FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE

LESSONS LEARNED

CISOs share how they measure success not only in achievements, but in lessons learned from an unprecedented year.

DECEMBER 2020
KLOGIXSECURITY.COM
617.731.2314

K logix

FEATS OF STRENGTH

LESSONS LEARNED

DECEMBER 2020

FROM THE Editor

2020 has been an extraordinary year for information security in the face of digital transformation, remote workforces and shifting priorities. This year CISOs were focused on accelerating cloud migration while securing data and maintaining transparency throughout the process. They were required to move rapidly, make concise, business-driven decisions and consider the bigger picture with every move they made. Information security became more integral than ever before and security teams with strong leadership and foundational strategies led the way to secure remote workforces and protected organizations.

Some CISOs saw the impact of COVID as a hindrance to productivity and resources, while some identified it as an opportunity to demonstrate their ability to positively impact the business. They worked alongside their business counterparts, discussing what immediate shifts in priorities needed to take place and communicated clearly to the entire organization.

New challenges arose such as assuring identities of remote workers, the limits of VPNs and productivity decreases due to bandwidth issues, among many other things. The change in online human behavior has significantly increased the attack surface and vulnerabilities. However, CISOs and their teams worked tirelessly to establish modified or new strategies to address these challenges. Many looked at these challenges holistically rather than solving point problems, ensuring overall corporate vision and goals were addressed.

On page 6, Deborah Wheeler, CISO, Delta Air Lines says, “The biggest shift in 2020 has been the drawdown of capital plans and strategic projects, and the pivot to the cloud. As a result, we’ve had to look at cloud specific security strategies, and initiate a training program to ensure that our people have the skills and training required to migrate, containerize and modernize our applications to reside in a public cloud. As we move into 2021, this migration to the cloud and the security challenges it brings will be our top focus and priority.”

For CISOs working at cloud-driven organizations, many said the transition to a remote workforce was mostly seamless. These CISOs felt prepared with limited strain on their team and resources, and avoided the challenges of on-prem datacenters and limited VPNs.

On page 9, Andrew Smeaton, CISO, DataRobot, says, “From a team perspective, we didn’t skip a beat to be honest. The team was fully functional with very little productivity loss. From a security point of view, it made us fast forward some of the strategic partnerships that we had already gone forward with which gave us more security intelligence. We also focused on education around the pitfalls of working from home, concentrating on the executive team to make sure they had secure networks to work from.”

Keyur Shah, Deputy CISO at Sema4, says his cloud-driven organization was prepared for remote workforces and on page 11 he says, “We have made ourselves more resilient to this challenge as our security team has a stronger playbook to analyze remotely. The strong collaboration between IT and security also plays a key role…”

Looking into 2021, we are excited to hear from our CISO community about ways they continue to innovate and make an impact on their organizations.

Kevin West

CEO, K logix

Magazine Contributors:

Katie Haug

Director of Marketing, K logix

Kevin West

CEO, K logix

Kevin Pouche

COO, K logix

Marcela Lima

Marketing Coordinator, K logix

About K logix:

We provide information security strategic offerings, threat and incident capabilities, education/awareness, and technology services. 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 150+ 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

617.731.2314

DEBORAH WHEELER

CISO & VP
DELTA AIR LINES

HEADQUARTERS: Atlanta, GA

EMPLOYEES: 91,000+ (2019)

REVENUE: $47.01 Billion (2019)

Throughout Deborah Wheeler's extensive career in information security, her responsibilities and skillset have evolved and shaped her approach to growing successful team members while garnering respect from business leaders. She held three CISO roles in the financial sector before moving to her most current role as CISO of Delta Air Lines.

As CISO of Delta Air Lines, Wheeler is responsible for establishing the vision, strategy and execution plan for the security program, overseeing the program's goals and objectives, reporting to the Board and senior leadership, and staying current with the broader security industry and regulations, to ensure that Delta stays current with security solutions to address emerging threats, and stays on top of compliance with regulatory expectations.

