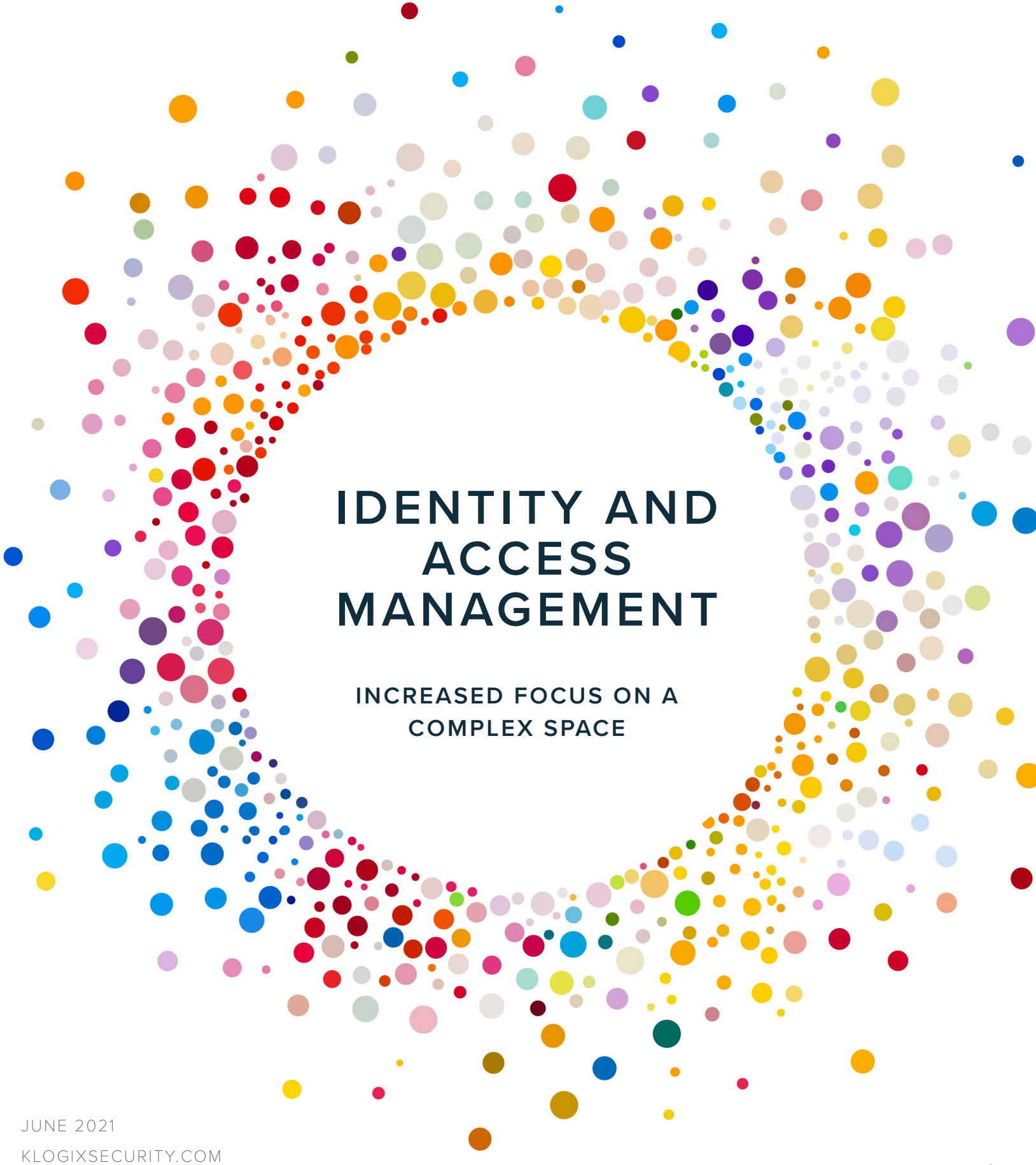
FEATS OF STRENGTH

A BUSINESS-FOCUSED CYBERSECURITY MAGAZINE



IDENTITY AND ACCESS MANAGEMENT

INCREASED FOCUS ON A COMPLEX SPACE

JUNE 2021

KLOGIXSECURITY.COM

617.860.6485

K logix

FEATS OF STRENGTH

IDENTITY AND ACCESS MANAGEMENT

JUNE 2021

FROM THE *Editor*

Dear Readers,

With Identity and Access Management (IAM) as our theme this issue, each CISO profile includes callouts about their approaches and thoughts on this complex and crucial space. My biggest takeaway is that IAM is not solved by technology alone, it requires a comprehensive, well-planned strategy. While IAM may be challenging, having a strong program demonstrates an opportunity for CISOs and security leaders to keep pace with business transformation and align with the organization's goals.

Here's what I'm excited about in this issue of *Feats of Strength*:

- Page 4 we profile Jerry Galvin, AVP Security, Northwell Health. Jerry discusses his strategic priorities, challenges he faces, and his approach to IAM at New York's largest Healthcare system.
- Page 6 we profile Tim Rohrbaugh, the CISO at JetBlue who discusses the challenges of justification and demonstrating the value of security. He shares how he approaches this through business context during Board or executive meetings, something many CISOs may struggle with.
- Page 6 read our profile of Robert Sherman, CISO at American Tower. He shares his top three strategic goals focusing on Zero Trust, ISO alignment and privacy.
- Page 8 we share the article – IAM: Making Sense of a Complex Marketspace. Read about the top challenges in addressing IAM as well as the three main areas of focus – Identity as a Service, Identity Governance and Administration, and Privileged Access Management.
- Page 10 read about Dwayne Steinway, CISO, Audacy Inc. who talks about the challenges of talent, budget, and visibility – something many security leaders may relate to.
- Page 12 we profile Chris Holden, CISO, Crum & Forster. Chris discusses his organizations move to the cloud, how security plays an integral part, and what his approach has been to ensure a smooth transition.

