will tell you the same definition of what AI is or what its implications are. I think we're still in relatively early days, both in terms of the benefits and the challenges of AI.

EMILY HEATH: I am so thrilled first and foremost to see RSA including women and talking about diversity, which is super important to me and it seemed to be a bit of a theme this year. The other thing I'm hearing about a lot more is the IoT space and third-party security. That's an interesting space for me because it's one of my priorities right now. Also, it's a fairly new field, which I don't think there's a great solution for yet.

EVAN WHEELER: The thing that struck me most is that we're starting to see a critical mass of people looking at more modern risk assessment methodologies, getting away from the heat maps and the qualitative, and being more data driven, more quantitative, more models and things like that. Also, CCPA and the privacy laws, and the pros and cons of what a federal privacy law might look like. There's a lot of speculation and interpretation of what CCPA really means. I think those privacy topics have been dominating conversations over the last year.

GOPAL PADINJARUVEETIL: Tony Sager Chief Evangelist for The Center for Internet Security, Inc. and retired NSA official, spoke here at RSA in 2014 and said we have a problem in cyber security called the "Fog of More." We see lots of new exciting technologies coming in, trying to solve many cyber problems. The reality is there's actually no silver bullet, yet.

One of my talking points at the conference is around the concept of the human element in cyber security. If you look at the data from all the past breaches, 99.5% of attacks that have happened have touch with the human. 91% of all the breaches had to do with either social engineering or phishing. It's really easy to hack a human because we, by nature, are

good. Understanding the human nature, human motivation, human behavior is key to solving this problem.

LANCE SPITZNER: A big one I'm starting to see is senior level leadership beginning to understand that security is not just an IT problem, it's also about business issues, soft skills issues, and human issues. We're starting to see the CISO not as an IT person managing an IT problem, but the whole business. It's less about technology and more about managing risk, and you can see it as more CISOs are reporting to the top.

ROB SLOAN: There is a continued skepticism about the extent to which cyber security vendors are actually helping fix problems. A walk among the 800 exhibitors at RSA induced sensory overload, but did not provide assurances that vendors have real answers.

Even among cyber security industry CEOs, I repeatedly heard that many 'solutions' are just not working, and that is not good enough. The industry needs to get better at calling out companies that fail to deliver on their promises. We simply cannot afford to waste our time and money on products that do not work.

Of the hundreds of cyber security startups, many appear to only provide a solution to a niche problem – they are features rather than fully-formed products – built to attract venture funding and be sold. Very few cyber security startups have the potential to stand on their own two legs in the longer term, though it may take a funding crunch to highlight that.

SUMMER FOWLER: There are two main areas of interest for me. One is in cloud security. We depend heavily on cloud services. That's something from a security standpoint that I'm really trying to learn more about and how we can lead in this space.

And the other is cyber security metrics. I'm passionate about metrics, I love metrics and how can I ensure that I'm measuring the right things at Argo to make sure that we're on track to meet our goals?

THOMAS MURPHY: I'm hearing a lot about the California Consumer Privacy Act. As a CISO, I'm more of a risk manager. There are security implications driven by privacy laws, like exactly what data we collect that's governed by new regulations and what are our obligations to provide logging, disclosures, and opt-out capabilities.

Some of the larger scale enterprise things I'm looking at during the conference are managed and unmanaged device visibility. We're on a path to increasing visibility from edge to end point, to help respond when bad things happen. We're moving down a path towards a platform that will increase that visibility.

ROLAND CLOUTIER: There's finally some focus on scoping down. So instead of 'we can do everything and solve everything and your infrastructure is safe', it's a little more specific and there's a little bit of hope that the market is finally turning in a direction that makes sense.

The other area is around the realistic user automation around risk. The problem is it takes an army to really go through it. It's objective for the most part. And you see companies taking the information, automating, and helping provide it in a way that's meaningful and useful, in a facilitated manner. You get real-time good use out of the information.

ADAM FLETCHER: The most interesting thing I heard yesterday was that Identity and Access Management is a top priority for CISOs by a big margin, even though it's as fundamental as fundamental gets. Specifically, I heard that 26% of CISOs surveyed said IAM was the biggest slice of their 2018 budgets and 37% of the same CISOs said that IAM would be the biggest slice of their 2019 budgets. What I found interesting is that although we are inundated with buzzword technologies that are going to transform the way we do security like Zero Trust and AI SOC, a foundational control like Identity and Access Management is still top of the list.

What are three characteristics you possess as a CISO that make you effective at your job?

ANDREW BJERKEN: I'm a good listener. I say that because honestly, I listen to what my business has to say and where they're trying to go. I'm also approachable. My default stance is yes how can we help. As opposed to no, you can't do it. Then the last thing I'd say is I'm transparent. I believe that transparency is vital to ensure alignment. It also encourages the business to be transparent as well.

BRANDEN WILLIAMS: One of the most important characteristics

ANDREW BJERKEN, Global CISO and Privacy Officer, Catalina
ROLAND CLOUTIER, CSO, ADP
ALAN DAINES, CISO, FactSet
ADAM FLETCHER, CISO, Blackstone
SUMMER FOWLER, CISO, Argo AI
EMILY HEATH, CISO, United Airlines
TOM MURPHY, CISO, Northwestern University
DR. MICHAEL MYLREA, Sr. Advisor, Cyber Security, Pacific Northwest Nat'l. Lab.

is being business savvy. All my training and education is on the business side, and my technical knowledge is hands on. I think security people have a mindset of distrust that they can apply in a lot of places, but if you don't understand the function of the business and how you fit into it and how you enable it, it's very much pushing a big rock up a hill. Technical is great too, but now we're getting into unicorn territory because somebody who's business savvy and super technical is a little more rare.

DR. MICHAEL MYLREA: CISOs need an enterprise vision and strategy that is flexible and evolves rapidly with the complex, dynamic and evolving cyber threats targeting organizations. This requires a deep understanding of both value creation and value destruction. CISOs' understanding of the former is key to aligning, balancing, and optimizing business and cyber security goals which is essential in any resource constrained environment. Understanding value destruction is about thinking like a hacker, knowing your organizations critical cyber assets, networks, and systems that need to be protected. When you have that dynamic understanding of an organization's business operations as well as the economic consequences of the threat it helps quantify potential cyber risk and make strategic investments to buy down that risk.

Number one is identifying what's their return on investment. If you're an organization that's not in the cyber security business, where is your return on investment for investing in cyber security? Most of the time when you make those investments, you now understand that you're exposed, but you don't necessarily buy down risk. So that's a huge problem.

ROB SLOAN: Curious minds, strong communication skills and the desire to continually improve security. I think very few people would get to be CISO if they didn't have curious mindsets, but communication skills do not always come so naturally: being able to stop thinking about the technology and the detail, and clearly communicate what the security program looks like at a high level in business risk terms is difficult for many CISOs, but critical for success. Last, a focus on continual improvement is required because there are always attackers determined to compromise networks.

CISOs also need to think beyond their job and what they contribute to the security community and think how they work to make the whole herd stronger.

SUMMER FOWLER: First and foremost, it's being able to think about strategy. I hear all the time that we must educate the board, and we have to make the board smarter about security. My challenge to my CISO colleagues is that we actually need to make ourselves smarter. We must educate ourselves on the business, what is happening in the business, and what is our organization's strategy.

Communication isn't always the strong suit of engineers and technical folks, but in this role you have to communicate, you have to communicate internally, externally, you have to communicate with executives at numbers of companies.

SHAWN RILEY: The CISO must possess some of the very same characteristics that I possess as a CIO. You have to be adaptable and open to any possibility of any sort of change. You must be able to overcome and evolve in any situation you're in very quickly, because the reality is that our threats constantly evolve and constantly change.

On top of that, you must be a communicator. If you can't communicate to your executive team, you're not getting anywhere. You have to be able to tell them really what's going on, on a constant basis and be able to translate that into language they can touch and feel, the real language wherever that business leader or executive leader comes from.

