imperva

A SECURITY PROFESSIONAL'S GUIDE TO THE NYDFS CYBERSECURITY REGULATION

5 Secure Steps to NYDFS Compliance

Executive summary

On March 1, 2017, the New York State Department of Financial Services[1] (NYDFS) introduced new cybersecurity regulations for financial services to protect their customers' data and to maintain security of operations within the industry.

The regulation, formally known as 23 NYCRR 500, but referred to as NYDFS, provides financial firms with a structure on which to build cybersecurity programs and policies specific to their business models to protect systems and consumers from the increased threat of cyberattacks. The comprehensive nature of the NYDFS means that even firms with existing security programs and procedures in place will benefit from implementing and maintaining the processes required by the regulation.

This guide is for CISOs, security professionals and compliance managers who want to get a better understanding of how NYDFS applies to their organizations and what the effects might be. You'll learn:

- How to identify your assets to protect your organization from a breach
- How to answer WHO is accessing WHAT data and WHEN
- How to protect your network and maintain operational uptime
- How monitoring who is accessing your data helps with compliance
- How data risk analytics can help accelerate threat investigation and response times

Financial firms face many challenges today, not least the growing number of cyberattacks. This e-book looks more closely at these challenges and explores the benefits of adopting a risk-based approach to security as encouraged by NYDFS.[2] It also outlines how Imperva solutions can help you comply with specific elements of the regulation.

[1] The NYDFS regulates approximately 1,500 financial institutions and banks as well as over 1,400 insurance companies.

[2] The NYDFS regulation encourages adopting a risk-based approach to cybersecurity. It was revised after considering feedback received during a 45 day comment period on the original proposal issued September 13, 2016.

Consequences of noncompliance

NYDFS has not outlined any specific information on consequences regarding penalties for noncompliance with the cybersecurity regulation other than including a requirement to notify the superintendent of a breach "as promptly as possible but in no event later than 72 hours"[3] after a breach has occurred. However, given the severity of penalties imposed under similar global regulations and considering penalties outlined in the New York Banking Law,[4] the penalties could be severe. See the table below:

REGULATION	NON-COMPLIANCE / VIOLATION OF REGULATION	TIME ALLOWED TO REPORT INCIDENTS
NYDFS	Up to (a) $2,500 per day during which a violation continues, (b) $15,000 per day in the event of any reckless or unsound practice or pattern of misconduct, or (c) $75,000 per day in the event of a knowing and willful violation (if New York Banking Law applied)	72 hours
GDPR	Up to 20 million euros or up to 4 % of a company's total global turnover of the preceding fiscal year, whichever is higher	72 hours
CCPA	Fines under the CCPA will cap at $7,500 per record breached	Not specified
MAS-TRM	Reputational Damage and Revocation of License	IT incidents and systems malfunctions within 60 mins. Incident report to be submitted within 14 days

[3] https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf

[4] https://www.nysenate.gov/legislation/laws/BNK/44

Market challenges

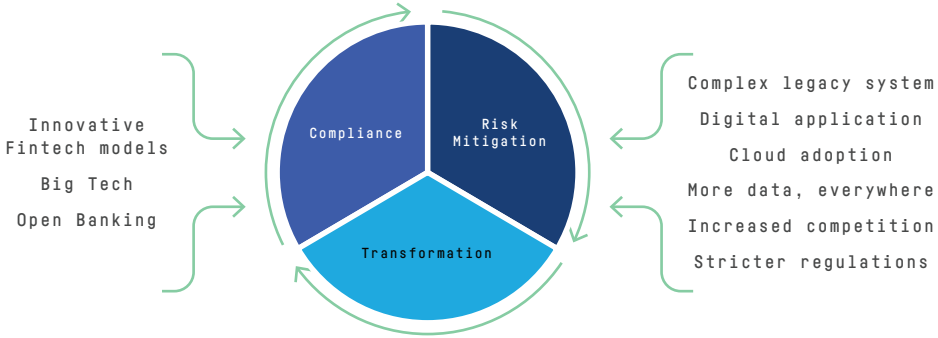
Maintaining normal business operations in today's rapidly changing market is a constant challenge for financial firms who find themselves balancing performance, compliance, and security to remain ahead of the game.

Digital transformation

The pressure is mounting to innovate with fintech start-ups developing the latest digital apps and solutions at a fast pace, and tech giants getting in on the act by offering their own range of financial products to their loyal customer bases. A lack of skilled security professionals is also hindering firms from keeping up with digital transformation and the move to cloud computing.

Pressures in financial services industry

Risk mitigation, transformation, compliance



The financial sector remains a prime target for cybercriminals because of the high value of the rewards to be gained.

According to Forbes, "Financial services firms also fall victim to cybersecurity attacks 300 times more frequently than businesses in other industries." [5]

[5] https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#39691b716e90

With DDoS and social engineering attacks on the increase, it only takes one bad actor to make its way into your network for a breach to occur.

Financial institutions were once considered bastions of security, protecting their valuable assets, including vast amounts of critical and sensitive data, by storing it within the secure confines of their data centers. Perimeter lines were clear, with the only people having access to the data being employees, using company-owned computers located on business premises.

