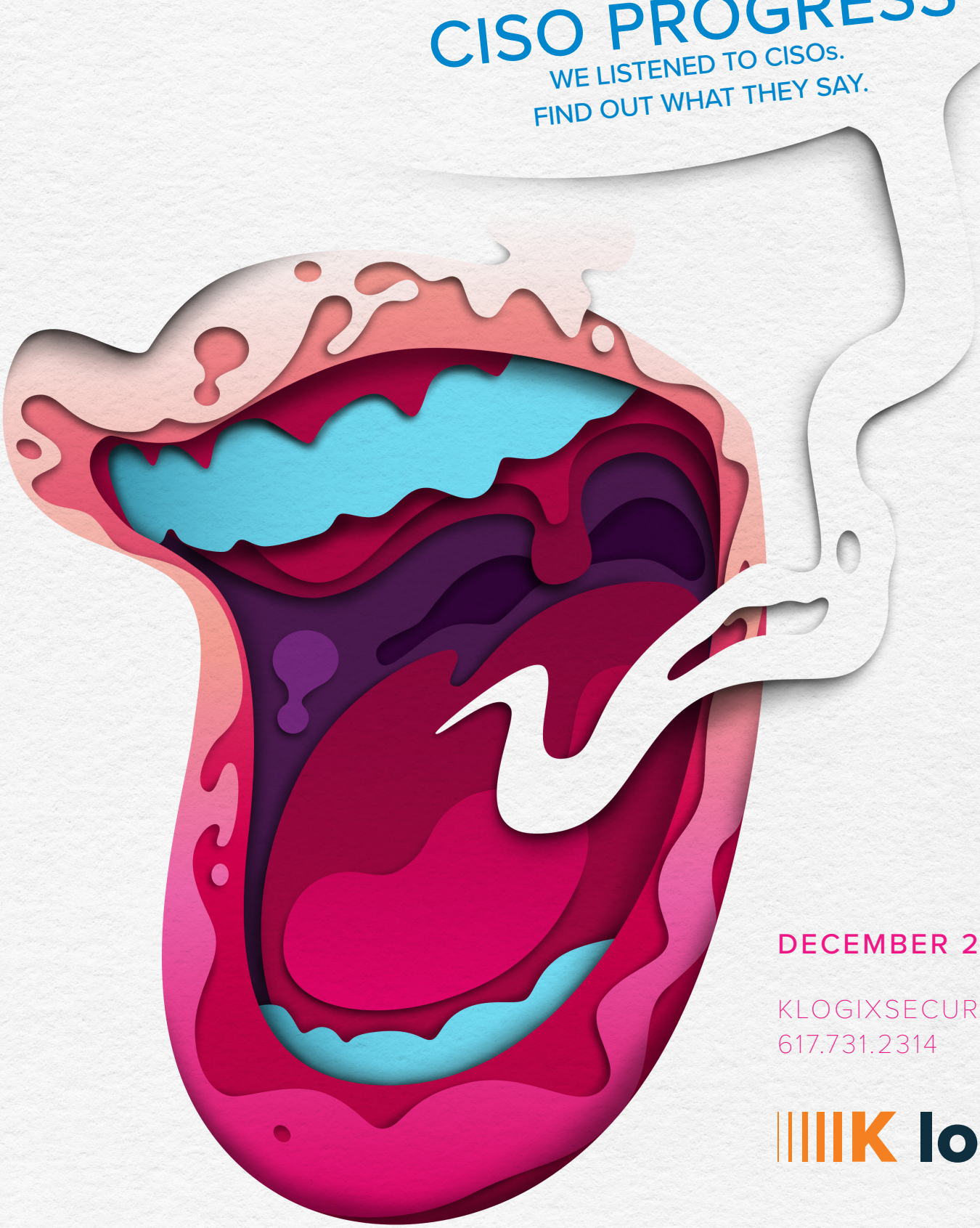
FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE

CISO PROGRESS

WE LISTENED TO CISOs.
FIND OUT WHAT THEY SAY.



DECEMBER 2018

KLOGIXSECURITY.COM
617.731.2314

KLOGIX

FEATS OF STRENGTH

CISO PROGRESS

WE LISTENED TO CISOs.
FIND OUT WHAT THEY SAY.

TABLE OF CONTENTS

To view past issues, visit:
www.klogixsecurity.com/feats-of-strength

Magazine Created By:

Magazine Contributors Include:

Kevin West
CEO, K logix

Katie Haug
Director of Marketing, K logix

Kevin Pouche
COO, K logix

Marcela Lima
Marketing Coordinator, K logix

Contact Us:
marketing@klogixsecurity.com
617.731.2314

We provide information security strategic offerings, threat and incident capabilities, education/awareness, and technology services. We craft our services to address specific customer and industry challenges. One of the ways we do this is through our thought leadership, business-focused publication Feats of Strength. Through 100+ CISO interviews, we extract trends in order to provide services that align business to information security.

LETTER FROM

KEVIN WEST

CEO

THINGS ARE LOOKING UP FOR CISOS

In this issue of Feats of Strength, we check-in with CISOs we previously featured in September 2015's issue, we profile leading CISOs, and we discuss the ever-evolving role of security leadership. The goal of checking in with CISOs we profiled three years ago is to gauge their progress, understand how their goals and challenges have grown, and compare all of this to current CISO trends. This enables us to gain a deeper, more thorough understanding of our CISO community. I want to share what we've learned and what you will read in this issue.

Based on what we are hearing from the CISOs profiled and industry trends, we found CISOs are switching roles more often than ever before. Compensation and executive support are two of the most important considerations when making the decision to change roles. It is important to recognize why executive alignment and empowerment are keys to success for a security program. CISOs want to make a powerful impact in a way that brings security and the business together in a unifying manner. Not only does this alignment enable decisions faster and more streamlined, but CISOs are able to accomplish their goals with less roadblocks. This means accomplishing objectives without having to spend a painstaking amount of time educating executives to justify their decisions.