If you are interested in working with K logix on any of your IAM needs, from strategy to technology selection, please don't hesitate to reach out.

Kevin West

CEO, K logix

Magazine Contributors:

Katie Haug

VP Marketing, K logix

Kevin West

CEO, K logix

Kevin Pouche

COO, K logix

Marcela Lima

Marketing Manager, K logix

About K logix: Cybersecurity Advisory and Consulting Services

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.

We craft our services to address specific customer and industry challenges. One of the ways we do this is through our thought leadership, business-focused publication *Feats of Strength*. Through hundreds of CISO interviews, we extract trends in order to provide services that align business to information security.

www.klogixsecurity.com/feats-of-strength

Marketing@klogixsecurity.com

JERRY GALVIN

AVP SECURITY
NORTHWELL HEALTH

HEADQUARTERS: New Hyde Park, New York

EMPLOYEES: 76,000+

REVENUE: $13.4 Billion

Jerry Galvin began his career in defense, then worked in the entertainment industry for eight years before going into healthcare in 2006. In 2006, Galvin joined Northwell Health, New York State's largest healthcare provider and private employer. Northwell is home to 23 hospitals and more than 800 outpatient facilities, as well as the Donald and Barbara Zucker School of Medicine at Hofstra/Northwell, The Feinstein Institute for Medical Research, urgent care centers, kidney dialysis centers, acute inpatient rehabilitation, sub-acute rehabilitation and skilled-nursing facilities, a home care network, a hospice network, and other services.

Galvin was the fifth member of the IT Security team back in 2007 and over the years witnessed the team grow to 80 people today. He has helped mature and strengthen the cybersecurity program and currently oversees Operations, Engineering, Identity and Access Management, Mergers and Acquisitions, and Project Management with about 40 people on his respective team.

> *"...we have seen the cybersecurity theater change greatly in the last six years. The whole theory of ransomware, phishing, drive-by downloads, insider threats, and more, has raised the roof of cybersecurity ."*

With a rich history of experience in security, Galvin says one of the biggest changes is threats. He explains, "Back in the 90s, you would just worry about Backups and Antivirus in case a virus came in the door or a drive failed. Even as far back as the 2010s, that was still very much the case. However, we have seen the cybersecurity theater change greatly in the last six years. The whole theory of ransomware, phishing, drive-by downloads, insider threats, and more, has raised the roof of cybersecurity ."

THE ABCs OF STRONG SECURITY

Galvin says that IT security is as easy as ABC. 'A' stands for 'all systems go' meaning they do everything in their power so none of the systems are down because of a cyber threat. 'B' is always 'be secure' and focusing on secure solutions and secure technology investments. Northwell is the largest private employer in the state of New York, so focusing 'C' on 'customer service' means keeping patients and employees secure and happy.

He continues, "As far as strategic priorities, the perimeter has changed. We can no longer secure just the enterprise. You basically built this fortress so that nobody could get in and you were secure about who could get out. And now your model has

> *"As the organization grows and the technology grows, the ability to protect also grows. And we always say this is such a huge organization that if you were to buy a $1 pencil for every employee, you are looking at $75,000 and that's just employees."*

changed because COVID came along and said, hey, we need people that will be able to work from home and not just for a snow day. And we need patients to be seen from home, not just come into a doctor's office, not just coming to a hospital. So you really had to open up those restrictions to support that ease and still keep it secure."

One of their biggest strategies is segmentation. Galvin explains, "The whole idea of everything being up to date to the latest vulnerability standard is very hard when you're dealing with historical systems and data, and all the technology that floats within any enterprise (printers, mobile devices, IP cameras, etc.). And then understanding IoMT where you are able to classify what a medical device is in the environment. What is the standard operation that it should have. When can you sense that something has gone wrong, whether it's under attack, whether it's data leaking, or the usage is three times what you normally see. So all these things are happening on a day-to-day basis in real time. And we want to make sure we stay ahead of any risks that arise."

TACKLING CHALLENGES

In most healthcare organizations, including Northwell, the standard project process could take months or sometimes years because of the large scale of work involved. However, many of the COVID solutions at Northwell were implemented in one week or month because they had to move fast to stay ahead of the waves of patients coming through their doors.

Budget is another challenge as healthcare dollars get harder and harder to earn, which Galvin says means they become harder to spend. He says they have been embracing multi-year deals or enterprise agreements to better maintain their overall spend. He comments, "As the organization grows and the technology grows, the ability to protect also grows. And we always say this is such a huge organization that if you were to buy a $1 pencil for every employee, you are looking at $75,000 and that's just employees. We still have a lot of people on top of that, vendors and consultants and community physicians. So at any given time, we're trying to keep tabs on a hundred thousand people."

"But the only other challenge has always been any time we are making a pitch about a trend or a direction, sometimes you come to the table and the first time you are there, people are looking at you like this is a little crazy, why do we need to do this? And then by year two, when you are coming back to that table, they say yes, some people are doing it, but we are not ready yet. And then by year three, it is what, this is not done yet? We have been lucky enough to always be one step ahead of the next cyber attack wave. We made a decision in the fall of 2019 to select and deploy an EDR solution and we got it out to 70,000 endpoints over a five-month period. Then March 2020 comes and that is when everybody went home because of COVID-19. That EDR was the one tool that protected those laptops and people's homesteads the most," explains Galvin.

