# Protecting The Financial Services Critical Infrastructure and Beyond

**An Interview with Bill Nelson,**
**President and Chief Executive Officer, Financial Services Information Sharing and Analysis Center (FS-ISAC)**

**EDITORS' NOTE** *Bill Nelson has held his current post since 2006. Prior to this, he was Executive Vice President at NACHA. He has also been a senior product manager at Mellon Bank. He graduated from Allegheny College.*

*Bill Nelson*

**CENTER BRIEF** *The FS-ISAC, Inc. (fsisac.com), is owned by its members. The FS-ISAC executive team functions under a set of operating rules and is overseen by the organization's Board of Directors. Based on the operating rules, FS-ISAC staff members determine member eligibility, enforce member eligibility verification through trusted third parties, and oversee the operation of the FS-ISAC. The Board of Directors is elected by the membership to serve three-year terms.*

**Will you define the role for FS-ISAC and the key areas of focus you address?**

We're a non-for-profit with over 7,000 member companies around the world so we now have a critical mass of experts and practitioners in the financial sector that participate actively in information sharing. We analyze the threat environment so that members have greater situational awareness of the changing threats and successful tactics for response and the defense of their customers. By extension, this protects financial operations and the critical infrastructure that backs the entire economy.

**Is the primary focus financial services or is it broadening to overlap with other industries?**

It's all of the above. Our core focus is on the financial services community, but we include every type of firm from the largest global financial services firms to the smallest credit unions and anyone in between. This includes the financial exchanges, broker/dealers, insurance companies, and asset management companies.

Also, because of the role financial services plays in terms of financing economic activity and of being connected to customers on the commercial side as well as on the retail side, we are right in the center of the action. This is where the sensitive data is that has value to the attackers, so our members are often the targets of these attacks. The financial sector is considered a thought leader when it comes to information security programs, customer education programs, and, of course, threat intelligence and information sharing programs.

FS-ISAC is considered an expert when it comes to information sharing and threat intelligence and so other critical sectors have actually approached us and asked us to help play a role in providing services. For example, we provide services through a group within the FS-ISAC called Sector Services. It provides support to the retailer sector, to major law firms, the oil and natural gas sector, and others. This is an area that we expect will continue to grow as other sectors come to us and ask us to provide this support. It also helps facilitate appropriate information sharing among sectors.

We are also very connected to the National Council of ISAC, which includes over a dozen other ISACs. We're in constant contact with them with regards to major events and coordination around how to respond to those events.

**Are you working at multiple levels with your members?**

Our focus is primarily with the Chief Information Security Officer and the Chief of Business Resilience Officer. We also provide cyber and physical alerts, so we have been talking more frequently with CEOs, COOs, and Chief Risk Officers, particularly since cyber has become a top board-level issue.

There is quite a bit of engagement at those different levels but the primary focus of our conversation is with those CISOs and the folks that report to the CISO – the threat intelligence analyst folks who are constantly monitoring the networks and trying to understand the environment.

**It seems the approach to cyber is not about if but about when, and is more about dealing with an incident after it has occurred. Is the focus today more about being prepared and what can be done to stop these attacks or is it more about what one needs to do once it occurs?**

It's both. Part of our approach is to enhance our resilience not only through real-time threat intelligence and information sharing and analysis, but also through crisis management response and coordination. We have spent a lot of time over the past years updating our all-crises hazards management playbook, which lays out the procedures for how we identify a crisis and respond to it. This oftentimes includes extensive coordination with government partners.

We've been conducting exercises like simulated cyber-attack exercises where we walk through a series of scenarios and talk about how we would respond. Through those exercises, which are conducted in a safe, non-attributed environment, we identify gaps that should be addressed and launch initiatives to address those gaps.

It's an ongoing conversation where the FS-ISAC is working with our partner associations like the American Bankers Association, Credit Union National Association, Financial Services Roundtable, Independent Community Bankers Association, and Security Industry Financial Market Association. We work with these associations to better connect the community and enhance resiliency. In some respects, this may involve helping our member firms comply with increasing regulatory requirements, which is another element that is somewhat unique in that financial services companies are so heavily regulated.

**When it comes to threats from intel sharing, there is an important element involving privacy and classified information. Does more need to be done to accelerate the sharing platform and allow further sharing, and how hard is it to find the balance when it comes to concerns over classified information and what can be shared?**

We spent a lot of time studying this and working with government agencies that can supply information and help us understand the context of certain types of attacks.

We have developed operating rules that our members have signed onto as a condition of being a member. These contain procedures for how members can tag information. We have a protocol called the traffic light protocol from which one can tag the information with different color levels. This allows for the information to be protected and controlled efficiently depending on how it is tagged.

In addition, we have been working diligently with our government partners to encourage them to declassify more information or provide us with appropriate parts of classified information that focuses on the context. We don't care about sources; we just want to understand if something is a malicious IP address and what type of entity it's coming from. This helps us understand what they might potentially be after and allows us to help the community better defend itself from different types of attacks.

There has been a great deal of work done over the years to try to improve that process and to encourage more information sharing bi-directionally from the industry to government and vice versa. This will help create greater awareness but also greater effectiveness in how to respond to different types of cyber-attacks. ●