Less than two weeks before Christmas 2020, news began to headline across the country: SolarWinds Orion had been compromised, potentially as far back as ten months, likely by a nation-state. Industry immediately recognized that this supply chain cyberattack was both sophisticated and widespread, potentially compromising dozens of government agencies, as well as financial institutions. The alarm bells about these types of new cyber threats are ringing loud and clear. This breach is a painful reminder of the cyber threat actors targeting our nation, including nation-states, criminal cyberattack groups, and hacktivists.

A recent U.S. Chamber of Commerce and FICO Assessment of Business Cybersecurity study described the risk to the financial sector as extremely high. And the Verizon 2020 Data Breach Investigations Report listed the financial industry as one of the most attacked sectors across all of industry.

In the past year, a record 28,591 security incidents were reported by Federal agencies to the Department of Homeland Security. The General Accountability Office made over 3,000 cybersecurity recommendations, 600 have not been fully implemented. Of these, 75 warrant priority and until fully implemented, GAO stated federal IT systems and data will be increasingly susceptible to cyber threats, cyber-attacks, and costly data breaches.

What should agencies with critical financial & regulatory missions do in the face of this onslaught?

Emerging data-centric technologies can create valuable efficiencies, as well as cybersecurity vulnerabilities to data breaches. Perspecta, a leading U.S. government services provider, is committed to helping the community accelerate adoption of leading digital transformation practices, while protecting critical infrastructure.

Perspecta worked with FedInsider to share lessons from an elite cadre of “defenders” at federal financial mission agencies who are experts in keeping their organizations and elements of the nation’s financial ecosystem safe.
The following are four key principles that some of those financial industry experts shared during a recent FedInsider roundtable discussion “Conversations on Risk: Cybersecurity in the Financial Sector”.

1. **Know what to do & who to contact before an emergency**

While individual financial institutions must oversee their own security, they are also part of an intricate system that underpins the U.S. (and global) economy. To emphasize that point, the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) designated the U.S. financial sector as one of eighteen components of the country’s national critical infrastructure. Like the electrical grid or interstate highways, the disruption of a national critical function in any of these financial institutions and agencies would have an immediate impact on the health, safety and stability of the nation.

Designation of financial institutions as a national critical function is just a starting point, according to Acting Associate Director of the Office of Compliance Inspections and Examinations for the Securities and Exchange Commission (SEC) Dan DeWaal. He says that the SEC has been working to help financial organizations fight cybercrime for a long time, and has recently increased the level of federal assistance to groups that need it.

“We implemented an incident response protocol. And as incidents occur in our respective financial institutions that each of the regulators oversee, we have a protocol to assess them based on several criteria including the type of incident, the potential disruption to operations and the impact on their ability to continue to deliver their critical national functions,” DeWaal said. “And when appropriate, we have automatic escalation so we can assist and unify communications. We really focus at the SEC around capital markets and investment activities, but there is also, through the national cyber and service response plan, the ability to look at consumer and banking services as well as funding and liquidity services.”

A data-driven and coordinated response with other financial institutions can pre-emptively address emerging threats.

2. **Adopt shared security frameworks to promote unified, timely protective actions**

Many financial institutions deal in very large digital transactions. For example, when a company needs to borrow several million dollars to help finance an overseas transportation project, the funds are transferred electronically, because it’s not really possible or practical to try and deal with hard currency at that level. Because of this, the Chief Information Officer of the Export-Import Bank of the United States, Howard Spira, says that financial organizations embraced a number of cybersecurity frameworks earlier than most other industries.

“In addition to being highly regulated, the financial services industry always had a strong incentive to understand cyber because of the reliance of financial services on information technology and all of the consequent risks of that,” Spira said. “One of the reasons that we are doing so well is the fact that financial regulators focus on that.”

As to which frameworks financial institutions should adopt depends on their business, their risk factors and where their IT landscape intersects with their non-cyber infrastructure.

“In terms of enterprise risk management, things like the Sarbanes–Oxley Act try to pull away from just a cyber-centric perspective and looks at the whole of the institution, which I think is very important,” Spira added.

