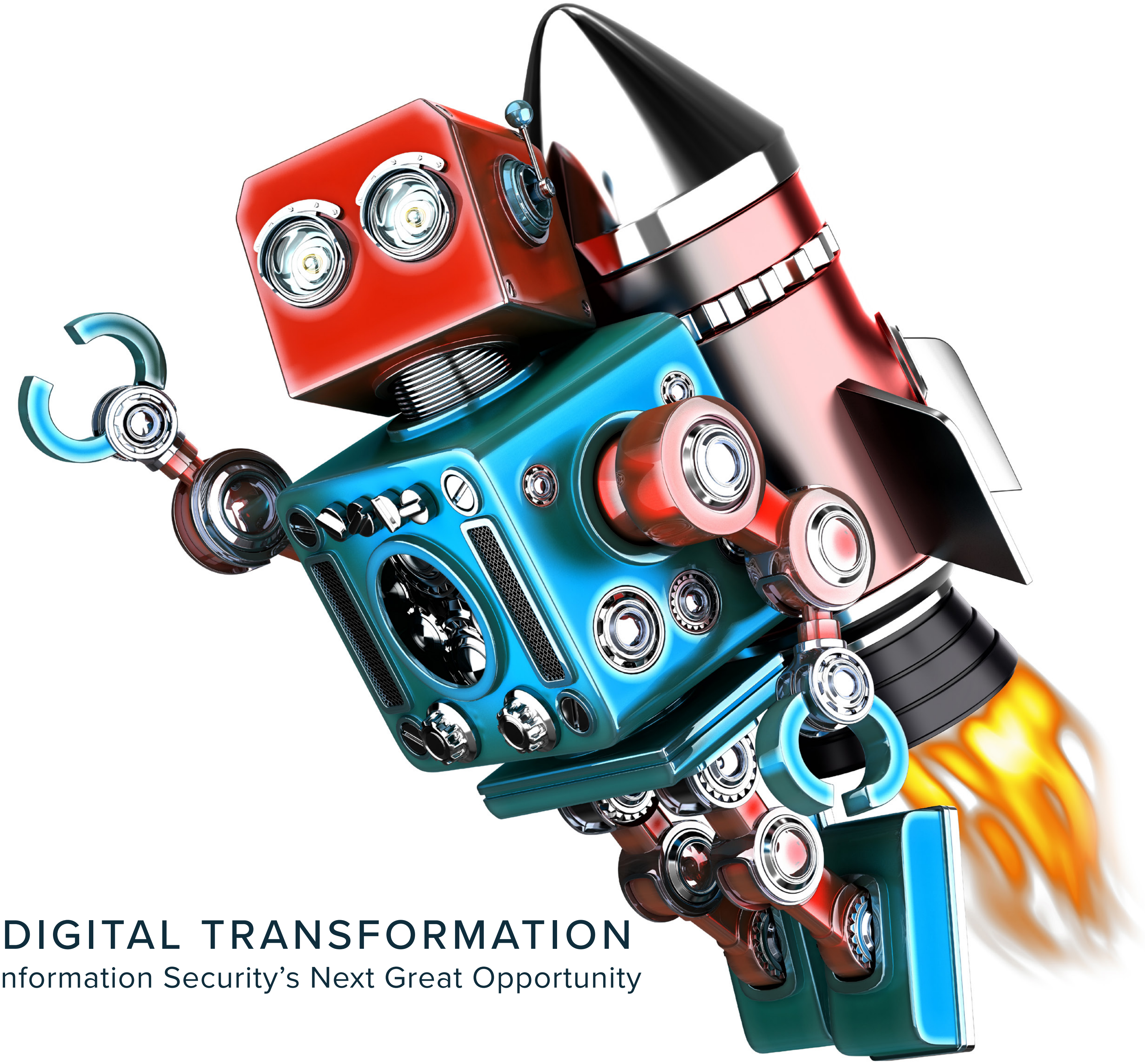
FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE



DIGITAL TRANSFORMATION

Information Security's Next Great Opportunity

June 2017

K logix

Earning the right to be confident
in information security

WWW.KLOGIXSECURITY.COM

888.731.2314

FEATS OF STRENGTH

JUNE 2017

PROFILES IN CONFIDENCE

FEATURES

LETTER FROM
KEVIN WEST
CEO

CISOs Next Great Opportunity

Showcasing CISOs to allow them to share their story, leadership experience, challenges, and goals, has always been our priority with Feats of Strength magazine. After three years, we've spent more than 100 hours interviewing 100 CISOs. We consider this to be a major milestone for K logix and for the CISOs who participate in our profiles and forums.

This milestone sparked us to commission a study to take these 100+ hours of interviews and extract key trends. Our goal is to share the results with our security leadership community and help make an impact on their programs.

Two main CISO goals emerged as top priorities, these include:

- Security closely aligned with business goals
- Security to be considered a competitive advantage

We also identified the major challenges facing CISOs. These include:

- Security's role in an organization's digital transformation
- Managing the noise that comes from vendors and the industry
- Solving the staffing shortage

All three of these challenges are major points of interest for the CISO community. As a result, these topics drive a lot of our focus and consideration. We dedicate this issue of Feats of Strength to understanding the CISO's role in addressing how digital transformation impacts their organizations.

Continued on next page

DIGITAL TRANSFORMATION IS THE CISOS GREATEST OPPORTUNITY YET

We believe digital transformation presents a great opportunity for CISOs to accomplish their two major goals – aligning security with business goals and making security a competitive advantage.

Historically, security was layered on top of already established processes within an organization, without much consideration. This resulted in resistance to the presence and impact of information security including uncertainty of increasing time to value, disrupting productivity and experiencing downtime.

Now, digital transformation is impacting organizations, and security has a key opportunity to be part of strategic discussions as solutions move to the cloud. The new standard for security to be built in from the start demonstrates a fundamental shift taking place.

Securing the cloud is hard work, and it requires a different knowledge set. In the article "Cloud Control" we learn how CISOs and their teams are evolving to address the cloud. Anthony Siravo, the CISO of Lifespan says, "There is a fundamental difference between traditional on-premise engineering and cloud-based engineering. Controls change and lines of responsibility change, and our team needs to be able to adapt to that."

Barry Abramovitz, the CIO of Liberty Bank, is excited about how the cloud may enable dramatic digital transformation and innovation. He says, "The cloud has enabled a rapid pace of spectacular innovation. I believe that the cloud's impact on innovation is more dramatic than the cost-savings benefits of the cloud. But some of the most dramatic innovators do not have the best security, so we need to find a balance."

While the cloud may present more work for CISOs, they now have the opportunity to stake out a leadership position and proactive approach. They have an opportunity to build secure solutions from the beginning and prove how security should be a business enabler. CISOs may decrease time to value for secure solutions and increase security efficacy.

ALIGN SECURITY WITH BUSINESS GOALS

In this issue we profile a number of terrific CISOs, including David Hahn, the CISO of Hearst Corporation. Hearst Corporation exemplifies an organization that has fully embraced digital transformation, with Hahn's security program at the forefront of business. He says, "Business strategy sets what you need to get done. Hearst went through a real transformation to become a digital company. As a result of the transformation we face new threats that make security a much bigger priority. We need to protect our data while operating without disruption."

MAKE SECURITY A COMPETITIVE ADVANTAGE

The advent of the digital transformation will have another benefit for CISOs. Today, consumers and customers are more aware of the need for security and privacy. Security-aware customers want to engage with organizations that provide secure digital solutions. For the first time, security can be a core differentiator, and it may be a valuable selling point for businesses. Importantly, security may only be a competitive advantage when solutions are built with the customer's security in mind. This needs to be articulated to senior leaders who are bullish on the cloud.

