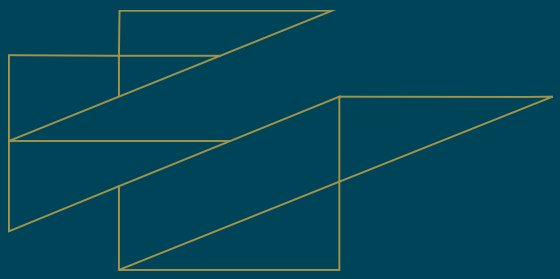
BNY MELLON | PERSHING



Cybersecurity in an increasingly complex world

SAFEGUARD YOUR BUSINESS AND YOUR CLIENTS FROM CYBERCRIME

Thieves have been trying to break into banks to steal money long before the Internet. At the time, thick concrete walls and heavy metal doors were among the strongest defenses against crime. Today, your clients' assets can be placed at risk because theft can take place practically in thin air as cybercriminals use technological means to steal information or assets. Although technology is making it easier to rebalance portfolios, draw up financial plans and communicate with clients, it's also creating a new set of challenges to defend against in your practice.

The perpetrators of cybercrime are not only keeping pace with advancements in technology, but they are also often on the leading edge – and the stakes are high if you don't take appropriate steps to protect your systems. When you're responsible for someone else's wealth, the risks extend far beyond the possibility of actual money being stolen: the reputational damage it may cause you and your firm can be even more devastating.

Cybersecurity breaches come in several forms, be it a virus infection through email, the introduction of fake, malicious websites (malware), the implementation of phishing schemes or other applications that might expose framework or system vulnerabilities. The attack may attempt to exploit internal and third-party provider vulnerabilities for financial gain or cause business disruption.

There is a growing imperative for advisors to embrace change and adopt new technologies, yet RIAs may not have a large technology infrastructure supporting them. The challenge will be for RIAs to ensure that their practices and their clients don't become the targets of cyberattacks.

With the constant threat of cyberattacks, it's not surprising that financial services firms are expected to continue ramping up cybersecurity spending, which could reach $43 billion globally by 2023.[1] For larger firms, added costs are painful but not prohibitive; the same cannot be said for smaller firms and RIAs.

Yet, as evidenced by recent breaches, the cost of inaction can be even higher. In recent years, highly publicized cybersecurity breaches have made the news. Target Corp. endured one and so did Equifax Inc. – just to name two high-profile cases. In 2017 alone, the average cost of a data breach was $3.62 million.[2] Financial services firms understand it is a priority to uphold effective cybersecurity policies, and that consequences will ensue if they don't.

For the past eight years, the Office of Compliance Inspections and Examinations (OCIE) for the U.S. Securities and Exchange Commission (SEC) has placed cybersecurity on its examination priority list. Recently, the OCIE released its cybersecurity and resiliency observations, which provide practical guidelines of what to look for and what the OCIE has been observing in the advisory industry. For instance, the OCIE noted that effective cybersecurity programs greatly benefit from a commitment by a firm's senior leadership to understand cybersecurity risks and prioritize the communication of these risks across the organization so they can mitigate them. Robust risk assessments, strict access controls and comprehensive testing of cybersecurity programs and systems are three of the best practices to follow.

Recognize your vulnerabilities

Using technology to fight technology offers a layer of protection, but technology alone isn't the answer. Advisors also need to be aware of the threats and vulnerabilities they're up against so they can know how to guard against them in order to protect themselves, their firms and their clients.

Ransomware

One major theme pertains to ransomware, where criminals threaten to publish the victim's data or prevent access to this data unless the victim relents to a specified financial transaction (known as a "ransom"). These actors typically demand wire transfers or other electronic means to extort money from the victim, as digital methods are harder to trace.

For issues like ransomware, it's critical to have reliable offsite backups and a business continuity plan that incorporates the use of those offsite backups. If an actor encrypts all your data or denies access to your servers, then you can use your backup to safely restore your systems. Although disruptive, it means you can resume business operations through another provider until your ransomware issue is resolved.

Denial of service

An important but often overlooked topic is the denial of service. That's when actors will initiate disruptive actions like overloading your network traffic or send innumerable requests in an attempt to deny people from getting work done. For example, Robinhood Financial experienced a massive service outage during a steep market decline, but nobody on Robinhood's system could execute a trade. So, the firm faced legal action by clients who lost money when they couldn't make trades as markets plummeted.

Robinhood identified the situation as a system malfunction, but it's also possible that someone flooded its system's front-end interface or inundated its website with traffic, denying access to anyone else. Larger firms have intricate filtering services and implement denial of service controls to address such problems.

Stolen credentials

Whenever you send client information, failing to conduct the proper checks and follow established security procedures can leave this sensitive data vulnerable. One of the most common cybercrimes involves people who pose as clients by stealing their credentials. The criminals try to lure you into communicating with them instead of the actual client to trick you into sending them a client's personal information.

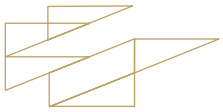
In addition to limiting the exchange of client data, one of the best ways to protect yourself from criminals who pose as clients is to be trained on the latest techniques and approaches that criminals use so you can recognize scams and avoid falling victim to them.

