LINEASECURE

Mitigating Cyber Threats for Funds

Steps Fiduciaries Should Take

Peter Dewar, President
703.850.4100
pdewar@lineasecure.com

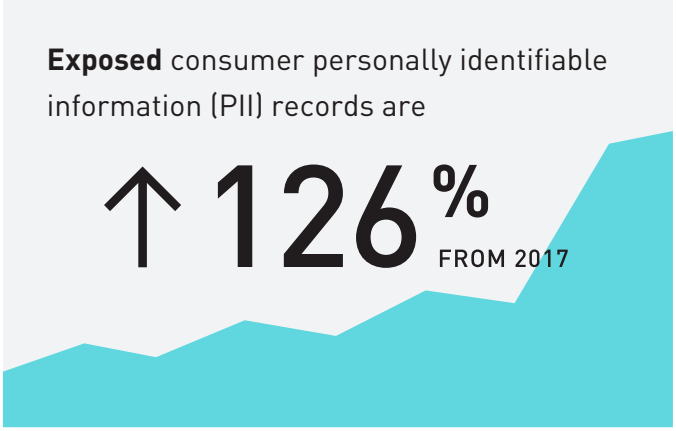
2701 Ocean Park Blvd, Ste 251
Santa Monica, CA 90405

T 310.331.8133
F 310.807.4356

Public pensions have been compromised and the rate is increasing

The Pension industry has problems with funding statuses. We have problems with investment returns. We have problems with declining active membership, with staff turnover, and with sudden changes to the legislation that regulates us. We also (most of us) have decades of experience dealing with these issues. However, there is a problem just as large and complicated as those above, one that fund managers and trustees may intuitively sense, but do not necessarily know if they are doing enough to address: **Cyber threat preparedness**.

As an industry we generally do a pretty good job of identifying risks in the areas identified above, as fiduciaries we perform due diligence in a number of areas from having an independent actuary perform annual valuations, periodic experience studies, and projections; certified public accountants performing an annual financial audit of both operational and fund accounting; visiting investment managers to perform due diligence to ensure they are still viable and are operating within our contractual constraints; we audit our payroll for fraud and accuracy and perform proof of life verification of annuitants.



What then of the systems that make all this possible? Do you have the same rigor in ensuring that they are protected, what standards are you following, how is that verified? The data contained in your systems is used to determine valuation, funding status, financial health, and benefit eligibility. If any of it is inaccurate, what then is the accuracy and viability of your plans? Are you operating on a sound footing, what is the quality of your decision making if you make false assumptions?

So yes, there is a problem! The problem is how do you protect the confidentiality, integrity, and availability of your data so that you are able to perform your fiduciary responsibilities with a sense of security.

Cyberinsecurity is a crisis faced not only by the pension industry, but across all industries and government because of the pervasive use of technology which is a must today, if we want to be as effective as possible in providing services. What can be done given this operating landscape? Fortunately, there is a solution. The solution lies in a number of approaches which is will outline below:

- Have a cybersecurity policy similar to an investment policy
- Be prepared in the event of an incident
- Have a roadmap for the implementation of cybersecurity capabilities
- Perform continuous monitoring and improvements to stay abreast of evolving threats integrity, and availability of your data so that you are able to perform your fiduciary responsibilities with a sense of security.

Developing a philosophy about the organization's approach to cybersecurity

Your cybersecurity philosophy represents your organization's recognition that the cyber threat exists. It represents how you plan to identify threats, protect against them, detect them, respond to them, and recover from threats. Before you begin, you should decide which standard is most appropriate for your operating environment. There are many standards to choose from, so decide carefully since this decision will impact how you proceed later. Federal agencies, for example, are required to follow the Federal Information Security Management Act (FISMA), and some state and local governments have adopted this standard. Others follow the standard developed by the International Organization for Standardization (ISO) or the Control Objectives for Information and Related Technologies (COBIT) standard. These standards are frameworks that provide you with controls which can be measured to determine how well you are protecting yourself.