Adoption of an agreed-upon set of security frameworks can strengthen rapid response across the financial ecosystem. If there is good news in the increasingly hostile environment, it is the accelerated attention to mitigating supply chain risks. “For agencies with a federal financial mission, adopting security frameworks like the NIST CyberSecurity Framework and using the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool are great ways to strengthen the cybersecurity posture going forward,” said Chief Technology Officer for the Civilian, State and Local Business Group at Perspecta, John Cho, who co-moderated the roundtable discussion. “NIST is finalizing a new publication, NISTIR 8276, that includes key principles for protecting IT supply chains and releasing the draft to update SP 800-161.”

3. **Moving federal financial missions to the cloud can bolster security, but agencies must understand & be responsible for their own risks**

Many financial institutions are moving their workloads to the cloud. Besides advantages in cost savings and operational speed, cloud deployments can also improve security. Nonetheless, organizations need to be careful because cloud technology comes with both risks and rewards.

“A lot of financial organizations and federal agencies are trying to get into the cloud to help implement automation, continuous diagnostics and monitoring, and other types of tools,” Cho stated.

“On the rewards side, and from a security perspective specifically, some of the security technologies integrated
into cloud are really helpful,” said Chief Information Security Officer for the Federal Reserve System Tammy Hornsby-Fink. “An example I would give is the encryption of data at rest, which is well-integrated into the cloud.”

Adoption of cloud technology with an external provider doesn’t transfer all of an organization’s risk mitigation along with it. It’s crucial to know the risks where responsibility should be directly retained. “The other thing I would note with the cloud on the risk side is the shared risk model,” Hornsby-Fink said. “There are plenty of controls that are satisfied through your cloud provider or your managed solutions provider, but you need to know what you are responsible for, and what they are providing for you so there are no gaps. Know your model well.”

Cho goes on to point out, “Look, in retrospect, to the SolarWinds supply chain attack. We’re still uncovering the extent of the damage. Cyber-managed services have to be comprehensive across an ecosystem. Automation and continuous diagnostics and monitoring need to focus on external attack vectors, as well as sophisticated cyber threats that may emerge internally like Insider Threat and context-aware malware.”

4. Tap into trusted partners with cloud adoption experience. Partnerships and collaboration are keys to success

Improving or upgrading the cybersecurity at a financial institution can be a very complex task, especially when part of a larger ecosystem. No matter where an organization is on that path, likely someone has successfully gone there before and is willing to help. It’s a lesson that Assistant Vice President for Information Technology with the Securities Investor Protection Corporation Bob Ferry learned during his organization’s cloud journey.

“Find help from someone that has done it before,” Ferry advised. “We brought on board a systems integrator because while there is a lot to be said for learning while doing, when you are moving your security stance from on-premises to cloud, you don’t want to do it for the first time alone. I suggest you align with a trusted partner that has seen the potholes and knows how to avoid them, and have them help you through that process.”

Perspecta demonstrates what it takes to assemble such partnerships and capabilities. Over 14,000 information technology (IT) and cybersecurity professionals are continuously developing new IT and cybersecurity innovations to enhance digital transformation and data security for our U.S. federal, state, and local government customers nationwide and internationally.

Perspecta both creates and leverages cybersecurity innovations through: internal independent research and development (IRAD) program; the Cyber Forensics Lab, an extensive Perspecta network of University alliances; strategic business partnerships with leading technology companies; and the nationally-recognized Perspecta Labs, with over 350 top information technology and communication scientists and engineers, who have been awarded over 280 technology patents. Perspecta Labs serves as a leading provider of cybersecurity research and development (R&D) for the Defense Advanced Research Projects Agency (DARPA), U.S. Army Research Labs (ARL), and the Intelligence Advanced Research Projects Agency (IARPA).

These are the kind of capabilities and partnerships needed to secure critical infrastructure ecosystems.

To further explore, Perspecta shares 2021 Top 10 Cybersecurity Trends and Proactive Cybersecurity Recommendations for our critical infrastructure ecosystem.