

FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE

CYBERSECURITY SKILLS SHORTAGE
FINDING TALENT THAT STANDS OUT

DECEMBER 2017

WWW.KLOGIXSECURITY.COM

888.731.2314

||||K logix

Confident information security

The background of the entire page is a teal-colored wooden surface with vertical grain lines. Scattered across the left side of the page are ten yellow rubber ducks, each with a red beak and black eyes. They are arranged in a loose, vertical column. The title 'FEATS OF STRENGTH' is centered in the upper half of the page in a large, white, sans-serif font. Below it, the subtitle 'FINDING TALENT THAT STANDS OUT' is also centered in a smaller, white, sans-serif font. In the bottom right corner, the date 'DECEMBER 2017' is printed in a small, white, sans-serif font.

FEATS OF STRENGTH

FINDING TALENT THAT STANDS OUT

DECEMBER 2017

TABLE OF CONTENTS

04 **Intro Letter**
From Kevin West, CEO, K logix

06 **Justin Somaini**
CSO, SAP

08 **Infographic**
Skills Gap Statistics

10 **Suzie Smibert**
CISO, Finning Financial

12 **Who is Your Next Hire?**
Which Industries to Focus On

14 **Doug Graham**
CSO, Nuance Communications, Inc.

16 **Q&A with Pedro Abreu**
Chief Strategy Officer, ForeScout

18 **Nicholas Shevelyov**
CSO, Silicon Valley Bank

20 **Q&A with Francois Lasnier**
SVP, Gemalto

22 **Fred Kwong**
CISO, Delta Dental Plans



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

Magazine Created By:

K logix

Magazine Contributors Include:

Kevin West
CEO, K logix

Katie Haug
Director of Marketing, K logix

Kevin Pouche
COO, K logix

Stephanie Hadley
Content Manager, 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.



SHORTAGE OR NOT, IT'S ALL ABOUT QUALITY OVER QUANTITY

The cybersecurity industry continues to boom, with market growth from \$3.5 Billion in 2004 to \$120 Billion in 2017, and spending predicted to exceed \$1 Trillion in the next five years.

Influxes of VC funding, increase in security budgets and significant numbers of CISOs joining the boardroom, all contribute to this remarkable growth in a short period. Paired with these industry trends, the role of cybersecurity professionals has evolved to encompass augmented expertise requirements. In his profile, Justin Somaini, the CSO at SAP (pages 6-7) points out, "In 20 years, security teams have evolved from offering simple technical solutions, to addressing compliance requirements, to understanding international law, and now we play a role in the customer purchasing cycle. As an industry, we have a massively increasing expectation

of skills every year for our security professionals."

Ten years from now the market could correct itself. But for now, CISOs are taking action on the lack of talent. Many are relying on their foundational beliefs in quality over quantity. We've done this at K logix by building a core team of trusted, hardworking and multi-faceted people. These are the team members who approach any challenge with confidence and an underlying sentiment that aligns with the fundamental values of our organization.

It appears CISOs may be moving away from growing their teams as quickly as possible, with as many people within budget. Regardless of size, an ideal shift for CISOs to make is strongly investing in 'anchor' team members who aspire to continually develop and grow as professionals. These people strive to contribute to innovation and progress, and will likely demonstrate clear advancement in their careers. The result of hiring these types of individuals is a nimble, competent, dedicated team, and when the market eventually does adjust, the

ability to increase staff size.

Many of the CISOs we interviewed in this issue understand the benefits of building core, quality teams. This issue explores how they approached the problem, whether it's re-framing the job description, re-training staff or re-thinking the challenge entirely.

TURNING TO TRUSTED PARTNERS

Large numbers of CISOs turn to partners for key outsourced help. At K logix, increasing numbers of customers partner with us to help them make an impact in strategic areas of need. When teams are working at full capacity, timelines are short and programs may lack formal processes in place, we take the burden off these teams. Whether it's understanding areas of investment for new technologies, or formalizing a board room presentation, CISOs will continue to rely on trusted partners for guidance.

In his profile (pages 22-23), Fred Kwong (CISO, Delta Dental Association), finds partnerships as one solution to the staffing problem. By leveraging the MSSP model, he is able to focus on strategic programs, while his partners are responsible for appropriately staffing the team. On page 23, he explains, "I have a small team at DDPA. There are only two of us dedicated to security within the association. The rest of my team is located at our MSSP. With the MSSP model our member organizations do not need to worry about hiring and retaining security staff. Our MSSP takes on that burden for us."

CULTURE AND OPPORTUNITY KEEP STAFFERS ON BOARD

Nearly all CISOs we interviewed say they effectively retain employees by providing opportunity to advance in their careers and make an impact on the organization.

As stated in his profile (pages 14-15), Doug Graham the CSO of Nuance Communications, Inc., focuses on defining realistic job descriptions, and empowering his staff. Graham says, "Security people have an unbalanced sense of duty. More than salary and work-life balance, they want to do the right thing and impact change. If you can pay the right people a fair salary and show them that the organization is behind the security vision, and if you are able to give them the opportunity to impact positive change, then you are much more likely to hire and retain talent."

In his profile (pages 18-19), Nick Shevelyov, CSO of Silicon Valley Bank states, "We are trying to cultivate a network of professionals. We are exploring ways to contact people in other industries and explain how cybersecurity fits into their career paths. Cybersecurity is a broad business problem, so there are many roles that do not require a technology background. For example, governance and information assurance often do not

require deep technical expertise. We are doing a lot of measurement in our analytics group, so a classic data scientist can be a good fit for that team."

IS THIS MUCH ADO ABOUT NOTHING?

In this issue, several CISOs suggest the staffing challenge may be a problem of our own making. They believe we might solve it by changing the way we think about staffing and who we recruit.

Graham succinctly sums up this line of thought. On page 15, he says, "I think there might not be as big of a gap in the market as we think. I think a lot of CISOs are looking for unicorns. They want to find one employee who can do every aspect of the security job. Someone who is technical, a visionary, an architect, and a skilled operations guy. That is just not realistic"

Suzie Smibert, the CISO and Global Director Enterprise Architecture at Finning International has this to say in her profile (pages 10-11), "I think we are bounding ourselves too much to specific degrees and technology or specific paths to get where you are. You could hire paralegals, auditors and HR people. We are restricting ourselves too much in what we are looking for in terms of talent. We keep looking for technical backgrounds. Other backgrounds might be more inclined to round up all the diversity of thought you need in a team."

OPPORTUNITY REQUIRES ACTION

Looking forward, the skills gap should close as the market catches up. What is evident in these potentially challenging moments, is the resilience and business aptitude of CISOs who are facing it head on. These are the leaders taking action by starting to build strong 'anchor' teams. Instead of faltering under the pressure to fill open job placements, they ardently shape opportunities of success and advancement for their core teams.

In the profiles ahead, you'll understand how CISOs approach the skills issue and be able to attain imperative methods from our industry research.



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
WHO ARE LEADING THE WAY
FOR CONFIDENT SECURITY
PROGRAMS



JUSTIN SOMAINI
CSO, SAP

HEADQUARTERS: Walldorf, Germany

EMPLOYEES: 84,000

ANNUAL REVENUE: \$26 Billion

"I think it is human nature to want to talk first, in order to communicate your point. But to build relationships within the company, you must ask questions and find alignment with others. It is important to start with a consultative approach to these initial conversations, as you work to understand their business goals and challenges."