> *"You cannot be a partner to your business if your answer is always 'no'. You have to find a way to get to 'yes' without compromising your organization's security."*

When first joining Delta Air Lines, Wheeler ensured there would be an opportunity for her to improve the state of security in the organization. She gravitates towards opportunities where the organization either hasn't developed a security program or what they have in place is inadequate to meet what they feel their needs are. She also focuses on a strong relationship with who she reports to, to ensure the advancement of the security programs, objectives and strategy.

2020: PIVOT TO THE CLOUD

Wheeler comments, "The biggest shift in 2020 has been the drawdown of capital plans and strategic projects, and the pivot to the cloud. As a result, we've had to look at cloud specific security strategies, and initiate a training program to ensure that our people have the skills and training required to migrate, containerize and modernize our applications to reside in a public cloud. As we move into 2021, this migration to the cloud and the security challenges it brings will be our top focus and priority."

Since Wheeler ensured she would have a good reporting relationship and strong communication with her CIO, security was at the table when conversations began about moving to the cloud. Security was armed with confidence to express concerns and ensure the role of security was recognized as a support to the business and business objectives. Wheeler says, "You cannot be a partner to your business if your answer is always 'no'. You have to find a way to get to 'yes' without compromising your organization's security."

Wheeler says security moving or migrating to the cloud is something many security practitioners may not be prepared for because the language of the cloud is different. She recommends building a basic understanding of what the cloud is, what the services are, and how to implement the same level of controls from the on-prem environment into the cloud-based environment. She believes it is important to understand what aspects of those controls you have control over versus what is being provided and managed by the cloud provider.

By leveraging partnerships and relationships with strategic partners, Wheeler's team benefits from strategic help in cloud planning and migration. She also encourages her team to go out and learn from resources that meet their specific learning styles. She explains, "I've really encouraged my team to look at what's available online. There are so many fantastic resources available online. We've done a lot of online training, a lot of self-paced training with tools that are available to us from within Delta, as well as with tools and educational opportunities available outside of Delta. There is some aspect of being a professional in IT of continuing to learn and having that continuous education mindset. It's critical to your role and your value as an IT professional, whether you love the company you're in today or whether you plan on moving to a different company or changing roles, to have a mindset of continuous learning in order to stay current with everything happening in the IT space."

POSITIVE-FOCUSED LEADERSHIP

Wheeler takes five to ten minutes every day to think about what her team may be going through, given the complex challenges posed by 2020. She comments, "Having a positive attitude day over day is a skill in and of itself that is little valued, but highly necessary when everything around you and your team appears negative and challenging. Our day in and day out job content is little changed from what we were doing before; we're just doing it now with the added distractions of being at home, working reduced work weeks, and therefore at less pay than we were before. And we don't have the advantage of "watercooler" time with peers and coworkers. So leading through this year has made me realize the value and importance of being positive for the sake of others."

She works hard to understand challenges faced by her team members and focuses on remaining positive to lift them up. She finds inspirational sayings and other people who have unique ways of looking at negative situations and turning them into something positive to be inspired by the good things that are happening.

CLEARING THE VENDOR CLUTTER

A source of frustration for Wheeler, along with the vast majority of CISOs, is finding the signal through the noise when it comes to security vendors. To do so, she leverages her peer network and understands what has worked well for them. She never rushes to the latest and greatest products that just hit the market, but instead sees what works and what has acquired a following. With an influx of venture capital funding flooding the market, Wheeler believes in seeing who the viable products are that amass significant customer bases without getting acquired.

> *"Having a positive attitude day over day is a skill in and of itself that is little valued, but highly necessary when everything around you and your team appears negative and challenging."*

Wheeler's team is comprised of exceptional subject matter experts who she relies on to stay close to the market for their respective subject areas and to bring forward anything they feel is a product or tool they should seriously consider.

Wheeler is not big on point solutions; she instead focuses on platform-level solutions. She explains, "If a vendor requests time to review a point solution, my answer is always going to be 'no'. I've got to focus on solutions or platforms that can solve multiple problems if I'm going to make a multi-million dollar investment."

