Linedata

7 Cybersecurity Best Practices to Prevent Data Breaches and Regulatory Fines

Fund Managers: Maintain SEC and FTC Compliance with These Essential Cybersecurity Steps

Table of Contents

> *"Investment advisers and broker dealers must fulfill their obligations concerning the protection of customer information. It is not enough to write a policy requiring enhanced security measures if those requirements are not implemented or are only partially implemented, especially in the face of known attacks."*[2]
>
> ***Kristina Littman, Chief of the SEC Enforcement Division's Cyber Unit***

Asset managers face a greater threat from cybercriminals than ever before, due to changes in the cybersecurity landscape accelerated by the pandemic. In fact, cybercrime has increased by 600% since the pandemic started.[1]

At the same time, government bodies like the Securities and Exchange Commission (SEC) and the Federal Trade Commission (FTC) have introduced new cybersecurity regulations and signaled their intention for more stringent enforcement.

If you've seen the recent news about the steep fines for cybersecurity breaches, you know federal penalties can be severe — not to mention the damage to your brand and reputation.[3] The consequences of even one data breach can result in millions of dollars in fines or even the dissolution of your company.[4]

To prevent potentially catastrophic consequences, firms need to ensure their data and confidential information are secure. Unfortunately, what worked ten (or even three) years ago, won't necessarily work today.

1 | Factors That Have Changed the Cybersecurity Landscape

The threat landscape has evolved since the pandemic, and firms must adapt to a changing world. What's different now than a few years ago?

> *"I think this is kind of a watershed moment for the SEC and its cybersecurity oversight."*
>
> ***Sachin Bansal, Chief Business and Legal Officer at SecurityScorecard***

Remote work

When cities locked down due to COVID, employees began to work from home at unprecedented rates. And the easing of lockdowns didn't stop the remote work wave. According to Gartner, 53% of U.S. knowledge workers will work remotely at least one full day per week this year.[5] While many employees love this flexibility, remote work creates more vulnerabilities for cybercriminals to attack.

Increased cybersecurity activity

Partially due to the upward trend of remote work, companies have seen an increase in the sheer volume of cyberattacks. In fact, 81% of global organizations have experienced an increase in cyberthreats since the COVID-19 pandemic.[6]

New leadership in government agencies

Gary Gensler was appointed as SEC Chair in April 2021. Since then, he's announced his intention to expand the commission's regulations relating to cybersecurity, noting its importance to national security.[7]

New regulations and proposals from the SEC and FTC

In addition to the FTC making significant updates to its Safeguards Rule,[8] the SEC announced several proposed rule changes directly dealing with cybersecurity, including requiring firms to report cybersecurity incidents within four business days,[9] provide a detailed summary of cybersecurity policies and procedures,[10] and likely add staff and technology tools,[11] among other actions.

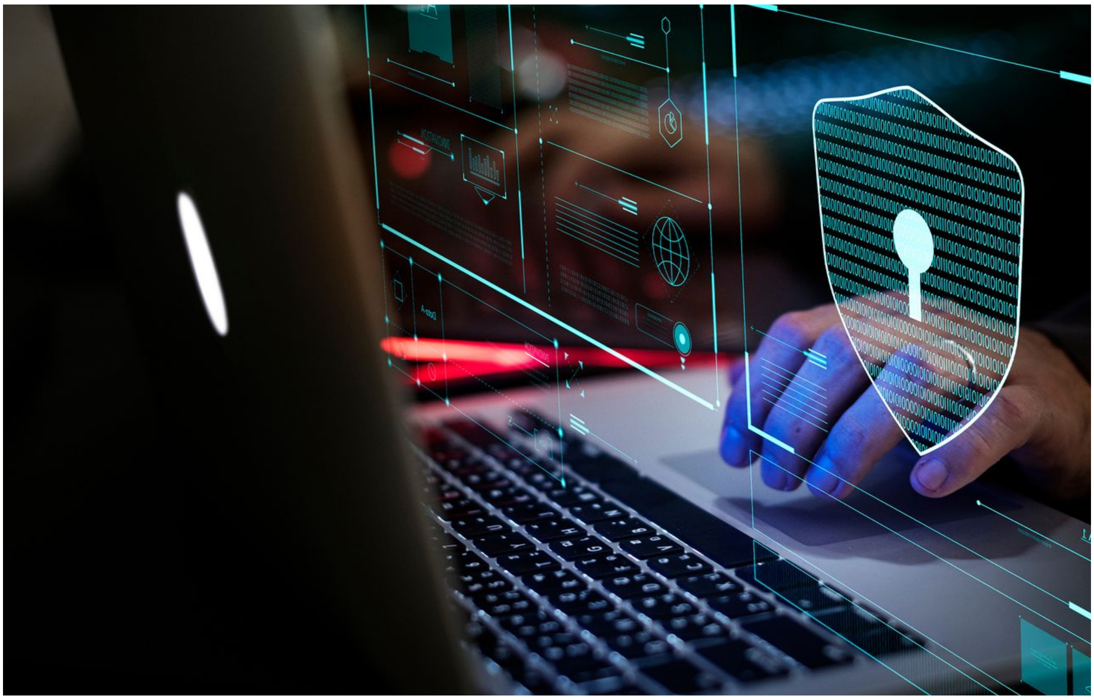
With these changes, companies can't use the same cybersecurity playbook they've used in the past. And fund managers in particular can't afford anything less than diligent cybersecurity measures, given the large amounts of money and other valuable assets they manage and the highly sensitive data they handle.