One of the most useful frameworks for pension funds is the National Institute of Standards and Technology Cyber Security Framework (CSF). The framework encourages organizations to document their current cybersecurity posture, decide on their target state for cybersecurity, identify and prioritize areas of continuous improvement, assess their progress towards their stated goal for cybersecurity, and communicate with internal and external stakeholders about cybersecurity and their progress.

No framework works out of the box for all organizations, so you must customize it based on your needs. You need to identify your risk factors and the likelihood that those risks could be realized. The CSF contains 5 main components:

IDENTIFICATION[1]

Being able to identify that threats exist is the first step in developing an organization's philosophy. You must be aware of the assets under your management, their value, and how they could be compromised.

PROTECT[2]

Which safeguards will you employ to limit the damage that could be caused by an event? This is assisted by understanding the assets that need protection that was initiated in the previous step. How will it be determined who has access to assets, the level of authority they will have when accessing assets, including separation of duties are considered? It is also important to consider the type of training that the organization makes available to staff and select service providers, so that they are educated about the threat.

DETECT[3]

How will you become aware that you are under attack? Detection methods must be understood and discussed. This important step requires continuous monitoring and improvement, and the organization may be required to implement intrusive technology to give it this capability. Thus, it is important to decide which devices

[1] April 16, 2018 NIST Cybersecurity Framework V1.1 page 7

[2] April 16, 2018 NIST Cybersecurity Framework V1.1 page 7

[3] April 16, 2018 NIST Cybersecurity Framework V1.1 page 8

will be authorized on your network and the complete set of tools that will be deployed on them to enable this capability.

RESPOND[4]

Once a threat is detected, you must decide how it will be contained and how you will respond. You must have and an incident response plan, and understand how it addresses who is notified, how information is communicated, and which resources will be activated to assess and mitigate the damage.

RECOVER[5]

After identifying the magnitude of a threat, and determining which services have been affected, the activities that restore those services must be agreed upon, documented, tested, and activated as appropriate.

Into action

You now understand the nature of the threat, you know what it involves, you understand your capabilities, and you realize that the technology you employ today, and that you will deploy in the future is required for your business. The list of things to do may seems overwhelming! How do we get started and what should we work on first? This dilemma is addressed with a **cybersecurity assessment**. The assessment identifies the issues that require immediate attention so that triage can be performed to prevent exploitation of threats.

The assessment should follow the framework that most closely aligns with your business, regulatory and operating requirements identified in the previous step. It should cover key control areas such as access control, identity management, incident response, awareness and training, etc. The resulting Systems Assessment Report or SAR will identify compliance or weaknesses in the areas covered and will give you a detailed account of areas of concern. These areas

[4] April 16, 2018 NIST Cybersecurity Framework V1.1 page 8

[5] April 16, 2018 NIST Cybersecurity Framework V1.1 page 8

are tracked in a document called a Plan of Action and Milestones (PoAM). This gives you the ability to determine your progress towards addressing your areas of vulnerability whereby you can focus on the high priority areas.

The next step is to implement protections that address your highest areas of vulnerability. You will want to immediately update any configuration aspects to your technical implementations, such as ensuring that your systems are patched to the highest appropriate level, or that physical security tightened depending on the findings in the assessment step. You might continue with reviewing, strengthening, and implementing new policies to provide an organizational wide context to further actions. Additional steps might require budget and capacity conversations to address findings that require more resource allocation and time.

Some findings **will not** be easily addressed or mitigated. In cases where an organization decides a risk cannot be mitigated, it must decide if it could be transferred, avoided, or accepted. These decisions are not foreign to you, you already make such decisions regarding investments, funding levels, and third parties who provide services to you.