LOOKING TO THE FUTURE

When looking into 2021 and beyond, Wheeler comments, "I think strong identity, access and authentication management solutions will always be a top industry trend; reliability strategies and solutions in the face of so many ransomware attacks is trending high right now and of course cloud and cloud security offerings. So many companies made decisions to move their IT assets to cloud in 2020 and as a result, vendor offerings and solutions that are both cloud-based and can address multi-cloud environments have surged in popularity."

ANDREW SMEATON

GLOBAL CISO
DATAROBOT

HEADQUARTERS: Boston, MA

EMPLOYEES: 1,100

REVENUE: Undisclosed

Andrew Smeaton is a career security professional with over 25 years of technology experience working in government, banking, healthcare and now his most current role as CISO for DataRobot, the leader in enterprise Artificial Intelligence (AI). Smeaton comments, “DataRobot is known for its unique approach to AI and machine learning that appeals to a broad mix of users, including data scientists, business analysts, data engineers, software developers and executives. Our proven combination of cutting-edge software and world-class AI implementation, training and support services empowers any organization - regardless of size, industry or resources - to drive better business outcomes with AI. Some of the very best data scientists in the world work for DataRobot. Certainly, some of the smartest people I’ve ever worked with. That makes it so interesting for me and our team, we are working with giants in the data science industry.”

Smeaton has a passion for building world-class security programs while focusing on business enablement. He says, “I must say, I love security, it’s the first thing I think about when I wake up. I truly love what I do. Over the years, offers regularly presented themself to serve as a CIO, but I have never been interested. My passion is security and that’s where my career started, working for the government 32 years ago. Over the years I think my Liverpudlian sense of humor, constant willingness to learn and passion has postured me in good stead.”

COMMON SENSE APPROACH TO STRONG SECURITY

Smeaton takes a common sense approach to security, with efforts equally focused on doing the basics flawlessly, recruiting a strong workforce, utilizing artificial intelligence, security data analytics, leveraging automation, ensuring there is a sound security architecture and providing a platform to be successful.

Since becoming CISO over 16 months ago, Smeaton has reviewed the organization’s risk model, created a culture where users want to engage proactively, improved processes and worked across relevant departments to attain DataRobot’s strategic goals.

Smeaton comments, “As our team has grown, so has the need to formalize and mature existing security, compliance and privacy processes that reach throughout the organization. Our entire company has been incredibly supportive of our initiatives to drive security forward over the past year and we plan on taking that into 2021.”

He continues, “We have worked very hard to build strong relationships across DataRobot and have seen huge wins from this teaming. We have become closely aligned with our Engineering teams, Human Resources, Sales and Legal staff and we plan on focusing even more on this in order to deliver the best possible products to our customers."

FOCUS ON AN INNOVATIVE TEAM

Keeping pace in a fast-moving environment means Smeaton must always focus on business alignment, innovation and his team's success as top priorities.

Smeaton comments, "Strategically, I think one to two years ahead while recognizing how to stay aligned with business objectives. It's very important that a CISO has a seat at the executive-level during strategic or business discussions. As a CISO, relationships are incredibly important. The language of the boardroom is business language, so I always talk in business terms and about the cost of business."

As a leader, Smeaton measures himself by the growth of his team, and believes there is nothing more rewarding than helping other people grow and inspiring them to reach new goals.

He says, "The first step in driving innovation is to build an innovative team and find rock stars. Sometimes you must recruit, other times you can find natural rock stars within your organization. It is important to identify and recruit innovators and people who think outside of the box, because that is what it takes to be great at security. These are the big ideas people, who think beyond incremental innovation and have broad interests, diversified backgrounds and present not only their hard skills, but also their soft skills. I identify mavericks and non-conformists, people who are not afraid to break the rules and existing paradigms."

The next step to an innovative team is creating open, honest dialogue. He explains, "I create an environment where people are not afraid to blow things up and start again. As a CISO, don't be scared to be challenged and open to thinking differently. CISOs shouldn't dictate to their team, they should create an environment where every idea is utilized in one way or another. Every year I tell my team that it's a blank piece of paper and to think differently. Individually, we come up with ideas, and together we evaluate as a team and prioritize initiatives."

