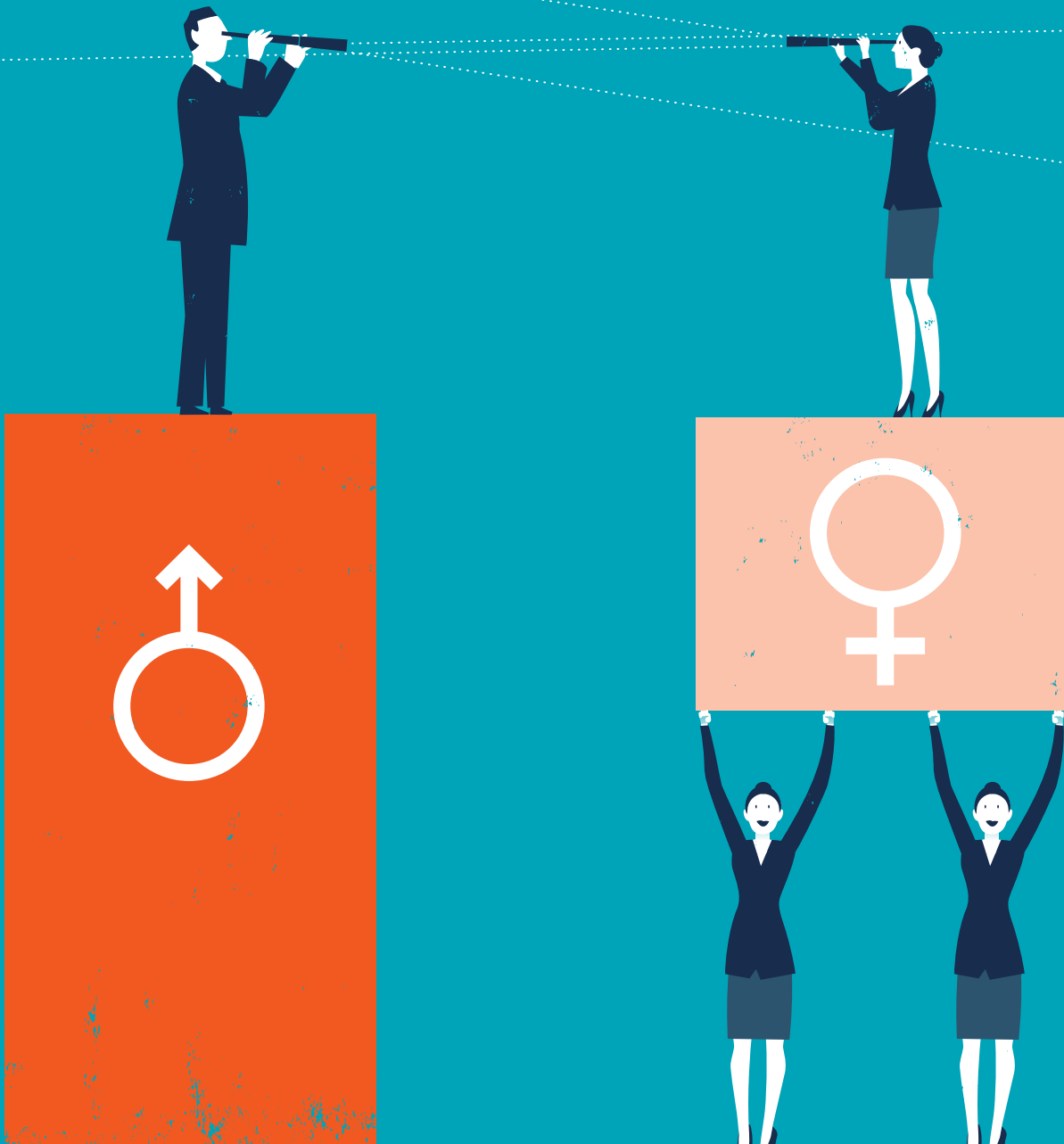


FEATS OF STRENGTH



THE MOTHER OF ISO PAVING THE WAY

PAGE 6
PAGE 10

PROFILES IN CONFIDENCE

Theresa Payton, White House
Hussein Syed, Barnabas Health
Sue Schade, UMHHC
Darrell Keeling, Land's End
Ann Delenela, ERCOT
Howard Whyte, NASA
Michael Bedford, PCG
Michele Thomas, USDA
Ernesto Digiambattista, Sentinel

PAGE 4
PAGE 8
PAGE 14
PAGE 18
PAGE 20
PAGE 22
PAGE 26
PAGE 28
PAGE 30

MAKING SENSE OF A CROWDED ENDPOINT SECURITY MARKET

PAGE 16

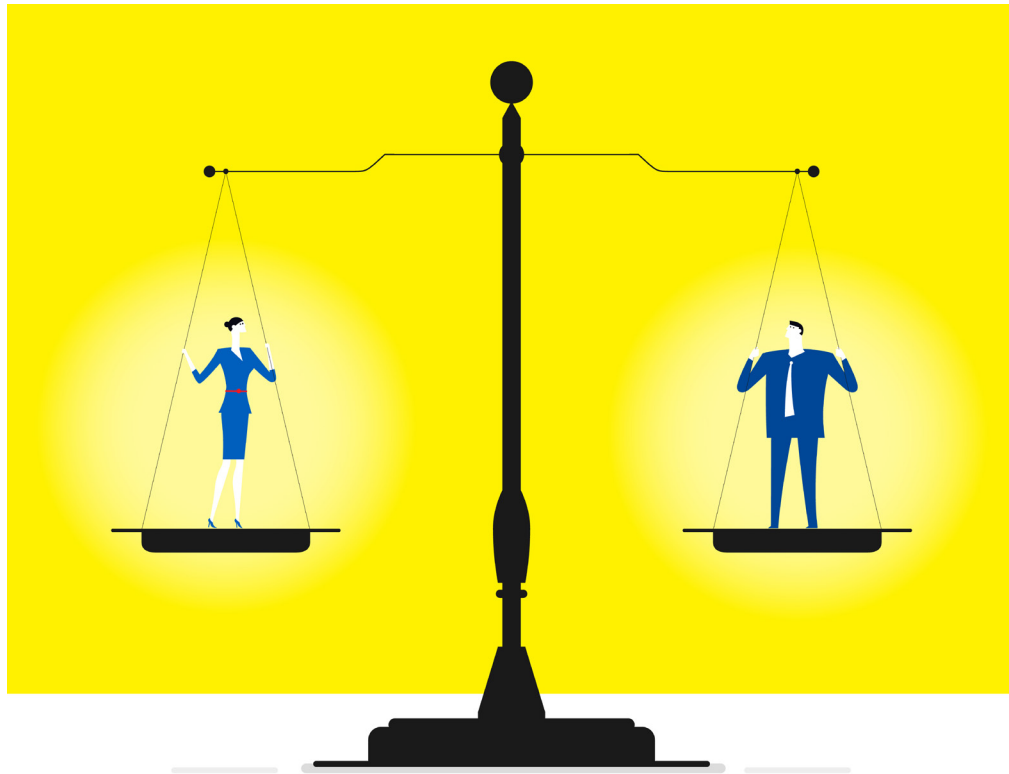
WOMEN IN SECURITY

SEPTEMBER 2015

WWW.KLOGIXSECURITY.COM 888.731.2314

K logix

Earning the right to be confident
in Information Security



Putting Aside Assumptions to Recognize and Nurture Talent

It is summer in New England and my two daughters and son love to enjoy these dog days at a local beach. Recently, while digging for clams at low tide, my girls noticed a fearless flyer doing aerial stunts over the ocean. They were amazed by the turns and loops and asked, “Dad how does he do that?” I answered, “How do you know the pilot is a man?” Without missing a beat, the girls both responded in unrehearsed unison that all pilots are men. People make gender-based assumptions every day, and it is obvious these assumptions start at a very young age.

My daughters’ comments on the beach made me realize the limits they will put on themselves if they become part of another generation of girls lost in the gender gap. Will they bow out of opportunities because of assumptions? This is exactly what has happened in Information Technology, and more specifically in Information Security, and may be a big reason why we lack security

talent in the marketplace today.

In this issue of Feats of Strength we dive into the topic of both women and minorities in Information Security. With our industry facing nearly -10% under-employment, we examine how to put aside our assumptions about what a security officer should look like. We explore how to widen the pool of candidates, and put aside our assumptions of who is qualified to do the job.

Our Industry Is Growing Faster Than Almost Any Other

A recent survey from Robert Half Technologies found that 85% of CIOs were seeking to expand their security teams with staff that possess a diverse skillset, technical certifications, and the soft skills required for communicating and collaborating with other business units. US News & World Report has listed cyber security as one of its ‘Hot College Majors’ because of high demand in the field, yet only 200 universities are accredited to teach cyber security.

An Early Introduction

Many of the Information Security leaders we have spoken with and profiled, believe we need to introduce more of the digital natives generation (both male and female) to the Information Security industry. Just like educating our own organizations, we need to start by making sure young people are security aware - which is important to their own safety, but also will make them smarter consumers and employees in the future. We need young people to be excited about science, technology, and math, but we also need them to develop the skills necessary to be good investigators, communicators, and collaborators. Young people who are naturally talented at understanding and finding risk should take advantage of this skill and turn it into a security-related career. Several of the leaders we profiled in this

issue believe that as an industry we need to commit to partnering with high schools, Boys and Girls Clubs, and other organizations to develop programs that nurture children's interest in technology and problem solving.

Building a Diverse and Inclusive Workforce

While training at the earliest levels matters, there is much more we could do to ensure we meet demands for highly skilled security professionals. As an industry, we should make opportunities available to the largest possible talent pool. We need to look no further than trade show floors to see that our industry is too homogenous. Plainly, we should do more to involve minorities and women in our ranks. While we feature many strong women in this issue of the magazine, it should be noted that women make up only 28% of the IT workforce, and just 11% in information security. That compares to almost 50% of the total workforce. Minorities are also under represented, with just 6.4% of security professionals identifying as Hispanics and 8.3% as African American, according to the International Consortium of Minority Cyber Security Professionals (ICMSP), an industry organization focused on expanding minority participation in the security industry.

