# Statement of Euclid Fiduciary

**ON:** **Cybersecurity Insurance and Employee Benefit Plans**

**TO:** **Advisory Council on Employee Welfare and Pension Benefit Plans**

**DATE:** **July 19, 2022**

**BY:** **Daniel Aronowitz, Managing Principal, Euclid Fiduciary**

**EUCLID FIDUCIARY**
100 East Street SE • Suite 204 • Vienna, VA 22180
P 571.730.4810 • F 571.730.4813 • euclidfiduciary.com

**Written Statement of**

**Daniel Aronowitz, Managing Principal, Euclid Fiduciary**

**Before the**

**Advisory Council on Employee Welfare and Pension Benefit Plans**

**Meeting on**

**Cybersecurity Insurance and Employee Benefit Plans**

**June 19, 2022**

As a leading provider of fiduciary, cyber and crime insurance to thousands of America's best managed employee benefit plans and plan sponsors, including some of the country's most sophisticated multiemployer, governmental and single-employer benefit plans, Euclid Fiduciary presents this testimony to answer the Advisory Council's questions as to how cybersecurity insurance works to protect employee benefit plans from modern cyber risks.

## INTRODUCTION

Cyber insurance policies issued to employee benefit plans provide comprehensive coverage that help a policyholder respond effectively to a cyber breach, including forensic assistance, complying with regulatory notice requirements, and responding to cyber extortion demands, as well as defense and indemnity protection from regulatory and third-party lawsuits. Cyber carriers also provide valuable cybersecurity risk management services, including upfront and ongoing cyber alerts of potential threats to an insured's systems.

Five years ago, less than ten percent of benefit plans were protected by cybersecurity insurance, whether by an insurance policy issued directly to the plan or as part of the cyber policy issued to the sponsoring entity. Most benefit plans also had deficient controls to prevent common cyber threats. But that has changed dramatically in the last two years: many benefit plans have improved their cybersecurity controls, and more plans are covered by cyber insurance. Over 95 percent of multiemployer or other similar stand-alone benefit plans or trusts are now protected by cybersecurity insurance coverage, and we estimate that approximately 60 to 75 percent of single-employer plans are protected under the plan sponsor's cyber policy [with a higher uptake of cyber coverage for large plan sponsors, and a lower uptake of protection for smaller plan sponsors].

At the same time, the cyber insurance market is in a sustained hard market, with increased premiums and more thorough underwriting of prospective and renewal accounts. The threshold requirements to secure cybersecurity insurance has increased substantially in the last two years with heightened underwriting requirements, which has led to improved cybersecurity risk management programs by plan administrators and sponsors. In order to obtain quality coverage currently, even for policy renewals, benefit plans and plan sponsors now must demonstrate that they have key cyber security controls in place to prevent data breaches and protect plan assets, like (1) multi-factor authentication, (2) quality data backups, (3) email security controls, and (4) endpoint detection and

response and other more sophisticated anti-virus software protections. The cybersecurity insurance industry has thus played a vital and primary role in helping benefit plans improve their cyber controls to prevent data breaches, and will continue to be a crucial component of the overall risk management profile for plans and plan vendors.

Improved cybersecurity protocols and cybersecurity insurance protection for benefit plans is critical because Euclid claim statistics reveal that cyber incidents now represent 15-20 percent of all potential liability claims faced by benefit plans – second only in frequency to participant benefit claims. Most of these cyber claim events affecting benefit plans start with data breaches caused by plan administrators or other vendors, including health care providers, actuaries and recordkeepers, and thus benefit plan professionals must focus on vendor and business associate contracts and indemnification from vendor partners to protect their plans. High-profile data breaches of third-party administrators, recordkeepers and other plan vendors like the recent Horizon Actuarial data breach underscores this point. Given that benefit plans face common cyber threats and often use common vendors, the potential exists for an aggregated event that implicates many plans at the same time, meaning that the severity of the event could prevent plans from realizing full indemnification potential from the vendor or under the vendor's cyber insurance policy.

Euclid Fiduciary considers that cybersecurity coverage is just one element of a comprehensive cybersecurity risk management program. We believe that cybersecurity best practices for employee benefit plans are best considered in three areas:

(1) a **cyber-security program** that includes data safeguards (technological solutions) and comprehensive training for all employees and plan fiduciaries;
(2) **vendor-management** and indemnification from third parties working with your plan; and
(3) an **insurance backstop** that includes high quality cyber, fiduciary and crime insurance issued directly to the employee benefit plan [and not shared with the sponsoring entity].

For purposes of our testimony today, we focus on the insurance protection needed by employee benefit plans to protect against modern cybersecurity risks, but do not want to lose sight of the importance that insurance is just the backstop and not the primary way to protect assets and participant data. After outlining the insurance coverages needed by benefit plans to protect against modern cybersecurity threats in **Section One**, we then explain how underwriters assess and rate cyber risks in **Section Two**, and in **Section Three** we consider what cybersecurity protocols are now required to secure quality cyber and third-party crime coverage. In **Section Four**, we provide a checklist of coverage issues to consider when purchasing cyber insurance coverage.

Finally, we end this introduction by emphasizing two points: (1) that single employer plans should consider purchasing cyber coverage separately from the sponsoring entity to ensure dedicated limits for sponsored plans; and (2) that cybersecurity insurance is not sufficient to protect against all benefit plan risks, because many cyber policies contain ERISA exclusions and otherwise offer insufficient third-party crime coverage for social engineering risks that must be supplemented by third-party crime insurance. First, while the vast majority of multiemployer or other independent trusts now purchase a cybersecurity insurance policy issued directly to protect the plan, nearly all single-employer plans, including governmental benefit plans, do not purchase a separate cybersecurity policy, and instead rely on the cyber policy of the sponsoring entity. This risks insufficient coverage to protect plan assets and participant privacy risks when the plan is competing for limited policy limits purchased by the plan sponsor. Second, in the current sustained hard

market for cyber insurance, carriers have been making policy changes and restricting certain coverages. We have seen leading carriers insert ERISA exclusions in the standard cyber policy, which could eliminate critical coverage for breaches of fiduciary duty under ERISA, a common claim brought by plan participants when a data breach occurs. This exclusion has not been tested in courts, but it could be used to deny coverage for participant lawsuits alleging breach of fiduciary duty for account losses. This demonstrates how fiduciary liability insurance plays a critical role in a comprehensive cybersecurity insurance program. The experience of recent vendor data breaches also highlights how cyber liability claims intersect with potential fiduciary and crime coverages, and how plans need comprehensive protection with a coordinated cyber, fiduciary and crime insurance program.

**BACKGROUND: THE CYBER RISK TO EMPLOYEE BENEFIT PLANS: Benefit plans rely on technology to run the plan and maintain extensive personal data.**

It is useful to understand the cyber risks faced by benefit plans and the most frequent claim scenarios in order to better understand the insurance coverages required to protect against these risks. Like most organizations in the modern world, employee benefit plans rely on technology for the vast majority of daily activities to expedite transactions that used to occur only in paper or hard copy. Plan information has been digitized, and account information is now stored online, including information about participants and beneficiaries. Plan participants access their accounts on-line and communicate with plan administrators by email, and participants have online access to the investment options and funds in their accounts. Given the reliance on technology, plan data is at risk from both criminal hackers and employee mistakes. Benefit plans have both significant assets and extensive personally identifiable and sensitive data that make them attractive targets for hackers. In addition to the accessibility of vast sums of money and detailed personal information, most benefit plans rely on third-party administrators to manage the benefits and investments, which provides an additional avenue for security breaches, both intentional and unintentional.

Benefit plans face the same risk of cyber security incidents that affect other financial service entities that use technology to process business. Cyber security incidents that can affect employee benefit plans stem from both employee mistakes, including breaches of security protocols, as well as the more commonly known criminal incidents. The most common cyber threats to employee benefit plans are:

- **Cyber-Extortion/Ransomware and Malware Attacks:** Ransomware refers to the common situation in which a bad actor encrypts and disables access to business-critical systems and data until a ransom payment is made. Data may also be exfiltrated and exposed if the ransom is not paid. Ransomware and extortion demands are an existential threat to benefit plans.
- **Business Email Compromise [BEC]:** The most common business email scam faced by benefit plans consist of banking instructions to divert money from plan or participant accounts. BEC refers to any email intrusion resulting from spoofing, phishing, or spear phishing that can result in a data breach or funds transfer loss. BEC includes phishing schemes and email account breaches in which hackers read emails to perpetrate hacking schemes.
- **Wire Fraud/Retirement Account Fraud:** Wire fraud is when a bad actor uses social engineering, sometimes in concert with phishing attacks, to cause funds to be sent to the

attacker instead of the proper recipient. The wire fraud threats include fake invoice schemes; unauthorized loans and withdrawals, including from portals from plan administrators and the set-up of new accounts or loans on the portal. The risk is that it can take weeks or months to get the system back up and working to process benefit payments.

- **Data Breaches:** Exposure of personally identifiable information (PII) or protected/personal health information of plan participants. The most frequent claim under a cyber insurance policy is the need to comply with state requirements to notify participants of security breaches of information involving personally identifiable information.
- **Legal and Regulatory Claims:** Participants and other third-parties can file lawsuits alleging that the plan and its fiduciaries are responsible for data breaches. Plans also face liability for violations of legal or regulatory frameworks, such as CCPA or GDPR.

## SECTION ONE: CYBERSECURITY INSURANCE AND OTHER POTENTIAL SOURCES OF INSURANCE PROTECTION FOR CYBER EVENTS

At the outset of this review of cybersecurity insurance, we stress that insurance is just one component of a holistic risk management framework, as insurance is the final failsafe when training and risk management protocols break down and a cyber incident takes place. Insurance provides the backstop when cyber security risk management protections inevitably fail, but the vast majority of cyber breaches – up to 95+% -- can be prevented with quality cyber risk management protocols, including email security and other measures. For example, the implementation of multi-factor authentication eliminates many potential threats. Second, while every benefit plan needs coverage under a stand-alone cyber policy, it is important to note that potential insurance coverage for cyber events can be found in other types of insurance, including fiduciary and crime insurance policies. Four general types of insurance policies potentially apply to data breaches affecting employee benefit plans:

**(1) Cyber Liability Insurance –** the most comprehensive protection for data breaches and claims from participants and other third parties;

**(2) Fiduciary Liability Insurance –** the foundational errors and omissions coverage for the trustees and fiduciaries of employee benefit plans. While it will likely not have coverage for breach notification and other first-party cyber coverages like forensic investigation, crisis management, and extra expense or business interruption coverage, fiduciary liability insurance may nevertheless cover third-party claims from participants that allege breach of fiduciary duty for failure to maintain adequate and prudent cyber security practices to prevent data breaches, or imprudent management or selection of service providers.

