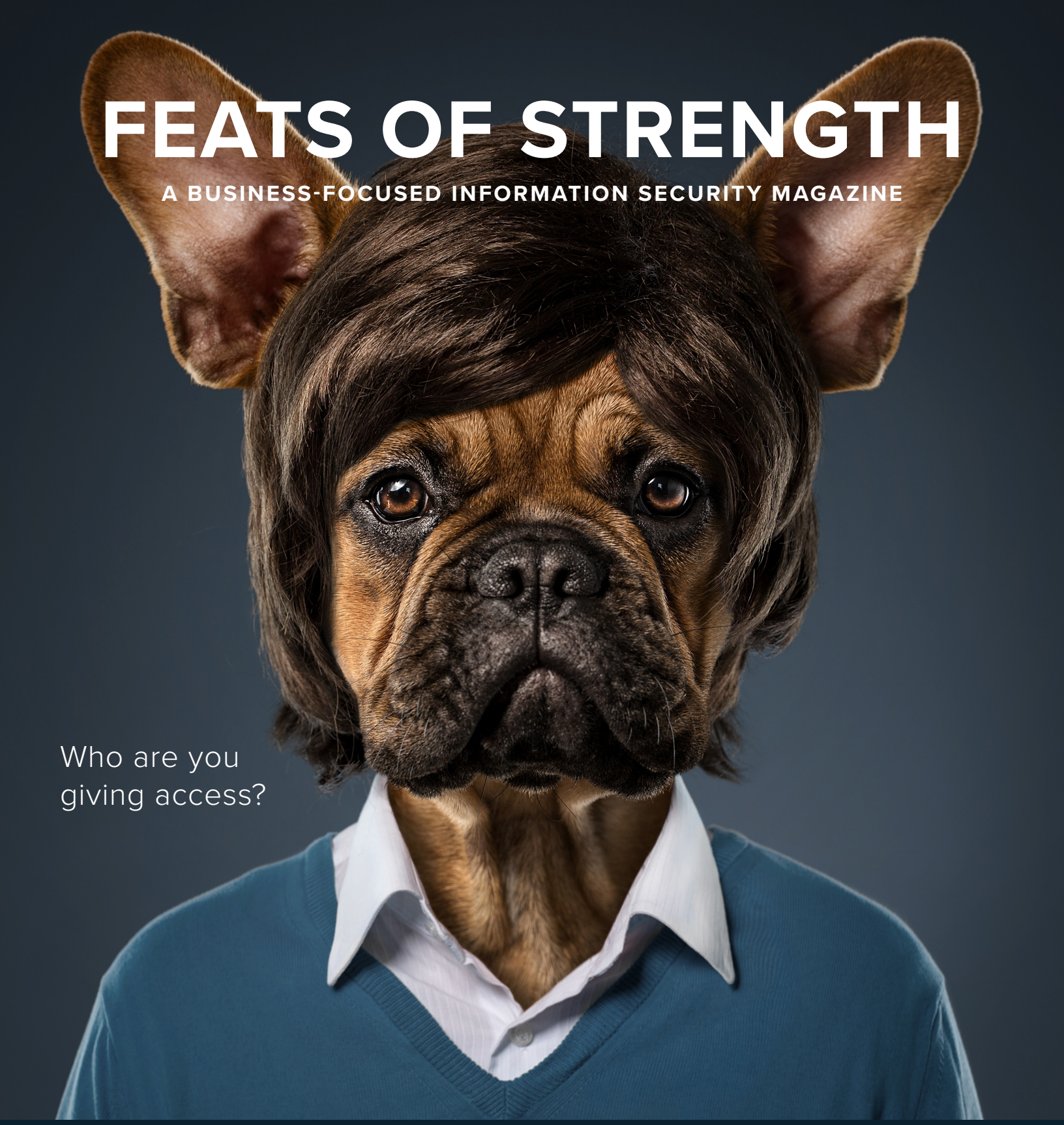
FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE



Who are you giving access?