The security team at DataRobot is comprised of experienced professionals who have worked across the globe in a multitude of sectors. Smeaton ensures he allocates budget for innovation to provide his team the time to work on projects and their ideas. He states, "After you've done all the hard work in hiring and creating the right environment, the next step is exhilarating; it's letting the horses run. Of course, as a CISO you still have to manage, but as a leader you have created the environment for success."

SEAMLESS TRANSITION TO REMOTE WORKFORCES

When workforces went remote this year, DataRobot was poised for success as a cutting-edge SaaS organization. Smeaton says that when their employees began working remotely, they took their laptops home and had the same work environment as they would in the office. While many organizations struggled with on-prem solutions, datacenters or limited VPNs, DataRobot was seamlessly prepared.

Smeaton explains, "From a team perspective, we didn't skip a beat to be honest. The team was fully functional with very little productivity loss. From a security point of view, it made us fast forward some of the strategic partnerships that we had already gone forward with which gave us more security intelligence. We also focused on education around the pitfalls of working from home, concentrating on the executive team to make sure they had secure networks to work from."

LOOKING FORWARD: TOP SECURITY TRENDS IN 2021

Smeaton focuses on these trends to look out for in 2021:

Ransomware will change yet again. Smeaton says The Department of Treasury and FBI have indicated that ransomware funds are ending up in the hands of individuals and regimes sanctioned by the United States. He believes this will force the underground economy to shift their tactics and not necessarily run adversaries out, but we may see yet another evolution in ransomware.

Proprietary CPUs will help level the playing field. With the introduction of Apple's M1 chip and Microsoft's Pluton chip, a huge leap in more control and greater security will take place according to Smeaton. He says there will be less interdependence on vendors, undoubtedly leading to greater software security.

Zero Trust. Another top trend for Smeaton is Zero Trust, rooted in the principle of "never trust, always verify". He says Zero Trust is designed to protect modern digital environments by leveraging network segmentation, and organizations should prioritize focusing on building a strong Zero Trust program.

Location-agnostic security operations. Smeaton says these should be designed to support customers everywhere, enable employees everywhere and manage the deployment of business services across distributed infrastructure.

Hyper automation Security Orchestration, Automation and Response (SOAR). According to Smeaton, SOAR helps accelerate incident response and maximize security tools while standardizing processes and should be another focus area for security leaders.

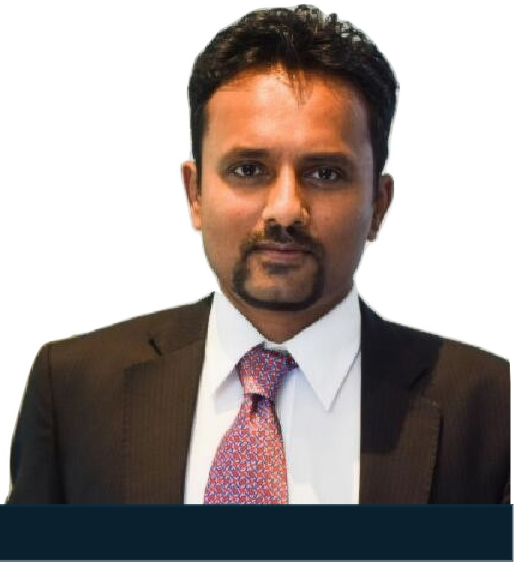
KEYUR SHAH

DEPUTY CISO
SEMA4

HEADQUARTERS: Stamford, CT

EMPLOYEES: 1,000

REVENUE: Privately Held Organization



Having started his career in India, Keyur Shah moved to the United States in 2000. He has been in the security field for over twenty years and has worked with multiple organizations gaining valuable experience.

Shah's work has not been limited to working in the corporate sector. He has actively worked in the development sector, helping children from the lowest economic strata with their right to education and good health. Shah volunteers for Vibha, a nonprofit organization and has been awarded the Lifetime President's Volunteer Service Award by the President of the United States. He practices mindfulness by meditating regularly and believes in spreading Metta – loving kindness.

