FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE

ZERO TRUST: ILLUSION OR REALITY?

SEPTEMBER 2020
KLOGIXSECURITY.COM
617.731.2314

K logix

FEATS OF STRENGTH

ZERO TRUST

SEPTEMBER 2020

FROM THE Editor

In this issue of the magazine, we talk about the highly debated concept of Zero Trust. Within K logix there are a myriad of opinions about whether Zero Trust is an illusion of marketing or a reality worth spending time and money. To better understand this concept, we asked our CISO community how they define Zero Trust, what it means to them, their approach and if it is achievable.

Here's a snippet of what the CISOs interviewed in this issue are saying about Zero Trust:

- Anthony Siravo, CISO, Lifespan says, "Our approach here in healthcare, and probably other sectors as well, is a hybrid approach because for healthcare, we're required to use systems, applications and devices that don't support even basic antivirus, never mind advanced security tools. No matter what, we need a hybrid approach because we won't be able to do host-based Zero Trust security on these devices since we're not even allowed to install security tools on them."

- Andre Bromes, former CIO & CISO of Goodwill Industries, believes Zero Trust is achievable in spirit. He says security departments must understand and prepare for attacks that may happen with the right safeguards and processes in place. While there is no way you can lock down everything from everyone with a silver bullet, you should be able to formulate a plan and adopt it within your security program.

- Kathy Hughes, CISO & VP, Northwell Health explains, "Previously it was a buzzword, but now it's something that people really need to start paying attention to because working from a physical location from one device is no longer the norm. Now people are working from multiple locations, including home, and they're accessing systems from multiple devices. It could be their home computer, a mobile device or a kiosk device that they're accessing from a cafe. It's not always the same device."

- Kevin Hamel, Former CISO, Baystate Health, comments, "Zero Trust at times feels similar to the 'least privileges' concept that was around 10 or 20 years ago, where you give staff or vendors access to only those things that they need to have access to. The buzzword was 'least privilege'. So to me, I don't find the Zero Trust concept too different than giving people access to only what they need access to."

As many of the CISOs in this issue state, there is no one size fits all approach for Zero Trust and in many cases it may not be 100% achievable. CISOs who deeply understand their businesses, have robust visibility into their security programs and who think strategically are able to construct an actionable plan to address Zero Trust that correlates directly with their business goals and risk tolerance. What we do know is that Zero Trust cannot be solved by technology. It is a methodology that must be ingrained into a security practice and organization as a whole that is assisted by technologies to address defined gaps.

K logix works with customers who are looking to develop, strengthen or assess their Zero Trust approaches through our white glove, strategic security consulting services. Please don't hesitate to reach out and learn more, or visit www.klogixsecurity.com/zerotrust.

Kevin West

CEO, K logix

Magazine Contributors:

Katie Haug

Director of Marketing, K logix

Kevin West

CEO, K logix

Kevin Pouche

COO, K logix

Marcela Lima

Marketing Coordinator, K logix

About K logix:

We provide information security strategic offerings, threat and incident capabilities, education/awareness, and technology services. We craft our services to address specific customer and industry challenges. One of the ways we do this is through our thought leadership, business-focused publication *Feats of Strength*. Through 150+ CISO interviews, we extract trends in order to provide services that align business to information security.

www.klogixsecurity.com/feats-of-strength

marketing@klogixsecurity.com

617.731.2314

KATHY HUGHES

CISO & VP, NORTHWELL HEALTH

HEADQUARTERS: New Hyde Park, New York

EMPLOYEES: 68,000+

REVENUE: $12.5 Billion

Kathy Hughes was previously featured in a 2016 issue of Feats of Strength magazine. Today, Hughes shares her professional and team growth as it relates to strengthening the security program, continuing to ensure business goals are met and that Northwell Health is kept secure.

Hughes says the Information Security department has grown significantly over the past few years, with a heavy investment in awareness training and education, a strong focus on technologies and processes and steady progress within her team's roles and responsibilities. She comments, "At a very high level, my career has really been evolving based on the way the industry, and the needs placed upon CISOs, has been changing. We've had to look at how we're organized and how we're investing on a continuous basis to make sure we keep pace and adjust our processes and procedures. We've also had to change the way we work and interact with our staff, employees, business associates and patients, to make sure that we're doing it in the most effective, safe and efficient way."

She continues to focus on relationship building and relationship management to ensure the rest of the organization is aware and informed about security issues, threats, opportunities, challenges or gaps that might affect the security program. Hughes explains, "I'm on several committees where I have a seat at the table. Although it's virtual now, I get the opportunity to provide status on our security program to our senior management. My boss also provides an annual update to our Board of Trustees and quarterly updates at the Executive Audit and Compliance Board meetings."

The best way for Hughes to keep her business peers informed is through formal committees and meetings. She sits on the IT Risk Governance, Privacy and Security, Executive Audit and Compliance and PHI committees. Through these different committees, she communicates with her peers outside of Information Services and keeps them informed about what her team is working on, industry trends and where continued investments in people, process and technology are needed.

