

FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE



SEPTEMBER 2016 | INTERNATIONAL INFORMATION SECURITY

WWW.KLOGIXSECURITY.COM

888.731.2314

K logix

Earning the right to be confident
in Information Security

FEATS OF STRENGTH

BY K LOGIX

PROFILES IN CONFIDENCE

- 4 Kathy Hughes, Northwell Health
- 8 Thom Langford, Publicis Group
- 12 Jim Didonato, Baystate Health
- 16 Arthur Ream, Cambridge Health Alliance
- 18 Michael McGovern, Metro Credit Union

FEATURES

- 3 Letter from Kevin West, CEO K logix
- 6 International Cybersecurity Map
- 10 The Age of Privacy Shield & GDPR
- 14 Instilling Security Programs Across the Globe
- 15 Q&A with Ryan Kalember, Proofpoint

LETTER FROM KEVIN WEST

CEO

While watching the Olympics this summer, I could not help but get caught up in the spirit of the games. More important than the medal counts, I witnessed how the perseverance, commitment, passion and sportsmanship of the athletes were a truly motivating force.

On the track was Abbey D'Agostino and Nikki Hamblin. When the unexpected happened – a crash and fall – they did not accept defeat, or place blame. They picked each other up and moved on to finish the race together.



On the court was the US Men's Basketball Team – all of them celebrities and multi-millionaires, most of them already All Stars – they each could have easily decided to take the summer off and rest up for the NBA season. But there they were, playing with foreign rules, adapting to the etiquette of the international game.

In the water was Gevvie Stone, a US rower who failed to make the team in 2008 and finished seventh in 2012. She could have easily retired from rowing, content with having achieved the Olympic experience. Instead, while finishing her medical degree, she rowed the Charles River in Boston, more focused and more determined than ever to medal in Rio. She won the Silver medal this year.

Each Olympian has their own story of overcoming challenges, committing to goals and finding motivation in unexpected places. As information security professionals, we may not be world-class caliber athletes, but we can take the attributes of the Olympic Spirit and apply it to our efforts in business.

Given the global nature of the Olympics, it is fitting that this issue of Feats of Strength focuses on

international concerns for information security programs. Certainly we can apply the lessons of D'Agostino and Hamblin to both domestic and international security programs. In information security, the unexpected is expected. It is how we respond and adapt to those surprises and challenges that ultimately determines the success of our security programs.

The US Men's Basketball team was expected to win the Gold, but let's not overlook the fact they did so playing with a different set of rules than in the

NBA. In our article on GDPR and the Privacy Shield, we talk about adapting security programs to Europe's different requirements. We also feature advice and best practices for applying the principles of existing security programs to international offices, third party outsources and partners. Like the NBA players, as security experts we need to remember we are playing the same game, whether in the US or abroad. We simply have to make

modifications and adjustments for differences in regulations and cultural practices.

And finally, as information security professionals, we all know how Gevvie Stone felt in 2012 – accomplished, but incomplete. In information security there is always more to accomplish. For CISOs at large and international organizations, like Thom Langford of Publicis Group and Kathy Hughes of Northwell Health, it is about learning from new challenges and channeling success in one area into accomplishments elsewhere.

As the excitement of the Olympics fades into a blur of summer memories, I hope we can all keep in mind the spirit of these athletes – their commitment, passion, and perseverance – all attributes that will make our information security programs stronger.



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

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS
WHO ARE LEADING THE WAY
FOR CONFIDENT INFORMATION
SECURITY PROGRAMS



KATHY HUGHES
CISO, NORTHWELL HEALTH

HEADQUARTERS: Great Neck, NY
EMPLOYEES: 61,000
ANNUAL REVENUE: \$7.4 Bliion

AT THE HELM OF EMERGING DEPARTMENTS

Kathy Hughes began her career in manufacturing as a financial analyst, but she quickly transitioned to the computer and technology field, which was in its infancy. A business major with minors in computer information systems and economics in college, she was one of the few people well-versed in computer technology before most knew what computers were. She established centralized computing centers, installed computer networks and implemented distributed computing technologies. More recently, her career path has evolved to information security, where today she is CISO at Northwell Health, a healthcare network based out of New York.

As she developed in her career, she worked for industries as diverse as government contractors, publishing and retail. The one common thread across each job was being consistently tasked with developing programs to respond to changing business demands. "I like the challenge of establishing programs from scratch or bringing them to the next level of maturity by creating efficiencies which bring value and benefit to the organization. I also enjoy

challenging the status quo, motivating staff to think outside the box and empowering them to drive change," said Hughes.

While working at a government contractor, Hughes created and managed the first Information Center, a shared computer center for company employees. From there, she took on positions of increasing responsibility, creating infrastructure services departments at other companies. A position as a outsource service provider for Northwell Health overseeing the Infrastructure teams, led to an opportunity to create and manage Northwell's

“ I like the challenge of establishing programs from scratch or bringing them to the next level of maturity by creating efficiencies which bring value and benefit to the organization. ”

disaster recovery program which gave her exposure to risk management. With the disaster recovery program well-established, the CTO of Northwell Health asked Hughes to take on the role of interim Director of IT Security, a position that lasted three years. Once a new Director of IT Security came on board, Hughes transitioned again, this time to develop a new, formal program for risk management. "In developing the risk management program, I was able to develop strong relationships with the Chief Compliance Officer (CCO) and Chief Internal Audit Officer (CIAO) which established a level of credibility when I transitioned to the CISO position," said Hughes.