- JUSTIN SOMAINI

TACKLING BIG CHALLENGES, FROM THE GLOBAL THREAT LANDSCAPE TO SECURITY SKILLS SHORTAGE

While Justin Somaini believes there are only two main reasons he took the newly established role of Chief Security Officer at SAP in 2015, it might better be described as more than 300,000 reasons. He explains, "The first thing that motivated me to take this role at SAP was the challenge of tackling the threat landscape on a global scale. The second reason was SAP's more than 300,000 customers. SAP's product security is critically important to our customers, because our solutions deal with their most critical business information."

As Chief Security Officer at SAP, Somaini leads a team of 250 security professionals, providing physical security, enterprise security and product security. For Somaini, the high stakes nature of SAP's security program is very appealing. He comments, "Probably more than many other companies, SAP sits right in the middle of the information security challenge on a global scale. My team has the ability to shift the needle on security and solve big problems for our customers."

Somaini says SAP made a significant commitment to security starting in 2015, when the Board created the CSO role. This high-level commitment holds important to Somaini's ability achieve success within the role. He explains, "SAP is not just paying lip service to security. This is obvious in the way the organization is structured." Somaini first reported into a Board member, and now into the CTO. He says, "Security remains a Board-level priority and many conversations about information security take place at that level."

"YOU HAVE TWO EARS AND ONE MOUTH FOR A REASON"

A true veteran as an industry leader, Somaini has held many distinguished security positions before,

most notably the CISO at Yahoo and Chief Trust Officer at Box. He explains, “The first three months as a new CSO can feel like vacation. It’s all about kissing babies, shaking hands, and understanding the environment.” He explains one of his first priorities is to understand the objectives and challenges of business owners. “In the first three months, you want to gauge security maturity within the company, ensure security is aligned with business priorities, identify major problems and most importantly, build strong relationships with peers inside the company.”

He continues, “But the first year can be a real challenge too, you need to make strategic decisions while dealing with tactical problems, and sometimes without all the information you would like to have. That is why it is so important to form strategic relationships with line of business executives.”

Somaini notes that at SAP, the line of business leaders are very open and receptive to having conversations about security, and making changes to address security problems. He has advice to pass on from one of his mentors, John Thompson, the former CEO of Symantec.

“John said to me, ‘You have two ears and one mouth for a reason. Use them to listen twice as long as you talk.’ I think it is human nature to want to talk first, in order to communicate your point. But to build relationships within the company, you must ask questions and find alignment with others. It is important to start with a consultative approach to these initial conversations, as you work to understand their business goals and challenges.”

Somaini also suggests new CISOs should prioritize learning the business, first and foremost. He suggests, “New CISOs need to educate themselves on the business. For example, understand how marketing works, and how it can impact the sales cycle. Sometimes security teams are out in left field, with no visibility and no desire to understand how businesses operate. But to build alignment and to figure out how to build security into the business you need to be able to speak the language of business. Few line of business leaders will participate in security efforts if you cannot speak their language.”

UNDERSTAND CUSTOMER REQUIREMENTS AND PRIORITIES

According to Somaini, after the first year, security efforts should evolve beyond internal operations to understand customer priorities. “We have to understand how our customers are using SAP products and what their specific vulnerabilities and requirements are for the product. We have customers across multiple vertical industries, and their expectations are not always the same. We must realize what a financial services organization needs and expects

is different from what a healthcare or oil and gas company needs. I am constantly assessing if my team has a good read on customer expectations and if our security measures are meeting and exceeding those expectations.”

STAFF A PYRAMID TO CONQUER THE SKILLS SHORTAGE

“I’ve been doing information security for more than 20 years, and I can tell you that the skills gap is nothing new. In 20 years, security teams have evolved from offering simple technical solutions, to addressing compliance requirements, to understanding international law, and now we play a role in the customer purchasing cycle. As an industry, we have a massively increasing expectation of skills every year for our security professionals,” explains Somaini.

He continues, “Information security is a tough business. Every company is looking to hire from the same mature talent pool, which cannot expand quickly enough to meet our needs. When you really think about it, this is a silly way for us to be addressing the growth of our industry.”

“When we only hire mature and experienced professionals, we stifle growth. That is why I staff our organization as a pyramid. Most companies staff information security like a diamond. There is a CISO, then a large staff of experienced security professionals, then only a handful of early talent. With pyramid staffing we have experienced security professionals distilling difficult challenges down to simpler problems that early talent can address confidently, while also learning from new experiences.”

At SAP, Somaini introduced a two-year training program to bring more employees into the security program. His managers identify young professionals, recent college grads, or IT support staff who are curious, technically adept and have a strong moral compass, and put them through a two-year on the job training program. This gives young professionals the opportunity to mature more quickly into more senior roles.

Somaini points out that on-going training is required, as once a security professional reaches the management level they need another set of training in managing people and programs. He says simply, “Our organization needs more mature and skilled employees, and it is our obligation to train people to fill those roles.”

He is also quick to note the need for on-going education does not stop outside the CISO’s office. He explains, “The role of the CISO is continuing to mature as we would expect, and as result we need to have leaders that are continuously educating themselves.”

THE SKILLS GAP: TACKLING CHALLENGES AND CHANGING APPROACHES

Katie Haug, Marketing Director
Marcela Lima, Marketing Coordinator

THE SKILLS GAP

According to the Forbes' article "*One Million Cybersecurity Job Openings In 2016*", the cybersecurity market is expected to grow from \$75 billion in 2015 to \$170 billion by 2020. It's no secret there is a prevalent skills gap in this industry. The CSIS (Center for Strategic and International Studies) published a study in 2016 which revealed that 82% of security professionals report a shortage of cybersecurity skills in their organizations.

Sources including Cybersecurity Ventures and Security Magazine have predicted close to 1.5 million unfilled cybersecurity positions globally by 2020. This tremendous amount of growth means the skills gap may eventually close as organizations catch up with the market expansion. However, the current situation and challenge demands CISOs to strategically work within their own organizations, as well as with the industry to find talent.

CISOs and security leadership struggle to fill open job postings due to lack of skilled applicants. When polled, 34.5% of security managers cited lack of security expertise as a key reason to why they could not fill open positions. Cybersecurity professionals, when hiring, are unsure of what skills or qualifications are most important when looking to recruit employees (451 Research study). The CSIS study showed that 77% of security professionals believe education programs are not fully preparing or urging students to enter the cybersecurity industry. These statistics on why the skills shortage exists imply the challenge of unfilled positions is one of a lack of education and knowledge regarding the industry.

HOW TO MAKE STRIDES AS AN INDUSTRY

As an industry, it is key to take a step back and understand the root cause of the challenge we are facing. The cybersecurity workforce lacks a diverse array of professionals. According to a 2017 study "*The Global Information Security Workforce*" conducted by the Executive Women's Forum, only 11% of cybersecurity professionals are women. The industry must encourage more women to enter careers related to STEM (science, technology, engineering and math). Integrating more women in the industry will not only lower unfilled positions, but potentially add a stronger

variety of traits including different skillsets and problem solving approaches.