SOLID SECURITY FOUNDATION & COVID

"Expanding the remote workforce, making sure our research data was being protected and turning the knob up on monitoring those particular areas were things we had not planned to focus on prior to January. We also needed to expand protection on our internet connections, which required capacity upgrades as a result of the expanded workforce for intrusion prevention and for detecting potential DDoS attacks. We had all those foundational pieces in place, but the expanded use of these services literally happened unexpectedly overnight. That forced us to reevaluate the investments that we had planned for this year and shift priorities to make sure we could meet more current requirements the business was saying that they needed us to support."

Fortunately, Northwell Health had a solid foundation in place around remote workforce processes and technology, so when remote work became mandatory, the organization was prepared. Hughes explains, "We just had to turn the knob up because there were some adjustments that had to be made, some additional capacity that had to be purchased, but we had a really solid foundation that we had to just expand upon. We also had to educate people who weren't familiar with how to access that environment. This was one of our biggest challenges, not only for Northwell, but for every organization that had to contend with an overnight expanded remote workforce. We were very well prepared for this and were able to very successfully execute in a short period of time."

She continues, "The second issue that we had to deal with was that instead of people accessing our network through office connections to data centers and cloud services, they were now accessing those same resources, through their home internet connections. So we had to expand other types of infrastructure, like our intrusion prevention system and our DDoS protection services, as examples, to coincide with the shift of the traffic from the internal network to the exterior."

Northwell's healthcare network includes research organizations, so Hughes and her team had to intently examine how to protect critical research data. They focused on ensuring anomalous behavior was closely observed, with help from local FBI Outreach resources who provided guidance, advice and suggestions.

FOCUS ON OUTPACING ADVERSARIES

Top of mind for Hughes and her team is consistently keeping pace or outpacing adversaries, and doing so in a forward-thinking, automated and comprehensive manner. One of the most important approaches her team is taking is understanding adversarial techniques and tactics for infiltrating systems, whether through social engineering or technical malware-type methods. They are focusing on threat management and threat intelligence to understand how these threats might potentially impact Northwell Health's systems.

Hughes comments, "The areas of artificial intelligence and machine learning, as it relates to not only threat detection, but also threat response, are key focus areas for us that we've continued to invest in. For example, if there's a zero day vulnerability that is identified and an IP address known to be exploiting the vulnerability, we want to make sure the IP address is blocked quickly. We do this by either manually blocking that particular IP address or by using our security technologies to automatically detect and block anomalous activity."

She continues, "We've been focusing on automation and behavior analytics solutions that put some of the work that normally or historically would have been done by people, into software that can now do it better, quicker, faster and more efficiently. Otherwise, people would be reading through billions of meaningless events and trying to pick out those that might indicate an incident requiring further investigation. Our strategy is to automate and leverage technology to the extent we can, and where it makes sense, instead of hiring additional people to parse through logs, so the staff can focus on the more critical tasks."

ZERO TRUST: PROCESS, APPROACH AND METHODOLOGY

To Hughes, Zero Trust is a process, approach and methodology - not a product or technology solution. She defines Zero Trust by never trusting and always verifying that someone is who they say they are.

She explains, "When you look back, even as recently as last year, people typically would work from a particular physical location. They go to an office building and in our case, they'd go to hospitals or physician practice sites. They would typically sign in from the same device, whether it's a laptop or workstation, to access systems and data. Now, the concept of Zero Trust has really gained momentum because that dynamic has changed significantly. Previously it was a buzzword, but now it's something that people really need to start paying attention to because working from a physical location from one device is no longer the norm. Now people are working from multiple locations, including home, and they're accessing systems from multiple devices. It could be their home computer, a mobile device or a kiosk device that they're accessing from a cafe. It's not always the same device. So this has introduced a number of challenges because the concept of securing an office building and making sure that you have firewalls to protect your perimeter has become an outdated concept."

To address Zero Trust, Hughes recommends having a process that includes different principles. She comments, "Zero Trust programs require Identity and Access Management solutions, an Asset Management system and a Multifactor Authentication system. It also requires making sure you have the appropriate technologies in place to segment the network which can be done statically or dynamically. It's making sure that users, based on least privilege and need to know, have access to only what they need and what they should have access to, and only the privileges that they need to carry out their job functions. If somebody does get onto your network who isn't authorized, you must be able to contain them by limiting what they can do and where they can go."

ANDRE BROMES

FORMER CIO AND CISO
GOODWILL INDUSTRIES

CURRENTLY IN TRANSITION

Andre Bromes spent the majority of his career working at Goodwill Industries of Greater New York and Northern New Jersey. He began as a Network Administrator, moving into Network and Security Engineering, then as a Manager of Information Technology. He then worked as Vice President of Information Technology, Engineering and Security, before becoming the CIO and CISO of the organization.