BAPTISM BY FIRE

Northwell Health's CIO knew Hughes was the right person for the CISO position. Hughes acknowledges that her background in infrastructure, disaster recovery and business continuity, ability to successfully build programs, and the strength of her relationships with the CCO and CIAO, led to the CIO entrusting her with the increasingly important CISO position.

"I transitioned to CISO just as security was really becoming critical to healthcare organizations. As an industry, we have transitioned from paper to electronic medical records over the past few years, which has made us a prime target for cybercrime. This reality became a baptism by fire for me as well as for other healthcare CISOs."

"Really quickly in my tenure, we had some difficult incidents come up," continued Hughes. "I realized we needed to further enhance our programs. My team and I have worked very hard over the past year and a half to mature our programs, with adjustments to our organization, structure, budget and with senior leadership support. I communicated the program changes to senior executives at Northwell and helped them understand the environment and the threats. Other CISOs have had a bigger struggle than I have in that regard."

Hughes takes a plain language approach to communicating with senior executives. "Most people are very intimidated by security," said Hughes. "They know security is something they have to do, but the return on investment is difficult to calculate so it can be hard to justify. One session at a conference helped me put this into perspective. The speaker's advice was to relay complex security concepts into words that people can relate to. The best way to do that is through stories. Tell them a story of what happened at an organization like our own, what lessons were learned and how some of those lessons can be applied to our environment. When you explain security through stories, people can relate and quickly understand the very real risks

involved. It helps people understand the business impact and get support for our initiatives."

TECHNOLOGY IS CHANGING THE HEALTHCARE INDUSTRY

At Northwell, similar to other healthcare organizations, the focus weighs heavily on creating innovative solutions to improve the delivery of healthcare services. For example, the company's Telestroke service allows doctors who may be offsite, to immediately respond and care for stroke patients. A timely response is especially important when dealing with stroke victims, enabling the Telestroke solution to save lives. Protecting the secure delivery of patient data from the hospital to the remote doctor is an important part of the process.

Northwell built an Innovation Lab, where vendors like Philips, Allscripts or GE may co-develop wireless or mobile tech solutions in a health environment without impacting patient care. "As the security team, we need to make sure we are involved from the beginning, and not viewed as an impediment to fast progress," said Hughes. "We need to enable innovation in a secure environment that is as transparent as possible."


According to Hughes, "While we have state-of-the-art security technologies in place supported by people and process, healthcare as an industry is playing defense and continually preparing for a security incident. We need to make sure we have a good response plan in place, if something does come up. We need to be prepared to respond with a tested process and already have in place alliances with outside entities like law enforcement, PR, media, cybersecurity firms, and forensic firms. We need to have the whole infrastructure of a response plan laid out, regularly tested and ready for different scenarios."

In some regards, Hughes believes the healthcare industry is lagging other industries, primarily due to recent government incentive programs to shift from paper to electronic medical records. As a result, Hughes looks outside of the industry when hiring. "I specifically look to onboard employees from financial services and retail because those industries lead in cybersecurity. They have faced more incidents and have more mature processes in place which can be applied to healthcare. I tell my employees you are protecting data in the same way, but in healthcare the responsibility is even more critical. When it comes to things like medical device and application security, you are literally protecting people's lives."

GLIMPSE INTO: INTERNATIONAL CYBERSECURITY

Here is a glimpse into the International Cybersecurity map we created. For a more detailed version including key concerns, laws, and initiatives in even more countries, please contact us. We are happy to send along the poster sized version.

Crimes in cyberspace will cost the global economy **\$445 billion in 2016** according to an estimate from the World Economic Forum's 2016 Global Risks Report. Threats will increasingly come from China and Russia, however, US companies have more than just cyber threats to be concerned with when it comes to international business. US companies also need to be mindful of foreign regulations and guidelines dictating privacy and data protection, which in places like Europe, are more stringent than in the US. Here are the top data protection and cyber security items to keep in mind in each region.



EUROPE - Privacy Shield

- Privacy Shield is a proposed framework for transatlantic exchanges of personal data for commercial purposes between the European Union and the United States.
- US companies that receive personal information of EU member states must take steps to insure they are in compliance with the new directive.
- US companies also must have processes in place to address privacy complaints in a timely and effective manner.

LATIN AMERICA - Lack of Cybersecurity Plan

- 80% of countries in Latin America lack a cybersecurity strategy or plan to protect critical infrastructure (*The 2016 Cybersecurity Report by Inter-American Development Bank*).
- A large majority of prosecutors in Latin American countries lack the capacity to punish cybercrime.
- American companies with offices and business in Latin America must rely on their own set of standards and security measures to limit incidents.

RUSSIA - Hackers

- It is not just the Democratic National Committee that has to worry about threats from Russia. Russians have proven even more adept than the Chinese in some instances of hacking US systems, including the electrical grid.
- Russian and Ukrainian hackers were responsible for one of the largest hacks in the history of the United States. It cost companies over \$300 million in bank-card fraud from 2010 to 2013.

CHINA - Private Corporate Data

- In January of 2016, a new Chinese law went into effect that requires any Internet or telecomm company in China to provide law enforcement with technical assistance, including decrypting sensitive user data to investigate terrorism.
- More than 40 global firms with business in China are actively fighting another new law. The law creates government security reviews that could threaten the protection of intellectual property. The law also introduces strict requirements to keep data in China that will make it hard for international businesses to conduct standard operations.