In contrast, today's use of cloud technologies means users are connecting to networks remotely using multiple devices, and data is stored across hybrid hosting environments as firms rely on legacy systems while they transition to the cloud. As a result of all these changes, data is experiencing exponential growth, and while more data brings business benefits and opportunities, it also poses real challenges for the industry.

With the advancing data sprawl, the once-clear security perimeter lines have become blurred and the threat surface has expanded. Security teams are struggling to cope with the sheer volumes of data and the subsequent numbers of threat alerts received daily. According to the CyberEdge Group's 2019 Cyberthreat Defense Report,[6] the biggest inhibitor to establishing effective cyber threat defenses for security teams is having too much data to analyze.

Firms must discover new ways to strengthen their security posture to better protect their assets from a breach.

Compliance

In parallel, financial firms must comply with more complex regulations to prevent large enforcement fines, reputational damage, and intervention by the regulators.

Since the European General Data Protection Regulation was introduced in 2018, the matter of data privacy has come under the spotlight for all industries across the globe and, as a result, firms are much more cautious about protecting data that is of a personally identifiable nature (PII) and are looking for ways to simplify and automate their regulatory compliance processes.

[6] https://www.imperva.com/resources/reports/CyberEdge-2019-CDR-Report-v1.1.pdf

Risk mitigation

Digital transformation and compliance are major drivers of change for financial services and change brings risk as organizations adapt to new processes and workflows and growing volumes of data increase the threat landscape. However, the pace at which firms are adjusting their security posture is disproportionate to the speed at which the attack surface is expanding.

There are several ways that firms can mitigate change-driven risks including having a robust governance framework in place, regularly monitoring the risks, and consistently risk-assessing the changes.

"In times of transformation, it is critical to pay attention to operational risk - the risk of loss due to errors, breaches, loss or damage."

BAIN & COMPANY REPORT, 2018[7]

[7] https://www.bain.com/insights/how-banks-can-manage-operational-risk/

The insider threat

Despite the growing threat landscape today the traditional approach to cybersecurity concentrates on network endpoints, the assumption being that by protecting attackers from entering the network you will keep your assets safe from untrusted external threats.

Security at the edge is, of course, critical, as it addresses inbound traffic to combat external threats to your applications, APIs, and infrastructure. But despite advancements in edge security, many firms struggle with solutions that do not adequately address managing the escalating volume of data and number of applications, making it more difficult to protect themselves from a breach. Security teams are suffering from alert fatigue from the tsunami of security alerts they receive daily, which increases the risk of a real threat slipping through the net. There is also the very real issue of insider threats that occur due to lack of care, compromised credentials, or malicious activity.

The most effective way to buy-down risk for your organization is to secure the data itself and to take a unified approach using both edge and data security to give you the defense-in-depth you need to fully protect your assets.

"As the business becomes digital, security must become Data-Centric."

FORRESTER RESEARCH, 2018

INCIDENT OVERLOAD AND ALERT FATIGUE

54% of companies admitted that they tend to ignore security alerts.

imperva

The risks of a risk-based approach

Many businesses store large volumes of personal and sensitive data that they are unlikely to use. However, regulation often requires that organizations be able to prove that they have identified all sensitive data to protect it accordingly, and organizations tend to focus on monitoring and protecting the data that helps meet these regulatory requirements. For example, PCI applies to credit card data only where HIPAA regulation covers health information only.

According to Gartner,[8] businesses should conduct a risk-based review of their assets "to assess the size of potential liabilities and prioritize them according to impact," the idea being that only those datasets representing the most value and highest liability for the company, would be ring-fenced for protection.

Adopting a risk-based methodology to your data protection allows you to evaluate your data according to your organization's risk profile and priorities, significantly reducing the likelihood of a breach.

However, while this may seem like a sensible approach, it is important to remember that data that is important for regulation is not the only data that can get you into trouble,[9] and that other data, such as unprotected live production data, can also be monetized by hackers. While you focus on protecting only the data that matters for compliance you risk leaving live production data open to a breach which could bring down operations for your business. In short, by not protecting all of your data you might as well hand the cybercriminals the keys to the castle.

Buying down risk for regulatory compliance and risk mitigation for data security are two completely separate value drivers for firms. Risk mitigation is far less data privacy-centric and instead, is centered around quickly and easily identifying data access and usage risk, regardless of the data type. The data classification required for the risk-based approach can be a long and arduous task, sometimes taking months to complete, and, while security professionals are well aware that regulatory compliance is not security best practice, they get weighed down with the process, preventing them from implementing the best security measures for their business.

[8] Gartner - Develop a Financial Risk Assessment for Data Using Infonomics - Published 30 January 2019

[9] The Federal Trade Commission (FTC) has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury.

Mitigate risk from day one

To mitigate risk effectively and reduce your overall security vulnerability, Imperva recommends using data discovery techniques to identify and monitor all of your data wherever it resides. By doing so you buy-down risk across the full breadth of your assets even before prioritizing your data for deeper regulatory audit purposes.

But how does this monitor-everything-approach solve the problem of alert fatigue for security teams inundated with millions of threat alerts?