Ravi Thatavarthy, CISO of iRobot, shares key insight about the pros and cons of the cloud in this issue. He understands how the cloud supports digital transformations that are valuable to his company and customers. He also knows the importance of his job in protecting the company and client data. He has a tight grasp on the realities of security in the cloud, and as a result he is influencing strategic direction at the highest level. Ravi explains that if senior leadership believes a move to the cloud makes strategic business sense, he needs to be there ensuring security. He says security requires shared responsibility between the company and the cloud vendor. "It is very important to make time to understand exactly what the [cloud vendor's] contract includes."

Conversations about digital transformation are happening in nearly every organization. By participating in the discussion and elevating security to the strategic level, CISOs align with business goals and create competitive advantage.

Digital transformation is the next great opportunity for CISOs to truly be part of strategic, impactful discussions and decisions.

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

CISOs on Their Approach to Cloud Security

CONTRIBUTORS INCLUDE:

Anthony Siravo, CISO, Lifespan
Barry Abramowitz, CIO, Liberty Bank
JP Saini, CTO, TRC Companies
Kevin Hamel, CISO, COCC
Ravi Thatavarthy, CISO, iRobot

Whether for infrastructure, platform, software or a combination of all three, the cloud is a growing part of nearly every IT strategy. Due to clear business advantages, including cost efficiency and availability, the cloud is here to stay.

46% of companies cite availability as their top reason for moving to the cloud.

41% of organizations cite *cost-savings* as a main driver for **cloud deployments.**

Source: ISC2 Cloud Security Spotlight Report

While some CISOs are still wary about cloud security, they understand that saying "no" is not an option. Instead, CISOs are adopting policies, procedures and best practices to ensure data is secure and risks are managed, whether on-or-off premise, or in the public or private cloud.

We spoke with CISOs from across the United States, in industries as diverse as technology, healthcare and financial services, to see how they are approaching cloud security. Here are some of their responses:

SECURE THE WEAKEST LINK

"Since we are only as secure as our weakest link, we run all of our security enterprise-wide. We are a geographically dispersed organization, so we need to know who you are and what you are accessing. Everything goes through OneDrive and Office 365 to protect data in motion. We combine that with Identity and Access Management. On top of all of this, we run an Endpoint security product, for advanced threat prevention. But the biggest boon to our security program - cloud or otherwise - has been our security awareness training. We made our people smarter, and so now we are more secure."

- JP Saini, CIO, TRC Companies

74% of all companies store at least some sensitive data in the public cloud

Source: McAfee

EXTEND INCIDENT RESPONSE TO THE CLOUD

"This is the question we all have to answer as security teams: how does the organization respond to an incident at a cloud security provider? For us, the cloud is just one of many sources of a potential incident. We modified our existing incident response plan to accommodate the cloud. It is now just a different workflow in the same incident response process."

- Ravi Thatavarthy, CISO, iRobot

HIRE THE RIGHT TEAM

"We are making an investment in staff to be well-prepared to address specific cloud challenges. There is a fundamental difference between traditional on premise engineering and cloud-based engineering. Controls change and lines of responsibility change, and our team needs to be able to adapt to that. Our security architecture team as well as our infrastructure team are well aware of cloud security and cloud compliance."

- Anthony Siravo, CISO, Lifespan

BALANCE SECURITY WITH INNOVATION

"The cloud has enabled a rapid pace of spectacular innovation. I believe that the cloud's impact on innovation is more dramatic than the cost-savings benefits of the cloud. But some of the most dramatic innovators do not have the best security, so we need to find a balance. The major cloud vendors address security well, but there are some gaps that need to be filled. We need to combine on-premise security solutions with cloud security. We can reach a comfort level with cloud security by putting the effort in to get it right."

- Barry Abramowitz, CIO, Liberty Bank

DIG INTO VENDOR SECURITY CONTROLS

"You really have to drill deeply and ask the right questions to truly understand the security of cloud vendors. That includes pre-migration assessments and ongoing assessments once you have made a commitment to that cloud vendor."

- Anthony Siravo, CISO, Lifespan.

"Once you start peeling back the layers of the onion, you start to say: what did I really buy with this cloud service? Where is my data going to reside? Is data encrypted? Are they providing firewall services? Are they patching the infrastructure or am I? Where is my platform being recovering to? How quickly is my platform getting restored in a disaster? Once companies start poking a bit at those questions with their cloud vendor the answer is often that they need to buy more services from the cloud vendor to get that level of protection. Costs go up as a result and so the cost-savings argument loses its traction. Costs savings should not be the selling point for the cloud."

- Kevin Hamel, CISO, COCC

FRAMEWORKS AND AUDITING THE CLOUD

Abramowitz, at Liberty Bank, says that auditing cloud vendors via specific standards is an ever-evolving process. The bank uses a NIST framework married with an automated assessment tool from the FFIEC.

For Abramowitz, auditing of cloud vendors needs to be a bigger priority for the industry. "The audits that vendors have performed themselves are not very helpful. That can have a negative effect on our ability to move forward and innovate. When we cannot get a sense of adequate controls we cannot move forward with our contractual processes. We need a more standardized approach to ongoing audit and monitoring of the cloud vendors."

The Cloud Security Alliance (CSA) fills a role in managing cloud security strategies, and many organizations are using it as a guideline on top of traditional security frameworks like NIST or the SANS Top 20.

Siravo says, "We use Cloud Security Alliance as a guideline more than as a framework. As a healthcare organization we need to be HIPAA compliant, so HITRUST is a bigger influence. We review NIST and CSA, but do not follow them step-by-step."

Staffing up

61% or organizations plan to train and certify existing staff in cloud security

Source: ISC2 Cloud Security Spotlight Report

Q&A WITH MARK SETTLE

CIO, OKTA

Currently the CIO of Okta, the leading independent provider of identity for the enterprise, Mark Settle has more than 25 years of experience driving IT transformations in large enterprises. As a seven-time CIO, including tenure at five Fortune 500 companies, Settle now leads Okta's global enterprise IT strategy and operations, and collaborates closely with the executive leadership team to align strategic technology initiatives with broader business goals. With a focus on empowering people through technology, Settle ensures Okta's employees have streamlined access to the most important technologies and services to increase business efficiency.

Q: WHY DID YOU CHOOSE OKTA?

In our digitally-transformed, "always on" world, identity is emerging as foundational. Individuals expect access to the applications and data they need to manage their work and personal lives anyplace, anytime and on any device. Okta is on the cutting edge of addressing these needs in an increasingly complex world.

Okta's internal culture was also very appealing. We have a unique sense of community and a quiet self-confidence. I'm able to support the team by scaling and integrating our internal business systems in ways that can increase productivity and accelerate the delivery of new functionality to our customers.

I feel privileged to work for a recognized leader in the IT industry. In 2016, Gartner named Okta as a leader in the Magic Quadrant for Identity and Access Management as a Service (IDaaS). That was the third consecutive year Okta was recognized as a leader, and the only vendor named a leader for all three years of the report's existence.

Q: WHAT DIFFERENTIATES OKTA IN THE MARKETPLACE?

Our solution was built from the ground floor as a cloud-based service. Consequently, our capabilities are more redundant, scalable and secure than legacy identity management solutions initially developed for on-premises operations.