THOMAS MURPHY: First, is that ability to take those security constructs, maybe it's a technical conversation or a theoretical one, and translate to language that's meaningful for different

GOPAL PADINJARUVEETIL, CISO, Auto Club Group
CHRISTOPHER PAINTER, Former Coordinator for Cyber Issues, US State Dept.
SHAWN RILEY, CIO, State of North Dakota
ROB SLOAN, Research Director WSJ Pro, Dow Jones
LANCE SPITZNER, Director, SANS Institute
BRANDON SWAFFORD, CISO, Webster Bank
EVAN WHEELER, CISO, Financial Engines
BRANDEN WILLIAMS, Director, LATAM/Canada BISO, Union Bank

constituents. So plain English versions of security terms when I speak with our community.

Second, I align myself with the community and put a face to cyber security. Anybody can sit behind a policy and shoot out an email that says, "Effective Thursday you'll have to do this to use VPN", for example. Meeting in person, or having already met someone, helps when new policies or procedures go into effect.

Thirdly, I rely on the strength of the team supporting me, because I couldn't be any of these things if I didn't have qualified, competent people looking at data and responding to reports of suspected incidents.

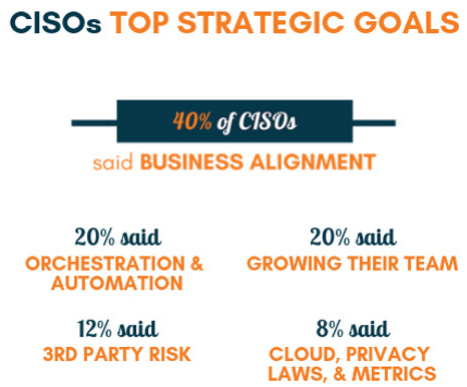
ROLAND CLOUTIER: I think one of them is the willingness to learn. Second, is execution. This job is an operations role. Whether you call it strategic or policy or whatever, you better be able to execute and you better be able to do things fast because in this world, you are the 911 of your company. Third is my focus on people. I've got an organization of a few hundred people that perform important functions across the globe on a daily basis for the millions of people on our platform.

What are your top strategic information security goals for 2019?

ADAM FLETCHER: The first, not surprisingly, is enhancing our ability to secure the cloud, whether that's Software as a Service or Infrastructure as a Service.

The second is building and integrating automation and orchestration capabilities into Identity and Access Management. When it comes to automating and orchestrating identity and access, i.e. provisioning and deprovisioning, we are investing more time and energy because it fundamentally reduces risk and creates a better user experience.

BRANDEN WILLIAMS: For financial sectors in general, there's a desire to find better ways to work with third parties. Safer ways to work with third parties to where we could have data exchange in a safe and secure way and try to create value on both sides of that equation. Also, I think moving to a more flexible cloud-based infrastructure is something that is important because it's difficult to change that paradigm and get people who are looking at technology to look at it differently.



EMILY HEATH: I've been doing this for two years since I've been at United and to understand the landscape is still a number one goal for me. If you don't understand what you've got, you don't know if it's vulnerable, and you don't know if it's been exploited. So, it's a focus for me always. I never want to become complacent. We have to keep evolving because technology is not stopping anytime soon.

Also, we're focused on building talent pipelines. At United, we've grown a lot in the last couple of years. We continue to grow and build our talent for the future technologies that we're going to need to support because we want to solve tomorrow's problems, not just today's.

EVAN WHEELER: Targeted awareness and training, being more data driven, and making good on the promise of correlation of data are part of my strategic goals. We do a lot of blanket awareness and training, which gets you an arguable amount of benefit, but the really targeted training I think is far more effective. Being more data driven is something we've been talking about for years, but really getting some of those insights and figuring out where we've got lack of visibility and making use of all the data we've got in our environment. Finally, making good on the promise of correlation of data. People are gaining momentum with getting useful insights out of data analytics.

LANCE SPITZNER: At the highest level, CISOs are focusing on how they can demonstrate value. When the Board asks how are we managing risk, how do we know we're effectively managing risk, things along those lines, what does a CISO communicate? The challenge our community faces is we lack a common way to measure or communicate risk.

DR. MICHAEL MYLREA: Strategically, the big trend is going to be on moving beyond cyber security to cyber resilience.

ANDREW BJERKEN, Global CISO and Privacy Officer, Catalina
ROLAND CLOUTIER, CISO, ADP
ALAN DAINES, CISO, FactSet
ADAM FLETCHER, CISO, Blackstone
SUMMER FOWLER, CISO, Argo AI
EMILY HEATH CISO, United Airlines
TOM MURPHY, CISO, Northwestern University
DR. MICHAEL MYLREA, Sr. Advisor, Cyber Security, Pacific Northwest Nat'l. Lab.

Resilience is really about operational excellence, agility and moving beyond compliance to a more holistic, comprehensive approach to cyber security. It's top down, it's bottom up. Holistic. It is a dynamic defense in depth approach that combines people, processes, technology to foster a culture of cyber security excellence.

SUMMER FOWLER: We had five employees at the end of 2016 and over 400 at the end of 2018. We've had tremendous growth, and we're continuing to grow. I'm going back to some fundamentals like getting a handle on the most critical assets inside the company, making sure that we have focused our cyber security program on the critical few and then building out from there. There are multitudes of things in terms of asset management, identity management, and a really critical component is third-party management.

ROLAND CLOUTIER: Number one, many companies have significant innovations in Hybrid Cloud Management. For example, our three most strategic platforms are being built native cloud. We're cloud based. We have to retool and innovate. This is all about innovation, beyond the product. This is about innovating and how to protect a company. How do you have integrated control capabilities, how do you reduce your cost to operate in the cloud environment?

Many organizations are also going to take a renewed focus on insider threat. We've all been reading about it. You see Apple's success in stopping intellectual property theft.

Lastly, is around automation. many organizations are automating a lot and it's not just doing SOC automation. For example, we ingest daily, roughly 20 billion events per day into our security platform. We are an intelligence-led organization. We're on our third revision in the last five years of our technology stack around big data and analytics. As we go into this year, I think it will be extremely interesting to see how much noise we can take out of the system.

What are the top challenges preventing you from achieving your strategic goals in 2019?

ANDREW BJERKEN: Resources will always be the top challenge, as far as I'm concerned. Another is aligning to the business. The other challenge is prioritization of my side projects.

BRANDEN WILLIAMS: For many CISOs, a challenge will be looking at how many different vendors they're working with and how they make sure they're getting all the information from those vendors to help normalize what's going on. I think that's one of the bigger challenges just in general with so many vendors, and in some cases they do a very poor job of articulating the value problem correctly without using buzzwords such as machine learning and artificial intelligence.

EMILY HEATH: Time is number one. I'm very, very lucky at United to have received all the support and funding I've asked for. I'm one of the lucky CISOs who can say that, because so many of my colleagues cannot. United understands this is a big issue and they invest in it. I've got funding, I've got people, I just need the time to go deliver on some of the challenges that we face.

EVAN WHEELER: I think one of the biggest challenges companies in my space have is the fact that we are service providers to other institutions and the third-party assessment process may be over the top in terms of the requirements. Nobody wants to use anything standard and there's a huge amount of effort that smaller service providers have to put into just responding to these requests and audits.

DR. MICHAEL MYLREA: Emerging threats targeting converged environments that combine operational technology and information technology. These IoT environments are inherently vulnerable, lack basic monitoring and defenses, tough to inventory and increasingly part of a CISOs responsibility. Unlike traditional information assurance, these environments are increasingly integral to safety and security of critical infrastructures from advanced manufacturing to electricity infrastructure. Failing to secure these environments can lead to major loss of life and severe economic consequences.

CISOs TOP CHALLENGES

36% said
TIME & MONEY

18% said
PUBLIC PERCEPTION

18% said
EMPLOYEE RETENTION & WORKFORCE DEVELOPMENT

Another major challenge is workforce development.


GOPAL PADINJARUVEETIL
CISO, Auto Club Group


CHRISTOPHER PAINTER,
Former Coordinator for Cyber Issues, US State Dept.