JAPAN - Act on the Protection of Personal Information

- Japan has recently updated regulations with the Act on the Protection of Personal Information (APPI). The APPI protects things like biometric codes and codes for goods and services.
- An entity can transfer data outside of Japan only if the country has similar legal requirements to Japan or the company demonstrates that it has met specific privacy requirements.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS
WHO ARE LEADING THE WAY
FOR CONFIDENT INFORMATION
SECURITY PROGRAMS



THOM LANGFORD
CISO, PUBLICIS GROUP

HEADQUARTERS: Paris, France

EMPLOYEES: 77,000

ANNUAL REVENUE: \$10.6 Billion

PRESENTING SECURITY TO THE BOARDROOM

Thom Langford, the CISO of Publicis Group, believes his experience presenting to large audiences at global information security events has helped him better communicate with senior executives at his organization. Whether presenting to a room full of CISSPs, or strategic business executives, he strives to engage in concise, relatable, relevant and engaging content.

"In 2010, I decided to start doing more public speaking. I got engaged in the information security event circuit and I crashed and burned a few times," said Langford. "But I worked hard to hone my presenting skills. I studied the industry, and solicited honest feedback from friends and colleagues." Langford learned the fundamental key for presentations is less is really more. "Instead of presenting a lot of data and facts, focus on simple statements that you can back up with facts," said Langford. "Overtime, I got to the point where I could deliver a presentation without breaking into a sweat."

For Langford, presenting to the Board should not differ from how he presents to conference audiences. "In the Boardroom, you still have a fixed amount of time. You have a set amount of time to deliver information that will be understood and remembered more than 30 minutes later." Langford recommends Slideology and Presentation Zen to those looking to fine-tune their presentation skills. "They helped me boil down what I want to get across into a two minute visually impactful presentation."

OPPORTUNITIES, MENTORS, AND MISSTEPS

Langford started working at Sapient in 2002, after a long career spanning IT and facilities roles in global companies such as PWC. At Sapient in 2008 he identified a gap in the company's internal services, specifically related to information security. "I spoke to the COO and explained what I felt was missing and that I could do the role. He added four or five other components to it and I was tasked with starting the security office on two beans."

"I was learning the business relationships and the politics of the environment. It is my job to make sure the business knows who we are and what we can do for them. We have to market ourselves hard, talk to stake holders and ensure they know how and why they can engage with us. . It is important to have empathy and understand their problems."

Eventually, Sapient brought in an official CISO to work with Langford. The two quickly developed a close working relationship and Langford realized the many learning opportunities he could glean from the new CISO. "We got along really well and I was fortunate to work with him. I learned so much from him. It is always valuable to have someone who has been in the industry and understands your perspective. It is also good to have a mentor to champion you and be in your corner, to validate your decisions and say, 'yes, you are right', even if the company ultimately goes in another direction."

An early failure with a big security project was just as integral to his development. "I tried to overcomplicate a solution and that meant the business was not behind me in the roll out. The project did not get the results it needed and I got a stern talking to from the COO," said Langford. "We ultimately made it work because we simplified, simplified, simplified. Now, whenever we need to engage directly with the business for a security project, we simplify. It works."

Ultimately, the CISO left Sapient for another role and Langford quickly moved into the CISO position. Soon after, Publicis Groupe acquired Sapient and the marketing and advertising giant recognized the strength of Sapient's security program and put Langford in charge of the global company's security effort.

"The transition into Publicis Groupe was straightforward in some ways, but challenging in others. The team was made up of existing Sapient and Publicis people. I had to lean heavily on the team to keep the wheels on, and they were fantastic at responding to requests and getting the job done while I navigated the new corporate structure. As a CISO, you need to be able to trust your team, give them a framework and empower them to make decisions."

"In many ways, we were a new team last year. We were largely the same group of people, but in a whole new environment. We had to focus on delivering the basics. Now our goals are broader. We are establishing consistent policies and working on consolidating our business continuity and disaster recovery programs. A new program is focused on threat intelligence and being proactive about identifying zero day threats. Security awareness

and training is a priority this year as it is critical to everything we do. We are one year in and we have started to establish ourselves as the security team and people are now coming to us with their issues," said Langford.

SECURITY AS A COMPETITIVE ADVANTAGE

Now that Langford's security team has settled within Publicis Groupe, he seeks to positively impact the business through strategic security initiatives. "I am just back from a conference where I delivered a talk on competitive advantage. We can make security a competitive advantage by supporting the business. To do that we have to be flexible and adapt at the same speed the business adapts to changing business decisions."

Langford continued, "Within the advertising and marketing services industry, security can be a competitive advantage. Campaigns take in a lot of sensitive consumer data and it matters how we handle that. We don't want data stolen or lost to competitors. A client told me that it takes them three months to accept code from their suppliers because of multiple security reviews. If we can do security code review before we send it to the client, then we can cut that timeframe down to a single security review. Testing then takes just three or four weeks. For Publicis, that means we can finish and bill projects more quickly and clients can get to market with their campaign more quickly."

HOST UNKNOWN

Described by fellow performers as both a "dinosaur" and the "grand-daddy of information security", Thom Langford is the sole founder of Host Unknown, a Loose collective of three infosec luminaries who take an irreverent look at the cybersecurity industry. You can catch their musical parodies, "CISSP" and "Accepted the Risk" amongst other content on their website, www.hostunknown.tv or on YouTube.

PREPARING FOR BUSINESS WITH EUROPE:

THE AGE OF PRIVACY SHIELD AND GDPR

PART ONE | By Stephanie Hadley

For most of the world, Brexit was the big news out of Europe this Summer. The EU-US Privacy Shield and the European Union's General Data Protection Regulation (GDPR) are garnering just as much attention from those of us in the information security industry. Organizations in the US and Europe are gearing up for the adoption of the two separate, but tangential, programs. Most CISOs agree that the new requirements promote good data protection strategies, and should be a part of any data security effort.