Many CISOs we interview for this magazine believe their greatest accomplishments are when they influence and make an impact on young people interested in entering the field. Some encourage internships with high school and college students at their organizations. Others host students for educational cybersecurity days or teach at local colleges and universities. A large amount of CISOs who teach use this as a way to give back, but also to recruit future team members.

PROMOTING AND GROWING

To retain a strong, quality workforce, many CISOs invest heavily in a core group of team members. These professionals aspire to grow within the organization and seek to take on more leadership roles. Promoting cybersecurity job openings amongst other departments within an organization may be key to attaining additional talent.

Many CISOs agree they can teach cybersecurity skills to anyone, but the soft, business skills are what they look for in candidates. When this is the case, looking outside of professionals with cybersecurity backgrounds may prove beneficial. Employers may consider hiring lawyers, accountants, or HR professionals who can bring other core business functions to a technology position.

In conclusion, the skills gap is a fundamental and persistent challenge that is continuously growing. Industries and organizations must work together to: promote cybersecurity careers by way of internship and training opportunities for students, encourage women to work in the STEM field, develop talent from within and look outside of traditional tech fields to procure talent.

SOURCES:

Forbes, "*One Million Cybersecurity Job Openings in 2016*"

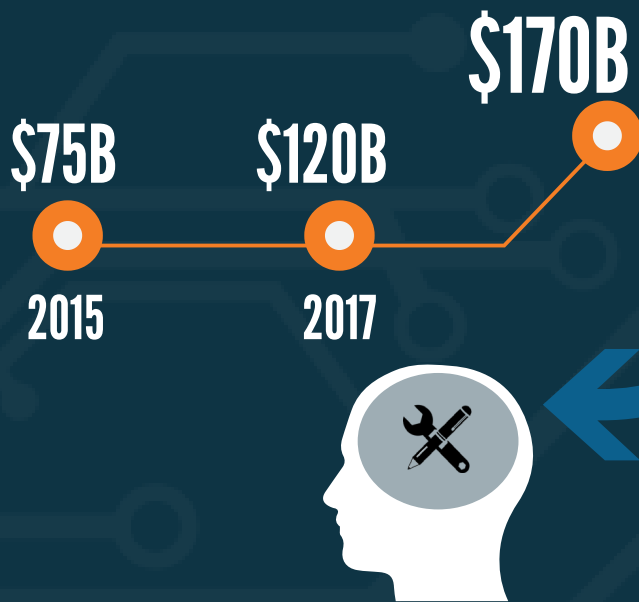
CSIS, "*Hacking the Skills Shortage*" 2016 Study

Security Magazine, "*How Cybersecurity Education Aims to Fill the Talent Gap*"

VentureBeat, "*Digital organizations face a huge cybersecurity skills gap*"

Executive Women's Forum 2017 Cybersecurity Workforce Study

CYBERSECURITY MARKET



CYBERSECURITY MARKET EXPECTED TO GROW TO \$170B BY 2020

YET

82%

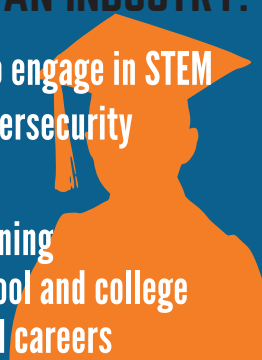
of security professionals report a shortage of cybersecurity skills in their organizations



The Global Cybersecurity workforce will have
MORE THAN 1.5 MILLION
unfilled positions by 2020

BUT WHY IS
THERE A SKILLS
SHORTAGE?

WHAT WE CAN DO AS AN INDUSTRY:

- 
- Encourage more women to engage in STEM careers (only **11%** of cybersecurity professionals are female)
 - Offer **internships** and training opportunities to high school and college students to promote STEM careers

WHAT ORGANIZATIONS CAN DO TO ATTRACT MORE TALENT:

- Look **internally** for talent
- Look outside of cybersecurity sphere - consider **lawyers, accountants, and others** who could bring valuable skills to the company
- Step up **company advocacy**

- **34.5%** of security managers cited lack of security expertise as a reason why they could not fill positions
- Companies are unsure of what skills or qualifications are most important when looking to recruit professionals
- **77%** say education programs are not fully preparing students to enter the industry

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS
WHO ARE LEADING THE WAY
FOR CONFIDENT SECURITY
PROGRAMS



SUZIE SMIBERT

CISO & GLOBAL DIRECTOR ENTERPRISE
ARCHITECTURE, FINNING INTERNATIONAL

HEADQUARTERS: Vancouver, British Columbia

EMPLOYEES: 14,500

ANNUAL REVENUE: \$6.9 Billion (Canadian Dollars)

BUILDING A CULTURE OF CYBER SECURITY

Suzie Smibert, the Global Director of Enterprise Architecture and CISO at Finning International, the world's largest Caterpillar dealer, knows her strengths. She explains, "When I get hired, it is because they want to build something from scratch, create a culture of cybersecurity, bring on a team, processes and vision, and execute on it." Finning brought her on board to set the cyber security groundwork for the company.

When Smibert joined the organization, she understood the cyber security program required dedicated work and a strong, positive influence. She comments, "The existing cyber security program was still very much a dinosaur. It was a program predicated on saying 'no', not wanting to enable business and find a different way of getting things done. My team was motivated to switch that mindset and we wanted to find a creative way of making things secure."

Almost three years into the role, Smibert reports the company has advanced significantly, but as most security programs, still requires continued support. She says, "Finning is a large organization that historically has not thought of itself as innovative in technology, yet we are

transforming and growing our digital business."

To that effort, Smibert notes the company has made tremendous progress with regards to cyber security awareness. She notes, "That is the easiest and cheapest way to reduce risk to an organization and engage the end user communities and executives in wanting to support cyber security."

Smibert continually works to instill security as a basic safety issue for the company. She explains, "People do not think twice when they see a cable on the ground. They say, 'Hey, that's a safety hazard' and then they make sure no one trips on it. We're transforming our culture so cyber security becomes the same as our reaction to health and safety issues like that. "

The work of Smibert and her team are paying off in this regard. She says, "We went from an industry average click-rate on our phishing campaigns to less than 10% globally. That is a tremendous achievement for our organization over the last few years. Once we achieve a very solid foundation, and our security culture is more mature, we are able to leverage automation capability for e-commerce and for IoT devices for our customers."

MAKING CYBERSECURITY PERSONAL

To transform Finning's cyber security culture, Smibert made security personal for the company's almost 15,000 employees across the globe. She explains, "We have a multi-faceted approach to training. Not everybody learns the same way. One of our team members is a behavioral psychologist. He made us realize the mind works differently depending on our countries and languages. Some people need to read, others need to hear, others need to see."

To address these different learning styles, Smibert's team provides various security training tools, including videos, posters, face-to-face training and third party-led sessions. She states, "We focus on making learning fun, and reaching an individual with the tools they need to succeed."

Her personalized approach extends beyond diverse training tools. "We are making cyber security awareness about the individual, not about the organization. Our employees need to understand there is something in it for them, as opposed to making cyber security all about compliance and protecting the company. We make our training personal by providing tips to improve security at home, while shopping, and for child safety online." This approach helps Finning employees internalize the value of cyber security.