In fact, like IT and Information Security, women are underrepresented in the airline industry, accounting for just 5.4% of all airline pilots. So my daughters' assumption that the pilot was a man was probably correct. The important thing is they do not let that assumption, based in today's realities, influence their goals. By the time my daughters are ready to start their careers, my hope is that assumptions will not become limitations, but instead be opportunities to flourish.



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

WAYS to expand the CYBERSECURITY talent pool

1 WATCH CODE: DEBUGGING THE GENDER GAP

This excellent documentary examines why so few women enter the IT industry, and even fewer of them remain after ten years. Many companies are hosting viewing parties.

2 HIRE INTERNS

Work with local colleges and universities to bring college students in to be mentored by your technical staff.

3 OUT-OF-THE-BOX HIRING

Look to non-traditional majors and resumes to fill non-technical roles such as awareness trainers and project managers and give those people opportunities to gain technical skills.

PROFILES IN CONFIDENCE

WOMEN WHO ARE LEADING THE WAY
FOR CONFIDENT SECURITY PROGRAMS



THERESA PAYTON
FORMER CIO
WHITE HOUSE
2006-2008, BUSH ADMINISTRATION

“We are doing security wrong, and also doing it a disservice, because security should be an enabler through enhancing customer experience and revenue”

As the former CIO of the White House and with many years of experience, Theresa Payton is a recognized name in security, and a truly dynamic figure whose intelligence, passion, and drive permeate to all of those around her. With a hunger for identifying key cyber security solutions, Theresa has evolved into one of the most respected experts, and she embodies a true evangelist with her forward-thinking perspective.

Payton shares her thoughts on women in security, as well as key considerations for continuing to push the industry forward.

GEEK IS CHIC

Payton has only a small circle of close female friends who work on the technical side of security. “It is fabulous that more women are on the product, sales, and marketing side, but I would like to see more women in the analytical, technical, and ethical hacker side.” This lack of female presence is in part due to the image problem security faces.

Payton mentions a Girl Scouts of America study that discusses how women have historically chosen careers where they have a connection and direct correlation to helping people. “Security has not done a good job of showing how cool it is to join the ‘good fight’ and protect friends, family, and corporations from the bad guys,” says Payton. The industry has failed in demonstrating this exciting side of security, and the obvious correlation to helping

people is often lost. When Payton is evangelizing and recruiting people to join the industry, especially women, she tells them 'it's chic to be geek', and promotes the image of having a direct impact on customers. She believes that this will influence more women to seek out security-related professions and move the needle on elevating the attraction to security.

THE POWER OF MENTORSHIPS

Payton's mentor always told her that when you are the first female manager or first female on a project, be aware that people might be uncomfortable because it may be new to them. Payton says, "If you can disarm and charm them by asking if anything you are doing makes them uncomfortable, then you open up an honest dialogue that helps avoid issues later on." She emphasizes the importance of striving for open, authentic, and constructive dialogue in order to achieve collaborative success.

Payton believes that all women should seek out a mentor and do so with a clear notion of purpose and dedication. "You get out of it what you put into it and you should work hard to show your mentor that you are willing to put in a lot of effort. Make sure your mentor understands that they will see a return on their investment and time. If you do this, is it hard for someone to turn you down, and you are going to see a lot out of that relationship," says Payton.

SECURITY AS A BUSINESS STRATEGY

In many organizations, executives view security as a compliance and risk exercise. "We are doing security wrong, and also doing it a

disservice, because security should be an enabler through enhancing customer experience and revenue," she comments. The vital piece of strategy that many organizations lack is the impression that they are a technology company first. For example, banks are technology companies that do banking for a living and retail companies are technology companies that sell clothing and merchandise for a living.

While there is no one size fits all approach, Payton believes that the CISO and CIO should not be competing roles. "My hope is that over time, if you have hired the right CIO and CISO, then they do not have to report up to different places in the organization. They should not be competing roles, they should be complimentary," she says. This alignment, paired with a business-focused value strategy, is a recipe for success. By enabling the Board Room to understand that customer confidence and revenue are key competencies of security, many challenges of gaining budget and resources will dissolve.

For a CISO or security leader to attain this level of maturity, Payton recommends starting with great online resources and watching videos of how others solved complex security problems, such as TedTalks which present in terms of business value. She also believes in reading business periodicals that anyone on the Board would read and noting the words they use so you may speak their language and provide solutions that they easily understand. Payton says, "It is important to learn from luminaries in the industry who have cracked the code on how to speak 'tech and exec' at the same time, so when they hear from you, you receive the funding and resources you need."

Security AWARENESS CULTURE

Since 95% of breaches are due to human error and 78% by tricking the user, Payton recognizes that many awareness programs are proving ineffective.

"What companies need to do is take a step back and ask themselves which assets their employees, vendors, and contractors are touching. They need to ask if it would prove catastrophic if they made a mistake and 'bad guys' got in. It is important to recognize which one to four assets fall into this category and then focus an education and awareness program around these," says Payton. An example she provided was a healthcare organization that switched up training and focused on how employees could protect their elderly parent from internet fraudsters and children from reputation risk and internet predators. By tying corporate security goals back to lessons they were teaching, they experienced a large improvement in their post-training social engineering exercises and had better retention.

THE MOTHER OF ISO 27000



HOW DEBORAH HURLEY'S SEMINAL REPORT ON THE SECURITY OF INFORMATION SYSTEMS BECAME THE BASIS FOR ISO 27000 INTERNATIONAL STANDARDS

Deborah Hurley is Principal of a consulting firm, which she founded in 1996, and a Fellow of the Institute for Quantitative Social Science at Harvard University.

From 1988 to 1996, Hurley was an official of the Organization for Economic Cooperation and Development (OECD), an international organization based in Paris, France. At the OECD, she was responsible for identifying emerging information and communication technology issues. Between 1989 and 1992, Hurley wrote the seminal report on security of information systems, followed by an international accord on the subject, breaking new ground on this burgeoning, important issue, which had not yet received much attention.

"I was really interested in doing things globally, because technology is global," she says. The international accord was adopted by governments around the world in 1992 and also became the basis for the ISO 27000 international standards.

Looking Back 25 Years

"The thing that is most striking to me is that 25 years ago we were identifying what needed to be done to provide better security of information systems, something that we are still largely failing at today," she says. Hurley believes the United States failed to instill basic values and laws around the security of information systems when computerization was emerging. In the early 1970's, the U.S. led the way in modern day protection of personal data and privacy. The U.S. adopted the 1974 Privacy Act in response to the growth in computerization. The U.S. encouraged other countries to adopt similar laws to protect personal data. However, during the mid-1980s, when most countries continued to adopt, amend and mature privacy legislation, the U.S. became an outlier by consciously pulling away from these types of regulations.

The 1980s also saw concerns around U.S. competitiveness, amid continuing globalization. The computer industry was one field in which the U.S. had a clear lead. "In this era, the U.S. worried about falling behind. Computing was a clear

bright spot, creating a mindset towards information technology to penetrate every market, be everywhere, and sell everything, all with a hands-off, no regulations approach," she explains.

As far as global dominance in information industries, this strategy was successful. But, the "no regulations" approach came with a number of costs. "There was no incentive structure to provide better computer security. During that time, many products out there were insecure, had vulnerabilities, and were poorly designed. If the product was substandard, the companies were not penalized," she comments.

The U.S. failed to impart fundamental security policies within businesses when computers were developing, a mindset that continues to exist. Today, business executives do not fully recognize the value of security, preventing most CISOs from gaining proper alignment and resources within their organizations.

"The thing that is most striking to me is that 25 years ago we were identifying what needed to be done to provide better security of information systems, something that we are still largely failing at today"

Gaining Momentum for Global Standards

Recently, Hurley spoke at an event about one of the newer ISO Standards – ISO 27018. This standard provides guidance aimed at ensuring Cloud Service Providers offer suitable information security controls to protect privacy of their customers' clients by securing PII (Personally Identifiable Information) entrusted to them.

Even though this standard is voluntary, it is expected to become the benchmark for Cloud Service Providers moving forward. ISO 27018 provides a uniform approach across all industries worldwide. "The standard provides mechanisms for compliance and audit, thus decreasing or removing the need for negotiations over privacy and security provisions," she says.

One of the most compelling aspects of this standard is its adoption by U.S. organizations. "This standard is exciting for the U.S. because companies may have a competitive advantage if they are ISO 27018 compliant," Hurley comments. Greater U.S. adoption of ISO 27018 could mean a new era of aligning with global standards and implementing stronger privacy and security policies.

Q&A WITH DR. HUGH THOMPSON

CTO & SVP, BLUE COAT

Dr. Hugh Thompson is the CTO and SVP of Blue Coat. He has spent his career in the information security space systems and has co-authored three books on the topic. For over five years, he has also been the Program Committee Chairman for the RSA Conference.

Kevin West, CEO of K logix, interviewed Hugh to gain the mindshare of this world-renowned expert on IT security.

West: Based on our findings from interviewing CISOs, 76% of CISOs meet with the Board, but only 29% are involved in two-way discussions about business strategy.

What are your thoughts on the current relationship between CISOs and the Board?

Thompson: One of the biggest things I see CISOs struggle with is being able to translate what they do to protect the enterprise into the language of business that the executive team and board can quickly relate to. To be invited

for a security professional to be successful?

Thompson: We are seeing a significant skills shortage in security. One of the biggest challenges is that when kids in high school and college are trying to plan out a path for themselves, Information Security is not one of the careers that typically comes up on a list of jobs in IT or business. Cyber security is a fascinating career for people who love to solve problems, are creative, and have

open minds. These are the types of people who do very well in the security space and these are the types of folks we need to attract into the profession of IT security.

There are also people who are naturally talented around finding weaknesses in

systems. We need to get to them early enough to show them they can take their skills and interest in computing and create an amazing career path in an exciting and fast-growth space.

West: Why is there a lack of women and minorities in IT? How can the industry change this?

