protiviti®
Face the Future with Confidence

The Biden administration's executive order on cybersecurity and possible effects for financial services firms

Safer supply chain, more information sharing, additional compliance

Having faced more cyberattacks than other sectors, banks and other financial services firms have been at the forefront of the fight against cybercrime in recent years. To protect themselves, banks have substantially invested in cyberattack prevention and increased their incidence-response capabilities.

The U.S. government has also been involved increasingly in this fight. The president's May 12 executive order announcing new measures on national cybersecurity is, in many respects, a war cry, escalating the government's willingness to take a stronger leadership and coordinator role in the struggle. In that call to arms, the executive order also laid out specific ways the administration will try to improve the nation's cybersecurity defenses. Many of these measures require additional efforts by the private sector. As expected, we are also seeing continued focus from regulators that further the cybersecurity discussion. Most recently, the Federal Financial Institutions Examination Council (FFIEC), which sets standards for regulatory examinations of financial firms, updated guidance on Authentication and Access to Financial Institution Services and Systems, the first notable update on the topic in a decade.

The impact on the financial services industry will come in two ways. The direct impact will result from banks and other financial services institutions that do business with the government having to comply with specific new measures and reporting requirements. The indirect impact will be the potential improvement in the security environment that these measures will likely produce.

Even though financial services organizations are not typically thought of as government contractors, they do in fact provide services to the government, whether it's servicing loans secured by government-sponsored mortgage lenders, marketing Treasury bonds or insuring government employees. Those types of services will force banks, insurance companies and other financial services firms to comply directly with some provisions in the executive order that are targeted at government contractors.

One of those increased requirements is quicker reporting to the government of cybersecurity breaches. Financial services firms already comply with strict reporting requirements due to rules enacted by states, as well as market and other regulators. The executive order will create additional compliance work for financial services firms, though, because they will have to report incidents to a proposed new government agency in addition to those governing bodies they are required to report to now. Furthermore, already existing regulations and standards aren't crystal clear on what constitutes a cyber breach in terms of reporting requirements, and the executive order may add new elements to the existing debate on what needs to be reported in a timely fashion.

The indirect impact of the executive order on the financial services industry will be mostly positive as the industry will benefit – like other industries – from the overall improvement in cybersecurity standards. The president's executive order focuses on the information and technological supply chain for the government. The Commerce Department will be developing new criteria for software security, which hardware and software developers will have to abide by going forward. Since financial services firms also rely on the same suppliers for much of their equipment and applications, the improved security standards will provide a safer supply chain for the industry as well as the government.

Banks, regulated much more strictly than most other industries, have had to comply with cybersecurity standards for many years. While regulators couldn't directly set rules for a bank's suppliers, regulators do examine many of these suppliers and wield significant influence in vendor selection. Further regulation of the supply chain thanks to the executive order will be a welcome security improvement for the industry and its regulators.

Another section of the president's order aims to remove barriers between the public and private sectors for sharing information regarding cyber incidents and criminals. Cybersecurity executives in the financial services sector have traditionally complained about the lack of government information flowing to them, even as they've increased the amount of data they

share with agencies over the years. Even though the intent has been there, structural hurdles – such as intelligence agencies still keeping analog records while banks have all switched to digital – have prevented this information exchange from being truly bidirectional. The executive order could help push government departments to do more to remove those hurdles and improve the communication between public and private sectors regarding cyberattacks.

In summary, the May executive order may add some new compliance requirements to the cybersecurity responsibilities of financial services firms, but it will mostly mean better resources in the firms' struggle to fight the bad guys, who never stop upping their game.

About Protiviti's Financial Services Industry Practice

Disruptive technologies, evolving customer loyalty and pressure to enhance economic returns define just some of the challenges financial services organizations need to overcome by innovating and managing risks in order to succeed over the next decade. The dynamic regulatory landscape and increased emphasis on cost reduction only adds to the complexity of financial services organizations achieving profitable growth.

Protiviti's global financial services team brings a blend of proven experience and fresh thinking through a unique 50/50 mix of "home grown" talent combined with former industry professionals, including risk and technology executives, commercial and consumer lenders, compliance professionals, and financial regulators.

As a major global consultancy, we have served more than 75% of the world's largest banks, many large and midsized brokerage and asset management firms, and a significant majority of life as well as property and casualty insurers, solving our clients' issues across all three lines of defense of the business to meet the challenges of the future, today.