As a security professional, his work in the United States started at PricewaterhouseCoopers as a Management Consultant, then moving to T-Mobile as a Senior Security Architect before spending thirteen years at Citigroup as a Global Security Manager.

After working in larger, formal corporate settings, Shah was excited at the opportunity to join Sema4, an independent company spun out of Mount Sinai Health System. The organization is a patient-centered health intelligence company focused on treating and preventing diseases by aggregating and analyzing data. Shah was presented an opportunity to help build the security practice of this cloud-driven organization from its infancy.

Shah comments, "Based on our intelligence-driven analysis, we provide better guidance to individuals to reduce their chances of getting sick. For this magic to work, we have designed and developed advanced technology platforms that have multi-skill, bioinformatic pipelines and predictive modeling. This high-performance computing platform is pretty scalable but has its own unique requirement for security network and design."

WEARING A DESIGN THINKING CAP

Shah always plans for future innovation and focuses on continuing to improve the maturity of the security program. He explains, "Within a few weeks of starting at Sema4, I realized that the biggest problem was not having a framework. After reviewing the assessments from a few different security audits, it was clear to me that we needed to align ourselves with the NIST Cybersecurity Framework with a crosswalk on HIPAA because we are in the healthcare space. I wanted to fortify our security with that framework in mind."

He continues, "Being a cloud-focused company, I have to rely a lot on automation and it really helped that I had a strong partnership with my CISO, Shay Hassidim and once we agreed on a framework, we had to work on aligning existing and new policies. At that point I was fortunate to find a good partner with my Director of Compliance, Kathleen Uzilov."

FOCUSING ON INNOVATION AND STRENGTHENING SECURITY

Two of Shah's priorities are evaluating emerging technologies and improving their Security Operations Center (SOC) and incident response capabilities.

Shah says by investing in and understanding new technologies, they continue to improve their security posture, especially as the cloud continues to evolve. When investing in a new technology, Shah does extensive research and relies on peer groups to understand their specific experiences and uses cases with certain products.

His second focus is around their SOC and strengthening the incident response function. He explains, "The way I like to look at it, it's not just the incident response team. If you just rely on the incident response function, then it's really a reactive mode. So, I try my very best to make security a larger part of the DNA of our company."

He continues, "Human centered design thinking means cultivating empathy with the people you are designing for. So, trying to understand what their problems are and making sure they see security as a valuable resource rather than a hindrance. When it comes to my team, for any incident response, I tell them to take a similar approach. It is all about empathy and building trust. Because if you have a culture that people care for each other, you'll have success as a team even when you are investigating a security incident."

MINDFULNESS AND OVERCOMING 2020'S CHALLENGES

As a cloud-based organization, Sema4 was already built for employees to work from anywhere. When remote work became the new normal, a new challenge emerged when dealing with incidents, because it was much easier to look at an affected device or somebody's laptop in person. Shah says, "We have made ourselves more resilient to this challenge as our security team has a stronger playbook to analyze remotely. The strong collaboration between IT and security also plays a key role – thanks to our SVP of IT, Anatol Blass."

Looking into 2021, Shah says the most important thing to think about investing in is threat intelligence, automation, and zero-day protection. He also explains that artificial intelligence and behavioral analytics are key to improving and maintaining a strong security program.

Shah says it is important to understand that staying secure is an infinite game. He explains, "The only way to win is to keep making yourself better by building a resilient organization, as threat landscape will keep evolving. There are no winners and losers, I believe in the why - the purpose of building technology platforms to support a healthier future for human beings, which is the vision of Sema4."

When thinking about the flood of complexities from 2020, Shah says, "I am dedicated to practicing mindfulness and meditation. We have no control of the storm, it may be COVID-19 or it may be a potential attack, but if we can develop the practice of self-awareness, I think with trust and teamwork, we can ride through it."

> *"The way I like to look at it, it's not just the incident response team. If you just rely on the incident response function, then it's really a reactive mode. So, I try my very best to make security a larger part of the DNA of our company."*

HOW TO MANAGE A REMOTE WORKFORCE

AN EXTRAORDINARY YEAR AND OPPORTUNITY FOR CISOs

By: Katie Haug, Director of Marketing, K logix

When we set out to write this issue of the magazine our main goal was to understand the lessons learned from 2020 from the perspective of our CISO community. To no surprise, almost every CISO we spoke with this year since COVID started, told us their biggest challenge was managing the newly remote workforce. Many of them said their now almost 100% remote workforce was unprecedented, with some feeling prepared while many scrambled to adjust.