In our research, 65% of enterprise organizations have CISO roles, up from 50% in 2016, an incredibly positive advancement in our industry. This increase is mainly due to more organizations recognizing the business value of having a CISO in their organization. Today, many boardroom members are calling for strong CISOs to help their organizations, a stark contrast to the lack of

understanding as recent as a few years ago. They want CISOs to be less of a figurehead and more of a business enabler, resulting in increased budget to hire and retain CISO positions.

Another significant statistic is the increasing cybersecurity program budget. With 9 out of 10 companies planning to increase cybersecurity spending by an average of 13% next year, CISOs are planning to increase their technology spend, add more headcount, and align with industry frameworks. Boards are becoming more involved in cybersecurity budget spending, moving them even closer to understanding the value of security being a true driver of business success.

On page 18, Thom Langford, previously featured in the magazine in 2016, shares his thoughts on the evolving role of the CISO and why security should be considered a competitive advantage. Thom says, "We're not separate from the business. We're a fundamental part of it. And also aligned in the security function towards the ultimate goals of the business." Again, CISOs are paving their ways to ensure security becomes cemented as core business functions.

So, what does this all mean? It means CISOs are tasked with balancing their elevated roles and ensuring they keep organizations safe. Not only are they navigating an increasing number of threats, but they are required to leverage their business skills to gain a stronger foothold in organizations. As a company, K logix is committed to helping CISOs accomplish this. I want to make sure I share more about who we are, since some of our readers may not be as familiar with our organization.

WHY DOES K LOGIX PUBLISH FEATS OF STRENGTH?

K logix founded *Feats of Strength* magazine to provide a platform for CISOs and security leaders to share their story. We wanted to bring together the security community and share the trends we analyze and research, while also educating on information security challenges and objectives.

Our team produces all content, interviews every CISO we profile, and publishes the magazine. We work hard each quarter to provide relevant information that resonates with the top challenges and goals of the information security community.

Not only do we want to provide a platform for CISOs to share their voice and deliver business-focused information security content, but we extract trends that directly impact our methodologies and service offerings.

WHAT DOES K LOGIX DO?

K logix is a business-focused information security consulting organization. Founded in 2001, we have always approached our work with a sole focus on information security.

For the past 17 years, we have worked with organizations to help their security teams align to the priorities of the business. We take a consultative and analytical approach to addressing the top challenges security teams face through our end-to-end capabilities.

We do this through our core focus areas:

We would love to share more about what we do with you, so please do not hesitate to reach out to learn more about us. You can also learn more about us at www.klogixsecurity.com.

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.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

TIM SWOPE

CISO, Catholic Health Services Long Island

HEADQUARTERS: Long Island, New York

EMPLOYEES: 18,400+

ANNUAL REVENUE: $2 billion

"An advantage of my consulting background is that people who are in an organization for a long period of time, might not see the whole picture. My entire career, I've been on the outside, so I see the whole picture a little bit better than others."

- Tim Swope

Currently the CISO of Catholic Health Services of Long Island (CHSLI), Tim Swope's career stands out due to his lengthy experience consulting and partnering with healthcare organizations in a wide range of strategic roles. While many CISOs come up the ladder through promotions in their respective security roles, Swope's consultative background has enabled him to consistently interact with C-levels and department heads. These include working with multiple executives from the finance department, HR, application development, and many others. He says, "An advantage of my consulting background is that people who are in an organization for a long period of time, might not see the whole picture. My entire career, I've been on the outside, so I see the whole picture a little bit better than others."

Beginning his career in business intelligence and data analytics for pharmaceutical companies, Swope recognized how his projects were rapidly evolving to include information security components. This included when he began identifying ways to provision people and put in the right security controls. He then started working as a consultant for New York-based hospitals. Swope says, "Across the board I want to make sure these hospitals all have the same security controls for patient safety and patient privacy information. Not being a doctor, I'm agnostic as to where they go. I don't care where they go, but as a patient that comes into any of the hospitals I interact with, I want to make sure their privacy is the same throughout."

Coming into CHSLI, Swope began working with their newly appointed CIO on key initiatives including ensuring the hospital could pass a DOH audit in six months' time, something that had not been conducted before. He comments, "The biggest challenge was right when I came in, they were under federal requirements. There's this program called DSRIP, where hospitals get paid for giving better service, reducing emergency room visits by certain percentages for Medicaid patients, etc. To do that, they had 402 security controls that had to be verified, tested,

and documented across the organization. And they didn't have them." Swope also addressed specific policy and procedure issues and implemented risk management programs that were not previously in place at CHSLI.

MOVING AWAY FROM SECURITY AS AN AFTERTHOUGHT

Whether it comes to digital transformation or engaging in a new project, Swope believes security should never be considered an afterthought. He strongly relies on empowering executives with information and knowledge that validates the need to include security in all strategic discussions.

As a healthcare leader, Swope understands the strong impact digital transformation has on the industry and he continues to ensure security is baked-in all cloud decisions from the start. One challenge he recognizes is the need to sometimes take vital time during decisions to ensure nothing is implemented unless he can guarantee it can be done securely.

Swope says, "Digital transformation is a big impact. A lot of our services are cloud-based. We also have clients who require a certain type of information that will go into a cloud area so that they can retrieve it easily. Over one third of the security controls from the National Institute for Standards and Technology for federal systems, which covers the Department of Health, are based on cloud security. So that's really changed the landscape a lot."

In organizations where security may be an afterthought to project decisions, Swope emphasizes the importance to mandate security as a core component. In his experience, to guarantee security is part of key considerations, he encourages strong secure development lifecycles and data distribution lifecycles for all vendors and healthcare professionals. He initially implements a security review, so no project gets approval until a thorough security assessment is completed. Once a vendor passes, or after necessary remediation takes place, only then can they get approval to move the project forward.