Even though Bromes began his career in IT engineering, as information security functions were added to his responsibilities, he gained extensive knowledge and expertise, eventually changing roles to have his main focus on security.

Today, he is a board advisor to many organizations, speaks at numerous conferences and is recognized as a well-respected leader in the industry.

FOCUS ON TRANSFORMATION AS A STATE OF MIND

Today, Bromes believes CISO’s priorities are the same as business priorities. He explains, “Companies are in a state of transition. They have been for many years; years before the pandemic. However, the difference is that digital transformation can no longer be a catchphrase: it has to be a state of mind to be properly adopted. Some places, without even fully understanding the technicalities of that concept, had to digitally transform to survive. They had to look at their workloads and their archaic processes and look towards things that were static and seemingly unyielding. Teams are spinning up services for a form of cloud adoption, and sometimes struggling to match their digital transformation with their cloud adoption strategy. Files of all content types and classifications are being stored in the cloud, and we need to put appropriate controls in place. We need to take a risk-based approach to understand the process, not roles. We need to understand how this data is going to be used, even before we identify who is using it. Questions such as: is it being synced across multiple devices? What are the profiles of these devices? Where are these devices being used, as part of what process? We need answers to these questions before we can truly identify what we can do to secure the data. Only after we have that understanding to empower the business to push forward can we identify what we can do to allow access for a work from everywhere culture shift. Now more than ever, CISOs and CIOs have found themselves in positions where the answer isn’t let me perform some analysis paralysis and get back to you in three months. The business needs an answer now. And that answer must scale. We don’t truly know where we will be this time next year, but the technology we implement must support the trajectory that the business is expecting to hit. As experts in the field of technology and security - you have only a matter of days to put something in place and hopefully it’s resilient.”

With a shift to remote workforces due to COVID, Bromes says if you are unable to provide employees the ability to work from anywhere, organizations will not be able to operate. He notes the uptick in social engineering and ransomware, both of which have skyrocketed because cyber criminals now have a new target. Remote workers are the target, with many home computers lacking adequate controls and protections as compared to the corporate network. Bromes says there are limitations on what some businesses can do with VPN and bandwidth, causing additional layers of concern for security professionals and organizations as a whole. Many businesses turned to RDP as a resource, only to find that it was being heavily exploited by threat actors to propagate ransomware.

Bromes comments, “I remember when I was first studying as a Certified Ethical Hacker, the instructor said something that stood by me all these years afterward: if it’s easy for you, you make it easy for the attacker. That is very telling because it creates a dichotomy. After all, the job of the CIO is to make technology easy for the customers, and the CISO’s job is to make it secure for all. The CIA triad that security professionals adhere to is confidentiality, integrity, and availability. Security professionals traditionally have thought of confidentiality first, then came integrity, then finally availability popped in. Today, CISOs had to become CISO 2.0, something coined several years before but has had varying degrees of difficulty being adopted. This was not just a digital transformation of technology. It was a transformation of people in the C-suite, namely security professionals. They had to look at the culture of technology differently. You can’t do things the same way that they were being done in the office, perspectives needed to change. The realization of Zero Trust and the task of securing a borderless network became an early reality for some, but a steadily encroaching truth for almost everyone. I think that transformation, a reinvention in some instances, was the biggest push for everyone coming through this pandemic.”

ACHIEVING ZERO TRUST IN SPIRIT

Bromes believes Zero Trust is achievable in spirit. He says security departments must understand and prepare for attacks that may happen with the right safeguards and processes in place. While there is no way you can lock down everything from everyone with a silver bullet, you should be able to formulate a plan and adopt it within your security program.

It is important for Bromes to understand what the security team is doing to ensure access on a system is not just based on who a person says they are, but instead, the behaviors within that system.

He explains, “If I’m Tom and my pattern of behavior from my job is once I log in, I access this data and this channel, then the moment those behaviors change, the moment they shift left, some system has to say there’s a problem. There’s no reason why Tom is now accessing three other systems and using those three systems to access a finance database and is now pulling down large volumes of data; that behavior is odd. I don’t trust it. I’m killing the connection. Actionable intelligence on behavioral anomalies needs to be part of the toolkit for businesses large and small.”

On the topic of Shifting Left, Bromes wholeheartedly believes in this concept, and if organizations do not take this approach, vulnerabilities will significantly increase. He says when you shift left, you bring in security earlier in the development lifecycle to avoid delays and costly changes. He remarks, “I think that for you to get there, the shift has to happen because the world is moving rapidly and staying in the cloud more so than before. Either you become a part of the process and design the shift or the absence of the shift will design your information’s fate. ”

EMOTIONAL INTELLIGENCE AND LEADERSHIP

“We’re all people; no one intentionally shows up to work to do a bad job. Some people are more outspoken than others, but no one shows up to do a bad job. And my job is to help you be successful. If we agree that you’re here to do a good job, then we agree that the main focus of your job is to make this business successful. If I believe that’s your main focus, why would I or anyone for that matter, put anything in the way of that? Furthermore, why not question broken, inefficient processes that get in the way of good work? If we can have that dialogue and promote change or, at the very least, come to an understanding that works towards improving the process, then we can improve output, culture and well-being. Because people, when they come to work, they’re owed at least three things: personal growth, professional growth and financial growth. People are the greatest asset for a business and must be treated as part of the solution, not part of the problem,” notes Bromes.