IDENTITY

"At Northwell, we look to identify everything from the user, to the device, to the application, to the data, to the location, to the timeframe. And there are probably a few more scenarios, but you really need to wrap your hands around every little piece of it because each one can give you intel. Obviously for years, people just monitored the user. Now, we can monitor if an endpoint is usually generating one gig of data a day, why did it generate 10 gigs on a Saturday. Or the location, this device is usually coming from site X, why is it now coming from another site? And even the timeframe, when you look at network detect and respond, I think the theory of just monitoring somebody for what they are doing today has now expanded to what have they done over the last seven, or the last 30, or the last 90 days? You just get bigger and bigger with your threat model so you can pick up the smallest risk," explains Galvin.

He continues, "In terms of challenges, I think for us as it becomes more and more standard in the environment, it's being asked to do everything and not all systems are there yet to support it. You have many different theories of what identity is to each vendor. We have one application where not only is the user controlled for what they can see and what they can do, but the device that they do it from is controlled for what they can see and what they can do. When you change that model, you're taking a level of that security and removing it. So, it becomes a higher risk. And then when you take somebody and say you are working remote, it makes it an even higher risk. There's always an ebb and flow of we're going to support this for the time being, but we're going to bring it back to a more secure model as soon as we can." Basically, Dr. No is Dr. Go, meaning if you just keep saying no, the customer will look to someone else to say yes. So, we do our best to be Dr. How. How can we make this work. How can we do it securely. And so far, that's been working for 15 years!"

TIM ROHRBAUGH

CISO
JETBLUE AIRLINES

HEADQUARTERS: Long Island City, New York

EMPLOYEES: 22,000+

REVENUE: $2.95 Billion (2020)

Tim Rohrbaugh began his career on the aviation side of the Navy, working in secure communication in the late 1980s and early 1990s. In his next role, he worked on projects related to air defense and Information Assurance and split his time teaching a course on securing systems at The Defense Information Systems Agency, enabling him to see both the practical side and the compliance side of security.

After moving into the commercial sector, Rohrbaugh worked in financial services as a CISO. He comments, "We gave consumers the first view of their credit file by bridging the three bureaus and then writing a contract with each of them to provide credit data to the named individual. We had to solve challenges like ID verification (having people prove who they say they are), some of the modern authentication schemes and the beginnings of what was to become the privacy sector. It was a very interesting time. I also spent six of those years on the board of the Online Trust Alliance where it gave me a view into the regulatory challenges, and I specifically looked at influencing what was, we hoped, national legislation around privacy."

He then worked for a compliance firm where he ran North America consulting services before they were acquired. After this, Rohrbaugh began his own virtual CISO company with JetBlue as a client. He took on an Interim CISO role and was shortly hired for the full-time role.

Rohrbaugh explains, "I stepped into JetBlue with a three-month Interim CISO contract and after about one month we found that it was a really good match between us. And they asked if I would apply for the permanent CISO role which started in late 2019. I think for me, I had almost forgotten how much I loved aviation because I had been out of aviation for a while. Being back in the middle of it and a strong positive culture like JetBlue, valuing passion and kindness, was exciting to me. That is what I found very appealing and unusual in today's commercial sectors."

He currently reports into the General Counsel and sees a strong benefit in this reporting structure. He finds it conducive because legal is focused on mitigating risk associated with compliance and regulatory, and Rohrbaugh and his team work to mitigate risk from a security perspective.

He says, "From 2003 to 2006, I reported to the CIO, the CEO, the COO, and then I moved under the General Counsel, and I found such a nice match of our objectives and also sometimes how we've characterized risk within the company. Everything that a CISO requires of IT is going to cause some amount of tension because it's going to add time to development, it's going to add labor cost, so we have to be very judicious about exactly what we're asking of them to do and doing it outside of the CIO reporting structure incentivizes both teams to work in a very cooperative fashion."

DEMONSTRATING VALUE

Like many security leaders, Rohrbaugh acknowledges the challenge of justification and leveraging a set of metrics to reflect progress and value of the security program. He believes anything presented to a Board or executives must be carefully curated to match the specific context of security risk for the organization. These could include technical and business requirements, controls, and objectives, to truly understand what the organization would benefit from, all from a risk reduction standpoint.

He explains, "I was brought up under the waterfall methodology. Unfortunately, many times we started and it took so long to complete a project, by the time we were done we chose the wrong technologies, or worse sometimes the mission changed. And once I was introduced to the Agile, I really fell in love with it as a product owner. I was also head of a product in the past, which is unusual for a CISO, but that experience was impactful in the way I look at security program improvement. I can tell you what I've tried to do is change the way security programs improve by focusing in on change in a way that's more akin to Kaizen - smallest change possible. What is the smallest change you can make that is going to improve security? And many times that means doing so by frustrating the criminal, by making it slightly more difficult, by giving you just a little bit more visibility. If you break down that work and improve the security posture with even four hours at a time of effort, effectively what you end up doing is avoid making big bets in one direction and knowing full well that criminality changes on a dime. Instead, we make a change, hypothesize how that's going to influence, then measure it and see if it does. And if it does not, well you did not invest that much time going the wrong direction. Instead, we try a different way. As a benefit for team members, no one is pigeonholed, as there is a chance for everybody on the teams to self-select based on the areas of the domains that they are most passionate about. And for the most part, they really enjoy it. I hope to tell you more about how it works out in the future, but right now all signs look that it's a good approach."