SHAWN RILEY,
CIO, State of North Dakota


ROB SLOAN,
Research Director WSJ Pro, Dow Jones


LANCE SPITZNER,
Director, SANS Institute


BRANDON SWAFFORD,
CISO, Webster Bank


EVAN WHEELER,
CISO, Financial Engines


BRANDEN WILLIAMS,
Director, LATAM/Canada BISO, Union Bank

Malicious cyber adversaries will continue to exploit human vulnerabilities in organizations using crude but effective phishing and social engineering attacks. For this reason, it is essential to foster a holistic approach and train personnel to increase cyber security situational awareness throughout the organization. Strong policy and processes can facilitate that goal and help protect us from ourselves, if you will.

I think another major challenge for leadership is strategic investment and quantifying the threat So, if cyber risk is loosely defined as threat times vulnerability divided by defense, but that threat is complex, it's not linear and it's evolving, it's very difficult as a cyber leader to quantify their cyber risk. And if you can't quantify, how do you as a leader make strategic investments to buy down that risk. A great example of this challenge can be seen with cloud security. As we move the IT stack to the cloud and increasingly rely on third parties, it becomes more difficult to quantify cyber risk, especially around identity and asset management.

Lastly, CISOs will have to keep up with new regulations around privacy and security such as GPDR and The California Consumer Privacy Act.

ROB SLOAN: Time, money and people. I think those three factors prevent most things from being achieved period, not just in security.

I am particularly concerned about how small to medium-sized businesses are faring. They don't have access to the best human capital, they don't have the budget to buy high end tools to help them manage risks or detect attacks, and they cannot afford third party consultancy. Additionally, the impact of a cyber attack is disproportionately high. Even a small incident can cost considerable amounts of time and money to remediate and, if not managed effectively, can be enough to put that company out of business. One of my 2019 goals is to contribute my efforts to helping the SMB community improve their cyber security.

SUMMER FOWLER: As I think about the autonomous space, another huge challenge we're going to have is public perception. You will never get into a car if you don't trust that it's safe. And security is fundamental to safety, so building trust from the public is absolutely critical. I want to do that by making security part of the fabric of the company and our products.

THOMAS MURPHY: Mostly financial. It is a function of not having enough people to do the work. Without the financial means we can't innovate as much. Finding the right technical skills is going to be a challenge too.

What security program areas do you spend the least and most amount of your time?

ADAM FLETCHER: The least amount of our time is spent on security awareness and monthly phishing tests. We've built a repeatable process for continuous education and reinforcement of key messages, and continuous testing. We're spending the most amount of our time right now making sure we have the right controls in place as we move into some transformational cloud services. We want to understand the cloud as well as we understand traditional infrastructure, so we can achieve the same standards and capabilities with respect to prevention, visibility, and response.

ANDREW BJERKEN: Ironically, contract review is the least amount of my time. It used to take the most when I first started but we've taken great strides to standardize and automate where we can. It was also helpful that I realigned from under the CTO to the Chief Legal Officer.

The area that takes the most of my time is actually my client security management. It takes so much time because of the lack of standardization across assessments or organizations want the information in a different format. It takes a lot of time. GDPR added a huge weight because it requires the organization to have notifications of who's got our data.

54%
of **CISOs** said they spend the most amount of time on **BUSINESS REQUIREMENTS/ALIGNMENT** and **STAKEHOLDER MANAGEMENT**

BRANDON SWAFFORD: My highest priorities taking the most amount of my time are configuration and asset management, identity and access management, enterprise logging and then end point and network control. I prioritize improving fundamental capability to understand what I have and where it

ANDREW BJERKEN, Global CISO and Privacy Officer, Catalina
ROLAND CLOUTIER, CSO, ADP
ALAN DAINES, CISO, FactSet
ADAM FLETCHER, CISO, Blackstone
SUMMER FOWLER, CISO, Argo AI
EMILY HEATH CISO, United Airlines
TOM MURPHY, CISO, Northwestern University
DR. MICHAEL MYLREA, Sr. Advisor, Cyber Security, Pacific Northwest Nat'l. Lab.

is in order to effectively use input tools.

SOC automation, internal network mapping, and deception take the least amount of my time right now.

EMILY HEATH: I always say that I probably spend less than 10% of my time with IT. I think it's a common misconception in security that it's just an IT problem. The biggest part of my day is spent with the business, trying to understand what is important to them. It's not up to me to decide what is important for United Airlines. I work with partners across the business. The second thing I'll add is I'm spending a lot more time looking at that intersection between physical and cyber security. Those areas cannot exist as two separate entities anymore.

EVAN WHEELER: I think the most time is spent around making our institutional clients comfortable with our controls. I would say where we luckily spend the least amount of time is patching. We've got a very automated process around that as we move more into the cloud environment, it's less patching systems and it's more just rebuilding them on a regular basis from a known good image.

CISOs said they spend the least amount of their time:

GOPAL PADINJARUVEETIL: I spend a lot of time looking at what kind of clear and present risks I have in my organization. There's a lot of information sharing, but it can be better. My vision is to have some kind of real-time threat intelligence sharing between defenders. Attackers talk to each other and share information, while the defenders do not talk or collaborate as much. My vision is creating an intelligence sharing platform for the federation where you're not sharing your sensitive information, but you're sensitizing and anonymizing valid actionable threat data, so they can take proactive action. We are seeing signs of progress in this area with the FS-ISAC and H-ISAC.

Most of my time is taken by looking into increasing our visibility in what is happening in our environment, making sure the technologies are performing efficiently and effectively, and the awareness, behavior and performance of the people in the organization is aligned to the real threats we see in the cyber and digital domain.

SHAWN RILEY: I would say the least amount of time for me comes in the sense of the actual day-to-day operations for me in my role.

For the most part, it comes down to working with our stakeholders. I would say I spend probably 40% of my time sitting down with leaders across the state and talking to them about what the needs are and what it is that we're trying to get done and how we're trying to really be able to move the world forward.

THOMAS MURPHY: Probably the least amount of time is security and awareness because we benefit from having a communications department within IT and we are able to set out a 12-month plan and execute once the materials are complete.

The most amount of my time is spent on operations, mainly with incident management and response.

ROLAND CLOUTIER: The least amount of time is engineering operations and SecDevOps. We have a mature program. We have an excellent leader in that position. I have excellent leaders across the board. Even critical incident response.

I think right now our aggressive approach to integrated risk is taking the most amount of time. At ADP this year, we're growing a single integrated risk platform, single taxonomy, single set of controls, a controlled taxonomy, single platform worldwide, all divisions, all business units, all corporate, under the GRC platform.

ALAN DAINES: The reality is I spend most of my time looking at compliance, controls, strategy, and way less time on operations and technology. I spend most of my time managing up, managing my peers. Defining what the security strategy of the organization is and less time worrying about the operations aspects.

What cyber security technology area are you investing in that will be the most transformative to your security program?

ADAM FLETCHER: IAM automation and orchestration. We last looked at this space a few years ago and we ultimately chose not to buy anything off the shelf. We believe that the solutions have matured, and some new ones have emerged, and we're going to take another look. I think that area holds a lot of potential for us.

ANDREW BJERKEN: My pet project this year will be deception; it is going to be the most transformative. Beyond adding another layer of security, I think it will help delineate us from our competitors. Our security program is very much business aligned. I think that this new layer of security will pay dividends.

ALAN DAINES: I would say threat detection is the most important, tactically. Building core controls for hardening the environment and implementing detection and visibility. This is always a big sell because the investment is high, so when doing so I like to use physical building analogies. We've got a building, it's got a bunch of doors and windows, some of those doors and windows are wide open. We need to get the doors closed, install the video surveillance cameras and station the security guards. Therefore, I have my threat detection once we've got security guards, all the video surveillance cameras and trip wires are installed, and we are watching.

CISOs Top Transformational Investments

#1
THREAT DETECTION AND INTELLIGENCE

#2
GRC, IDENTITY AND ACCESS MANAGEMENT, CLOUD/CASB

BRANDEN WILLIAMS: In general, if the artificial intelligence and machine learning claims could actually be true, there is potential there. I think one of the challenges with those types of algorithms is that we slap those words onto things without understanding it. I would love to see that type of technology really advancing.

CHRISTOPHER PAINTER: I'm not unique in saying this, but you'll see more consolidation. First, there's a dizzying array of products out there making it difficult for even a seasoned CISO to choose. Second, folks are unlikely to buy products from just one vendor because everyone wants to diversify, right? I think that consolidation coupled with vendors that offer platforms that allow customers to choose among technologies and products that can be integrated might be where things are going.