**(3) Fidelity Bond/Crime Policy –** if the plan has secured third-party crime coverage in its fidelity bond, the crime policy can cover certain cybercrime events, such as funds transfer and computer fraud loss. Crime policies also may offer coverage for social engineering or payment instruction fraud. Many cyber policies are deleting or reducing coverages for cybercrime, and thus social engineering coverage may only be available in the third-party crime policy. But even if both policies offer the coverage, it is likely sub-limited, and plans can maximize their coverage by securing coverage under both policies.

**(4) Commercial General Liability (CGL) and Property Policies:** coverage under a plan's CGL policy is usually limited to property damage, and loss of data is likely excluded, but still could be a source of potential cyber coverage.

All four types of insurance policies are analyzed below, starting with a primary focus on cyber liability insurance, which is the most important insurance backstop in the event of a data breach.

## CYBER LIABILITY INSURANCE

Cybersecurity Liability Insurance is protection for (1) **Data Security** and (2) **Privacy**. These are two distinct concepts: **Cybersecurity refers to how data is secured; and Privacy refers to how data is used.** Cyber data security risks stem from when the plan uses the internet, computer networks and digital databases, or transmits information electronically or online. Data privacy risks result from collecting, handling and using Personally Identifiable Information (PII) of plan participants. Cyber liability insurance policies can minimize loss in the event of a data or security breach. Cyber liability insurance is intended to protect against liability and property losses that may result when an entity engages in various electronic activities, such as selling on the internet or collecting data within its internal electronic network. The main purpose of the insurance is to reimburse the insured when it suffers an unauthorized intrusion of sensitive data that is stored electronically. It covers a plan's liability for a data breach in which its participants' personal information, such as social security numbers, bank account information, or confidential health records, is exposed or stolen by a hacker or other criminal who has gained access to the plan's electronic network. The policies cover a variety of expenses associated with data breaches, including: notification costs, credit monitoring, costs to defend claims by state regulators, fines and penalties, and loss resulting from identity theft. It also covers website content. Some polices also cover property exposures from: (1) business interruption; (2) data loss/destruction; (c) computer fraud; (d) funds transfer loss; and (e) cyber extortion.

Unlike most types of insurance, cyber liability insurance policies are not standard or uniform. The reason is that cyber liability is still relatively new and entities like the Insurance Service Office (ISO) has not issued a standardized policy form like it does for commercial general liability insurance. Every cyber policy is different, and essential coverages are labeled differently from policy to policy. Cyber coverage will likely standardize over time, but until then, this makes it challenging for prospective policyholders to understand what they are buying and to compare different policies, particularly based solely on price. Coverage is changing constantly as the product continues to develop. For this reason, every prospective buyer of cyber liability insurance needs an experienced insurance broker or insurance advisor to guide them. This lack of uniformity and constant policy changes underscore the important point that cyber liability insurance is not a commodity.

Most insurance companies present their coverage options under the headings of various insuring agreements that are typically designated as **first- or third-party coverages**. First-party coverage refers to an insured's own losses (when no third-party is seeking damages) as distinguished from third-party coverages that reference losses from claims by third-parties. This is often confusing, and best understood if you consider a potential loss from the perspective of the policyholder's relationship in the insurance contract and who is asserting the claim against the insurance policy:

- The **first party** is the insured individual or entity.
- The second **party** is the **insurance** company.
- The **third party** is another individual or entity unrelated to the insured individual or entity.

Therefore, a first-party insurance claim is made by the policyholder for its own losses seeking to recover its out-of-pocket expenses; whereas a third-party insurance claim is made by someone who is not the policyholder or the insurance company. Cyber insurance thus covers:

(1) A policyholder's **own first-party** privacy and data security risks, such as coverage for loss of data and loss of income arising out of breaches in network security caused by hacking events; and

(2) **Third-party liability risks**, such as network security and privacy liability for claims made by third parties, including participants and regulators, when personal data that is collected, handled, or used by the insured has been compromised or stolen.

**First-Party Example:** Mary, an account clerk at the fund office opens an email from Microsoft 365 software to confirm her sign-in password, which turns out to be malware. By clicking on the email link, Mary inadvertently released a virus that destroyed several internal data files before the virus could be contained. The fund office incurred expenses to recreate the data files and eliminate the virus. This is a first-party loss to the fund office.

Business interruption is another type of first-party loss. For example, a plan administrator can experience a network problem that disrupts an online business during the holiday season, or the destruction of participant data by a disgruntled employee. If the network goes down, whether because of hurricane or malware, then the fund cannot make benefit payments to participants. The extra expense to get the network back online is a first-party potential loss.

**Third-Party Example:** By contrast, a third-party loss is potential liability to your beneficiaries and regulators, such as liability claims from third parties. This would include suits alleging negligence from (1) participants or other beneficiaries (ex. if a participant sues); (2) regulator lawsuits, or fines and penalties under privacy laws; and (3) website liability.

The following are the most common first- and third-party insuring agreements found in modern cyber and privacy policies:

| **FIRST-PARTY COVERAGE – Your Own Losses** | **THIRD-PARTY COVERAGE – Losses from claims by third-parties** |
|---|---|
| **Breach Response Costs:**<br>1. Privacy Notification and Crisis Management Expense Coverage | 1. Network/ and Information Security and Privacy Liability |
| 2. Business Interruption and Extra Expense Coverage | 2. Regulatory Defense and Penalty Coverage (including GDPR and TCPA) |
| **Direct Property Loss Coverages**<br>3. Systems Failure/Data Assets Restoration Coverage | 3. Multimedia Liability |
| 4. Cyber Extortion/Ransomware | 4. Technology Errors and Omissions |
| 5. Computer Replacement/Bricking | 5. Payment Card Industry Fines and Assessments [PCI DSS Liability] |
| **Crime Coverages**<br>6. Computer fraud | 6. Bodily Injury (BI) and Property Damage (PD) Liability -- third party |
| 7. Funds Transfer Fraud | |
| 8. Social Engineering/Payment Instruction Fraud | |

| | |
|---|---|
| **Enhancement Coverages**<br>9. Court Attendance Costs | |
| 10. Reputation Loss | |
| 11. Crypto jacking | |
| 12. Bricking – Computer Replacement Coverage | |

You may not find this exact list in any cyber insurance policy, as carriers use different labels for key coverages. Carriers also often combine certain coverages into related categories, and other key coverages – like social engineering and computer and funds transfer fraud coverages – are often included as policy endorsements to give insurers maximum flexibility in crafting a coverage proposal to a client. For example, one prominent carrier has the following categories of coverage in its policy[1] without labeling the coverages as first or third party:

(1) Cyber Incident Response
(2) Business Interruption and Extra Expense
(3) Digital Data Recovery
(4) Network Extortion
(5) Cyber, Privacy and Network Security Liability
(6) Electronic, Social and Printed Media Liability

But yet another prominent carrier has the following categories of coverage[2]:

(1) Enterprise Security Event Claim
(2) Privacy Regulation Claim
(3) Crisis Management Expense
(4) Fraud Response Expense
(5) Public Relations Expense
(6) Forensic and Legal Expense
(7) Extortion Loss
(8) Business Interruption and Data Recovery Coverage
(9) PCI-DSS Fines Coverage
(10) Ransomware Loss Coverage
(11) Social Engineering Fraud Loss Coverage
(12) Telecommunications Theft Loss
(13) Website Media Liability Coverage

[1] Chubb Cyber Enterprise Risk Management Policy PF-48168 (10/16).

[2] AXIS Pro Privasure PVSR-201 (03-16). For another example, the Corvus Smart Cyber Insurance Policy has the following fourteen insuring agreements: Third Party (1) Network Security and Privacy Liability; (2) Regulatory Investigations, Fines and Penalties; (3) Media Liability; (4) PCI DSS Assessment Expenses; (5) Breach Management Expenses; First Party (6) Business Interruption; (7) Contingent Business Interruption; (8) Digital Asset Destruction, Data Retrieval and System Restoration; (9) System Failure Coverage; (10) Social Enginering and Cyber Crime Coverage; (11) Reputational Loss Coverage; (12) Cyber Extortion and Ransomware Coverage; (13) Breach Response and Remediation Expenses; and (14) Court Attendance Costs. Note that Breach Management is provided as a third-party coverage and Breach Response is provided as a first-party coverage. This is an example in which the first- versus third-party distinction can be confusing, and why it is more important to the policyholder to focus on what is needed functionally in responding to the breach.

**A More Practical Approach to Understanding Cyber Insurance**

While most cyber policies list their coverages by first- and third-party insuring agreements, this is a confusing way to understand the coverages of the policy, particularly since many coverages, such as breach response and network security or data loss, involve both first- and third-party elements. It is further confusing when policies have insuring agreements with different labels for the same basic coverages. Given this confusion, Euclid believes that the best way to understand a cyber liability policy, including whether to evaluate whether a policy is comprehensive and provides what a benefit plan needs, is to **evaluate each type of coverage by function**. Viewed by functionality, a cyber policy with comprehensive coverage should provide the following categories of coverage:

**KEY CYBER COVERAGE GRANTS: The Essential Coverages**

**(1) Breach Response**: This is the coverage necessary to manage, contain and respond to a cyber incident. It includes privacy breach notification services, computer and legal experts, including data forensics to determine whether a data breach has taken place, data restoration and digital data recovery, and public relations.

**(2) Cyber Extortion/Ransomware:** Coverage for the assistance and losses in responding to an extortion threat and demand for ransom against the insured's computer system.

**(3) Business Interruption/Reputational Harm/Loss:** Reimbursement for the costs or extra expense stemming from a network interruption.

**(4) Liability to Third Parties**: Coverage to respond to regulators or claimants who allege they were injured by a data breach including network security and privacy liability; regulatory proceedings; regulatory fines and penalties; media liability and reputational harm; and PCI DSS Assessment Expenses related to the use of credit cards.

**(5) Cyber Crime**: Coverage for theft and property loss: including computer fraud, funds transfer fraud, and social engineering. As noted above, cybercrime is not always available in a cyber policy, and may need to be covered or supplemented under the third-party coverages of a crime policy, because any available coverage is usually subject to small sublimits that will not fully cover many crime incidents.

A comprehensive cyber policy should have these five essential coverage grants in the policy, regardless of how the insuring agreements are labeled. The following explains each coverage category and what you need to protect your plan.

**(1) THE FIRST ESSENTIAL COVERAGE GRANT: Breach Response**: Breach Response Coverage or Cyber Incident Coverage is the coverage necessary to manage and respond to a cyber incident. It will help a policyholder contain a data breach and reimburse the policyholder for the costs to manage and respond to a cyber incident. Breach response coverage includes privacy breach notification services, computer and legal experts, data restoration and digital data recovery, and public relations. Although labeled differently between policies, cyber security and privacy policies should contain an insuring agreement that addresses breach response costs, sometimes labeled "crisis management" or "privacy notification coverage."