EXECUTIVE SUPPORT BY ALIGNING SECURITY TO BUSINESS GOALS

Executive alignment, including valuable support from Finning's CEO and CIO, strongly helped empower Smibert's security program transform the culture of the company. Furthermore, her relationship with the Board weighs strong, she says, "It is respectful; there is trust, and the right questions are being asked. I have been privileged to not be confined to only five minutes, once a year, in front of the Board. We have a dialogue and ongoing conversation on the state of cybersecurity, risk profiles and the trends we see. The CEO and CIO have empowered me to execute on my strategy. That has helped me drive lots of change."

Smibert gained the confidence of Finning's Board by focusing on key, valuable business-aligned metrics. She comments, "What I do must support what the company's objectives are. I like to understand where we are in terms of maturity. What are we missing? What are the biggest risks? Then, I need to understand the senior leadership's and the board's overall risk tolerance."

Her presentations to the board constantly relate to business

goals and risks. As a result, the Board understands and acknowledges the state of the program along with Smibert's goals and what she needs in order to execute on the program. She notes, "We are not presenting metrics about how many attacks we have thwarted. Instead, we are translating our content from security in terms of maturity, in terms of impact to bottom-line and in terms of reasonable and prudent operating model."

Building a High Performing Team

Smibert believes great talent attracts more great talent. She explains, "Empower your people when they join your organization. My job is to remove obstacles and give them guidance. Let them fail and fail fast, and do not dwell on it. Instead, celebrate and make progress."

When it comes to the perceived lack of available talent in the cybersecurity industry, Smibert believes security leaders are being self-limiting. "I think we are bounding ourselves too much to specific degrees and technology, or specific paths to get where you are. You could hire paralegals, auditors and HR people. We are restricting ourselves too much in what we are looking for in terms of talent. We keep looking for technical backgrounds. But those technical people, they hate writing policies and they do not like to present when it is security awareness month. Other backgrounds might be more inclined to round up all the diversity of thought you need in a team."

"I see the stigmas around the security industry changing. I have a diverse team comprised of different ethnicities, backgrounds and genders. While my team is one third female, integrating women into the security industry is key and must start with encouraging more women to be interested in STEM fields. We need to promote, be visible and not tolerate anything that goes against diversity."

Who is your Next Security Hire?

Where to look outside of information security

In addressing the skills gap in cybersecurity, CISOs and their human resource counterparts now engage in creative tactics to recruit and retain employees to join their teams. Here we look at other industries where the next great cybersecurity professional might be found.

CATEGORY: TRIED AND TRUE

1. LAW ENFORCEMENT AND MILITARY

Type Casting: Professionals in these industries are generally astute forensic investigators, and shrewd when it comes to identifying suspicious activity.

The State of Their Industry: The Bureau of Labor Statistics reports that employment of police and detectives is projected to grow 4% from 2014 to 2024, which is slower than average compared to other occupations in the United States. However, the contract defense industry is projected to grow rapidly as the United States defense budget increases, after years of steady decline. Military veterans interested in staying in the defense industry will find opportunities there.

Fit Factor: Based on statistics of CISOs we have featured in our magazine, roughly 30% are veterans of the armed forces.

Learning Curve: Technical and engineering degrees are not generally required for employment in law, so these cross-over hires may need additional training on technology.

2. IT GENERALISTS AND NETWORK ENGINEERS

Type Casting: Employees who already understand the systems, networks and applications that need protecting are obvious candidates. According to Digital Guardian, 59% of CISOs came up through the IT ranks.

The State of Their Industry: According to a recent report in USA Today, this year, there are 627,000 unfilled IT jobs in the United States. Many IT

professionals might decide to transition into information security to broaden their skillsets.

Fit Factor: There is a reason most CISOs come from IT - a strong knowledge of technology is important to protecting a company's vital assets, and IT workers possess that knowledge to great degrees.

Learning Curve: Familiarity with technology can help IT professionals hit the ground running in information security, but sometimes these tech-savvy contributors need education and training to understand business goals and to communicate security to business users.

CATEGORY: WHERE COMPLIANCE MEETS SECURITY

1. LAWYERS

Type Casting: Increasing industry and government regulations, the importance of security policy and the introduction of tools such as cyber risk insurance, have all made a law degree highly-valuable for specific strategic roles on the information security team. There is also a spike in organizations adding Chief Privacy Officers to their executive teams.

The State of Their Industry: Young lawyers may be on the hunt for non-traditional roles. Recent graduates of law schools are 5% less likely to be employed in their field than they were in 2007, according to the National Association for Law Placement.

Fit Factor: A prospect with a law degree may be a good fit for a CISO's e-discovery and forensics team, and has the ability to help navigate compliance and customer and employee privacy issues.

Learning Curve: Lawyers will be naturals at dealing with corporate privacy concerns and the legal ramifications of non-compliance. They will be adept advocates for sound security policies. They likely will not come with a technical background.

2. ACCOUNTANTS

Type Casting: An accountant's time-tested skill in

performing audits will make them a natural fit for the compliance and audit group within an information security organization.

The State of Their Industry: According to the Bureau of Labor Statistics, the accounting industry is projected to grow 11% from 2014 to 2024.

Fit Factor: Accountants are skilled in investigations and capable of understanding complex laws and regulations. Tax accountants have a reputation as detail-oriented, ethical and diligent employees.

Learning Curve: While a natural fit for audit and compliance teams, they may lack the skills and training to work on the technical side of information security, or the appetite to work in threat detection.

CATEGORY: THE COMMUNICATORS

1. BUSINESS ANALYSTS

Type Casting: Business analysts are the bridge between IT and business users, tasked with taking business requirements and helping developers and engineers create systems that meet the needs of the user.

The State of Their Industry: Business analysts often grow into positions of project management within the IT department. To advance beyond middle management, analysts must pick a field of focus, such as information security.

Fit Factor: Business analysts are skilled in communicating in both business and technical language, a core attribute CISOs seek in their team members.

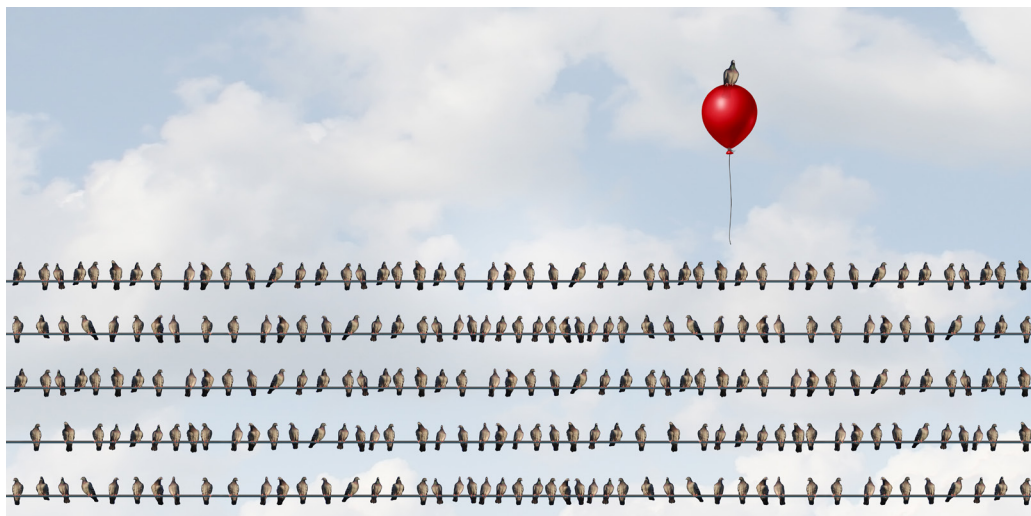
Learning Curve: Most business analysts have some technical knowledge, although an IT degree is not a necessity for the role. Business analysts will be comfortable in outward-facing security roles, as

well as performing testing, systems monitoring and investigations as a security analyst.

