



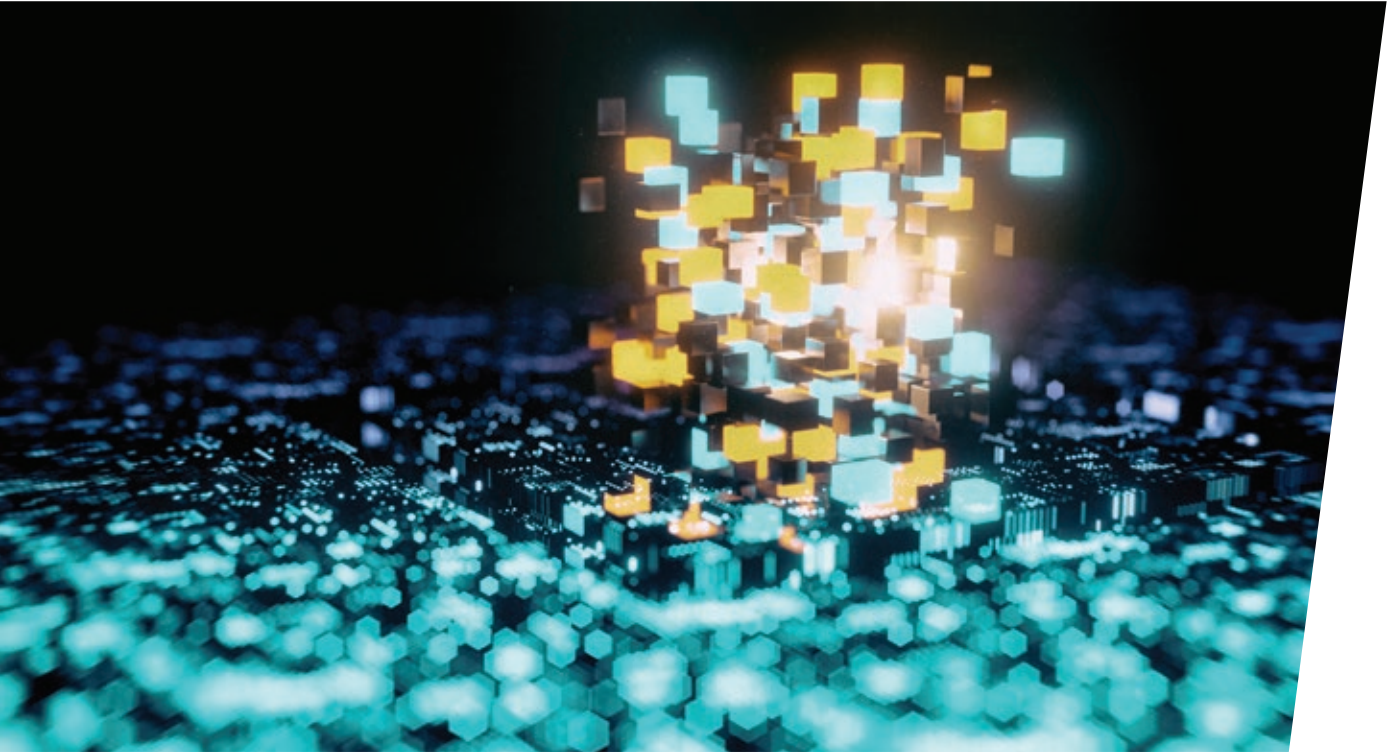
KORN FERRY®

Perspectives

SECURE YOUR ASSETS

With more money and competition than ever before, asset management firms are increasing their focus on cybersecurity to meet market pressure and consumer demand.





The problem:

Increased use of data and AI, more external partners, and more sophisticated cyberattacks are creating immense pressure on asset management firms to protect assets and brand integrity.

Why it matters:

Investors are more concerned and educated about cybersecurity than ever before.

The solution:

Leverage investments in talent and technology to differentiate cybersecurity operations, which will help attract and retain clients.

One of the most sophisticated cybersecurity operations in the world is housed inside a massive skyscraper in downtown Manhattan. The command center features a wall of monitors flashing red, yellow, and green lights blinking with the frenzy of a video game. The lights show firewalls being bombarded with constant penetration attempts. Each blink is analyzed and correlated with hundreds of other data points in real time to determine the level of significance as to which breaches need an immediate response and which barely need attention.

But this isn't a national security or defense command center. Nor is it part of the NYPD. Rather, it's the cybersecurity command center for a global financial services firm with a significant asset management business.

Welcome to the new world of asset management. "Investors, CEOs, and boards of directors are more concerned and educated about cybersecurity than



ever before,” says Craig Stephenson, a senior client partner and managing director with Korn Ferry’s Technology Officers practice in North America.