IDENTITY & ACCESS

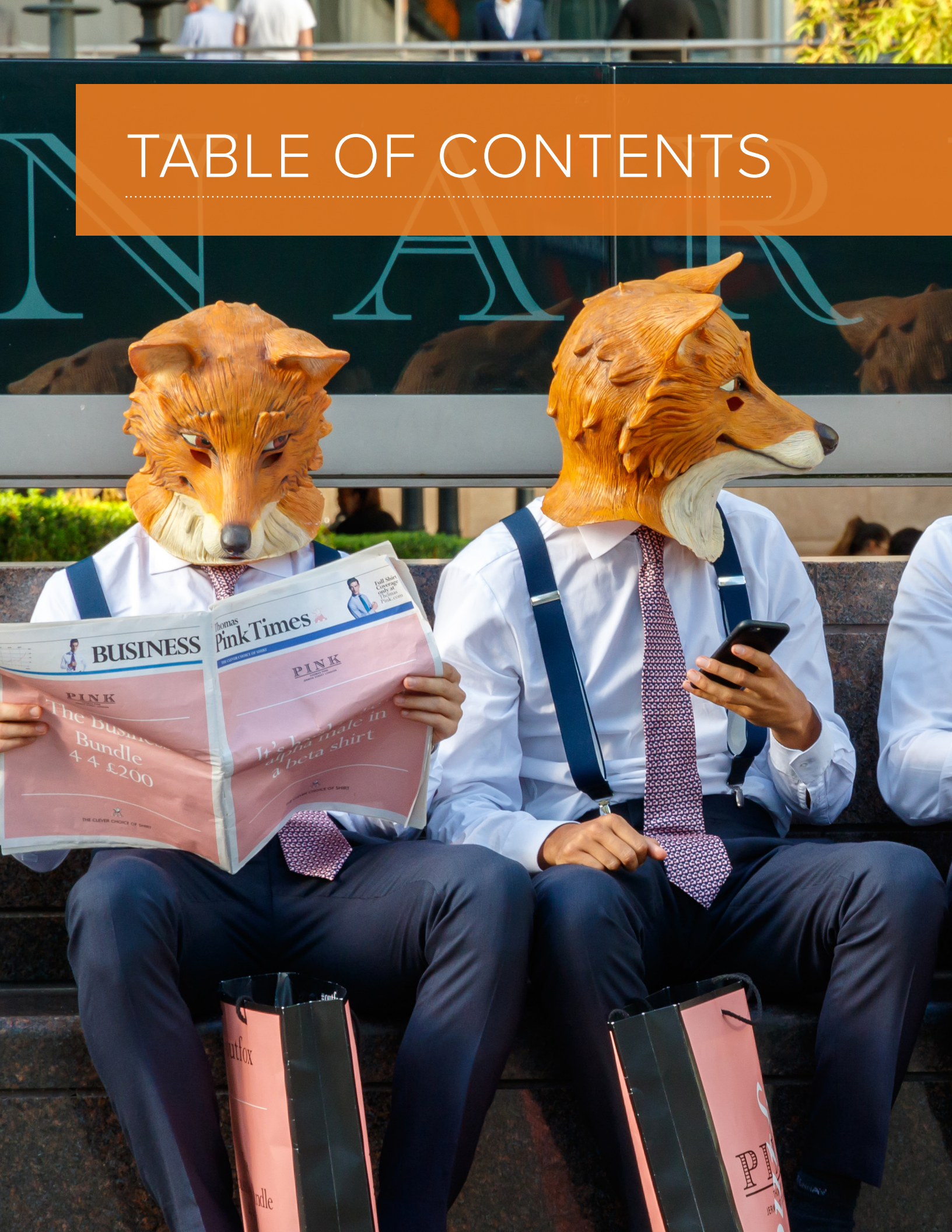
SEPTEMBER 2017

WWW.KLOGIXSECURITY.COM 888.731.2314

K logix

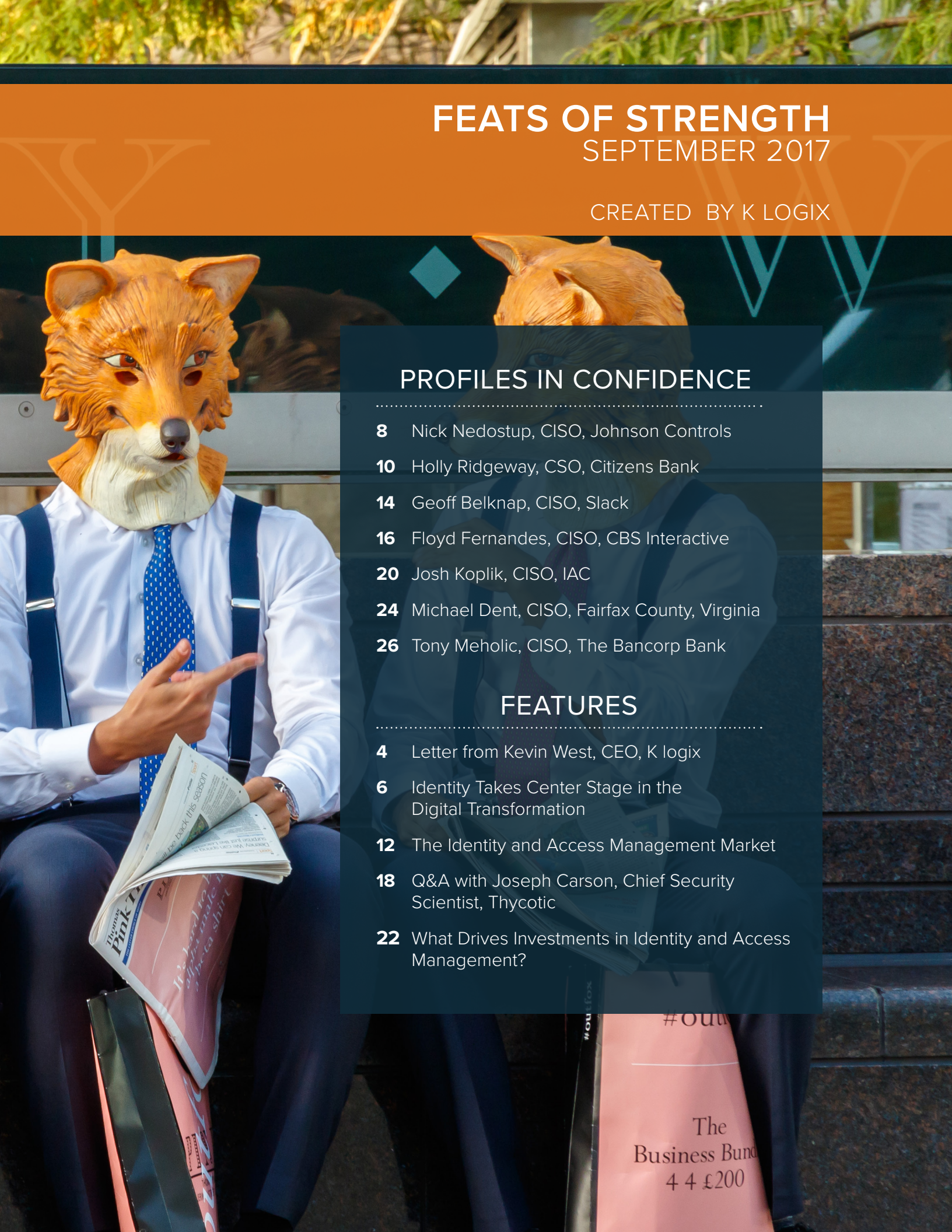
Earning the right to be confident in information security

TABLE OF CONTENTS



FEATS OF STRENGTH
SEPTEMBER 2017

CREATED BY K LOGIX



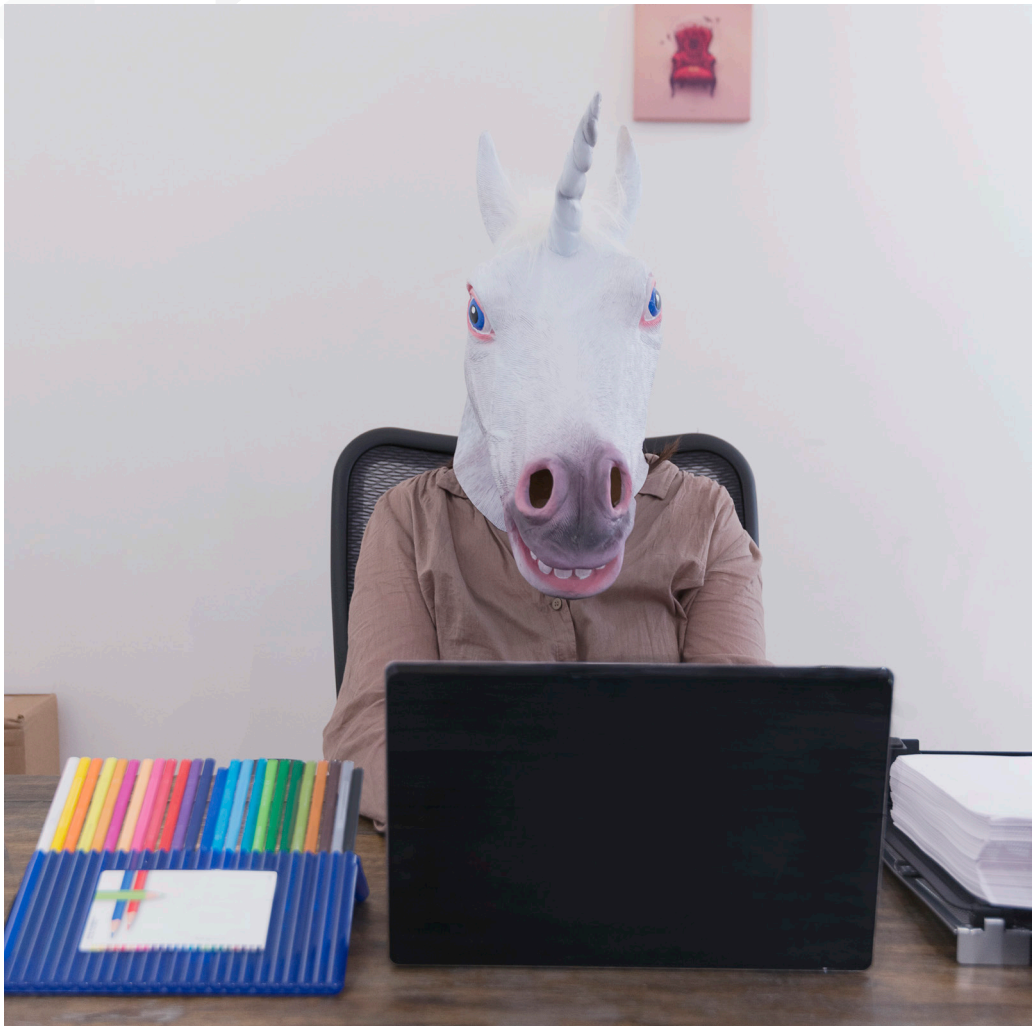
PROFILES IN CONFIDENCE

FEATURES

LETTER FROM

KEVIN WEST

CEO



MY PASSWORD IS 1MPO$$!BLE

I dislike passwords immensely. Sounds crazy coming from a CEO of a security company? Maybe not. I think nearly everyone knows the anxiety and frustration when making their third and sometimes final attempt to get into an application before they get locked out. Trying to maintain so many different passwords for business and personal applications is mind bending. At work, my employees hear me exploding and they know it is for one of two reasons; I forgot a password or I'm being asked to change an existing password. Our internal IT team dare not give me their canned answer around the need and value of passwords. My rants always include how I truly understand why information security programs get a bad rap as productivity inhibitors.

Passwords are a burden and they make me less effective. Multiple passwords create inefficiencies, limit effectiveness and are a drag on productivity. If password management is a nightmare for someone like me with years of security experience and a real understanding of the value of identity protection, we have to know this is a major problem for enterprise users.

No matter how strong the security awareness training program, when identity and access control impede productivity, CISOs lose the support of their organization. And, when CISOs are seen as an impediment rather than an enabler, it puts the entire security program at risk.

STRATEGIC IDENTITY PROTECTION

The good news is that as an industry we are

re-imagining identity protection. Until recently, identity was not a strategic element of any security program. Combined with access controls and user provisioning, identity management was viewed as a tactical element that lacked a coherent and thoughtful strategy. That is just one of the reasons why we have so many passwords.

Identity is not just a security concern, and not just a password problem. In fact, as we explain in our article on the significant market growth for IAM, identity is fundamental to nearly every part of the organization. Chief Marketing Officers have made customer identity central to their marketing campaigns, creating unique user profiles and targeting customers based on their digital footprint. Human resource and IT departments assign identities and user privileges each time an employee or contractor joins or leaves the organization. Risk and privacy officers view identity proliferation as a challenge they must manage to achieve compliance and protect personally identifiable information.

Every executive at the table has a stake in identity, but the onus is on the CISO to lead. As Fairfax County CISO Michael Dent says in his profile, "our leadership is clear that identity is a security issue." As explained in "Identity Takes Center Stage," also in this issue, next generation identity protection strategies will incorporate intelligent identity monitoring, understand a user's entire digital footprint, and leverage behavioral analysis to predict threats. Strategic CISOs will embrace these new tool sets as part of their overall IAM program.

AN OPPORTUNITY TO MAKE AN IMPACT

Regular readers of our magazine will recall that CISOs we interview report three top priorities.

1. Align with business goals

2. Enable competitive advantage

3. Make an overall positive impact on their business

Creating a strong identity protection program affords CISOs the opportunity to align with the business goals of other executives, and enable agility, which is a competitive advantage, at the same time.

There is another piece of the puzzle that makes this the perfect time for CISOs to re-engineer their identity protection programs. Nearly four out of five CISOs list digital transformation as their major challenge. Floyd Fernandes, the CISO at CBSi, discusses this challenge in his profile in this issue of the magazine.

Digital transformation, in and of itself, represents significant change for users. They must learn a new way of working with data and applications. CISOs who engage early on in digital transformation discussions may influence how identity is addressed and secured in the cloud. This allows CISOs to introduce a comprehensive identity strategy as part of the change that digital transformation requires, making it a lot more palpable to business users, and therefore a lot easier to roll out.

Whether they are tackling identity protection challenges in the era of digital transformation, or other program elements, I continue to be impressed with the quality and vision of the CISOs that we profile in Feats of Strength. In this issue, in addition to Fernandes and Dent, we also profile Holly Ridgeway, EVP and CSO at Citizens Financial Group, Geoff Belknap, CISO of Slack, Josh Koplik, CISO of IAC, Nick Nedostup, CISO of Johnson Controls, and Tony Meholic, CISO of The Bancorp Bank. Each of these executives share their insights on tackling specific challenges with thoughtful and strategic security programs.