TECHNICAL DEBT AND NEW INVESTMENTS

Rohrbaugh says the airline industry is currently in a period of rebuilding since most airlines recently experienced significant budget cuts among other changes. In this moment of rebuilding, there is a significant amount of technical debt that exists.

He explains, "Every business is trying to adapt. As they are adapting technology, you make choices and sometimes when you try to actually produce the features and functionalities that are requested by the business, you take shortcuts, or you take solutions that may not provide the visibility from a security perspective. Maybe the visibility that you need into the transaction details to determine if something is normal or abnormal falls short. Sometimes we use technologies that may constantly require updating because they're being attacked or found flawed, whatever it may be, those choices are generally not the ones that you would make if you had enough time, or if you had timelines that were reasonable. So all of those little choices, which are not conducive to stopping misuse or preventing discovery or whatever it may be, must be addressed post release. Meaning, you must go back and clean those up. Technical debt is sometimes development, sometimes systems, sometimes features other times visibility. Right now, as we try to compete with required changes for the business such as new features and functionality, we have to sequence in some of these cleanup activities."

When investing in new products, Rohrbaugh believes the security product marketplace is filled with misconceptions and miscommunication. He comments, "I don't want to be constrained when I'm thinking about a solution to a bunch of checkbox features that were identified by X. I specifically don't like to see those marketing terms in any communication or sales pitch, I like product owners and sales staff to talk about what they're doing, why they are doing it, and what value they bring. But beyond that, for me it starts with humans, the people are how you solve the most complex problems, there's no product that's going to compare with the cognitive ability of a trained analyst. Yes, they might be able to react faster with automation, but you still need the experts to actually program or influence some of those rules."

IDENTITY

With his background working in the financial space, Rohrbaugh has keen experience around identity and says many people may struggle with understanding the difference between ID verification and authentication. He explains, "You have to have some amount of confidence in the person you have actually created the account for. They must prove they are who they say they are. Authentication on the other hand comes after this step, then you need to capture enough data on them so you can test later. You then have to exchange some mechanism for them to log on successfully with you."

He continues, "The techniques that we use today, with respect to ID verification are pretty strong in specific sectors e.g. the banking sector, but if you keep reusing these tools in other ways, you de-value them. I found in the past that somebody could go through an ID verification, and you would find that a criminal could pretend to be somebody else taking the test faster than the actual individual. And so you could almost pattern that it's more than likely fake or fraudulent, the faster the test, which is counterintuitive."

Behavior analytics is underutilized yet considered a key component of account monitoring according to Rohrbaugh. By having a strong focus on patterning normal and abnormal behavior, Rohrbaugh believes criminals will be more challenged to steal an identity or account and first determine what is normal behavior and operate in the confines of this normal activity, or risk being discovered.

ROBERT SHERMAN

CISO
AMERICAN TOWER

HEADQUARTERS: Boston, MA

EMPLOYEES: 6,000+

REVENUE: $8.04 Billion (2020)

Rob Sherman has worked at American Tower for over two decades, giving him the opportunity to build and grow the security department while strengthening both maturity and culture. He leads the team responsible for information governance, risk, and compliance, and delivers technology solutions across American Tower's global footprint.

American Tower provides the infrastructure for modern digital communications. Starting in 1995 with several thousand towers, they have grown their global portfolio to more than 200,000 communications sites. Sherman says, "In 2000, I did my job interview on a payphone. They told me - hey, we're building a data center. We think we need an email system. We've heard that you know Windows and Unix. Can you come help us out? So, I came on a six-week contract and I've stayed two decades. Today, we are a critical infrastructure provider for the major telecommunications providers on six continents, providing communications real estate, including ISO 27001 certified data center sites, worldwide."

> *"In 2000, I did my job interview on a payphone. They told me - hey, we're building a data center. We think we need an email system. We've heard that you know Windows and Unix. Can you come help us out?"*

Sherman's main responsibility is establishing security governance and overseeing how American Tower's global teams engage both in the internal organization and with their customers and vendors. He also oversees information security operations, which is different depending on the division of the company. In 2018, he worked with executive management to move the security function into the General Counsel's remit. He comments, "We wanted security to be seen as a function that, like legal, people needed to consider whenever they were making any change. We're a real estate investment trust and it made sense from a governance, risk, and compliance perspective to have the CISO function sit alongside legal."

ZERO TRUST, ISO ALIGNMENT, AND PRIVACY

Three years ago when Sherman saw some of the workforce beginning to work remotely, he began putting a larger focus on Zero Trust, which today is one of his top priorities. Not only did workforce changes impact this focus, but merger and acquisition activity became a focus for onboarding new companies quickly and securely. Sherman explains, "The next area for a lot of companies will be granular user privilege inside of Zero Trust. Once you've gotten comfortable that you're trusting the right people, the next step is figuring out how to make sure those

people can only access the very minimal set of data that they absolutely need."

Alignment to ISO 27001 is Sherman's next priority. This meets two goals, Sherman explains, "We now have customers asking us how we protect their data. Explaining to them how we've built our program in alignment with ISO 27001, along with the level of trust that comes with the certification, goes a long way towards answering that question. In addition, the Board is always interested in how we measure our cyber program. ISO 27001 controls provide an independent, third-party review which we can use to benchmark our program." He says by measuring against a framework, you are able to gauge how well your program is doing and track progress over time.