That’s putting it mildly. A confluence of factors—among them a massive increase in the use of data, artificial intelligence, and machine learning, as well as a move to cloud-based storage—means that investor assets are now managed by more than just asset management firms. Moreover, an increasing reliance on external partners, a regulated operating environment, and more sophisticated state-sponsored attacks are creating immense pressure on firms to protect assets.

“Data is the backbone of what we do and how we make business and investment decisions. Because it also resides with our external partners, we require from them proper cybersecurity controls,” says Henrique Francisco, chief technology officer at PineBridge Investments, a global asset management firm with roughly \$100 billion under management.

Global assets under management are at an all-time high of nearly \$90 trillion, with industry profit about half that amount. At the same time, however, digital transformation is shrinking management fees and compressing profit margins for firms. With the difference between making and losing millions of dollars a mere millisecond, firms are pouring tens of billions of dollars into digital technology. While in the past that investment would be focused on lowering costs and executing trades faster, now an increasing share of it is going toward hiring talent and developing systems to protect against digital malfeasance. After all, a firm could lose as much from a security breach, if not more, just as quickly and easily as it can from a poor trading strategy.

“The more ways to analyze data the better given the sophistication of cyberattacks.”

”

As the asset management industry matures, it is becoming more and more difficult for firms and managers to differentiate themselves, says Chad Astmann, a senior client partner and global cohead of the Asset and Wealth Management practice at Korn Ferry. Recently, for instance, brokerage firms such as Charles Schwab, TD Ameritrade, E-Trade, and Fidelity Investments all announced plans to eliminate the fees they charge clients to execute stock trades.

But with only so much firms can do to differentiate themselves on pricing, and only so much disparity between investment products and advisory services they can offer without confusing customers, asset management leaders are looking for other ways to stand out to attract investors. Increasingly, they are turning to cybersecurity as their calling card.

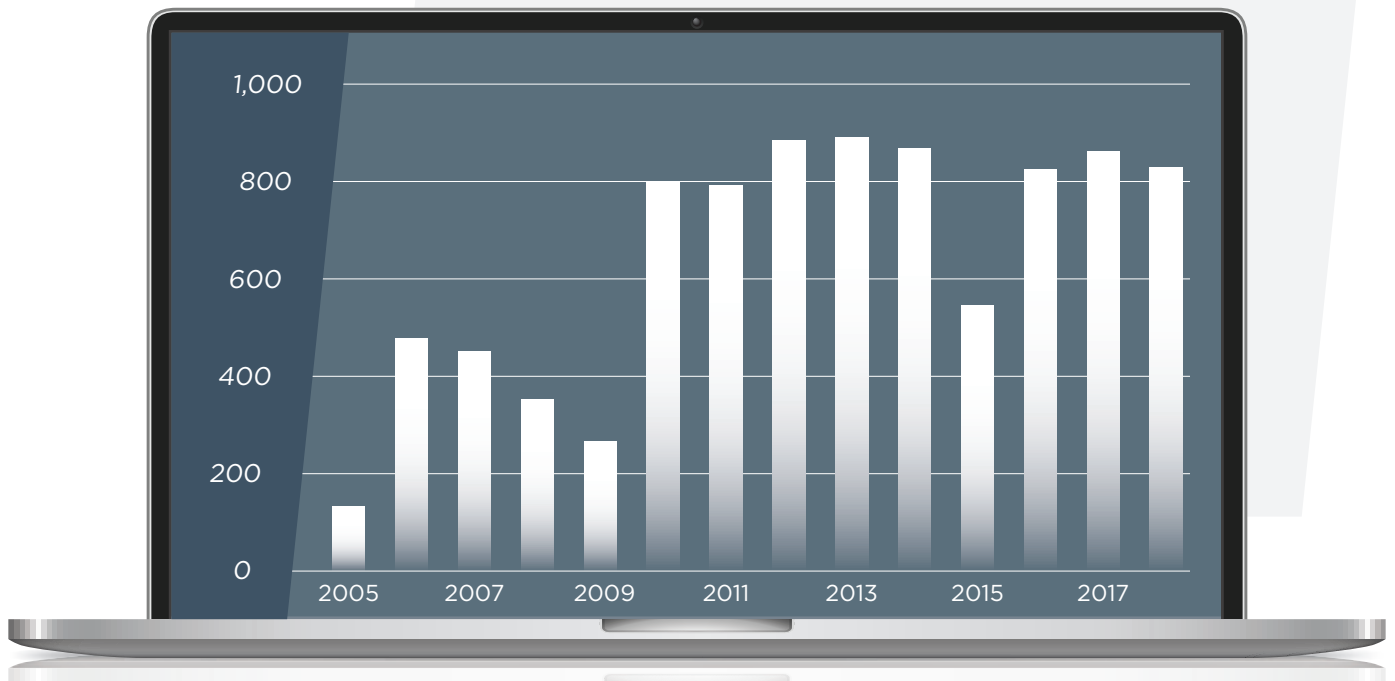
“Substantial, highly capable cybersecurity operations can certainly differentiate firms and help evolve their business models to meet market pressures and consumer demands,” says Astmann.