As I consider our path forward to solve the identity protection challenge, three things are clear to me. First, digital transformation represents a great opportunity to usher in a new identity strategy. Second, CISOs will gain even more organizational leadership credibility when they deliver seamless and transparent data and application access that empowers user productivity. Third, I cannot possibly remember one more password.

Please enjoy reading this issue and learning more about this pivotal topic. As always, we love to hear your feedback.

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.

Identity Takes Center Stage in the Digital Transformation

By Stephanie Hadley
Marketing Content Manager

Mobility, cloud computing and the Internet of Things (IoT) are game-changing technologies that are enabling massive innovation in business. With all the innovation, efficiency and advancement they bring, they also expose new security risks.

- **Threat vectors are multiplying**
- **Access control is overwhelming burdened security staff**
- **Data and information are being accessed from outside of the secure enterprise network**

Despite the risks and exposures, saying no to these innovations is simply not an option for most CISOs; the business benefits are too clear. According to our own data from K logix interviews of CISOs, 79 percent of organizations have already, or will soon, invest in digital transformation.

As a result, security teams must embrace this evolution and enable their enterprises to reap the business benefits of these innovations in a secure and transparent manner.

A key piece to securing the digital transformation is identity. As identities proliferate within cloud computing, securing those identities and limiting access to only appropriate users is a high priority.

AVOID AN IDENTITY CRISIS

Identity protection, long bundled with access management as an administrative function, is now a critical component of comprehensive security strategies. We asked CISOs and other C-level executives how identity protection programs are evolving this year.

"As we see more of a digital transformation continue within organizations, the proliferation of digital identities along with internet enabled devices will become more of a reality, and also a challenge to properly secure. Intelligent and effective identity protection strategies are crucial to cover the breadth of a user's total digital footprint." - Rick Grimaldi, Chief Strategy Officer, K logix

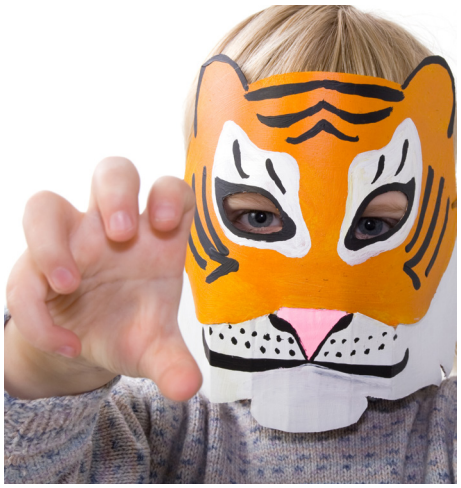
Identity protection strategies must enable an organization to understand and secure a user's complete digital footprint while being transparent to the business user and operations.

Many organizations are aspiring to least privileged access models, both to meet compliance requirements and to ensure better protection of critical assets. Tony Meholic, CISO at The Bancorp Bank says, "User access is a huge priority for us. Now we know everyone's system access automatically and systems that interact with PCI data are flagged. The participation from management is much better, largely because the systems is web-based and simple to use. Our user access levels decreased 8 percent in June. Now we are trending towards least privileged access."

> "Intelligent and effective identity protection strategies are crucial to cover the breadth of a user's total digital footprint."
>
> - Rick Grimaldi, CSO, K logix

80% of all security breaches involve privileged access

Identity is the Weakest Link



Forrester Research estimates that 80 percent of all security breaches involve privileged access. In the age of cloud computing, user access is the weakest link in the network, and ripe for exploitation. As a result, identity protection is increasingly a first line of defense.

In PWC's 2017 "State of Information Security", Richard Kneeley says, "Identity has been at the heart of almost every breach in the past two years. Many of these breaches have involved someone gaining access by using compromised identity, then changing their identity once inside the network to ratchet up access to data and systems by taking over a privileged account and in the process gaining unlimited access to the network, to systems and to data."

HOW ARE YOU ADDRESSING IDENTITY IN THE ENTERPRISE?

As a broad technology category, Identity and Access Management has a long history in security and IT departments. As a result, many organizations are running multiple IAM solutions, and controlling user access in a variety of ways across systems and departments. This patchwork strategy creates confusion, limits efficiency and is difficult for strapped security teams to manage.

As CISOs look to next generation IAM tools that enable behavioral analysis and intelligent identity protection, many need help understanding the capabilities of their existing investments and mapping a go-forward strategy.

K logix's Identity and Access Management project advisory service helps clients understand the following:

• Identity management solutions for on-premise and cloud environments;

• Ways to address elevated privileges with security and monitoring;

• How to empower individuals with access to the right resources at the right times and for the right reasons;

• When to enforce second factor or adaptive user authentication to critical or sensitive infrastructure, apps, accounts, and data;

• Available solutions to analyze normal and anomalous user behaviors that may be indicators of an attack or insider threat activity.

K logix's project advisory service helps security organizations strategically address their specific identity protection challenges with organization-specific decisions about appropriate technology and policies.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

NICK NEDOSTUP
CISO, JOHNSON CONTROLS

HEADQUARTERS: Cork, Ireland

EMPLOYEES: 120,000

ANNUAL REVENUE: $37.7 Billion

"We are constantly maturing our program, and doing everything possible to create a secure environment in ways that do not prohibit the business from meeting customer expectations and achieving our goals."

- NICK NEDOSTUP

THE CONVERGENCE OF PHYSICAL AND DIGITAL IDENTITIES

"There is a lot of focus in the information security industry on digital identities," explains Nick Nedostup, CISO at Johnson Controls. "But we also must consider physical identities, such as when someone enters a building, and which system controls - like lights or heating systems - they access. In the future, we must combine physical identity with digital footprints to track a person's complete identity as it relates to the enterprise."

When it comes to the convergence of physical and digital identity, few people have more direct experience than Nedostup. As CISO of Johnson Controls, which creates intelligent buildings, efficient energy solutions, integrated infrastructure and next generation transportation systems that work seamlessly together to deliver on the promise of smart cities and communities, Nedostup is responsible for the organization's enterprise cyber security program and is a major contributor and advisor to the company's Building Technologies & Solutions business development team.

One area of focus at Johnson Controls is the ability to help its customers' organizations understand and track physical and digital identity as one. "Our Buildings business development team is looking into the convergence of physical and cyber worlds, and exploring opportunities in the space," comments Nedostup. He works in a consulting capacity with the business, helping shape understanding around the capabilities of specific start-ups and to evaluate market demand as Johnson Controls considers new lines

of business, or adding security components to existing technologies.

Nedostup is a contributor to the company's business priorities in other ways as well. Johnson Controls sells many environmental controls which are now network-connected. He explains, "There was a big push to IoT, and early on I realized that security needed to be a component of these solutions. I raised this as a risk to the executive management team, and now I collaborate with the right leaders to build cyber security into our IoT 'Smart Building' products where appropriate."

He also plays a role as security advisor to the engineering team, and a sounding board for product development and marketing. "In the past, the client's CIO or CISO was not involved in purchase decisions. But now with these systems connecting to the network, information security has a seat at that table. I provide advice to our Buildings engineering team on what types of security controls should be built into the systems, and the specific concerns our clients' CISOs will have with the products," says Nedostup.

> "Being seen as a credible source is one of the most effective ways to grow the security budget."

ENABLE THE BUSINESS TO MEET CUSTOMER EXPECTATIONS

Nedostup's multifaceted role enables him to contribute to the solutions that impact the bottom line, while simultaneously maintaining the enterprise security program. Acquiring an MBA provided Nedostup a well-rounded, business-minded perspective. He says, "I understood that to provide real value to my organization and my internal customers, I needed to step outside of a traditional technology role, and shift into a business role. This shift allows me to see that security will never be the sole focus for an organization – we operate in the buildings and energy storage platforms. The function of information security, and I as the CISO, must enable the business to go forward in as secure a manner as possible, knowing we are not going to mitigate every risk. We are constantly maturing our program, and doing everything possible to create a secure environment in ways that do not prohibit the business from meeting customer expectations and achieving our goals."

Nedostup is proud of the achievements his team has made in the area of cyber security. "Our cybersecurity capabilities and maturity levels are far higher today than even a couple years ago. We've experienced rapid, focused and efficient advancement. We now have greater visibility into cyber issues, faster response times, and ability to contain and remediate threats." While these factors are critical to a strong security program, Nedostup says, "It's also critical that I serve as a trusted advisor to the business, that I have the ears and attention of our executives in understanding security as a risk area. We will always be refining what we do, of course, but I am proud that the security team operates at the business level, not just in the technology space."

BUILD CREDIBILITY TO GROW THE SECURITY BUDGET

Nedostup believes in the importance of building credibility with senior executives as a key element to grow the security program. He comments, "At times, I feel our industry focuses too heavily on fear, uncertainty, and doubt to drive program growth. But to be a trusted advisor to the other executives, I need to make them aware of risks, without blowing things out of proportion. Being seen as a credible source is one of the most effective ways to grow the security budget."

"Specifically, it is important to gain trust from the CIO, CFO and CEO – without it, it is rather difficult to be successful," suggests Nedostup. "That trust is built on being excellent stewards of our cybersecurity investment dollars, and ensuring we're supporting the business in every way necessary. We have to be purposeful and prudent in our requests, and be clear about how security investments enable the business to reach goals and mitigate risks."

Nedostup's effective campaign to build credibility and influence has enabled him to structure his team in a way that naturally and effectively aligns with the business. "Our team consists of experts from across the cybersecurity space, who are also knowledgeable about our business demands. We strive for continued partnership and alliance with the business to best enhance our cyber security program and effectiveness, and help the business achieve its growth and customer satisfaction goals."