**Breach Response Coverage** will cover the direct expenses required to conduct a timely and effective response to a data breach. The number one goal is to figure out what happened, evaluate whether you have legal obligations to notify affected participants, and then minimize the loss. Carriers offer pre-negotiated services with third-party vendors experienced in post-breach

requirements and services. Breach Response Coverage also indemnifies the policyholder for the complex and expensive regulatory burden of complying with the state notification laws described above. Privacy notification and crisis management coverage should include the following coverages and access to cost-effective experts to assist in containing and responding to the loss:

- **Breach Coach:** This service is assistance from the insurer's panel of experts to provide the insured with immediate help in a crisis situation. The cyber incident response or breach coach is the quarterback of the cyber incident. The policy will usually direct the insured to call the Breach Coach at the claims hotline, and the Breach Coach will walk the insured through the steps necessary to take full advantage of the first-party breach response coverages of the policy to address the situation. The coach is usually a lawyer at the panel law firm hired by the insurer with expertise in cyber breach and cyber notification requirements. The use of a lawyer creates an attorney-client privilege and confidentiality when necessary.
- **Forensic Investigation Coverage:** Covers the cost and expenses related to determining whether a cyber breach has occurred, how it occurred, and how to stop the attack or loss of data. The insurance company will hire a computer forensic expert to secure the insured's information system following a breach, determine the cause of the breach, and offer advice as to how to prevent future breaches. Indeed, some policies will go further to pay for assistance to prevent future breaches.
- **Notification to Participants:** The insurer will take responsibility to notify affected policyholders of the breach and that their personally identifiable information may have been exposed by the breach. Some policies only cover the notification costs that are required by law. Others provide coverage for voluntary notification. This allows the insured to notify participants of a cyber incident, even when not required by law, if doing so likely reduces liability the insured may incur for the breach. Still other policies cover notification costs if requested by the insured. Finally, some policies handle breach responses on a *per affected individual basis*, and some of these costs can be in addition to the aggregate limit of liability.
- **Post-Breach Call Center:** The policyholder will have access to a post-breach call center that allows customers [i.e., participants of a benefit plan] of the insured to answer questions about the breach and learn how their personally identifiable information may have been exposed as a result.
- **Public Relations:** The insurer will engage a public relations firm to assist in communicating with the public about the breach.
- **Credit Monitoring and Identity-Theft Monitoring:** The policy will allow the policyholder to sign up for credit monitoring and services like LifeLock. The policy will specify how long the service will last – usually one or two years. Some policies also will cover costs necessary to restore stolen identifies. Identity theft monitoring is even more valuable and comprehensive than credit monitoring because it can detect additional fraudulent uses of PII.
- **Notifications to Banks and Credit Cards:** Coverage for the costs to notify banks and credit card companies of plan participants whose credit card numbers have been accessed.

## (2) THE SECOND ESSENTIAL COVERAGE GRANT: Cyber Extortion/Ransomware

Ransomware is extortion that prevents you from accessing your system or data until a sum of money is paid. In a cyber extortion scheme, the criminal notifies an entity that unless specified demands are met, the criminal will introduce a virus to destroy the company's data, implement a DDoS attack, or damage the company's data or systems in some other way. Sometimes, the criminals threaten to release confidential customer information unless their demands for payment are met. Modern extortion attacks typically include ransomware, which encrypts network data assets and requires payment of a ransom before an encryption key is provided to release data. An extortionist can threaten to shut down the fund's computer system. The best risk management technique is to back-up information on a detached system. Cyber Extortion coverage in a cyber liability insurance policy provides a valuable backstop when all technical safeguards fail. [NOTE: Since many insured entities have developed improved backups, this lessens the viability of a ransomware threat to shut down the victim's network. This has led hackers to adjust tactics, switching to threats of disclosure of confidential information as hackers adjust to the new reality of increased use of data backups.]

Cyber Extortion or Ransomware coverage covers costs to respond to hackers who attempt to extort money by threatening to release sensitive information or data if a ransom is not paid or to hold a network or data on the network hostage. The applicable insuring agreement will be labeled with some variation of "Network Extortion," "Cyber Extortion and Ransomware Coverage," or "Extortion Loss" coverage. Quality extortion coverage should pay for:

- The money necessary to meet the extortion demand or threat against any network to disrupt business operations, alter or destroy data, use of the network to transmit malware, or threat to disclose personal or business confidential information;
- The costs of a consultant or expert to negotiate with the extortionist, and may further advise on future prevention efforts;
- The costs of an expert to stop the intrusion and block future extortion attempts; and
- The cost to conduct an investigation to determine the cause and scope of a cyber-extortion threat.

Cyber Extortion is valuable insurance coverage because most trust funds and plan administrators will have no experience in negotiating with extortionists. The value of the insurance policy is instant access to leading experts with substantial experience in negotiating ransomware demands.

The insuring agreement for **Network Extortion Threat** indicates that the policy will pay extortion money and expenses the insured incurs for any claim involving a threatened attack on the insured's system or to disseminate confidential plan data. "Network Extortion Threat" or "Extortion Threat" should be broadly defined to ensure maximum ability to trigger coverage for this increasingly common event:

> Sample Policy Language: **Extortion Threat** means any credible threat: (1) to commit an attack against computer hardware, software and all components thereof linked together through a network of devices accessible through the internet or the **Insured Entity's** intranet or connected with data storage or other peripheral devices and operated by and either owned by or leased to an **Insured Entity**, or (2) to disseminate **Protected Data** for which the **Insured Entity** is legally responsible; for the purpose of extorting funds from an **Insured Entity**.

Some policies will list the types of threats that can trigger Extortion Coverage, including credible threats to (a) release, divulge, destroy of use Protected Information as a result of unauthorized access to the Insured's Computer System; (b) cause a network security failure; (c) alter, corrupt, damage, manipulate, misappropriate, delete or destroy Digital Data; or (d) restrict of inhibit access to an Insured's Computer System.

Some policies require an extension or endorsement that expands the definition of "Extortion Loss" to cover a Ransomware Attack or Loss. "Ransomware Attack" is defined as the "insertion of malware by a third-party perpetrator on computer hardware, software or components thereof linked together through a network of devices accessible through the internet or the Named Insured's internet or connected with data storage or other peripheral devices and operated by and either owned by or leased to a Named Insured that prevents or limits an Insured's ability to access data thereon for the purpose of obtaining a ransom from the Insured to end or remove the attack." If unclear, it is critical to clarify if your cyber policy covers a ransomware attack. It is also important to understand if the ransomware or cyber extortion limit is sublimited, as this is the highest severity claim in the last three years. The exponential rise in ransomware events is what triggered the hard market in cyber insurance in which cyber carriers began to manage limits more closely and raise premiums to ensure long-term rate adequacy of the insurance product. It also caused carriers to heighten underwriting standards and restrict coverage to only insure accounts that have strong cyber controls designed to prevent ransomware claims.

### (3) THE THIRD ESSENTIAL COVERAGE GRANT: Business Interruption/Reputational Harm or Loss: Costs stemming from network interruption

Business Interruption (BI) is considered by insurance underwriters to be a "time element" coverage that was traditionally in the province of property insurance and not a liability insurance policy. Nevertheless, business interruption is a key loss factor for cyber incidents and is now a universal offering in cyber liability policies. But this history may explain why some policies include Business Interruption Coverage by endorsement and not in the main policy agreement. The key issues for Business Interruption coverage are: (1) the period of recovery and the time of the waiting period before coverage is triggered; (2) what is the trigger of coverage; (3) the scope of extra expense coverage; and (4) whether dependent business interruption applies.

The BI insuring agreement covers loss of income during the "period of recovery" in which an insured's business is unable to operate, such as when an online retailer must shut down because of a data breach for a period of time and cannot take orders from customers. BI coverage is subject to a time deductible (as opposed to a money or dollar deductible) or what is referred to as the "waiting period" before coverage applies. The period of recovery differs from policy to policy, but it is now common for non-retail policyholders like benefit plans to obtain BI coverage with a minimal waiting period of six to twenty-four hours following an "electronic disruption." A common waiting period is eight hours. Some insurers' BI coverage covers an extended period of indemnity during a period of time following an electronic disruption if sales or operations have not resumed to pre-breach levels.

It is now common for cyber policies to include coverage for **Contingent or Dependent Business Interruption**. This covers the situation in which a policyholder's vendor or supplier incurs some

form of cyber-related downtime and cannot deliver services to the insured as expected. Dependent BI is a mandatory coverage for employee benefit plans that use a third-party administrator, recordkeeper, or otherwise outsource any portion of the benefit or investment administration. The typical insuring agreement for Contingent/Dependent Business Interruption reads as follows: "We will pay income loss and expenses incurred by the Insured during the period of restoration resulting directly from an interruption in service to you by a qualified service provider caused directly by a failure on the part of the qualified service provider's network operations security, but only if such failure would have been covered under the terms and conditions of this policy had the qualified service provider been you."

The companion coverage to BI is **Extra Expense Coverage (EE)**. It is sometimes combined with BI coverage, offered separately, or not at all. The EE insuring agreement covers additional costs that an insured incurs in an effort to expedite its return to normal operations following an "electronic disruption" or "systems failure." Additional costs may include overtime labor, express parts shipping, and the costs of hiring special experts to address the breach. Under some policies, EE coverage applies only if the extra expense actually reduces the loss, whereas under other policies the insurer will more broadly cover the extra expenses incurred, even if they do not actually expedite an insured's return to full operating capacity. EE Coverage is critical for employee benefit plans, as traditional business interruption coverage that indemnifies for lost profits is not relevant to a benefit plan. Instead, a benefit plan values continued operations. To this point, some EE coverage is expanded to reimburse extra expenses required to maintain operations following a data breach. The trigger of coverage for business interruption is some form of an "electronic disruption" for a "failure of computer security," which is defined as "material interruption" and "network security failure," but varies greatly between policies. For example, some policies will only include a data breach, while others will also include introduction of a virus or other type of disruption. The coverage is typically limited to outside intrusions, such as hacking, data theft, or malware. Cyber business interruption traditionally would not cover time element losses caused by other non-cyber or physical damage perils, such as fire, flood, windstorm or earthquake. The thinking was that, if a computer system is disabled by these kinds of perils, coverage for business interruption or extra expense should have been secured under standard property insurance policies. Nevertheless, some insurers have expanded their business interruption coverage to include system failures as a result of unplanned and unintended outages of a computer system that are not related to a cyber breach, such as an insured's unintentional or accidental error in modifying, creating, handling, or maintaining data or computer systems. System failures would normally be excluded from a property insurance policy.