FOCUS ON RISK MANAGEMENT LEADERSHIP

While many security leaders focus on cybersecurity, Swope focuses his programs on risk management. He explains, "Risk management is the overriding thing for cybersecurity because, let's say you have the cybersecurity tools, right now, they'll tell you what happened. You can do a lot of anomalous behavior analytics and it'll tell you what's happening, but only through risk management do we identify the security risks upfront before anything happens, and then we remediate them before they're a problem. I spent a lot of time with clients and hospitals looking at what could be a risk in the future, like medical device security, things like that. And rather than attacking it with software, we look to remediate a lot of those issues before they even happen."

When coming into a new organization as a CISO leader, Swope strongly believes in conducting an internal assessment to get an understanding of what controls and technologies are in place. While some CISOs may rely on an outside firm to conduct these, Swope chooses to do them himself, putting himself in an outside auditor's shoes. He says, "So rather than looking at somebody else to do it for me, I'll do it myself and I think that's the key thing a CISO should do, is understand his or her landscape and do their own personal assessment and only then can you see what you really have. That's the only way to get a good feel of it, by doing it yourself. That's the biggest hands-on thing a CISO should do in the first couple of months."

Swope strongly believes in starting cybersecurity governance councils within organizations bringing together the board of directors, CIO, head of audit and compliance and any other key executives. He explains, "I bring them all into the conversation and let them know that if they look at security first, it won't hold up these projects, but they actually do have to be a piece of the plan. I let everybody know what our plan is long-term. So, it's not a surprise to them because a lot of people really don't know what information security does and they look at it as a detriment to their progress, not an enhancement."

The Need for Virtual CISOs

Due to the salaries skyrocketing for New York CISOs, Swope believes the option of virtual CISOs may become normalized. He says cost is one of the key benefits, with New York CISOs average salaries around $400,000, something not all hospitals can afford.

He explains, "The advantage of a virtual CISO, is there are a set of federal requirements that govern hospitals, and this is just with security. All of these hospitals have the same requirements. So, the value I bring to one is the same that I bring to the other, and they could share the cost. The reason why the cloud is so cost effective is because you're sharing it with other companies. It's the same sort of thing. They're going to share me with others. It's got to be the same industry, the same size entity. So, it would be, let's say three hospitals the same size as Catholic Health Services. I could officially do those because the type of attacks, vulnerability requirements, they're all the same. Let's say there's a huge incident at one or you need to enact a disaster recovery at one without the others. That's when you rely on the team and you have to build a very good team under you. It's like a coach of 11 players on the field. They're all doing it. I'm telling them how to do it."

CISO **SPOTLIGHT**

We check-in with CISOs we previously featured and profiled in our magazine.

Learn about how their roles have changed, how they've grown as leaders, and their accomplishments.

Read Q&As from:

Michael Newborn, CISO McKinsey Digital Labs

Sue Schade, Principal, StarBridge Advisors

Darren Death, CISO, ASRC Federal

What has been the biggest change since we last spoke in 2015?

I left Bloomberg in 2016, and a little later in the year started at McKinsey in two distinct roles. I'm the CISO for one of the practices here, similar to previous roles I've had where I manage the cyber risk program for the organization, and I'm an associate partner serving global clients, primarily on the topic of cybersecurity. Although I've only been here for two years, it feels like a decade – I've been introduced to a wide range of companies, domestic and foreign, across many industries.

How has your alignment with executives changed?

In the past couple of years here, I've been exposed to a broad range of challenges executives face and the complexity involved in their decision making. It has helped me better understand the business perspective – and enables me to take a more holistic approach across technology, business strategy, and compliance. This includes everything from top-of-mind cyberrisk issues and improving digital resiliency, to social engineering and how you effectively build and operate a cyber risk management program for a company – and how you approach all of this as it changes based on company size.

What industry changes have you experienced over the last few years?

Over the past couple of years, our industry has seen everything from election tampering to the rise of ransomware. We're also seeing an increase in the average person's understanding and awareness that there are real cyber risks out there that don't just impact big companies, they can impact all of us as individuals. I think that's also driven an increased awareness within organizations' senior leadership, a realization that cybersecurity still needs to remain top of mind. It's not going away. This increased awareness has led to a demand that is greater than ever for cybersecurity talent. There's a noticeable gap between demand for jobs and the number of people available for them.

In terms of trends, I've seen an increase in cloud adoption, yet too often, basic security controls aren't effectively being met. It's the same thing with patching. We've had to patch things for years, yet getting to a 90+ percent patch compliance rate seems to be very challenging for most organizations.

We've also seen a big proliferation of Internet of Things (IoT) devices, whether it's home automation, semi-automated cars, baby cameras, etc. I think over the past few years, we've seen a significant number of attacks with IoT devices and I think that trend will continue.

How do industry trends impact your approach to cybersecurity?

We stay on top of the latest trends and help develop industry knowledge. Earlier this year, I co-authored a paper, *Making a secure transition to the public cloud*. We interviewed 100 organizations over a six-month period. The report offers a perspective on how to build an operating model around public cloud adoption to make sure security is part of the process from the beginning. It considers what organizations need to know if they're using IoT devices – including where the devices are, since many organizations have them in wide use. Often times, organizations don't make it a priority or don't have an easy way to classify and identify those assets to ensure they're being protected and segmented properly.

What has been the biggest challenge since we featured you in the magazine in 2015?

I have served as interim CIO in two different organizations in the past few years. One of the first areas a new CIO, whether permanent or interim, looks at is security. The strength of the IT security leadership and maturity of the overall security program. In one organization, we had a very strong CISO and had just opened a SOC – security operations center. In the other organization, we were strong on user education, policies and procedures but needed some work on the technical side of our program. Figuring out your security gaps, gaining executive and financial support to address, and then implementing necessary changes is critical in your first 90 days.

How has your executive alignment changed?