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

HOLLY RIDGEWAY
CSO, CITIZENS FINANCIAL GROUP

HEADQUARTERS: Providence, RI

EMPLOYEES: 17,600

ANNUAL REVENUE: $5.25 Billion

THE POWER OF MENTORSHIP

"I would not be where I am in my career if not for my very first mentor. She was the Deputy CIO at the FDIC when I worked there as an assistant early in my career," explains Holly Ridgeway, the Executive Vice President and Chief Security Officer of Citizens Financial Group. That early and critical mentorship set Ridgeway on a successful trajectory, from college through the government, private sector and to her current role as CSO at Citizens.

Ridgeway continues, "The mentorship relationship is extremely important for everyone in IT and information security, but especially for women and minorities. I have selected a mentor at every organization for which I have worked. My first mentor from the FDIC is retired now and I asked how I could repay her for all she did while I was under her wing. She said I should pay it forward. I have tried to live with this as my core philosophy ever since then."

Ridgeway has taken that request to heart. She is concerned that the United States is lagging behind other nations in the development of cyber security talent. That concern combined with her commitment to mentoring inspired her to take on a number of advisory roles as

> "I would not be where I am in my career if not for my very first mentor."

she has advanced in the information security industry. Ridgeway teaches the capstone course in information security at the University of Maryland University College. She strongly supports the Wounded Warriors program, as well as women and minorities to help them understand the exciting opportunities available in the cyber security industry. Recently, Ridgeway attended the National Governor's Conference and made contact with Girls Who Code to support groups that help close the gender gap.

She encourages other CISOs to reach out to young people to educate them about careers in information security. She says, "We need to start at an earlier age, we need to give students access to curriculum that will drive their interests. Everyone thinks forensics is what they see on CSI, and they are excited by that. Forensics is

also important to cyber security, but right now the interest is not driving enough people to enter our industry." Ridgeway believes one reason is the negative press attention given to cyber security. "The breaches and hacks in the media make cyber security seem scary. The truth is there are many interesting aspects to cyber security, but we do not do a good job of educating them."

In Ridgeway's opinion, young people can be a tremendous asset to her team. She says, "These are our team members who are recent college graduates/interns just starting their career in cyber security. They are not boxed in by assumptions or past-preconceptions. They are extremely innovative."

APPLYING LESSONS LEARNED

In her diverse career, Ridgeway helped build out the FDIC's FISMA compliance program, participated in the creation of the information assurance program at the FBI and has stood-up many Security Operations Centers, the first one being at the FBI years ago. Ridgeway has collaborated with many government and private entities including; NIST, DHS, BITS and the FSISAC. She took on the CISO role at PNC, then expanded her expertise across more industries while consulting at Mandiant. She currently is on the board of Directors at the NCFTA.

Now as CSO at Citizens, Ridgeway reports into the Head of Business Services, who reports directly into the CEO. This organizational structure gives Ridgeway strong visibility within the company, and exemplifies the bank's commitment to security. Her team is comprised of approximately 200 employees who work across seven specific functions ranging from cyber defense and physical security to identity and access management.

Over the years, Ridgeway has defined an established method for starting her program with any organization. "In the first 90 days, I observe. I dig into all the programs, I build relationships and I emphasize collaboration. Citizens had already made great strides in security before I arrived. As I looked at the program it was already in alignment with the business, and I can focus on ensuring our program evolves to address new risks and requirements." She explains how the company is currently reviewing required adjustments to be in compliance with the NY DFS cyber security regulations.

Ridgeway is applying her deep understanding of risk assessments and gap analysis to identify the improvements to keep pace with business changes. In addition to helping her identify new risks, the assessment provides a good baseline, helping Ridgeway understand which data is most important to the organization, and where that data resides.

Ridgeway notes, "My team is strong, and the foundation of the program is very strong as well, but it is my job to understand emerging threats and most importantly ensure we are continuing to align strategically with the business. Each time a business unit unveils a new distribution area or a new service, our security risks also change. My team needs to be able to adapt to that within our program. We have to ensure that security is transparent to the business and customers."

FOCUS ON PROTECTING DATA

Ridgeway keeps her team and program on track by maintaining clear tactical priorities as well. She explains, "In the end, security is all about protecting data. Data, data, who has my data? That means we need to take a close look at the technologies that we rely on and also the third parties that have access to our data. We need to understand what their security looks like as well."

Among Ridgeway's first steps at Citizens is an evaluation of the security technologies running inside the company. "We are in the middle of a total review of our systems. First, we are looking at those systems that require a lot of daily care and feeding – intrusion detection systems, tools for monitoring correlation, identity and access management and network visibility. Are we maximizing the performance of our investments? There is no point in running a security tool that does not deliver actionable data and value."

Ridgeway suggests that while many of the larger security vendors have added technologies to their product suite, those new solutions sometimes suffer from lack of funding and focus. "We have to be careful about consolidation. 'Jack of all trades' and 'master of none' definitely applies to some of the bigger vendors. As an organization, we still need specialty products. In general I am a fan of mixing it up as part of a defense in depth strategy. That way an organization's network is not exposed to the vulnerabilities of a single product."

For advice on which new security innovations to bring into the organization, Ridgeway relies, in part, on the same people she herself is mentoring. She explains, "My students are required to do a technology evaluation as part of the course curriculum. The information they pull together is very insightful." She combines input from her students' reviews with insight from all industry sectors, conferences, employees and peers, and relies on bake offs and proofs of concepts to validate solutions before implementing them at the bank.

THE IDENTITY AND ACCESS MANAGEMENT MARKET: DEMAND FUELS INNOVATION, GROWTH, INVESTMENT

North America is the largest revenue generator of the Identity and Access Management Market

North America is contributing maximum toward the Identity and Access Management Market through component, deployment type, and organizational size. The changing needs of the workforce, adoption of cloud applications, BYOD, and mobile practices along with meeting the heavy compliance regulations are driving the organizations in North America to adopt IAM solutions. Europe and Asia-Pacific are the second and third-largest regions in terms of market size for identity and access management.

(Report by Markets&Markets; Identity and Access Management Market by Component (Provisioning, Directory Services, Password Management, SSO, & Audit, Compliance, and Governance), by Organization Size, by Deployment, by Vertical, and by Region - Global Forecast to 2020)

The Identity and Access Management (IAM) market is flush with cash from private investments as well as customer deals. Venture capitalists and enterprise organizations alike are investing in new artificial intelligence and machine learning solutions for managing the rapid proliferation of identities and achieving least privileged access.

A quick walk of the RSA Conference floor, or a listen to your voicemail inbox is proof enough that the IAM market is among the hottest segments in cyber security. However, just in case you need numbers to back up this claim, we have data from industry pundits and research firms that emphasize the point.

Global Identity and Access Management market will reach **$20.87 billion** by 2022, growing at a rate of 14.8%.*

The Identity and Access Management market reached **$8.09 billion** in 2016.**

* Orbisresearch.com
** Markets & Markets

Reports on spending priorities from CISOs validate these market numbers and growth potential

Access and authentication outpace other security technology priorities including advanced malware, endpoint security and data protection technologies. (PWC's Global State of Information Security)

Access and authentication is the number one spending priority for CISOs this year. (SANS)

Venture capital investment in identity and access management

With the influx of VC funding and intense interest in the marketplace, IAM solution providers raised $362 million across 34 deals in 2016. (CBInsights)

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

GEOFF BELKNAP
CSO, SLACK

HEADQUARTERS: San Francisco, CA

EMPLOYEES: 800+

ANNUAL REVENUE: $150 million

AN 'IMPACT JUNKY'S' APPROACH TO FINDING THE RIGHT OPPORTUNITY

"One thing that I have learned about myself is that I am somewhat of an impact junky," explains Geoff Belknap, CSO of Slack. "It is very important to me that the decisions I make matter to the business and customers. I want to make a positive impact." The desire to be involved in change is what lead Belknap to take the CSO position at Slack, the fast-growth collaborative communication start-up known for changing the way businesses work.

"First, I was excited by the opportunity at Slack because the founders were behind Flickr, a tool that had a big impact on my own life. I became more intrigued during the interviews for the CSO position when I learned exactly how many enterprises and businesses are changing the way they work with Slack." Belknap points out that "many of the Fortune 500, and nearly every media company is using Slack today."

Belknap realized Slack was making a difference, and his desire increased to understand the type of impact he could make as CSO. The answer: a big one. Belknap comments, "Slack has a very serious security program and it is very important to the business and users. The truth is you are not free to do your best work and innovate if you are not sure your platform is secure. That is the promise Slack is making to our customers - a secure platform to make change happen."

> "I'm not focused on addressing any one specific security problem. My priority is to make sure Slack can continue to grow and enable our customers to innovate."

Slack's commitment to security is ingrained in the product and

culture, which makes Belknap's job easier in terms of getting executive-level buy-in for policies, programs and budgets. He says, "When I first met with Slack executives about the security program I said we really need to lean forward. I told them I needed to build a team of 100 security experts. I was joking; but they were committed. They said, 'If that is what you need, we will give it to you.' I do not need a team of 100, but knowing that I have that level of commitment from the executive team is very satisfying."

During the on-boarding process Belknap met with Slack's Board of Directors, another sign of the organization's steadfast commitment to security. He explains, "In those meetings it became clear to me I was going to influence the strategy and tactics of the business from a security perspective. One of the hardest things for any CSO to do is to convince their peers or the Board of the importance of security. That was a non-issue for me. I already had their understanding."

