CAPITAL GROUP® | AMERICAN FUNDS®

Cybersecurity best practices for fiduciaries

The explosion in online transactions and cloud-based recordkeeping has put employer-sponsored retirement plans at increased risk of exposing personally identifiable information (PII) – which is legally protected from disclosure. How can plan sponsors and service providers balance fiduciary standards with the need to store and share personal data as part of their daily operations?

The Department of Labor's Advisory Council on Employee Welfare and Pension Benefit Plans (Council), looked into cybersecurity from the standpoint of DC and DB retirement plans. Its recommendations can help plans protect themselves legally and financially from today's cyberthreats.

The NIST framework

The Council, in its 2016 publication "Cybersecurity Considerations for Benefit Plans," encourages plan sponsors, fiduciaries and services providers to look to the National Institute of Standards and Technology (NIST) Cybersecurity Framework as they establish cybersecurity risk management processes. NIST is a three-part voluntary guideline designed to protect critical infrastructure in terms of overall U.S. national security.

Step 1: The Core

The first part of the NIST framework identifies the five functions that together form an effective cybersecurity risk management program:

Identify

To identify the types of risks a plan faces, the organization should create an inventory of data that may be collected, such as social security numbers, names, birth dates, hire dates, retirement dates, compensation information, medical record information and asset balances.

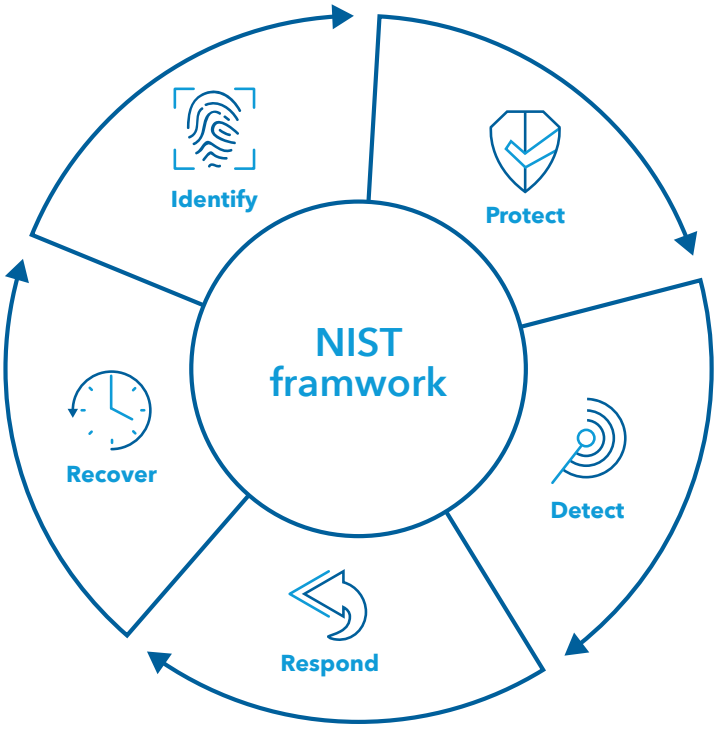
Plan sponsors and service providers should also understand how this data is being used. Most employee benefit plans rely on third-party service providers, such as plan administrators, actuaries, trustees, insurers and consultants. In the normal course of delivering services, these vendors collect, maintain and share sensitive employee data. This can result, the Council found, in some of the most significant cybersecurity breaches in the benefits arena. A hack into any of the systems where data is shared by outside service vendors could result in employees' identities, personal information or plan assets being compromised.

The easiest way to protect data is to limit who has access to data. Plans therefore should begin their cybersecurity journey by asking questions such as: Who has the data? How much data do they need to do their job? How is data accessed? How does it travel to an offsite center? Can unrelated parties disrupt the data flow? Will the service provider assume liability for breaches?

Plan sponsors and their service providers should maintain and share only the data and asset information that is necessary to meet the needs of the plan and no more.

Protect

Protection can take a number of forms depending on the particular risks the plan faces. Organizations should implement the appropriate safeguards to limit or contain the impact of a potential cybersecurity event. These include managing access to assets, providing awareness education and training to employees, putting processes in place to secure data and deploying protective technologies, e.g. malware protection, network security controls.



Detect

Experts say that breaches will occur, so it is important to implement capabilities to quickly detect an intrusion, which may include continuous monitoring solutions that detect malicious behavior. Your organization should have visibility into its networks to anticipate a cyber incident and have all information at hand to respond to one. Plan sponsors and service providers may wish to consult a cybersecurity expert to determine the best approaches to implement these capabilities.

Respond

How will the organization respond to a breach? The strategy states what the response will be to minimize the impact from the breach. The organization may wish to create a cyber incident response plan (CIRP), which is a comprehensive approach to tackling eventual cyberthreats and cyberattacks. A CIRP can outline contingency plans, define communications during the event and identify the correct way to address different kinds of attacks to ensure recovery.