Scalability was one of the biggest concerns, with CISOs rapidly creating more robust remote infrastructures. Capacity upgrades with additional VPNs was crucial to address employees now working from home. With intrusion prevention and detecting potential DDoS attacks top of mind, security teams ensured the home networks of their employees were secure and stable.

The additional layer of developing new security controls around a more secure remote infrastructure required extensive amounts of time for some security teams.

One of the most important elements in undergoing a rapid transition to a secure remote workforce is establishing a strong strategy to support the business and adhere to security protocols. We spoke with many CISOs who felt their organization had a strong foundation already in place, resulting in a steadfast plan of action.

For organizations who were already 100% cloud-based, many said there were some concerns around scalability, but overall they were already prepared for an entirely remote workforce. These CISOs had an advantage and many of their peers relied on them for advice.

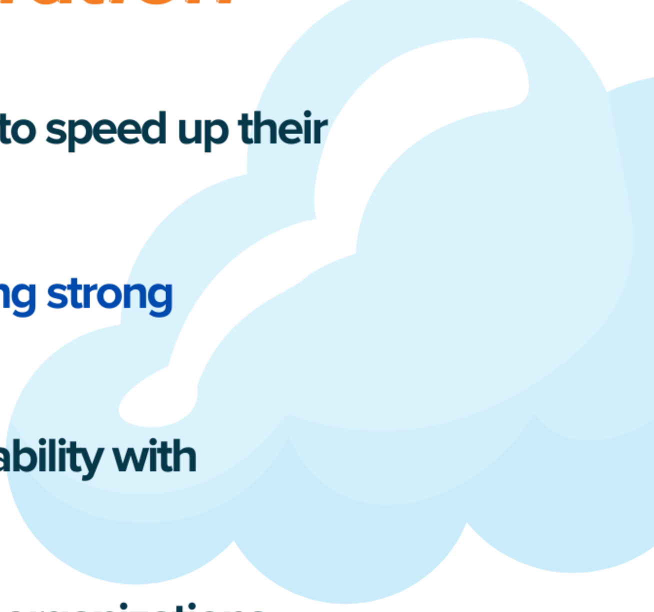
FOCUS ON EDUCATION

Educating the entire workforce was something almost every CISO we spoke with said they had to focus on more than ever before. Many employees had not used remote technologies before or have limited knowledge or practice with multi-factor authentication. CISOs had to come up with training and education plans to communicate with every employee and make sure they were given adequate instruction on making these technical adjustments. Many CISOs already had security awareness and training programs in place, but had to shift education topics that were more relevant to their workforces during COVID.

Not only did the non-security or non-IT employees require training, but many security teams had to ramp up their staff trainings. These trainings included cloud, mobility management, remote connectivity tools, among others, to help support their new strategies and focus areas.

On the following page, we have included some trending stats collected through the multitude of CISO interviews we conducted this year.

Accelerated Cloud Migration



80% of CISOs we spoke with said they had to speed up their transition to the cloud

Top of mind for many CISOs is: implementing strong cloud-specific security strategies

Almost 100% of CISOs had to focus on scalability with additional VPNs and capacity upgrades

Only 20% of CISOs working at cloud-based organizations considered the transition to a remote workforce "mostly seamless"

Education & Training are Top Focus

90% of CISOs said they invested more time and resources in training their newly remote workforce

Top employee training topics for 2020:

- **How to use remote technologies, using multi-factor authentication, and navigating video and communication programs they had not used before**

Investing in security staff training around cloud was a focus for 60% of CISOs, including mobility management and remote connectivity tools

*These proprietary statistics come directly from K logix CISO interviews conducted in 2020

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

LESSONS

LEARNED

FEATS OF STRENGTH DECEMBER 2020 K logix