Executives in both of the organizations where I served as interim were supportive of continuing to strengthen the security program. The CIO and CISO must be able to educate, without fear mongering, the executive team on security risks and gain their support for necessary changes that may be unpopular or viewed as too restrictive by end users.

How has the industry changed and what impact has that had on your security program?

My new health IT advisory firm, StarBridge Advisors, provides IT consulting and interim management. As I work with CIOs I am seeing an increased demand for experienced CISOs overall in healthcare. For small organizations with low budgets, security programs have not been invested in to the extent needed. Discussions with those CIOs often include security assessments and either part-time or virtual CISO options. Overall I see an increased awareness by boards and the C-suite as cybersecurity risks increase.

Also, I'm encouraged that more women and men are willing to talk about the challenges facing women in the workplace and the need for more women in STEM fields. I'm currently working on developing coaching services for women at different stages of their career.

What has changed most from a personal perspective since we profiled you?

I made a decision in early 2016 to leave my permanent position at the University of Michigan Health System (now called Michigan Medicine) to live near family in New England where I now have four grandchildren and to become an entrepreneur doing IT consulting, interim management and leadership coaching. I wanted more flexibility in my career at this point.

What has changed most from a professional perspective since we profiled you?

As my first interim CIO engagement ended in the fall of 2016, I formed StarBridge Advisors with two colleagues. We just celebrated our two year anniversary as a firm and are providing a range of health IT advisory services to healthcare organizations, including security assessments and interim CISOs.

What has been the biggest challenge since we featured you in the magazine in 2015?

My biggest challenge has been implementing a full scope Information Security program while implementing major Information Security frameworks. My team and I delivered ASRC Federal's fully compliant rating with NIST SP 800-171 on 09/29/2017. This rating was delivered $2 million dollars under budget and three months ahead of the government mandate. The team and I also brought ASRC Federal into compliance with the Center for Internet Security (CIS) – Consensus Security Controls (CSC) on 07/26/2018 with minimal financial impact to the organization. I am currently bringing ASRC Federal into compliance with ISO27001 and planning to achieve ISO27001 compliance by the second Quarter of 2019.

How has your executive alignment changed?

I still report to the CIO of our organization. We have a great relationship and this certainly benefits the team and the organization. The big difference now is that I brief my company's senior leadership quarterly regarding cyber risks and information security program status.

How has the industry changed and what impact has that had on your security program?

The federal government and private sector customers require a lot more out of their vendors in terms of security offerings and postures. This has been great for the information security programs as it justifies the needed work that every organization should be implementing.

What has changed most from a personal perspective since we profiled you?

I can now stand on my paddle board without falling in, which is fantastic. Everyone in the family has a paddle board and we go out on the water often.

What has changed most from a professional perspective since we profiled you?

I completed my master's degree and I am currently working towards the completion of my Doctoral Degree in Cyber Security.

I wrote a book in 2017: *Information Security Handbook: Develop a threat model and incident response strategy to build a strong information security framework* and in 2018 I've had eight articles published, including Forbes, SecurityCurrent, CIOReview, and CIO Applications.

CHECKING THE FACTS:

WHAT'S CHANGED THE MOST? WHERE ARE WE HEADING?

CISO Progress

BY: KATIE HAUG, MARKETING DIRECTOR

Over the past five years since we started this magazine, we not only feature and profile leading CISOs from all over the United States, but we also collect trends. These trends are then correlated to industry stats to help make an impact on the information security community. We want to share with you some of the most important trends we have collected ourselves, along with specific industry trends that stand out.

We focus on changes for CISOs in terms of responsibilities, approach, and acceptance as a leader.

CISO TURNOVER

Based on our research interviewing over 100 CISOs, one out of every four CISOs change organizations every four years. We have seen the highest amount of CISO turnover in healthcare organizations, with almost 50% moving jobs every four years. Banking and finance CISOs come in second with an average 37% moving jobs every four years.

We wanted to understand why this occurs and discovered key statistics from industry research.

In a recent ISSA survey, they concluded:

- 38% of CISOs change jobs when they are offered higher compensation packages from other organizations.
- 36% of CISOs change jobs when their current employer does not have a corporate culture that emphasizes cybersecurity.
- 34% of CISOs change jobs when the they are not active participants with executive management and the board of directors.
- 31% of CISOs change jobs when cybersecurity budgets are not commensurate with the organization's size or industry.
  (Source: The Life and Times of Cybersecurity Professional, ISSA)

While money clearly matters when it comes to CISO career choices, also evident is that they want to work for supportive executives and organizations. Vital to a CISOs' success is the opportunity to work in an environment that willingly funds a security program as well as one that recognizes the impact security has on an organizations' ability to function and grow. CISOs want to work at organizations where executives are buying-in and participating in the planning and execution of security priorities.

GROWTH OF CISO ROLES

It is reported that 65% of enterprise organizations have filled CISO positions, up from 50% in 2016. Whereas, only 22% of SMB organizations have filled CISO positions. We anticipate this number to continue to grow as more organizations recognize the value of a CISO role in their organizations. *(Source: 2018 IDG Security Priorities Survey)*

65% of enterprise organizations

have filled CISO positions, up from **50% in 2016**

We examine why more and more organizations are hiring CISOs. With the striking increase of cyber threats and cyber crime, a new age of professional cyber criminals has escalated the past few years, resulting in a form of organized crime. These sophisticated and proliferating threats target critical data, posing a threat for any organization without a strong security posture in place. Without a CISO leader, organizations are more at-risk to a negative impact by threats, while also hindering innovation or operational growth.

The role of the CISO is impacted by this, as both a challenge and opportunity. CISOs continue to

evolve into business enablers and strategists, moving away from the technologist reputation and approach. They must articulate the risk to the business, have two-way, meaningful communication with executives, and demonstrate business metrics.