The third focus is around privacy, as countries around the world, including the United States, make traction on different laws regarding privacy. Sherman must ensure that American Tower is compliant with any new laws and they are able to respond to data requests timely and accurately. Sherman has a law degree, giving him a unique perspective and additional layer of skills and oversight to privacy regulation adherence.

OVERCOMING CHALLENGES

Luckily for Sherman and his organization, the impact of a newly remote workforce in 2020 was minimal. While many companies scrambled to set up their employees for working from home environments, Sherman and his team already had strong technologies and controls in place. He feels fortunate that this did not pose a significant challenge to his organization and security program.

However, staffing to build a top functioning team can be a challenge given the current job market conditions in this area, more so, Sherman says, than even one to two years ago. He comments, "We've leveraged good consultants to fill any gaps that arise, and that's fine, and works well to solve a point problem, but over the long term, the internal knowledge, or the relationships that an employee can build makes a real difference to the organization."

Another challenge is leading the team through constant change. Sherman says, "Identifying what the priorities are and making sure that you're picking the right ones is an ongoing exercise. Especially with the rapid evolution of threats, something that may be low priority today might become really important tomorrow. We rely on our strategy to form the foundation of our program, and we have a robust planning process, but included in that is a recognition that the nature of what we do in security requires the team to be ready for the unexpected, and that includes plans changing."

COMMUNICATING THROUGH STORIES

To communicate effectively during Board and committee

"Identifying what the priorities are and making sure that you're picking the right ones is an ongoing exercise. Especially with the rapid evolution of threats, something that may be low priority today might become really important tomorrow."

meetings, Sherman focuses on telling a story. He says, "I've approached each presentation as a story. I try to stay away from technical jargon and lots of words on slides. The Board wants to understand how you've identified risk, how you're managing risk, what they should be looking at over the next year, and how we measure ourselves. You need to be ready with the technical details if you are asked. But from what I have sensed, it seems doubtful that a Board member is especially eager for a CISO to do a deep-dive presentation on the latest data coming out of the SOC."

As a leader, Sherman says the only way cyber may become truly embedded in the culture is if everyone feels they have some level of ownership. He says, "People need to understand why the rules exist and feel like they own compliance. It's the way I've embedded it in my team. It's the way we've embedded it collectively across the company. Everyone owns a piece of company security."

IDENTITY

While internal identity presents one set of challenges, Sherman believes these are relatively manageable by ensuring the right people are on-boarded and they have access to what they need, and when they leave, that access is revoked. Since workflows similar to this have been implemented in organizations for some time, they are somewhat repeatable, requiring just minimal adjustments over time.

The new challenge for Sherman is external identities, specifically third-parties as digital transformation expands. He explains, "You have to consider suppliers, consultants, contractors, all these people accessing different pieces of your environment. And you need to build a robust platform to manage that and then maintain it. There's no one size that fits all. When building a program, we had to understand the unique needs of our different business and IT groups around the world. What we found were very use case driven, which makes it a challenge when you're building a strategy, because everyone wants to solve the use case and not focus on the strategy. We've been driving everyone to look at the digital transformation strategy and embed "Identity" in that strategy. Once we do that, implementing solutions for the use cases becomes much easier."

IDENTITY AND ACCESS MANGEMENT
MAKING SENSE OF A COMPLEX MARKETSPACE

By Katie Haug (K logix) and Marcela Lima (K logix)

Identity and Access Management (IAM) is a strategic goal for many CISOs and security leaders, and the need for strong programs is more important than ever before. The approach, program strategy, and technology investments around IAM vary based on an organization's specific requirements.

IAM is a structure of business processes, policies, and technologies that facilitates the management of identities. With an IAM framework and program in place, security professionals may control user access to sensitive and important information inside their organizations.

IAM CORE COMPONENTS

One of the top challenges around IAM is peeling back the layers and understanding what types of IAM technology to invest in based on an organization's specific requirements, technologies they already have in place, implemented processes, among many other nuances. Through K logix's Research Department, our experts have identified the three most prominent areas of IAM as: Identity as a Service (IDaaS), Identity Governance and Administration (IGA), and Privileged Access Management (PAM). We have defined them as:

IDENTITY AS A SERVICE (IDAAS)

IDaaS products synchronize identities within a business and across that business's relationships offering a single source of truth for identity management. These platforms also manage the depth of access, regulating not just who gets access but what is accessed and how.

IDENTITY GOVERNANCE AND ADMINISTRATION (IGA)

IGA platforms are "tools designed to manage digital identity and entitlements (access rights) across multiple systems and applications" (Gartner). Sitting at the nexus of business and security objectives, IGA platforms contextualize and then map the relationship between identities, users, access, and data.

PRIVILEGE ACCESS MANAGEMENT (PAM)

PAM solutions discover, monitor and regulate the creation, removal, storage and use of privileged credentials, facilitating visibility and control over privileged users, accounts, applications and systems. By centralizing privileged environments, PAM solutions minimize the risk of credential theft and privilege misuse

Since much of the language used to describe the three areas have some areas of similarity and overlap, we have created a Venn Diagram to showcase these areas (see graphic on page 11).