Andy Matthiesen, Vice President of Security at Gen Re, a global provider of reinsurance solutions, said "GDPR is both one of the most ground breaking regulations on data privacy and what we should already be doing from a security perspective." He believes that GDPR is a game changer for security executives and their programs because it will bring greater attention and mindshare to security efforts. The extra attention will bring extra budget in addition to increased scrutiny. He continued, "The potential fines are up to 4% of global revenue (per incident) and a company doesn't even need to have a physical presence in the EU in order to be liable. As a result, international security will get much more attention from Boards and CEOs."

Currently, businesses are assessing their own programs against the standards, identifying gaps and implementing policy and procedural changes to ensure alignment and adherence with the regulations. We break down the most important things

to know about GDPR and the Privacy Shield. K logix Director of Program Management Don Cook gives his advice on how companies can prepare their security programs for the changes in Europe.



Things to know about PRIVACY SHIELD

The Privacy Shield is a proposed framework for transatlantic exchanges of personal data for commercial purposes between the European Union and the United States. It replaces Safe Harbor, which the European Union invalidated in October 2015 when a high court judge ruled that US businesses did not have the appropriate controls in place on US-based servers that stored personal information of members of the EU.

1 US COMPANIES THAT RECEIVE PERSONAL INFORMATION OF EU MEMBERS MUST TAKE STEPS TO ENSURE THEY ARE IN COMPLIANCE WITH PRIVACY SHIELD

2 UNDER THE PRIVACY SHIELD, THE US IS REQUIRED TO BEEF UP ITS MONITORING AND ENFORCEMENT OF US COMPANIES THAT RECEIVE EU MEMBER PERSONAL INFORMATION

3 COMPANIES THAT DO NOT COMPLY WITH THE PRIVACY SHIELD MAY BE SANCTIONED OR EXCLUDED FROM BUSINESS WITH EU MEMBERS

4 INDIVIDUAL EU MEMBERS SHOULD EXPECT QUICK RESPONSE AND REDRESS FROM US COMPANIES. US COMPANIES MUST OUTLINE A MECHANISM TO QUICKLY AND EFFECTIVELY ADDRESS PRIVACY COMPLAINTS OR RISK FACING FTC INVESTIGATION, OR INVESTIGATION BY A PRIVACY SHIELD PANEL

What about the United Kingdom after Brexit?

Brexit brings another challenging layer to the equation, as it is unclear how GDPR and the Privacy Shield would apply to companies holding data in the UK or transferring data out of it to European or US-based businesses. In Data Privacy Monitor, Melinda L. McLellan and Jenna N. Felz, attorneys with BakerHostetler write, “the Privacy Shield agreement may not cover transfers of personal data from the UK. That said, the UK International Commissioner’s Office could explicitly approve Privacy Shield certification as an adequate means of data transfer from the UK to the US, or it could establish a similar mechanism for such transfers, not unlike the US-Swiss Safe Harbor framework that served as an analog to the US-EU Safe Harbor framework. It will take at least two years for the UK to effect its withdrawal from the EU, with many estimating that the complicated negotiations will take much longer. In the interim, the existing EU-US data transfer landscape will continue to include the UK.”

Understanding GDPR

The GDPR replaces an earlier directive with specific regulations to strengthen data protection for individual members of the European Union. Its regulations apply to businesses in the EU and outside of it.

- Multinational companies working across the EU will be required to appoint an independent Data Protection Officer.
- If a data breach occurs, the organization is required to notify the appropriate supervising parties within 72 hours.
- Data Protection Impact Assessments will evaluate how and why companies handle Big Data
- A new “Right to be Forgotten” allows individuals to request erasure of all personal data from a company’s systems.

**A Q&A with our expert,
Director of Program
Management Don Cook**

Please explain the difference between Privacy Shield and GDPR?

Cook: The Privacy Shield is specific to EU member personal data transferred between the US and EU companies. The GDPR is a broader set of regulations governing acceptable use and protection of EU member personal data by any corporation or entity that does business, whether goods or services, with EU members. Essentially, Privacy Shield is specific to data transfer and GDPR casts a bigger and wider net. Any US company doing any business with EU customers must be concerned about both.

Should businesses tackle one requirement before, or over, another?

Cook: There is a nine month grace period for compliance with the Privacy Shield for any business that begins the process by September 30 of this year, so timeliness matters there. While GDPR is bigger and broader, an assessment for Privacy Shield readiness can be a jumping off point for GDPR compliance, which is required by mid-2018.

What are the three most important takeaways for a business that is preparing to comply with GDPR?

Cook: While the GDPR sets specific requirements for things like data breach notifications, and gives customers the ability to request removal of records, the basic steps that companies need to take are standard security best practices. So, the first thing I would say is know your data. Just like for any other data protection strategy a business needs to know what data it has and how it uses that data in order to protect it.

Second, make sure that you conduct regular risk assessments to understand your exposures. Third, prepare and practice an Incident Response Plan to respond to exposures in a timely manner and mitigate losses.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS
WHO ARE LEADING THE WAY
FOR CONFIDENT INFORMATION
SECURITY PROGRAMS



JIM DIDONATO
CISO, BAYSTATE HEALTH

HEADQUARTERS: Springfield, MA

EMPLOYEES: 12,000+

ANNUAL REVENUE: \$2.1 Bliion

FROM HIPAA COMPLIANCE TO THE HITRUST CSF

Jim DiDonato has worked at Baystate Health, a large healthcare organization in Massachusetts, for over twenty five years. During DiDonato's early career, he worked twenty years in internal audit where he audited taxes, financial forms, IT controls, and many other areas. Just prior to 2000, he made the switch to IT where he filled the first security position at Baystate Health. While his first large project consisted of contingency planning and efforts to meet the Y2K challenge, DiDonato quickly transitioned into preparing the company for HIPAA. "HIPAA was really instrumental for me, and everyone in the industry, because it gave us a path or roadmap to create the organization's first comprehensive security program," said DiDonato. He continued, "Of course, that was back when security was based on compliance and not best practices." The industry and DiDonato have changed paths since then.