**COVERAGE TIP: Employee benefit plans need broad Extra Expense Coverage to ensure continuity of operations. Plans also need contingent or dependent coverage to ensure that the EE coverage applies to data handled by plan TPAs and other vendors.**

**Data Asset Coverage:** A coverage related to Business Interruption and Extra Expense Coverage is Data Asset Coverage. Data asset loss is usually caused by failure to patch or update software. This insuring agreement, if provided, covers the cost of restoring and recovering the data lost from "the failure of an insured's computer security" – or if expanded, to "systems failure." For example, a hacker could introduce a virus into the plan' participant database that deletes participant contribution or benefit payment history. The Data Asset Insuring Agreement would pay the cost of restoring the lost participant database. The most comprehensive data asset coverage includes the cost to recreate lost data by recovering the data from paper records, although some policies restrict

restoration to recovery by "electronic means" and not actual research to recover lost data assets. The coverage will not pay for upgrades to security or antivirus software [often called "betterment"].

**(4) <u>THE FOURTH ESSENTIAL COVERAGE GRANT: Liability to Third Parties</u>**: This coverage responds to regulators or claimants who allege they were injured by a data breach, including privacy & security/network security and privacy liability; regulatory proceedings; regulatory fines and penalties; media liability/reputational harm; and PCI DSS Assessment Expenses related to use of credit cards.

Employee benefit plans face potential liability claims from participants, regulators or other third parties relating to alleged losses from wrongdoing by a plan in connection with a computer system or breach of privacy due to theft, loss, or misuse of data.

**<u>Information Security and Privacy Liability – Claims by Participants</u>**

Although labeled differently from policy to policy – "information security," "enterprise security," or more commonly "network security" liability coverage, **<u>Network Security Liability Coverage</u>** covers claims made by third-parties against an insured for failure to protect its systems against unauthorized access or denials of service. It provides coverage for claims made by participants and others who allege they suffered financial harm because of the Insured's wrongful acts or its failure to secure its network adequately. It also covers claims for failure to protect systems against unauthorized access or denial of service. **<u>Network Security</u>** is usually defined in terms of the security risks it is designed to defend against:

- Unauthorized access (hacking) over internet or wireless medium;
- Unauthorized release or theft of confidential information stored on physical devices (laptop/USB);
- Distributed Denial of Service Attacks (DDoS); or
- Transmission of a Virus or Malicious Code or malware from your network to third-party network.

Insureds will want broad definitions of "network security" and "network operations" to cover any type of attack on their computer systems and data. The key is to ensure that the policy covers more than just theft of assets, and includes broader coverage for intrusion or introduction of a virus. In other words, policyholders need to make sure that the policy covers damage inflicted on a third-party, i.e. transmitting a virus to a third-party computer system. Not all policies offer this coverage in the base policy, and it may need to be added by policy endorsement.

An example in the employee benefits arena is the 2017 data breach affecting health insurer Anthem Inc. in which the PPI of approximately 78 million people was exposed, many of which were participants in employee benefit plans. The aggregated claim example affected hundreds of health benefit plans, and highlights why plans need strong indemnification provisions in business associate contracts. Benefit plans also need to verify and validate that business associates and other plan vendors have sufficient cyber insurance coverage, which should respond first as the primary cyber policy to any vendor cyber incident – i.e., before the benefit plan's own cyber policy is triggered. The cyber insurance program insuring Anthem paid for the significant costs to comply with state notification laws to notify plan participants of benefit plans using the Anthem health network of the data breach, as well as the cost to provide required credit monitoring to plan participants. Of the dozens of Euclid policyholders affected by the Anthem breach, none incurred any costs from the

Anthem cyber breach due to Anthem honoring its indemnification commitments in the business associate agreements with its benefit plan clients.

The insuring agreement for **Privacy Liability** covers claims made by third-parties against the insured for specific wrongful acts: claims alleging failure to properly handle, manage, store, destroy, or otherwise control personal and confidential information. It covers defense costs, judgments, settlements, and related liabilities caused by plaintiffs who bring suit against the insured due to a cyber event. Some policies only provide coverage if there is a theft of data (e.g., a hacker obtains personally identifiable information). Other policies will provide this coverage even if there is an intrusion without theft. This is an important distinction. Privacy breach risks have been the result of:

- Hackers
- Employee negligence or employee complacency
- Lost mobile devices of stolen computers
- Third parties, such as subcontractors or vendors
- Social engineering tactics, such as phishing

While fines and penalties under federal statutes can be severe, liability to customers and clients has generally been limited by courts. Customers who have had personal data stolen or compromised sometimes file a lawsuit against the company, often as a class action on behalf of affected individuals. These lawsuits may allege negligence in securing the data, failing to prevent unauthorized access, and breaching the plaintiffs' privacy. Several such lawsuits have been filed against Euclid-insured health and retirement plans. Courts have generally dismissed these claims, asserting that until some type of damage occurs, the plaintiffs have not suffered any harm that needs to be remedied, but many of these lawsuits are settled before a court ruling on the plausibility of the complaint. Plaintiffs can have difficulty proving a causal link to the compromised data, particularly given that most Americans have had their personal data compromised by many vendors like large department stores and commonly-used websites. Nevertheless, the frequency of these lawsuits against benefit plans continues to increase, and can be expensive to defend.

**Regulatory Defense and Penalty Coverage – Claims by Regulatory Authorities**

The Regulatory Defense Insuring Agreement covers defense costs to prepare for and defend against regulatory proceedings involving state data breach laws and federal statutes that apply to employee benefit plans, including HIPAA, that governs protected personal health data. The two key components of regulatory coverage include (1) coverage for the costs of the legal defense required by regulatory actions, and (2) coverage for the fines and penalties that may be levied against an insured by various regulators, including legal, technical and forensic work. Policies should also cover certain fines and penalties and limits assessed by federal and state regulators for failure to comply with security and privacy rules, including HIPAA and notification laws. Policies should also cover the costs to respond to government inquiries about the cybersecurity [although most benefit plans seek coverage under the fiduciary insurance policy for Department of Labor audits of cybersecurity protocols].

**Payment Card Industry Fines and Penalties and Loss Assessments**

The Payment Card Industry Data Security Standard [PCI DSS] is a set of security standards intended to ensure that all companies use credit card information in a secure manner. Payment card industry data security standards are a set of proprietary information security protocols that businesses must

follow and merchants must agree to if they accept payment from the leading credit cards like Visa, MasterCard, American Express, and Discover. The Payment Card Industry Insuring Agreement covers contractual liability for: (1) **fines and penalties** assessed against the policyholder to the extent such fines and penalties are insurable by law for failing to comply with PCI DSS; (2) **loss assessments** – the costs to replace lost credit cards or fraud costs associated with stolen credit cards; and (3) **defense costs** incurred in challenging or defending against assertions that the insured failed to comply with PCI DSS. This insuring agreement excludes coverage for losses sustained by an insured merchant from accepting a disputed credit card transactions, because this is considered a business rather than a fortuitous risk. While employee benefit plans do not operate as merchants, they sometimes accept certain co-payments or other payments from participants by credit card, which could make PCI DSS coverage relevant.

**Website Media Liability**

The Website Media Coverage insuring agreement covers the liability incurred by the insured relating to the material published on its website – i.e., improper use of information on the insured's website. Website Media Coverage provides coverage for copyright infringement, libel, slander and other alleged improper web-based acts (such as deep-linking to another entities web page without permission) that is published on an insured's website. This coverage includes personal injury claims for invasion of privacy, libel, slander, or defamation. For example, a health plan could be accused of violating a participant's right to privacy if it posted a picture of an insured participant or inadvertently posted confidential personal information of a participant. This coverage is not for losses related to data breach or intrusion Media coverage in cyber policies has traditionally been limited to an insured's website, but many carriers have begun offering full media liability coverage that includes coverage for both online and offline media. Offline media coverage would extend to published papers, broadcasting, personal appearances, and coverage for social media-related acts.

**Bodily Injury and Property Damage**

The Bodily Injury and Property Damage Insuring Agreement is sometimes added to a cyber liability insurance policy because the Network Security and Privacy Liability insurance agreement limits coverage to financial losses resulting from a data breach and will contain an express exclusion for bodily injury and property damage that is included in most management liability and errors and omissions insurance policies. This coverage is needed for high-risk industries like construction and manufacturing, and should not be needed by employee benefit plans, but we mention this coverage to provide a complete view of cyber coverage.

**(5) THE FIFTH ESSENTIAL COVERAGE GRANT: Cyber Crime: Coverage for theft/property loss: including computer fraud, funds transfer fraud, and social engineering**

The final category of theft of property is the usual province of commercial crime policies, but some crime coverages is offered in comprehensive cyber policies. Many cyber carriers avoid property loss coverages, or offer them only by endorsement with sublimited coverage, because the loss involves breakdown in accounting controls, not typical cyber losses. The sublimits are often between $25,000 and $250,000, with most policies offering $100,000 or less in coverage, and subject to retentions of $25,000 to $100,000 before coverage applies. Employee benefit plans can obtain additional property loss coverage by expanding their fidelity bond to include the third-party crime coverages. Indeed, the traditional distinction was that cyber insurance covered data loss, and crime coverage covered money or property loss. That distinction began to blur five years ago as more

cyber insurance policies added cyber-crime coverage to the policy, including specific social engineering coverage, notwithstanding that most of the claims involve accounting and not cybersecurity controls. Nevertheless, the trend in the current difficult cyber market is that cyber carriers are pulling back from offering or limiting cyber-crime coverage, particularly for social engineering claims.

**Computer Fraud Coverage**

The Computer Fraud insuring agreement covers loss from unauthorized or fraudulent entry into a computer system, resulting in theft of money or securities. A typical scenario is when a hacker obtains information about an insured's client and uses that information to withdraw money from the client's bank account through an ATM. This coverage does not cover fraudulent acts of employees, independent contractors, or persons under the insured's supervision.

**Funds Transfer Fraud Coverage**

The Funds Transfer Fraud insurance agreement covers loss sustained when funds are fraudulently transferred from one financial institution to another. The coverage grant requires the fraudulent transfer of funds from one financials institution to another. For example, a hacker can gain the security credentials of the plan administrator or the bank's computer system, and then wire instructions to the plan's back to transfer money to the hacker's bank account. The difference between computer fraud and funds transfer fraud is that funds transfer fraud involves the transfer of money between financial institutions.