EVAN WHEELER: Cloud automation. And I think the opportunities we have there around infrastructure as code and things like that, can really make it so much easier. We've got much better visibility into the cloud environments. We can have a lot more control over what changes in those environments.

SHAWN RILEY: It's definitely behavioral analytics and artificial intelligence analytics. We are spending the vast majority of our money for the next three years in the spaces of artificial intelligence and behavioral indicators of compromise. We want to be able to ensure that we understand the aspects of when an individual does their job, what is expected or not expected around that traffic and how bad traffic moves across the system. There's just a huge amount of our cap x resources that are going towards overall analytics and artificial intelligence.

How do you judge how well you are performing? How do your executives judge your performance?

ADAM FLETCHER: For better or worse, I think executives primarily judge any CISO's performance by the occurrence or lack of occurrence of a material incident. In a less macro sense, I think that key stakeholders judge CISOs on how well we're able to manage the cyber security day to day. We're constantly reacting to the latest threats, suspicious emails, and vulnerabilities, so are we doing that with a level of rigor and consistency that enables us to articulate to our stakeholders with confidence that we're managing the threats before they cause harm, and that we're learning from every experience and continuously improving. Executives also judge CISOs by asking how our programs are doing with respect to industry benchmarks and our peers. Knowing what those guideposts are and using them to demonstrate that we're continuously progressing is a key indicator of how we're performing.

ANDREW BJERKEN, Global CISO and Privacy Officer, Catalina
ROLAND CLOUTIER, CSO, ADP
ALAN DAINES, CISO, FactSet
ADAM FLETCHER, CISO, Blackstone
SUMMER FOWLER, CISO, Argo AI
EMILY HEATH CISO, United Airlines
TOM MURPHY, CISO, Northwestern University
DR. MICHAEL MYLREA, Sr. Advisor, Cyber Security, Pacific Northwest Nat'l. Lab.

BRANDON SWAFFORD: We should really focus on key risk indicators. So how do you prove that you've reduced risk? How many assets do I have under management? How many things are at baseline? And if you can't do that, then don't buy it. So that's how I justify things with management. And I think that actually starts to make sense. As soon as you start talking about risk reduction by dollars, it becomes a lot easier. The biggest complexity was to try to make an argument for visibility because it's not as interesting. It doesn't bring down risk inherently.

HOW **CISOS** JUDGE PERFORMANCE:

#1 Metrics
#2 Staying out of the news
#3 KPIs/KRIs

CHRISTOPHER PAINTER: I don't think managers at the C-suite level know how to judge a CISO because it often comes down to, if everything's going great, they're good, but if there is any major incident it's the CISO's fault. They think - we have a CISO, therefore we've done everything we needed to do for security. CISOs have told me they need to have contact with, and educate the board so the board understands what the risk level is, just as they do in the physical world, and that it is not binary, but a continuum that needs to be addressed and mitigated if and when an incident occurs.

EMILY HEATH: It's hard to know how to measure yourself. You can choose to measure how many incidents, how many things you've blocked and how many vulnerabilities you've found and remediated. It doesn't prove anything. Oftentimes this is a problem with things like security assessments. Sometimes companies bring in outside organizations with a little checklist, but it depends on what questions you're asking. So, it's really hard to know how to measure your performance because you never want to declare victory on anything in this business, that's a slippery slope. But the more we can work together, the better. That's the way you're really going to tackle things.

LANCE SPITZNER: Primarily metrics, especially when reporting to senior leadership like the Board. This is where frameworks such as the NIST Cyber Security Framework, help. These frameworks give you a model to communicate to senior leadership what you're doing, why you're doing it, and how you benchmark or measure up.

> *"PROBABLY THE MOST IMPORTANT FIRST STEP IS BENCHMARING AGAINST YOURSELF. YOU MUST FIRST KNOW HOW YOU'RE DONE. THEN, OVER TIME ARE WE GETTING BETTER OR GETTING WORSE?*
>
> – LANCE SPITZNER

DR. MICHAEL MYLREA: We need to do a better job of quantifying success as it relates to CISOs enterprise vision and strategy. Realizing a strategic vision is a continuous process for a CISO - one that aims for pareto optimality where investments optimize both business and security goals, which is challenging when they are diametrically opposed. To realize both business and cyber security goals, we need to develop key performance indicators and better understand the return on investment for cyber security.

THOMAS MURPHY: If we're looking at the performance of the program, then it's obviously not having newsworthy events involving Northwestern data. But if we're looking at the return on investment and how I'm performing it's a multilayered answer. My CIO knows I've set out goals and objectives for the year for myself and the team. It's a continuous cycle of assessing whether we accomplish those goals. If we didn't, what were the things that prevented us from succeeding? Both of these combined help us judge progress over time.

How do you effectively benchmark against yourself and the industry?

CHRISTOPHER PAINTER: In terms of benchmarking your performance, it's often difficult to measure a negative – i.e., how often you have escaped a major breach. There are a number of possibilities but they aren't perfect, including tracking the number of significant attempts, tracking how many of these attempts were blocked, tracking the remediation or mitigation time following a successful penetration and comparing your organization's performance to other like sized or similar organizations and/or to your own organization over time. Yet, despite the difficulty, for CISOs to have the conversations they need to have with boards (both to educate them and garner necessary resources) and to make progress in securing an organization, metrics are important, just like they are in any other corporate endeavor.

EVAN WHEELER: It definitely seems like people are relying very much on maturity models and sometimes I worry that we rely on those because we don't actually know what our risk


GOPAL PADINJARUVEETIL
CISO, Auto Club Group


CHRISTOPHER PAINTER,
Former Coordinator for Cyber Issues, US State Dept.


SHAWN RILEY,
CIO, State of North Dakota


ROB SLOAN,
Research Director WSJ Pro, Dow Jones


LANCE SPITZNER,
Director, SANS Institute


BRANDON SWAFFORD,
CISO, Webster Bank


EVAN WHEELER,
CISO, Financial Engines


BRANDEN WILLIAMS,
Director, LATAM/Canada da BISO, Union Bank

exposure is and how much we've reduced our risk. At a previous company, one board member actually said I don't want to hear any more benchmarking, I want to know what our actual risk exposure is.

LANCE SPITZNER: Probably the most important first step is benchmarking against yourself. You must first know how you're doing. Then, over time are we getting better or getting worse? But the problem many organizations have is the CISO changing every two to three years. The technology is changing, the priorities are changing. So once the Board finally figures out exactly what they want, things have changed.

ROB SLOAN: There is a severe shortage of help in this area. We conducted a study last year with 1,300 companies globally as a first step towards allowing CISOs to compare their organization's progress with others in their industry, with a comparable revenue size sector, or by geography. When you look at the scores, it went from companies of $50 billion or above in revenue doing the best, right down to $250 million performing the worst. Regardless of geography, there is a clear correlation between how much you were spending and your performance, which raises further concerns about the state of security at the SMB level.

SUMMER FOWLER: I don't have a single precedent that I could use to compare Argo right now. We don't really have anything in that space, quite frankly, because there's nothing publicly available. When you think about it, Lyft is trying to IPO this year. So, they've opened up a little bit more and we see more of what they're doing and finances, but you know, frankly, everything's private right now, so we don't really have that comparison. I'd rather focus on making Argo's security program the best that it can be without comparison.

THOMAS MURPHY: Through collaboration with the schools in the Big Ten Academic Association. Every quarter the CISOs of all the BTAA schools get together. We talk about what we are seeing at our respective schools. We share threat intelligence and talk openly about responses and solutions or tools that either work or don't and why. We have some internal benchmarking capability to check our controls against frameworks and score ourselves over time.

> *"I HOPE CISOS BECOME MORE RELEVANT TO THE BUSINESS AND THEY ARE ABLE TO SPEAK IN LANGUAGE THAT HELPS ENABLE THE ORGANIZATION TO TAKE ON RISKIER BUSINESS, MEANING MORE PROFITS.*
>
> - BRANDEN WILLIAMS

ROLAND CLOUTIER: We do it externally. I have an oversight organization that sits next to me during the year and pulls out what we've committed to the board. Think of one of the big four types, they did a baseline and they measure us and then they follow us over the year. Part of that is to say, where are we at with spend? Where are we at with patching? We look at those industry trends, we report on it, and we report ourselves against that. Money's one thing, but operational metrics are more important to us.