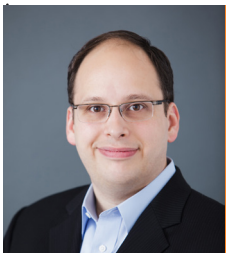
Thompson: The great thing about IT is that there are so many different paths people can take. It is an industry where creative thinking matters and can make a real difference. The bad guys are made up of an incredibly diverse, talented group of people. To counter their efforts and stay a step ahead, enterprises and governments need a people from all disciplines—whether they are computer scientists, linguists, mathematicians, or statisticians. Attackers think beyond traditional pathways or vulnerabilities, so we need an eclectic group of talented people working on the solutions side. There are terrific examples of incredibly talented woman and minorities in the security field but we don't have anywhere near the diversity that we need to confront the challenges ahead of us.

West: What are your top priorities?

Thompson: Blue Coat is one of the most trusted brands in enterprise security. The most trusted brands in the world trust us to protect them from even the most sophisticated threats while taking full advantage of the cloud mobility and new services on the internet. This is a big mission and we have invested an incredible amount of resources in growing our portfolio to protect against even the most sophisticated attacks, including building out a global cloud infrastructure. It is not only a large business opportunity for Blue Coat, but it is also our responsibility to bring those kinds of capabilities into our customer base.

West: At your recent partner conference in Chicago, it was clear that Blue Coat listens to its customers and respects the investments they have made in various solutions. Does Blue Coat seek out technology partners to ensure customers can leverage their existing investments?

Thompson: Blue Coat is a foundational part of the IT security architecture for about 80% of the Fortune 500. These companies have the resources to evaluate, procure, and deploy the best technologies the marketplace has to offer. We see it as our responsibility to provide an open architecture and be a leader in integrating with the broader technology ecosystem. This is fundamentally ingrained into our company culture. I like to tell our customers that when you bet on us, you are not just betting on Blue Coat, you are betting on the entire security ecosystem. New technologies and whole solution areas may emerge in security, but our customers can be confident that they will be able to integrate well with us. This is an area we feel very passionate about.



“The ability to get business executives’ mindset around the concept that failure and recovery are competencies, would be a huge step forward.”

back to the Board Room, not just in emergency situations, but as a partner, CISOs must be great explainers. They must have the ability to take something complex and put it into an analogy that anyone can understand and wrap their head around. As an example, take the processes that enterprises are putting in place today to not only defend against attacks, but to recover from successful attacks. It is similar to the evolution of car safety. If you look at safety features inside of the car, the vast majority are focused on protecting the driver in the event of a crash, like airbags, rollover bars, crumple zones, etc. Failure is built into car safety as a core competency, so when they do fail, they fail well enough to protect you. Because avoidance and recovery are both important, there are also a wide range of features that help you avoid crashes in the first place. The ability to get business executives’ mindset around the concept that failure and recovery are competencies, would be a huge step forward.

West: Do you think there is a lack of talent in security? What skills are most important

READ AN EXTENDED VERSION OF THE INTERVIEW ON [KLOGIXSECURITY.COM/BLOG](https://www.klogixsecurity.com/blog)

PROFILES IN CONFIDENCE

Highlighting information security leaders who are leading the way for confident security programs



HUSSEIN SYED CISO, BARNABAS HEALTH

HEADQUARTERS: WEST ORANGE, NEW JERSEY

NUMBER OF EMPLOYEES: 21,000

ANNUAL REVENUE: \$2.9 BILLION

Hussein Syed is the CISO of Barnabas Health, New Jersey's largest integrated health care delivery system, which provides treatment and services to more than two million patients each year. At Barnabas for over thirteen years, Syed experienced the evolution and maturity of the security program. He noticed the need to institute a dedicated leader responsible for managing the overall security, and played a key role in the discussion to develop this position, along with the "Security Oversight Group". Recently, he took on this role as the first-ever CISO at Barnabas and with a few months under his belt, he possesses a vision for success and desire for continued growth.

THE EVOLUTION OF **SECURITY**

"The need for security has evolved, especially for the healthcare industry, which is one of the largest targets for hackers. As the value of healthcare information steadily increases, the

industry is starting to concentrate on security as more of a business problem," says Syed. With this heavy focus on security, healthcare organizations are able to focus on important aspects of their work such as progressive medicine and preventive care, instead of worrying about being in the news for a breach.

"Security has been reactive and tactical for most companies, even the well-structured ones, because they have not looked at security from a business strategic objective," says Syed. He acknowledges that there are many surveys conducted by reputable organizations which identify cyber security maturity as below the median range for most companies. While Syed recognizes there are organizations that do in fact build strategic planning around the business objectives, most find themselves struggling to bring the problem and potential solutions to the Boardroom-level. "It is important to identify risk and present options

“ MY ADVICE FOR NEW CISOS: DURING THE FIRST MONTH IN YOUR NEW POSITION, LEAVE YOUR OFFICE, TAKE A PEN AND PAD, AND WALK INTO YOUR PEERS’ OFFICES. TALK TO THEM, INTRODUCE YOURSELF, FIND OUT WHAT PROBLEMS THEY HAVE, AND MEET WITH ANYONE IN EXECUTIVE MANAGEMENT. LEARN FROM THESE PEOPLE, TRULY FIND OUT WHAT THE BUSINESS DOES, AND BUILD RELATIONSHIPS WITHIN YOUR ORGANIZATION. THIS BUILDS CREDIBILITY AND LATER BECOMES A KEY IN GETTING THINGS DONE. ”

for mitigating that risk, not just from an IT perspective, but from a business perspective,” he comments. Furthermore, Syed knows that business leaders want to hear how risks were mitigated and see metrics that are easily understood from a business perspective. Syed recognizes that the industry is rapidly approaching a stage where security is at the forefront of business.

A PLAN FOR **ADVANCEMENT**

Syed understands that the Board is no longer waiting for security events to happen. Instead, they proactively seek opportunities to address security, and if something happens they are in a position to react quickly with minimal damage. For Syed, positive visibility with the Board means they recognize that the security department is being hands-on and security positions itself to better articulate and speak the language that management understands.

Syed has leveraged his connections with other security leaders to educate himself and share best practices. He comments, “It is sometimes easier to learn from other security leaders’ experience than try to reinvent the solution. The most important piece of advice I have heard was to learn your business and speak the language of your business. This is what CISOs need to do to survive.” By attending Roundtable Network events hosted by Steven Katz, networking with as many CISOs as he can, and attending many other industry events, he has acquired key knowledge to gain influence, build credibility, and increase recognition.

FUTURE OF THE **CISO**

Some organizations already have the CISO reporting directly to the CEO and Board, a trend Syed believes will only increase as organizations realize the significant value in information security

and as CISOs start to mature and learn the business acumen of working at a higher, executive level. Syed believes the role of the CISO will continue to expand and will ultimately be a crucial part of every Board Room discussion. “The biggest challenge for many CISOs is that they do not have a business education. This is something they will have to understand to help set the overall strategy of the organization and be a part of the bigger picture.” For Syed, he looks forward to continued industry growth, as well as evolving his position to eventually align and report to executive management.

The Right **TEAM**



“There is always a notion that there are not enough people in security, and although we do feel the same way from time to time, we have a high powered team here at Barnabas. Our security team of six is small compared to the 21,000+ employees and 5,200 physicians in the organization, but we have organized ourselves in a manner that produces results. We allow our team to seek professional education whenever we can, and as we grow and the environment becomes more mature with processes, we are looking forward to growing our team even more.”



Heather Fowles

Director of Information Security, Massachusetts Eye and Ear Infirmary

Heather had a non-traditional start in Information Security. During the dot com boom, she saw that companies were hungry to hire people, and even though she did not have an IT degree, she sold herself as a sponge who was going to soak up whatever she was taught. When she moved into security in the 1990's, she worked at larger insurance organizations, and has worked in a number of leadership roles in financial services and healthcare organizations since then.



Susan Schueller

Release Engineer, Best Doctors

Susan has worked in IT for over 30 years. She received her B. S. in Computer Science from UMass Lowell, and returned to receive her Master of Science in IT 29 years later. She is currently working toward her Doctorate of Science in Cybersecurity at Capitol Technology University. She is heavily involved in many groups and organizations and has spoken at numerous events, including outreach to young girls about STEM careers.



Deborah Gelch

Chief Information Officer, Lassell College

Currently Chief Information Officer, Deborah Gelch leads and develops technology strategy for a unique umbrella organization that encompasses Lassell and Pine Manor Colleges, a continuing care retirement community called Lassell Village, and four other partner organizations. Starting with her earliest job selling the first personal computers on the market, she now has over 25 years of IT experience with 14 of these years in the CIO role.



Nadya Bartol

VP of Industry Affairs and Cybersecurity Strategist, Utilities Telecom Council

Nadya is the VP of Industry Affairs and Cybersecurity Strategist at Utilities Telecom Council (UTC), a global trade association for the communications and information technology interests of electric, gas and water utilities, pipeline companies, and other critical infrastructure industries. Nadya bridges the technical to nontechnical divide by translating the complexities of security into business and risk-based terms. She leads UTC cybersecurity initiatives that help utilities address their most pressing cybersecurity needs.



Joyce Brocaglia

Founder, Executive Women's Forum on Information Security, Risk Management, and Privacy

Joyce is the CEO of Alta Associates, the most prominent boutique executive search firm specializing in Cybersecurity. In 2002, Joyce founded the Executive Women's Forum on Information Security, Risk Management, & Privacy (EWF), a trusted community and global network of influential women who empower one another. Leading an executive search firm and a women's organization has provided Brocaglia with a unique set of skills and knowledge of the challenges organizations face in advancing and retaining women executives.

P.A.V.I.N.G

THE WAY

Strong, empowered, and savvy. A few words to describe the remarkable women featured in this article. They are true leaders and their many contributions are moving the needle on encouraging young girls and women to join the industry. We asked them to share their experiences, successes, and challenges.

How did you become interested in Information Security?

Susan: I had two amazing mentors in my career - my uncle who was a master electrician and my 6th grade math and science teacher. They both greatly encouraged me to follow my passions in technology. When I was in high school, computer classes were just starting and they became my favorite classes, prompting me to follow this path into college. I began my Computer Science degree from UMass Lowell in 1981, a few years after the program was founded. The program itself was amazing, the professors treated the women as equals and encouraged us to succeed. I was able to associate myself with other women in the program, some with whom I am still friends today, and gained confidence by forming these tight bonds. Back then, it was amazing for me to be a maverick, and as a woman, to have a non-conventional career.