IAM CHALLENGES

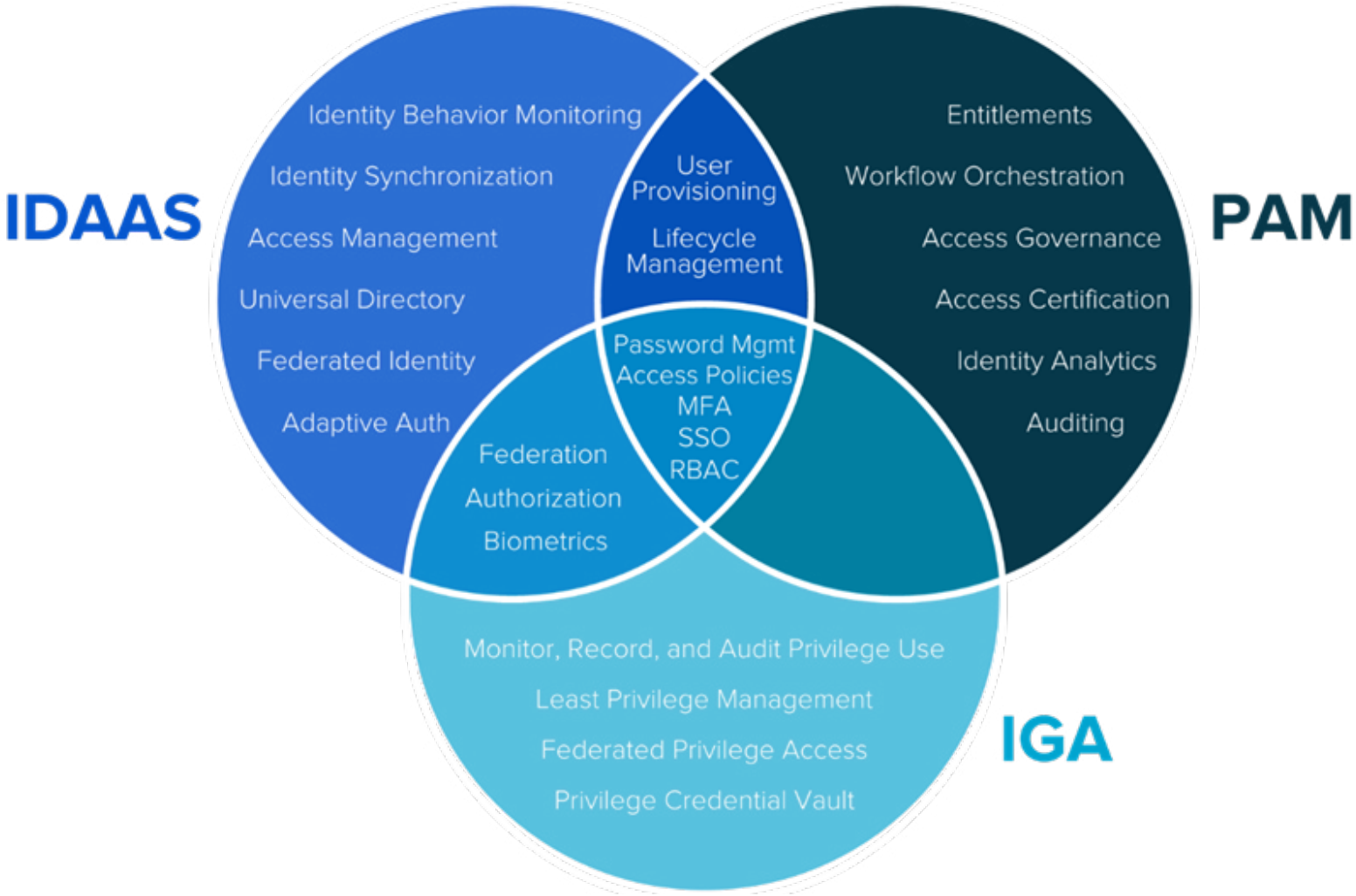
According to K logix CISO research, these are the top IAM challenges security leaders will be addressing in 2021 and beyond:

- Collaboration between technologies to deliver robust IAM capabilities
- Managing the impact of digital transformation
- Driving IAM standardization and automation
- Third party customers, their suppliers, consultants, contractors, etc. accessing different pieces of an organization's environment

A strong IAM strategy in place is paramount for organizations to address the transformative landscape of businesses. In a cloud-native world, identity is

IAM CORE COMPONENTS

Created by: Sydney Solomon, K logix Research Team



the new security perimeter. As the Zero Trust model becomes more widely adopted, security professionals are implementing IAM controls that grant users access to the network from anywhere while still maintaining centralized security.

IAM addresses the need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet rigorous compliance requirements. A crucial undertaking for any enterprise, IAM is increasingly business-aligned, and requires business skills, not just technical expertise.

Keeping the flow of business data while simultaneously managing access has always been a top challenge for security programs. The cybersecurity environment is ever-evolving, and the difficulties have only become greater with recent trends such as bring-your-own-device (BYOD), cloud computing, mobile apps, and remote workforces. There are more devices and services to be managed than ever before, with diverse requirements for access privilege. An IAM program must be business-aligned to ensure the organization can protect its sensitive information and allow it to move with the pace of digital transformation.

If you are interested in learning more about K logix's agnostic IAM research, please reach out to us.

DWAYNE STEINWAY

CISO
AUDACY, INC.

HEADQUARTERS: Philadelphia, PA

EMPLOYEES: 4,000

REVENUE: $1.46 Billion

Dwayne Steinway began his career in the Navy as an Intelligence Specialist, where he worked in IT with some aspects of security-related work. After leaving the Navy, Steinway was recruited to a consulting organization, where he was introduced to security practices within the consulting ranks. He had the opportunity to begin working on firewall and security infrastructure projects, with the rest of his security career blossoming from there.