SHAWN RILEY: Since I started in this new role, our organization has started a national benchmark model. We are benchmarking against NIST. We also benchmark against other organizations that are similar to us. We're also using an external organization to come in and do a specific zero to five matrix against our entire operations. That gives us a day-to-day view of where we're falling behind and where we have opportunity to improve. But it also shows us that long term vision of where we can strategically improve ourselves.

How is CISO role transforming and what is it transforming into?

ADAM FLETCHER: I think the CISO's role has, and always will be, to protect the intellectual property, sensitive data, and reputation of the business. While I don't see that part of the role transforming, I do see a change in the "field of play", which is to say that many people are starting to move to Software as a Service and Infrastructure as a Service, which brings both new challenges and new opportunities to transform ourselves and our teams. I also think there's a growing expectation for CISOs to have more business acumen. Do CISOs deeply understand the businesses that they support? Can they speak in business terms and can they articulate cyber security risk in a way that non-technical leaders can relate to?

ANDREW BJERKEN: In my opinion, the CISO role is going to take one of two paths or it may split and take both of them. One, it could morph into a risk officer role; a belief that has been around for a while. Security would be one means of controlling risk. The other, which I'm hoping it takes, is more of a business leader role where the CISO is brought into more conversation

ANDREW BJERKEN, Global CISO and Privacy Officer, Catalina
ROLAND CLOUTIER, CSO, ADP
ALAN DAINES, CISO, FactSet
ADAM FLETCHER, CISO, Blackstone
SUMMER FOWLER, CISO, Argo AI
EMILY HEATH, CISO, United Airlines
TOM MURPHY, CISO, Northwestern University
DR. MICHAEL MYLREA, Sr. Advisor, Cyber Security, Pacific Northwest Nat'l. Lab.

proactively vs reactively and the opinion is valued.

BRANDON SWAFFORD: I think what you're going to see is a much harder swing towards either more technical CISOs or a division at the leadership level where one is handling policy and the other's doing technical. A lot of the laws are being written where the CIO or CISO are criminally responsible and you're going to start to see a really well-defined archetype to fit that role. I fear that a nontechnical CISO is going to have unsatisfying answers for the board and C-level executives. And the other issue is that your staff underneath is going to change. If you're relying upon a bunch of people that aren't you to maintain your technical understanding, then you're in hot water. My own management is asking me those questions and we're not a technical product company.

BRANDEN WILLIAMS: I hope CISOs become more relevant to the business and they are able to speak in language that helps enable the organization to take on riskier business, meaning more profits. If that person is considered an advisor to the CEO, it really doesn't matter where they sit in the organization. If the CEO calls them and listens to them, trusts them, and asks them questions, then they can sit in the CIO, they could sit in Chief Legal, or they can sit somewhere else. But if there's that direct line and there's a good relationship there with the security person saying, 'I'm here to enable the business,' I would hope that's where we go.

LANCE SPITZNER: The CISO will be more business focused, they are becoming less of an IT expert and more of a business risk expert. Think MBA vs. Computer Science degree. A big step is ripping the CISO out from under the CIO and having them report to the CEO. They have to be put up at a business level.

DR. MICHAEL MYLREA: CISOs are entering a brave new world of emerging technology, evolving threats and increasing complexity across the enterprise. One example of this transformation can be seen in converged IoT environments where operational technology and information technology, industrial control systems and SCADA, cyber and physical systems are woven together. In these IoT environments traditional cyber security best practices for access, asset and identity management are increasingly difficult to implement. Some of the challenges include converged environments with cloud and on prem legacy systems, analog and smart systems, devices that can't be patched and are difficult to monitor, as well as the increase in the speed and size of data being collected, stored and exchanged. Even as CISOs' responsibilities are transforming, the attack surface is growing and technology is rapidly changing, getting the basics right requires a strategic vision and holistic approach that aims for cyber resilience.

ROB SLOAN: The CISO role definition is too broad and can change significantly depending on the experience of the individual and the varied priorities placed upon them by their reporting line.

We must also consider the role of a CISO. As security programs mature, the focus becomes less about technical detail and more about the business. As that happens, cyber security oversight will more naturally sit with an executive who is intimate with the business, meaning the role of the CISO must adapt, or another C-level executive will take over.

SHAWN RILEY: With cyber security landing in the top two of most, if not all, state's key focus areas, the CISO role must have real-time visibility into the "state of cyber security". In North Dakota, our strategy is a unified approach to statewide cybersecurity, and a more concerted effort to work with 7 branches of government to elevate our ability to prepare and defend against cyber-attacks. Protecting our state systems and our citizens' data is a top priority so a proactive approach and "working as one" is essential, as well as investing in tools to help automate our cyber defense capabilities.

Let us help you justify decisions and educate your organization.

If you are interested in learning more about how this information can help you justify decisions or educate executives, let us know. We have compiled these into a presentation that includes strategic, business-aligned information backed by direct quotes and statistics from our CISO community.

All statistics included in this article were compiled from the 16 CISO and security leader interviews we conducted at the RSA conference, as well as input from CISOs on K logix's Advisory Board.


GOPAL PADINJARUVEETIL
CISO, Auto Club Group


CHRISTOPHER PAINTER,
Former Coordinator for Cyber Issues, US State Dept.


SHAWN RILEY,
CIO, State of North Dakota


ROB SLOAN,
Research Director WSJ Pro, Dow Jones


LANCE SPITZNER,
Director, SANS Institute


BRANDON SWAFFORD,
CISO, Webster Bank


EVAN WHEELER,
CISO, Financial Engines


BRANDEN WILLIAMS,
Director, LATAM/Canada BISO, Union Bank

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

LEON BROCKWAY
ISO, TOMPKINS FINANCIAL

HEADQUARTERS: Ithaca, NY

EMPLOYEES: 1,000+

ANNUAL REVENUE: $6.7 Billion

Leon Brockway had his first exposure in information security while working in military intelligence for the United States Army over 18 years ago. From there, he transitioned into the Department of Defense contracting sector, working on large projects for various federal agencies to support technology and security programs. Over the last three years he has led the Information Security Program as the ISO for Tompkins Financial, a New York state-based financial services holding company. He comments, "My work experience so far has been a case study of the transition of information technology, to IT security into information security to where we are today, what we're seeing quite a bit of in the industry is information security more appropriately aligning with business function(s) and risk management specifically, it is really an exciting time to be part of the maturity of the Information Security profession."

CONCENTRATING ON KEY STRATEGIC GOALS

Brockway approaches 2019 with clear strategic goals in mind including aligning with business and IT strategy, forming strong coalitions with business partners, recruiting, training and retaining top security professionals, establishing operational excellence and creating and maintaining key risk indicators.

Alignment. Alignment is a constant strategic objective for Brockway, as he continues to expand maximum participation around strategic discussions. He also emphasizes the importance of collaborating with his business and IT counterparts.

Strong Coalitions. He encourages and empowers his team to form strong coalitions with business partners by engaging at the appropriate management levels. He explains, "We must make sure there's good communication channels with each one of our business partners. We'll be looking to maximize that kind of coalition around information security across different departments."

Risk Indicators. On focusing his time around key risk indicators, Brockway explains, "I think we're in the intermediate step and we'll continue strategy around making sure we have solid key risk indicators, and that we have matured our program to be

"THIS IS A FINANCIAL INSTITUTION, SO IT'S IMPORTANT TO ALIGN THE INFORMATION SECURITY PRESENTATION AND REPORTING TO SOMETHING THAT MIGHT LOOK LIKE ANOTHER DEPARTMENT REPORTING."

able to measure the effectiveness of our control framework. We're in the financial industry and moving those types of indicators to a numbers game is critical, we're going to have to continue to align our metrics with the numbers that our board and our senior leadership team are accustomed to getting from other business departments."

OVERCOMING CHALLENGES

Brockway believes many of his challenges are common among information security and other business sectors. These include buy-in and adequately balancing time and resources.