The Okta Identity Cloud includes single sign-on, user provisioning (commonly referred to as lifecycle management), a virtual user directory that can be federated with pre-existing directories, mobile device management, customer and consumer identity management, etc. It's a comprehensive way to manage identity and authenticate access to a wide variety of systems and databases from an employee, customer and partner perspective.

Because of our operations and foundation in the cloud, we have speed and agility on our side. Okta solutions can be implemented quickly with no extended incubation period of having to learn how software works or bring it up in the data center. We are uniquely suited to federate identities across multiple legacy platforms in a short period of time. This enables a business to narrow what we call "the innovation gap" and fulfill their missions as quickly as possible.

Q: WHAT CONVERSATIONS DO YOU HAVE WITH CUSTOMERS?

The Okta Identity Cloud has been adopted by every vertical, but regardless of the sector, when I speak with our customers, they bring up their challenges. One of these is "identity proliferation."

A good example is healthcare, where patients have more and more access to information and are using different channels to manage their health needs. The problem our customers run into is people signing up for health information or services on multiple sites and then having to juggle usernames and passwords — or even worse, they're replicating the same login across all sites. Health care providers are trying to integrate or federate these many access points so it's a one stop shopping experience for the healthcare consumer.

There are many, many other examples of the ways Okta customers leverage our capabilities to support their unique business models and day-to-day business operations. Ultimately, Identity management is no longer an out-of-sight out-of-mind utility function.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

DAVID HAHN
CISO, HEARST

HEADQUARTERS: New York, NY
EMPLOYEES: 20,000
ANNUAL REVENUE: $10.7 Billion

DIGITAL TRANSFORMATION BRINGS NEW SECURITY CHALLENGES

Four years ago, as the historic and venerable Hearst Corporation underwent a digital transformation, it became obvious to company executives that a more strategic, centralized security effort was required. David Hahn arrived on the scene as the company's first Chief Information Security Officer. Now, Hahn's task is to drive a more strategic, centralized approach to cyber security for Hearst's more than 300 unique operating businesses.

Hahn works closely with Hearst's Chief Technology Officer to map security to business strategy for the entire organization. "Security starts with business strategy," says Hahn. "Business strategy sets what you need to get done. For our industry in media, the world has changed. Technology has evolved and the needs of viewers and readers have changed. Hearst went through a real transformation to become a digital company. As a result of the transformation, we face new threats that make security a much bigger priority. For us, security is all about protecting and enabling availability for our media properties. We need to protect our data while operating without disruption."

"Due to strong CTO relationships, it is easier for me to work with the business partners and explain how security can help them. The important thing is making sure the business partners understand that we want to enable them with security."

- DAVID HAHN

Prior to Hahn's arrival four years ago, security was handled at the individual business level. Information Security Officers (ISOs) at each organization ran unique security programs. With Hahn in place as the central CISO for the global conglomerate, the business ISOs are tasked with more operational and tactical security efforts. Hahn and his team run what is essentially an information security services team at the enterprise level, setting strategy for the company. It is a geographically distributed model that ensures corporate data is protected, standards are met, and individual business needs

SECURITY COSTS RISE WITH THE CLOUD

> "The cloud is transforming IT and it will certainly change operations. While it is seen as a cost-saver for IT, it is not yet that for security. In fact, it's a reason security costs will continue to rise," predicts Hahn. "It is another thing for security to have to cover. Every business still has on premise systems, we cover legacy systems, data centers, infrastructures and networks. Now we are also figuring out how to secure the cloud - this requires even more capabilities from our team. Nothing gets eliminated when you move to the cloud, things just add up from a security perspective. In the long run the cloud strategy will save millions, but today we are not there."

are addressed.

The sheer size of Hearst and its organizational structure are both a challenge and inspiration to Hahn and his team, who took the position at Hearst seeking to expand his expertise. "The challenge was how to build a successful security program with more than 300 different businesses. We are in media, healthcare, financial services. We have 33 TV stations, and for them, availability is everything. There is no one simple security solution to address everything. It is very fulfilling work to be on the front lines of security protecting a business like this," says Hahn.

Hahn prioritizes understanding the company's goals, and understanding management and their expectations. He continues, "My role is to be strategic. I cannot get too tactical, but at the same time I must have a broad program. We are always moving forward. I do not want to try to predict the future, but I always need to examine my objectives against what has changed. In a digital transformation, and in cyber security, things are always evolving, so we constantly need to be looking forward to make sure we are addressing things appropriately."

"No one ever hires a CISO when everything is perfect," Hahn points out. "But you cannot come in feeling like a hired gun and install a bunch of solutions to fix problems without first understanding business strategy."

DISTRIBUTED ORGANIZATION WITH A DEEP TEAM OF EXPERTS

Like many CISOs, Hahn says the secret to a successful security program is the team in place. The unique model at Hearst equips Hahn with several skilled team members, a deep bench of ISOs, and a large network of CTOs and business partners at each distinct organization.

"One person cannot do everything," says Hahn. "But I do believe that one person can make a difference. While I focus on strategy and where to go in the future, I am very grateful to have a large team of contributors who are focused on the right areas and the particular controls that we need."

He explains, "I spend a lot of time with the CTOs at our various business units. The CTOs really understand what I am doing and together we look for effective integration points. Due to strong CTO relationships, it is easier for me to work with the business partners and explain how security can help them. The important thing is making sure the business partners understand that we want to enable them with security."

Security awareness is high at all of the Hearst organizations. "Today, every company, no matter how big, is focused on security. No one is immune to the internet. Every business leader is looking to me for guidance on what to do. What can we control, how do we make changes to protect and enable our business? There is no resistance, we work smartly together as partners."

Hearst's organizational structure provides much autonomy to the business units, and some of the ISOs report into their own CTOs. "As an enterprise we are connected via shared services, so I provide security services out to the businesses. While the ISOs focus on business specific challenges, such as managing HIPAA or compliance requirements, I focus on the back end infrastructure, the network and enterprise security. If a business unit has a legacy product in place that is working well, then they continue to use it. When it is time to overhaul or introduce a new security technology that is done by my central team."

Hahn reports up to his own CTO, who reports directly to Heart's CEO. "I produce a monthly Key Performance Indicator (KPI) deck. Right now it is 50 pages because we try to show all the different pieces. The KPI deck works to educate the team, and let them know what we are handling. They are not interested in hearing about the problems, they want to know how we are managing the problems. For example, it includes our mean time to detections and mean time to resolution," explains Hahn. As Hearst continues its digital transformation, Hahn's security team is laser focused on detection and resolution of security incidents, to enable business growth.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

THOMAS MURPHY
CISO, NORTHWESTERN UNIVERSITY

HEADQUARTERS: Evanston, IL

EMPLOYEES: 25,000+ Students & Faculty

ANNUAL REVENUE: $9.6 Billion

> "In speaking to other leaders here, I learned there was a perception that security was historically done in a closed environment. I'm working to change that. Our program will ensure business processes and needs are taken into account with all new security initiatives."
>
> **- THOMAS MURPHY**

EXPANDING THE ROLE AND VISIBILITY OF INFORMATION SECURITY

Thomas P. Murphy recently became the new CISO at Northwestern University, one of the premier universities in the nation. The university's mission is to provide excellence in teaching, innovative research and the personal and intellectual growth for a diverse student population, all backed by a dedication to information security. Murphy says, "At all levels of the organization there is understanding that, in order to deliver on our mission, we must protect information in a distributed environment where technology is evolving and being embedded in all areas of the university."