After working in a variety of security roles across different verticals, he joined Audacy, Inc. in 2020 as their Chief Information Security Officer. Audacy, Inc. is a scaled, multi-platform audio content and entertainment company. Steinway explains, "I came to Audacy essentially as their first formal security leader. For nearly 20 years, I managed security teams across different industries, but never audio. Audacy came forward with this position and I saw that it is a very technology-rich organization. There is a lot of unique infrastructure here that you do not see in many other industries. It became a really appealing opportunity for me to dive into a new industry and apply the familiar trade, but in a new way."

His main responsibilities include the traditional security operations functions of threat management, risk management, and compliance. He is responsible for incident response activities, managing both the incident responders within his security team and externally, evaluating threats and addressing any security issues. DevOps and cloud infrastructure also fall under Steinway's responsibilities. He comments, "We have a large cloud infrastructure that supports our audio distribution infrastructure and other related applications. I am responsible for the digital infrastructure team that manages those environments in the cloud. It's a relatively new thing for CISOs. I know some CISOs who have an indirect responsibility or a close connection to DevOps. I am actually directly responsible for them. So, I have SecOps and DevOps under me, in addition to the compliance functions that come with being in the CISO seat."

SETTING STRONG SECURITY GOALS

Security hygiene is one of Steinway's top focus areas, because the infrastructure is fairly diversified across Audacy's 47 markets and the cloud. His team works on unification under one security program. He says, "Every market has a team of experienced engineers, and in each market they're responsible

> *"...our goal is to make sure that at the very least our security practices are normalized across the markets, where we are seeing the events the same way, regardless of the technologies that are in place."*

for those stations that they support, and they may have different preferences for the mix of technologies they like to use to manage that. So we have a variety in the technologies that support the business operations. For our security program, our goal is to make sure that at the very least our security practices are normalized across the markets, where we are seeing the events the same way, regardless of the technologies that are in place."

Another goal is ensuring operational practices follow specific security guidelines, and making certain that operational work, and especially enhancements, support the organization's overall security strategy and expectations. He explains, "That's why the DevOps integration has been crucial for me, because now I can understand and help in the development cycles, and ultimately support the need for better threat monitoring and secure code reviews for example in the places and pipelines where they make the most sense. I could be the one to advocate for these, and even go to leadership and request the funding to do it. It is a little easier when I am directly involved with the team. I would say it has been beneficial relationship both tactically and strategically."

TALENT, BUDGET, AND VISIBILITY

One of the most significant challenges for Steinway, and most other security leaders, is talent. He said he struggles to find replacements if someone on his team decides to leave the organization, especially now with virtual workforces. Steinway acknowledges the competitiveness of recruiting strong cybersecurity talent and being able to work remotely has increased competition in hiring.

Another challenge is budget, which almost all security leaders face. Steinway comments, "I have a very supportive executive team. They truly listen when we have needs and their trust is important to me. We've been very careful not to abuse that trust and we're always looking for ways to make us more efficient. We try to get the most out of our security technologies. We keep the toolbox as simple as possible, and especially pay close attention to the quality of the alerts and actions the tools are producing and make decisions accordingly. We try to be good corporate citizens from a spend perspective, but of course we do need to spend a little."

Visibility is also a challenge, especially with the diverse infrastructure at Audacy, Inc. Steinway says, "I have 47 individual markets each with multiple stations per market. Each station has its own engineering team. I must keep an eye on all of them. Visibility for me is key. I do not want to get caught by surprise in any way. That is where we've spent a lot of focus."

MEANINGFUL COMMUNICATION AND METRICS

Steinway approaches relationships with executives as mutually beneficial with strong alignment to demonstrate the value of security and gain buy-in across the organization. He meets with executives to understand their key initiatives and focus areas, then correlates security in a meaningful way to avoid being a hindrance.

He comments, "We are constantly looking for opportunities to say, hey, we have this capability already, or we have seen this in some other area. Between SecOps and DevOps, we are much closer to development activity and other changes that are taking place in the environment, and we will sometimes find opportunities to connect two business processes that may not have previously met. It is especially helpful to us to look for ways to simplify something, especially if it promotes collaboration and makes the business more efficient. That alone often reduces risk. We're not always focused on security doom and gloom."

To demonstrate progress to executives, Steinway leverages a standard set of KPIs that comprise a mix of the ISO and NIST frameworks. He makes sure they focus on showing progress around areas of improvement. These are also adaptable metrics, appropriate for a variety of executives or executive committees.

With regard to risk metrics, Steinway identifies action items or other items executives should be aware of, with a cohesive storytelling approach. After working in law and legal as a director of security, he learned that security metrics are not always about the technical details, but if you include a strong story that correlates to the other person's core objectives and goals, you gain their attention in a meaningful manner.

IDENTITY

For Steinway, Identity goes beyond accounts and systems. He explains, "It is also keys and certificates, it involves APIs as well as logins. It is not an individual credential, but also a system credential that should also be part of the identity program. In addition to general system access, we share data between systems, with partners, and all of that involves some type of authentication. So the identity program I'm trying to build would have some capability of detecting where credentials, of all types, are normally used and where or how they should not be used."

He continues, "It is more than just people and credentials. I would say there's two components. You must merge all of that credential data from disparate systems to create a picture. API keys, certificates, system accounts, right down to the number of dual-factor tokens that a user has registered. I want to get all that information into one place - like a business intelligence tool that can aggregate and enrich it similar to what organizations might do with customer data. Then I want to overlay some type of monitoring system on top of that so I can say these credentials are used in these places and that looks right, then baseline everything and look for anomalies. That's the perfect scenario that I'd like to build."