**Social Engineering Fraud Coverage**

Social Engineering Fraud Coverage is also known as Payment Instruction Fraud, as it covers losses of funds that are transferred by means of fraudulent instructions. For example, a plan official receives what appears to be a legitimate email from a client or vendor asking the official to wire money to one of the banks in which the plan has an account. The plan official follows the fraudulent instructions in which the client or vendor has been impersonated, but the funds end up transferred to the bank account of a cyber thief. Payment instruction fraud losses can result from impersonation of a company officer or employee, as well as participants themselves, or even a vendor, regulator lender, or outside professional, such as a trusted attorney, accountant or investment banker. Whereas funds transfer fraud coverage applies to involuntary transfer of funds, usually by means of an unauthorized intrusion into a computer system, social engineering coverage involves the good faith or voluntary transfer of funds.

Cyber policies will usually limit social engineering coverage to a small sublimit of coverage, usually $100,000 to $250,000. Carriers will sometimes require proof of accounting controls for limits above $100,000 or even a lower amount, namely that (1) policyholder's computer system uses a two-factor authentication system with username/password and an entry code that is texted to the user of the email system; and/or (2) that any wire transfer of money is preceded by a call back verification from the financial institution before the money is disbursed. It is important to check the other insurance clause of the cyber policy, because the social engineering coverage may be excess or considered to contribute on a pro-rata basis with any similar coverage in the insured's crime policy. Also, some social engineering coverage only applies if the insured can validate that an account verification control protocol took place before the funds transfer. This final point is a key coverage issue that should be explored before binding coverage.

**The Mechanics of Cyber Coverage, Including What is Not Covered**

**Claims-Made Coverage:** The most important feature of cyber liability policies is that they are written, like most professional liability insurance, including fiduciary liability insurance, on a claims-made and reported basis. That means that coverage applies only to claims that are first made against the insured and reported during the policy period (or any extended reporting period, if applicable).

**Prior Acts Coverage:** The next consideration is whether the policy covers the cyber event that led to the claim, and that is determined by when the cyber event took place. The cyber event can take place before the policy period in which the claim is made against the insured [i.e., the claim is made when a lawsuit is filed or a demand letter is sent to the insured plan], but only if the cyber event took place after the prior acts or continuity date of the policy. Typically the continuity date will be the date upon which the insured plan first purchased cyber coverage. For example, in a policy issued from January 1, 2022 to January 1, 2023, but with a retroactive or prior acts date of January 1, 2019, the policy will cover a lawsuit first filed on July 1, 2022 against a plan alleging losses from a data breach that took place on December 1, 2021. But it would not cover a lawsuit filed on the same date if the data breach took place on December 31, 2018, which is before the prior acts date.

**Limits:** Most primary policies will have aggregate limits of $1 million to $5 million in the current market, and larger plans will need to find excess limits – usually offered in the same up to $5m increments offered by the primary carrier – to achieve desired limits to fully protect the plan. Many small plans purchase $1m policies, but plans with assets over $50m, and certainly over $100-250m will want to seek higher limits. Most primary policies will state the limit for each insuring agreement – such as a $1,000,000 limit for Breach Response Costs and $1,000,000 for Cyber Extortion – and will state the applicable retention for each coverage part.

For example, a typical declarations page for a $1 million aggregate limit policy for a small benefit plan would read as follows:

**Third-Party Liability Coverages**

| Insuring Agreement | Limit/Sub-Limit | Retention |
|---|---|---|
| A. Network and Information Security Liability | $1,000,000 | $2,500 |
| B. Regulatory Defense and Penalties | $1,000,000 | $2,500 |
| C. Multimedia Content Liability | $1,000,000 | $2,500 |
| D. PCI Fines and Assessments | $1,000,000 | $2,500 |

**Third-Party Liability Coverages**

| Insuring Agreement | Limit/Sub-Limit | Retention |
|---|---|---|
| E. Breach Response Costs | $1,000,000 | $2,500 |
| F. Breach Response Services | $1,000,000 | $0 |
| G. Crisis Management and Public Relations | $1,000,000 | $2,500 |
| H. Cyber Extortion | $1,000,000 | $2,500 |
| I. Business Interruption and Extra Expense | $1,000,000 | $2,500<br>i.Waiting Period: 8 hours<br>ii. Enhanced Waiting Period: 8 hours |
| J. Digital Asset Restoration | $1,000,000 | $2,500 |

| | | |
|---|---|---|
| K. Funds Transfer Fraud | $500,000 | $12,500 |

As noted in the summary of cyber policy coverages, some policy coverages are treated as enhancements that are not in the base policy form, but added by endorsement. Many coverage enhancements added by endorsements contain a lower sublimit of coverage and higher retentions than core policy coverages. A typical set of endorsements for the policy identified above include the following:

**Policy Endorsements:**

- Bodily Injury and Property Damage Endorsement – 1st party [$250,000/$2,500]
- Bodily Injury and Property Damage Endorsement – 3rd party [$250,000/$2,500]
- Computer Replacement Endorsement [labeled "Bricking" by some carriers] [$500,000/$2,500]
- Pollution Endorsement
- Reputational Repair Endorsement
- Reputational Harm Loss Endorsement [$1,000,000/waiting period: 14 days]
- Service Fraud Endorsement [$100,00/$2,500]
- General Data Protection Regulation (GDPR) Enhancement Endorsement
- Court Attendance Cost Reimbursement Endorsement [$250 maximum amount per day, subject to a maximum amount of $25,000 per policy period]
- Criminal Reward Coverage Endorsement [$25,000 sublimit/$0 retention]
- Breach Response Separate Limit Endorsement [$1,000,000 additional limit of liability for breach response services]
- Social Engineering Coverage [$100,000 sublimit/$25,000 retention]

**What is Not Covered by a Cyber Policy:** Although the modern cyber policy contains broad coverage, every policy contains exclusions from coverage. Common exclusions involve bodily injury [not otherwise covered under the bodily injury insuring agreements]; confiscation of computer systems by governmental authorities; certain contractual liability; claims of directors and officers liability; discrimination and employment practices liability; fraud by a senior executive; governmental orders; illegal remuneration; claims by one insured against another insured; intellectual property infringement; merchant liability; natural disasters [defined as any physical event or natural disasters, including fire, flood, earthquake, volcanic eruption, explosion, lighting, wind, hail, tidal wave, and landslide]; nuclear exposure; pollutants [other than defense expenses if added by endorsement]; prior knowledge; recall or repair of computer systems; incidents that took place before the retroactive date of the policy; tangible property; third party mechanical failure; unfair trade practices; violations of laws, including ERISA, the Securities Acts of 1933 and 1934, RICO, CAN-SPAM Act, TCPA, and antitrust laws [TCPA coverage can be available by endorsements]; and war and terrorism.

The two most noteworthy exclusions are the war exclusion and the ERISA exclusion. The war and terrorism exclusion has varying definitions from policy to policy, and is being litigated in pending coverage lawsuits as to what constitutes an act of war or state-sponsored terrorism that is excluded from coverage. One common definition of "war and terrorism" is "war, invasion, acts of foreign enemies, terrorism, hostilities, civil war, rebellion, revolutions, insurrection, military, or usurped power," but carves out "cyber terrorism," which in turn is defined as "the premediated use, or threatened use, of disruptive activities against computer systems by any person, group, or

organization, committed with the intention to hard or intimidate you to further social, ideological, religious or political objectives." The distinction between a war that is not covered, and cyber terrorism that would be covered, is whether the activity "is part of or in support of any military action, war, or war-like operation."

For employee benefit plans, an ERISA exclusion is potentially problematic. For example, in July 2022, a participant filed a lawsuit against the Colgate-Palmolive Company defined contribution plan and its recordkeeper, alleging breach of fiduciary duty against plan fiduciaries for failing to prevent a cyber theft in which the entire approximately $750,000 account balance of the participant was fraudulently withdrawn from the plan. Although the ERISA exclusion has not been tested in court, it is possible that the cyber carrier would deny coverage for the breach of fiduciary duty lawsuit under the ERISA exclusion. This demonstrates why plans need fiduciary and crime insurance coverage to ensure a comprehensive insurance program that includes more than just cyber insurance. Potential coverage under the plan's fiduciary insurance is the next topic.

## FIDUCIARY LIABILITY INSURANCE

Fiduciary liability insurance is the key professional liability insurance protection for the fiduciaries of employee benefit plans. It is essentially malpractice insurance for plan fiduciaries. Just like doctors and lawyers need malpractice insurance to protect against claims that they did not live up to their professional duties, the fiduciaries of employee benefit plans need malpractice insurance to protect against claims that they failed to live up to their fiduciary duties to the plan and participants.
A fiduciary liability insurance policy is a contract designed to protect plan trustees, other fiduciaries and the employee benefit plan against claims alleging breach of their fiduciary duties to the plan or claims alleging they committed an error in the administration of the plan. The insurance company issues the insurance contract to the plan itself or to an employer that sponsors an employee benefit plan. The policy provides two important basic benefits, **defense** and **indemnity**: (1) the policy pays for the expense of defending fiduciaries accused of violating their duties to the benefit fund [i.e., providing a lawyer to defend you]; and (2) the policy also indemnifies trustees for their alleged violations of duty and negligent administrative acts or omissions in the event of a settlement or judgment of liability [i.e., payment of covered damages you owe to the complaining party]. While fiduciary liability policies provide coverage to the plan itself, the primary purpose of the fiduciary liability insurance policy is to protect against the individual liability of plan fiduciaries.

Many insurance companies are attempting to eliminate cyber exposure in insurance policies that are not designed specifically to cover cyber events. The purpose is to eliminate what is referred to as "silent cyber" coverage. Plan fiduciaries should review any insurance renewal closely to make sure that a new endorsement excluding a cyber event is not added to the policy if cyber coverage is desired. Without a cyber event exclusionary endorsement, the plan's fiduciary liability insurance policy should cover claims asserted by third-parties for alleged breach of fiduciary. We note that most prominent fiduciary carriers do not exclude cyber events from the fiduciary liability insurance policy.

Potential coverage for a cyber incident can be found in several places of a fiduciary liability insurance policy.

- **First**, the primary coverage grant in a fiduciary liability policy is for breaches of fiduciary responsibility under ERISA or other applicable fiduciary law. In the event of a data breach,

participants can sue the plan and its fiduciaries, alleging breach of fiduciary duty in protecting plan assets. This third-party claim would be defended under a fiduciary policy.