Nadya: I came to the United States when I was twenty and continued my path as a pianist, getting a Masters degree in piano performance from The New England Conservatory of Music. I went on to get my MBA and Master of Information Systems from Boston University. After a brief job as a programmer, I joined Booz Allen Hamilton where I quickly grew to the management level focusing on building and delivering cybersecurity services.

Deborah: When I was selling the first edition MAC and PC computers, I loved it and knew I wanted to work in technology. I then moved from computer sales to actually working within IT environments. I worked at a law firm in Boston and installed the first local area network, which completely revolutionized the way the firm operated. This

really excited me and confirmed my love for technology, and the impact it has on business.

Heather: I was interested in science and the development of scientific ideas early on and received my Masters in History of Science at Harvard. When the dot com boom came along, I started working in IT support roles. I might not have gone into information security if there had not been a merger at one of my previous organizations. During the merger, the Information Security Officer left, and the company was not prepared to hire externally. I interviewed for the position, and went from being in charge of the help desk and the security administration team, to taking on the role as Information Security Officer. Although it was a steep learning curve, I had support of the organization which helped me succeed.

Why do you think there is a lack of women in security?

Susan: I think there is a lack of awareness for both young girls and women about what it means to work in technology. I speak at conferences and workshops, most recently a Boston University summer camp, focused on high school girls interested in STEM. I share the exciting things I have done in my career to encourage them to pursue their interests. I think that other women in STEM professions should encourage young girls as well. One excellent example is the actress Danica McKellar, who played the Winnie character on the television show "The Wonder Years", and went on to receive a mathematics degree in college. Her book, *Math Doesn't Suck*, teaches the value of confidence for middle school girls interested in math and is a great contribution to growing STEM interests. I also believe that women need to be aware of opportunities for them to go back to school and explore different IT careers, because it is never too late to get into the industry.

Deborah: Having two young girls, I witnessed first-hand that there is not enough emphasis on girls in STEM classes. One of my girls has a higher aptitude for math, yet she was not encouraged by teachers to join the

computer science elective, a group that is predominately male. Even with small increases in women entering the field, biases continue to exist and girls are not socialized into technology-related pursuits.

Heather: When I started in Information Security there were certainly not as many women as there are today, something that might have been influenced by many of first generation information security practitioners having military backgrounds. I also see that the “geek” culture fosters the male-only stereotype, which women might not want to be a part of. This goes for the male-dominated video gaming culture as well.

Joyce: There are many reasons, beginning with young girls not being encouraged to excel in STEM subjects and continuing through conscious and unconscious bias in the hiring process and workplace. Women of all ages are often discouraged from taking technical roles. I was speaking with a young, very bright woman recently who said, “I have an opportunity to go into IT, but people keep telling me that InfoSec is boring, so I’m afraid to go into it.” The reality is, there is nothing further from the truth. Information Security has one of the broadest spectrum of roles and responsibilities. I know many bright women that are highly technical cybersecurity experts as well as those with related roles involving IT Risk, Business Continuity, Governance, Compliance and Privacy.

What can we do to fix this?

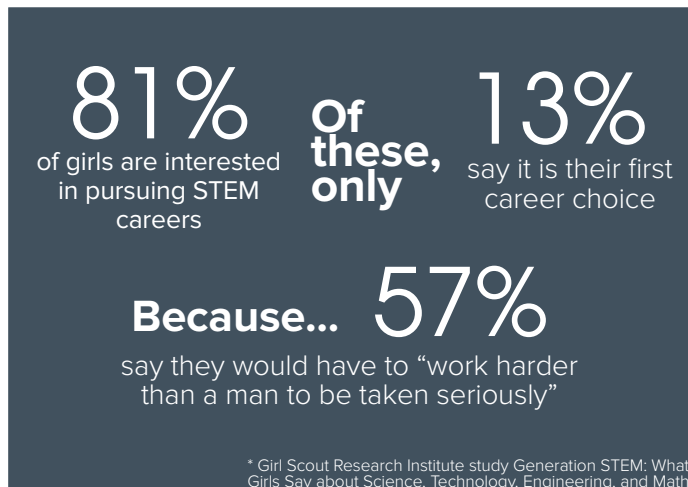
Susan: We need to show that IT can be a rewarding career that involves helping other people. This aspect is very innate to women, and it is important to show that we are not just going in and writing a computer program or answering calls at a help desk, but we are actually making a difference in the lives of our end users. We need women to understand what is behind IT job descriptions because there is such a wide open area to be explored and right now one of the best areas for people to get into.

Nadya: While there are definitely fewer women than men on panels at security conferences, it is probably not biased because it reflects the general demographic of the industry. That said, we need to increase the number of women who are visible at these conferences to inspire more women to participate.

Heather: I think organizations with college intern programs can help spark young women’s interest in

information security and technical disciplines. I have had female interns for the last three years and see that more and more women are showing interest in these programs. Especially in healthcare right now, there are some great opportunities, and I’m happy to see young women stepping up to the challenge.

Joyce: I focus on the 10% of women that are already in the industry by helping companies to develop women leaders and keep them from opting out of senior positions. The EWF Leadership Journey equips women with skills and competencies to lead at senior levels and focuses on developing the self-awareness, personal capacity and resilience necessary to flourish in these critical roles. Companies that are most successful in advancing and retaining women have a commitment from the top to invest in them early on in their careers and drive down the message that sponsoring women is part of every managers responsibility, not something extra they have to do. Women can’t promote themselves, so sponsorship is a key ingredient to achieving gender balance in senior roles.



What about the lack of minorities?

Deborah: My only experience with minorities in security is through hiring for my own department, where I see the major problem as the lack of minority applicants. Minorities with strong STEM skills are not guided into areas of technology and there are statistics to prove this. According to the U.S. Bureau of Labor Statistics, of the American workforce which is 47% female, 16% Hispanic, 12% Black and 12% Asian, just 1% of tech staff are Black and 2% Hispanic.

Joyce: Many companies are just checking the boxes and forming Employee Resource Groups (ERG), but not taking the next steps to truly engage and develop the high potentials in their LGBT, Veterans, Hispanic, or African American communities. We encourage bringing ERG leaders together to build best practices and relationships with each other, as well as assigning executive sponsors who may not be part of that population.

What challenges have you overcome?

Susan: Throughout my career I’ve had a reputation for being helpful to everybody, even difficult people, and I believe I’ve been successful because of this positive attitude. While I have encountered some challenging men, I always look beyond them and remind myself that my main goal is to help advance technology. By showing people that I do not let little things bother me, as well as my long-standing career experience, I have earned

respect and leveraged this to pass the torch to other women.

Nadya: Cybersecurity is a huge challenge for society. Everyone who deals with technology is responsible for cybersecurity but the knowledge resides in the heads of the few. I have the privilege of educating technology practitioners in utilities whose jobs involve security, but they are new to it. Being able to get this knowledge to the right people makes a tremendous impact.

Deborah: There are assumptions that women are not as technically savvy as men. My background and experience is on the technical side, from desktop to network admin roles. Often, I have to over emphasize the technical part of my resume due to this natural assumption that men are innately more technical.

Heather: In high school, I was one of the top students in Chemistry class, which positioned me to take a competitive exam that was only offered to a few students. My teacher hosted a study group for the exam and made a point to tell me that he didn't know if I would want to be in the group based on the fact that only boys would be participating. He said I was doing as well as the boys, but made me feel it would not be appropriate since I would be the only girl, so I did not participate. It wasn't until several years later that I realized and regretted how easily I had let him talk me out of the opportunity.

What advice do you have for other women?

Susan: All organizations should have forums for women to get together and discuss any issues they may have. From my experience, having some sort of internal or networking group helps boost one another. I also think that companies should sponsor women-focused groups by hosting events, providing resources, and encouraging their own employees to join. When working at iRobot, they encouraged me to join the Society of Women Engineers, a national organization over 50 years old. I have been a member since 2005. I am also a member of the Institute of Electrical and Electronics Engineers' Women in Engineering organization. I also encourage women to keep up with technology by taking classes and seminars (not necessarily having to pursue a degree). I have chosen to further my technology education, research and teaching, by pursuing a Doctorate of Science in Cybersecurity, a very crucial technological discipline. There are several women in my cohort, though we are still a minority.

Deborah: My advice for other women is to work smart and take risks, especially when you are younger. Take risks that you aren't sure will work out, those are the risks that can move you ahead quicker. Be confident in saying yes to all opportunities, then figure out how to do it once you are in the job or project. Just go for it! Make sure you have a strong sense of yourself and surround yourself with people who you can count on and they can count on

Jennifer Dennard is a healthcare IT writer and founder of the #HITchicks community, which seeks to grow awareness of gender-related issues in the workplace within [the] healthcare IT industry. This community includes Twitter chats using their hashtag, discussions in their LinkedIn group, and meetups at healthcare events.

While her professional career is in media and marketing, her innate knack for bringing the community together online has resulted in moving the needle on gender diversity awareness among men and women. Many of the #HITchicks chats focus on equality within technology and related [STEM] fields, leadership, work-life balance, government and global policy, health and well-being, and the [wage gap].

Some recent hot topics between group members include gender equality on speaker panels, banning "booth babes" at conferences, and the role parents play in encouraging young girls to pursue interests in STEM.

The #HITchicks community is certainly making waves and has an exciting road ahead for continued growth and impact. Dennard is planning an initiative to highlight non-profits who work with girls interested in STEM; she will also continue to provide inspirational leaders a platform to share their thoughts at group meetups.



Jennifer Dennard
#HITChicks Founder,
Healthcare IT Writer

you. Women should also think gender-neutral and not make the mistake of feeling that it is "us" versus "them". Lastly, women have to help other women – nobody reaches the top without the help and support of others.

Heather: Don't let anyone tell you or make you feel like it is not your club. Don't be overly sensitive to how you are perceived or whether you "belong".

Joyce: Many women think they have to lose their identity as a woman and be a "man with a skirt on". That is not true. Women need to stand in their own power and accentuate their strengths. They need to get comfortable with being uncomfortable, which includes taking risks and speaking up. It also includes actively seeking mentors and sponsors. A mentor is someone who you tell the good, bad, and ugly to, and someone who shares their expertise with you. A sponsor is an influential person in your organization who has your back and can help you with a raise, promotion, and other development opportunities. The more sponsors you have, the better you position yourself in the organization.