In 2001, DiDonato was named Information Security Officer at Baystate Health, a position mandated by HIPAA. With that title, his role and responsibilities evolved and again in 2015 when he was promoted to Director & Chief Information Security Officer. He recognized that more could be done

to build out a stronger security posture. "Three years ago, a new CIO came on board and I proposed a change in our security program. I explained that a targeted HIPAA compliance program was not sufficient to cover information security for Baystate. We were both in alignment that we needed to find another security standard to adopt."

"We make a good team," said DiDonato, of his relationship with the CIO. "He supports my requests and he has the support of senior leadership. We have made significant changes in the last three years. Before, there were two of us doing information security for the organization and today there are six of us, with plans to hire two more this Fall. The President and the Board are showing their support with staffing and the resources to acquire the security technology tools we need to build out the program. "

DiDonato and his team have aligned with the HITRUST Common Security Framework (CSF), which is designed specifically for the healthcare industry. The HITRUST Alliance website describes the CSF as a "certifiable framework that provides organizations with a comprehensive, flexible and efficient approach to regulatory compliance and risk management". HITRUST was chosen by DiDonato, because the framework is designed specifically for healthcare providers and payers, is frequently updated for regulatory

changes and has three levels of graduated safeguards depending upon an organization's size and complexity.

"Before we adopted the CSF, we had a security assessment done, so we knew what we needed to accomplish. We set a baseline and now we know that we are gradually elevating up the maturity ladder. The ladder gives us a grading system to make it very clear how we are performing," said DiDonato. For him, the CSF ladder represents a tool to easily communicate information security and risk to other business people. "We can clearly articulate our current level, the steps needed to get to the next level, and how getting to the next rung makes us better prepared and more secure."

DiDonato said that nearly every CISO knows how well prepared or exposed their organization is, but it may be difficult to explain current postures to business people. "Pictures help – the ladder gives a clear indication of where we are, and where we are headed. Our plan for this multi-year effort is to continue to execute on security priorities to move up the ladder."

DiDonato benefits from a very supportive CIO, President, CEO and Board, who are all interested in making continued security improvements. He continues to rely on the CSF within his presentations to senior leadership and the Board. DiDonato said, "They are very receptive to the CSF and they understand the value of aligning with the framework."

DiDonato's meetings with the Board are not just presentations of the CSF. He said, "The Board does not want to see detailed flow charts or diagrams of networks. They need to understand the security program from a business perspective. I build credibility with them by explaining security's impact on the things they care about." They are outcome oriented. For example, DiDonato recently presented on the opportunity security has to become a competitive advantage for the organization.

COLLABORATING ON SECURITY OUTSIDE OF IT

At Baystate Health, interest in security extends down from the Board throughout the entire organization. Senior leaders, including the General Counsel and the CFO, stay engaged with DiDonato. "Our CFO is concerned about the potential financial impact of breaches and incidents, so he purchased cyber insurance as a way to manage that risk. His group has been targeted for wire transfer fraud, but they are an alert group and always investigate first. Our General Counsel is always sharing phishing scams, news of viruses and regulatory alerts with me."

DiDonato believes that working with others outside

of IT is both a big challenge and great opportunity for CISOs. Bringing other business units on board with information security efforts is vital to the program's success. "It is the CISO's responsibility to interact and communicate with leadership and people outside of IT," said DiDonato, whose early career in auditing gave him an understanding of business terminology and objectives. DiDonato acknowledged that for CISOs who grow up in IT, collaborating with other departments might pose bigger challenges.

DiDonato acknowledged the fact that information security is relatively new to many departments, with little to no historical precedent for collaboration. "Most departments have no idea how they can best help us. We need to educate, and reach out to them, to set expectations for our role and how we can work together," said DiDonato.

In the Information Security Office within Baystate, DiDonato puts in a strong effort to ensure his own team understands how meaningful and key their job is to the overall organization. He said, "One way I do that is by removing barriers for them. I show them we are getting the resources to make the program stronger. I depend on the professionals on my team to put together criteria for the technology resources that we need and then I go get it for them."

Baystate Health continues to make investments in information security, enabling DiDonato's team to grow and further advance their skill sets. "When they have the chance to learn new technologies it is exciting for them. When we give them tools and resources to do another level of investigation and analysis of incidents they are intrigued and motivated," said DiDonato.

This on-the-job-growth is an important aspect of DiDonato's team management approach, as he has almost exclusively hired from within. "My approach is to identify true professionals who take their jobs seriously and are dedicated and interested in security. Most of my hires have shown a dedication to security even before they join my team, by sitting for the CISSP certification, for example." However, DiDonato did not rule out looking outside of the organization for his next two hires to bring on more advanced security expertise along with unique skill sets. It will depend upon the skills of each hire.

Regardless of who joins the team and the specific skill set they bring, the group already knows it has a clear focus and strategy for the future – to continue to climb the HITRUST CSF ladder and further evolve the security program for Baystate Health.

Instilling Security Program Adoption around the Globe

Will it Play in Peoria?

By Stephanie Hadley | Content Marketing Manager

The old adage that if it works in Peoria it will work anywhere might be true for the United States, but it does not translate across the globe. Every country has its own unique culture, which extends to the office. It is important for security professionals to keep culture in mind as they roll out security awareness programs and policies across international companies.