Companies can address this problem and reduce monitoring scope for their security teams through implementing security measures such as data masking and data risk analytics.

Data masking reduces monitoring scope by anonymizing sensitive or production data while it is being used for non-production purposes, such as dev and testing, allowing you to monitor all your assets without leaving large segments of your data unprotected.

Data risk analytics uses machine learning to identify the most critical threats by uncovering suspicious data access behaviors that could put your enterprise data at risk. It also applies grouping and scoring algorithms for each incident and, as a result, only a few high-risk incidents bubble up to the surface making user access much easier to manage.

Conclusion

The final NYDFS regulation issued in 2017 was a revised version based on feedback from industry consultation. One of the biggest concerns was that a 'one-size-fits-all approach was not suitable for an industry with firms with such diverse risk-profiles. The outcome was that NYDFS adjusted and reissued the 23 NYCRR 500 regulation in 2017 to allow firms to take a risk-based approach to compliance.

At Imperva, we believe that, while taking a risk-based approach to data protection reduces the risk of regulatory noncompliance, it is not a best practice for security and will still leave your business vulnerable to a breach.

In the next section, we look at five of the policies required by the NYDFS regulation and how Imperva's Application and Data Security solutions can help you to comply while effectively buying down the security risk for your organization.

Five secure steps to NYDFS compliance

1. **Data governance and classification**

   Imperva Data Security provides a proven methodology to discover and classify data, which is a critical aspect of the NYDFS compliance. It provides visibility into what personal data your organization holds and processes enabling you to monitor and protect all of your data wherever it resides. Key deliverables include: identification of database assets, data owners and data custodians; risk classification of data; and control recommendation.

   Imperva Data Security also includes data masking capability that replaces real data with realistic fictional data that is functionally and statistically accurate. It facilitates the processing of personal data beyond original collection purposes and also limits the spread of personal data beyond "need-to-know".

   Masking copies of production data for non-production purposes such as development and testing reduces monitoring scope and eases the burden for security teams.

2. **Access Controls and Identity Management**

   The NYDFS regulation requires organizations to implement and maintain a policy for access controls and identity management. To comply with NYDFS, you need to be able to answer WHO is accessing WHAT data, WHEN, and HOW that data is being used. Imperva Data Security provides complete visibility into data activity. It continuously monitors and analyzes all database activity, including local privileged user access and service accounts, in real time.

3. **Systems and Network Security**

   NYDFS states that firms should have a policy in place to address websites and APIs and to ensure systems operations remain functioning and available for your customers. Imperva Application Security provides a full-stack application security solution to protect your websites and APIs and to ensure systems operations remain functioning and available for your customers. With integrated Cloud WAF, CDN, DDoS protection and Attack Analytics, plus Bot Management and Runtime Application Self-Protection (RASP), your business will be protected on the inside as well as at the edge, offering a true defense-in-depth solution to comply with this part of the regulation.

MORE LEGITIMATE DATA ACCESS

34% of workers said they share passwords of accounts with their coworders.

4. Systems and Network Monitoring

To comply with NYDFS regulation, firms are required to implement and maintain a policy on Systems and Network Monitoring. Imperva Data Activity Monitoring (DAM) provides enterprise-wide visibility into all database transactions, including local privileged user access and service account activity. It continuously monitors across on-premises or cloud environments and collects consolidated records of all logins/logouts, updates, privileged activities and more to create granular audit trails that pinpoint the who, what, when, where and how for each database. DAM makes it easier for security teams to identify a genuine threat by giving them visibility of user access across multiple data storage locations.

5. Incident Response

In the event of a breach, the NYDFS dictates that "the entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred." Imperva utilizes machine learning and data risk analytics to pinpoint and prioritize high-risk incidents, filtering out the noise and allowing security teams to accelerate threat investigation and response. Reducing the influx of threat alerts received speeds up the threat investigation process by improving visibility of the alerts that matter. Data risk analytics also helps mitigate the risk of an attack on the inside.

Additional resources

More information

- https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf
- https://blog.focal-point.com/understanding-the-4-phases-of-the-nydfs-cybersecurity-regulation-23-nycrr-500
- https://www.forbes.com/sites/zakdoffman/2019/04/29/new-cyber-report-25-of-all-malware-hits-financial-services-card-fraud-up-200/#6bae3bdd7a47
- https://www.psdgroup.com/workshop-operational-risk-assessment-of-change/

About Imperva

Recognized by industry analysts as a cybersecurity leader, Imperva champions the fight to secure data and applications wherever they reside. In today's fast-moving cybersecurity landscape, your assets require continuous protection, but analyzing every emerging threat taxes your time and resources. For security to work, it has to work for you. By accurately detecting and effectively blocking incoming threats, we empower you to manage critical risks, so you never have to choose between innovating for your customers and protecting what matters most. At Imperva, we tirelessly defend your business as it grows, giving you clarity for today and confidence for tomorrow. Imperva – Protect the pulse of your business.

Protect the pulse of your business.

Imperva is an analyst-recognized, cybersecurity leader championing the fight to secure data and applications wherever they reside.

+1 (866) 926-4678
imperva.com

imperva