CHRIS HOLDEN

CISO
CRUM & FORSTER

HEADQUARTERS: Morristown, New Jersey

EMPLOYEES: 3,000+

REVENUE: $19.8 Billion (2020)

Chris Holden was interested in cybersecurity from an early age and decided to attain his Bachelor of Science degree in Cybersecurity and Information Assurance during college. After graduating, he applied for an internship with HP's Cyber Forensics department and was hired immediately, later finding out he was the only person who applied with a degree in Cybersecurity. After holding various cybersecurity jobs, Holden began working at Crum & Forster, a leading national property, casualty and accident & health insurer with a large, diversified specialty platform.

Beginning as Manager of Cyber and Information Security at Crum & Forster, Holden moved to Associate Director, before becoming the Chief Information Security Officer in 2020. Transitioning into a leadership role meant stronger alignment with the business. He explains, "The biggest change is the exposure to the business and how to efficiently and effectively implement security with the lowest impact possible. When you're early in your career working as a security engineer, your goal is to implement the most robust security control first, taking care to ensure it doesn't inhibit the business from being operationally effective."

REMOTE WORKFORCES AND CLOUD MIGRATION

Moving workloads to the cloud is a top strategic priority for Holden, with remote work exposing many new considerations for security. The organization already had significant initiatives to move to the cloud, yet when virtual became the new normal in 2020, Holden says it sped up the company's timeline. He comments, "We saw it was much easier to realize the return on investment of moving to the cloud while being remote. It provided us a lot more flexibility, as well as a better experience for our employees. We were fortunate that we had pre-existing infrastructure to securely support remote employees."

Another initiative Holden and his team are working on is the planning around shared office space. Crum & Forster is in a unique position where it owns several of its offices around the country, and because the employee base, in large part, works remotely, it has opened some of that floor space to other businesses in the local areas. With its strong cybersecurity guidelines in place, Holden says he and his team are mindful of all the considerations and, importantly, are ready for having nonemployees working within the company's walls for the first time. He says, "How do we segregate or prevent access to sensitive data, whether that's physical files and the file cabinets that we have around our office, or more strictly enforcing clean desk policies for some of our users, but also who can connect to the network and how we're facilitating those connections as well. I think those are our biggest and most interesting initiatives right now."

One challenge Holden says he faces is around designing and implementing many newer controls in ways that are feasible and adoptable. Holden notes at the forefront of all the company's and his team's initiatives is to build a culture of security, enabling Crum & Forster's entire workforce to conduct business in a highly secure manner. Since historically that was done when employees were all working in an actual office, the tools are now changing, including a portion of the company's technology, to bring colleagues into the new era of cloud and remote work. Employees are now working differently and interacting with different applications and systems. He knows his team is up to the task of getting a significant portion of the company's 3,000-plus employees used to securely working remotely.

BUILDING A STRONG CULTURE

For Holden, culture building starts with hiring. His main focus when hiring is looking for individuals who are passionate about cybersecurity, because they will end up being the ambassadors of the security program. He says, "They are the ones that are going to be designing the controls and implementing the change. They are the ones who are going to be working with our employees and our business groups when issues arise. If they are not excited about it, our stakeholders are not going to be excited about it either. That's the key driver there."

He continues, "The other thing that we have done is more frequent employee outreach. We initially started this a couple of years back, during Cybersecurity Awareness Month in October. Outside of our standard training, we often have speakers come who are focused on cybersecurity. We have had a couple of retired and current FBI agents talk about the threat landscape, not only from a work perspective, but also in their personal lives. We've also done more interactive training and "Ask a Cyber Expert" program, both of which have been huge successes."

This type of outreach has been received well by the workforce, and something the company is coordinating into a longer-term approach. Holden says they are not just doing this during the October Cybersecurity Awareness Month, but rather making regular outreach efforts and interacting with various business groups. This is done both formally and informally to provide training and feedback throughout the year on a consistent basis.

MOVING TO FINANCIAL-BASED RISK REPORTING

To track the progress of the security program, the first thing Holden did was align controls to an industry-recognized cybersecurity framework. This is key for measuring maturity and identifying gaps, to continually measure growth and make a strong impact on the organization. His latest efforts have moved to quantifying risks, which Holden says can be a cumbersome and incredibly time-consuming task. He comments that at the end of the day, "You often see it gets to a point of analysis paralysis, where you are putting a large amount of time into the analysis and defeating the purpose of identifying what the real threats and risks are."

Holden says he is seeing a significant shift throughout the industry of moving to financial-based risk reporting, which speaks to executives in business terms. He explains, "I've shifted the approach; I'm looking for two key things in all of my metrics and KPIs. One is the dollar value, and what we have found is that it is not always easy. The second most important thing that I put into perspective though, is time. Those are the two key things that the business can relate to. Time and money. From a time perspective, I am not necessarily concerned about the thousand vulnerabilities that have come up on my latest scan report, but how many of those vulnerabilities have I missed the SLA on remediating? Those are very tangible to illustrate how effective we are as a program."

IDENTITY: KEEPING IT SIMPLE

Holden approaches identity with a core focus on keeping it simple. He reveals, "There's a lot of potential for an identity and access management program to be a very bad experience for both your employees and your clients. Keep it as simple as possible. This will help with future provisioning, user access reviews and audits and a cleaner experience for your stakeholders. It is also critical when implementing to keep in mind who your stakeholders are. There have been a lot of great developments recently in providing flexibility with how they choose to prove their identity and access your applications and systems. Supporting a few different options will ultimately provide a better user experience as well as increased security if your users don't see authentication as a hassle."

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485