Have a plan

Now that you have performed triage on the most pressing issues, what do you do next? It is always good to have a plan, but what do you to start? As a fiduciary, you are responsible for protecting fund assets and your organization, therefore it might be helpful to think of the cybersecurity risks that you face in three areas:

- Investment Assets
- Member Records
- Reputation

Let us take a closer look at some questions that should be considered in each area:

Where are the cybersecurity risks in the investment and financial areas of operation?

- How are strategy executions performed?
- Do we have pending acquisitions?
- How are financial transfers and margin calls handled?
- Who has access to our investment accounts? Including third parties?
- How are pension payroll accounts funded and disbursed?
- What about organization operating accounts?

For member records, where do those risks lie? We might ask:

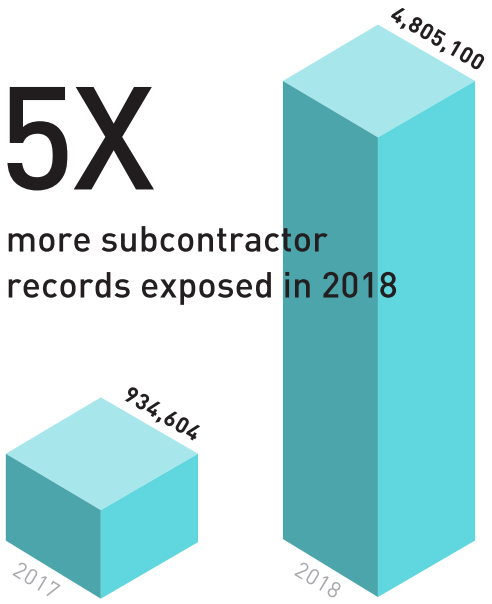
- How are member records secured?
- Is our network segmented?
- Are our databases encrypted?
- Are staff roles clearly defined and separated?
- Do we have a self-service application? Can records be updated?
- Do employers report electronically? How do we secure information exchange with them?
- What technology does our Pension Administration System use? What are the vulnerabilities there?
- Do we use third party administrators?

Keep in mind that insider threats and third parties that have access your data might be the greatest sources of risk to your organization. An organization is well advised to have complete ethics, privacy, and cybersecurity policies that govern the activities of its staff. These should be supplemented by a required cybersecurity training course.

Third party risk could materialize in many forms since you are required to share member, financial, and investment information with actuaries, auditors, custodial banks and investment managers. Ensuring that these organizations follow a program like yours is strongly recommended. You may implement a good cybersecurity compliance program, but if your data could be easily targeted by other means, then the job is only half done. The graph below illustrates the rising rates of compromises due to third party data breaches. Some large examples are Marriott, Target, and Equifax.

Now, how do we protect our reputation? Reputational risk is an intangible that is difficult to quantify but is easy to recognize when lost. Calls increase to member services, governing bodies including boards and legislatures require increased reporting and may increase oversight. Therefore, we consider:

- How is the organization perceived by your membership?
- What is your compliance and reporting responsibilities?
- What happens if a breach occurs?
- How will negative cybersecurity news be handled?
- Who reviews your vendor compliance?