Unreliable Reporting

One of the biggest issues with assessing the number and scope of cyber breaches is timely reporting by organizations. As the chart below shows, breaches have clearly increased since 2005, though one can safely assume the number of actual incidents is even larger than what's been reported.

Cybersecurity breaches that were made public, 2015-2018

Number of breaches



Sources: Privacy Rights Clearinghouse; CEA calculations.



“Highly capable cybersecurity operations can certainly differentiate firms to meet consumer demands.”

According to the World Economic Forum, 82% of the leaders surveyed for its latest Global Risks Report believe cyberattacks leading to financial theft or data fraud will increase this year, citing the “deepening integration of digital technologies into every aspect of life.” To be sure, with trades and portfolio management being executed more and more via mobile devices, every tap on a smartphone increases the chance of a security breach.

The combination of digital advances and changing consumer behavior means asset management firms are dealing with a multitude of outside vendors. The more partners involved, the more vulnerable firms are to breaches, which means they need to do more vetting of vendors and put more protocols in place to oversee them. Korn Ferry’s Stephenson says the complexity of oversight means cybersecurity leaders need to work in unison with previously isolated and disparate functions to mitigate threats. One way to foster collaboration is through the development of “fusion centers” like the one in downtown Manhattan.

“These centers sit a layer above cybersecurity by fusing together siloed functions to create better intelligence gathering, faster response times, and more accountability,” says Stephenson, noting that such centers are growing rapidly throughout the financial services industry. They also serve as a nice “differentiation factor” to show off cybersecurity capabilities to attract or retain clients. The downtown Manhattan center, for instance, not only allows for easier collaboration with internal and external stakeholders across the organization, but also invites clients to tour the facility when in town, showing off the firm’s focus on safety and security.

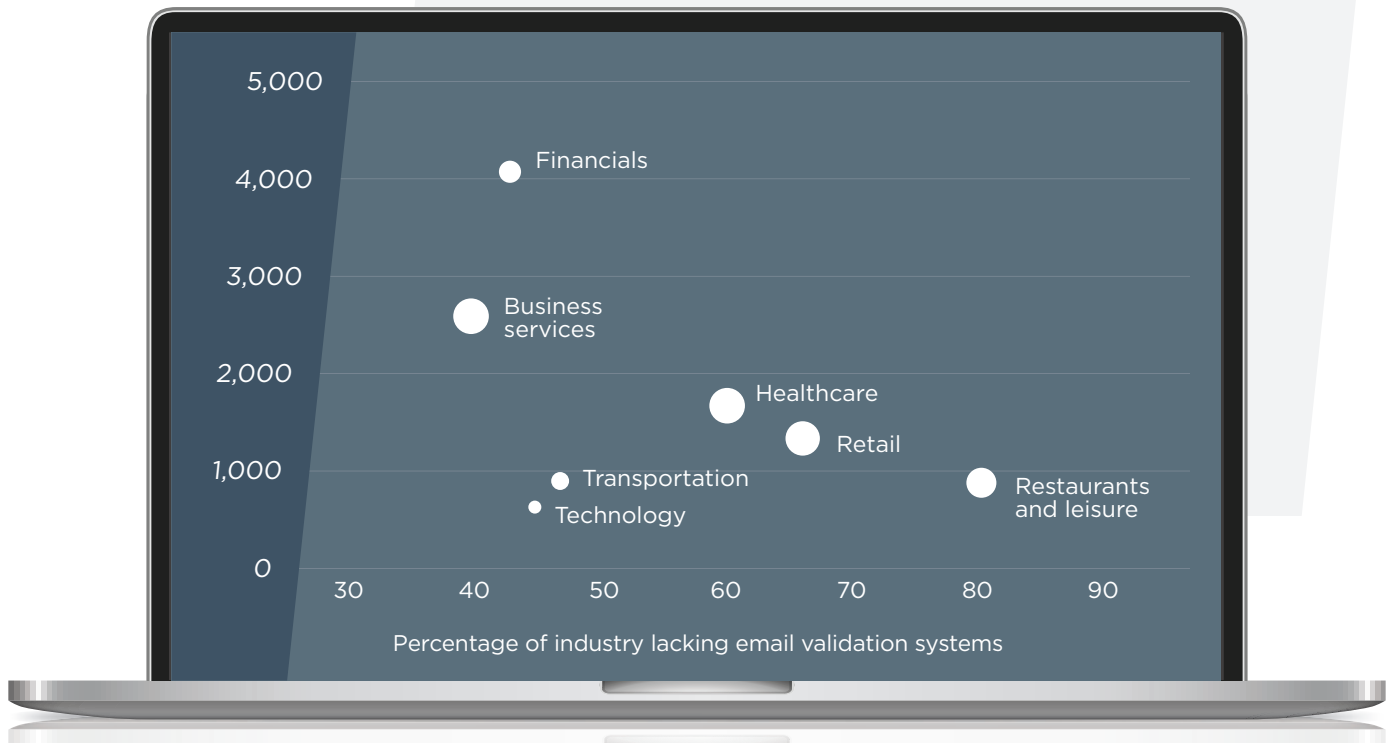
More importantly, from a talent perspective, bringing together this wider range of experience and skill sets creates diversity in how the same data is viewed. “The more ways to analyze data the better given the sophistication of cyberattacks,” says Stephenson.