- **Second**, the second coverage grant is coverage for negligent errors in the administration of the plan even if the errors do not constitute breaches of fiduciary duty. In this context, administration commonly includes handling paperwork and records for the plan, providing interpretations with respect to any plan (including calculating and determining benefits), or giving advice to participants regarding the plan. Participants could allege that a data breach represents negligence in the administration of the plan.
- **Third**, a quality fiduciary liability insurance policy will provide coverage for regulatory enforcement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy and security rules that were broadened by the enactment of the Health Information Technology for Economic and Clinical Health Act (HITECH). One of the significant changes in the final rule is the expanded scope of the Department of Health and Human Services (HHS) enforcement authority, including civil monetary penalties up to an annual maximum for identical violations of $1.5 million, which is adjusted higher for inflation every year. The key for HIPAA coverage is to ensure that your carrier provides cover for both HIPAA's privacy and security rules, as some policies only refer to the privacy rule. Many carriers will provide $25,000 to $100,000 for HIPAA violations, but better policies will provide up to $1.5M in coverage. This will not be adequate to cover alleged intentional violations, or multiple violations in the same calendar year. If you have a health or welfare plan, you need at least $1.5M in HIPAA coverage, and should try to secure full policy limits if possible.

In sum, a fiduciary liability insurance policy should cover claims asserted by third parties – namely participants or regulators – that plan professionals failed to protect participant data and caused consequent losses. But while a fiduciary policy may cover third-party cyber claims, plans cannot rely solely on their fiduciary coverage to cover all cyber exposures because over 90% of cyber loss exposure is first-party risk. Specifically, plans have to notify participants under state privacy law in the event of a breach, often even where there is no proof that any participant has suffered any financial harm. Plans will also have the expense of a forensic investigation and other extra expenses in getting back to normal operations. This is why a cyber liability insurance policy is an essential insurance purchase for employee benefit plan, as none of this first-party exposure will be covered under a normal fiduciary liability insurance policy. But fiduciary insurance remains a necessary supplement to ensure complete coverage of third-party lawsuits alleging breach of fiduciary duty.

## FIDELITY BOND/CRIME POLICY

A fidelity bond is a contract under which the issuer of the bond, typically a surety company or an insurance carrier, agrees to reimburse a benefit fund for losses caused by theft, fraud, or other dishonest acts covered by the bond. A fidelity bond covers losses due to intentional acts to deprive a benefit fund of fund assets. By contrast, a fiduciary insurance policy covers losses caused by negligence or other acts or omissions not intended to cause the benefit fund to lose assets. But unlike fiduciary liability insurance that is discretionary, fidelity bonding is mandatory under ERISA.

The two key issues for a fidelity bond is to ensure that the proper plan officials are covered, and to ensure that the policy provides broad ERISA fraud and dishonesty coverage.

**Who must be bonded?** The ERISA standard is that each person who handles plan assets must be bonded. The ideal bond not only names the plan as the insured and covers the plan's trustees and employees, but also covers any natural persons employed by a vendor who would be required to be bonded. The reason is that fund assets are often handled by third parties. Euclid's coverage is even broader, expanding coverage to ". . . any other natural person who handles Employee Benefit Plan assets, whether or not required to be bonded . . ." With this language, coverage is automatic not only for the employees of a plan vendor, but also for the employees of entities typically exempt from ERISA's bonding requirements, such as banks and insurance companies. An employee of a non-fiduciary service provider would also be covered if they embezzle plan assets. The key provision to review is the definition of "Plan Official" or "Employee" to ensure that your bond meets the ERISA requirement.

**What scope of coverage is required?** The scope of coverage requirement under ERISA is "fraud or dishonesty." The bond is intended to protect the plan from loss by reason of fraudulent acts or dishonesty on the part of persons required to be bonded. Many bonds sold by insurance companies use a lesser, different standard of coverage for "employee theft" that may not meet the higher "fraud or dishonesty" standard of ERISA. Indeed, the Department of Labor has issued findings that bonds with the standard employee theft coverage are deficient.

**What limit of liability is required?** The bond limit is for each person required to be bonded and must equal ten (10) percent of the plan assets "handled," subjected to a minimum limit of $1,000 and a maximum required limit of $500,000. This maximum limit of liability increases to $1,000,000 if a plan's assets are invested in securities of any sponsor or contributing employer, unless these investments are via a "pool" such as a mutual or index fund. The ERISA limit requirement is the maximum required, but not necessarily the correct amount for your plan. For plans with assets in the tens or hundreds of millions, or even billions, trustees should consider higher limited. ERISA does not allow for a deductible on the "fraud" or "dishonesty" coverage for the required $500,000 or $1,000,000 limit of liability, however any additional third-party coverages may contain a deductible.

ERISA compliant bonds should contain an inflation guard provision which provides for an increased bond limit should the plan grow in assets during the policy period, thus requiring a higher limit to satisfy the ERISA minimum limit requirement. For policies covering more than one plan on the same policy, a provision allocating ERISA's required limit to each plan should be included to ensure that a covered loss which affects more than one plan does not exhaust the limit.

**Third-Party Crime Coverage:** Although ERISA only requires employee theft coverage, which is first-party coverage for just theft of assets by plan employees, broader coverage is available in a crime policy to address crime threats from third-parties (non-employees), including third-party computer fraud, wire fraud and forgery. Because many financial records are maintained and transactions conducted with computers, the risk is that third parties can hack into computer systems to steal plan assets. All of the standard commercial crime coverages except employee dishonesty contain exclusions that typically would eliminate coverage for theft accomplished via computer. The most important such exclusion is of loss from unauthorized property transfer. This exclusion eliminates coverage for loss to property that has been transferred outside the insured's premises (or a banking premises) on the basis of unauthorized instructions. There are two crime coverages that address this loss exposure:

- Computer fraud coverage
- Funds transfer fraud coverage

In the current ISO commercial crime forms, these two coverages are combined into a single coverage called computer and funds transfer fraud coverage.

- **Computer Fraud Coverage:** Computer Fraud coverage covers direct loss of money, securities and other property resulting directly from the use of any computer to fraudulently transfer insured property from inside the insured premises or bank premises to a person or place outside of the insured's premises. For example, a former employee used his supervisor's password to enter the insured's building and gain access to the supervisor's computer. He activated transactions to receive fake reimbursements allegedly made to the company's customers using his own bank routing number. Another example is an employee of a vendor fraudulently gained access to the insured's computer system and changed the bank routing number from the vendor to the employee's bank routing number in order to transfer a sum of money directly to the employee instead of the vendor.
- **Funds Transfer Fraud Coverage:** Funds Transfer Fraud coverage covers the direct loss of money and securities in the insured's transfer account on deposit at a financial institution committed by a third party and directly caused by:
    - Electronic, telephone or fax instruction which purports to have been transmitted by the insured but which was fraudulently transmitted by someone else without the insured's knowledge or consent;
    - Written instruction issued by the insured which is then forged or altered by someone else without the insured's knowledge or consent, or which purports to have been issued by the insured but was fraudulently issued without the insured's knowledge or consent; and
    - Electronic, telephone or fax instruction received by the insured which purports to have been transmitted by an employee but was fraudulently transmitted by someone else without the insured's or employee's consent.
- **Forgery and Alteration Coverage:** Forgery or Alteration Coverage covers loss due to dishonesty in writing, signing or altering checks, bank drafts, and other financial instruments.
- **Payment Instruction Fraud/Social Engineering Coverage:** As noted in the cyber section above, in social engineering schemes, scammers use official-seeming email communications to induce plan employees to transfer plan funds to the imposter's account. Most crime insurers have taken the position that payment instruction fraud is not a covered direct loss because the schemes do not involve a "hacking" of the company's systems – rather, the actual fund transfers are considered an indirect loss because they are voluntarily committed by an insured person with such person's knowledge or consent. In other words, the plan official or employee made the payment voluntarily, even though they were tricked into doing so by the social engineering scheme. Payment Instruction Fraud coverage is thus crucial to address this coverage gap because of the growing number of social engineering schemes to trick plan officials into sending plan asset to a fraudster's account. This coverage will usually be sublimited to a $100,000-$250,000 maximum, and subject to a sublimit, and

will require additional disclosures to confirm plan controls to guard against social engineering scams.

**Investigative Expenses:** Crime policies also typically include a sublimit of coverage for Investigative Expenses, which means the reasonable expenses incurred and paid by an Insured in establishing the existence and amount of any direct loss covered under the policy.

**Commercial General Liability Insurance**

As noted above, most security incidents are likely **not** covered by traditional commercial general liability (CGL) policies. The reason is that for liability coverage to apply under an insurance policy, there must first be either an "occurrence" or "personal and advertising injury." Most policies define "occurrence" as bodily injury or property damage caused by an accident, or words to that effect. The reason is that failure to prevent a data breach is not an "occurrence" under this definition.

Specifically, most CGL policies define bodily injury as "physical injury, sickness, or disease to a person." Data breaches do not typically result in such injuries. As for "property damage," a common definition is "physical injury to tangible property, including all resulting loss of use of that property" or "[l]oss of use of tangible property that is not physically injured or destroyed, provided such loss of use is caused by physical injury to or destruction of other tangible property." Again, this is not the type of injury normally associated with a data breach, especially with most CGL policies specifically stating that "electronic data is not tangible property." Courts routinely uphold such unambiguous provisions. In addition, many courts hold that purely economic losses are not included in the definition of "property damage." So, with no bodily injury or property damage, the chances of a data breach claim triggering the insuring agreement of your CGL are minimal, but should not be discounted in the event of a major data breach.

The final insuring agreement under CGL policies is "personal and advertising injury." "Personal and advertising injury" is specifically defined under most CGL policies, with only the listed items falling within that coverage – almost like a "named peril" policy. Most of the listed events are inapplicable to a data breach (e.g., false arrest, detention or imprisonment; malicious prosecution; wrongful eviction; copyright infringement). But there are two listed items under "personal and advertising injury" that some argue provide coverage for data breaches: (1) oral or written publication, in any manner, of material that slanders or libels a person or organization or disparages a person's or organization's goods, products or services; and (2) oral or written publication, in any manner, of material that violates a person's right of privacy.

Based on how most courts define "publication" (typically requiring communication to the public or the like by the insured), these parts of a CGL insuring agreement are also not triggered by most data breach allegations. The reason is that there is not a communication to the public in most data breach situations, and no such communication being made by the insured. To the contrary, it is usually through the criminal act of a third party that the data breach is conducted and then disseminated.

Finally, even if a data breach claim does trigger the insuring agreement of a CGL policy, there are numerous exclusions that would likely apply to still preclude coverage (such as the criminal acts

exclusion, and others). CGL policies exclude both data breach related financial liability losses and bodily injury and property damage liability claims caused by data breaches.

## SECTION TWO: UNDERWRITING STANDARDS – How Insurance Underwriters Evaluate and Price Applications for Cyber Liability Coverage

Modern cyber underwriting uses technology and system engineers to assist in risk selection. Initial underwriting of any application for cyber coverage starts with a cyber scan that attempts to find what hackers look for in potential victims. The cybersecurity scanning process is designed to detect the flaws in an applicant's system that real attackers are using today. Most of the scans are passive, meaning that they are performed using third-party data that is collected or hosted by outside resources. For example, the cyber carrier will check domain name system (DNS filtering) records for email configurations without touching an applicant's computers at all, or in most cases without directly interacting with an applicant's computers or networks. It is essentially knocking on an applicant's internet door without ever turning the doorknob. The purpose is to help identify system issues before an attacker finds them. If an automated scanning process is deemed insufficient, some accounts are selected for a secondary review in which a security engineer takes the additional time to manually inspect an insured's domains. Most carriers provide applicants with the result of the scan that identifies system issues which can be improved to proactively prevent cyber-attacks.