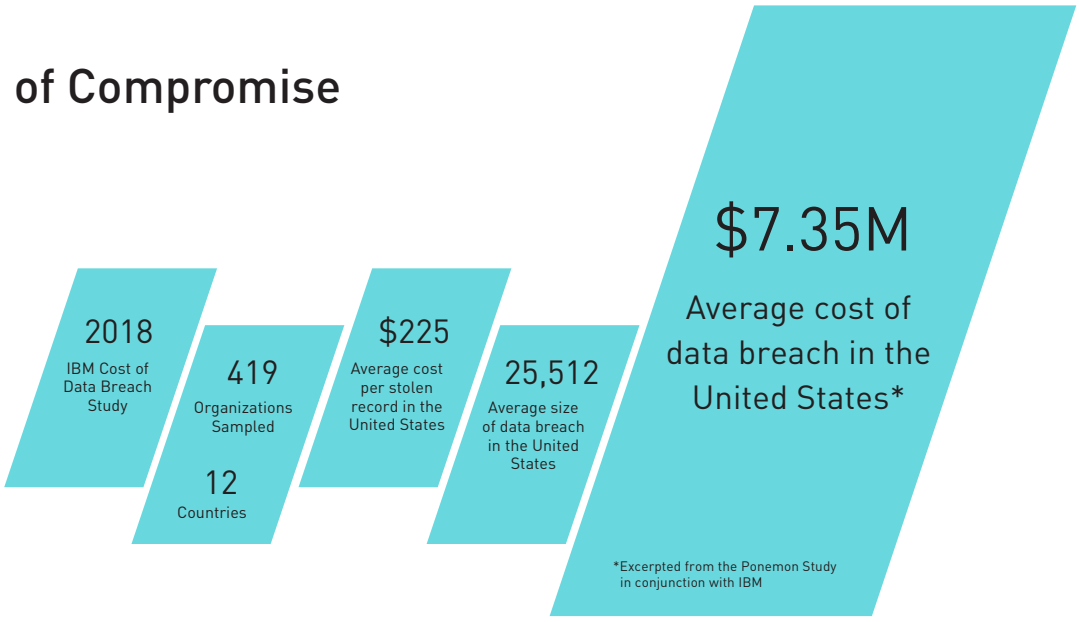
Once these areas of cybersecurity risk are identified, the next step is to create a roadmap to address them. The plan takes into consideration the areas of concern identified above and addresses specific actions you will take to protect each area. Some items to consider using would be a system security plan for your major systems. This plan will identify the type of information stored by each critical system, it should classify the type of data retained, and should identify the controls that will be put in place to protect the information and will specify how you will validate that these protections are occurring. You should develop an Incident Response Plan, that directs actions that should be taken if an incident occurs. Develop playbooks to game out scenarios so that you are prepared to act and know which actions to take depending on the incident, and finally, you should update your business continuity plan to include how you respond to a cyber incident.

Perform continous monitoring and seek to improve

If you create a culture of cybersecurity awareness for your organization, you are on your way to reducing this area of risk. But there are no guarantees! Cybersecurity insurance helps to cover costs in the event of an incident, which could be driven by many factors:

- Conducting investigations and forensics to determine root causes
- Determining probable victims
- Conducting communications and outreach
- Organizing an incident response team
- Audit and consulting services
- Service interruptions

The Cost of Compromise



IBM and Ponemon Institute Cost of Data Breach Study

The Ponemon Institute found that the cost of a data breach in the United States averages $7.35 million, with the cost of each stolen record to average $225.

These costs could be higher or lower depending on the extent of the breach and the type of services that are required to mitigate it. Therefore, having the appropriate coverage helps in this area, and implementing the protections recommended above will help to reduce the likelihood that an event occurs and arm you with the tools to respond to one.

The totality of the actions above may seem overwhelming to an under-resourced organization, so let's put it in a frame of context that you already undertake today. During your annual course of business, you have actuarial evaluations performed to determine the health of your plan and may increase the Required Contribution Rate of employers if deemed necessary by the plan rules. You perform annual financial audits to determine and demonstrate the financial health and compliance of your organization. You rebalance your investment holdings to comply with your diversification policies. You perform due diligence on money managers. Cybersecurity risk mitigation is like many- if not all- of these activities. Think of the Cybersecurity Assessment as you would a financial audit, view the SAR as a manager watch list, and the PoAM and Roadmap as you would an investment strategy and a strategic plan. Taken in this context, cybersecurity activities could be planned for and managed utilizing the tools you already possess and could become a normal operational task.

2701 Ocean Park Blvd, Ste 251
Santa Monica, CA 90405
T 310.331.8133 | **F** 310.807.4356

Peter Dewar, President
703.850.4100
pdewar@lineasecure.com