Northwestern's considerable student base, and the open and collaborative environment typical of a large-scale research university, presents some unique challenges. Murphy comments, "I interact with my peers and senior leadership about information security concerns on a daily basis. Among the top concerns is whether we have the right resources to respond to an attack, not "if" but "when" it occurs. Another concern is that security awareness and training may be a lower priority in an environment where teaching, learning, research and other efforts take most of our time."

Murphy is confident those challenges can be addressed successfully. He plans to roll out a major security awareness training initiative in the Fall, when the academic year resumes. In the near term, he addresses information security by getting out of the "back office", walking the campus, introducing himself, and demonstrating that he and his team are interested in a true partnership with the leaders of the university.

Information security is constantly evolving at Northwestern, and the role of the CISO becomes a more prominent role in the community. Murphy continues, “I’m bringing a more public face to information security. Professors, department chairs, and administration are all accustomed to seeing policies listed on the website. Now, as I go out and talk to more of the community, they are asking great questions and are very engaged. I have been invited to present to a wide variety of groups and departments across the campus.”

THE NEW CISO ON CAMPUS

Since Murphy’s arrival, after educating himself on goals, understanding the existing security program and making introductions across the university, he is eager to move forward with a number of programs and a security plan he is developing with the help of the CIO, to whom he reports.

Among Murphy’s first priorities is refining the university’s security policies. “Our current policy suite is very verbose,” explains Murphy. “A seven page policy is difficult for people to wade through to get the guidance they need, especially when they have other responsibilities and priorities. I need to pare down those policies to make them more easily read and actionable.”

“In speaking to other leaders here, I learned there was a perception that security was historically done in a closed environment. I’m working to change that. Our program will ensure business processes and needs are taken into account with all new security initiatives. Early feedback shows that our community is very responsive to this approach.”

Murphy has plans to involve the information security team in all aspects of the enterprise-wide response program. “Whether it is a physical security incident, or a cyber incident, our systems need to be ready for a coordinated response. I plan to work with the university police department to ensure our response and communication systems are in place, and Northwestern is prepared for any incident.”

His other plans for the security program include mitigating the university’s top threats with appropriate tools and user awareness training. “A big stress center for us is phishing and ransomware. Our community is constantly faced with these types of threats. They want to know how they can help protect Northwestern,” says Murphy.

SECURITY EXPERTISE AND A LAW DEGREE COMBINE FOR A UNIQUE PERSPECTIVE

While many Chief Privacy Officers come out of law school, and increasingly CISOs are pursuing MBAs, only a few CISOs are J.D.’s, like Murphy. “My law degree helps me understand regulatory compliance at a deeper level. It also helps with things like electronic discovery requests, which are increasing as data is stored online. I also have a Master of Science in Information Protection and Security, so I combined legal and technical knowledge, which is an advantage in creating security policies and programs.”

Murphy encourages anyone interested in growing in the field of information security to pursue an advanced degree. “Inevitably in information security, you will be in a position to act with regards to business administration or law so it makes sense to have knowledge and credentials in those areas.”

Use of the Cloud

“Use of Cloud services is a major initiative at Northwestern,” says Murphy. “We are taking an aggressive, but careful approach to using cloud services where appropriate. For example, we have HIPAA requirements that dictate the type of commitments and agreements we need from cloud providers. We also want to make sure we are working with cloud service providers that offer high availability and failover, in addition to world-class security.”

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

BRIAN MILLER
CISO, HEALTHFIRST

HEADQUARTERS: New York City, NY

EMPLOYEES: 4,300

ANNUAL REVENUE: $8.7 Billion

FROM NASCENT SECURITY PROGRAM TO STATE-OF-THE-ART IN TWO YEARS

Brian Miller is the first CISO at Healthfirst, a provider-sponsored health insurance company that serves poor and underserved people in New York City. The ability to work with an organization that is truly making a difference in people's lives is what drew Miller to the role. "We provide top quality care to people that have traditionally not had access to the best services," says Miller. "We have four- and five-star quality ratings for our Medicare and Medicaid products, respectively. Those are very hard scores to get, and we are very proud of that. It is really compelling to work in an organization with this mission. It is definitely worth investing my time and energy."

In his first year, Miller diligently and optimistically tackled accomplishing 26 major projects with 43 unique goals. Luckily for Miller, everyone at the C-Level and on the organization's Board of Directors was supportive. According to Miller the Healthfirst Board of Directors is highly engaged with the security program. He reports to the Board on risks as well as accomplishments. While he keeps the information high-level, there is usually opportunity to dig deeper. "The Chairman and the Board dive into specific questions about what we are doing and how we are responding to risks. That requires more granular metrics about performance, which we have as well."

> "I tell my employees to consider the risks of every question or decision. Ask yourself, 'Are you willing to accept the risks?' If not, raise up the issue until you find someone willing to accept the risk and make the decision."

Buy-in and commitment from the highest levels of the organization allowed Miller to hit the ground running. “It was daunting, but also very exciting to be a part of such a big transformation,” says Miller. “To be able to take hold of and drive the transformation of security - to take it from troubled to state-of-the-art was very appealing to me. It was a very fast-paced first year. We were always bringing the best solutions possible to the table. Seeing the program come to life was very exciting.”

Starting nearly from scratch, Miller and his team first embraced the HITRUST security framework. “We focused on people, process and technology and ensured we had a policy that aligned with HITRUST. The policies and procedures we implemented gave us a strong foundation for future projects such as applying security to application development and other programs.”

Miller’s initial 26 projects spanned a wide array of security functions such as plugging holes in Healthfirst’s network and systems, including Endpoint Protection projects and Identity and Access Management. Incident Response and Governance Risk and Compliance were other big priorities for Miller in his first year and a half.

Much of Miller’s initial effort was focused on Vulnerability Management and Patching. “The SANs Top 20 Security Controls include basic patching, which is conceptually very simple, but organizationally we had to go on a journey from ad hoc patching to a very disciplined approach. Our people and processes needed to mature. It took us approximately 12 months before we were on a regular cadence. Now we scan, patch and scan again on a regular basis.”

A CONSULTING ORGANIZATION BUILT ON FLEXIBILITY AND AUTONOMY DRIVES SECURITY ACHIEVEMENTS

Miller is passionate about how far Healthfirst’s security program has come in two years. Much of the program’s success is due to his talented team and their approach. Miller’s successful experience in consulting enables him to run his security program like a consulting organization. He comments, “As consultants, we are guiding the organization through dramatic security changes.”

Miller continues, “A client once said to me, ‘If you do this project well, you will be here forever. If you do not, you will not see another dollar from us.’ I always think of that conversation because it is the essence of what everyone wants. They want you to bring value to the table every day. Our job as a security team is to figure out what different people need and provide them with value.”

In two years Miller has grown his team from six employees to twenty. He is focused on hiring and retaining the right team members. Miller says, “Hiring the right people in the right places was so important. I focus on diversity among my staff. I believe that diversity makes our team stronger. This broadens the perspective of our team in a positive way. Having a diverse team helps us to avoid ‘group think’ and creates an environment where people are pushed out of their comfort zones in good ways. If managed correctly, diverse teams communicate better.”

In the ultra-competitive security hiring market, Miller retains and motivates his team with flexibility, autonomy and training. “Even though we are based in New York City, my team works from anywhere. I hire the best people for the role, no matter their location. For example, my Head of Cyber Operations works from Boston, and our team member in charge of Patch Management is in Florida. Nearly everyone on the team works from home one or two days a week. I am very results-oriented. If the work is getting done, it makes no difference where or when the team works. It is about performance, not about being in the office.”