COMMITMENT TO SECURITY STARTS AT THE BOARD LEVEL

As CSO of Slack for nearly two years, Belknap's relationship with the Board continues to mature and they remain focused on security as a critical component. He says, "I talk to the Board on a quarterly basis. We talk about the types of threats facing us as a business and what we do with the information we have on specific threats. We cover changes to our long-term security strategy. I think that the Board most appreciates our question and answer sessions. They share their concerns and problems that they are hearing about at their own organizations as well."

Belknap also meets regularly with the audit committee and performs an annual risk assessment. He explains, "On a monthly basis, I meet with the executive risk committee. We look at steps that we are taking to mitigate risks and review the accepted risks of the organization." The audit committee includes other senior leaders at Slack, including the CTO, CFO, and the risk and compliance director from Belknap's own team.

BUILDING CUSTOMER TRUST THROUGH TRANSPARENCY

Belknap says the company's risk program is focused on building long-term customer trust, something mission-critical for Slack. He explains, "It is hard to build trust and easy to lose trust. It is nearly impossible to regain trust you have lost. Our security program is focused on delivering a solution that our clients can trust. As a result we focus on the things our clients ask us to do to prove our trustworthiness." That list includes security engineering, operations, risk management, and application and platform security.

Part of building long-term trust is delivering absolute transparency to customers. This is something Slack tries to do at the corporate-level, and Belknap's security team aims for total transparency as well. He admits it is hard. He asks, "How many people are happy to expose all their flaws? I'd argue no one. But, that is also what you really need from the people with whom you do business. It is not easy to be as transparent as Slack is, and we get a lot of criticism that stems from our sharing of flaws. But what we are providing is real transparency, and that is important to our customers." For Belknap, transparency means making sure clients understand any vulnerabilities, and know Slack has addressed them, or put a plan in place to do so.

"I'm not focused on addressing any one specific security problem. My priority is to make sure Slack can continue to grow and enable our customers to innovate," states Belknap.

The Future of Information Security Is Advocacy and Education

"Information security is easy to understand in broad brush strokes, but to fully understand the situation there is a lot of science involved. We need to educate both consumers and lawmakers so that they can better understand the technical nuances driving the digital economy. That will help them understand the requirements needed for security. As an industry, we need to do more education. We need the equivalent of 'seatbelts save lives', or the anti-smoking campaigns. Consumers need to understand that they can make smart choices when it comes to security, and that those smart choices can impact the broader community in positive ways."

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

FLOYD FERNANDES
CISO, CBS INTERACTIVE

HEADQUARTERS: San Francisco, CA

EMPLOYEES: 3,000

ANNUAL REVENUE: $1 Billion

BUSINESS FOCUSED LEADERSHIP

Floyd Fernandes is a first time CISO currently working at CBS Interactive's head office in San Francisco, CA. Prior to CBS Interactive, he gained extensive security experience in several roles including one where he built an application security program from the ground up. He says, "I didn't see much of a fundamental shift when moving into the CISO role as I was still in charge of building business wide strategic security programs. However, one key aspect that changed the most was building relationships with the business side of the organization. I had to understand their functions, challenges and how security could play a fundamental role as a business enabler."

Less than one year into his CISO role, Fernandes leads the information security strategy for CBS Interactive's online content network & operations. The media company includes some of the top native digital brands in the industry, with more than 290 million unique visitors each month and a global top 10 web property covering business, entertainment, games, news, sports and technology.

The challenge of fulfilling the role of first-ever CISO was compelling to him. He felt confident taking on this new role because of the organization's clear executive-level commitment to security. He comments, "Ultimately, our core function is to deliver content with 24x7 uptime and availability. The C-Suite recognized how critical a strong security program is to protecting that revenue stream."

BUILDING EXECUTIVE BUY-IN

When coming into a new organization as CISO, Fernandes says, "The first focus during an interview process should be understanding if you have buy-in from the C-suite and Board. Security must be a focus and the leadership team must back you in terms of helping make your programs actionable. The second and third things are budget and talent."

A key recommendation is conducting a third-party risk assessment when coming into a new organization. He says, "The risk assessment process should include interviewing business leaders to gauge security awareness, risk and performing an assessment of the environment. This type of assessment can be completed in two-to-three weeks and provides a lot of ammunition for a new CISO starting a program." He believes it is beneficial to have the third parties' findings of the assessment included in the executive briefings so the new CISO has actual quantitative data to back the proposed strategy.

Security awareness and education are top priorities for him and he believes CISOs should ensure they continue to educate

stakeholders, leadership & business leaders on current risks, key security initiatives & establish key performance indicators. While compliance may be a requirement, risk management tied to key business risk will gain greater traction and ability to execute.

He continues, "CISOs should meet weekly with business leaders. These meetings help facilitate the strategy and direction of were the security program is heading. The security team should be viewed as advisors not enforcers of change. Instead, CISOs must help foster a culture that is security aware. We need to provide business users with the appropriate processes & tools to reduce risk through their current workflows."

Fernandes explains, "I work to understand the business leaders' operational challenges. For example, how they are ensuring 24x7 uptime of content. I look at their pipeline and their workflows and then I work to embed security process and tools into that pipeline."

"As we all know the truth is security is front page news, so executives want to do the right thing. They need to understand from that risk profile what the right thing is in the context of their business. They want to understand the resources they need and how to onboard new solutions. CISOs must explain the importance of identifying and protecting important assets, such as content, PII, credit card data, and more."

ALIGNING CORPORATE PRIORITIES AND ENABLING DIGITAL TRANSFORMATION

Fernandes shares his approach to a successful security program:

1. Strategic: Strategic programs should map to the company's strategic vision. For media and other organizations, that could mean a focus on enabling digital transformation.

2. Tactical: Tactical goals should include prioritized security initiatives such as identity & access, metrics, threat management and staff development.

3. Operational: Operational programs should include the roll-out and support of relevant security tools to support the strategic and tactical initiatives.

With the large impact of digital transformation on many organizations, Fernandes knows the benefits and challenges of transitioning to the cloud. He says, "When you are moving to the cloud, one important thing is that all the principles you had for the data center are effectively different because with the cloud you lose the visibility and control of the infrastructure level. That means your team's talents and focus need to change as well. The people who understand the data center must become knowledgeable and relearn what the cloud means. A key aspect of this is investment in staff development. It's important to focus on hiring people with a developer background even more than a security background when it comes to the cloud."

He continues, "The move to the cloud also requires a focus on vendor management. In the cloud, the guarded wall around the data center no longer exists. You have to take a close look at the entire environment in a new light and determine how the security controls holds up."

Fernandes points out that digital transformation and the pace of innovation in general has forced him and other CISOs to consider the effectiveness and relevance of security technologies in their environments. He notes that companies struggle with too many security products installed and many more start-ups to consider.

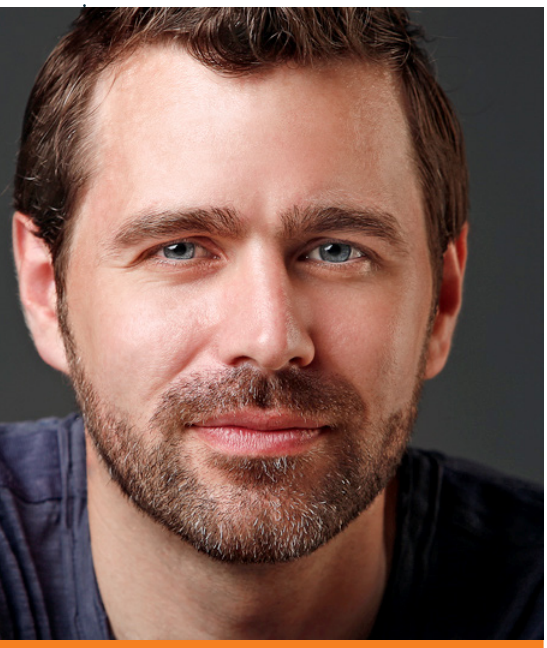
To avoid clutter and technology overload, he sticks to a strict set of requirements for technology purchases. "It's not about the technology, it's how you develop processes to effectively manage the risk in the cloud to support the digital transformation. Focus on the following: increase visibility into the network, protect the identity of all users, & the data they access. Maintaining that focus helps eliminate some of the noise from the market."

Retaining Talent

When competing to retain and attract top talent to an information security team, Fernandes recommends selling the mission of the business and not the security program. He says, "You want a new team member to come on board because the organization you are working for is doing something that excites them. For me, I'm always focused on the importance of culture and vision."

Q&A WITH JOSEPH CARSON

CHIEF SECURITY SCIENTIST, THYCOTIC



Joseph Carson has more than 25 years' experience in enterprise security specializing in blockchain, endpoint security, network security, application security & virtualization, access controls and privileged account management.

Q: WHAT ARE THYCOTIC'S CORE VALUES?

Our company believes in our people. When you have passionate, intelligent thought leaders all working together, it allows for synergy and excitement.

We care about solutions. As a company, our core focus is on privilege access management. All of our efforts and passion are to make sure we are the most experienced and knowledgeable about what we do. As a global leader, we protect against one of the most targeted and compromised areas in the industry, and we need to be sure what we offer provides this.