The next phase of underwriting involves assessing critical cyber controls of the applicant, based on the responses of the applicant to the cyber application required for most accounts. The following is an outline of the cyber controls in the underwriting evaluation of a potential risk:

- **Information and network security controls:**
  - Use of anti-virus software and a firewall to protect the network?
  - Use of a cloud provider to store data?
  - Does applicant encrypt all sensitive and confidential information stored on its organization's systems and networks?
- **Ransomware Controls:**
  - **Multifactor Authentication:** Which of the following services does the applicant enforce Multi-Factor Authentication (MFA):
    - Email
    - Virtual private network (VPN); Remote Desktop Protocol (RDP); RDWeb; RD Gateway; or other remote access
    - Network/cloud administration or other privileged user accounts
  - Does the applicant use 2-factor authentication to secure remote access to your networks?
  - Does the applicant use 2-factor authentication to secure remote access to your email accounts?
  - Do the applicant use endpoint detection and response (EDR) or a next-generation antivirus (NGAV) software (e.g., CrowdStrike, Cylance, Carbon Black) to secure all system endpoints?
- **Email Security:** Does the applicant use an email filtering solution designed to prevent phishing or ransomware attacks (in addition to any filtering solution(s) provided by your email provider)?

- **Data Backups: Does the applicant employ a data backup solution for all critical data?**
  - Does the applicant maintain at least weekly backups of all sensitive or otherwise critical data and all critical business systems offline or on a separate network?
  - How frequently does it run? Daily/Weekly/Monthly
  - Which of the following best describes your data backup solution?
    - Local backup
    - Network drive
    - Tape backup
    - Off-site storage
    - Cloud backup
    - Other?
  - The data provider used by the applicant
  - Is the data backup solution segregated or disconnected from the network in such a way to reduce or eliminate the risk of the backup being compromised in a malware or ransomware attack that spreads throughout the network?
- **Phishing Controls:**
  - Do any of the following employees at the applicant complete a social engineering training [that includes a phishing simulation]?
    - Employees with financial and accounting responsibilities;
    - Employees without financial or accounting responsibilities.
  - Does the applicant send and/or receive wire transfers? If yes:
    - Does applicant require a secondary means of communication to validate the authenticity of funds transfers (ACH, wire, etc.) requests before processing a request in excess of $25,000?
    - Does any wire transfer authorization process include the following?
      - A wire request documentation form?
      - A protocol for obtaining proper written authorization for wire transfers?
      - A separation of authority protocol?
      - A protocol for confirming all payments or funds transfer instructions/requests from a new vendor, client or customer via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer **before** the payment or funds transfer instruction/request was received?
      - Whether the protocol for confirming any vendor, client or customer account information change requests (including requests to change bank account numbers, contact information or mailing addresses) requires a direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer before the change request was received.
- **Prior Claims History:**

- Prior claims – loss history: cyber incidents resulting in a claim – usually last three years:
    - Within the last three years, has applicant been subject to any complaints concerning the content of its website, advertising materials, social media, or other publications?

- **Other Underwriting Factors:**
    - Does the applicant implement encryption on laptop computers, desktop computers, and other portable media devices?
    - Does the applicant have access to personally identifiable information (PII) or Protected Health Information (PHI) other than employees of the named insured? No records; less than 100,000; 100,000 to 500,00; 500,000-1,000,000; over 1,000,000
    - Does the Named Insured enforce procedures to remove content (including third-party content) that may infringe or violate any intellectual property or privacy right?

Some carriers require even more detailed underwriting for higher ransomware limits [note that some of these questions are duplicative of the underwriting controls detailed above, but are listed in full to demonstrate what is often required for ransomware coverage given the significant increase in these types of claims]:

**Ransomware Underwriting:**

- **Email Security:**
    - Does the applicant allow users to access email through a web app on a non-corporate device, and if so, do they enforce Multi-Factor Authentication?
    - Which email security filtering tool does the applicant use?
    - Is the applicant using all available security features (like quarantine service, sandboxing and URL rewriting)
    - Does the applicant conduct regular phishing training and testing? [and how often?]
    - Does applicant have a secure web gateway or proxy solution to secure inbound internet traffic?
- **Data backup and recovery:**
    - How frequently does the applicant back up electronic data? [daily with multi-generations retained?: daily; weekly; less than weekly]
    - Are all of backups kept separate from your network ("offline") so that they are inaccessible from endpoints and servers that are joined to the corporate domain, or in a cloud service designed for this purpose? [if no, what compensating controls are in place?]
    - Is multi-factor authentication required for access to backup files?
    - Has applicant tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months?
    - As part of the applicant's data back-up strategy, do they maintain at least 3 separate copies of your data stored in different geographic locations? [production, local copies, and off-sight storage]
- **Internal Security and Controls:**
    - Does the applicant use Multi-factor Authentication to secure all domain or network administrator accounts?
    - Does the applicant restrict employee access to sensitive information on a business need-to-know basis?

- Does the applicant use and Endpoint Detection and Response [EDR] or a Next-Generation Antivirus [NGAV] [i.e., CrowdStrike, SentinelOne, CybeReason, Carbon Black) software to secure all system endpoints?
- Does the applicant allow remote access to your network? If Yes: do you use:
  - A properly configured and secure VPN
  - Multi-factor authentication to secure all remote access to your network?
- Does the applicant have a Business Continuity Plan (BCP) or Disaster Recovery Plan (DRP) in place? If yes, is your BCP/IRP tested at least annually?
- Does the applicant encrypt all sensitive and confidential information that is:
  - Stored on your organization's systems and networks?
  - Stored on your organization's backups?
  - Segregation of servers that store sensitive and confidential information?
  - Access control with role-based assignments?
- Does the applicant encrypt all sensitive and confidential information that is:
  - Stored on mobile devices?
  - In transit from your network?

**How Premium is Calculated:** Once initial eligibility is determined, the initial premium for many carriers is calculated by two primary factors: (1) the number of records handled by the plan in paper or electronic form with private or sensitive information (including medical records, personal health information, social security numbers, back account details); and (2) the revenue of the insured. For purposes of benefit plans that are non-profit entities without real revenues, underwriters will typically use the plan contributions as the proxy for revenues in the premium rating model. Once the initial premium is calculated from sensitive records handled and contributions, the initial premium can be adjusted up or down with premium credits or debits based on the underwriter's perception of the cyber controls of the applicant.

Depending on your perspective as a purchaser or provider of cyber coverage, premiums have historically been very reasonable for employee benefit plans. Nevertheless, premiums have increased each of the last two years by thirty-five to one hundred percent. Many small plans with under $25 million in contribution traditionally could traditionally secure premiums for $1 million in coverage for between $1,000 and $2,500 premiums. Those minimum premiums have doubled, but are still reasonable [from our perspective as an insurance provider] given that they started from such a low base premium, but nevertheless have come as a shock to some plans who came to expect cyber as a low-cost insurance product. Premiums range from $1,500 to $20,000 per million of coverage, depending on the size of plan contributions and the number of records handled by the plan. We have seen $5m limit policies range from $7,500 for small plans to $200,000 for large plans [with over $1b in assets]. Plan sponsors should seek advice from an experienced cyber broker that can properly benchmark the plan's limit needs and whether the premium and coverage terms are appropriate.

## SECTION THREE: WHAT CYBERSECURITY CONTROLS ARE NEEDED TO SECURE CYBER COVERAGE

Before 2020, cyber insurance was readily available to most applicants with minimal underwriting. But with the rapid rise in ransomware and high-profile cyber losses, that changed abruptly two years ago. In the last two years, the standards for cyber coverage changed dramatically as underwriters

heightened underwriting criteria to qualify for coverage. As discussed in section two above, underwriters are now evaluating whether the plan applicant has a robust cyber security program to protect participant data and prevents cyber-attacks. The heightened cyber underwriting requirements apply to both new applicants and renewals, with renewals being denied if the insured does not have adequate multi-factor authentication and data backups. In the last year, the minimal cyber control threshold has expanded to the requirement for more sophisticated anti-virus software and use of endpoint detection and response. To evaluate cyber controls of potential applicants and even for renewals, underwriting applications about cybersecurity practices have expanded from one or two questions to multiple pages of required information.

While every carrier has different underwriting standards, and larger plans may be required to employ even more sophisticated cyber controls, the industry has standardized three key controls that are now required to obtain cyber coverage, even at renewal:

**Key Control #1: Multi-Factor Authentication**
Applicants can no longer obtain cyber coverage without verifying that they have employed multi-factor authentication for all remote access. The following are the types of MFA questions that require an affirmative response to obtain coverage:

**MFA Minimum Requirements:**

1. Do you implement Multi-Factor Authentication for all remote access?
2. Is Multi-Factor Authentication required to Access the following? Critical information, Personal devices, Administrator access and non-critical information and applications.
3. Is Multi-Factor Authentication required for access to Remote Desktop Protocol and Microsoft 365 Users?
4. Are backups subject to Multi-Factor Authentication?

**Key Control #2: Data Backups**
The second key control required to obtain cyber coverage is confirmation that key plan data is backed up offsite with segregated and multi-layer backups to ensure redundant sources of data storage.

**Backups – Minimum Requirements:**

1. Do you maintain offsite and/or cloud backups that are less than 1 month old?
2. Can you recover all of your business and critical data in less than 10 days?
3. How frequently is critical information backed up?

**Key Control #3: Endpoint Detection and Response**
Endpoint detection and response is the next generation of anti-virus protection that monitors in real-time what comes into your system to identify threat patterns.

**EDR – Minimum Requirements:**

1. Does the Applicant employ an endpoint detection and response solution?: Carbon Black Cloud, Cisco AMP, Crowdstrike Falcon, Cylance, Endgame Endpoint Protection, Symantec EDR, Windows Defender.

**<u>The Four Pillars of Cybersecurity</u>**

Cyber experts estimate that 95% of all breaches can be prevented with good cyber protocols. The idea is to make your entity a less enticing victim than other entities with poor controls. From Euclid's perspective, there are four pillars of cyber security:

(1) **Multi-factor Authentication [MFA/2FA]** – an electronic authorization that verifies a user is who they say they are;
(2) **Data Backups** – backup data you cannot live without;
(3) **Email Security** – tools to minimize bad emails getting through; and
(4) **Endpoint Protection and Response [EDR]** – monitor what comes into your system

Given that these four cybersecurity practices are now required nearly universally in order to apply for cyber insurance coverage, we review each key cyber control in more depth below.