Good cybersecurity is more than technology

Combatting cybersecurity issues requires significant training and awareness, both internally for firms and for clients. It extends beyond technology and involves vigorous, up-to-date education. The SEC has recommended that firms address governance and risk management, which involves having senior-level engagement in cybersecurity and resiliency strategy.

An important element of a cyber resiliency program is developing and conducting risk assessments. List your actual and potential cyber risks, where these risks may exist and what issues they may cause. Aside from technological aspects like firewalls and access controls, a good risk assessment involves understanding risk mitigation processes. For example, do employees know their role in cybersecurity? If an employee is a point of escalation, he or she should know exactly what the next steps would be if an escalation occurs.

Another valuable non-technology action is regular testing and monitoring of the entire cybersecurity program to ensure all measures remain relevant and effective. A firm's cybersecurity program includes comprehensive policies and procedures that must be



clearly documented. To validate the effectiveness of these policies and procedures, the firm must adopt a robust testing, monitoring and evaluation regimen – on both a scheduled and unscheduled basis – using available cyber threat intelligence to help set parameters. If any audited policies or procedures fail to fulfill their cybersecurity functions, the firm must promptly address those systemic gaps or deficiencies.

Securing the home office

With many people working from home on an ad-hoc basis or as part of their regular work schedules, a major challenge is taking extra care in managing information. At the workplace, you're inside a secure enclave with the ability to protect client information. At home, if you print sensitive files, assemble folders for clients or have paper containing sensitive client information, you must follow established protocols to protect the data.

Practice vigilance with passwords

We encourage using one-time passwords (part of two-factor authentication), in which a person logging into an account will receive a text message with an authenticating number to use. That extra layer of security helps reduce account takeovers as cybercriminals can't easily take over these accounts because access relies on more than a single password.

Recently there has been a significant attitude shift toward one-time passwords. Most people still consider the practice to be bothersome, but they recognize its importance for good cybersecurity and accept it.

Security tips for working from home

1. As a general rule, minimize printing. When you must print sensitive paperwork, dispose of it by shredding or locking it up to prevent misuse.
2. Think of your home as an extension of your workplace and adhere to the same risk protocol. If possible, work in a space that can be properly secured.
3. Examine how you're accessing your work systems. If using a personal computer, it may not have the same level of security controls as your machine at work, so install updated anti-virus software and other base controls.

Tips for firms with employees working from home

1. Consider instigating system controls to prevent remote printing and utilize encryption technology to protect the exchange of data.
2. To prevent unwanted access, promptly revoke all credentials of employees who have left the company and purge inactive accounts to remove them from your system.

Potential consequences of cybercrime

On top of ransomware issues and phishing expeditions, vulnerabilities exist when people use third-party vendors. If a vendor encounters a cybercrime, advisors need to assess their vulnerability. What customer account information is out there and what other sensitive information is shared with that vendor?

Advisors who don't take adequate cybersecurity measures could lose a lot of money – and their businesses. When a trade is missed or a client claims something wasn't done properly, the client will need to be made whole again. So there's real money at stake for advisors and their firms. If you encounter a ransomware situation, not only would you be unable to conduct business, but you could also lose significant money in fines and credit monitoring, given that client data might be at risk of being lost and misappropriated.

Although there are financial consequences if you fail to sufficiently protect your clients, there may also be a reputational consequence that could severely harm you and your firm's brand and compromise the trust you've established with clients.

Regulatory consequences of cybercrime might result in anything from a fine to extra disclosures, but these are clear and finite penalties. A reputational loss, however, is harder to quantify and difficult to overcome. Clients are more educated than ever and will ask questions about system safety measures for ensuring the confidentiality of personal data. Increasingly, clients understand the importance of cybersecurity and the value of keeping their information secure. If you don't deliver on your security commitments, your reputation (and your firm's) may be damaged, and in today's connected world of mass media and social media, the damage may be substantial.

Be educated and prepared

How do you maintain good cybersecurity practices? It's an ongoing process. Advisors can take proactive measures to help protect clients. Being educated is crucial and advisors need a robust cybersecurity program to reference and follow. The OCIE has created a basic framework regarding the need for implementing strong technology, policies and procedures. Also, consider your resiliency program because you will likely have to deal with cybersecurity threats at some point.

Cybercriminals are getting smarter and more deceptive, with access to better technology and tools. The more you and your firm educate yourselves, the more you can do. Keep apprised of the SEC's releases and what they're saying. The SEC recommends sharing information through its financial services information sharing and analysis center.

Compare the National Institute of Standards and Technology's (NIST) cybersecurity framework to your own, as the NIST framework is worth emulating. Another useful organization to reference is the American Institute of CPAs (AICPA). The AICPA's System and Organization Controls reporting framework enables organizations to communicate information about their cybersecurity risk management program to help satisfy stakeholder cybersecurity information needs.