Bromes is a strong supporter of emotional intelligence, where he must know himself and provide his team with a sense of empathy and the ability to put himself into the shoes of others and understand what they are experiencing. He collaborates with everyone from the help desk technician to engineers, developers, and executives within an organization. His first and foremost role is to collaborate and understand where there are challenges and find robust solutions.

He says, “My understanding of leadership in IT is that the business has goals. Those goals are things that are important to the strategic direction the business needs to head in. In all instances, promises were made and expectations established with auditors, to the board, to customers (both internal and external) and others, and we must seek to answer and fulfill them. We must execute on what we said we would do. My job is to translate that to the different members on the team and how it relates to their individual and sometimes team functions. The translation between goal and service delivery is how a leader works with their team to see those strategies and goals to fruition.”

IS ZERO TRUST ACHIEVEABLE?

IS IT AN UNREALISITIC SECURITY MODEL, EASY TO IMPLEMENT OR SOMEWHERE IN BETWEEN?

OPINION PIECE

Sydney Solomon,
Cyber Security
Research Anayst,
K logix

Trust is a vulnerability. That is the chief motto of a Zero Trust security model, with the goal of eliminating any unauthorized access to data and services. And yet, its simplicity is deceptive; there is no single technology or method to help organizations achieve Zero Trust (Forrester, 2015).

Zero Trust challenges the traditional, perimeter-based “castle and moat” security model by changing the “perimeter” to anywhere within an organization where access control decisions occur (Nather, 2020). With a “castle and moat” security model, hackers do not meet much resistance moving inside internal systems. But, by following Zero Trust principles, security is ubiquitous within an organization as its users, devices and applications need to regularly re-establish trust to an organization’s assets.

Security professionals have been moving away from the “castle and moat” model for a while now. So, why then, is Zero Trust such a pervasive term in security circles today? John Kindervag, when inventing the term in 2010, identified three core Zero Trust principles: 1) verify and secure all resources, 2) limit and strictly enforce access control, and 3) inspect and log all traffic (Forrester, 2010). These principles have encouraged and guided security professionals to build bottom-up approaches for implementing a Zero Trust architecture. Notable models include ones published by Google and NIST (Google, 2014; NIST, 2020). The security market also offers better tech to implement Zero Trust, further explaining its current fame (Nather, 2020).

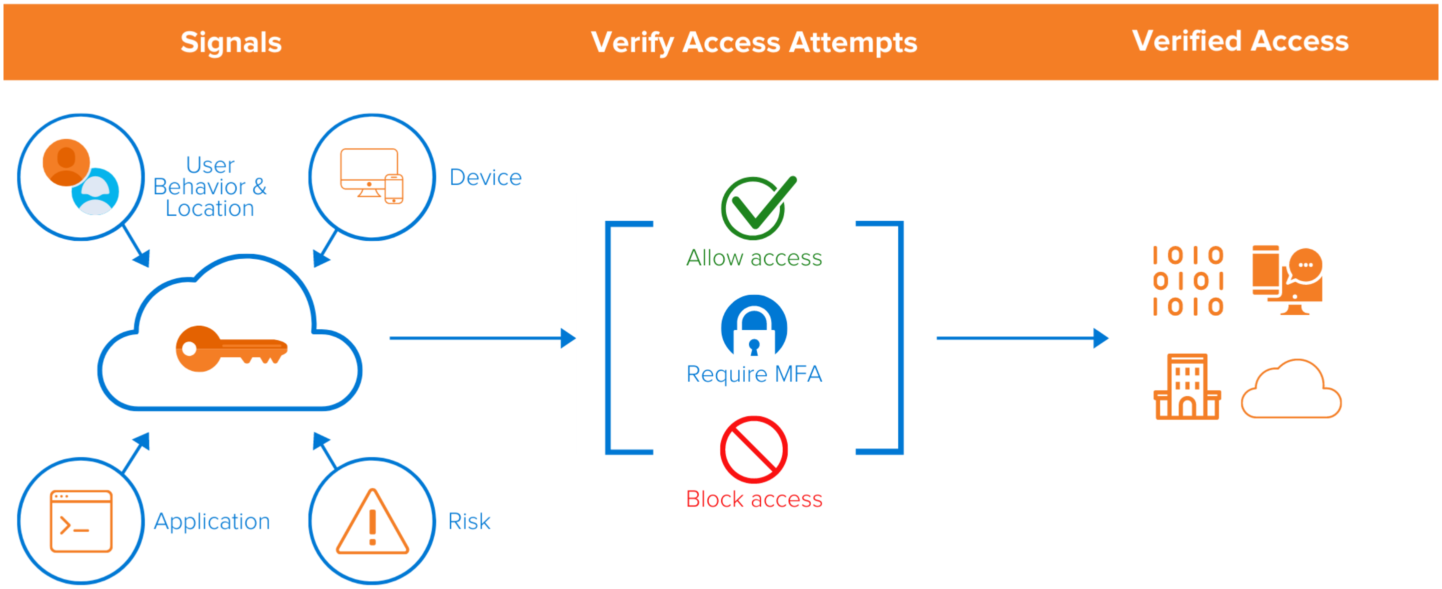
Zero Trust gets a bad rap in some circles because many models for implementation assume systems are being built from scratch, as is the case in Google’s notorious Zero Trust initiative, BeyondCorp. Google wanted to give employees the ability to work remotely from an untrusted network without requiring the use of a VPN. In doing so, over the course of eight years, Google reinvented its network architecture by 1) identifying the applications, services and infrastructures subject to access control and assigning those entry points a minimum trust tier, 2) allowing only managed devices to access corporate applications via a device inventory database, 3) securely identifying users via a user and group database, and SSO, 4) creating an unprivileged network, 5) externalizing applications and workflows, and 6) implementing inventory-based access control. Just reading the steps Google took will leave a person winded, so needless to say, it’s not an achievable model for most organizations.