**Pillar #1: Multifactor Authentication [MFA]**

MFA is an authentication method that requires that the user provide two or more credentials in order to gain access to an account. MFA is crucial for email and major lines of business applications. It is a second confirmation that you are an authorized user of the system. It is an electronic authorization method that verifies a user is who they say they are. The user is prompted with a secondary authentication method, which can be done through text, email, biometrics or facial recognition. The theory of MFA is to block the hacker and notify the user if an unauthorized user is trying to access your account. MFA has proven to be a game-changing control to prevent email compromise. Combined with outgoing payment controls to confirm that payment instructions are valid, MFA can prevent most cyber scams.

**Pillar #2: Data Backups**

The theory of backups is to backup data that you cannot live without to reduce ransomware leverage by a hacker. A backup is a copy of computer data that is stored at an alternate location for restoration in the event of data loss or breach. A well-constructed backup can help reduce the risk of downtime and data loss from a hacker. Plan administrators should consider the recovery-time objective (RTO) to evaluate what is an acceptable time to be down. Backup procedures should be multi-layered. The first consideration is the choice of image-level backups [that takes a mirror-copy of the entire system] versus file-level backups [that takes only copies of individual files and folders]. Image-level backups are full-system restoration, but take more space. The second backup consideration is onsite storage [on premise servers with backup data] versus cloud storage [unlimited storage saved in guarded data centers]. Backup best practices include: (1) testing the restoration of plan data to make sure the backup data is reusable; and (2) segregate backups to make sure the hacker cannot get to your backup data if your system is hacked. See Euclid's Fid Guru Blog for an explanation of the best practices of data backups: Implementing the 3-2-1 Backup Rule for Your Plan - Euclid Fiduciary (euclidspecialty.com)

**Pillar #3: Email Security**

Cyber experts estimate that 85% of all breaches involve email, and the number one cause of email breaches is phishing emails. This is why employee education is critical, as they are the first line of defense. Three tools work together to minimize bad emails from getting through: SPF; DKIM; and DMARC.

**Sender Policy Framework (SPF):** SPF is designed to verify the IP address of the sender's email services is actually an allowed IP address.

**Domain Keys Identified Mail (DKIM):** DKIM is designed to verify an encryption key and digital signature for each email to ensure it was not spoofed.

**Domain-based Message Authentication, Reporting and Conformance (DMARC):** DMARC brings SPF and DKIM together and creates a set of rules to determine how to treat emails that fail the authentication methods. Stated differently, it is a set of rules to authenticate incoming emails.

**Pillar #4: Endpoint Detection and Response [EDR]**

EDR monitors what comes into your system. It is real-time continuous monitoring of the system and a collection of endpoint data with rules-based automated response and analysis capabilities. EDR is a tool designed to find new threats as they are happening in real time and then execute to protect the endpoint or network. EDR is an advanced version of anti-virus software: anti-virus takes known malicious codes or software and protects against it, whereas EDR is artificial intelligence akin to active threat hunting. EDR, however, needs constant monitoring to be effective. EDR is now required to qualify for cyber insurance coverage, even on renewal.

The next level of protection is Managed Detection and Response or MDR. MDR is a service that monitors your network 24/7/365 in order to detect, triage, and respond to cybersecurity threats. While EDR is a tool-based approach, MDR is a people-using-tools based approach. As cyber technology experts explain, EDR works like a security system, setting off an alarm if a window is broken in an attempt to scare off the intruder and alert the business owner that something is amiss. By contrast, MDR is more like hiring a security guard that is the expert onsite, keeping an eye out for any suspicious activity.

**SECTION FOUR – THE EUCLID CYBER COVERAGE CHECKLIST: Coverage Tips When Buying Cyber Insurance**

An experienced cyber insurance broker will guide a plan through the policy negotiation, but the following is a checklist of coverage issues and thoughts to consider when purchasing cyber coverage.

- Broadest possible definition of triggering clauses or events – including "reasonably suspected events"
- Broadest possible definition of "computer system," including hardware, mobile devices, cloud storage, industry controls and IoT; including systems of third-parties on which business of policyholder depends.
- Business income loss triggered by interruption of business as a whole, rather than "computer system"
- Make sure BI coverage includes partial suspension or disruption
- Interruption of or attack on systems of third-parties (when in care & control of third parties, like plan TPAs, investment advisors, or TPAs)
- Business interruption expanded for operational errors
- Coverage for disruption of upstream (supplier; vendors) and downstream (participants and beneficiaries)
- Work upfront to schedule any preferred specific vendors that the applicant wants to use
- Review any coverage waiting periods and monetary retentions to ensure that the applicant understands its own obligations
- Social Engineering: not all policies cover social engineering; and some policies limit coverage to impersonating the CEO – the best coverage applies to anyone at the insured entity who can be impersonated. Also, applicants need to confirm whether there is a coverage requirement that the entity called back the person requesting funds for

verification. Also, applicants need to evaluate if social engineering is covered under the cyber and/or crime policies – and how are these sources of social engineering coverage coordinated.

- Some policies only cover certain types of "data" and/or limit coverage based on when and where it exists. Review any limits covering only electronic data – are paper files coverage? When possible, it is better to cover all types of data.
- Be sure that loss caused by insiders/employees is covered. Are insiders/employees covered? Some policies only cover loss caused by outsiders.
- Make sure the coverage does not require "updated software protections." Review limitations to ensure it does not require "updated software protections."
- War Exclusion: What is the scope of coverage for state-sponsored attacks, and how is the war exclusion defined? Ensure the war exclusion is not overreaching by precluding coverage for "acts of foreign enemies" and that there is a broad cyber terrorism carve-back.
- Make sure the insured's computer system includes coverage for data with third parties – more data services are transferred to third-party service providers, frequently called cloud services; also trust funds frequently have their data housed at their TPA. It becomes more important that these providers be included in the definition of "Insured's Computer System." Policies that do not include or specifically exclude cloud services create a significant exposure for the insured, which actually lacks coverage in this regard.
- Review all coverage limitations:
  - ****is there an exclusion for ERISA claims?**
  - Exclusions for professional services [potentially problematic for plans or internal TPAs that provide administrative services to other or related plans]
  - Conduct exclusions for criminal acts or intentional acts
  - Exclusions for "failure to follow minimum required practices"
  - Exclusions for failure to implement and enforce adequate cybersecurity measures
  - Social engineering claims will also fall outside cyber liability insurance policies unless specifically added
  - Mechanical/electronic failure exclusions removes coverage for claims caused by a mechanical shutdown, such as when your computer stops working – need carveback for cyber incidents
  - Laptop exclusions for portable electronics, including cell phones – ask if personal devices are covered
  - Patent, software, copyright infringement exclusion
- Breach Notification Trigger: does your policy's trigger of coverage allow for notification when there is no formal legal obligation to notify. Most policies require an affirmative data notification law, but some policies provide voluntary notice coverage. The event trigger must be a "failure to protect PII" as opposed to "failure to prevent an unauthorized disclosure."
- Definition of Computer System/Network: definition should not be restricted to just "hardware, software and components that are owned, operated, controlled or leased by the insured organization," but should include third-party service providers that host computer applications or that process, maintain or store the insured organization's data;

cloud storage used by the insured; and personal devices used by employees with the permission of the employer and subject to a Bring Your Own Device (BYOD) policy.

- Retroactive Coverage: many cyber policies state that the retroactive data is the date of the policy's inception for third-party actions and in some cases for first-party costs as well, which could limit or eliminate coverage for malware that was in your system unknown to you at the time you bought insurance.
- Other Insurance: how fiduciary, cyber, and crime policies will respond to a claim. May have multiple retentions.
- Compliance Coverage, including GDRP, CCPA and TCPA Coverage: Not all policies clearly cover regulatory fines that federal or state regulators may impose for a company's violation of a privacy statute where no underlying cyber incident occurred. Instead, some policies link reimbursement to the existence of a breach and its documentation. With the adoption of laws like the GDPR and the CCPA, some insurance companies are also offering cyber coverage that includes a "compliance" element. This is important because regulatory fines present significant potential costs. Under the CCPA, state regulatory fines range between $2,500 and $7,500 (intentional) per violation. A breach exposing 10,000 records could, if each record is considered a separate violation, lead to fines of tens of millions of dollars. Compliance coverage provides protection for regulatory fines where there is no underlying cyber incident.
- Coverage for Litigation Costs: Not all policies cover data breach- and privacy-related litigation costs, and others limit the type of litigation costs covered. The CCPA includes a private right of action that many believe will spawn a new wave of privacy class actions. The CCPA provides consumers a private right of action in the event their personal information is affected by a data breach and certain other conditions are met. Consumers may seek the greater of either actual damages or statutory damages ranging from $100 to $750 per consumer per incident. Defense costs could similarly increase as companies defend against shareholder lawsuits and other related litigation. A cyber policy that covers litigation defense helps a company prepare for and mitigate these costs.
- Coverage for Intentional Acts of Employees: Some cyber policies exclude coverage for intentional acts by the insured's employees. It is important to understand how this limitation may affect coverage for costs related to the access and disclosure of information by an employee not authorized to access such information. Some new state laws expand the definition of a breach to include "access," not just acquisition, in certain circumstances. For example, the CCPA may be interpreted as expanding the definition of "breach" to include unauthorized access and disclosure. The New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act similarly expands the definition of "breach of the security of the system" to include unauthorized access.

## CONCLUSION

Euclid hopes that this overview of cyber insurance is helpful to the ERISA Advisory Council as it evaluates how best to advise the Department of Labor and plan sponsors to protect employee benefit plans against modern cyber risks. Several themes are worth a final emphasis.

First, cyber coverage provides valuable coverage to respond to data breaches and to restore lost data but plans and plan sponsors should also ensure that they have coordinated fiduciary, crime and cyber insurance to ensure comprehensive first- and third-party protection against cyber threats.

Second, Euclid recommends that single-employer plan sponsors, including governmental plan sponsors, consider purchasing a separate cyber policy issued directly to sponsored employee benefit plans in order to protect plan assets and participant privacy risks.

Third, in order to qualify for cyber coverage, applicants must confirm that they have the four pillars of cyber security controls: (1) multi-factor authentication; (2) multi-layered data backups; (3) email security protocols; and (4) endpoint detection and response controls. These threshold cyber controls requirements demonstrate how cyber carriers have played a primary and critical role in improving the cyber controls of America's benefit plans.

Finally, cyber insurance is complex and not uniform, and thus plans must seek guidance of an experienced insurance broker with specific cyber insurance expertise in order to best protect the plan's interests.