Xtreme Solutions, Inc.

STATEMENT OF HERVIA INGRAM, PRESIDENT & CO-FOUNDER

ABSTRACT

This document will discuss the cybersecurity risks related to the U.S. Department of Labor's Welfare and Pension Benefit Plan. This document will focus on cybersecurity components, such as risk management and asset management, that will advise the council on best practices for safeguarding personal identifiable information (PII).

Executive Summary

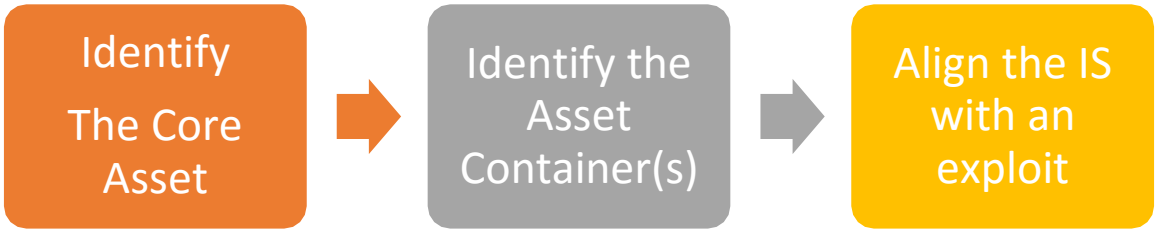
Due to the nature of increasing complexity and often impervious nature of cyber threats and attacks, it is virtually impossible to Eliminate threats. Many will venture into developing and implementing a cyber risk strategy with the goal of risk mitigation. Instead, the focus should be on risk management, instead of risk mitigation; no matter what type of organization.

Over the years, the methods used to fight sophisticated threats are proving to be obsolete. The relentless changes in technology, cyber landscape, and threats, demand that we employ the very best methods to thwart attacks. Protecting against cyber attacks means understanding your infrastructure and knowing your enemy.

- Your enemy will use what you have (your current infrastructure) to identify exploits; with the purpose to infiltrate.
- This means your protection begins with you.

Asset Identification Strategy

1. **Properly identifying the asset:**
    i. Benefit members Personal Identifiable Information (PII)
    ii. Since PII is the core asset, you must begin to recognize/identify the asset containers
    iii. It is the asset containers which are the exploitable information system
        1. For example: The database that administrates the PII and server(s) that house the database become the target systems
2. Now that the asset containers (target systems) are identified, you can now assume the types of attacks that you face.



2. **Perform Audit**
    1. Performing an audit

i. Network Audit - to map and identify the network with the purpose of identifying any holes (hacker exploits) in the network.

ii. Security Audit – determining the effectiveness of the security components (hardware or software) that are in place to protect the network from infiltration.

iii. Process Audit – reviewing all of the security process that are in place to determine feasibility and effectiveness to protect PII. This also means identifying lacking processes that are not in place, which needs to be developed.

iv. Compliance Audit – Under a compliance audit, the organization will begin to validate their alignment with standard policies. The organization should check for standard policies such as:

1. Sarbane Oxley
2. HIPPA
3. FIPS
4. ISO

And other related compliances and regulations

3. **Implement a third party administrator (TPA) strategy** - Many TPAs are required to comply with extensive regulations regarding privacy and security of data in the ordinary course of their business, and at least some of these institutions have required that their affiliated TPAs comply with these regulations. Compliance is up to you. TPA compliancy will be as strong as you force it be. It is critical that a retirement plan sponsor take affirmative measures to vet its TPA's cybersecurity program.

A solid vendor risk management strategy should include:

i. A contract outlining the business relationship between the organization and the TPA.

ii. Consistent monitoring and audit of vendor performance to ensure that contract stipulations are being met.

iii. Guidelines regarding who will have access to what information as part of the vendor agreement.

iv. Stipulations to ensure that vendors meet regulatory compliance guidelines for your industry, and a method to monitor this compliance.

An effective cyber risk management strategy requires a retirement plan sponsor to:

- thoroughly monitor its third-party administrators and vendors (TPAs);

- implement and periodically review contractual protections and insurance requirements in arrangements with its TPAs, while aligning them with standards
- periodically monitor the TPAs' cybersecurity compliance and related risks

Cybersecurity Considerations for Benefit Plans A-F

A. As background, review the general types of cybersecurity risks that benefit plans are exposed to and how the overall threat environment is evolving.

Besides the common hacker attacks that disrupt operations and those geared to steal data, there are more and more advance threats evolving every day making it very difficult for companies to try to protect their processes using just technology. Here are some of the new threats that could cause tremendous issues to those processing benefit plans:

Jailbreaking the cloud

As more and more companies rely on cloud and cloud infrastructure to include virtual machines, it has become easier to for hackers to go after them, as they are software-based computers and they have started to develop code specifically designed to crack cloud-based systems. For cybercriminals, this type of attack is a lot more lucrative because the number of operations in the cloud keep increasing at all levels.