It's also strongly advised to designate at least one person at your firm to stay current with cybersecurity news and trends. Sharing information lets you learn about other firms' experiences and exposes you to best practices that you can adapt. There are no one-size-fits-all cybersecurity solutions, so be aware of what's out there and customize relevant practices for your firm.

Good education, awareness and training also allow you to take immediate action if a cyber breach occurs. If you're scrambling when you encounter some type of failure, that's a problem. Have a robust plan and test it often. You should have a clear plan of what you need to do, what systems are affected, which people to engage and what notifications to issue. Gather as much information as you can to make the best decisions possible.

Your set protocol for dealing with cybersecurity issues may include notifying your vendors, partners and internal team. Will there be a shutdown? If so, what's your contingency plan

and how does that roll out? If you work with a partner (such as BNY Mellon's Pershing) and advise that you've experienced a threat or successful cybersecurity issue, what can be done if you're offline? What can your partner do, what do you need to know and whom should you contact? Those are questions you must answer to help inform a robust resiliency program that can keep your firm and clients protected.

Assessment checklists are crucial

It's good practice to house your cybersecurity policies and procedures in a comprehensive catalog of risk assessment. Check them regularly and make updates, as required, and make your team aware of these policies and procedures. It's only valuable to have them in place if everyone knows where they are and what they mean.

Going through an assessment checklist – and amending it when needed – should be an annual exercise or performed whenever you experience a notable change (e.g., if you absorb or merge with another business or switch service providers).

> "The Federal Financial Institutions Examination Council (FFIEC) offers a useful security self-assessment. It's a cybersecurity checklist that's available for free on the FFIEC site. We recommend this self-assessment to our broker-dealer clients."
>
> *-Jeffrey Davis*
> *Director, Sr. Group Manager, Information Security, BNY Mellon's Pershing*

How we can help

Pershing is committed to helping clients (and their clients) with cybersecurity. For instance, our leading-edge "rules engine" allows broker-dealers to set parameters. If a transaction is beyond a certain dollar threshold or if a 401(k) account starts making uncharacteristic, high-volume transactions that resemble day trading, the rules engine will flag that and require additional authorization. That's one way advisors and broker-dealers can keep abreast of transactions.

> "The customizable rules engine is part of our system. Our clients can configure it or ask their relationship manager to help with configuration, and they can decide which rules they want to implement and which ones they don't."
>
> *-Nina Weiss*
> *Chief Compliance Officer, BNY Mellon's Pershing*

The rules engine includes a base set of recommended rules – numbering into the thousands – with thousands more from which advisors may select. In addition, BNY Mellon's Pershing Advisor Services takes many actions on the back end to ensure our systems are secure by searching for vulnerabilities through penetration testing and vulnerability scanning. A third party performs assessments on our systems and issues a cyber trust certificate that attests to system security, while our ISO 27001 certification is updated every three years.

Other ways we support you

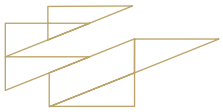
Pershing can help develop and support your firm's resiliency programs, so you have a viable plan that maps out the steps you need to take and the people (such as vendors) you need to contact, as well as determining who needs support in the event of an outage.

For advisors who want to help clients keep their systems secure, we can advise if they need to run the latest anti-virus software, if they should be utilizing factor authentication or one-time passwords, and why they shouldn't use common passwords for different systems. After all, if one of those accounts gets compromised, the cybercriminal may try the same credential against other related accounts.

As a custodian and a partner/vendor with its own stringent risk controls, BNY Mellon's Pershing is well positioned to add a nuanced perspective in this area. As the area of cybersecurity is constantly evolving, we hold regulatory and compliance webinars as an avenue to relay timely information. On our annual security and fraud webcast, we share what we're hearing from regulators, what new cybersecurity rules and regulations might be on the horizon, and common best practices. Whenever we learn anything new, we disclose that in releases to our advisory clients. It's all about providing the best possible technology and support to bolster our clients' cybersecurity.

[1] Rouse, Tim. "Cybersecurity poses strain between plan sponsors, record keepers," InvestmentNews.com www.investmentnews.com/cybersecurity-poses-strain-between-plan-sponsors-record-keepers-78751 (accessed on April 16, 2020).

[2] van Kessel, Paul. "Is cybersecurity about more than protection?" ey.com (accessed on April 16, 2020).



Pershing

BNY Mellon's Pershing and its affiliates provide a comprehensive network of global financial business solutions to advisors, broker-dealers, family offices, hedge fund and '40 Act fund managers, registered investment advisor firms and wealth managers. Many of the world's most sophisticated and successful financial services firms rely on Pershing for clearing and custody; investment, wealth and retirement solutions; technology and enterprise data management; trading services; prime brokerage and business consulting. Pershing helps clients improve profitability and drive growth, create capacity and efficiency, attract and retain talent, and manage risk and regulation. With a network of offices worldwide, Pershing provides business-to-business solutions to clients representing approximately 7 million investor accounts globally. Pershing LLC (member FINRA, NYSE, SIPC) is a BNY Mellon company.

pershing.com

One Pershing Plaza, Jersey City, NJ 07399

WP-PER-WT-01-20