Go Phish

According to the 2019 *Economic Report of the President*, despite being the most valuable industry among Fortune 500 companies measured, more than 40% of financial firms lack basic protocols to authenticate whether an email message is legitimate or a spam or phishing attempt.

Industries that are most lacking email validation systems among Fortune 500 companies by value added, 2017

Value added by industry (billions of dollars, 2017)



Points are scaled by industry employment in 2017, and only the top 10 sectors (ranked by employment) are plotted.

Sources: Rapid7; Bureau of Labor Statistics; Bureau of Economic Analysis; CEA calculations.



The best evidence for how big of a concern cybersecurity in banking has become came on April 10, 2019. On that date, roughly a decade after the financial crisis, the CEOs of the seven largest banks in the United States appeared before the House Financial Services Committee. During the nearly six hours of testimony, ostensibly about how the banking system has evolved since its near collapse, the issue of cybersecurity upstaged all others, being mentioned literally hundreds of times during the proceedings. When asked what was the most prominent threat to the financial system, for instance, most CEOs cited cybersecurity. State Street Corp. CEO Ron O'Hanley called cyber risk a "clear and present danger" that requires banks and regulators to cooperate.

But while bank CEOs testifying before Congress about cybersecurity risks conjures up images of state-sponsored attacks meant to bring down the financial system, in reality the clearest threat is among employees. Across industries, current employees commit 34% of all cybersecurity breaches, and former employees commit 29%.

Many breaches result from the most basic of mistakes, such as opening a phishing email that downloads malware on the firm's systems or sending sensitive or classified data over text or internal group chats. "The most important protection is training," says Daniel Longmuir, chief technology officer at Cohen & Steers, an asset management firm of more than 300 people and \$70 billion in assets. Longmuir says phishing exercises are an absolute must, for instance, and the more frequent and sophisticated the better. "We need to constantly monitor how our people are behaving and communicating electronically," he says.

"The most important protection is training."



Korn Ferry's Astmann says there is a major push among asset management firms to drive talent at all levels of the organization to own cybersecurity personally. "Firms realize they can't rely solely on the cybersecurity team and that they have to build a security culture," he says.

To be sure, PineBridge Investments' Francisco says anyone who designs a piece of software needs to have a security framework in mind. And he has a test to see if they indeed do. He says during the interview process he always asks candidates to tell him how they would secure the systems they build. It's a seemingly simple question, but Francisco says the open-ended nature of it allows him to assess how much and at what level a candidate thinks about security.

"Some will say they don't think about it, that the operating and cyber teams will provide support, while others will say it is critical to the design process," says Francisco, whose firm employs around 700 people who manage roughly \$100 billion

in assets. "The question can go anywhere, and the answer gives insight into the candidate's mindset around security."

From a leadership perspective, Korn Ferry's Stephenson says firms are also putting a lot of focus on broader change-management efforts. Historically, cybersecurity talent is siloed, with a lot of deep experience in one particular area but not much across functions. To be effective today, however, cybersecurity leaders must be able to

assess technology risk across ever larger and more complex ecosystems. In order to get potential leaders that necessary experience, firms are increasingly employing rotational assignments. Moving talent through a variety of functional domains—e.g., from the network team to the business continuity team to the action and response team—helps

"We need to constantly monitor how our people are behaving and communicating electronically."

to rapidly evolve culture and establish common goals and objectives. "Rotations help give potential cybersecurity leaders the enterprise perspective necessary to manage in highly dynamic environments," says Stephenson.

For more information, contact Craig Stephenson at craig.stephenson@kornferry.com or Chad Astmann at chad.astmann@kornferry.com.