Recover

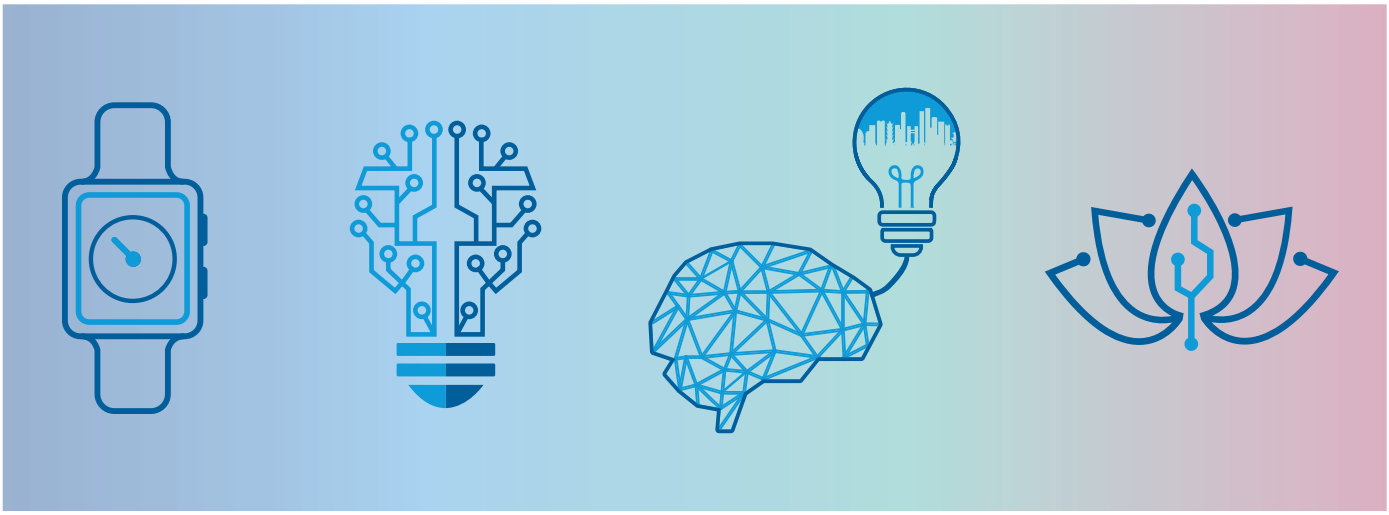
Recovery can be the most difficult and expensive part of the program, so recovery should be a critical component of the strategy. This may include factoring in ahead of time the costs to the organization of a breach, vs. the cost of remediation.

The NIST framework

Step 2: Implementation

The second part of the framework focuses on implementation of a risk management program and assists organizations in understanding where they are with regard to implementation.

The framework defines four implementation categories:



Partial	Risk informed	Repeatable	Adaptive

Users of the NIST framework should evaluate where they are on the spectrum of implementation and determine whether and how to move along that spectrum.

Step 3: Organization Profile

The most suitable cybersecurity program is the one best geared to the specific needs of the organization and plan. Thus, the third part of the framework focuses on creating an organizational profile that priorities the business drivers and risk factors.

It may include the following elements:

Prioritize and scope.

What resources are internally available to evaluate cyber risks, implement a cybersecurity risk management program, and respond to breaches? If expertise is not available internally, should external resources be considered? Are there other commercially available resources or tools that can be used?

Orient and scope within the entity.

If the organization is part of a larger entity, for example, can cybersecurity risk management be integrated (and costs shared) with the rest of the administration?

Develop a current profile.

Is it a small firm that wishes to rely on cloud-based resources, or a large, heavily regulated firm that wants a higher level of protection, such as conforming to SAFETY Act anti-terrorism standards?

Conduct a risk assessment.

Who uses the data and how is it being used? What standards are in place among these parties to prevent breaches?

Identify a target profile.

Are there industry certifications that the plan and service providers can explore that can enhance the cybersecurity risk management strategy?

Analyze gaps.

What measures can be put in place to balance data privacy needs with the need to disclose and retain material personal information?

Implement an action plan.

Who is responsible for designing, documenting, implementing and maintaining the overall cyber strategy?

The benefits of cyber insurance for small plans

Small and mid-sized plans that may not have the resources to develop and implement a cybersecurity risk management plan on their own may find it more cost effective to obtain cyber insurance to assess risks, implement a strategy, provide services in the event of a breach and provide liability coverage to third parties.

What about **cyber** insurance?

Plan sponsors, administrators and service providers usually carry insurance, including fiduciary, commercial, errors and omissions, officers and directors and other coverage. Anyone dealing with employee benefit plan data should understand whether the insurance covers the consequences of a cyber breach. To meet perceived gaps here, cyber insurance has become a growing part of plan's insurance coverage.

Components of cyber insurance may include:

- Reimbursement of company costs in responding to a cyber threat,
- Payment of fees and damages that a company may pay in response to litigation from a cyber incident,
- Reimbursement for revenues lost or expenses incurred due to disruption.

Striking the **right** balance

Plan sponsors under fiduciary standards of care should consider creating a cybersecurity risk strategy that outlines what actions the firm will take in the following areas:

Implementation and Monitoring

Reporting

Controlling Access

Data Retention and Destruction

Third Party Risk Management

In doing so, plan fiduciaries will need to determine the balance of preventive measures relative to the probability of the threat, the loss exposure and the cost of protective action.

3 tips for third-party risk management

Inventory all service providers who have involvement with the plan's participant and/or asset data.

Understand whether those service providers outsource activities to other providers.

Request information, once a comprehensive list has been developed, on each provider's security procedures, such as automatic notification and audit obligations.

Maintaining **Trust** in a New Era of Risk

We are coming to a collective realization now of the degree to which we've shared – willingly or unwillingly – our personal data through our mobile and web devices, and the risks that such access may pose. The concerns may be heightened for employer-sponsored retirement plans, which store and share personal data as part of their daily operations.

A scalable, individualized cyber risk assessment strategy is the prudent starting point to protect long-term plan assets from an increasingly sophisticated range of short-term threats.

Lit. No. RPGEBR-181-0819P Litho in USA CGD/CNP/ 10157-S75181 Printed on recycled paper.