2. TRAINING MANAGERS

Type Casting: Training and internal communication professionals are experts in delivering complex information in easy to understand ways.

The State of Their Industry: According to PayScale, the average salary of a training manager is \$66,000, and the average salary of a mid-level information security professional is over \$100,000. Training jobs are readily available, the salary increase may make a jump to information security very appealing.



Fit Factor: Business user training and effective communication skills are crucial among CISOs' reported challenges. These professionals are creative thinkers adept at presenting information in articulate ways, making them expert liaisons between the business and more technically-savvy information security professionals. They may also be enlisted to deliver important end-user training, assist in writing clean policies and run security ambassador programs.

Learning Curve: It is likely corporate trainers or internal communications professionals will need to be trained in information security specifics.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS
WHO ARE LEADING THE WAY
FOR CONFIDENT SECURITY
PROGRAMS



DOUG GRAHAM
CSO, NUANCE COMMUNICATIONS, INC.

HEADQUARTERS: Burlington, MA

EMPLOYEES: 14,000

REVENUE: \$1.93 Billion

DOUG GRAHAM IS A CHANGE AGENT AT NUANCE

Doug Graham, the Chief Security Officer at Nuance Communications, views the CSO position as a “change agent, driving transformation across the organization.” Before he joins any organization, he evaluates the company’s commitment to the security program, and the company’s ability to withstand the kind of change required to build a next-level security program.

Graham notes, “While the interview process is the organization’s chance to learn more about me and determine if I am a good fit, the interview process is equally my opportunity to gauge if the security program is well-supported within the company.”

He continues, “At the C-Level, information security is more about chemistry, fit and philosophical alignment than it is about technical capabilities. Of course, a CISO or CSO needs to have a technical resume, but if he or she cannot work with the other executives, or within the existing company culture, it will be difficult to be successful in driving change. In the interview process, neither the company nor the candidate will have all the answers, but both sides should be able to come to a shared

understanding of what a good program will look like.”

At Nuance, Graham says his charter is, “to strengthen the security posture and build out a strong team, and make the security program match the company’s culture.”

VETERAN CISO ADVICE FOR THE FIRST 90 DAYS

With many years of leadership experience in information security, Graham offers advice to CISOs who may be new to the role. “There is a bucket of things to consider in the first 90 days in a new organization,” explains the veteran CSO. Graham recalls these priorities:

1. Assess the maturity of the security function

Graham encourages CISOs to first understand the knowledge levels of team members across technology, governance, risk and compliance and policy. A new CISO must determine if team leadership accurately reflects the structure required to effectively enhance the security program. When possible, review previous security efforts and understand where the previous CISO succeeded and failed.

2. Understand the operating model of the company

Graham points out the importance to understand organizational structure. For example, he states, “Identify if there is a single IT entity across the organization, if shadow IT is a concern, and if the company operates offsite data centers and global operations.”

3. Build a network of support

“Build support for the security program from the top down, as this will provide the necessary mandate for security changes,” explains Graham. It is also important to note the relative security expertise across the entire organization. Security savvy organizations will more easily adapt to changes, while less savvy teams may need more persuasion.

Graham says at the end of sixty or ninety days most organizations will expect the new CISO to be able to provide a high-level read-out on the security program, including basic outlook, significant risks and priorities.

A FIVE-POINT PLAN FOR SECURITY

Once a high-level understanding of the security program is in place, Graham suggests implementing a strategy. Graham notes, “A twenty-page document or dissertation is not required, but something that can be modeled and repeated, and aligns with future activities, is a good starting point.” As an example, Graham shares his “five-point plan”. He says the plan provides clarity about your mission and encourages a consistent approach and set of core goals.

Nuance’s five-point security plan includes:

1. Company-Wide Security Hygiene

“Security needs to be treated like hygiene. Everyone needs to do it, just like brushing your teeth. Although every organization has a security team, security is everyone’s responsibility.”

2. Incident Detection and Response

“There needs to be a system of safeguards in place for when hygiene fails.”

3. Compliance Management

“At Nuance, we have a billion-dollar healthcare practice, and we often operate with financial services organizations. We need to understand compliance across those industries, and many others. We must understand privacy requirements and regulations, and acknowledge that sometimes those

requirements will conflict with our risk strategy.”

4. Risk-Based Strategy

“My goal is not to create maximum security. We need to balance risk with security. We always have to consider that too much security opens up its own risks, and presents challenges to business operations.”

5. Customer Transparency

“We will not meet our revenue goals if we cannot present a transparent security program to our customers.”

Graham notes, “These five points have been the five key pillars of our security program since day one. Everything we do aligns back to these points. We report to the Board based on these pillars.”

While this program, which tends to be more qualitative than quantitative, works well for Graham, he cautions new CISOs to resist a one-size-fits-all model for presenting to the Board. “You want to tailor your presentation to the Board based on context and situation-specific requirements. You need to do your upfront research. Understand who is on the board, what their security knowledge is and how they absorb technical information,” explains Graham. He continues, “The most important part of any Board meeting is the work you do before-hand and the action items that come out of it.”

CYBERSECURITY SKILLS GAP

“I think there might not be as big of a gap in the market as we think. I think a lot of CISOs are looking for unicorns. They want to find one employee who can do every aspect of the security job. Someone who is technical, a visionary, an architect and a skilled operations guy. That is just not realistic. This might be because we ask for five employees and we get budget for two, so we try to jam-pack our job descriptions. We must design our job descriptions based on realistic understandings of the talent pool.”

Graham continues, “Security people have an unbalanced sense of duty. More than salary and work-life balance, they want to do the right thing and impact change. I see security people get really frustrated when feel they are not listened to within the organization. If you are able to pay the right people a fair salary and show them the organization is behind the security vision, and if you can give them the opportunity to impact positive change, then you are much more likely to hire and retain talent.”

Q&A WITH PEDRO ABREU

CHIEF STRATEGY OFFICER, FORESCOUT



With more than 20 years of industry-leading operational and management experience, Pedro leads corporate strategy at ForeScout Technologies, Inc. Prior to joining ForeScout, Pedro was Senior Vice President of Strategy and Go-To-Market Operations at McAfee (formerly Intel Security). In addition, he has held several senior-level strategy and operations roles with EMC, Documentum and McKinsey. Pedro earned an MBA from Haas School of Business at U.C. Berkeley, and a CS in Computer Science from Instituto Superior Técnico in Portugal.

Q: IN A HEAVILY CLUTTERED MARKETSPACE, HOW DOES FORESCOUT STANDOUT?