But Zero Trust does not have to be radical. Many security professionals believe it has incremental value and the NIST Zero Trust report recommends organizations seek to

> *“Zero Trust gets a bad rap in some circles because many models for implementation assume systems are being built from scratch.”*

ZERO TRUST EXPLAINED

Graphic created by Marcela Lima



incrementally implement Zero Trust principles. The NIST report recognizes that organizations will likely operate in a hybrid Zero Trust/perimeter-based model for an indefinite period, but suggests organizations begin investing in Zero Trust initiatives today (NIST, 2020).

While there is no single approach to Zero Trust security, here are some useful steps, distilled from an assortment of sources, to guide an organization along its journey: 1) Identify the organization's protect surface - what is its network's most critical and valuable data, assets, applications and services?; 2) Gain visibility into the organization's network's activity and current solutions - how does traffic move within the organization in relation to the protect surface?; 3) Map the flow of the organization's sensitive data – does the organization have an up-to-date asset inventory?; 4) Create micro-networks and implement access control, and finally 5) Continuously monitor and authenticate (Forrester, 2015; Nather, 2020; NIST, 2020; Palo Alto Networks, 2018).

Works Cited

Forrester, 2015. Case Study: Westjet Redefines Its Security With Forrester's Zero Trust Model. Forrester.

Forrester, 2010. No More Chewy Centers: Introducing The Zero Trust Model Of Information Security. Forrester.

Google, 2014. Beyondcorp, An Overview: "A New Approach To Enterprise Security". Google.

Nather, W., 2020. Getting Real: Sorting What'S ZT And What'S Just BS. [online] Brighttalk.com. Available at: <https://www.brighttalk.com/webcast/10415/383057/getting-real-sorting-what-s-zt-and-what-s-just-bs>.

NIST, 2020. Zero Trust Architecture. NIST.

Palo Alto Networks, 2018. What Is Zero Trust?. Palo Alto Networks.

ANTHONY SIRAVO

CISO
LIFESPAN

U.S. HEADQUARTERS: Providence, RI

EMPLOYEES: 16,000+

REVENUE: $2.3 Billion

Since Anthony Siravo was last featured in our Profiles in Confidence in 2017, his role and responsibilities have evolved, along with his approach to addressing unprecedented challenges.

Siravo's IT security department has grown in size, with the addition of specific infrastructure team responsibilities, enabling significant growth in their security engineering capabilities. The new team added key functions such as web filtering, application whitelisting, network access control and mobile device management. Siravo explains, "The traditional security team wasn't necessarily a 24/7 shop in terms of being on around the clock to hop on a call at any time if needed. But now with network access control and application whitelisting, we're truly required to be in-line with the way our customers do business. And we are a 24/7 hospital system."

RANSOMWARE AND IoMT

Siravo has two key top priorities - addressing an influx of ransomware hitting their partners & affiliates and focusing on his IoMT (Internet of Medical Things) cyber protection program.

There has been a significant uptick in ransomware hitting their partners and affiliates which concerns Siravo from a security perspective for many reasons, especially since Lifespan is linked to them via VPN. To combat these persistent threats during partner outbreaks, the security team has cut VPN connections between sites, blocked emails and kept ransomware runbooks uptodate. Siravo feels his team has become faster at responding to affiliate ransomware threats in both a timely and appropriate manner.

He comments, "We're embedding testing into all of our controls on a monthly basis. It's a huge undertaking to find out what our weaknesses are for all this ransomware, which has a lot of variance. We're starting with the newest and working our way back. Tactically we are working on stopping what's called LOLBINS (Living off the Land Binaries) from executing maliciously in our environment. LOLBINS are actual legitimate files that are installed on your system by default and required by things like your operating system. When you install Windows 10 on your system, these files are installed and necessary for most normal operations. They're legitimate programs that need to run but the problem is all the new ransomware threat actors are taking advantage of LOLBINS."