He comments, "Buy-in across the organization can be a big challenge, which is also very common, and why coalition is so important across the organization. You must make sure you have really strong relationships to be able to execute these particular activities. The other challenging piece is around one of our tactical objectives, operational excellence; we're spending lots of time to make sure we're doing the fundamentals exceptionally well. And that takes a fair amount of resources and time from the information security team, and the organization, to be able to do the traditional cyber and IT hygiene fundamentals. Another significant challenge is overcoming regulatory control oversight vs. risk alignment, this will continue to be a challenge as our regulators evaluate our program against a control and threat landscape as opposed to basing it on our risks."

FOCUSING ON SECURITY PROGRAM AREAS

Brockway notes the program area that takes up the most amount of his team's time is information security administration. These fundamental tasks include day-to-day, week-to-week, or month-to-month activities around ensuring controls are operating in place and operating as expected. He says these are the 'bread and butter' of his program, yet take an exceptional amount of time.

From a culture perspective, getting traction and projects going in the right direction also takes a great deal of time, as he explains, "We particularly are a culture of collaboration, which is a good thing and you typically end up with polished and strong results. But the process of collaboration, maximum buy-in, and consensus takes a lot of time to get the right pieces in place. It's about all the right people moving in the right direction, sharing the same objective, and sometimes finalizing projects takes a lot of effort and time."

One of the more streamlined tasks with minimal time impact on Brockway's program is threat intelligence. He says, "Threat intelligence comes relatively easy and quickly into us, given we subscribe to multiple, different threat feeds, and different information sharing forums. We usually just get a lot of information from an emerging threat and a threat perspective, and we tend to be highly vigilant around emerging threats that we may need to take some type of action against."

COMMUNICATING AND REPORTING ON RISK

To judge how well Brockway's security program performs, he relies on identifying risk thresholds. He does this by starting with strong controls and identifying the appropriate thresholds of risk acceptance in order to report if the program is effective and operating properly. He subscribes to the CIS Critical 20 for control structure because they are prioritized, prescriptive, and a 'paint by number' approach, as well as mandatory controls from NY Department of Finances and the FDIC. If something bubbles up above the threshold, he then reports to senior leadership or the board.

He takes an educational approach with senior leadership, coupled with meaningful data. He encourages CISOs to find ways to take extremely complex security controls and processes, and turn them into a simple and digestible format. He pinpoints this as a key skill for CISO success and constantly challenges himself to improve and fine tune his approach.

During board discussions, Brockway will be simplifying his approach by correlating information security risk, controls, and program effectiveness into financial numbers his organization is accustomed to seeing. He explains, "This is a financial institution, so it's important to align the information security presentation and reporting to something that might look like another department reporting. So, massaging the information security report to something that can be presented in that same way, but conveys all the important things of the information security program, is certainly a big challenge for CISOs. You want to align with what your board might be accustomed to, to the best of your ability. That's a challenge. I can present this in a very technical way and we all know that's probably not the best way for people to digest it from a board and a senior leadership level."

Q&A WITH CAROLYN CRANDALL

CHIEF MARKETING OFFICER AND CHIEF DECEPTION (TECH) OFFICER, ATTIVO NETWORKS, INC.

As Chief Marketing Officer at Attivo Networks, Carolyn is responsible for driving market awareness and demand for deception-based detection technology. Carolyn achieves her goals through technology evangelism, brand awareness campaigns, multi-channel demand and customer-engagement programs, and through engagement with reseller, MSP, and technology partners. In her dual role of CMO and Chief Deception Officer (CDO), she actively speaks on security innovation at CISO forums, industry events, technology education webinars and podcasts. She has been a guest on Fox News, speaking about the role of deception in cyber security, along with being an active byline contributor to many technology publications. In 2018, she was recognized as a Business Woman of Year, Hall of Femme Honoree, and Reboot CIO/C-Suite Leadership Honoree. She was also profiled on the front page of The San Jose Mercury News Business Section in February 2019.

We spoke with Carolyn to learn more about Attivo Networks and her impact on company growth and success.

HOW DOES ATTIVO DIFFERENTIATE IN SUCH A CLUTTERED MARKET?

No doubt, the noise is deafening. I was recently at a security event observing the words vendors use to articulate what they do. It was clear that not only the words we choose, but how we put them together to communicate our differentiation are critical. Fortunately, Attivo's message stands out because the technology takes a different approach than traditional prevention technologies. Unlike other solutions, Attivo's offering is based on accurately detecting in-network threats that have bypassed perimeter defenses. The value is seen in reducing the time an attacker remains undetected (dwell time), engagement-based alerting for improved investigation and response, and in adding a pre-emptive defense that is not centered on reacting to an attack.

Deception becomes interesting if you accept that attackers can and will get into networks based on human error, misconfigurations, and the simple fact that innovation is outpacing security controls, leaving gaps related to IoT deployment, shared cloud security models, and the demand for shared information and Internet accessibility of everything.

People have used deception to outmaneuver their adversary in gambling, sports, and military operations for millennia. Attivo has now brought the same concept to cyber security by setting traps and bait within the network to detect and derail attackers who have bypassed the perimeter defenses. There's a tremendous value to the organization in detecting attackers before they can establish a foothold, create backdoors, or complete a breach. Additionally, unlike tools that simply deflect an attack, deception platforms gather engagement-based data and deliver rich threat, adversary, and counter-intelligence to allow the defender to confidently stop, eradicate, and prevent the successful return of threats.

HOW DOES ATTIVO'S THREAT DECEPTION WORK?

Attivo creates an in-network environment where an attacker cannot tell real from fake. By obfuscating the attack surface, attackers are tricked into engaging, making mistakes, and revealing their presence. The objective is to stop the attack early and to increase the attacker's costs, so the economics become undesirable for them to continue to attack. Deception can also be quite effective for detecting policy violations related to insiders, suppliers, and contractors.

Attivo creates a deception fabric that blankets the entire network with decoys that mirror-match production assets along with deceptive credentials and lures designed to attract the attacker into engaging. There are two major components to the efficacy of deception. The first is covering the attack surfaces such as cloud, data centers, user networks, and specialized deceptions for industrial control, medical, IOT, POS, network and telecom infrastructure. By mirror-matching these assets, a threat actor cannot tell what is real and a decoy. Adversaries are therefore motivated to take a look

as they seek to discover the network, instantly revealing their presence. Once they take the bait, a high-fidelity alert is immediately raised with concise information on how the attacker is attacking and the tools and techniques they are using. In cases where deception DecoyDocs are taken, security teams will also gather insight into the target or intent of the attack. This can be extremely valuable when trying to detect theft of IP, research data, patents, and case files. Ultimately having in-depth in network, endpoint, data, and application deceptions will provide the best detection coverage.

The other half of the equation is believability. Emulated or static deceptions are limited in their efficacy against advanced attackers. To trick the attacker, Attivo crafts decoys to look and act identical to the organization's environment. This includes using the same operating systems, services, and applications as what is in production. Attivo takes additional measures to integrate with Active Directory (AD) so that deception credentials validate within AD and look authentic to the attacker.

Collectively, with a deception network that blankets the environment and mirror-match authenticity, just one mistake and they will be discovered. Typically, a defender must be right all the time. Deception changes the asymmetry so that attackers, now too, must be right all the time.

WHAT ARE THE BIGGEST CHALLENGES ATTIVO HELPS CISOS OVERCOME?

It is now taking attackers, on average, less than 5 hours to get into a network, 4.5 hours to move to their first hop, and 15 hours to exfiltrate data. That in itself is bad, but even more bleak is when compared to an average of 79 days to find an attacker. Early and accurate in-network detection is essential.

In today's world of fading perimeters, deception provides an efficient layered defense, covering all attack surfaces and evolving attack vectors. By adding deception, CISOs can reduce their dwell time, gain in-network threat visibility, and better respond to an attack. This is done without friction to operations or need for additional staff.

WHAT IS THE CULTURE AT ATTIVO?

It's what I love most about Attivo. Innovation, creative thinking, and a customer-first mentality are inherent in everything we do. Our company motto is that we do great things together. This brings a strong spirit of collaboration and a collective unity in doing whatever it takes to achieve our goals.