We ensure ease of use. There can no longer be software that takes months to install, is complicated to integrate and hard to use. Threats evolve quickly and sometimes software cannot keep up. What we do helps companies with an easy installation, ease of use, and ability to effortlessly integrate. This way, companies may advance and evolve quickly to address evolving new threats. I help with security research to ensure our knowledge and vision in the security industry is making a difference and adding value to our customers.

Q: HOW DOES THYCOTIC PROTECT ORGANIZATIONS?

Today, privileged passwords and privileged accounts are the primary targets of hackers. Thycotic secures passwords, protects privileged accounts and controls access. We make it simple and easy to manage for IT admins and security staff. We are also highly adaptable and scalable as well as the least intrusive and readily accepted by all users.

The way we created our solutions make it easy to meet compliance. Thycotic solutions assure the protection and control of your privileged accounts while being the fastest to deploy, easiest to use, and scalable solution. We also automate security without requiring training or consulting.

Q: WHY IS RESEARCH SO IMPORTANT TO THYCOTIC?

We don't just sell software, we become strategic advisors to companies through our innovation and research. We know we have great technology and we don't want to just stop there, that's why we have become an educator in the market. We do this through building relationships and helping guide and navigate companies in areas that are strategic to their business. I am passionate about this because our research papers address key concerns and challenges of security leaders.

Q: WHAT TRENDS ARE YOU SEEING IN THE INDUSTRY?

I attend many worldwide events and conferences as an industry expert. I focus on guidance and sharing knowledge with attendees because I believe helping educate is one of the most valuable things we can do. Combined with industry research, attending and participating in conferences allows

thycotic

THE 2017 STATE OF CYBERSECURITY METRICS ANNUAL REPORT by Thycotic

Failures in Cybersecurity Metrics

58%
scored a failing grade when evaluating their efforts to measure investments and performance against best practices.

4 out of 5
companies worldwide are not fully satisfied with their cybersecurity metrics.

Failures in Planning

1 in 3
invest in cybersecurity technologies without any way to measure their value or effectiveness.

4 out of 5
fail to include business stakeholders in cybersecurity investment decisions.

Failures in Performance

4 out of 5
never measure the success of security training investments.

60%
still do not adequately protect privileged accounts---their keys to the kingdom.

* Results from Thycotic's recently published research paper. Read the rest of the report at: **www.thycotic.com**

me the opportunity to track and discuss trends with my peers.

I've witnessed a significant change to the traditional perimeter. Early on, 'castle walls' were the main defense, and we worked harder and harder to build them bigger with more layers. We added moats and different types of detection. The threat landscape has now changed and technology has advanced. The perimeter is no longer the 'castle walls' since every employee is now a data connection with the potential to leak data or attackers to use them to penetrate the network. Digital transformation has made a significant impact on the way security protects an organization and unique digital identities have now become the new security perimeter.

Q: WHY ARE STRATEGIC ALLIANCES IMPORTANT FOR THYCOTIC?

Having strategic partnerships and alliances helps us become part of a holistic security approach. We work closely with our alliance partners to add significant collaboration to combine solutions and solve greater challenges.

We meet with the best of breed vendors and have strategic conversations about how we can join our technology together to make it seamless for customers to get the most value.

Q: HOW DOES THYCOTIC CONTINUE TO GROW?

We have been through an amazing transition this past year. We've invested heavily into international business. We went from one person to almost forty people internationally.

We also work hard to make sure we strengthen our strategic alliances with the channel. We want to continue to empower our partners so they can become voices for Thycotic.

We are constantly innovating our technology, and continue to grow and add more functionality to our solution. One way we do this is through acquisitions of other companies that complement our technology. We believe it is important to continually look at high value technologies to add more value to our core mission.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JOSH KOPLIK
CISO, IAC

HEADQUARTERS: New York City

EMPLOYEES: 5,800

ANNUAL REVENUE: $3.14 Billion

"In three years my role has evolved from program-building to enabling broader business objectives with security controls. Now business leaders are proactive in coming to me to discuss security as it relates to various strategic initiatives at the corporate level."

- JOSH KOPLIK

FIRST TIME CISO IN A NEW ROLE

When Josh Koplik joined the team at the media conglomerate IAC, he became the company's first CISO. It was also his first time in the role. He says, "It was exciting and refreshing to build the program from the ground up." Koplik says the chance to come into IAC as a trusted expert without inheriting any security "baggage" or pre-existing security programs drew him to the role.

IAC is a portfolio company, which Koplik describes as a "collection of loosely federated businesses." Each individual business, including well-known Internet brands such as About.com and Tinder, have their own IT team. The largest companies have dedicated security staff to handle the operational aspects of the IS program. Since the portfolio companies always had responsibility for security, IAC did not employ its own CISO until the Board of Directors made it a priority.

"To their credit, when a Board member inquired about information security at the company, the senior leadership recognized this area as a weakness and immediately sought to hire for the role. They made a very smart decision in that they aligned the CISO role outside of IT, giving me a lot of authority out of the gate," explains Koplik. "The senior team is very supportive. From the get-go, they have looked at me and said, 'you are the security guy, tell us what to do.'

Koplik reports into the Chief Administrative Officer, and regularly updates the CFO, General Counsel, and the head of Internal Audit on the security program. In regards to the finance and legal teams, Koplik says, "They want to know what is going on with security, so I am in constant contact with them. I do not

Security Challenges of Cloud-Based Businesses

Most of IAC's portfolio companies are only three to five years old. Nearly all of them are internet-based, consumer-focused brands. As a result, these businesses did not have to go through a Digital Transformation. Koplik explains, "These are companies that have been in the cloud from their inception. All the businesses are using Slack, all the teams are working remotely. If there is a trend out there, our businesses are on it. These are organizations that run at a rapid pace of change. That pace can bring about specific security challenges, so we need to be able to react quickly and keep on top of risks, even as new ones are presented all the time."

have to work for their attention."

SECURITY IS A BOARD-LEVEL PRIORITY AT IAC

Koplik presents a security update to the Board's Audit Committee every quarter. He says, "My reports are remarkably basic, and it works well that way. We are always measuring our progress against a scorecard. We have many businesses to track, and each one has its own set of risks. Each practice at each business gets a simple letter grade of A,B or C, to denote practice maturity."

The Board's interest and commitment to security empowers Koplik. He continues, "The Board wants to know of any problems, and 'problem children.' Thankfully, there are very few of those. The Board has made security a big priority, which makes it very easy to gain buy-in and acceptance of policy and programs at the business level."

ADVANCING FROM OPERATIONAL SECURITY TO STRATEGIC ADVISOR

Now three years into the role at IAC, Koplik is focused on governance, strategic direction setting and coalition building. While each business has autonomy to make their own security decision, Koplik makes recommendations, oversees risk assessments and leverages the scale of IAC's portfolio to negotiate better deals on security products that all the portfolio companies can leverage.

According to Koplik, "In three years my role has evolved from program-building to enabling broader business objectives with security controls. Now business leaders are proactive in coming to me to discuss security as it relates to various strategic initiatives at the corporate level. For example, as we look to opportunities in Europe, our executives want to make sure that they understand regional regulations and data privacy."

Koplik has two pieces of advice for CISOs that are working to establish security as a strategic business driver. He says, "First, do not overthink things. Until you get security operations figured out, there is no point in worrying about sophisticated measurement and key performance indicators. Stay focused on the things that really matter - the security hygiene of the business. A CISO has greater authority and more time to be strategic once their program is running well operationally."

He continues, "Second, do not be afraid to tell the truth. At IAC, the executives are very eager for reality. They want to know what needs to be improved. CISOs should not be scared to be loud about the important things that need to be addressed. You never want to disparage people, but you want to be honest. Of course, it is much easier to deliver this message from a position of credibility, and that is why it is so important to focus on getting the basics in place first."

STAYING FOCUSED ON SECURITY GOALS

Moving forward, Koplik and his team are focused on meeting two main security goals:

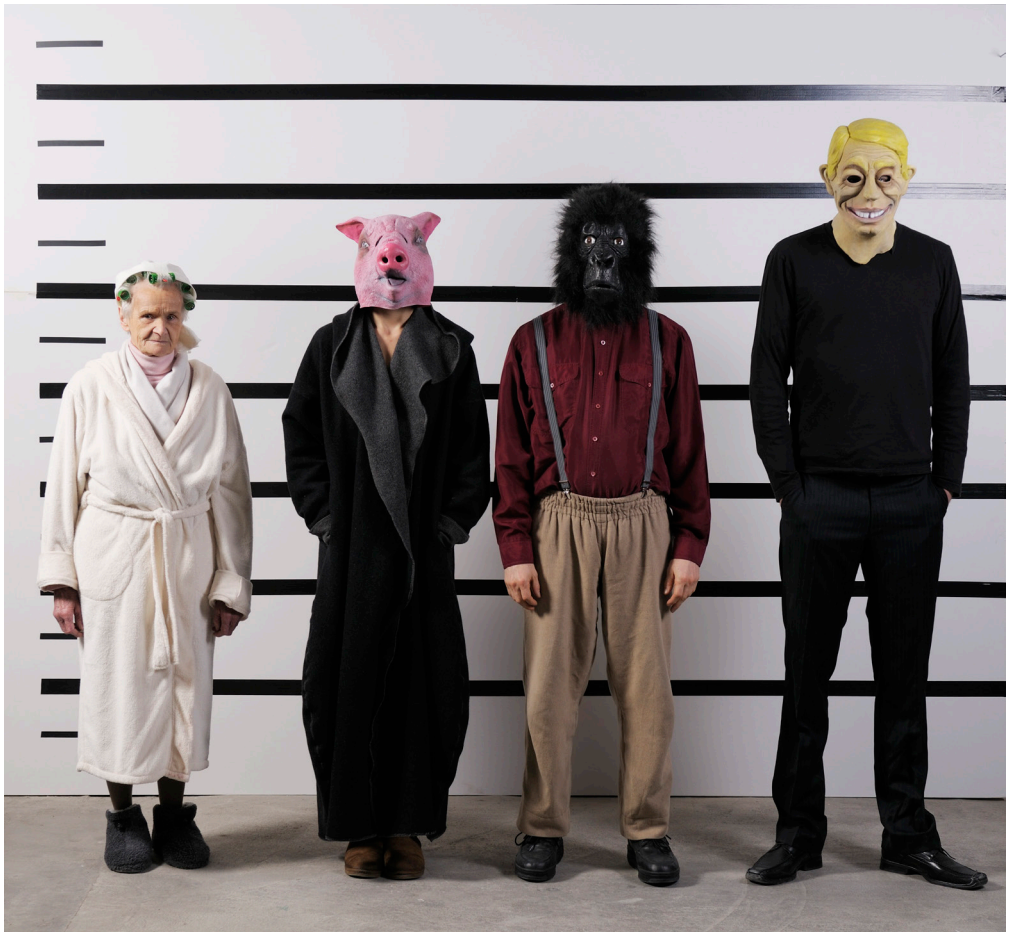
1. Improve Incident Response
He says, "We want to be much faster at detection. We want to be able to assess, contain and eliminate threats right when we find them."