One big challenge for CISOs today is clearing the security technology messaging clutter. There is such a large proliferation of companies coming out with statements that they solve all security issues that it's almost become a joke in Silicon Valley. We tend to look at ourselves differently in the market. While there are lots of startups saying they are the next silver bullet, we see ourselves as a foundational element of security strategy. It's not about the silver bullet, it's about being foundational. We integrate and partner with many of these new startups to learn something from the information they are capturing that can potentially enhance our solutions.

A large gap in our industry exists between the marketing claims that companies make about their products and what their product actually does. If there's one thing we're very proud of internally, it's that we have been very conservative in terms of our marketing and the claims we make. We stand behind our claims and our customers stand behind us, as references. That's a big part of why we've had success. It's that clarity—our customers know what they're going to get.

We gain many customers as references and invite them to be speakers on our behalf in the marketplace and among their peers. We depend on these formal and informal networks to spread the word, and that's how we get through the clutter created either by the industry giants or the small guys.

Q: WHAT ARE THE BIGGEST CHALLENGES ENTERPRISES ARE FACING AS THEY TRY TO SECURE IOT?

The biggest challenges most companies face when securing IoT is they don't know everything that is connecting to their networks. Over the last five years, the

user has become accustomed to the fact that everything is connected. All parts of the business are buying new devices they expect to be connected without asking permission from IT. This risk around visibility is pervasive.

The second challenge is the ability to know what each device is supposed to do on your network. If you can control and put limitations on those devices, you've solved 80 to 90 percent of risk associated with your connected network.

Q: HOW DO YOU HELP CUSTOMERS UNDERSTAND HOW FORESCOUT FITS INTO THEIR BROADER SECURITY STRATEGY?

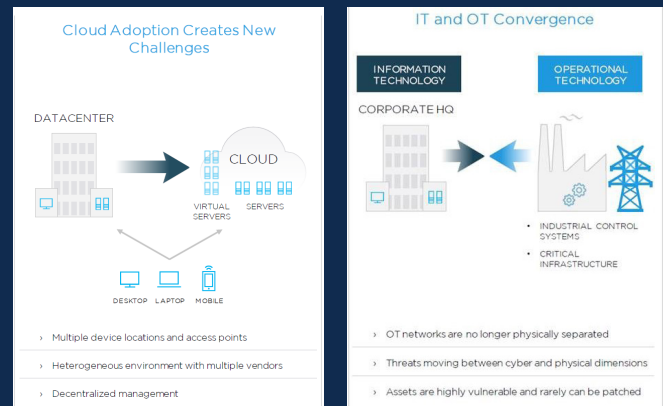
We spend time with CISOs building the case as to why controls and visibility are critical. We help them and equip them to allocate the right budgets to invest in these initiatives. Today, this may be challenging for CISOs because they are constantly moving their dollars around to multiple initiatives in efforts to reduce risk.

The first step is to help CISOs clearly communicate how visibility fits within their underlying foundational element of security strategy. The second step is helping them understand that the current approach and tools they have may not be sufficient or provide 100 percent visibility. The third step is determining return on investment (ROI). Visibility only becomes an ROI when you start automating what you are seeing with an entire set of other tools. When you get visibility into your environment, you can automate with different technologies to accelerate incident response. That's when you can detect things earlier and act much faster.

What's the next wave of technology enterprises must secure?

Now that the world has moved to the cloud, it's extremely easy for companies and business units to bring new services and new servers into a virtual network or environment, creating an explosion of virtual instances that must be discovered and managed. The rapid adoption of cloud computing creates serious challenges for CISOs who are unable to gain necessary visibility of these activities. We see this as one of the next big areas of risk and security that companies must address.

The other area of future focus is Industrial IoT or the operational technology space. This could be the manufacturing environment for pharmaceutical companies, or bridges for smart cities. Consider nuclear plants, to take it to an extreme. They designed these things decades ago, but now they're seeing they can pull information out of those environments to the cloud, do some predictive maintenance and potentially get a lot of value back into their business. Organizations are being forced to break that air-gap network and realize that, when they do, they're creating new risks.



We're seeing a huge demand now in organizations where senior management—including the board of directors—is requesting that CISOs take responsibility for the operational side of the business, and not just the corporate IT environment.

Q: WHAT IS THE MOST INTERESTING INTEGRATION AND USE CASE BASED ON YOUR ORCHESTRATION CAPABILITIES?

Visibility is valuable, but becomes more valuable when it's getting used more broadly by companies across all security tools. Over the last few years, we've worked on how to take visibility and integrate it into other platforms.

Integrating with the security information and event management (SIEM) space allows the ability to accelerate incident response. We make it possible for SIEM tools that might be simple dashboards to actually allowing the users to take actions directly on what is occurring on devices on the network.

For the advanced threat defense space, integrating means learning what threats are identified on their

environment and finding where else attacks could potentially occur. Then, we can immediately take action and stop the attacks.

Q: HOW DOES FORESCOUT HELP ORGANIZATIONS CLOSE THE CYBERSECURITY SKILLS GAP?

One of the biggest challenges security operations teams have is staffing. There's a risk today because companies are hiring incredibly talented individuals, but they are doing many manual, repetitive and somewhat boring tasks. This may result in attrition and people moving on to organizations that allow them to do more interesting types of work. More thoughtful CISOs/CIOs are looking at automation not just from a security perspective, but also from a talent-retention perspective, and they're leveraging our capabilities around orchestration.

We help organizations through orchestration and our Extended Models which represent various integrations so they can quickly share information without having to track manually. We do not automate every aspect of a security job but we automate the predictable and known parts of those jobs. There's a perceived fear that automation may not be effective, which is why companies might resist the idea. We did not build our orchestration vision to be a platform that automates every step of the process. It's intended to automate known tasks and steps that need to be responded to in real time to keep the organization safe.

With this, we're releasing individuals to do more advanced aspects of security. We help them reduce the time to respond, but more importantly, we help make the job a lot more compelling.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS
WHO ARE LEADING THE WAY
FOR CONFIDENT SECURITY
PROGRAMS



NICHOLAS SHEVELYOV
CSO, SILICON VALLEY BANK

HEADQUARTERS: Santa Clara, CA

EMPLOYEES: 2400+

TOTAL ASSETS: \$51 Billion

EXPERIENCING THE EVOLUTION OF CYBERSECURITY FIRST HAND

Nicholas Shevelyov, the Chief Security Officer of Silicon Valley Bank says the bank's mission is to improve the probability of success for entrepreneurs all over the world. He explains how his security organization is directly aligned with that mission, "The bank cultivates an ecosystem for innovation. Part of providing that ecosystem is protecting the interests of the bank and our clients in a rapidly evolving digital world."

In his ten years as CSO at Silicon Valley Bank, Shevelyov's role and the role of cybersecurity in general have evolved to be more vital to that mission. He comments, "Technology used to be just a cool innovation, but now technology permeates every aspect of our lives and business. The technology that empowers us simultaneously may imperil us, so cybersecurity is now a fully-integrated aspect contributing to the success of our business."

With a decade of experience to call upon, Shevelyov recalls when cybersecurity's ability to impact business was not as acute. He says, "Ten years ago, or maybe going back twenty plus years when I started in technology consulting at Deloitte, IT security was seen as an offshoot of technology. It was a nuisance for the business. But now the discipline

has evolved so much that it is just a matter of good business practice to have a complete cybersecurity program. We are no longer an offshoot of IT. We are integral to the success of the business."