Cultural norms influence how people react to security policies, and for the greatest success rates, CISOs must ensure their programs are culturally sensitive. While policies should be standard across the organization, the delivery of the policy must be nuanced country-to-country. For example, business people in Japan rarely use the word “no”. A CISO delivering an update on security policy in that country needs to frame policy in regards to permission and positive behavior, not negatives.

Here are our top five tips for CISOs who want to ensure their security programs are effective around the globe.

- 1 Speak their Language** - Even those international employees who speak English in business meetings still benefit from hearing and reading policy delivered in their native language. Not only is this a professional courtesy, it can improve retention and reduce the risk of confusion. Thom Langford, the CISO of Publicis Group, an organization with more than 100 offices around the Globe, says “If it is important to hear then say it in their native language. Otherwise you always lose something in translation.”
- 2 “When in Rome”** – The old adage rings true in business. Follow the accepted norms of the country you are visiting. For example some countries might expect a security policy to be rolled out in person via a company meeting, while others will need to read the policy first and want time to ask questions. Follow the recommendations of on-site employees in rolling out new programs.
- 3 Staff Locally, Plan Globally** – While a security plan can be administered from headquarters or the CISOs home office, it still makes sense to have a globally distributed team. A security expert in each region establishes a presence for the team, can help reduce language-related confusion and give employees a security partner that can respond more quickly, without time zone challenges.
- 4 Open Channels of Communication** – Even if you can’t be in their office every day, you can still make sure global employees feel you are a partner. Global offices need to know that even if security is not located in the building the team is accessible and interested. Langford says, “Open lines of communication helps the global offices realize that we want to know them, and we want to hear about concerns.” Create open channels of communication by establishing a security hotline, naming Security Ambassadors in each office and facilitating easy reporting of incidents.
- 5 See and Be Seen** – Just like a CISO needs to “walk the halls” and get to know the other executives, they also should visit with the remote offices to put a face to the name and establish a personal relationship whenever possible. Just make sure that when you visit with employees in those offices you are mindful of appropriate greetings, dining etiquette and other social norms.

Q&A WITH RYAN KALEMBER

SVP, CYBERSECURITY STRATEGY, PROOFPOINT

proofpoint



Ryan Kalember is the senior vice president of Cybersecurity Strategy for Proofpoint, a next-generation cybersecurity company. Proofpoint provides cloud-based solutions that protect the way people work today across email, mobile devices and social media channels. Backed by ongoing innovation, Proofpoint enables organizations to protect their users from advanced attacks, protect the information their users create from loss and compliance risks, and respond quickly when incidents occur. More than 50% of the Fortune 100 trust Proofpoint.

Q) WHAT DIFFERENTIATES PROOFPOINT IN THE MARKETSPLACE?

A) Right now there is a hurricane of messaging in the advanced threat and advanced malware product market. In essence, the messages are all variations of each other and many sound similar. I'm happy to say that no startup in 2016 is getting funding to create a mail gateway product, which is our core offering, and no other company protects how people work across all communication platforms.

Our secure mail gateway is not only a security product, but also a fundamental piece of company infrastructure. As advanced threats increase in frequency and sophistication, email has become the number one threat vector. Proofpoint uniquely combines a world class email gateway solution with the industry's leading Targeted Attack Protection technology, catching and stopping cyber threats from malicious links and attachments hours or even days before traditional defenses.

Another differentiator for us is getting our product into the market by having people test it out in their own organizations. More than 50% of the Fortune 100 use our products simply because they work. If you want to do anything correctly in security, you cannot rely on lab tests, PowerPoint presentations, or company messaging to make good technical decisions. You have to test to clear the clutter. You have to test because your environment is unique and the way the threat landscape affects your environment is unique. At the bottom line, there is no substitute to actually seeing how it performs in your environment.

Q) HOW DOES PROOFPOINT HELP CISOS PROTECT THEIR ORGANIZATIONS?

A) We help CISOs at both a technical and strategic level. Let's look at security as a funnel of threats either targeting people or infrastructure, that come in through various vectors such as email, web, social media and mobile. All attacks are fundamentally targeting people and if you pair those with set of attacks on infrastructure side, you have a whole universe of inbound threats you are facing. If these threats get through the gateway they become problems for other layers, and for your security's defense in depth infrastructure to solve. If you go back to the gateway and reduce the funnel by stopping the email from getting through in the first place, you are in a much better position. In terms of broader architecture, the value

of stopping threats at the gateway, where the attack is maximally exposed, allows you have the best chance of stopping it before damage is done.

Q) HOW DOES PROOFPOINT HELP CISOS SPEAK TO THEIR BOARDS?

A) Proofpoint identifies who incoming attacks are targeting, something most Boards want to know about, especially when targets are the C-suite. There are two types of C-suite attacks, first are malware attacks sent to the C-suite over email. The second type of attacks are spoofing, where a fake email appears to be sent from the CEO asking for something such as a wire transfer to be approved by the CFO. CISOs can use our solution to create reports on how the C-suite and Board are being targeted and protected, which turns into a very compelling story.

Q) HOW DOES PROOFPOINT KEEP UP WITH GROWING TRENDS?

A) We are growing over 40% as company and more than 20% of our revenue is reinvested back into R&D, one of the highest rates in the industry—and our threat team is growing even faster. We are trying to stay ahead of threat landscape by giving customers visibility into areas they might not have previously examined. For example, we are seeing the same threat actors now target social media and mobile devices, in particular apps on smartphones. I was recently talking to the CISO of a large university who encountered a professor who studied politically sensitive matters. Even with numerous password changes on his laptop, someone continued to have access to his sensitive emails. The CISO discovered that a malicious app on the professor's iPhone was able to go in and steal his password. It is stories like this that demonstrate the need for us to continue to stay one step ahead.