2 |

The Great Mystery: What to Prioritize in Cybersecurity

As a fund manager, this much is clear: cyberthreats are on the rise, and firms' cybersecurity practices have never been under more scrutiny.[12] It's obvious that you need to prioritize the protection of your digital ecosystem, but the discipline of cybersecurity impacts so many facets of the business that it can be hard to know what to focus on first.

Do you need a financially prohibitive, all-encompassing security solution to protect against the most common cyberattacks? The answer is almost always no. So, what can you do to keep your data — and your clients' data — safe?



Firms can start by adopting proven best practices.

These actions will boost data security quickly and create safe environments without years of planning, preparation, and onboarding.

We'll go through the best practices starting with a focus on end users *(numbers 1-3)* and continuing with organizational best practices *(numbers 4-7)*. As we move through each action, it's important to remember that strong security is about **layers**. No single product or solution will cover all of your systems and keep them protected. You need to think about each solution as a spoke in your cybersecurity wheel. They all work together to strengthen your organization's protection.

Now, let's dive into the 7 cybersecurity practices you should prioritize first.

1. Multi-Factor Authentication

Multi-Factor Authentication (MFA) is when an application, online account, or VPN requires two or more independent credentials to verify a user's identity for access. It is a fundamental building block of modern cybersecurity.

The reality is that authenticating users with the traditional model of a username and password is no longer secure enough to protect against today's sophisticated cybercriminals. Using readily available systems and technology, these nefarious actors can easily hack your passwords and infiltrate your systems. In fact, according to a Verizon study, 80% of hacking-related breaches are linked to passwords.[13]

> *"Based on our studies, your account is more than 99.9% less likely to be compromised if you use MFA."*
>
> ***Alex Weinert, Director of Identity Security, Microsoft*** [15]

So what happens if a hacker gains access to an account in one of your systems? For starters, they can view and share highly confidential and sensitive data, which sits in your systems and is too often transmitted via email. With this data, criminals can plan a whole host of attacks, all meant to steal funds, compromise company secrets, and damage your brand.

With multi-factor authentication, firms have an extra layer of protection to defend against account takeover or account compromise. Using MFA has the same effect as adding six characters to every password and changing each password every 30 to 60 seconds.

So even if your team has a password written down on something as insecure as a sticky note — which 42% of IT professionals admit to doing — your systems will maintain their security.[14]

2 Reasons
Why MFA is So Effective

Multi-Factor Authentication:
- Effectively adds 6 characters to every password
- Changes the password every 30-60 seconds

How can you initiate this practice?

There are several ways to implement MFA. Perhaps the most well-known method is by having a text message sent to the user's mobile number for additional authentication. However, when using text-based identification, you risk falling victim to a SIM swapping scam,[16] so using an app or a push notification is the safest route.

2. Phishing Training and Testing

Individual users are the weakest link in any security solution. With more users working remotely since the pandemic, phishing attacks were up 22% in the first half of 2021.[17] And gone are the days when a user actually had to click a suspicious link in an email to initiate the phishing attack. With today's advanced techniques, a user need only open a phishing email to activate the intrusion.

That's why phishing training is so important. To prevent breaches, your users — both internal employees and external or third-party users — must understand:
- What are phishing emails?
- How do you identify phishing emails?
- What do you do when you receive a suspicious email?