At the same time, because apps rely on the cloud, mobile devices running compromised apps will provide a way for hackers to remotely attack public and private clouds and access corporate networks.

Ghostware to conceal attacks

Cybercriminals are now using ghostware that makes it extremely difficult to detect a compromised system. This attack uses blastware to steal information and destroy or disable a system if the attack is detected. Ghostware is used to cover its tracks. Law enforcement and those with forensic capabilities are having a difficult time to track how much data has been compromised and persecute cybercriminals.

Two-faced malware

This attack uses malware capable of looking benign while traversing surveillance devices like a sandbox and then morphing into malicious code once is no longer under suspicion.

This type of attack is becoming the most common among cybercriminals.

B. Obtain information about the steps, processes and controls that plans and third party providers are taking to address these risks.

One of the most important steps that companies must address is the enforcing of security policies. Policies should be based on governance standards according to their trade. Here are some examples of governance standards:

International information security standards - ISO/IEC 27001:2013

U.S. Federal Government information security standards - NIST Special Publication SP 800-53 revision 3

U.S. Department of Defense information security standards - DoD Instruction 8500.2

Other steps being taken to address these risks from third party providers are to provide security devices with the capability to update their software in order to patch new vulnerabilities. A patch management plan must be implemented by the company to maintain their operating systems up to date, to include antivirus software and end point security devices.

An information security awareness training plan is another step used to minimize the possibilities of risk on companies, this training should be done periodically and users must agree by signing a formal document that list the consequences if they knowingly engage in unsafe computer behavior.

The best process to maintain a safer computer environment in your company is to create an information security plan that involves everyone in the company and has the top management as their champion. An information security plan should be a living process that adapts to new technology as well as the new threats associated with it. This plan must follow a set of governance standards and add more stringent local requirements if necessary. A process to monitor and measure the effectiveness of the plan should be in place. And independent validation that validates the compliance against the standards should be implemented and executed periodically (at least every 3 years). Here are some of the documents that should be used as a minimum to maintain this process:

- Local Plans and Policies
- Risk Management Plan
- Business Impact Analysis
- Continuity Plan
- Configuration Management Plan/Configuration Control Board
- Contingency Plan for each critical systems/processes
- Current asset inventory/software inventory
- Patch management
- System specific security documents
- Physical and Environmental Control Plan
- Personnel Security Management Plan
- Ports, Protocols, and Services document

- Network diagrams/Local boundary
- Facility Security Plan
- Acceptable Use Policy/Rules of Behavior agreement
- Incident Response Plan
- Computer Security/Information Assurance Awareness Plan
- Implementation and Verification process

C. Examine how cybersecurity risks and exposure differ between small plan sponsors and large plan sponsors, with the objective of tailoring guidance and education accordingly.

Cybersecurity risks are very consistent between small and large plan sponsors. The risks and threats are dependent on the technology used. But some industries are more exposed than others based on their trade. Government and banking are targeted at a higher rate than medical or administrative companies. Without a risk assessment and a business impact analysis is very difficult to tailor guidance and education accordingly.

A small plan sponsor would require less security devices implemented and a smaller number of security specialists. A periodical (once a year) information security awareness training program would be sufficient.

A large plan sponsor would require more security devices, bigger security appliances, a more in- depth continuity plan, a separate contingency site to continue operations (Hot site), a bigger number of security specialists. A continuous information security awareness training program and a specialized training for security specialist is required for a large plan sponsor.

D. Draft materials that may help plan sponsors identify and establish a scalable cyber risk management strategy.

E. Draft materials that may help plan sponsors incorporate cybersecurity risk management in the vendor selection and monitoring process.

F. Invite interested parties to submit sample tip sheets, checklists and other educational tools that can be used to provide plan sponsors, vendors and plan participants with guidance on navigating cybersecurity risks related to their benefit plans.

Risk Management Plan

The plan should clearly identify critical infrastructure and processes. These should be ranked from most critical to less critical, the priority decision should be accomplished through a Configuration Control Board or some other management group that allows the input from those that are familiar with the project.

After identifying critical processes then a Risk Analysis should be completed. There are many ways to perform a risk analysis, but as a minimum it should include the following:

- Risk analysis –
    - Event/Probability
        - What could happen
            - Natural Disasters
                - Hurricanes
                - Flood
                - Earthquakes
                - Tornadoes
                - Etc.
            - Manmade
                - Fire
                - Vandalism
                - Terrorism
                - Etc.
            - Cyber Security Threats
                - Hackers
                - Disruption/Denial of Services
                - Ransomware
                - Etc.
            - Technical
                - Network Connectivity
                - Critical Infrastructure issues (hardware)
                - Data loss
                - Etc.
        - What is the probability of occurrence:

