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