These types of ransomware threats have garnered Board and executive interest who engage with Siravo and his team to discuss their approach and progress, along with any questions they may have. He says, "I've been giving more presentations and done more reporting to the Board.

They have a lot of the metrics that I report to my different information security governance committees. We now report out to them as well. Because things are getting closer to home, there have been some organizational changes and overall more interest from the executives, which obviously helps me get funding and support."

Siravo's second priority around the IoMT cyber protection program is a challenge due to strict FDA regulations, vendor security ignorance and the legacy nature of medical devices. These devices include things such as infusion pumps and x-ray machines that are not managed by the information systems teams in any way, and Siravo's security team has limited or no access to them. Many times, operating systems and applications may be out of date with legacy technology and vulnerabilities, posing a challenge for Siravo and his team to secure them.

He explains "As an example, an infusion pump has Telnet open, which is an insecure, clear text protocol. It doesn't even need Telnet to run, but these things are so antiquated and non-secure that they're not hardened. We must make sure that unnecessary and potentially vulnerable ports and services can't communicate from a network level, so nothing can be taken advantage of from that standpoint. That's a huge undertaking because we have to call up these vendors and say, hey, we know you're not going to work on security, but can you tell us what ports you actually need? What does this thing actually need to do to communicate? We're going to secure around it, we're not going to break any functionality of your device. We're not going to break the FDA regulations. We're going to go from a network level and not touch your device, but we're going to secure it to the best of our abilities."

REMOTE WORKFORCE IMPACT

Aside from budgetary and resource-driven restraints caused by COVID, Siravo says addressing the shift to a remote workforce has been a significant challenge and undertaking to address. The information systems team was required to create a more robust remote infrastructure that allowed additional VPN and Citrix connections which the security team now must apply controls to. Furthermore, his team continues to spend time educating the workforce on how to use remote technologies, Multi-Factor Authentication, and navigate programs they might have not used before.

From a leadership perspective, Siravo has shifted his approach to ensure he continues to boost morale and communicate effectively. He explains, "Previously, I'd pop in my team's offices on a daily basis. Obviously, I can't do that anymore. Before, I always knew what was going on and what people were working on by seeing them in-person. So now with COVID, I can't do that. Typically, security and IT people don't like video chat. My leadership style has shifted to a lot more items being tracked in a more formal written format via Kanban SaaS type applications versus verbal. That's how I keep track of what everyone's doing and have updates that way."

HYBRID APPROACH TO ZERO TRUST

Siravo says for most healthcare organizations, Zero Trust is not 100% achievable. His approach to Zero Trust is hybrid due to the complex nature of the healthcare industry inundated with legacy systems and applications, and complexities around the Internet of Medical Things. He comments, "It doesn't matter if you're behind the firewall, you don't trust that network. So that's how we're defining Zero Trust. Our approach here in healthcare, and probably other sectors as well, is a hybrid approach because for healthcare, we're required to use systems, applications and devices that don't support even basic antivirus, never mind advanced security tools. No matter what, we need a hybrid approach because we won't be able to do host-based Zero Trust security on these devices since we're not even allowed to install security tools on them."

He continues, "For the IS managed devices, including things the information system team manages and my team secures, all of our endpoint controls work on-premise the same way when you're off-premise. For example, when you're here on-site at Lifespan we may have Dropbox blocked, and when you pick-up your laptop and bring it home, Dropbox will also be blocked at your house. We have the same malware protection checking every URL link and file, advanced persistent threat detection, everything. It works the same way because all of the security we're setting up is host-based. It doesn't matter how bad that network is, it's the same rules applied. However, for the non IS-managed devices, we have to mitigate those threats as much as possible. These systems are not going home. They're all on our Lifespan production network but have no controls on them. There's nothing we can install on them. They can't really be Zero Trust because they're on that network. There's nothing we can do to them from a host-based security perspective, so we have to utilize network based protection to the best extent possible."

KEVIN HAMEL

FORMER CISO,
BAYSTATE HEALTH

CURRENTLY IN TRANSITION

Since his last Profile in Confidence feature in 2016, Kevin Hamel has transitioned roles and industries, garnering increased exposure and experience. He has grown significantly as a leader, from both a technical and business alignment standpoint through his CISO positions in both banking and healthcare.

Hamel provided updates on how his career has evolved since we last interviewed him, and discussed the extensive knowledge he gained in regard to the nuances, challenges and complexities of the working in the healthcare industry. He says, "While there's a lot of similarities in the technology that's used in banking and healthcare, there's a lot of differences as well. I think the healthcare technology environment is more complex in many ways, especially when you start to think about medical devices. For larger healthcare organizations, you may be looking at tens of thousands of IoT devices that are hard to manage. Trying to keep all of that data flowing and flowing securely is certainly no easy task."