Miller prioritizes his employees’ career and personal motivations, to keep them energized and happy at Healthfirst. “I have one employee who is so talented, and making top dollar, but he could go elsewhere and make even more money. At Healthfirst he appreciates that he has opportunities to speak at conferences and train in cutting edge technologies. That’s what keeps him motivated.”

To enable autonomous workers, Miller gives them the authority to make their own decisions. “I tell my employees to consider the risks of every question or decision. Ask yourself, ‘Are you willing to accept the risks?’ If not, raise up the issue until you find someone willing to accept the risk and make the decision.”

Miller considers the growth of Healthfirst’s security program as the biggest achievement of his career. He proudly states, “Our CIO said that success would be measured based on those first 26 projects. We did not get to everything in the first six months, but we moved everything along. It was a challenge to execute on those programs while simultaneously hiring a full team, but with the right people on board, we were very successful.”

Q&A WITH LARRY BIAGINI

CHIEF TECHNOLOGY EVANGELIST, ZSCALER

> “Our founder Jay Chaudhry started Zscaler nine years ago because of his view that the world was going mobile, not just in terms of devices, but people as well. He knew the way we were doing security was changing and we had to build for scale from day one. He didn’t inch his way in, because he knew if he was going to be successful in this market, we had to plan for billions and billions of transactions for some of the largest organizations.”

Q: DESCRIBE YOUR CAREER PATH

Prior to Zscaler, I spent 26 years at GE, retiring as VP and Global CTO. In my time at GE I held many CIO, CTO and CISO roles globally and in various business units. In my final position as CTO, I led the information technology strategy and execution for cloud, software as a service, user experience, security as a service and network transformation.

In the last 8 years I have been focusing on the rapid advances in technology (cloud, mobile, security, IOT), and how companies must transform themselves in order to take advantage of new opportunities, as well as protect from new threats being created. At Zscaler, my role is to work with large companies to help them think through the implications of this new environment, especially as it pertains to user experience, network transformation and cloud security.

Q: WHY DID YOU JOIN ZSCALER?

Joining Zscaler was a natural fit from both a philosophy and execution standpoint. While at GE, I implemented Zscaler and experienced why they are considered a leader.

Our founder Jay Chaudhry started Zscaler nine years ago because of his view that the world was going mobile, not just in terms of devices, but people as well. He knew the way we were doing security was changing and we had to build for scale from day one. He didn’t inch his way in, because he knew if he was going to be successful in this market, we had to plan for billions and billions of transactions for some of the largest organizations.

I’m thrilled to be with a company that is revolutionizing internet security. We now protect 15 million users in 185 countries, blocking 100 million threats a day, all in the cloud. The key value in what we offer is no need for on premise hardware, appliances or software.

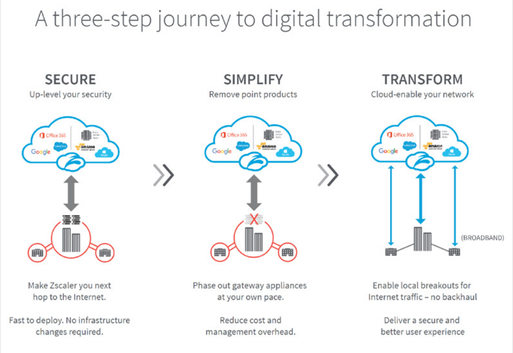
Q: WHO USES ZSCALER?

Every industry that uses the internet for business needs our technology. Service organizations have been at the forefront because they have a very distributed footprint and the cloud experience is often far superior, increasing user satisfaction. In manufacturing,

Why Zscaler?

Reduced Risk (CISO)	IT Simplification (CTO/IT Head)	Impressive Value (CIO/CFO)	Productivity (End-users)
Unmatched security – all users, branches, devices	Consolidate point products and simplify IT	No CAPEX – elastic subscription fee	Fast response time – local breakouts
Consistent policy and protection	Cloud-enabled network	Reduced OPEX – no box management	Localized content
Always up to date	Rapid deployment	Reduced MPLS cost	Users empowered to leverage cloud apps

HOW DOES ZSCALER ENABLE DIGITAL TRANSFORMATION?


A three-step journey to digital transformation

SECURE
Up-level your security

Make Zscaler you next hop to the Internet.

Fast to deploy. No infrastructure changes required.

SIMPLIFY
Remove point products

Phase out gateway appliances at your own pace.

Reduce cost and management overhead.

TRANSFORM
Cloud-enable your network

Enable local breakouts for Internet traffic – no backhaul

Deliver a secure and better user experience

Users and applications have both moved off the network. We access applications in the cloud from our homes and mobile devices without ever touching the corporate network. And when we are on the corporate network, the internet is the more frequent destination than the data center. Further, we have often provided unfettered network access to third parties via VPNs.

While this notion of the perimeter is eroding, threats have evolved. This generates more spending on gateway appliances, but all of this spending is going to protect the illusion of a hardened perimeter when none exists. Therefore, the security needs to be focused on protecting the user wherever they go rather than just when they go through the corporate network. I could write you a book on all the wrong minded things enterprises do to try to keep users on the corporate network like VPN access, tromboning traffic over LAN and WAN, and other complex solutions.

To address all of this, Zscaler built a cloud security platform to secure this new world of IT with no hardware to deploy and manage. The Zscaler cloud security platform consists of two principal elements: Zscaler Private Access (secure access to private apps without exposing them to the Internet) and Zscaler internet access (inline inspection of all traffic to make sure nothing bad comes in and good leaves).

they were an early adopter because they constantly face IoT challenges and realized the control points they had in the past did not work anymore. Healthcare requires cloud for regulatory issues and although not all are transitioning yet, many know it's the next step. Many financial services are moving in the direction of cloud. For retail and banks, cloud is a large priority.

Q: DO YOU HAVE COMPETITORS?

Our chief competitors are established companies who are trying to move their functionality to the cloud. Most are trying to get where we are today, but Zscaler was not built overnight, we've come a long way from our start. Competitors that we run into want to deliver services from the cloud to the user, and they're taking an interim step right now moving stuff off premise, but it's still not as effective as what we do.

Q: WHAT DIFFERENTIATES ZSCALER?

CISOs, CIOs, and CTOs, must have discussions with their boards about security vs. risk, because they are two different things. In the past they've concentrated on security and tried to secure everything in the enterprise. The discussion needs to switch to think - 'what are we concerned about as an organization that can fundamentally hurt us, up to the point of where we can't recover from?' - that's where organizations need to spend their resources and budget.

Security leaders need to start thinking about tearing down all they've built in the past that has been ineffective. A very simple example is users who are very well protected while in the office, but when they take their laptop home it gets infected, without visibility. They then go back into the office and the organization can hopefully protect from what happened while they were away. In the Zscaler world, this wouldn't happen because you are always protected.

What is most important about Zscaler is we protect the user anywhere, at any given time. We provide full visibility into the security side and the compliance side, regardless of being on or off network, this is part of our mission.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

BRIAN NESGODA

CIO & SVP ENTERPRISE RISK MGMT
SIKORSKY FINANCIAL CREDIT UNION

HEADQUARTERS: Stratford, CT

EMPLOYEES: 135

ANNUAL REVENUE: $750 Million in Assets

Many CISOs believe the future of information security is as an autonomous unit outside of the IT organization, yet the majority of CISOs report into the CIO. At Sikorsky Financial Credit Union, Brian Nesgoda is pioneering a new path. Formerly the CISO, Nesgoda is now CIO and Senior Vice President of Enterprise Risk Management which includes the CISO responsibility. As he puts it, "IT now reports into security."

