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."