Why is preventing phishing attacks particularly crucial for fund managers? Well, the ultimate goal of any phishing attack is to monetize the exercise — either through ransomware or by diverting funds. When your business is based around managing funds, you quickly become a target. And if your business involves cryptocurrency, look out. Cryptocurrency cybercrime hit an all-time high in 2021,[18] and several high-profile attacks in the first half of 2022 have highlighted the vulnerability of this asset class.[19]

What Phishing Training Entails

- Control CEO fraud
- Control SIM swapping
- Set up secure passwords
- Enable secure remote access
- Protect their environment

How can you initiate this practice?

Many small or midsized firms don't have the legacy systems or experienced personnel in place to train against sophisticated phishing schemes on their own. Typically, it makes sense to leverage the expertise of an external partner for phishing testing. The right partner will have proven training protocols and a deep understanding of the latest phishing techniques.

In addition to training and education, an external partner can provide testing to ensure organizational compliance. Testing at regular intervals (quarterly is common), and the training you provide for your employees can mean the difference between a quickly resolved incident and a disastrous data exfiltration.

3. Endpoint Security

Endpoints (devices such as desktops, laptops, and mobile devices that end-users utilize to access your network) are any organization's most vulnerable entry point. In fact, a recent report noted that 70% of all breaches originated at an endpoint.[20]

The problem with today's remote work business culture is that endpoints are no longer housed under the security umbrella of the office environment. So the risk of malware and other malicious activity has increased.

68% of organizations have experienced one or more endpoint attacks that successfully compromised data and/or their IT infrastructure. [21]

Traditionally, endpoint solutions have consisted of antivirus programs, web and email filtering, and firewall services. While each one of these solutions can be effective for individual users, they don't create a sturdy enough defense for asset managers. Firms are consistently targeted in attacks, and the stakes for security failures are too high. Combining endpoint protection with monitoring and remediation typically makes the most sense for asset and fund managers.

How can you initiate this practice?

You want to implement an endpoint security solution that can intelligently understand the actions taken at the endpoint whether these are connected to the corporate network or connected to a home WiFi.

The solution should have the capability to detect, analyze, and stop malicious actions, and isolate the endpoint until remediation takes place to avoid any production impact.

Now that we've looked at endpoint-focused best practices, let's dig into the ones you'll run from an organizational level.

4. Infrastructure Security Monitoring

Modern network infrastructure consists of so many moving parts — from the endpoint protection systems to operational fundamentals like servers, routers, switches, and security logs. And, as you can imagine, it's difficult to keep that many moving parts working in perfect coordination. That's why infrastructure monitoring is a crucial best practice.

When companies practice infrastructure monitoring, they observe and track their essential technical infrastructure to ensure all their production environments are up and running — maximizing uptime, providing quality user experiences, and ensuring secure interactions. At a high level, monitoring your infrastructure helps you identify and minimize any negative impacts to the confidentiality, integrity, or availability of your solutions or data.

When you are actively monitoring your infrastructure, you can immediately be alerted if an essential system — a server, firewall, service provider, etc. — is offline. Because if one component of your digital ecosystem goes down, it can cause downtime for your entire network.

And infrastructure security monitoring should also incorporate your intrusion detection and prevention systems. So you (or your service provider) can monitor security logs for any attacks, and even refer to them for audit purposes.

Finally, you want to ensure that your solution is integrated. Too often, companies will have several teams working on different systems, but communication breakdowns between the teams will expose vulnerabilities. With an integrated solution, one team can monitor your endpoints, monitor your cloud environment, gather all logs for analysis, and identify any breaches before extensive damage is done.

Tip: Want maximum visibility into your environment?

Integrate as many log sources as possible, and aggregate and correlate across those sources.

Key Benefit: Spotting Security Event Trends

Additionally, infrastructure security monitoring helps you identify and analyze event trends. So if you or your service provider see any security issues related to the network, they can be addressed immediately. The practice helps you **proactively** address and correct issues that could otherwise go unnoticed. This is crucial for optimizing performance.

How can you initiate this practice?

There are several technologies used for infrastructure management, and many firms opt for agent-based and probe-based monitoring packaged into a Managed Detection, Response and Remediation (MDRR) solution.

5. Vulnerability Assessment

Most firms already have a substantial and diverse tech stack. And for many, that stack expands each year, with more and more software systems added to an ever-growing ecosystem.

Software companies periodically announce software vulnerabilities that need to be "patched" with updates. If no action is taken, these vulnerabilities leave a company open to breaches or malware. So it makes sense to immediately patch the software, right?

Vulnerabilities: The List Keeps Growing

Over 8,000 vulnerabilities were published in the US government's National Vulnerability Database (NVD) just in Q1 of 2022. 22

Well, if you have dozens of systems running simultaneously, it's difficult (especially for smaller IT teams) to keep up with all of the patches as they are released. The result: the software is left without a secure configuration for weeks, months, or even years, leaving the door open for cybercriminals to infiltrate.