"The biggest challenge facing our industry is getting CISOs the visibility that they need within their organization. That means getting them out from behind the CIO and giving CISOs independence," explains Nesgoda. "Unfortunately, until auditors write recommendations addressing this conflict, we will see few changes industry-wide."

At Sikorsky, the organization is set up around risk. "We have a different structure than what you see out there [in other organizations] since IT reports into me. I hope to see more organizations make this change because I think it is long overdue for security to be at the top of the hill," says Nesgoda.

He continues, "As part of ISACA's CISO Working Forum, I speak with 30 other CISOs and hear their concerns. Many of them feel frustrated reporting into the CIO. I am fortunate in my role because I have direct communication with the Finance & Enterprise Risk Management Committee and attend every Board meeting. There is communication all the way up the ladder so effective governance can be applied as it relates to risk. This is an uncommon structure for an organization today, but I am lucky to have it."

BUY-IN AND COMMITMENT FROM THE BOARD FOR A NEW ENTERPRISE RISK PROGRAM

Nesgoda's team strategically created a risk assessment methodology and built out a comprehensive and effective enterprise risk management framework. "In introducing a risk management program, we started with a top down approach," Nesgoda explains. "We received buy-in from the CEO and Board-level committees, and we spoke with senior management. We explained our process and the changes to expect. We explained what management should expect from us in terms of risk."

NESGODA'S THOUGHTS ON CLOUD SECURITY

> “We are leveraging the cloud and Web services. A big challenge for us is determining how we extend our security policies out to those vendors. We are looking at the CASB market, but it is still largely in its infancy. We will be using Office 365 and Microsoft has done a good job of documenting security controls, but we still need to ensure that it meets our specific security standards. A CASB can help with that.”

A key to Sikorsky's risk management program is that each group in the organization is made aware of their own risks and what must be addressed. “We have regular meetings among executive leadership. In those meetings I, and my department, report risks by department, and then slice it further by risk category, such as reputational and strategic risk. This makes it easier for business executives to understand and react to risks,” describes Nesgoda.

Rolling out this program constituted great effort for Nesgoda and his team. “We sat with project managers and subject matter experts and attempted to automate and streamline processes as much as possible. We leveraged an advanced vendor management process and we built a risk assessment questionnaire for all systems.”

Now, risks are reported up to the Board on a regular basis. “If the Board sees high level risks they can ask further questions. The Board's attention to risk lends the program greater priority in the organization,” says Nesgoda.

The Board asks a number of questions to Nesgoda as they work to understand the credit union's risk posture. Nesgoda comments, “For example, I'll present a risk assessment that may have an aggregate risk of medium, my chairman of the Board will say, ‘Is that ok? What do we need to do about it?’ Those are excellent questions. I explain, what we need to focus on is ‘what are the gaps and what are we doing about them?’ I'll explain this to them, then let them know the actions we need to take to mitigate a particular risk. Of course there is only so many resources to go around, so part of risk management is ranking projects by risk that need to be addressed. We put the most dollars to the highest risk priorities. That's the second most common question that I get from the Board - ranking the risks for remediation.”

ALIGN WITH BUSINESS PRIORITIES TO IMPROVE SECURITY CONTROLS

Nesgoda and his team make certain their efforts stay aligned with Sikorsky's four main objectives, which are reinforced each year at strategic offsite planning meetings. “As an organization we have four objectives. They include financial stability, creating an effective workforce, building and protecting the credit union identity, and pursuing organizational excellence. We align all of our security and risk management initiatives to support these four business objectives,” he explains.

To drive security programs forward with strategic business alignment, Nesgoda recommends other CISOs partner closely with business units. He comments, “Start by talking to business leaders and be proactive in communicating with them as they take on new applications. Ask, ‘How can I help you move this project forward?’ Be part of the project team from the beginning. This will allow you to bake security concerns and controls into the application while you help your colleagues solve their problems. Do not be the person who says everything is high risk, prioritize the risks for them and help them find solutions to mitigate those risks which helps them accomplish their objectives.”

Nesgoda's security and risk program relies heavily on Managed Security Service Providers (MSSPs) and consultants. His dedicated security team is small. “With so many unfilled security jobs in the market, I know that it will be difficult to hire and retain the best resources, so I leverage consultants and MSSPs,” says Nesgoda. Nesgoda also points out that his IT team is very security-aware and capable.

“We are focused on creating a more adaptive security architecture, and leveraging third party vendors to do so. We are strengthening our incident response program, so that is our big focus in 2017.”

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

RICHARD TIMBOL
ISSM/CISO, DAVIS POLK & WARDWELL, LLP

HEADQUARTERS: New York City, NY
EMPLOYEES: 2,000
ANNUAL REVENUE: $1.18 Billion

COMMITTED TO PROTECTING CLIENT DATA

> "From the beginning, management empowered me to grow my team as needed. The people on my team are creative, out-of-the-box thinkers. They need to be. Our field changes every day, so we have to be able to think creatively about solutions."
>
> **- RICHARD TIMBOL**

Richard Timbol took the role of global head of security at the New York based law firm Davis Polk & Wardwell, LLP almost two years ago. He says, "I was not actively looking to move. We all know security has a hiring problem and nearly all of us field a dozen recruiter calls a month. I ignore most of them. But when Davis Polk called it was different. Management really sold me on the role because they are so committed to protecting client information. Davis Polk is not just completing an audit, we are committed to doing security the right way."

With a long history in the IT and information security industry, Timbol knows the commitment the firm shows to security is not always the case. "One challenge for our industry is that security programs are all over the map in terms of maturity. Across every vertical there are companies doing security the right way, and others that are doing the bare minimum to meet compliance. It is a real challenge because the 'bad guys' are all innovating. We really need every organization to step up."

When Timbol started in information security a decade ago, he recognized the need for the industry to embrace security in a positive way. Quickly, he understood it is not enough for companies to approach security as a check box for compliance. Early in his career, Timbol leaned on peers and colleagues for advice about how to build successful security programs and how to position security as a business imperative. He says, "In the beginning of my career, I learned a lot about information security from

TIMBOL SHARES HIS THOUGHTS ON CLOUD SECURITY

“CASB is a huge market. Its advancements show that the cloud in general has matured a great deal. But many security executives still have concerns and prejudices against the cloud. They think that data in the cloud is not safe.

The cloud is not an appropriate option for every instance. You have to consider how and why you are putting data in the cloud. It requires a whole new way of thinking about security. A lot of organizations simply do not have that knowledge in house and they are learning as they go.”

a network of peers and at conferences. I learned how to approach security in a strategic way. I remain grateful I had this kind of a start in the industry.”

Now at Davis Polk, Timbol is a seasoned security veteran in a company that embraces security. From the start of his tenure at the law firm, Timbol has focused his team on empowering the organization to achieve its goals within a secure environment.

“My approach to the role is the same at every organization,” says Timbol. “I first understand the specific objectives, processes and goals of the business. A law firm generates revenue in a certain way. My last position was at a market research firm. They had a completely different revenue model. I cannot use the same security playbook from one organization to the next - that would be a disaster - but the basic approach of creating a security program that reflects and understands business goals is the same.”

He continues, “Step one is to identify the firm’s priorities and align with business goals. This does not mean my past experience is irrelevant. You can build a holistic security practice when you combine technical expertise with business acumen. Once my business goals are identified I can then easily pick out the low hanging fruit - the specific initiatives that can be executed on quickly to drive exponential growth in data protection and cyber security for the firm.”