Since **2015** – the rate at which boards are formally updated on **cybersecurity risks**

is up 20%

The importance of this evolution is evidenced by growth in CISO reporting structures and the prescene of CISOs in boardroom discussions. Since 2015, the rate at which boards are formally updated on cybersecurity risks are up 20%. Furthermore, 35% of CISOs today report directly into the CEO of an organization. *(Source: The Global State of Information Security Survey 2018 PwC)*

CYBERSECURITY BUDGET INCREASES

When we first asked CISOs how much their budgets increased each year, we found 85% said their information security budgets increased 10-15% per year.

Nearly 9 in 10 companies plan to increase cybersecurity spending next year, up 10% from the 76% that said the same thing in 2017. Worldwide numbers are slightly smaller, with 78% reporting plans to increase spending on cybersecurity, compared to 73% last year. *(Source: 2018 Global Threat Report 451 Group for Thales)*

9 in 10 companies

plan to **increase** cybersecurity spending next year

In turn, the total worldwide cybersecurity spend predicted for 2019 is $96.3 billion. According to Gartner, the $96.3 billion that organizations will spend on security products and services next

Total worldwide cybersecurity spend **predicted for 2019** is

$96.3 billion

year represents an increase of 8% over 2017 and a more than 17% jump over the $82.2 billion that organizations spent in 2016.

According to research conducted by IBM, the ideal spend on cybersecurity is 9.8 to 13.7% of an IT budget. This percentage per Gartner and other research firms, is estimated to grow along with the increased integration of security into all facets of IT infrastructure.

In fact, cybersecurity spending is expected to grow to $1 trillion between 2017 and 2021. However, there is still a sizable gap between the threat level and reality, with a majority of businesses delaying or downright denying the importance of a cybersecurity budget that exceeds 3% of a company's capital expenditures.

As noted in the numbers above, organizations are spending more than ever on security. Yet 7 in 10 say they want at least 25% more spending, and 17% want up to a 50% increase. However, only 12% believe they will actually receive a security budget increase of over 25%. The rest clearly will just have to make do with whatever increases they get. *(Source: EY Global Information Security Survey 2017-18)*

Even with many things in their favor, some CISOs believe they will need additional budget to keep up and ensure their programs remain strategic.

So, what are CISOs spending their budgets on? According to a recent IDG CSO study, 46% of budgets are spent on purchasing new technology, 34% on conducting audits and assessments, and 32% on adding new skills or capabilities.

In the same study, IDG asked leading CISOs what factors help them determine the priority for security spending? In the results, 73% of CISOs said best practices are the number one factor fueling their spending, with compliance mandates coming in second at 69%. Coming in at 36% was responding to an incident that occurred,

33% mandates from the Board of Directors, 29% responding to a security incident that happened at another organization, and 22% partner mandates. *(Source: 2018 IDG Security Priorities Survey)*

BUDGET SPEND:

- 46% of budgets are spent on purchasing new technology,
- 34% on conducting audits and assessments, and
- 32% on adding new skills or capabilities

Something that has become more prevalent in the past five years is board engagement when it comes to budget discussions. 45% of CISOs said their corporate board participates actively in setting security budgets. *(Source: EY Global Information Security Survey 2017-18)*

45% of CISOs

said their corporate board participates **actively** in setting security budgets

COMBATTING THREATS AND ALIGNING WITH EXECUTIVES

One of the top strategic goals for CISOs is the balance between addressing the ever-evolving threats impacting their organizations along with adjusting to their higher-profile status in the C-suite.

In the past five years, CISOs have become more prevalent in the boardroom and executive meetings. This shift is in part due to CISOs becoming more business-focused paired with the rising publicity received by cybersecurity, making executives more aware of the necessity to have strong cybersecurity programs.

According to data from Deloitte's CISO Labs, building capabilities to better integrate with the business is a consistent priority among CISOs. Over 90% of CISOs hope to improve the strategic alignment between the security organization and the business, yet nearly half (46%) fear the inability to accomplish that alignment.

Featured in this issue is Sue Schade currently the Principal of an advisory firm (originally interviewed as CIO of University of Michigan Health System). She states, "The demand is greater than ever for cybersecurity professionals. There's a lot of opportunity out there and I think there's a noticeable gap versus the jobs and the number of people that are available for those jobs. I think that's also driven an increased awareness within senior leadership in organizations and a realization that this still needs to remain top of mind. It's not going away."

Over 90% of CISOs

hope to **improve the strategic alignment** between the security organization and the business

CISOs are ensuring their programs have strong foundations based on key strategic goals such as aligning with the business and making a positive impact on revenue. Based on our research, cybersecurity plans are focused on running strategic, business-minded program. While many security leaders are engaging more frequently with senior executives, according to Deloitte CISO lab research, 79% of CISOs reported they were "spending time with business leaders who think cyber risk is a technical problem or a compliance exercise." As a result, most CISOs "have to invest a lot of time to get buy-in and support for security initiatives."

TOP CHALLENGES

IDG asked CISOs - What security-related challenges are most often forcing you to redirect your time and focus away from more strategic tasks?

Based on IDG's results, compliance and external threats continue to 'eat away' at strategic efforts. In many organizations, notably healthcare and finance, regulations and compliance reign over most cybersecurity decisions as roadblocks to focusing on key strategic initiatives.

(source: 2018 IDG Security Priorities Study)

Lack of talent poses another challenge for CISOs and according to recent estimates, there will be as many as 3.5 million unfilled positions in the industry by 2021. Furthermore, according to The 2017 Global Information Security Workforce (GISW) Study, two-thirds of its nearly 20,000 respondents indicated that their organizations lack the number of cybersecurity professionals needed for today's threat climate.

Organizations must broaden the pool of candidates and the skills they require. When looking beyond certifications or degrees, hiring managers should focus on core soft skills such as business aptitude and eagerness to learn.