Vulnerability assessments give firms the opportunity to identify cracks in their systems and patch them before a breach occurs.

How can you initiate this practice?

Conducting vulnerability scans on a regular schedule is a task some firms can perform on their own. Open-source tools exist on the market, and they typically suffice when scanning for vulnerabilities.

However, scanning is the simplest component associated with addressing vulnerabilities. The tougher tasks are building complete vulnerability assessment processes and taking actions to remediate any issues.

For that reason, many firms opt to have service providers handle the entire operation. With a provider, you don't need to divert your staff to stay up to date with your software patches. The provider will scan, identify, and patch any vulnerabilities for you.

How often should you scan for vulnerabilities?

The SEC requires firms to conduct vulnerability assessments annually, at a minimum. However, to maintain secure systems throughout the year, monthly assessments are ideal.

6. Security for Office 365

Microsoft Office 365 is so robust that it can function as the hub for all of your data. Among other applications, it includes widely used features like Exchange Online (email), OneDrive for Business (file storage), SharePoint (information sharing and collaboration), and Teams (communicate, chat, collaborate). These four systems alone likely hold an abundance of confidential and sensitive information.

Microsoft Office 365 by the Numbers

- Used by over 1 million companies worldwide
- controls 47.5% of the office productivity software market share
- Teams grew 894% from March to June of 2020. Talk about a COVID bump! [23]

And because so much sensitive data is transferred using Office 365, cybercriminals often target it to probe for vulnerabilities. Think of all the confidential information and documents you've sent to co-workers via email alone.

So naturally, companies need to secure the solution against phishing and account compromise.

How can you initiate this practice?

In an ideal world, you would have secured your Office 365 system when you deployed it. Fortunately, you can secure it after implementation. A service provider will typically run an assessment that analyzes dozens of configuration settings (based on your license). Depending on the current configurations, the provider will recommend the optimal settings to keep your environment secure.

7. Incident Response

Even with excellent cybersecurity protocols, no organization is 100% protected against every threat. Inevitably, incidents will occur. The difference between firms that suffer severe financial consequences and reputational damage — and firms that escape mostly unharmed — is a solid response plan.

The value in a defined incident response policy isn't that you'll have an answer to every scenario that could possibly occur. That's not realistic. Instead, a response plan gives you the framework to quickly implement resolutions for incidents.

So, if you need to notify a regulator, patch a software solution, contact a third-party vendor, or take any other post-breach action, you have documentation on how to perform each task and who will perform it. You don't need to waste precious time deciding on the plan. You can simply act.

An effective incident response plan has three important benefits. After a breach, the plan helps you:

1. Limit damage
2. Eliminate revenue loss
3. Reduce recovery time

When your system has been compromised, speed is of the essence, and having a plan enables you to reach rapid incident resolutions.

How can you initiate this practice?

Document an incidence response plan for your organization based on common scenarios. If you work with a service provider, they can help you create this documentation. You'll want to define representatives from different teams and what their roles will be (who is managing the incident, who contacts your PR team or regulators, and when, etc.)

At least once per year, run a mock incident to test your response. In the process of mocking an incident, you'll learn how to improve your processes and update your protocols. Select a progressively more difficult scenario each year.

3 |

Cybersecurity Best Practices Checklist

Are you prepared to protect your firm from cybercriminals? Do you have the following cybersecurity best practices in place?

1 **Multi-Factor Authentication**
The verification of a user's identity with two or more independent credentials. Authenticating with an app or push notification is the safest route.

2 **Phishing Training and Testing**
Train users to identify phishing emails and follow correct protocols. Education combined with testing at regular intervals leads to organizational compliance.

3 **Endpoint Security**
Protecting endpoints (desktops, laptops, mobile devices, etc.) utilized by end users is essential in our remote work environment. Fund managers should combine endpoint protection with monitoring and remediation.

4 **Infrastructure Security Monitoring**
Monitor security events on essential infrastructure (servers, routers, switches, etc.) to keep production environments running smoothly. Many firms rely on agent- and probe-based monitoring packaged as a Managed Detection, Response and Remediation (MDRR) solution from a reputable provider.

5 **Vulnerability Assessment**
Patch known vulnerabilities in your (often robust) tech stack. Vulnerability scanning is essential, and the ability to quickly scan, identify ***and patch*** vulnerabilities with a proven process ensures even greater cybersecurity.