He continues, "Cybersecurity used to be a topic only for industry periodicals, now it is front-page in the Wall Street Journal. The discussion has evolved from the IT conference room to the executive board room."

The industry shift Shevelyov notes has played out within Silicon Valley Bank. He comments, "Our executives and our board are highly engaged. They want to know, 'What are we doing? How do we compare to others? Are we making the right investments of people, process and technology?' We are reporting that information to executives and the board on an on-going basis."

Shevelyov reports that heightened executive awareness is driving cybersecurity's larger role in business strategy. He explains, "I think there is a lot more investment in security-related learning by executives. They are interested in understanding the information we share and often seek out education on their own. They have realized that cybersecurity is something the entire business needs to think about. They understand that we all need to be good security stewards for the ultimate benefit of the organization."

When sharing information with other executives, Shevelyov is careful to consider their perspective. He clarifies, “When speaking with the CEO, I share a quantitative analysis with a qualitative perspective. We talk about our opinions of the assessment but also talk about accurate ranges of hard dollar impact as well.”

Shevelyov’s standing and visibility within the bank has increased over the years, signaling to the entire organization that cybersecurity is a top priority. “Increasingly, I am seen as a peer to other C-level executives at the bank, and that has a big impact on the overall traction and awareness for the security program,” he says.

BUILDING A STRONG RELATIONSHIP WITH THE BOARD THROUGH EDUCATION

Shevelyov describes a “healthy relationship” with the bank’s Board of Directors. His team provides quarterly updates to the audit committee and deeper dive presentations to the whole board as needed. He encourages an open dialogue between his team and the board about industry-wide cybersecurity concerns, and threats. He says, “Typical presentations are only 15-20 minutes but we have also conducted a half-day offsite meeting where we went into all the rules and regulations impacting our program. In the meeting, we examined industry threats and facilitated a

more robust discussion.”

More standard presentations to the Board focus on near and long-term security strategy. He continues, “We discuss how we are engaging across the organization and where we are headed over the next few years. We have a first horizon, highlighting where we are today and a second horizon, which projects two or three years out. We also report on a third horizon that is a little more speculative and considers cutting-edge technologies that could impact our world in the future.”

With years of experience in the role of CSO at Silicon Valley Bank, Shevelyov shares a veteran perspective on Board meetings and communicating with executives. He jokes that new CISOs preparing for their first Board meeting should, “fundamentally know thyself and know thy enemy and you will survive 100 board meetings. That of course is tongue and cheek, but you really need to have a technical grasp of the field and be able to analogize, empathize and translate security’s impact on the business. Remember the security team is here to serve the success of the business, so you need to have a multi-disciplinary perspective on the issues. Explain how cybersecurity issues impact the business’ mission and critical objectives. We need to evolve from a technology discussion to a business and operational risk conversation. This is business resilience for the 21st century.”

BUILDING A TEAM WITH DIVERSE SKILLS

Shevelyov’s team recognizes that change is a constant in cybersecurity. His organization is structured to ensure changes in risk and threats are addressed with appropriate people, processes and technology. He explains, “I have a traditional cybersecurity operations group and a security engineering team. We also have a Security Analytics and Assurance group which is perpetually measuring and evaluating our programs and identifying where we need to make course corrections.”

Finding and securing the right talent to staff his teams is a priority for Shevelyov. He comments, “According to reports, there were one million unfilled cybersecurity jobs in 2016. I have heard this number will grow to as much as 3.5 million next year. Finding the right talent and the right expertise for our team is a challenge. To address that, we are exploring alternative methods of recruiting. We are widening the net and thinking outside of the box so that we recruit from backgrounds beyond the traditional technology and law enforcement fields.”

He explains, “We are trying to cultivate a network of professionals. We are exploring ways to contact people in other industries and explain how cybersecurity fits into their career paths. Cybersecurity is a broad business problem, so there are many roles that do not require a technology background. For example, governance and information assurance often do not require deep technical expertise. We are doing a lot of measurement in our analytics group, so a classic data scientist can be a good fit for that team.”

Shevelyov is focused on cultivating what he calls “T-shaped professionals.” These are security professionals who may have very deep expertise in a specific technology or area, but also broader knowledge and awareness across the many different aspects of cyber security.

To build out the expertise of his team and to recruit and retain more employees Shevelyov emphasizes education. “Education is essential and fundamental to being a successful professional in the field. We make a very deliberate effort to get employees the right training. We encourage them to network and learn from peers, and add hard skills to their skill set.”

Q&A WITH FRANCOIS LASNIER

SVP IDENTITY PROTECTION & AUTHENTICATION, GEMALTO



As SVP of Gemalto's Identity & Access Management product line, Francois Lasnier maintains a focus on identity protection for the enterprise market. Francois' history with Gemalto spans many years, beginning in product development, moving into marketing and business management across various verticals.

Q: WHAT DIFFERENTIATES GEMALTO?

Gemalto is unique because our solutions are at the heart of modern digital life, from payments and the cloud to big data and the Internet of Things. They encrypt data and authenticate people and things – enabling our clients to deliver secure, innovative services for billions of individuals and devices. Gemalto ensures the authenticity of your banking transactions, safeguards your health records, protects the purchase of your morning cup of coffee, and helps organizations to control risk, manage security, and maintain compliance.

We are involved in many different industries from telecom, banking, government, and enterprise in general. Each vertical has a different set of problems and solutions, which gives us a unique perspective on how we could approach the customers' needs from a non-traditional angle.

Gemalto's "secure the breach" approach is top of mind for customers who have seen over 9 billion records breached globally since 2013, resulting in the loss of millions of dollars. Our differentiated approach enables customers to envision a unique approach to protect their data WHEN they get breached. With Gemalto's encryption, security is attached to the data wherever it resides, and by managing the encryption keys, and controlling user access, you are able to maintain control of your data, prove compliance, and facilitate governance – even in a dense virtual or cloud environment.

Q: WHAT IS GEMALTO'S APPROACH IN THE MARKETSPACE?

Right now, it's a fragmented market with lots of innovation moving at a very fast pace. The reality of cyber-attacks and increased sophistication in these attacks is forcing the industry to innovate and reinvent itself. This dynamic situation makes it confusing and difficult for customers to understand what solutions actually address their challenges and how to judge efficiency of solutions.

To stand out, we've taken the approach is to be crisp on how we define our space and how we believe we can help. While it is difficult to be heard above this crowd, we try to avoid the pitfall that we solve every single problem. We are defining our space and focusing exactly on where to put resources and innovate.

We do this through Gemalto's Enterprise and Cybersecurity Division led by the data protection and identity protection business units.

Our data protection business allows organizations to encrypt data and manage an encryption key. This addresses the specific data security aspect. The identity protection group looks at how to authenticate users and authorize users for accessing applications and resources.

Based on the market shift and evolution of hacks, there is an increase of regulations and compliance, so we are taking a more holistic view of our offerings and moving into identity centric resource protection.

We provide a platform framework that allows customers to protect not only their applications, but also their

critical data. We allow customers to take a centralized approach to protecting data based on policies they've defined. All this visibility is provided through our dashboard.