3.5 million predicted

unfilled positions

in the industry by **2021**

We have produced previous magazine issues on the lack of talent and lack of women in security. The lack of women, veterans, and minorities is a tremendous issue facing the industry, and although we could address this topic with extensive information, we will focus mainly on the stat of women representing only 14% of the cybersecurity workforce. Organizations must empower more women to join their teams, and create work environments conducive to all employees, both men and women.

CONCLUSION

In conclusion, we are at a pivotal time in information security. The past five years have given way to cybersecurity becoming an executive and boardroom focused topic, enabling CISOs to engage more with these leaders. With threats becoming more sophisticated, CISOs will continue to focus on keeping up while at the same time addressing their strategic priorities. Due to increased salary offerings or lack of cultures that do not support cybersecurity, CISOs are starting to move positions more frequently than ever before. The lack of talent in the industry is still prevalent and becoming more impactful on security programs growth.

CISOs are in a unique position – they are respected, yet must possess the skills to properly educate business leaders on how to strategically improve their security programs. They are getting creative to address the lack of talent by searching outside of specific IT security experience and focusing on business acumen skills for candidates they can then train. Their budgets are significantly increasing, allowing them to not only focus on combatting threats, but to also engage in security awareness and other strategic priorities within their programs.

Looking forward to the next five years, we believe organizations of all sizes will hire, retain, and support their CISO leaders in a way never done before. Not only because of rising threats, but because they believe in security as a business enabler.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

DAVID LOEWY

CISO, SUNY DOWNSTATE MEDICAL CENTER

HEADQUARTERS: Brooklyn, NY

EMPLOYEES: 8000+

NET POSITION: $2.9 BILLION

In the early 2000s, David Loewy began working on HIPAA projects, his start in getting involved with information security. He says, "Back then, the government put out in the congressional record, this is what you have to do to comply with the laws of HIPAA. And it used to be very much that you had to click off policies and you had to show how the policies were implemented and that you were compliant. Since the early or late nineties, HIPAA has evolved into a risk-based compliance program, if you will. And the natural evolution of HIPAA and the security piece of the risk-based part of assessments is how I evolved into security."

In 2015, after working as a HIPAA risk assessment consultant for State University of New York, Downstate Medical Center, they decided to hire him as their full-time CISO. SUNY Downstate Medical Center includes multiple graduate colleges in healthcare, a hospital and a large-scale research facility. Loewy was tasked with stabilizing and developing the information security program, starting with conducting outside assessments, remediating holes, then addressing policies and procedures.

One key challenge early on was ensuring all initiatives were applied to all units under the university's umbrella. Loewy explains, "We have the university and the teaching component, we have the medical and the hospital component, and we have the research component with the administration sitting over the top. And we must make all of our policies work for each one of those segments. Procedures are different. To enforce a policy may be a very different procedure for the hospital than it is for the medical school, but the policy must be able to meld across the entire institution. And that's what we started working on."

STRENGTHENING COMMUNICATION AND RELATIONSHIPS

Loewy believes his long-standing success at SUNY Downstate Medical Center is attributed in part to his relationships with C-level executives and his team. When discussing the importance of strong communication and relationships with his team, Loewy states, "When I hire people, one of the things I tell them their job is, is to make me look like a hero. And my job is to give them the tools and the support they need to do that. If you can pull that together, everything suddenly becomes copacetic. And I'm not going to tell you it's easy, because it keeps me awake at night. But you must rely on them. You have to build that relationship. And that makes my job a hundred percent easier when I'm not worried at night, whether a specific individual is going to do what needs to be done."

Armed with a strong sales background, Loewy believes sales skills significantly impact who he is as a leader and communicator. He says being a sales person means being quiet and listening, because that's when you learn vital information from someone. He also strongly encourages making time to care about your team and business counterparts.

THE IMPORTANCE OF SECURITY AWARENESS

"There's a lot of really good technology that is available in the marketplace, but 70 percent has nothing to do with gizmos, it has to do with people being aware of what the bad guys look like and how they're trying to break into our environments. 90 percent of cybersecurity tools are promulgated through email," says Loewy. As an industry, Loewy explains how most organizations are finding email as the number one tool people use in their organization. And through email, adversaries are getting into networks by clicking links or providing information like passwords.

He continues, "In the United States, I believe 30 percent of the people who get emails, will click on an email not knowing where it's coming from. Some 20 percent will click on links they don't have a clue where they're coming from. 8 to 10 percent of the people in this country will give out personal information, passwords, or login credentials, without having a clue where it is going. We have been able to drive Downstate down to less than 1 percent of our people will give that out. And that's a risk we're willing to assume, and less than 3 percent of the folks will click on links."

Loewy's resilience with security awareness campaigns means his network remains safe from most ransomware and viruses. For his role as CISO, it is his job and his team's job to make sure the organization is safe from adversaries getting in, because people's lives depend on their network not being penetrated.

ADDRESSING GOALS AND CHALLENGES

As a state-run organization, Loewy's goals are to remain transparent and keep the organization out of the press, maintain financial viability, and ensure they leverage the latest technology to achieve these goals.

One of Loewy's top challenges is secure communication between 'bring your own device' due to many of their medical residents moving between up to six or seven different hospitals. Loewy explains, "The face of healthcare in New York is changing probably faster than some of us want to think. We need to hammer that down. We need to figure that out."

Loewy believes healthcare is five years behind banking when it comes to securing innovation. He notes the ability to deposit checks through cellphones as an advancement in respect to how security can leverage new technology. He would like to see healthcare mirror these types of technological capabilities, and says, "Five years ago, they would have told me I was crazy if I suggested that's where we were going in banking. And in healthcare, we need to be able to ramp up the way the banking industry has and utilize all the marvelous tools we have and that are coming out of research and keep them secure."