2. Mature the Security Practices at Portfolio Companies
"My team is also focused on maturing the security practices at IAC businesses, including increasing staffing, and operationalizing security responsibilities such as vulnerability management within the businesses."

Koplik is putting programs in place to help IAC achieve these goals. "We are making a huge investment in security incident management right now," he says. "We are building and staffing a security operations center (SOC) at IAC to handle centralized incident response for all of the portfolio companies. This is a vote of confidence from our leadership and from our businesses that they trust Corporate to perform this function for them."

What Drives Investments in Identity and Access Management?

We discuss the factors contributing to the market demand for IAM



There are several unique factors driving demand for IAM technologies at enterprise organizations today. Notably, the problem IAM addresses is unique. Unlike other technology implementations, IAM should be considered a process, not a project. A project has a specific end date, but a process is fluid and always changing.

Most CISOs will agree there are few things more fluid in an organization than user access and employee status. At the most basic level, this explains why organizations such as SANS, Gartner and PWC continue to report IAM as a top corporate priority. However, there are other factors contributing to the market demand for IAM.

By Stephanie Hadley
Marketing Content Manager

PACE OF CHANGE AND INNOVATION IN BUSINESS

Nearly every business trend today directly complicates a company's identity and access management program. Many organizations struggle to keep up with changing trends that directly impact not only the information security program, but the business as well. The process of managing identities is made more cumbersome by:

- Digital Transformation and Cloud Computing
- Shadow IT
- Mobility
- Bring Your Own Device
- Internet of Things

TECHNOLOGY ADVANCEMENTS IN THE MARKET

Many CISOs agree that early IAM solutions such as single sign-on and password managers are incapable of meeting the requirements of today's enterprise. New solutions leverage artificial intelligence, biometrics and machine learning to more smartly manage identities and assign access.

It is important that security leadership fully understand the implications of each solution and the technical and business impact on their own programs. Not only do they need to understand this, but they must balance how IAM solutions impact other technologies and parts of their infrastructure.

As technology advances, CISOs are making decisions on the appropriate IAM solutions to end of life, and where to make new investments.

EXECUTIVE-LEVEL REQUIREMENTS FOR IAM

As Michael Dent, the CISO of Fairfax County, Virginia explains, "Sometimes identity and access management presents an organizational dilemma. Who owns it? Security or IT? Sometimes it seems like if it breaks I own it, and when it does its job, IT owns it. In the end, though, our leadership is clear that identity is a security issue. Users gain access to data on a need to know basis."

In reality, the Chief Information Officer, Chief Compliance Officer and Vice President of Human Resources all have a stake in investing in strong IAM tools. While too many cooks in the kitchen can sometimes make IAM difficult to manage, CISOs that take a collaborative approach with their business partners are often rewarded with executive-level sponsorship for IAM investments.

To become a collaborative partner to other parts of the business when it comes to IAM decisions, CISOs must understand the needs of each business unit. Gaining a full grasp of their concerns and objectives ensures a cohesive approach. In the end, this results in clear priorities laid out from the beginning of decision-making, and a proactive and productive outcome.

For example, the Vice President of Human Resources can often lay claim to managing employee access to systems. It is often left to them to notify IS to turn off access to the network. However, IAM solutions automate previously manual notification processes that historically have been to blame for system breaches by disgruntled employees.

BOARD-LEVEL CONCERN

Access management is also a top consideration at the Board-level for many companies.

Tony Meholic, CISO of The Bancorp Bank explains, "The one issue that gets the most attention from the Board of Directors is user access. Incidents like Heartbleed made the Board extremely interested in understanding our preparations around access management controls and limiting our exposure."

As CISOs align their security programs with the businesses' strategic priorities identity and access management takes on a heightened role in security programs.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

TONY MEHOLIC
CISO, THE BANCORP BANK

HEADQUARTERS: Wilmington, DE

EMPLOYEES: 500+ Employees

TOTAL ASSETS: $4.3 Billion

"I always try to highlight the contributions of team members, as it is their work that makes the bank secure."

- TONY MEHOLIC

CISO WHO SPECIALIZES IN BUILDING PROGRAMS

Like many CISOs, Tony Meholic, the CISO of The Bancorp Bank, moved to the information security industry from another career entirely. Backgrounds in military service, the intelligence industry and IT are common among CISOs, but Meholic might be one of the few CISOs to get his start in the hospital emergency room. Meholic shares, "I was studying for the advanced cardiac life support test and found flow charts for treatment modalities in the back of my prep book. I had always dabbled with programming, so I realized this too could be charted out in a program. To help in my study prep, I wrote a model that simulated cardiac arrest. When the emergency room residents saw it, they wanted to use it, too." Meholic aced the cardiac exam and, at the same time, found a new career path.

"In 2000, I joined First USA Bank as an application developer in their application security group. My job was application security and helping with secure coding, code reviews and training, so that I-banking, which was new at the time, was done securely," he explains.

Meholic steadily advanced at First USA Bank, taking on a managerial role leading application security for the entire organization, not just the information security team. When the bank was acquired by JPMorgan Chase, Meholic created the first team of ethical hackers. Meholic explains, "It was a hard sell to hire hackers at the time. It was considered an unorthodox approach, but I was able to bring in talented people who quickly proved their worth. We saved $360,000 that we would have spent on external

penetration testers, because we had our own hackers on the team."

From JP Morgan, Meholic made a jump that he says, "is not typical, and not always advised." He left the international banking giant, where budget was not an issue, for a regional bank. While the regional bank did not have a global reputation, it represented a step up in responsibility and title for Meholic. He says, "It was my first CISO role and an opportunity to create a security program from the ground up. It was also a chance to work more closely with C-level executives and get exposure with the Board of Directors."

TAKING THE CISO REINS AT THE BANCORP BANK

After establishing the security program at the regional bank, Meholic joined The Bancorp Bank. He recalls, "I was attracted to the CISO role here because it provided an opportunity to build the security program from scratch again, but this time with an international component."

At The Bancorp, Meholic inherited a team of one. He says, "Now we have 8 people and a well-established security program. I am proud that we have recently mapped our program to the NIST framework. This is important because we are now able to show our full security program in an audit-friendly manner."

As he considers his career trajectory, Meholic realizes he is especially adept at building out new programs. He shares, "I helped develop the application security program at First USA, established the technical consulting and ethical hacking teams for JP Morgan Chase, and then the complete security program for The Bancorp."

KEYS TO CREATING A COMPREHENSIVE SECURITY PROGRAM

Given his expertise in building out security programs, Meholic has specific advice for CISOs who are new to the role. He suggests starting with these three steps:

1. Understand Staffing Levels - "We have to look at the support system in place, whether that support comes from within the organization, or IT or business units, we need a team of people supporting security efforts."

2. Identify and Review Existing Policies - "It is important to understand current policies as they are written and applied. Do they meet requirements for privacy, security and compliance?"

3. Know the Data - "Data classification is key. We cannot expect security awareness from the staff if we have not classified the data. We need to identify confidential data, understand where it resides and build protection around it."

Once the basics of his security program are established, Meholic follows a few guiding principles to take his security program to an appropriate level.

- "Let the professionals do their job." - Like other CISOs, Meholic keeps his team motivated through education, training, mentorship and advancement. Importantly, he says, "I am a hands-off manager. I clearly communicate corporate and team goals. Our tasks are well-defined. I know my team has the skills to get the job done, so I give them the freedom to work in the manner that's best for them."

- "Choose the right technologies." - The market is flooded with new security technologies, and it can be hard to find the best solutions. He says, "I rely on my peers. Nothing beats an unsolicited review from a trusted colleague. I also rely on Gartner, although Proof of Concept is still the best way to determine if a solution will do the job for our company."

- "More tools do not equal better security." - Meholic reports The Bancorp runs 8-10 security tools. "It's not the number of tools that will make you secure, it's the way they are deployed in practice," Meholic explains. He prioritizes security solutions that can report on their own performance and measure return on investment.