Finally, as Madeline Albright says, "There is a special place in hell for women who don't help other women." I think that paying it forward is huge and that you truly reap what you sow. It is important that women "lift as they rise" so that as they mature, they have a legacy of being a leader dedicated to developing the future generation of thought leaders. That is what I am passionate about achieving.

PROFILES IN CONFIDENCE

WOMEN WHO ARE LEADING THE WAY
FOR CONFIDENT SECURITY PROGRAMS



SUE SCHADE

CIO

UNIVERSITY OF MICHIGAN
HOSPITALS AND HEALTH CENTERS

Headquarters: Ann Arbor, MI
Number of Employees: 26,000+
Annual Revenue: \$2.5 Billion

“You need a CISO with a level of domain expertise, but you also need someone who can communicate and have the appropriate presence and credibility at the C-suite level. It is a difficult mix, but I look at these skillsets very closely”

Sue Schade, CIO of The University of Michigan Hospital and Health Centers (UMHHC), is a role model through her many contributions to the industry, and uses her platform to inspire young girls and women. She is a forward-thinking CIO with a heavy focus on elevating and progressing security programs to meet business priorities.

CIO AS A SECURITY ENABLER

“For CIOs who are not security focused, that time has passed,” says Schade. While the CIO at Brigham and Women’s Hospital in the 2000s, Schade viewed a publicly disclosed breach as an opportunity to increase awareness efforts with employees and executives. This breach was an important call to action for leadership to understand the importance of strengthening security.

“Until you get your security program where it needs to be, the CIO will play a greater role in security,” says Schade. When Schade first started as CIO of UMHHC, she spent some of her time on security-related activities, a trend she witnesses among other healthcare CIOs. One of Schade’s priorities is to strengthen the UMHS security program by hiring a health system-level CISO. “To achieve this, I have had to educate upwards with executive leadership and the Board, as well as

raise awareness and answer questions and concerns,” explains Schade. Schade’s goal going forward is to provide an objective perspective that contributes to the fluidity and success of the organization.

Schade understands the changes healthcare organizations need to make to maintain an acute awareness that they are a target from a cybersecurity perspective. These changes may eventually include the CISO reporting into the CEO or the auditor/compliance function and an emphasis on not only technical, but also communication skills. “You need a CISO with a level of domain expertise, but you also need someone who can communicate and have the appropriate presence and credibility at the C-suite level. It is a difficult mix, but I look at these skillsets very closely,” Schade comments.


YES YOU CAN: ENCOURAGING GIRLS TO PURSUE CAREERS IN IT

This is one of the titles on Schade’s blog, Health IT Connect. In much of her blog, she provides encouragement and motivation for young girls to follow their interests in IT. She backs up this encouragement with research and her own first-hand experiences. Schade not only writes about empowering young girls, but she takes action by speaking on the topic at college events, conferences, and female-run groups.

Schade believes there are a number of reasons why so few women are in IT. She cites that 18% of Computer Science undergrads are women, a significant drop from 37% in 1984. “There is some analysis that when the PC was introduced in the early 80’s, it was marketed more towards men. This may account for some of the drop-off,” says Schade. Furthermore, she believes there is a certain amount of stereotyping, and a social order in place, which leads to the lack of encouragement for girls to pursue interests in science, technology, engineering, and mathematics (STEM). “We have to support girl-focused STEM programs and expose them to opportunities by opening up their minds to what they could pursue in this particular field,” she comments.

SUPPORTING WOMEN IN THE WORKFORCE

The impact of evolving gender stereotypes and encouraging young girls is evident, yet creating work environments that empower women poses another challenge. “As leaders, we need to create supportive environments for all employees, while encouraging women in particular,” says Schade. She emphasizes an industry-wide effort in conjunction with organizational initiatives, such as female-run groups like HITChicks, Digital Divas, and Women Rising. Recently, Schade took a risk at an 80% male conference by focusing her keynote speech on unlocking the potential in women. “I told my story, shared the data, described the problem, and talked about a call to action. Afterwards, men came up to me to share stories about their daughters’ interests in STEM or programs their companies had for women,” she comments. This receptiveness aligns with the heightened attention the issue is receiving and confirms the need for both men and women leaders to acknowledge the problem, understand solutions, and talk about it.



“ 18% OF COMPUTER SCIENCE UNDERGRADS ARE WOMEN, A SIGNIFICANT DROP FROM 37% IN 1984 ”

MAKING SENSE OF A CROWDED ENDPOINT SECURITY MARKET

BY RICK GRIMALDI, DIRECTOR OF INFORMATION SECURITY

PART TWO

How K logix helps organizations increase efficacy without impacting productivity or reputation

As outlined in the Spring Feats of Strength magazine, K logix's Project Advisory Service gives organizations a head start on endpoint security projects.

According to a recent Piper Jaffray survey, 78% of CIOs cite endpoint security as a top priority. Their interest in next generation endpoint security is fueled by a move away from traditional anti-virus solutions that are ineffective and disruptive to the enterprise. But, there is so much noise and clutter in the endpoint market that security teams struggle to identify the appropriate solution for their environment. There are more than 50 vendors laying claim to endpoint security and more than 20 are "next-gen" products. It can be difficult for security teams to understand the varied approaches and to differentiate between products. It can also be hard to understand how a solution will fit within the enterprise, and if multiple solutions are required to effectively secure the endpoints. It is a complex, but important and highly-visible decision. Security teams must ensure the solution does not impact worker productivity because that can damage credibility for the product and for the security team.

K logix Project Advisory Service Brings Clarity to the Market

The experienced Information Security Services team at K logix performed a Project Advisory Service on the endpoint security marketplace to help clients evaluate solutions based on business requirements. In the review the team identified a number of market-wide realities.

The market still lacks clear definitions for basic terminology such as "prevent", "detect", "contain", and "visibility", which misleads the public's perception of each solution's capabilities. It is necessary to clarify these terms with each vendor to ensure an accurate review. In short, the market is still emerging, and therefore difficult to navigate, which is why K logix undertook this evaluation process to help clients make better and more

informed decisions. K logix evaluated nine of the leading endpoint security solutions. Those solutions each fall into one of four approaches to endpoint security. Those include:

DATA DETECTION/VISIBILITY AND INCIDENT RESPONSE

– These solutions silently collect and observe countless critical operating system components such as processes, registry changes, file writes, network connections, etc. Once collected, this information is forwarded to a central brain where deep analytics is performed. Differences exist between products as to how data is analyzed and presented to administrators; some solutions provide additional context to data by incorporating threat intelligence while others compare individual host data against other machines within the enterprise to spot anomalies. Products may block some traditional forms of malware, yet as core competencies, typically will not provide direct prevention or blocking capabilities against advanced malware, and instead, are intended to be used as powerful visibility stop-gap tools to reduce the time administrators spend to evaluate indicators of compromise across the organization.

ADVANCED PROTECTION – Solutions falling in this category provide protection through detection and prevention by leveraging unique, vendor-specific malware detection techniques such as machine learning and artificial intelligence. These solutions are typically paired with capabilities for memory and exploit protection. Products differ in the level of protection they offer; some solutions are better suited for a direct replacement to existing signature based AntiVirus and are extremely effective at blocking malware, while others offer complementary protection against advanced exploits.

ISOLATION/SANDBOXING – This approach provides protection by "roping off" certain high risk applications from the underlying operating system. Individual applications, such as web browsers,

78% of CIOs cite endpoint security as a **top priority**

office suites, email clients, or other high-risk programs can be shunted to a separate, self-contained processing area (container) within the computing environment so that if a threat is present, it will not have access

to other critical system processes. These secure areas typically self-destruct when an infection is detected to return the container to a known good state.

WHITELISTING - Whitelisting allows administrators to “lockdown” endpoints so that they will only run approved applications and their supporting dependencies. This type of protection is accomplished by creating an initial system baseline consisting of hashes and application specific fingerprints and comparing all files and programs attempting to run against it. Good and approved applications matching the system baseline will run while unknown ones will be denied the ability to execute. Whitelisting is a strategy to reduce the available attack surface on endpoints.

As standard in the Project Advisory Service, the K logix Information Security Services team formulated a set of business and technical requirements from stakeholders. These requirements were documented and weighted in the K logix Project Advisory Evaluation. The evaluation is not a ranking system; the highest score does not always equal the best solution for the specific environment. Rather, it is a resource to help streamline the product selection process and to prompt conversation amongst stakeholders. For this reason, we have chosen to anonymize the vendor names, so their specific evaluation results were not taken out of context.

For the Endpoint Marketplace Evaluation “General Business Requirements”, including zero impact on worker productivity, protection regardless of network connectivity, and malware protection capabilities were given the greatest weight. Additional business and technical requirements including hardware & software support, ease of administration, reporting capabilities,

vendor maturity, and seven other functional categories were also accounted for in the review.

The results of the Project Advisory Service give clients a comfortable starting point when reviewing endpoint security products for specific business requirements. Companies can glean the following from the service:

- Understand the impact various endpoint security solutions might have on worker productivity when deployed within their environment.
- Identify the leading solutions for specific use cases such as point of sale systems, compliance requirements or real-time visibility with incident response capabilities.
- Identify and engage the right endpoint security solution more quickly, by eliminating solutions that do not meet specific business requirements at the start of the project.
- Utilize the right endpoint security solution to ensure the ability to detect and prevent destructive malware.

The evaluation is updated on a quarterly basis as the market evolves quickly and vendors address feature and functionality requirements.

Contact K logix to review the Endpoint Security Marketplace evaluation & identify the best endpoint security solution for your organization.

DATA DETECTION/ VISIBILITY/ IR	ADVANCED PROTECTION	ISOLATION/ SANDBOXING	WHITELISTING
PRODUCT A PRODUCT B PRODUCT C PRODUCT D	PRODUCT E PRODUCT F	PRODUCT G PRODUCT H	PRODUCT I

PROFILES IN CONFIDENCE

Highlighting information security leaders who are leading the way for confident security programs



DARRELL KEELING CISO, LAND'S END

HEADQUARTERS: DODGEVILLE, WI

ANNUAL REVENUE: \$1.6 BILLION

EMPLOYEES: 6,000

SECURITY AS A COMPETITIVE ADVANTAGE

“Today, security is truly a business enabler and proves to be a competitive advantage,” says Darrell Keeling, the CISO of retailer Land’s End. Keeling believes that CISOs who accept certain risks to do business, show due diligence, and establish thorough processes, are influential leaders who drive security in a way equal to revenue, creating a robust competitive advantage.