Timbol states one of the most important aspects of developing the security program is transparency with business users and management. “When building out the team, purchasing new technology or implementing a new policy, it is important to get buy-in from peers and management. Ideally, if you do security correctly, the user base feels nothing. But sometimes security does impact processes. If changes are required, it is important to explain the benefits. It is important to evangelize security efforts. Clients increasingly ask our lawyers questions about security, so it is important they understand and can communicate our security posture.”

REPORTING ON RISKS AND EVANGELIZING AT THE HIGHEST LEVEL OF THE ORGANIZATION

Like many other security leaders, Timbol reports into the CIO. He is also a key member of the firm’s information security committee that includes leadership representation from many areas of the firm. “I present a report on the state of our security to this committee. That report includes updates on the effectiveness of our security and on ongoing initiatives to continue to lower the firm’s security risk. We talk about overall security posture, more than operational updates.” explains Timbol.

His communication with the firm’s leaders does not end there. In fact, Timbol reports an open door policy with the firm’s directors. “They want to enable security in the organization and most have an interest down to the operational level of security.”

Timbol credits his team and the firm’s management with the firms security success. “From the beginning, management empowered me to grow my team as needed,” says Timbol. “The people on my team are creative, out-of-the-box thinkers. They need to be. Our field changes every day, so we have to be able to think creatively about solutions. When hiring, I ask questions that help me to understand how the person solves problems. Of course my team is technically competent, but their ability to solve problems is just as much the key to our success.”

As Timbol reflects on his career he considers building teams and mentoring security professionals among his successes. He thinks the future for his team, and the industry in general, is bright. “There is no limit to growth for smart, talented people in security,” suggests Timbol. “I have seen interns rise to the point where now they are my peers in the industry. There is so much innovation and opportunity in security.”

Q&A WITH KRISHNA NARAYANASWAMY

FOUNDER & CHIEF SCIENTIST, NETSKOPE

A highly regarded and awarded researcher in security, behavioral anomaly detection, and deep packet inspection, Krishna brings over two decades of technical and thought leadership as founder and chief scientist of Netskope. Krishna leads Netskope's data science and user behavior research and is a prolific writer and speaker on a range of cloud security topics. He has authored over 40 patents and co-authored the industry's first Cloud Security for Dummies book. He is a co-chair of the cyber incident sharing center working group for the Cloud Security Alliance. Prior to Netskope, Krishna held numerous leadership positions, including founding Top Layer Networks and serving as a distinguished engineer at Juniper Networks.

Q: DESCRIBE THE FOUNDING OF NETSKOPE

We founded Netskope with the belief that enterprises needed a new approach to security where the adoption of cloud applications required more visibility and control.

From day one we focused on real time enforcement. We believe if someone is accessing your sensitive data then you must be able to take action and stop it in real time. Data Loss Prevention was also one of the key motivations for deploying our solution. While many cloud apps have good security controls, they lack the uniformity and depth across the apps. Enterprise security admins are looking for a common pane through which they can get visibility and control of all the cloud apps in their environment.

There was an inflection point in the market when Microsoft was driving the adoption of Office 365 in all enterprises. This was when we saw a lot of uptick in inbound request and a big turning point for us.

I'm proud to say that Netskope is the only cloud app security and enablement company that offers real-time analysis and policy creation to prevent unwanted behavior, and the ability to monitor all cloud apps.

Q: WHAT KIND OF CUSTOMER AWARENESS DO YOU EXPERIENCE?

When we first meet with customers, they may think they have 10 apps, when in reality they can have upwards of 1000. With so many cloud apps in the workforce, the majority come in from users and are unknown to IT, called "shadow IT".

BYOD is a trend that continues to increase, meaning more and more unmanaged devices will enter into organizations and request access to corporate data. Historically, IT had to choose to block all unmanaged devices or endure a lack of monitoring of their data.

We encourage IT to embrace BYOD and "shadow IT" by using our solution to safely enable cloud app usage without compromising the corporate data.

We perform a Cloud Risk Assessment to make the customer aware of their true cloud app challenges. We take one month of their user data and present the full picture back to them. They are often shocked at the number of apps we actually discover.

Q: WHY IS NETSKOPE IMPORTANT FROM A BUSINESS PERSPECTIVE?

Compliance is a huge part of business cases. Since the world has moved into a digital economy, data is gathered everywhere, while at the same time we see more breaches occurring. From a business point of view, it's very important from a compliance perspective to protect your data. I hear many conversations at the board level about taking proactive measures to protect data.

The entire existence of most businesses is around their intellectual property. When moving to the cloud, it's key to protect your "crown jewels" so you don't compromise your entire business.

Q: WHAT TRENDS DO YOU SEE IN THE MARKET?

Threats like malware and ransomware are now happening more often in the cloud. The bad actors look at the most vulnerable points of any enterprise where data may be exchanged from an untrusted entity to a trusted enterprise user. Cloud apps are especially targeted in this way and many of these attacks are going undercover. Enterprises must be able to look at these data exchange points in the cloud and inspect the data before allowing it into their trusted environment.

Q: ASIDE FROM TECHNOLOGY, WHAT DIFFERENTIATES NETSKOPE?

From day one, we had an open culture environment. Our engineering team is encouraged to be agile and innovative. They continue to innovate to stay ahead of threats and provide value to our customers. I believe in mentoring and giving back to the community. From speaking at conferences, to interacting with our customer advisory board, or being active on industry organizations, it's important for me to give back.

Cloud Security at a Glance

It's no secret, the cloud is here to stay and more enterprises are running ever increasing numbers of applications in it.

$$$

$141 Billion by 2019

Worldwide spending on public cloud services will grow at a 19.4% compound annual growth rate from nearly $70B in 2015 to more than $141B in 2019

Too Good to Ignore: The **Business Benefits** of the Cloud

AVAILABILITY

90% of worldwide mobile data traffic will come from cloud applications by 2019

MOBILITY

46% of companies cite availability as their top reason for moving to the cloud

COST SAVINGS

41% of organizations cite cost-savings as a main driver for cloud deployments

In 2017, CISOs are prioritizing cloud security. They are training staff, and assigning more budget to the cloud. Worries are still there, but dissipating.

STAFFING UP

61% of organizations plan to train and certify existing staff in cloud security.

BUDGETS UP

59% of organizations are increasing security spending for their digital transformation efforts.

CONFIDENCE UP

Today, 37% of organizations rate cloud security a significant challenge, compared to 41% in 2015.

Sources:

PWC's Global State of Information Security Services Report

IDC Worldwide Quarterly Cloud IT Infrastructure Tracker

Spiceworks "Diving into Cloud" Survey

ISC2 Cloud Security Report 2016

Two Sides to Every Cloud

Every cloud is different.

Each organization has different needs and goals when it comes to cloud adoption and management. CISOs and security leaders must ensure their cloud decisions positively align with their corporate goals and mission. We asked CISOs to weigh out some of their pros and cons.

Smooth Sailing

Barry Abramowitz, the CIO of Liberty Bank is fully committed to the cloud. “We outsource our core banking services to a private cloud. Critical applications such as internet banking and loan origination are in the cloud. Before it was the cloud, it was software as a service - it’s the same thing and I am a huge proponent of it. In my role as CIO, I try to be a change leader in the organization, not just from a technology perspective but from a risk perspective. We need to adequately answer security questions that arise.”