PROFILES IN **CONFIDENCE**

HIGHLIGHTING PROFESSIONALS
WHO ARE LEADING THE WAY
FOR CONFIDENT INFORMATION
SECURITY PROGRAMS



ARTHUR REAM
CISO, CAMBRIDGE HEALTH ALLIANCE

HEADQUARTERS: Cambridge, MA
EMPLOYEES: 6,375

“ I try to engage the leadership in security and help them understand where our security program is today and where we need it to go. ”

BALANCING MULTIPLE RESPONSIBILITIES

“Most moderate to mid-sized healthcare organizations have yet to commit to a full-time CISO,” said Arthur Ream, the CISO and Director of Applications for Cambridge Health Alliance (CHA), an innovative health system serving more than 140,000 patients in Cambridge, Boston and surrounding communities. “In fact, most managers, not just the CISOs in a healthcare organization of our size, have multiple responsibilities.”

To be clear, Ream is not complaining. “I enjoy the fast-paced nature of the CISO role. In security, we always have to be planning for the future and reacting to the changing landscape. There is always something to learn and, a new issue to prepare for, or address. In my role as Director of Applications, things are a bit more methodical.”

While Ream’s dual position may be the rule and not the exception, in the healthcare industry today it still poses specific challenges. The biggest challenge for Ream’s team is time and resource management as they balance application and information security demands.

"With a non-dedicated staff we are challenged to manage volume. We must be focused to ensure we are safeguarding our patients, our assets and our integrity within our budget and with the resources we have available," said Ream.

Ream addresses this challenge through education and discussion with senior management and the Board. He said, "I try to engage the leadership in security and help them understand where our security program is today and where we need it to go."

As a mid-sized organization, Ream has become more creative and adaptable when creating his security program. Without the resources of a larger healthcare organization, he focuses less on following the details of specific standards. "We use NIST and ISO. We don't report against the frameworks. We work to the intent of the standard," said Ream.

For similar reasons, Ream is holding off on embracing any specific certifications. "We have to constantly weight the value versus the cost, and I am still watching to see exactly where the industry will fall in terms of which certifications are industry standard. The certifications do have value, but often times experience is what matters most. I am a big fan of on the job training."

BUILDING A HEALTHY COMMUNITY

One of Ream's favorite aspects of working at CHA is his dual roles and his team's flexibility. He commented, "We get exposure to so many things, no one is pigeon-holed."

Ream also appreciates the impact CHA has on the community, something that truly motivates him and his team. "Cambridge Health Alliance is the organization of the public health commission for the city of Cambridge and a teaching hospital for Harvard Medical School. Our mission is to improve the healthcare of the community we serve, which includes a large behavioral health population. My teams value and me as the CISO is to wrap appropriate policy and technology around the assets to safeguard our patients and our corporate integrity."

Recently, CHA rolled out a program for e-prescribing controlled substances via Bluetooth. Doctors may now send prescriptions straight to the pharmacy, helping limit prescription fraud and curtail the city's opioid epidemic, but also to help patients. Ream remarked, "Many of our patients might have needed to take time off work to pick up a paper-based prescription before. Now the prescription is waiting

for them at the pharmacy. This type of program has a direct impact on the city and our patient's lives." Ream's team played a key role in ensuring the integrity and security of the applications and systems supporting the program.

PRACTICE AND EDUCATION AT THE EXECUTIVE LEVEL

Beyond working on application specific security efforts like eScripts, Ream and his team regularly work with other senior managers to ensure the organization is doing its best to protect critical assets.

In addition to occasional presentations to the Board, Ream regularly meets with senior leadership. "On a monthly basis I run a committee meeting that oversees the overall security of Cambridge Health Alliance," said Ream. Participants in the committee include the General Counsel, Chief Compliance Officer, Chief Privacy Officer, CIO, HIM Director and Senior Director of Technology. "This groups reviews new applications in our environment, current threats, HIPAA requirements, policy updates and our security plan."

Ream and his team also participate in quarterly breach drills with the CEO, marketing and other senior managers. "All of the drills are based on scenarios that could really happen at Cambridge Health Alliance. A private contractor who knows our environment creates the scenarios for the drill – no one on our team knows about it in advance. For the next several hours we run through the logistics of the breach, practicing policy roll out, communication skills, action and remediation. We receive a report and feedback based on how we performed. As a result of these drills we have been able to improve policy, open better communication channels and make our overall efforts more effective."

Ream sees more involvement with the CEO and senior business leaders in his future, and in the future of CISOs in general. "There will be a transformation in information security at healthcare organizations. I think we will see CISOs evolve to a position similar to how the Chief Compliance Officer is currently positioned. CISOs and their teams will roll up directly to the CEO. But, there will always be a tight and integrated relationship with the CIO, working collaboratively at a peer level." To get there, Ream pointed out that CISOs need to be comfortable speaking the language of business and translating technology into relatable stories. He expects more CISOs to come in with MBAs in the future.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS
WHO ARE LEADING THE WAY
FOR CONFIDENT INFORMATION
SECURITY PROGRAMS



MICHAEL MCGOVERN SVP, CISO, & CTO, METRO CREDIT UNION

HEADQUARTERS: Chelsea, MA

EMPLOYEES: 300

ASSET SIZE: \$1.5 Billion

INFORMATION SECURITY AND DISASTER RECOVERY GO HAND-IN-HAND

Michael McGovern, CISO and CTO of Metro Credit Union, stands in a unique position. He leads the company's security effort, but also holds responsibility for the organization's disaster recovery planning. Within this role he provides regular reports to the organization's Enterprise Wide Oversight Committee (EWOC). The EWOC is comprised of the CEO, CFO, COO and SVP of Operations, each with a strong interest in supporting and advocating for the company's security and disaster recovery programs.

