Cybersecurity for Institutional Investors:
Resources Protecting You in Cyberspace

Cybersecurity should be a top concern for all institutional investors. Bad actors continue to find innovative ways to use ransomware and other techniques to gain access to systems and data for malicious purposes.

In the first part of this series, we discussed the basics of ransomware, trends, notable examples of recent attacks, and how to guard against attacks. In this second part, we spoke with Murray Kenyon, Information Security Director with the Information Security Services team at U.S. Bank, in an effort to better understand U.S. Bancorp Asset Management's (USBAM) cybersecurity infrastructure and what it means for the public sector investors served by PFM Asset Management (PFMAM).

Can you summarize the breadth of resources USBAM dedicates to cybersecurity?

Kenyon: U.S. Bank employs a Defense-in-Depth approach. This includes devoting hundreds of staff across the globe to protect the Bank.

We accomplish this through a combination of active cyber defense mechanisms, secure software and architecture solutions, and security consultation with partners across the entire range of information technology (IT) operations. It also includes a range of other risk management assessments and evaluations, as well as ongoing management of compliance with Information Security policies and regulatory requirements that align with rules, laws, and industry best practices.

What are the most significant cybersecurity threats facing institutional investors?

Kenyon: Cybersecurity threats run the gamut from social engineering attacks, business email compromise, malicious software (malware), ransomware, and cyber-enabled scams. As ubiquitous as Artificial Intelligence (AI) has become in our daily lives, it's not without its risks; it can generate text, images, audio (voice cloning), and videos (deepfakes) that can be used to deceive authorized users, thus enabling unauthorized access to networks and business processes. Regrettably, in the present environment, the weakest link in the security chain is the human who accepts a person or scenario at face value.

How does our cybersecurity strategy align with broader public sector risk management goals?

Kenyon: U.S. Bank is an Executive Member of the Financial Services Sector Coordinating Council (FSSCC), a high-level platform for collaboration with the federal government departments and agencies that oversee the financial sector. Through the FSSCC, member institutions work with the federal government to develop joint risk management policies, positions, and goals. By remaining engaged with other members of the government and the financial sector through FSSCC, Trade Associations, and other forums, we can work toward broad alignment within the public and private components of the financial sector on priorities and goals.

What regulatory requirements must USBAM meet, and how does it stay compliant?

Kenyon: U.S. Bank rigorously adheres to regulatory requirements across our footprint, encompassing those set forth by the Federal Financial Institutions Examination Council (FFIEC), Securities and Exchange Commission (SEC), U.S. Government Publishing Office (GPO), and regulatory bodies in Canada, the European Union, the Central Bank of Ireland, the Bank of England, and Japan. Our commitment to regulatory compliance is reflected by our strong compliance teams. Despite the ever-evolving regulatory landscape, USBAM maintains a collaborative regulatory change management program and conducts comprehensive enterprise

compliance assessments to evaluate and monitor our regulatory compliance environment.

How does strong cybersecurity contribute to the long-term value and stability of investments?

Kenyon: Robust protection of IT networks minimizes the risk of unauthorized access, operational degradation, or out-and-out compromise of the Bank's sensitive data through cyberattacks. Protecting cyber networks in this way reduces risk to the institution's value, stability, and reputation as it helps safeguard the Bank's business processes so that they may be conducted in a secure network environment.

What role does artificial intelligence play in our cybersecurity defenses?

Kenyon: The U.S. Bank artificial intelligence ecosystem is based on cross-organizational collaboration and transparency between technology, information security, legal and other risk disciplines. Despite the risks of AI in the hands of bad actors, we can leverage AI to augment and strengthen the resilience of our resources and more rapidly identify and prevent cyber threats to our critical infrastructure. We use AI to increase the speed and ability to mitigate cyber threats, enhance defensive capabilities through automation and orchestration, and improve advance notification of attacks.

What emerging technologies or trends are shaping the future of cybersecurity in institutional asset management?

Kenyon: Quantum computers can perform certain mathematical functions (e.g., calculations, simulations, and advanced modeling, etc.) exponentially faster and more efficiently than a standard computer. This allows enhanced threat modeling and simulations, faster processing, enhanced financial modeling, and more complex computations. However, it can also result in bypassed firewalls and controls, broken encryption, increased third party risk, and loss of customer data and trust.

For questions about this report, please reach out to your relationship manager.