6 **Security for Office 365**
Secure applications within Office 365, which holds a bevy of confidential and sensitive information. Run assessments and use optimal security settings.

7 **Incident Response**
Incidents are inevitable, but having a documented response will save you precious time when an incident occurs. Create documentation that defines roles and actions to be taken by specific representatives.

4 |

Protect Your Firm with Industry Experts

By implementing these best practices, your organization will be well on its way to securing your data and protecting yourself against cybercriminals. If you want to skip the trial and error, working with an expert provider will ensure the highest level of security and keep you SEC and FTC compliant.

Linedata can provide that expertise with our Linedata Protect and Linedata Protect Premium cybersecurity solutions. With our award-winning MDRR solution, you get enhanced endpoint and network protection and up-to-the-minute threat intelligence at a price you can afford.

☞ **Click here to get protected**

References

1. The Latest: UN warns cybercrime on rise during pandemic, The Associated Press, May 20th, 2020

2. SEC Announces Three Actions Charging Deficient Cybersecurity Procedures, U.S. Security and Exchange Commission, August 30th, 2021

3. The biggest data breach fines, penalties, and settlements so far, Swinhoe, Dan, January 28th, 2022

4. Eleven Lessons from Cyber Hack That Forced an Australian Hedge Fund to Close (Part One of Two), Barton, Robin, Hedge Fund Law Report, February 4th, 2021

5. Gartner Forecasts 51% of Global Knowledge Workers Will Be Remote by the End of 2021, Gartner, June 22nd, 2021

6. Cyber Threats Have Increased 81% Since Global Pandemic, McAfee Enterprise and FireEye Highlight At-Risk Industries this Holiday Season, Businesswire, November 9th, 2021

7. Northwestern Pritzker School of Law's Annual Securities Regulation Institute, Gensler, Gary, January 24th, 2022

8. Trends in privacy & data security: Looking back at 2021 and ahead to 2022, Thomson Reuters Institute, April 7th, 2022

9. SEC Continues Rolling Out Cybersecurity Rules, this Time Targeting Public Companies, National Law Review, Volume XII, Number 73, March 14th, 2022

10. SEC Continues Rolling Out Cybersecurity Rules, this Time Targeting Public Companies, National Law Review, Volume XII, Number 73, March 14th, 2022

11. Cyber Rule Would Require New Staffers, Isenberg, David, February 22nd, 2022

12. SEC Proposes to Enhance Private Fund Investor Protection, U. S. Securities and Exchange Commission, February 9th, 2022

13. 25+ Password statistics (that may change your password habits), O'Driscoll, Aimee, January 31st, 2022

14. The 2020 State of Password and Authentication Security Behaviors Report, Manning, Ronnie, February 19th, 2020

15. Your Pa$$word doesn't matter, Weinert, Alex, July 19th, 2019

16. Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public, Public Service Announcement, Federal Bureau of Investigation

17. Phishing attacks increase in H1 2021, sharp jump in crypto attacks, Help Net Security, August 19th, 2021

18. Chainalysis: Cryptocurrency crime reaches all-time high

19. Defi Hacks Are on the Rise

20. Endpoint Security Tools Eventually Fail, Says Report, Security Magazine, June 17th, 2019

21. 50 Endpoint Security Stats You Should Know In 2022, Jones, Caitlin, May 6th, 2022

22. National Vulnerability Database, National Institute of Standards and Technology

23. 17+ Marvelous Microsoft Statistics to Mull in 2022, Galov, Nick, April 6th, 2022

Don Duclos, CISSP, CCSP, CISM, CISA. Chief Information Security Officer (CISO), Linedata.

Don has 20 years of Information Security experience at leading financial institutions and technology services providers. Prior to joining Linedata, he led teams in all three lines of defense (within the business line, Information Security, and Internal Audit) at regulated firms, where he frequently engaged with regulators and examiners from the SEC, OCC, FDIC, and FRB.

Linedata Protect and Linedata Protect Premium

Our award-winning Cybersecurity Services evolve with the threat landscape to protect your assets and reputation while supporting compliance with SEC requirements and other applicable regulation.

With over 1 million endpoints already being protected, Linedata Protect EDR and Linedata Protect Premium MDRR solutions package cutting-edge technology and human expertise to deliver fully managed security operations.

Learn more at www.linedata.com/linedataprotect.

About Linedata

With 20 years' experience and 700+ clients in 50 countries, Linedata's 1100 employees in 20 offices provide global humanized technology solutions and services for the asset management and credit industries that help its clients evolve and operate at the highest levels.

Linedata