THE RISING FOCUS ON CLOUD AND REMOTE WORKFORCES

With over 16 years' experience in information security, Hamel understands the constant evolution and growth taking place in the industry. Currently, he says CISOs' goals and challenges have changed dramatically due to the impact of COVID. He explains, "There's been a huge shift to remote work and companies have migrated hundreds or in some cases, thousands of employees to a remote work situation. In many cases, this happened over the span of only a few weeks. I think that's really brought the question of how to manage a remote workforce to the forefront. Not just from a security perspective, but a lot of the obvious things come into play. Things like how to make sure employees are the only ones connecting to an organization's remote connection, or other basic considerations like Multi-Factor Authentication."

Hamel says we must take into account the security implications of a remote workforce, but also consider business-wide concerns such as communicating with employees if there is a system outage. He says in many cases, companies may have an emergency notification system they blast out to let their employees know their system is down. However, many are not prepared for the sudden impact of thousands of employees working remotely and may struggle to adequately maintain the same level of company-wide communication.

With a heavier focus on cloud and remote endpoint technologies, Hamel sees this trend continuing to increase, potentially resulting in additional training budget for information security staff members. He explains, "I'm not sure

> *"For me, I need more digital, I need more cloud, I need more remote technologies. I think that's going to be a big area of focus going forward over the next few years."*

that companies have invested appropriate training dollars in cloud and remote workforce technologies over the past five years. If companies are going to go down this road of having 50% or more of their workforce working remote, technology teams must understand how they're managing remote access to platforms such as Teams, Dropbox and Box."

Hamel says the quote 'the cloud is now my data center, any device is now my endpoint, my network is now the internet' resonates with him because it clearly depicts the new challenges faced by security leaders. He comments, "It has just completely changed the landscape that all companies are operating on. And I think it requires, in some ways, technical skills that I'm not sure every company has. I know I'm looking to invest in staff training around cloud, mobility management and remote connectivity tools so we can support the new workforce."

THE PUSH FOR DIGITAL EXPERIENCES

Hamel believes there is a significant push within organizations for accelerated digital experiences, whether it's internally with employees or externally for consumers and customers. For example, in the healthcare field, digital advancements may include telemedicine or leveraging medical devices outside of the hospital, such as at-home blood testing.

He comments, "So far, a lot of our conversation has revolved around employees, remote workforces and accessing cloud solutions, but it is also important to think about your patients, consumers or customers. You can't ignore the customer or patient side of things. I think this pandemic is going to force a lot of businesses to revisit if they need customers or patients to come directly into their facilities for certain services, or if they should leverage digital channels to consume business services from the comfort of their own home. That's going to put new demands on IT and information security and you're going to see pressure on both sides. Since most employees are now remote, customers and patients need to engage in a digital capacity. For me, I need more digital, I need more cloud, I need more remote technologies. I think that's going to be a big area of focus going forward over the next few years."

IMPLEMENTING ZERO TRUST

Hamel does not believe there is a one size fits all approach for Zero Trust that applies to every organization and industry. Most companies have varying definitions of what Zero Trust means to their program and mission, and their goals ultimately differ.

Hamel explains, "To make a broad statement and say Zero Trust is achievable, is something that's hard to do because every company is probably going to have a different definition of what that means and a different definition of what their Zero Trust end state would look like. Maybe one company decides to do Zero Trust only with certain platforms or another company that is focused on only a certain extent, but across all of their platforms. I don't think there's a one size fits all. Everybody has to chart their own course and figure out what their Zero Trust goals look like."

Zero Trust is a worthwhile and beneficial endeavor according to Hamel. He believes every company should have Zero Trust implemented in some fashion. He says, "Zero Trust at times feels similar to the 'least privileges' concept that was around 10 or 20 years ago, where you give staff or vendors access to only those things that they need to have access to. The buzzword was 'least privilege'. So to me, I don't find the Zero Trust concept too different than giving people access to only what they need access to."

He continues, "Admittedly with Zero Trust, we're talking about different tools to make that happen and more automation, and more on the fly analysis to figure out what resources or IT services a user has access to. But I think that concept is still largely the same where you give someone only what they should have access to at this point in time. I think every company should be moving in that direction and trying to implement some form of Zero Trust, but whatever's right for them as a company and to whatever degree is right for them as a company."

THE REALPOLITIK OF ZERO TRUST

THINKING BEYOND BUZZWORDS

OPINION PIECE

Erik Kamerling,
Lead Information Security Consultant,
K logix

> **"How we live is so different from how we ought to live, that he who studies what ought to be done rather than what is done, will learn the way to his downfall rather than to his preservation."**
>
> - Machiavelli

ZERO TRUST: AN ARCHITECTURAL IDEAL

Zero Trust is an aspirational security architecture meant to redesign computer networks with the express goal of limiting the inherent trust between systems, applications, people and data owners, network segments and transactions. The concept is meant to address the failings of conventional perimeter security paradigms by redefining the trust posture, security controls and monitoring technology in such a way as to do away with border centric control. The goal is to distribute that control in a more pervasive fabric throughout the enterprise that minimizes single points of failure and maximizes resiliency and survivability in the face of cyber threats. In essence, Zero Trust is a natural evolution of the networking model due to society's movement from a high trust (low surveillance scenario) to a lower trust (high surveillance) environment.