Abramowitz explains how Liberty Bank has moved many departments to the cloud, and other mission-critical areas are being considered as well, “Our entire human resource system is cloud-based, including the mobile solution. We are focused on creating a customer-centric digital eco-system and revising our whole approach to delivery of digital solutions via the cloud.”

He continues, “Every time we do an assessment of an on-premise solution I say to my team, ‘well this is probably our last year that we will do this.’ The benefits of moving to the cloud are dramatic.”

Safer in the Cloud

JP Saini is the CIO at TRC Companies. He says, “Business outcomes are the driving factors for all of our technology decisions and the cloud is no exception. We consider how effectively we can scale and handle that scale. We leverage the cloud for infrastructure, platform and software as a service. The cloud makes us more agile.”

Saini believes the cloud also makes TRC’s security posture stronger. “From a risk perspective, we evaluated how we could secure the platforms versus how the cloud vendors are able to do it. We realized that the established cloud vendors have a much better ability to protect it than we can on our own.”

Rick Grimaldi, CSO of K logix agrees. He says, “Across our client base we are seeing more of an acceptance that the cloud is inherently more secure. As long as clients understand how their cloud vendor is assessed and audited on a regular basis, this transfer of risk to the cloud vendor is a good solution.”

CONTRIBUTORS INCLUDE:

Anthony Siravo, CISO, Lifespan
Barry Abramowitz, CIO, Liberty Bank
JP Saini, CTO, TRC Companies
Ravi Thatavarthy, CISO, iRobot
Rick Grimaldi, CSO, K logix

The Cloud Has its Limits

Ravi Thatavarthy, CISO at iRobot says one thing the cloud cannot yet support is the Security Operation Center (SOC).

He says, “You have to ask yourself, how comfortable are you with moving security operations to the cloud? And, how comfortable are you with letting somebody else run your SOC? I am not at a stage where I am comfortable outsourcing the SOC. Cloud or not, I am not ready for any third party to take that responsibility. Cloud security operations vendors are still maturing. They are not yet fully integrated with the major players like AWS or Azure.”

Importance of Due Diligence with Cloud Vendors

Thatavarthy has taken a cautious approach to the cloud. He sees the benefits of a private cloud for infrastructure services and specific use cases for highly-scalable or high-availability applications. But, he cautions about the importance of conducting on-going assessments of the potential risks of any cloud providers.

Rick Grimaldi agrees. He says, “Often companies will do a single pre-purchase security assessment of a cloud application, but to truly limit risks organizations must continue to revisit those assessments, just as they do with on-premise solutions.”

It is important for organizations to understand that moving applications or infrastructure to the cloud does not absolve them of responsibilities. Thatavarthy explains that it is a relationship of shared responsibility between the cloud vendor and organization. “It is very important to make time to understand exactly what the contract includes. Typically, if a breach occurs, the cloud vendor is not responsible. On the other hand, if something goes wrong on your end that affects other clients of the cloud vendor, then you are responsible. You have to understand these risks, before deploying a cloud solution.”

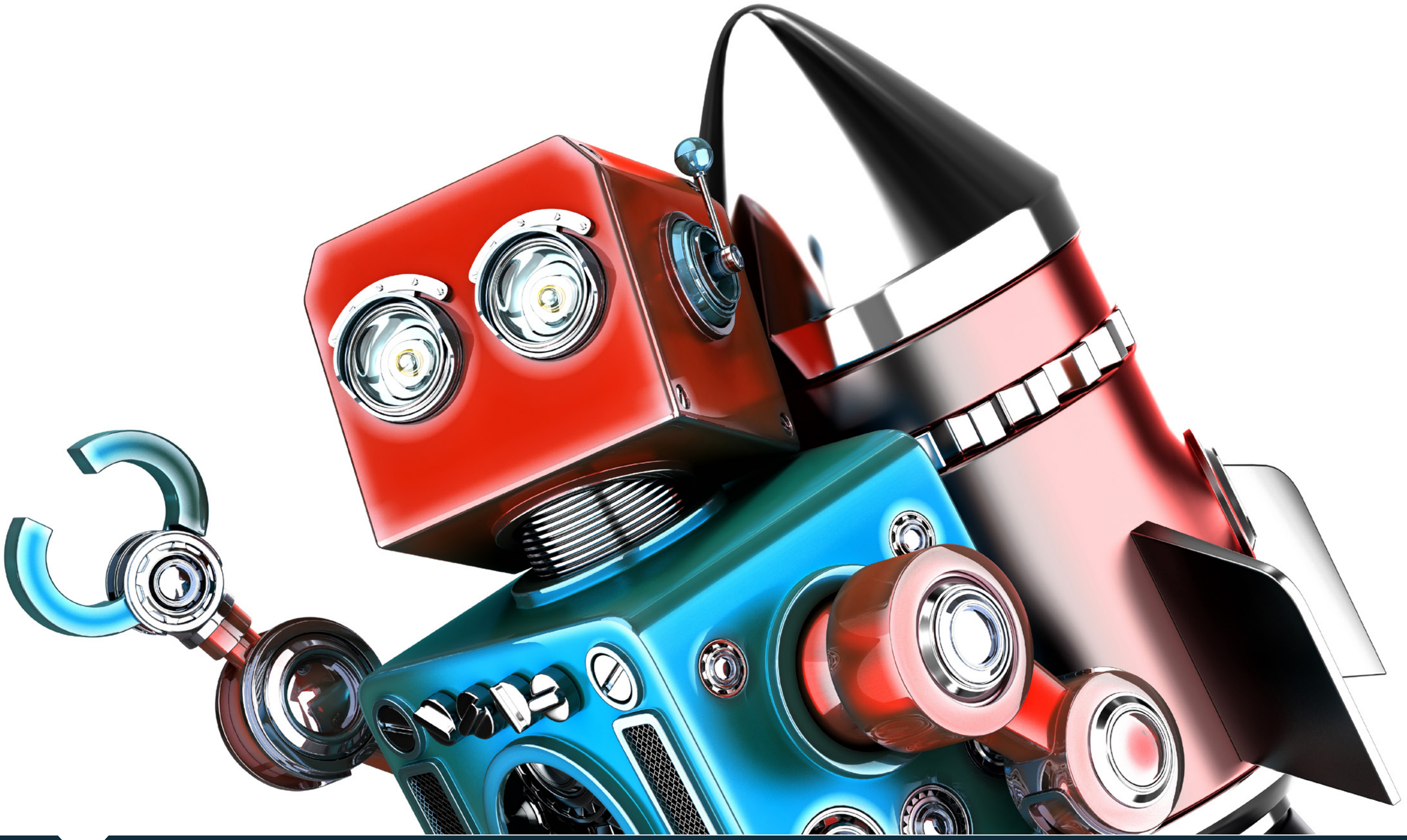
The cloud is enabling rapid innovation, and new vendors are emerging all the time. The pace of change means that sometimes security is lacking - even at cloud security vendors.

The Cloud May Cast a Big Shadow

Anthony Siravo is the CISO of Lifespan, where they have adopted cloud services for the cost savings and efficiency gains. But the advent of the cloud has brought new challenges in the form of shadow IT for Lifespan. “We have incidences where users purchase cloud services on their own credit cards. This opens up a range of vulnerabilities for us. We have no insight into the security measures of those cloud providers. It can become very difficult to effectively manage an incident in those situations.”

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446



DIGITAL TRANSFORMATION

JUNE 2017

K logix

WWW.KLOGIXSECURITY.COM
888.731.2314