We aren't trying to sell something that is unrealistic to accomplish, we are instead taking an approach that if you keep layering security you are able to sleep better at night knowing if a breach occurs, you have put a strategy in place to protect your identity and your data.

Q: HOW DO YOU ENSURE YOUR PRODUCTS MEET THE NEEDS OF CUSTOMERS?

We have product owners who focus on managing the product road map. They tend to focus on everything that will be released in the next 6 months, balancing carefully short-term priorities with more strategic long-term initiatives. All the customer requests and feedback coming from the field are typically addressed by our product owners.

In the middle phase are solution owners, who are field-facing and focused on six to eighteen months. They are involved and responsible for user experience and conduct extensive user research. They try to anticipate what we could do to improve the experience of our customers by going into the field to understand how the product is used.

The third phase is run every three years as long range planning. This phase looks ahead at where the market is going and what

WHAT ARE THE MOST IMPORTANT THINGS YOU DISCUSS WITH CISOS?

When I meet with CISOs, CTOs and CIOs, what keeps them awake at night is how they can continue to protect their assets and which assets they need to protect the most. Proper cataloguing and understanding what is most important to the business are vital. Then once they have visibility, they need to know how to protect it in the best manner.

The discussions I had with CISOs a few years ago were about building the biggest wall around the enterprise and trying to defend against any attack. The discussion has changed, because now most CISOs assume there is going to be a breach whether it's internal or external. They ask how they can add layers of security or encryption so if the first wall of protection falls down, they can still protect their critical assets. They are asking how they can maintain visibility over their assets and what users are doing within the company. Compliance plays a big role in this as well.

disruptive moves Gemalto could make. The combination of these three groups gives us a better understanding of how to plan activities and reserve engineering bandwidth. This new platform has had a profound impact on how we operate as an organization.

Q: WHY DO PEOPLE WANT TO WORK AT GEMALTO?

I've been part of Gemalto for 21 years and had the opportunity to move several times, including overseas. We encourage our people to move regionally, geographically and functionally. We are lucky to be a diverse, multi-cultural company. It's something that is unique for Gemalto and continues to motivate and shape our team.

One of the great reasons why I love the company is the level

of freedom and empowerment myself along with our employees have. When people have great ideas, they are empowered to take the initiative to share with leadership.

Q: WHAT IS YOUR FAVORITE PART OF YOUR ROLE AT GEMALTO?

I love to meet customers and listen to their needs, feedback, complaints, and concerns. I like customers who are frank and open minded, and for me that's big part of the role. I don't go into the field just to have strategic discussion with CISOs, I like to hear honest feedback about how we perform. This feedback helps us focus on things like performance execution and product operations, and provides an opportunity for me to improve what we offer to our

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS
WHO ARE LEADING THE WAY
FOR CONFIDENT SECURITY
PROGRAMS



FRED KWONG CISO, DELTA DENTAL PLANS ASSOCIATION

HEADQUARTERS: Chicago, IL

EMPLOYEES: 44

ANNUAL REVENUE: \$23 Million

In all aspects of the security program, I am looking for synergies where a security investment makes sense not just for DDPA, but also for Delta Dental companies. I call this modular security. As I build out our security programs, I want to have every single security component available for our member companies.

- FRED KWONG

MODULAR SECURITY PROTECTS BRAND REPUTATION

Fred Kwong is 18 months into his role as Chief Information Security Officer for Delta Dental Plans Association (DDPA). He is the not-for-profit's first CISO and is tasked with managing security operations for the association, protecting the Delta Dental brand identity and driving security standards across DDPA's national network of 39 independent companies.

With independent companies functioning under the Delta Dental brand, sharing security standards and best practices is a critical part of reputation management. One of Kwong's main priorities at DDPA is to build out security programs that may be replicated and leveraged by the Delta Dental companies at low costs, and with limited resource investment.

"In all aspects of the security program, I am looking for synergies where a security investment makes sense not just for DDPA, but also for Delta Dental companies. I call this modular security. As I build out our security programs, I want to have every single security component available for our member companies. They need to be able to take advantage of our programs and implement systems without any heavy lifting in terms of technical expertise or financial burden. To do this, I am working with vendors to provide synergistic mindshare across the system."

Kwong says, "For example, we needed a vulnerability management program for the association. While we implemented this first at DDPA, we also completed a

THE CYBERSECURITY SKILLS GAP

“I have a small team at DDPA, there are only two of us dedicated to security within the association. The rest of my team is located at our MSSP. My security model is all about modular security. Our programs need to be able to support Delta Dental across the nation. That cannot be done if we rely on a large internal team, because security expertise is in high demand.

There is a real shortage of proper skill sets in security today and it is difficult to hire and retain appropriate skills. With the MSSP model, Delta Dental companies do not need to worry about hiring and retention of security staff. Our MSSP takes on that burden for us.”

template for standing up vulnerability management at Delta Dental companies. We give them everything they need – a pricing model, properly vetted products and access to a MSSP.”

He continues, “Some Delta Dental companies are very small with only four or five employees, others are quite large. For smaller companies, I provide more counsel and advice, whereas with the larger organizations, I partner with their internal staff.”

ALIGNING RISK MANAGEMENT WITH STRATEGIC OBJECTIVES

Kwong’s overall effort at DDPA is focused on ensuring his security program aligns with the association’s strategic pillars.

To align the security program with these pillars, Kwong takes a quantitative approach to risk management via a business impact model. In his first 90 days at the company, he listened to the security challenges and concerns from other executives in the association and at the network of companies, and he performed an internal Gap Analysis. From there, he worked to deploy the risk management strategy.

“With the help of our CFO and General Counsel, I now have a plan to decrease risk to the organization. With this model, we can correlate risk to goals. If these are the areas where we want to decrease risk, then this is what we must prioritize. We have a three-year roadmap with a goal of reducing risk year-over-year.”

As part of the business impact model Kwong and his team focus on the following six risks:

1. External threats against business partners and members

2. External threats against DDPA systems

3. Malicious actions by trusted parties

4. Social engineering against employees

5. Unintentional data loss

6. Ability to react quickly to incident response

He explains, “We correlated these six risks back to our business goals, the strategic pillars. Now, each security project we put in place has a correlation to the amount of risk we are mitigating and how that impacts the business. We define the success of the program by the decrease in severity or likelihood that an incident will occur in the future.”

Kwong notes there will always be inherent risk in doing business. He says, “CISOs struggle with risk management. It might be because we do not all come naturally to risk. Many of us have compliance or technical backgrounds instead. The other problem is that the risk models available to us are not very good. Most are flawed in the ways that they account for risk, some are missing threat intelligence or they are not taking proper account of other areas.”

He believes risk management is an evolving area for CISOs. “I was on a CISO panel with three other CISOs last year to talk about risk management. Each one of us had a different methodology in terms of reporting risk. My model was the most quantitative in nature, other models were spotlight models at a high level. We were able to agree that it almost does not matter what model you use, as long as the Board understands it and as long as it provides the information the Board desires to know. I think that as Boards become smarter about security they are going to want to understand risk in a more quantifiable way.”

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446



FEATS OF STRENGTH MAGAZINE

CYBERSECURITY SKILLS GAP

FINDING TALENT THAT STANDS OUT

DECEMBER 2017

K logix

WWW.KLOGIXSECURITY.COM
888.731.2314