When founders build successful organizations, they bear many risks, something that is no different to security. When security teams take a step back and analyze the holistic risks, they are able to focus their energy on conveying business value. Keeling says, “It is important to leverage analytics and data to evaluate risk, something that has traditionally not been done. We can then use the results to help make employees more efficient, and to

improve our practices to make the consumer experience better from a security perspective.”

THE RISE OF SOFT SKILLS

A business-focused security program starts with the CISO, but only sees true success when the entire security team is also enabled. Keeling believes that security talent must possess fundamental soft skills, as much as technical skills, however he recognizes that these soft skills are gradually evolving amongst security professionals. To develop these soft skills, Keeling dedicates himself to opening up new doors and opportunities for his team. “The most important thing for me is to get IT security out within the rest of the business. I give them opportunities to be more engaging to the business and get them out in front of more departments and people. I also challenge them to know the business and be more engaged by breaking down these traditional silos.”

“ I SEE GREAT VALUE IN GETTING MYSELF OUT THERE. OUR RESPONSIBILITY [AS CISOS] IS TO GET OUT THERE AND BE AN ADVOCATE FOR SECURITY. I WANT TO GET SECURITY FURTHER IN THE SPOTLIGHT AND HAVE PEOPLE RECOGNIZE THAT WE ARE DRIVING BUSINESS STRATEGY ”

MOVING BUSINESS STRATEGY FORWARD

SECURITY AWARENESS

Keeling recently introduced himself at a company meeting and asked the security team to stand up, which his team of six did. While they were still standing, he again asked the audience for the security team to stand up. When no one else rose, he asked everyone in the audience to stand. “It takes a team to combat risk and there is an importance on everyone being a part of the security team. Hackers are out there working in teams and in groups by sharing information and working together. We have to do that also,” says Keeling. His goal is to ensure that everyone knows that his door is always open and there is no risk too small to discuss with him. “I want to make a big change in the organization and lower risk by making sure everyone is confident to come forward. I am driving a culture of collaborative conversation.”

ANALYTICS

“There is a huge value in security analytics with regards to efficiencies and the ability to change the overall user experience in what we do today from a security perspective.” Most organizations have not tapped into the

great amount of potential within analytics. Keeling believes that some organizations are taking a “block and tackle” approach and not leveraging the data to help reduce risk and streamline many diverse areas that continue to have high costs.

INCIDENT RESPONSE

According to Keeling, incident response must be baked into the culture, regardless of industry or revenue. He affirms the necessity to review all incidences, evaluate the level of risk, and continuously learn from them. “Our role here [in the retail industry] is to ensure that the risks we are accepting are communicated, acknowledged, and that we have the critical processes in place to support our policies, because that is what our consumers believe we are doing. It is most important to maintain consumer trust.”

CISO SUCCESS

“Ultimately I think any CISO can be successful with any Board as long as they support you and make the risk conversation meaningful to their experience”

120 Day CISO

“There is a lot of talk about the 120 day CISO. I can’t speak about others, but I can speak to my reality. The 120 day CISO is a great start, but it’s vital to look at it from a business perspective,” says Keeling. Keeling just started at the \$1.6 Billion company and is invoking a business-concentrated 120 day strategy to drive significant change. It is important for him to step back and focus on areas where he can be successful by setting the bar through measuring security across the organization and essentially driving change. Accomplishing this mandates a set of principles that rely on building meaningful relationships, bearing substantial influence, and navigating the established company culture.

PROFILES IN CONFIDENCE

WOMEN WHO ARE LEADING THE WAY
FOR CONFIDENT SECURITY PROGRAMS



ANN DELENELA

CSO

Electric Reliability Council of Texas

Headquarters: Taylor, TX

Number of Employees: Approx. 730

“Leadership is not about a title, it is about influence. You can influence without a title, or lead without a title, by being a subject matter expert and collaborator”

Ann Delenela is an expert security strategist with over 25 years of experience covering information technology, information security, and cyber/physical security management. As Chief Security Officer of the Electric Reliability Council of Texas (ERCOT), Delenela developed, implemented, and matured ERCOT’s information and physical security organization to become a nationally recognized center of excellence. ERCOT serves 24 million consumers of electricity for approximately 90% of the state of Texas. ERCOT has four primary responsibilities – system reliability, open access to transmission, retail switching process for customer choice and wholesale market settlement for electricity production, and delivery.

LIKE FATHER, LIKE DAUGHTER

Delenela’s father was a computer scientist who first helped her get comfortable with technology when she was in the 7th grade and he purchased an Apple 2 computer. “When I was growing up, you were hard pressed to have a computer. While the school had a few, I was the go-to for teachers who needed assistance because I had experience with my computer at home,” says Delenela. Though she initially thought she wanted to be a doctor, after interning at a hospital her freshman year of college, Delenela decided she needed to choose a new major. With guidance from her father, she decided to pursue a Computer Science major, where she ended up as one of two girls in the entire program.

OVERCOMING CHALLENGES

“I had some challenges early on in my career, specifically because of my gender and the fact that I looked very young for my age,” says Delenela. She felt she had to prove herself a little more, something that came easy because she possesses an innate sense of determination. In an early internship working with oil reservoir engineers, Delenela went above and beyond, with the net result of her receiving privileged access to the entire computer systems and network. She worked in the data center where she taught herself the necessary skills to build and automate a system for the organization. Due to her hard work and drive for success, she ultimately earned the engineers’ respect and they truly valued her contributions.

Once Delenela began working in the consulting and business world, she noticed that when entering a business meeting with older male colleagues, there was often an automatic assumption that they were the seniors. “I found often that assumptions quickly dissipated once I spoke about the subject at hand and demonstrated knowledge in the area,” says Delenela. She soon gained respect within her field and earned promotions and recognitions throughout her career.

“As women, we have to advocate for ourselves and ask for things that we want,” says Delenela. She also believes that there is a corporate responsibility for the industry to recognize contributions by women in technology. Another important facet of empowering women is to reach further into the next wave of young women, and get them engaged in technology so they do not feel intimidated by it. “It is important for those of us in high-level positions to be role models for the younger generation and demonstrate that it is achievable and not something they are incapable of doing,” says Delenela. Delenela instills these same values in

“
I found often that assumptions quickly dissipated once I spoke about the subject at hand and demonstrated knowledge in the area
”

her twelve-year-old daughter, who she encouraged to participate in Lego Robotics classes, math camp, and computer coding camps. She believes that we are all partners influencing the future generation for both girls and boys.

THE POWER OF INFLUENCE

Delenela comments, “Leadership is not about a title, it is about influence. You can influence without a title or lead without a title by being a subject matter expert and collaborator.” Another key point in empowerment is to push yourself to step into areas where you might not be comfortable. She believes that women in technology need to recognize the importance of thinking beyond their own gender. During meetings, even though Delenela is normally the only female in the room, she solely focuses on the value of her own contributions. “It goes back to knowing yourself and knowing your subject, which empowers you to promote yourself as a subject matter expert,” says Delenela.

BOARD ROOM COLLABORATION

Through continually pushing herself in uncomfortable situations and thinking beyond her own gender, Delenela embodies a forward-thinking leader who has achieved great success. Gaining mindshare with the Board Room demonstrates an accomplishment that Delenela achieved through educating them in a way that accelerates their comfort levels with the language of security. “I regularly present to the Board, where I inform them about information security and physical security topics in a way that speaks the language of enterprise risk. “My goal is to get to the point where they are confident in what we are doing and they understand what the risks are, so we can align to positively influence the direction of our security program,” says Delenela.

PROFILES IN CONFIDENCE

Highlighting information security
leaders who are leading the way
for confident security programs



HOWARD WHYTE CISO, NASA

HEADQUARTERS: WASHINGTON, DC

EMPLOYEES: APPROX. 61,000

“I have regular, direct communication with everyone in the agency. I get out and meet folks, and I run all-hands meetings to explain how each team member fits into the security strategy”

Howard Whyte has performed the CISO role at NASA since October 2014 when he was appointed as “acting”. Many others have held this position since the agency’s first CISO took office a few decades ago. “Most NASA CISOs are in the position for 2-3 years. This is a highly visible and stressful job as we protect the security of the space mission. There is pressure to get it right all of the time, while our adversaries only need to get it right once,” said Whyte.

One way Whyte attempts to diffuse the anxieties of the job is by engaging the entire NASA team in security efforts. “If you don’t have support from the top all of the way down to program support it can be very stressful,” said Whyte. “We have to make sure agency executives, and system admins who have control of the technologies, are clear on their role in protecting our mission. They each have to know how they can help to minimize our attack surface.”

To ensure the agency employees effectively participate in security efforts, Whyte maintains a focus on education and awareness. “I have regular, direct communication with everyone in the agency. I get out and meet folks, and I run all-hands meetings to explain how each team member fits into the security strategy.”

CHALLENGES TO THE ROLE

“Our biggest challenge is that we are a federated environment, that means we have multiple centers with their own authority and resources,” said Whyte. In fact, while Whyte is the NASA CISO and reports to the agency CIO, each of the ten centers across the US have their own CISOs and CIOs. Whyte must work closely with each Center’s CIO and CISO, setting security strategies and standards for the agency. “We have to focus a lot on collaboration. We have to get out in the field

and not be empirical. We need to work with those in charge of running NASA's missions to make sure security objectives are met across the board – whether on the ground or on the space craft.”

A big challenge that Whyte is facing, together with his security professional peers, is moving beyond the tactical security approach of reducing threats to understanding the value of data and how to safeguard it. “NASA has endured a lot of attacks, from all kinds of hacktivists, nation-states and people just looking for notoriety. We have to be concerned with the full spectrum of breach and react based on the risks we face every day,” said Whyte. While threats will always be there, Whyte believes that in the next five years he and the security community will become more focused on data protection, instead of threat detection and prevention. Whyte worries about the cloud eco-system, and he prioritizes understanding who has access to agency data and how they use it. “Data protection requires risk management. You need to know what you have and the value of that data, then conduct the needed assessments to ensure that cost effective measures are in place to protect it. Effective risk management demands all stakeholders (internal and external) work together to tackle risk from an agency-perspective and not just from a security standpoint. You should be aligned with the Agency strategy and mission objectives and work with the IT Security steering committee and business leaders to make sure you allocate security resources to reduce the risk to our assets.”