Zero Trust is an architectural ideal. Similar to how structures are designed to withstand earthquakes, Zero Trust provides a model for network resiliency in the face of the improbable. Where Earthquake Engineering (a best practice) provides guidance and standards for building in seismically active areas, architects and engineers must adhere to these ideal practices when building in tectonically active arenas. However, these seismic standards are realistically not held as a baseline for all of architecture and are chosen only when appropriate. Zero trust should be leveraged in the same capacity, as a scenario-based best practice.

Why is this an issue? Because network security often lacks the ability to provide a measurable ROI. Making Zero Trust re-architecting a dubious proposition in environments with low security risk, or where perimeter security capabilities are effectively inhibiting damaging incidents. Couple this with the pressure on network professionals to meet cloud macro transformation demands, while also micro-segmenting the remainder of the infrastructure. Network engineers are expected to expand purview outward and inward simultaneously. Imagine being asked to design a way to securely lose control outward, while at the same time gain further control over the wire, the transaction and trust. This conundrum points to a need for a pragmatic, systematic approach to determining what level of effort should be allocated to idealistic goals such as Zero Trust.

REALPOLITIK: RESPONSIBILITY AND CONVICTION

Realpolitik is a system of principles and methods based on practical rather than moral or ideological considerations. It is a political and tactical stratagem designed to penetrate the idealistic dependencies of social and political problems and to efficiently reach solutions. We strive to understand the most basic building blocks of specific security technologies, standards, initiatives, trends, etc. More importantly, we strive to comprehend the phenomenology behind certain market movements. We had to go backward in time to find practicable Realpolitik approaches to technical change, and to appropriately frame modern technical ideals that fall within contemporary information security.

In the late 1800s, Max Weber spearheaded the political philosophy behind Realpolitik by outlining two ethics: responsibility and conviction. The ethic of responsibility states that an action is given meaning only as a cause of an effect in the empirical world. The ethic of conviction suggests that an agent should be able to choose autonomously not only the means, but also the end of the challenge faced. Both ethics were imperative to Weber. Accordingly, he said in order to find an optimal solution to technical challenges (and challenges in general) we must strive to force the two ethics together to form a solution portfolio. His combinatory ethic states that we should pursue a passionate conviction to the ideals that politics has to serve while pursuing a sober rational calculation of its achievability in the world sphere. This is the Realpolitik needed to drive Zero Trust from an oft unachievable aspiration, to a realistic achievable goal.

Realpolitik may be used to analyze aspirational technical challenges and idealistic design trends. A realistic dual ethic of analysis would help us make sense of Zero Trust while our defenses are simultaneously being exposed outward into cloud environments. In addition to Zero Trust; mixing solutions rooted in both realism and idealism would facilitate solutions to persistent comparable challenges such as CASB (while already owning effective egress proxies, certificate management, application aware Firewalls, and IDS/IPS), to DLP (where we already have MDR, UEBA, Firewalls, IDS/IPS, proxies and SSL-Strip capabilities).

REALPOLITIK AS A SOLUTION TO TRENDS

Is Zero Trust a trend or fad? Yes. And it's an aspirational trend rooted in sound secure design principles. It is a collection of valid architectural security engineering principles and achieved by utilizing existing strengths, by focusing on program maturity, by emphasizing proper design and by automating and orchestrating where possible. Success cases in the security field almost always slow roll changes and perform risk-reducing actions incrementally. If we involve security teams and set realistic goals while seeking the best-fit balance against other sizeable security challenges (Cloud, Sec-Dev-Ops, CASB, DLP, UEBA/MDR, etc.) then we're using a Realpolitik approach. Aside from using analytical ethics to produce pragmatic solutions to aspirational challenges, isn't it self-evident that applying security strictures closer and closer to the endpoint, to the person, to the identity, is what we strive for in an ideal security design?

It is our challenge as security professionals to identify a number of these factors prevalent in today's environment, and to make the best sense of them when we can. We must develop analytical frameworks equivalent to the political science of the past, which allowed thinkers, practitioners and workers to identify the differences between aspirational goals and realistic solutions. Not only to identify these differences between ideals and pragmatic reality, but to identify when security concepts become part of marketing buzzwords and promotion, particularly when they are unsolvable challenges. Armed with a method composed of responsibility and conviction ethics, the security industry may be able to see beyond marketing hype to view the substandard yet promising infrastructure behind the facade. And to construct a realistic solution set to these idealistic goals, thus executing decision making and growth using a Realpolitik of Information Security.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446