He continues, "And that is a problem with the Internet of Things and with all the new medical devices. When somebody's had an epileptic seizure, they previously would shave spots on the head and put on probes so they could get readings on what the brain was doing. It took a long time to do that and sometimes the seizure would end before that was done. They've now developed a watch cap you just pull over your head and they can instantaneously start reading what the brain's doing. This all goes out over an internet and it's captured on a computer."

However, Loewy believes there is still a large risk with some advancements in technology, from a security perspective. He explains, "The benefits are greater than the risk usually, but there's a large risk in that side of healthcare and there's a large risk with the Internet of things. One year ago, we were moving out of one of our main offices, and some folks put copy machines out in the hallways and didn't realize that every copy ever made was captured on a hard drive. It was sitting right out there in the hallway and it's those kinds of things that we just are not cognizant of. And that's going to be the next big black hole that we're going to have to struggle with and get our arms around."

HOW TO MAKE CYBERSECURITY A COMPETITIVE ADVANTAGE

Q&A WITH THOM LANGFORD, CISO, PUBLICIS GROUPE

Over the last five years, the concept of security being a competitive advantage within organizations has become more prevalent and increasingly discussed. We recently spoke with Thom Langford, CISO of Publicis Groupe about what it means for information security to be a competitive advantage.

ABOUT THOM LANGFORD

As Chief Information Security Officer of Publicis Groupe, Thom is responsible for all aspects of information security risk and compliance as well as managing the Groupe Information Security Program. Additionally, the role is responsible for business continuity capabilities across the Groupe's global operations. Having successfully built security and IT programs from the ground up, Thom brings an often opinionated and forward-thinking view of security risk, both in assessments and management, but is able to do so with humor and pragmatism (mostly). An international public speaker and award-winning security blogger, Thom contributes to a number of industry blogs and publications. Thom is also the sole founder of Host Unknown, a loose collective of three infosec luminaries combined to make security education and infotainment films. Thom can be found online at both thomlangford.com and @thomlangford on Twitter.

What's the starting point for security professionals in creating a competitive advantage?

Thom: For me, it's a mindset. I think it's starting to view information security as not the business prevention unit or the unit that says 'no' to everything. I think in the past, as security professionals, we've all been guilty of just wishing to say 'no' to everything because we are held accountable for things that we're not responsible for, we're just simply told to reduce risks and make things secure and actually not playing a part within the business. I think that mindset needs to shift to more of a new school approach, to where we are a part of the business. We're not separate from the business. We're a fundamental part of it. And also aligned in the security function towards the ultimate goals of the business. So, for instance, knowing precisely what your business does, what product it sells, what the shareholders are after, what the long-term strategic goals of the company are, etc. Once you know what those are, you can start to align your business to those goals.

I think the shift to trust and competitive advantage requires a shift away from the old school thinking of security. Security used to be the department of 'no', the business prevention unit. We were being held accountable for things that we weren't responsible for. And so, we would simply try to reduce risk as far as possible by saying 'no' to everything or being the big hoop that everybody has to jump through; security for security's sake. I think as we shift to a new way of thinking, which is - we are a part of the business, we're here to support the business. And actually, my role as a CISO is not to make the company the most secure company in the world, but it's to help the business sell more stuff, do more things, then that's going to make life much easier.

Is that part of a strategy of educating executives?

Thom: Actions speak louder than words. I think it's around creating security programs that put business challenges and business outcomes first. I think if executives are reluctant to hear that, to hear your message, look at why that is, what's happened in the past? What are the activities that you're carrying out today that might be making them feel wary of engaging with you? Again, it comes down to trust and trusting your intentions as a security leader. What are you here for? Are you here to help the business meet its goals or are you just here to implement security blindly? And I think it's that kind of education and those kinds of conversations that are absolutely vital, and it will take time. It could take a year or two years to actually turn an organization around based on the reputation of either your predecessors or even just the general viewpoint of information security as a function.

Talk to us a little bit about your executives, do they align with this?

Thom: Yes I think so. I think with cybersecurity and physical security becoming far more in the public eye, that first and foremost they see the threats and vulnerabilities, as any sane person would. But I think also they are being communicated to in a way that's beneficial for security and the competitive advantages it can bring. Things like security testing so that code is supplied in a safe stable manner. For instance, with fewer testing cycles required, it is a competitive advantage over some because of the speed of delivery and the ability to deliver more cycles of work in a defined period of time.

WE PREVIOUSLY PROFILED THOM IN SEPTEMBER 2016. WE CHECKED IN WITH HIM FOR THIS ISSUE TO HEAR HIS THOUGHTS ON SECURITY AS A COMPETITIVE ADVANTAGE.

I think there can be a variety of different activities that will bring competitive advantage. I mean even ones down to simple personal safety. Do you buy a car from a company that demonstrates it has no interest in fixing vulnerabilities in those remote driving capabilities or do you buy a car that actually has proven to be resilient to remote attacks to your car while you're driving?

What part does customer trust play into a competitive advantage?

Thom: Trust is fundamental. For example, people don't use or will be very reluctant to use, any kind of new technology or new service they don't trust. You know, I think there are many examples when people would do the complete opposite. I think Facebook is an example of that in the way that data has been used. But I also think they try to make strides towards actually regaining that trust so they can take on more customers and take on more business. But fundamental to it all is trust, because if you don't know how your data is being used, if you don't know how that technology is being rolled out amongst your house, for instance, in the case of things like Siri or Alexa or Google Home, then you're going to be far more reluctant to buy the product or even invest further.

Should security be marketed as a competitive advantage?

Thom: I don't see why not. Front and center, maybe not. I think it depends on the product that's being sold. Certainly anything that involves the delivery of codes or delivery of technology or anything like that is a fundamental part of the business. So sure, I think it should be part of it in the same way that agile methods and use of certain coding languages and the use of certain project management processes are marketed in materials. Then absolutely, I think it should be very clearly front and center as a part of that offering.

Does that mean that CISOs should be more customer facing?