Rating/(Value)	Description	Likelihood of Occurrence
1/(0.01 – 0.2)	Rare	Highly unlikely, but it may occur in exceptional circumstances. It could happen, but probably

2/(0.21 – 0.4)	Unlikely	Not expected, but there's a slight possibility it may occur at some time.
Rating/(Value)	**Description**	**Likelihood of Occurrence**
3/(0.41 – 0.6)	Possible	The event might occur at some time as there is a history of casual occurrence at the University &/or similar institutions.
4/(0.61 – 0.8)	Likely	There is a strong possibility the event will occur as there is a history of frequent occurrence at the University &/or similar institutions.
5/(.81 – 1.0)	Almost Certain	Very likely. The event is expected to occur in most circumstances as there is a history of regular occurrence at the University &/or similar institutions.

- Impact/Mitigation – How bad will be if it happens (Cost) and how can you reduce the possibility of happening (how much will it cost?)
- Contingency – How can you reduce the impact after the mitigations (Cost)
- Risk is the cost of the impact times the probability
- Reduction is the cost of mitigation times contingency
- Exposure is the difference between Risk and Reduction. This is the amount of risk you simply can't avoid. Exposure may also be referred to as Threat, Liability or Severity, but they pretty much mean the same thing. It will be used to help determine if the planned activity should take place. This is often a simple cost vs. benefits formula. You might use these elements to determine if the risk of implementing the change is higher or lower than the risk of not implementing the change.
- The following tables are examples of a Risk Impact descriptors:

Rating/(Value)	Description	Financial Impact	Business Interruption	Reputation & Image	Corporate Objectives
1/(0.01 -0.2)	Insignificant	Minimal financial loss; Less than $300,000	Negligible; Critical systems unavailable for less than one hour	Negligible impact	Resolved in day-to-day management
2/(0.21 – 0.4)	Minor	$300,000 to $2M; not covered by insurance	Inconvenient; Critical systems unavailable for several hours	Adverse local media coverage only	Minor impact

3/(0.41 – 0.6)	Moderate	$2M to $5M; not covered by insurance	Client dissatisfaction; Critical systems unavailable for less than 1 day	Adverse capital city media coverage	Significant impact
Rating/(Value)	**Description**	**Financial Impact**	**Business Interruption**	**Reputation & Image**	**Corporate Objectives**
4/(0.61 – 0.8)	Major	$5M to $10M; not covered by insurance	Critical systems unavailable for 1 day or a series of prolonged outages	Adverse and extended national media coverage	Major impact
5/(0.81 – 1.0)	Catastrophic	Above $10M; not covered by insurance	Critical systems unavailable for more than a day (at a crucial time)	Demand for government inquiry	Disastrous impact

- After completing the risk analysis on critical processes, the plan must address the actions required for each of them. Here are some typical risk responses:
  - Retain/accept the risk - if, after controls are put in place, the remaining risk is deemed acceptable, the risk can be retained. However, plans should be put in place to manage/fund the consequences of the risk should it occur.
  - Reduce the Likelihood of the risk occurring – e.g. by preventative maintenance, audit & compliance programs, supervision, contract conditions, policies and procedures, testing, investment, training of staff, technical controls and quality assurance programs, etc.
  - Reduce the Consequences of the risk occurring - through contingency planning, contract conditions, disaster recovery & business continuity plans, off-site back-up, public relations, emergency procedures, staff training, etc.
  - Transfer the risk - this involves another party bearing or sharing some part of the risk through contractual terms, insurance, outsourcing, joint ventures, etc.
  - Avoid the risk - decide not to proceed with the activity likely to generate the risk, where this is practicable.

The risk management plan should also include a periodic review of the process. Risk Management is a fluid process because risks are always changing. Today, you might assign

some risk with a high probability and a high impact. Tomorrow, the probability or the impact might change. Some risks might drop completely off the table while others come into play.

How to protect assets

Physical security is the first step of securing assets. Make sure that critical infrastructure is located behind lock doors and that environmental controls are available to prevent damages.

Make sure that only authorized personnel have access to critical infrastructure and that separation of duties is in practice.

Privileged users must comply with a background investigation to verify trustworthiness. Maintain privileged users trained on their roles.
Maintain assets up to date with patches and upgrades. Run vulnerabilities scans frequently.
Maintain assets with warranties with 24/7 support, to include parts and labor.

Recommendations and Tips

Perform a Risk Analysis and Business Impact Assessment to know what needs to be protected and how many resources are required to mitigate any risks.

Create an Information Security Plan that creates a safe computer environment. Perform a validation and verification test to ensure compliance at least every 3 years.
Create a Plan of Action and Mitigations to correct any vulnerabilities identified in the test. Involve all users into the security process.
Provide information security awareness training.

Make sure top management buys in into the security process.
Enforce rules and policies.
Balance security procedures with productivity.

Accept exposure of risk after all mitigation factors have been put in place or remove service if the exposure is too great.