It's a big family where everybody interacts and is appreciated for the value that they bring in their roles. This is led from the top, with the CEO setting the framework for everyone to pull on the rope in the same direction. It is a core part of our secret sauce as a company. I'm pleased that we've been able to maintain this culture, even with rapid global expansion. Our global sales kickoff was a few weeks ago and the way that everybody worked together to share best practices and successes in selling the technology was inspiring. The winning culture of Attivo shines clearly in the 75+ awards the company has received for its technology innovation, company successes, and leadership team. A true testament to the quality of the organization.

WHAT PLANS FOR GROWTH DOES ATTIVO HAVE?

Attivo is well positioned to address the growing demand for detection technologies. The company is well-funded for expanding its global sales, channel, and services operations as well as technology innovation. Development will cover enhanced threat deception for advanced attack techniques, tools for increased threat visibility, and overall risk mitigation. Expansion is also occurring for automations on attack investigation, forensics, and native integrations for accelerated incident response.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

CHARLES SCHARNAGLE

CIO, The Mohegan Tribe

HEADQUARTERS: Uncasville, CT

EMPLOYEES: 1,000+

ANNUAL REVENUE: Undisclosed

"We're focusing on information security more than ever because it's a greater threat today. The bad guys have always been out there, but let's face it, 15 years ago you didn't hear about the security breaches that you hear now."

- CHUCK SCHARNAGLE

As the CIO of The Mohegan Tribe for almost twelve years, Chuck Scharnagle oversees the entire IT department, along with a heavy focus on managing information security. With an influx of attention around information security in recent years, Scharnagle has shifted more of his focus onto security priorities. Scharnagle comments, "There was never as much of a focus on information security as there is today, especially when it comes to buying tools, education, training, awareness of end users, internal testing, and audits. Everything has grown so much. It's really been the last five to seven years where there's been a bigger focus and it's drawing up more of my time and thus my interest."

He continues, "We're focusing on information security more than ever because it's a greater threat today. The bad guys have always been out there, but let's face it, 15 years ago you didn't hear about the security breaches that you hear now. And we hear about them on a regular basis. We hear about them almost too much. So, I would tell you today alone, I probably put a quarter of my time on security related projects."

FOCUS ON SECURITY AWARENESS

Spending budget and utilizing resources to improve information security required Scharnagle to approach his Council to gain their awareness and alignment on his decisions. One key area he focused on was security awareness training. He explains, "We started mandatory security awareness training for everybody within the Tribal government and fortunately my management took it very seriously. This was something we made mandatory for everyone, in order to make sure we were protecting and educating the government employees as thoroughly as possible."

Buy-in from the Council was key to Scharnagle implementing a strong security awareness

program. He met with all employees and had meetings across the campus where he presented on the state of security and how it relates to not only their work, but their home life as well. He comments, "I started it out by telling everybody that all of this applies to you not only here at work but at your home as well. And it is interesting because you could see the lights go on for a few people. I talked to them about how people are targeting you at home, that people want to know your credit card information, and bad guys want to know your personal information. It's not just here at work. It's across the board. My philosophy has been to try to educate through open communication as much as possible."

STRATEGIC PRIORITIES

Scharnagle's top strategic priorities are aligning to the CIS controls and evaluating the current technology toolset. He is actively working with his team to ensure they have strong processes and policies in place to address most of the CIS controls. Evaluating his toolset requires a multifaceted, holistic approach, and brings up important considerations such as outsourcing to alleviate any unnecessary strain on his team. He also believes in being flexible and not engaging in longer-term contracts because of the diverse volatility of threats and the rapid speed at which capabilities of tools evolve. He explains, "You have to start evaluating if you want to buy the tool or if you want to start outsourcing or looking at the capabilities of some of these organizations that have tools they'll run for you. And I think that's where we're getting to because one of the things with us is that we're trying to find synergies with the properties that we operate and figuring out the tools that overlap."

When acquiring and purchasing new tools, Scharnagle believes in aligning with smart, experienced people with agnostic knowledge on different technology products. He relies on these experts to ensure all technology decisions align back to the overall business. This approach alleviates the potential to get stuck on a point-in-time technology decisions and helps Scharnagle make justified decisions on any new investments.

BUILDING A COMMUNICATIVE TEAM

Located in the quiet town of Uncasville, Connecticut, retaining and attracting talent poses a unique challenge for Scharnagle. As with many organizations who recruit IT and information security talent, the small talent pool may be exhaustive at times, and even more so for Scharnagle being located further from major cities. However, the desire to work for an organization with a healthy work life balance is attractive to many people and something Scharnagle pushes when recruiting. Perks include an 8:30-4:30 workday, full-size gym on site, and a smaller, more connected community environment.

When recruiting, Scharnagle focuses on finding talent who have the skill to speak to both business and technical people. He believes it is much easier to teach someone a technical skill if they already have strong business aptitude. He says, "I'm looking for somebody that can come in, likes to communicate, understands the value of it, understands the value of customer service, and any other similar qualities. Whether they're going to be a developer, a network analyst, a help desk person or my director of technology, I want them to be able to communicate. I can send them away to a class for them to learn a technical skill, but the customer service skills are very important."

Scharnagle practices what he preaches by communicating with his team about any strategic discussions he has with council members. He explains, "I try to be extremely transparent on where we're going, what we're trying to do, what we're trying to deliver, and why. It is a bit of a challenge because even though we're a government, we have a holdings company which is a series of businesses. So, we do have to support many different things and most of my team must wear many different hats, but they seem to like that challenge as well."

Scharnagle strives to secure budget so his team may engage in various trainings to stay up-to-date and fulfilled in their careers. He sits down with his team at their regular meetings and asks about their training goals for the quarter. He believes in asking them about how they want to build their career, what they need to do their job to the best of their ability, and how he can help them grow. Overall, he believes in investing in his team so they continue to build their skillset, enjoy their work, and set aspirations for future growth.

GROWTH

"My focus is how do we do more with less, like purchasing a tool that allows my team to focus on what's important by automating recurring tasks. When it really comes down to growth, I don't want to grow as far as adding more people, I want to grow as far as knowledge. I want my team to be trained as much as possible in new areas so that they can come back with an acquired skill that improves our security stance. Another goal is to find solutions that require little from us and allow us to really focus on the bigger and more complex issues. And that's what it really boils down to with security and our team. Again, I've got one set of eyes in security at all times, and I've got to find ways to take advantage of them."

Q&A WITH NICK LANTUH
CEO, FIDELIS

As CEO of Fidelis, Nick Lantuh focuses on growth, alignment, and strategic vision. Fidelis protects the world's most sensitive data through threat detection and response in one unified security platform. We spoke with Nick about his role and how Fidelis makes an impact.

SC 2019 awards
Winner
BEST DECEPTION TECHNOLOGY SOLUTION

WHAT IS YOUR ROLE AS CEO OF FIDELIS?

Overall, my work is to set the strategic vision and operational direction of Fidelis, to clearly articulate our unique offerings by communicating the value proposition, and to cement the company's position as a cyber security thought leader.

I'm focused on leading us through rapid growth, so we can assist even more companies in automating detection, threat hunting and response to keep their networks safe. My main task here is to make sure that we're aligned. We've got some very powerful technological capabilities and I work to make sure all our resources are focused in the right direction and to make sure that we're executing to our fullest. That's been the focus for the last 10 months. Finding things that are working and doubling down on them, finding things that haven't been working and taking them out, and replacing them with things that do work.

WHAT CHALLENGES DOES FIDELIS HELP CISOS OVERCOME?

We have one single platform that provides full visibility across your environment, whether it's on the network, at the end point, in the cloud, in the data center, or on-prem. We understand the network terrain to do real-time continuous monitoring, for both inbound and outbound threats. We've got a solution that captures and analyzes all ports and protocols bi-directionally for bad things coming in to attack you, and good data leaving the organization that you don't necessarily want to leave. We see all of the activity and provide deep forensic tools at the endpoint.

Ultimately, what we provide is a visibility solution that digs deep into the raw data we collect and then extracts rich, indexable metadata that is critical for understanding the who, what, when, where and how.