WHEN A BREACH HAPPENS - Delivering the Bad News

Whyte's image as a Security Ambassador for NASA was of benefit recently when he acted as a liaison between NASA and the Office of Personnel Management (OPM), while they reacted to their own significant breach. Though the breach exposed personal data of NASA employees, it did not impact NASA systems. The NASA security team was not in control of the breached systems. “My role was to be an information conduit, taking updates and information from the OPM security team and delivering the information to NASA's stakeholders.” In addition to making sure NASA's employees were aware of the extent of the breach, and the protections available to them, Whyte is tasked with ensuring the exposed data is not used to socially engineer an attack on his systems. “We really need to be diligent in making sure that countermeasures are in place to protect networks, systems and information,” said Whyte.

“

WE HAVE TO FOCUS A LOT ON COLLABORATION. WE HAVE TO GET OUT IN THE FIELD AND NOT BE EMPIRICAL. WE NEED TO WORK WITH THOSE IN CHARGE OF RUNNING NASA'S MISSIONS TO MAKE SURE SECURITY OBJECTIVES ARE MET ACROSS THE BOARD - WHETHER ON THE GROUND OR ON THE SPACE CRAFT

”

Q&A WITH DANA WOLF

HEAD OF PRODUCTS, OPENDNS

Dana Wolf is the Head of Products for OpenDNS, a leading cloud-delivered network security company that helps some of the world's largest companies keep their users safe online. With over twelve years of experience in information security, Wolf has worked on both the engineering and product side of security organizations. In her current role, Wolf leads the product management, product marketing, user experience, and design teams. She is passionate about building, mentoring, guiding, and empowering the next elite group of leaders in the technology industry.

When did you become interested in security?

My dad was an engineer and tech became a large part of my world from a young age. Growing up, my two sisters and I performed computer backups as part of our regular chores. All three of us were very involved in his work, which sparked my interest in pursuing a career in this industry.

Early in my career, I worked as an engineer during the day and spent my nights and weekends studying for my MBA from Northeastern University. Through balancing business studies

When I was younger, I was the only woman in my Computer Science major in college and the only female engineer at the majority of my previous jobs. Being the only woman for so many years, I had to be strong and argue for what I believed in, something that helped me achieve success.

How can organizations support women and diversity in the workplace?

OpenDNS is incredibly community-driven and works with groups such as

way does not set you up for success. By integrating a diverse group of people with differing personalities and opinions, you are able to come up with the most creative solutions possible. I believe that a melting pot of diverse and interesting people allows them to challenge one another; in some cases conflict produces the best, most creative results.

What advice do you have for other women in security?

My philosophy is to provide mentorship to others, which helped me get very far in my career. I learned important values from many of my mentors. I speak with them one-on-one, share advice, and guide them in their careers.

What is your biggest accomplishment?

I am incredibly proud of the way my team helps design products, and how focused we are on our customers. Our approach is about adding value and solving problems. My job is to make sure we have a crystal clear focus on making products that will continue to earn our customers' business year after year. Across the board, my team is incredibly focused on the needs of the security professionals using our product, so we consistently talk to our customers and learn from them. I am proud that we design alongside our customers and truly become partners with them, ultimately creating a unified culture around what we are delivering.



“Being the only woman for so many years, I had to be strong and argue for what I believed in, something that helped me achieve success.”

with a technical job, I realized that I had a knack for translating between technical people and customers. After many years as an engineer, I branched out to product management, while staying in the security industry. This ultimately led me to my position as Head of Products for OpenDNS.

What are your thoughts on the lack of women in security?

I think things are slowly changing. There are now programs like security-focused summer camps for girls, which try to address the gap between the number of men and women in security.

Girls Who Code, which inspires a younger generation of girls to pursue careers in technology, and Spark, a non-profit that engages underserved 7th and 8th grade children. We also host unofficial “Women of OpenDNS” happy hours to get together after work and connect.

It is important to have a diverse group of people in any department of any organization, especially women in engineering. My team is eight women and twelve men, all of whom have a technical background paired with creative skills. Having a group of people who think exactly the same

4 Ways to Elevate the CISO Role out of IT

In survey, CISOs Expect to Report Directly to the CEO in the Future

Today more than half of CISOs report to the CIO, and just 15% report to the CEO, with the rest reporting to the COO, or risk-related organizations, according to a K logix survey of 30 CISOs. But when asked about the future of the security organization, 50% of CISOs responded that the role will report into the CEO.

CISOs point out a number of important factors when suggesting the role should move out of the IT department. Some CISOs felt that reporting into the CIO introduced a conflict of interest as security teams assess the risks of specific technology systems and often recommend that technology be used to address the risk. Phil Curran, who reports into the Compliance Department as Chief Information Assurance and Privacy Officer at Cooper University Hospital, is one security leader who believes as much. His group reported into the CIO at first, but found that structure limited their ability to effectively communicate risk to other business units. He states, "The move out of IT was among the biggest factors in the success of our information assurance and privacy program."

Other CSOs believe that the CEO needs to hear directly, and frequently, about risk. Christopher Dunning, CSO at Affinion Group, a marketing services organization says that it makes business sense to run Information Protection or Security outside of the IT department. "Security is not just a technical problem, it is also a business challenge. It cannot be solved with just a technical solution. You have to also take a business-centric approach."

The CISOs in the study reported an average of ten months in their position, and 71% were in the role for the first time. While most CISOs still report into the CIO, it is notable that those in their second, third or fourth CISO role are the ones most likely to report into the CEO today. One reason could be because when CISOs look for their next opportunity they seek CEO-level sponsorship of the security organization. Steve Bartolotta, CISO at Community Health Network of CT., and formerly CISO at Yale New Haven Health System is a good example. He states, "Community Health Network elevated the role of CISO to report directly to the CEO just prior to my coming on board."

With just 15% of CISOs currently reporting into

the CEO, security leaders have some work to do in order to make this prediction a reality. The question remains, what can CISOs do to facilitate the move out of the IT organization to become a more autonomous and business-focused organization with direct access to the CEO and more influence with the Board of Directors? Here are four ways to position security for this change.

EXPLORE - First and foremost security leaders must be explorers. It is imperative to identify all the risks as well as opportunities that exist in the business environment. This requires a plan for exploration and identification. Most CISOs identify risk, but are not looking for opportunities. By identifying opportunities as well as risks, CISOs become business-focused allies to their peers.

EXPLAIN - Both risks and opportunities must be relayed to the business units in an effective, digestible and actionable manner. If risks and opportunities are explained correctly security has the ability to empower business users to make smarter decisions and work more effectively.

INNOVATE - Security leaders seeking to elevate themselves within the organization should also elevate their work beyond operational projects to a more innovative and transformational role. The right technologies can help them work smarter and be more analytical. By leveraging innovative, intelligent technologies security teams can spend less time running systems and more time analyzing performance to identify issues and opportunities.

ADVOCATE - Beyond deputizing employees and customers to be smarter about security, CISOs that report into the CEO will advocate for their teams and projects by explaining how security can impact business objectives.

The relationship between the CISO and CEO is already getting stronger, as CISOs report more one-on-one interaction with the CEO, and more requests for education and insight from the Board. However to become a trusted resource and direct report, CISOs must be perceived as critical to business performance and revenue, requiring some changes in function and focus.

.....
This article was originally published on DarkReading.com
Written by Kevin West, CEO K logix

>50%
of CISOs
report to CIO

only
15%
report to CEO

.....
In survey,
50%
responded that
CISOs will
eventually
**REPORT TO
CEO**

.....
71%
ARE FIRST
TIME CISOs

.....
WITH AN
AVERAGE
10
MONTHS
EXPERIENCE

PROFILES IN CONFIDENCE

Highlighting information security
leaders who are leading the way for
confident security programs



MICHAEL BEDFORD CISO, PUBLIC CONSULTING GROUP

HEADQUARTERS: BOSTON, MA

ANNUAL REVENUE: \$35 MILLION

EMPLOYEES: 1,800

A SECURITY LEADER IS A **BUSINESS LEADER FIRST**

While Michael Bedford was still in school he started his own business, an in-home computer repair service. “I learned a lot about being successful in business from that early entrepreneurial effort. I learned the importance of communication, knowing your customer, and providing a good level of service. Ultimately, the business failed, and I learned a lot from that too.” This early business experience has impacted his approach to running the security program at Public Consulting Group (PCG). “A security leader is a business leader first,” he says. “You have to work as part of the business, not outside of it. You have to have meaningful conversations and interactions with your business counterparts.”

CREATING AN OWNERSHIP MENTALITY IS THE BIGGEST **TENET OF SECURITY**

In fact, Bedford believes that communication and collaboration with the company’s business leaders and end users has the greatest impact on the success of the security program. “Most security issues involve people, so you have to make sure everyone is working as risk managers at their

respective levels,” said Bedford. Bedford states that you should know your audience and target your message to them based on their biggest concerns and priorities. “The key is to make sure you get people interested, and make sure they stay invested in security. You want them to understand they are a critical part of the solution. Give folks the right tools and education and they no longer are part of the problem.” This bottom-up and top-down approach is proving successful for PCG, as Michael and his team are not only creating a culture of security awareness, but also ensuring that leaders understand security risks in business decisions.

SHOW WHAT YOU **KNOW**

Part of managing security programs involves understanding that there will be ups and downs. Bedford makes sure the rest of the organization hears from the security team when things are going well, not just during an incident or breach. “You have to be able to tell your story, and champion your team. Make sure everyone knows about security’s successes, and the value of security, so that when a breach occurs it can be put into context of a larger program, with a trend towards better security.” Regular communications from the team also include proactive security education and training for staff on topics that have

“ A SECURITY LEADER IS A BUSINESS LEADER FIRST. YOU HAVE TO WORK AS PART OF THE BUSINESS, NOT OUTSIDE OF IT. YOU HAVE TO HAVE MEANINGFUL CONVERSATIONS AND INTERACTIONS WITH YOUR BUSINESS COUNTERPARTS. ”

meaning for them both professionally and personally.