Meholic works closely with other C-level executives at The Bancorp, and he meets with the Board of Directors on a regular basis. "Sometimes the Board wants a five-minute, high-level overview, and other times they have one hour's worth of questions. Usually interest is driven by bank initiatives or external news."

No matter the focus of the Board's inquiries, Meholic is careful to position security as a team effort. He comments, "I always try to highlight the contributions of team members, as it is their work that makes the bank secure."

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

MICHAEL DENT

CISO, FAIRFAX COUNTY, VIRGINIA GOVERNMENT

LOCATION: Fairfax County, VA

EMPLOYEES: 12,000

ANNUAL REVENUE: $3.8 Billion

VETERAN CISO CREATES PROGRAM TRANSFORMATION

Michael Dent has held the CISO position at Fairfax County, Virginia for fifteen years, making him a veteran and far outpacing the average tenure of most CISOs. He offers a historical perspective on the position, a long track record of success and an established reputation among the County employees.

Dent describes his start at Fairfax County, "In 2002 many places were not concerned about security incidents. The fact that Fairfax County leadership was hiring a CISO put them ahead of the curve. However, there were a lot of questions that did not yet have answers. At the time, the County did not have a documented IT Security Policy, and had no clear separation between IT and information security. Again, this was typical of County governments across the United States."

Through Dent's tenure, security awareness became one of his biggest priorities. Dent initiated the County's annual security awareness day for employees. During this day, employees learn and develop cyber security tactics applicable to their personal and professional lives. The speakers and break-out sessions cover topics such as protecting children online, using IoT safely, and best practices for secure banking. "Employees love the day. We provide them very useful information in a high energy environment, and we make it fun," says Dent. "While this is a service to help them in their personal lives, it improves the County's overall security posture. As a result of these sessions our incidents have decreased, employees are more knowledgeable about security, and they are more willing to work with me and my team to create secure processes."

The security awareness training helped Dent integrate himself with the staff of the County agencies, as they adjusted to working with a Security Officer for the first time. Dent says, "At first, the agencies did not understand why security was needed, or why we needed to document our processes. Some worried that my goal was to prevent or delay their IT initiatives as most implementations would be delayed when my office was included initially." Today, after years of training, security understanding in the County is much higher and the working relationship between Dent's team and County employees is strong.

Dent and his staff worked hard to rid themselves of the reputation as the "no" people. Dent comments, "Now,

The Next Generation of Security Experts

I had the honor and privilege of speaking with 30 High School students two weeks ago at a summer outreach program. I spoke about a variety of career pathways in cybersecurity and answered many questions around what happens in a cyber security organization and what a CISO is expected to know and do. This program is a partnership between Fairfax County Public Schools and Systemic Solutions (NOVA's college-wide STEM education outreach program).

employees know security has to be the first call at the beginning of the project. They realize this makes it easier for us to get it right from the beginning and build out a technology or process that works for them, and is secure."

DILIGENCE IS REQUIRED TO MAINTAIN A LEADERSHIP POSITION

Fairfax County has a reputation as one of the best counties in the United States, both in terms of size and government services, especially information technology and cyber security. Employees work hard to provide services to citizens quickly and efficiently. Dent's role is to make sure these services are delivered securely, with protections in place for citizen and employee data.

The County is comprised of more than 50 agencies, and the majority have multiple types of businesses within the agencies, including public safety, parks and recreation, and libraries, among others. "We are a centralized IT security team, so security for each agency falls under me and my team," says Dent.

"The simple fact is we are not going to maintain our image as the top county in the country if our data gets compromised. Our leadership has led the way through investments in the Cyber Security Program and has ensured that cyber security stays at the top of their lists of concerns. We can never say 'don't worry about it' to the board. In my option, all of the recent (within the last 10 years) major breaches we have heard about in the news were caused by negligence amongst leadership up and down the latter." Dent points out, "We need to be diligent and remain so to be successful."

Dent's two main goals are to protect data and privacy, and to educate employees and keep leadership informed to increase security awareness. "Our sole mission is to allow business to be conducted in a secure manner. I tell my team to never say 'no.' Instead we focus on giving employees and agencies multiple secure options to accomplish their goals. Therefore, we need to be involved from the beginning with internal IT folks and agency teams."

Fairfax County's environment is large and distributed across agencies, and Dent is realistic about what his team may uncover in advance. To keep threats at bay, they conduct yearly and quarterly vulnerability and risk assessments. He says, "I used to think I knew everything on the network. Now I realize that's not feasible. The assessment identifies the risks and unknowns that occur between assessments, then I have to take action to bring it into compliance."

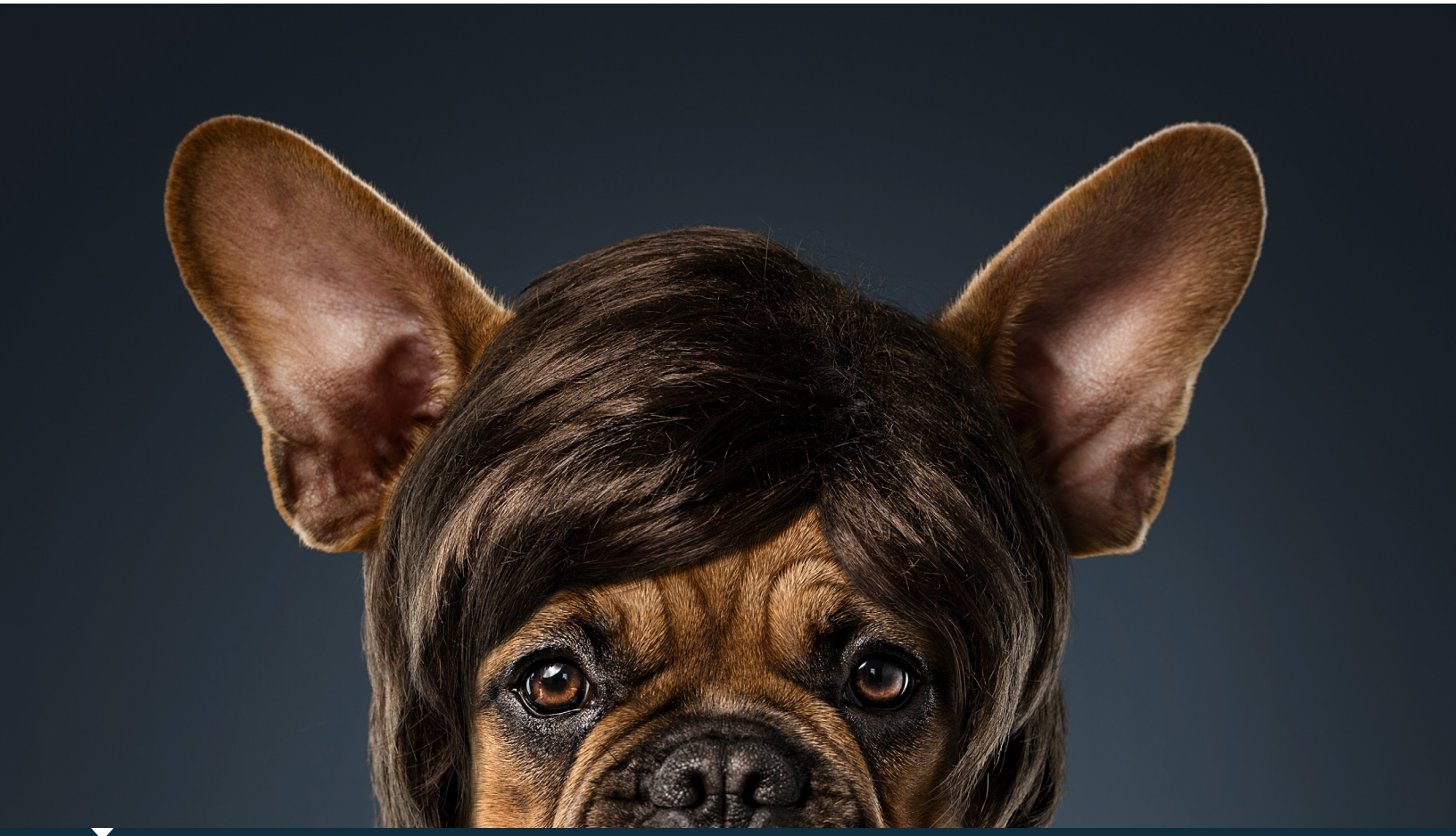
Dent works closely with the Senior IT Steering Committee, comprised of the County executive and his deputies, and includes the Director/CTO and Senior IT leadership, to identify and report on critical cyber security programs. Dent shares, "At those meetings we talk about current programs, and I do a status review of the security program. We review multiple facets of cyber and cyber risk along with any mitigation strategies we may need to take to ensure we have no compromises."

As most in the IT Industry, the County deals with the challenges of legacy systems that remain critical to agency operations but are difficult to secure. "We need to work to get those agencies solutions updated and/or upgraded with minimal down time that would affect services to our citizens. It is a delicate balance to make sure those systems can serve their purpose yet not be compromised. These legacy systems require additional measures to mitigate and create exceptions to IT Security Policy eventually becoming burdensome to IT and Security staff.."

Dent suggests these legacy systems are an example of how leadership in County agencies and IT should partner with the security team to improve the County's overall security posture. "Today, business decisions need to be made that factor in both security and efficiency," says Dent.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446



IDENTITY & ACCESS

SEPTEMBER 2017

K logix

WWW.KLOGIXSECURITY.COM
888.731.2314