All of this is integrated, automated, correlated and orchestrated to provide you with full context around potentially bad things that are happening in your environment - and we have the ability to do that in real-time and forensically. We are providing you with actionable intel right at your fingertips all in a single platform.

HOW DO YOUR CUSTOMERS HELP SHAPE FIDELIS OFFERINGS?

We can build models with our solution that collect all the raw data within a network environment. We get requests all the time from customers that ask us to take our entire data set and run specific models against it. And those models could be something like the nonstandard encryption types running on your network or showing customers every time there was more than one single password attempt on a device.

We have the ability to run 'N' number of queries against what we do and the data that we collect and carry. Those are an everyday event, whether they're coming through our customer success organization, account management folks, managed detection and response team, threat research team, SEs in the field, or data sciences team, we're in a constant mode of providing this to our customers daily.

HOW DOES FIDELIS DIFFERENTIATE IN SUCH A CLUTTERED MARKET?

We stand out because we have an engine from a metadata analysis standpoint that is able to look at our threat detection capabilities, we have the ability to detect what data is leaving

your organization, and we do this all in one single platform without needing anybody else's products. We've got a single platform that does all the automation, orchestration, correlation, integration in and of itself because we collect all the raw data and the reality is you can't hide in the raw data because that's where everything is.

We are used by our best customers as a last line of defense. So, when everybody else's products say that traffic is good and it should be passed through, we are there to actually look at that traffic as truly a last line of defense to say okay, what's going on in here, let's baseline what normal looks like, let's extract what looks strange or anomalistic, and let's determine what's really bad in that traffic. This is what we do really well. It really is a hunting platform that's self-contained. For our managed detection and response service and incident response service, we only use our products which provide the necessary depth of visibility and information.

WHAT IS THE CULTURE AT FIDELIS?

One of the initiatives we kicked off when I started here was an innovation initiative. I'd say that from a development standpoint, it's all about innovating. It's about bringing to market unique capabilities and a culture of high performance. We've brought in a number of A-players since I've been here and we've upgraded across the board the talent within the company. The focus is on performance and we reward people based on performance. Everybody here knows without a question of a doubt that performance is valued here and it's certainly a high-performance environment that we've created and continue to foster.

The technological base that we have is very unique and something that's attractive to many people because it provides differentiation, and we find people want to be a part of that. Everybody wants to be a part of something that's going to be a winning environment. We're getting a lot of people coming into the fold because of that and there's a lot of folks here that have done it before, so they had successful exits and know how to run successful teams. There's not a lot of trial and error here, it's tried and true, leaders that have done this before.

WHAT GROWTH DOES FIDELIS EXPECT IN 2019?

Above all, the team is growing and we're adding quite a bit of people from a revenue standpoint. We're well into double digits in terms of our growth rates. Also, from an innovation standpoint, we have our latest release coming out this next month across the various products. We've already mapped out what we're going to be coming out in the next release and haven't yet announced to the community. We're really excited on all fronts. As well as our revenue engine, that continues to chug up and to the right.

LAW & CYBER SECURITY

EXPERT OPINIONS ON HOT TOPICS

Interviews conducted by:
Katie Haug, Kevin Pouche, & Kevin West

During the RSA conference, we interviewed two lawyers who focus much of their work on cyber security. By interviewing non-CISOs, we are able to understand a different perspective on key industry trends and concerns.

We first spoke with Stephen Wu, Shareholder, Silicon Valley Law Group.

As a seasoned lawyer with a focus on information security, in what instances do you interact directly with CISOs?

We're working very much hand in glove with each other. Some CISOs are spending a lot of time with contract drafting and negotiation. The day-to-day work of contract review and negotiation calls takes them away from their core function of security management. Consequently, they have to hire people to help them. As a lawyer, I help them by taking on some of the burden of negotiating security agreements or security exhibits to larger contracts. We will take turns reviewing contracts and negotiating deal points on customer and vendor calls. From time to time, I also work with CISOs on meeting compliance requirements and to support security audits and certifications.

I recommend that CISOs hire people to interface with lawyers like me to further lighten the CISO's workload. Those people need to have skills that bridge between law and security. So, if you hired a security person who has no legal training, then that person must be trained in key legal topics. If you hire a lawyer who doesn't know information security, it's not going to work because then he or she doesn't know the security environment. Relying on checklists is not enough. Team members need to be able to bridge between law and security. I think there's an opportunity for information security professionals who have knowledge of both security and the legal aspects of contract negotiation.

How does Artificial Intelligence fit into your work?

I work in the areas of transactions, compliance, litigation, liability, investigations, and policies and procedures in AI and robotics as well as information security and privacy. I started in information security and privacy in 1997, but since 2007, I have been trying to incorporate more AI and robotics matters into my practice. My work in the area of automated transportation is a good example.

With transactions, I help AI and robotics companies sell their products and services. I advise clients on how to comply with various laws that apply to AI and robotics, such as GDPR and California's new bot disclosure law. With litigation and liability risk management, I counsel clients on taking steps today to win lawsuits tomorrow for products that you haven't even finished yet. It is important to build in safety into the products and services now, consider ways to eliminate possible bias, and think about legal issues that would come up in the future. My law firm also defends companies when they are sued. Our lawyers investigate accidents and data breaches and prepare for future legal proceedings. Finally, we help establish policies and procedures to govern AI and robotics development, procurement, and operation, similar to the privacy and security policies I write for clients in my data protection practice.

We also spoke with Adriana Sanford, International TV Commentator, Strategic International Consultant, AND Cyber Security Expert.

Adriana shares her expertise on the California Consumer Privacy Act. She says:

Much like the GDPR, the CCPA is expected to have far-reaching impact on businesses on a global scale. In contrast, however, while the GDPR applies to all EU citizens regardless of where they reside in Europe, the CCPA only protects California residents. The CCPA is expected to affect 1 in 8 Americans, but only while they reside in the state. The territorial protection of the GDPR is much broader; GDPR follows the EU citizen anywhere in Europe.

Although the law will not be effective January 1, 2020 and more clarification is coming, businesses should not take a wait-and-see-approach. Internal policies may need to

HEAR FROM STEPHEN WU AND ADRIANA SANFORD ON:

CISOs and Cyber Law, Artificial Intelligence, California Consumer Privacy Act, and More

be amended as compliance with GDPR and other current privacy laws may not adequately prepare some companies from the wide-ranging impacts of this new law. Businesses will need time to properly analyze and adjust contracts with service providers, conduct or review data mapping, as well as ensure that sufficient processes and resources are in place to adequately respond in a timely manner to consumer requests for access or deletion of their personal information. Personal information includes more information than what is required under GDPR. In addition to various types of internet activity ranging from searching and browsing to histories and tendencies, CCPA also includes inferences and attitudes, as well as interactions with online advertisements. Businesses need to start thinking about how CCPA requirements may impact their business operations.

CCPA will create a de-facto baseline standard for the US on data privacy controls and processes. California is the world's fifth largest economy and science and technology comprises a big sector of that economy. This may allow for more predictability of results in the future, particularly if Congress takes the lead or if other states begin to adopt a variation thereof.

Last year, many companies became consumed with GDPR and ensuring security and privacy were aligned. Businesses now need to focus their international efforts on a more territorial scale. They need to take a "glocal" approach to stay compliant. This may present a challenge for some businesses that have traditionally relied on a more simplistic approach.

The complex and rapidly evolving set of global data privacy regulations in the United States and foreign territories have radically changed the way that companies throughout the world handle data and their business operations. Within our changing global security landscape, several new foreign laws have an extraterritorial reach. There is a significant degree of frustration when demands from multiple regulators from different jurisdictions conflict with one another, particularly when there are hefty fines and potential liabilities for corporate executives, including criminal liability. Executives constantly need to re-shuffle their priorities.

I believe we need to be considerably more proactive in providing the private sector with guidance and direction when the laws conflict. The traditional 'reactive approach' leaves executives and general counsel exposed. There is currently is a lack of uniformity and predictability on the international level when laws do not mesh with one another. This scenario places multinationals and their employees in a terrible predicament. This has to change, as it is not fair to the executives or the businesses. The private sector has a significant challenge in this global space.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446