ACCEPT THAT CHANGE IS INEVITABLE - SECURITY PROGRAMS ARE LIVING, **NOT STATIC**

“In security, we have to make decisions without all of the information we would like to have. But you have to make decisions and be accountable. Sometimes you get it wrong. If a control is costing manpower or efficiency, without measurably improving security, it’s time to change the control,” says Bedford. He looks at each part of the program objectively and is always willing to change tactics to support the end goal and business priorities. “Metrics are key to making smarter decisions and not allowing personal biases to get in the way of doing what is necessary to maximize the effectiveness of your security program.”

BE FLEXIBLE AND ADAPTABLE - **AGILITY IS KEY**

Bedford believes that companies with confident security programs are built on the strength of confident people. These team members are able to adapt to company culture, become change leaders and champion business goals first and foremost. “You will fail as a CISO if you focus on technology when building your team. We can teach technology and how to support it,” says

Bedford. “We need to hire people who are focused on problem solving in cost effective and innovative ways. These are the people who are able to adapt to support evolving business requirements and risks. This is what separates ok security programs from great ones.”



The Limitations of Frameworks – Security Should Not be a Check-Box Approach

Bedford believes in frameworks, but he cautions against blindly following a list of requirements. “Frameworks are important, but security organizations need to make sure their priorities are focused on mitigating risk. If you can’t answer why your organization needs a control, or how it will positively impact the business, then ask yourself why you are doing it? If you were the Board would you support an initiative with no clear business value? Are you checking a box, for the sake of it, or doing effective risk management?”

PROFILES IN CONFIDENCE

WOMEN WHO ARE LEADING THE WAY
FOR CONFIDENT SECURITY PROGRAMS



MICHELE THOMAS

CISO

USDA - ANIMAL & PLANT HEALTH
INSPECTION AGENCY

Headquarters: Riverdale, MD

Agency Size: 8,000+

SMART AND EFFECTIVE REGULATORY RESPONSE DRIVES SECURITY AT THE USDA

Michele Thomas is the CISO for the Animal and Plant Health Inspection Service (APHIS) agency of the USDA. The USDA is the second largest civilian government agency in the United States and APHIS is one of its largest component agencies, with between 8,000 and 10,000 employees. Thomas' responsibilities include risk, compliance, identity management policy and guidance, and cybersecurity operations.

As one might expect, being CISO at a major government agency, most of Thomas' time and attention is spent ensuring that the organization is meeting cybersecurity regulations. For example, according to FISMA regulations, a system must be reaccredited every three years. This means

that Thomas' staff must review systems against hundreds of controls and then submit a report to the Security Control Assessor, a high-ranking official outside of the risk and compliance team. The CIO fulfills that role at APHIS. The Security Control Assessor then submits a request to the Approving Authority to approve the system for production use. While some balk at this level of reporting and auditing, Thomas believes that it is vital to ensuring security controls are met that enhance an organization's cybersecurity posture. If the private sector set policies to mandate these types of checks to the degree the government has, Thomas believes that certain news-making breaches would have been prevented, or in the least, had a smaller impact.

ADAPTING TO CHANGE: NEW CYBERSECURITY BILLS MEAN A CHANGE IN PROCESS

Change is hard for anyone, whether in the public or private sector. In December of 2014, the President of the United States signed several cybersecurity bills into law. As a result, the government essentially redefined how it handled, managed, and administered cybersecurity across the government. Congress legislated that the Department of Homeland Security (DHS) would manage cybersecurity for all federal agencies. This program institutionalizes Continuous Diagnostics and Mitigation (CDM), meaning each agency must continuously monitor their networks and cyber incidents, and report results every 72 hours to DHS. The regulations are recent enough that the USDA has just kicked off its program. As a result Thomas' main challenge for this year is digesting the new requirements and implementing appropriate USDA processes and solutions to meet these requirements. She says, "I'm not worried about it, but it will be a challenge when the fire hose turns on and we have to implement the appropriate changes."

One thing that will not be a challenge for Thomas is budget - at least in this instance. Congress has allocated spending for the CDM project, so it will not affect her overall security budget, which otherwise has seen cuts, just like every other federal agency.

WORKING SMARTLY WITHIN REGULATIONS

Because much of what the USDA does is regulated, Thomas believes that at times, the Agency automatically defaults to unnecessarily strict interpretations of the guidelines. Her job is to help USDA APHIS employees understand how to work efficiently within the standards. For example, there are regulations within the USDA mandating that every mobile device with access to IT systems must be connected to mobile device management software. Recently, an emergency operation involved sending staffers on location with iPads to map a pest infestation. When the group came to Michele's team for device management software, she explained to them that it was not required because they would not be accessing USDA systems from their iPads. The distinction meant the team was able to begin mapping the infestation much more quickly, and at a lower overall cost to the agency.



ADVICE FOR PRIVATE SECTOR CISOs

—

Know What You
Don't Know

For many years, Thomas has worked in the US government, but she previously had a career in the financial services industry. She believes the government is more advanced than the private sector when it comes to prioritizing cybersecurity and creating strong cybersecurity programs. She credits much of this to regulations, which she acknowledges may be a dirty word to some in the private sector. However, she says that between the government's focus on cybersecurity, specifically the recent Cybersecurity bills passed by the White House, the government is more forward-thinking than the private industry, when it comes to response and planning. "In my personal opinion, it doesn't take Target, Sony, or Anthem to show that the private sector lacks a sense of urgency. Our urgency in government agencies on the other hand, has been mandated by law. However, the current situation with the OPM breach illustrates that just having standards, policies, and regulations is insufficient. One must actually follow and implement them! That's exactly what DHS hopes to do with the CDM Program."

Thomas offers the following advice to her private sector peers: "Get the best consultants and experts you can find, and have them tell you what you don't already know. Take a look at your biggest vulnerabilities —make sure you know the hardware and software on your network and the operating systems they run. Make sure you know how you will manage those vulnerabilities and the processes you can put in place to mitigate them. Make sure you have an emergency response plan in place. Many companies do, but just as many do not." And to her government peers, she says "Implement!"

PROFILES IN CONFIDENCE

Highlighting information security
leaders who are leading the way for
confident security programs



ERNESTO DIGIAMBATTISTA CHIEF SECURITY & TECHNOLOGY OFFICER SENTINEL BENEFITS & FINANCIAL GROUP

HEADQUARTERS: WAKEFIELD, MA

ANNUAL REVENUE: UNDISCLOSED

EMPLOYEES: 250

“As a CISO, my duties are to drive the business from a strategy perspective – I must consider what the business wants to accomplish. I have a unique perspective and position where I help drive revenue, manage the company culture, and consider new acquisition opportunities”

CAUTION: PERFORMING MAGIC TODAY

Ernesto DiGiambattista, the CTO & CISO of Sentinel Benefits & Financial Group, wrote “Caution: Performing Magic Today” as one of the weekly whiteboard messages in his office. “People can’t see it, can’t feel it, and can’t touch it, but in my organization, they know security is happening,” he says. DiGiambattista wears three hats, that of the CTO, CISO, and CIO, and he navigates this balance by relying on his robust business-driven background. This important background gives DiGiambattista the tools and business acumen to be a part of the Operating Committee, which meets every two weeks and is comprised of the four partners, CFO, EVP sales, and EVP retirement. This committee fundamentally drives the organization’s inclusive 36-month business strategy, something that DiGiambattista strongly values.

COMING IN WITH A PLAN

DiGiambattista spent his first thirty days at the organization meeting people in business, fine-tuning his understanding of their processes, and creating his own foundation of business awareness. He then spent the next thirty days purposefully building a framework for the future of his program, as well as structuring the vital communication component in order to gain buy-in from executives. “Once I established a baseline, I had the ability to drill down and position a Subject Matter Expert in each area. I consider them my captains, who help improve processes and technologies, while at the same time are meeting with the business leaders to understand their needs and what they want to accomplish.”

The next step for DiGiambattista entailed expanding the organization’s understanding of security, something he still focuses on

through quarterly round table discussions. He meets with twenty different employees at a time, in any department or role, and paints a clear picture of his team's current projects, accomplishments, and goals. What DiGiambattista values most is the feedback he receives on improvements his team can make. These roundtables are clearly working, DiGiambattista receives a 70% response from a quarterly survey that is sent out, which asks employees if they feel the security in the organization has improved, along with performance reliability, and communication on pressing security issues.

SENTINEL UNIVERSITY

"Technology is important, but going above and beyond by doing something outside of your responsibilities is a reflection of how we work business into our security program," says DiGiambattista. Each month, DiGiambattista's team receives training from a different line of business about their department. The training is followed by a comprehensive test, which allows DiGiambattista's team to learn central details about each section of the business. Furthermore, the organization has a Management Program that instills dynamic managerial skills, along with a Leadership Development Program designed for high-performers to work on individual projects that grow their business awareness and expertise. DiGiambattista sees the impact of these programs – his team has been recognized as "business impact players" five out of the last eight quarters and over 67% of them actively participating in these programs.

SPEAKING TO BUSINESS EXECUTIVES

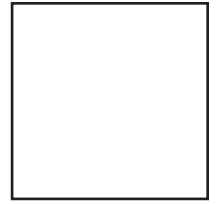
"The language of security is often misunderstood by business-focused executives, so it is important to correlate it back to something that they can understand," says DiGiambattista. He often uses sports or real estate analogies to explain certain components of his program. "I once correlated security back to a remodeling project. If someone has an outdated kitchen, and the building inspector comes on board and says that the regulations for certain parts of the kitchen have changed, the owner must then take the necessary steps to accommodate these new building codes. This is no different to being diligent and transparent with evolving compliance issues within security."

ANALYTICS & DATA

"I place a lot of value on data and analytics, something that was a challenge in the past. In the past 18 months, we have built a metric that helps the organization from a security perspective by understanding what our security risk is. This produces a "magic number" for executives, something that clearly identifies areas of risk within our entire environment that they can then track."

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446



FEATS OF STRENGTH



WOMEN IN SECURITY

SEPTEMBER 2015

K logix

WWW.KLOGIXSECURITY.COM

888.731.2314