"We meet with the EWOC once a month to go over Metro's information security posture. They want to know about new security threats that are seen by other organizations and out in the wild, areas where we can improve security. This meeting is our opportunity to share important information with the leadership team," said McGovern.

Conversations with the EWOC often become specific as they review data breach prevention tactics and McGovern

provides an update on threats and how personally identifiable information is protected. "Discussions with the CEO can get fairly technical. We talk about stats, data and metrics – including, for example, geo-blocking stats," said McGovern. He continued, "We want to make sure the key people in the organization understand information security threats and our objectives."

McGovern's disaster recovery work is strongly supported by the CEO and Board of Directors. "Because we receive the budget we ask for, we have built a strong technology-based infrastructure that allows us to replicate our data offsite to disaster recovery locations in a manner that is close to real-time. When I talk to other financial institutions, as well as auditors, they are surprised at the detail around our disaster recovery plan and the amount of testing we do on a quarterly and annual basis." For McGovern's program, disaster recovery covers technology (infrastructure), operations, as well as people. In the event of a disaster, he ensures a clearly defined process is in place that takes into account a number of different scenarios. He commented, "With my CEO and Board of Directors, we talk about recovery point and recovery time objectives. If we had a disaster today, what data would we lose? How quickly could we recover?"

TOUGH LEARNING EXPERIENCES

McGovern's interest in the intersection of disaster recovery and information security stems from his early career experiences. "I have been working in the financial services industry for about 15 years, and before that I was in the technology industry. Years ago, when I was in the high tech field, information security was not much of a concern. We were all concerned about 24x7 employee access and availability. But, I clearly remember my first experience with a virus – It was the Nimda virus and it took our company out for a week or more. It took our company down to its knees and we had to call in a lot of help to clean our network up and get virus-free. That was the first time I realized the huge role information security can play in business and uptime." McGovern also realized the key importance of establishing a thorough disaster recovery plan in preparation for this type of incident.

After learning this valuable lesson while working in high tech, McGovern then moved into his first role at a financial services organization as VP of IT at a large regional community bank. In the position for ten years, McGovern had the opportunity to greatly expand his security expertise. He said, "The financial services industry was ahead of high tech in terms of taking information security seriously and protecting member data. We were subjected to several audits by the state and the FDIC, as well as internal audits. In the early days, compliance was really driving our security efforts and purchases."

VALUE OF CORPORATE CULTURE

Since arriving at Metro Credit Union, McGovern and information security programs in general have evolved to be less compliance-driven and more focused on aligning with the business to ensure positive member experiences and better protection.

"Our role now is to make sure the credit union can perform day-to-day activities in a secure environment," said McGovern. "Our Board is really supportive of making sure we have a strong security posture. They want to know we are doing our best for our members' protection. We have put additional security mechanisms in place and now we are focused on strengthening as much as possible and still allowing our employees to service our members."

McGovern believes in the value of corporate culture and mindset when building out a strong security program, something which starts at the top. His Board represents a skilled and experienced group committed to making Metro Credit Union number one. Furthermore, McGovern reports into

a very involved and engaged CEO, who makes security a key priority. He said, "The CEO is involved in all aspects of the IT organization. We connect three or four times a day."

BALANCE IS KEY

One of McGovern's proudest achievements at Metro Credit Union was creating the credit union's disaster recovery infrastructure. In creating this, he pulled on lessons learned and experiences from earlier in his career, while realizing he needed to embrace innovations, such as Cloud technologies. "We built a great disaster recovery solution for my previous employer, but at Metro Credit Union I had to step back and evaluate if that same solution was still valid for Metro's environment. I looked at Cloud technology, which has matured recently. It took me six months to review new solutions and evaluate from a cost and control perspective and put the right solutions in place for a successful disaster recovery program."

Even with broad experience as a well versed leader, McGovern continually works hard to balance traditional IT functions, information security and business continuity planning with a relatively small staff. Because his team is responsible for a diverse set of requirements, he looks to hire well-rounded problem solvers with good time-management skills. McGovern ensures they receive the technical and business training they need to support the solutions in their environment. "We train at least two people on the team in every technology, so we can all collaborate to get our various tasks completed," said McGovern.

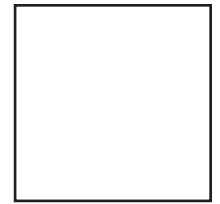
PEER COLLABORATION

McGovern commits himself to his own educational growth and continues to keep pace with evolving threats and emerging approaches to information security. He leverages communities like FS-ISAC, Infragard and ISSA to keep abreast of best practices and to share critical information with peers. McGovern attends monthly sessions at the Federal Reserve Bank to keep up-to-date on cyber threats. He said, "The Department of Homeland Security gave a recent presentation and individuals from the Federal Reserve have given presentations on the threat landscape. These are incredibly helpful forums."

McGovern said the events and exercises that involve peer collaboration represent learning experiences to the success of security programs. Just as critical to McGovern are key vendors and trusted partners that help keep him up-to-date on security best practices and emerging technologies. "It is impossible to manage all the vendors and keep pace with the innovations without help," said McGovern.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446



FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE

INTERNATIONAL INFORMATION SECURITY

SEPTEMBER 2016

K logix

WWW.KLOGIXSECURITY.COM
888.731.2314