Thom: Absolutely. And I think the traditional location of a CISO is to look at the internal functions of an organization and make it secure. I'm seeing, and I know others are as well, the more you engage with your client project managers and your account managers, the more trust there is. Given the statistics that it's not a case of if but when an incident happens or a breach happens, if you're responding to those situations in a very positive and transparent and open manner, there's no reason why your responses to those situations can't actually create more trust with your clients. That's something I've seen in a number of occasions.

Does competitive advantage introduce a vehicle to show us security ROI?

Thom: I look at ROI from two different directions. One is the traditional return on investment which we have to do anyway as contributors to the business, we have to show that what we are asking for in monetary terms is going to be invested wisely and is going to produce some kind of return. It might not necessarily be financial. It may just be opportunistic or quite literally the avoidance of greater costs, something we are all aware of. I think the other aspect to ROI is the risk of incarceration, and to be honest, with the amount of standards and regulations and laws that are coming out, I think this is an important one. Companies are compliant moving forwards and they are working in the best interests of their customers and the public at large.

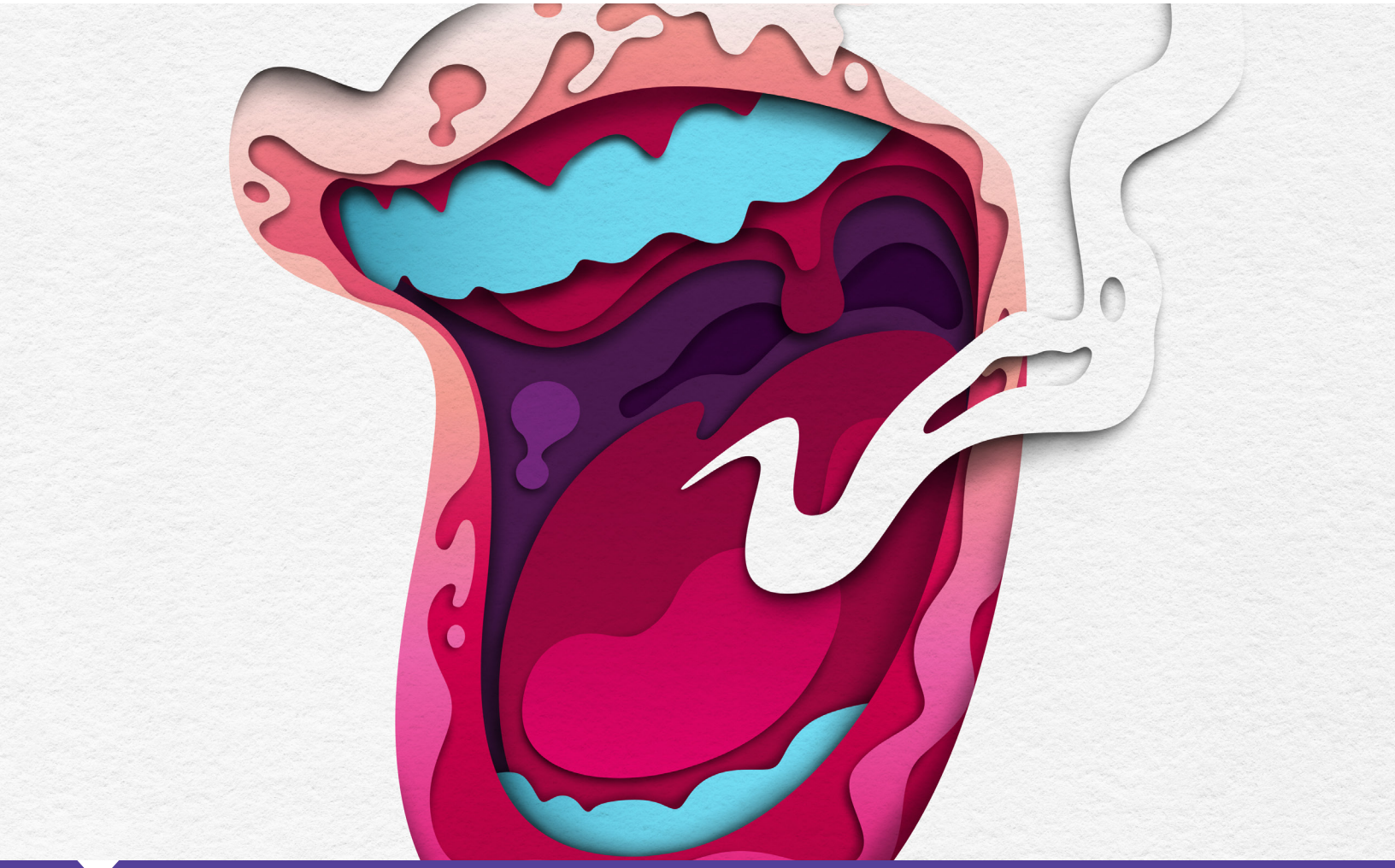
Where do you see the future of security as a competitive advantage in 5 to 10 years?

Thom: I think there's a twofold answer to that. The first one is I hope to see more of the same, in the sense of the good things that we do now, the positions in leadership that we're seeing, the CISO is increasingly less reporting to the CIO and more reporting to the CEO or the board directly. I think as long as you continue along that arch, we're going to see far greater opportunity for the business to capitalize on information security as a competitive advantage in the same way it does with finance, legal, etc. Getting the right people with the right attitude, etc. So I think the evolution of the CISO is important in that aspect.

I think the other side, as CISOs, in order to make that happen, we have to be significantly less concerned with technology. Again, that's about reporting outside of just the CIO because technology without underlying process or understanding is useless and yet, the whole industry, if you go to any industry event, is focusing so much on the purchasing of blinking boxes. The more we focus on the model where the CISO is a clear business leader, the better we'll be as an industry and as organizations in regard to what they deliver to their customers.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446



DECEMBER 2018

K logix

WWW.KLOGIXSECURITY.COM
888.731.2314