USI SOLUTIONS FOR COMMERCIAL RISK MANAGEMENT

PrivaSafe – A CYBER EVENT SOLUTION – ALL VERTICALS

THE USI ONE ADVANTAGE®

www.usi.com

PRIVASAFE – A CYBER EVENT SOLUTION – ALL VERTICALS

Executive Summary

Proprietary solutions – broader coverage than standard market, competitive pricing, and pre- and post-cyber event services.

CONTROL + COST + COVERAGE

Why is it Important

- More frequent cyber events, impacting all organizations
- More severe cyber events – costly lawsuits, fines/penalties and event response costs
- Companies have limited expertise to deal effectively with a cyber event

Impact and Benefits to Clients

- Standard or "off the shelf" cyber policies have several inherent coverage gaps which can mean uninsured losses
- "PrivaSafe" has pre-negotiated coverage enhancements and pre/post-event services that close coverage gaps and protect our clients
- Pre-breach services can help organizations avoid threats and losses
- Post breach services streamline response and recovery during and after a cyber event

PRIVASAFE – A CYBER EVENT SOLUTION – ALL VERTICALS

Cyber Exposures and Coverage

1. Companies are increasingly at risk of experiencing a Cyber event
2. A cyber event can be financially catastrophic for most organizations
3. Standard Cyber policies are often issued without the available coverage enhancements
4. USI's **PrivaSafe** provides coverage for most of these exposures

PRIVASAFE – A CYBER EVENT SOLUTION – ALL VERTICALS

PrivaSafe – The Complete Cyber Solution

Comprehensive Cyber Coverage Requires Three (3) Distinct Offerings:

- 1st Party restoration,
- 3rd Party protection, and
- Services: Cyber event services to assist companies if there is an event

First Party Coverage

- Breach Event Costs
- Reputational Harm
- Business Interruption – Security and System Failure
- Ransomware/Extortion
- Cyber Crime
- Bricking Losses
- Property Damage

Third Party Coverage

- Security and Privacy Liability
- Privacy Regulatory Defense + Penalties
- Multimedia Liability
- PCI Penalties & Defense
- Bodily Injury Liability

Cyber Event Services

Pre-Cyber Event Training:

- Risk Updates
- Vendor Best Practices
- Employee Training

Post-Cyber Event Response:

- Pre-approved Experts
- Event Response
- Network Recovery

PRIVASAFE – A CYBER EVENT SOLUTION – ALL VERTICALS

Who is it for? All Organizations

Any Company Exposed to Cyber Events:

Has Personally Identifiable Information (PII)

Has Personal Healthcare Information (PHI)

Manages a Network

Accepts Credit Cards

PRIVASAFE – A CYBER EVENT SOLUTION – ALL VERTICALS

Top 4 Cyber Threats – all Verticals with notes

DATA BREACH

Protected or confidential data has been viewed, stolen, or used by an unauthorized individual.

- U.S. average cost is $9.9M – highest in the world*
- Worldwide average cost is: $4.4M*
- Top 3 Verticals in 2022: Pubilc Admin/Muni's ($5M), Finance ($6M) and Healthcare ($10M)**

BUSINESS INTERRUPTION

Attack that directly or indirectly causes business interruption or network degradation, incl. recovery costs.

- Cyber Business Interruption Costs average Loss by industry, by minute****
  - HC ($8400), FI ($2600) and MF ($17,000)
- Top Targeted Verticals in 2022: HC, MF and Public Int

CYBER EXTORTION

Cyber attack or threat of an attack against an organization coupled with a demand or request for money or other actions to avert or stop the attack.

- Incidents up worldwide/most common attack type – 30% of all manufacturers hit in 2022!**
- Average Ransomare attack: $4.5M worldwide – not including the ransom! Higher than a breach!*

SOCIAL ENGINEERING

"Business Email Compromise" or "Phishing" uses deception to manipulate individuals into divulging confidential or financial information.

- Social Engineering Scam Losses Up to average of $123,672 per Successful Attempt*** (up 50% YoY)
- Remote Workforces More Susceptible To This Type of Attack (Email, Text "smishing", Phone "vishing")***

*Taken from the IBM Cost of a Data Breach Study 2022 – most recent available

**Taken from the Verizon 2023 Data Breach Incident Response Report

***Taken from FBI reported losses and average – Social Engineering Report 2023

****Taken from Datto and NE Digital Report – "The Cost of Downtime Due to a Data Breach"

USI Expands and Optimizes Core Coverages vs. Standard Market

Click on a Coverage to Learn More

- Breach Event Response Costs Coverage
- Business Interruption and System Failure "Broad Form" Coverage
- Cyber Extortion
- Cyber Crime
- Pre-Incident Risk Management Training

Next Steps

Items requested if Cyber Coverage Currently in Place:

- Current Cyber Policy including all endorsements and most recent application
- Copy of most recent audited financials with notes (at a minimum revenue size is needed)
- Copy of Organizational structure with ownership (most recent)

Items requested if Cyber Coverage NOT Currently in Place:

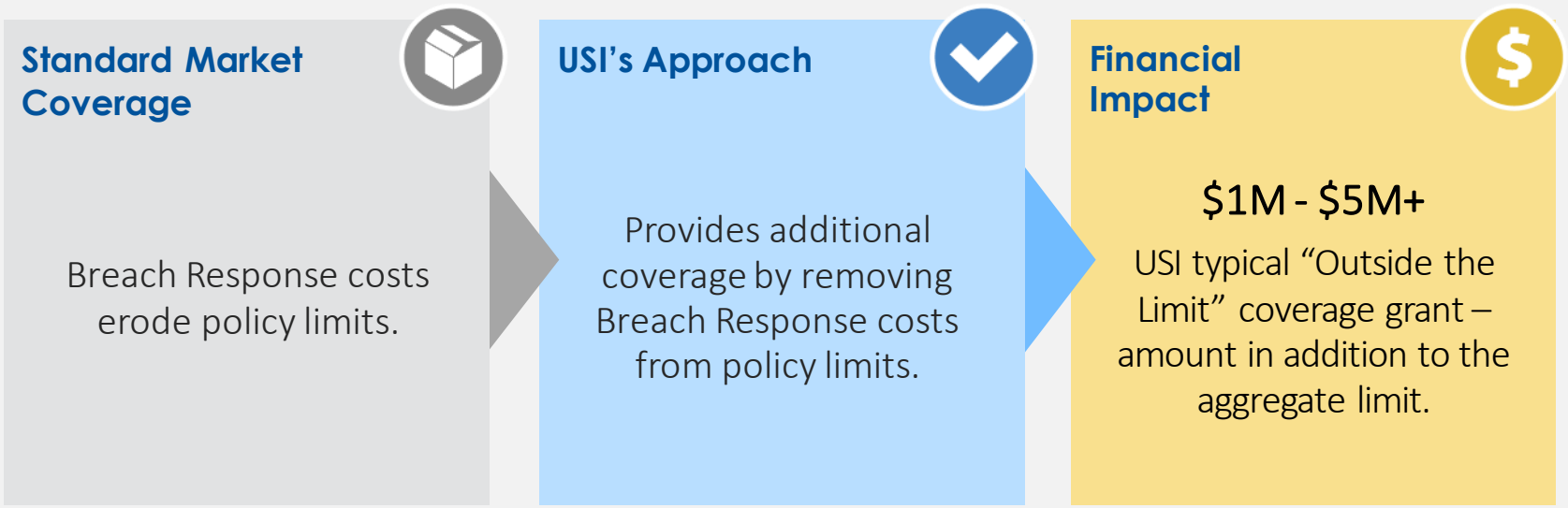
- Understanding of which cyber threat(s) does client believe pose the largest financial/operational impact to the organization
- Cyber preparedness plan
- Most recent audited financials

USI

USI Expands and Optimizes Core Coverages vs. Standard Market

Breach Event Response Costs Coverage – Outside the Limit

Breach response is required by statute. Costs covered include specialists for legal, forensic, notification, PR costs, credit monitoring/repair.



Coverages

USI Expands and Optimizes Core Coverages vs. Standard Market

Business Interruption and System Failure "Broad Form" Coverage

Covers the loss of business income and recovery expenses due to the interruption of an Insured's operations due to a Security Failure or System Failure.

Standard Market Coverage

- Direct Business Interruption (BI) must directly impact an Insured System and must be triggered by a "Security Failure."
- Contingent BI Cover: Non-IT providers are typically not included.

USI's Approach

- PrivaSafe includes both Direct and Contingent BI due to Security **and** System Failure ("Broad Form").
- Voluntary Shutdown and non-IT provider BI expansion is included.

Financial Impact

$1 Million +

USI typical baseline limit of coverage for Broad Form Business Interruption and System Failure.

Coverages

USI Expands and Optimizes Core Coverages vs. Standard Market

Cyber Extortion (aka "Ransomware) Coverage

Protects from a cyber attack or the threat of a cyber attack that includes a demand for payment.

Standard Market Coverage

Often does NOT contemplate crypto currency (such as bitcoins) or Personal Coverage for executives and their families.

USI's Approach

USI includes bitcoin and other "crypto" and has an exclusive "Personal Cover for Executives – Ransomware" option.

Financial Impact

$25,000 – $10M Impact

Coverages

USI Expands and Optimizes Core Coverages vs. Standard Market

Cyber Crime (Includes Social Engineering or "Phishing" Coverage, aka "Business Email" scams)

Standard Market Coverage

May be excluded and/or require specific request; additional Crime coverages may not be included outside of Social Engineering.

USI's Approach

Cyber Crime includes "Phishing" and USI also includes Crypto Jacking, Financial Fraud, Invoice Manipulation and Criminal Reward coverage.

Financial Impact

$125,000 up to $25M

While various sublimits may apply, USI can assist in "buy up" of Cyber crime coverage and placement of excess limit.

Coverages

USI Expands and Optimizes Core Coverages vs. Standard Market

Pre-Incident Risk Management Training – Carrier-Based and USI Unique Offering

Standard Market Coverage

- Pre-Incident Risk Management may not be included.
- Insureds not taught to use.
- Single carrier offerings can be very limited.

USI's Approach

- Pre-Incident Risk Management in all PrivaSafe offerings.
- "USI E-Risk Hub" – a broad form offering of Cyber Risk Management tools + training.

Financial Impact

$75,000 up to $37M

From an **average** of $75k to the $37M Toyota Loss.

A well-trained workforce is necessary to battle Cyber threats.

Coverages