NAIC NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

Date: 9/29/22

Virtual Meeting

RECEIVERSHIP AND INSOLVENCY (E) TASK FORCE
Tuesday, October 11, 2022
11:30 a.m. – 12:30 p.m. (Central)

ROLL CALL

James J. Donelon, Chair	Louisiana	Gary D. Anderson	Massachusetts
Cassie Brown, Vice Chair	Texas	Chlora Lindley-Myers	Missouri
Mark Fowler	Alabama	Troy Downing	Montana
Lori K. Wing-Heier	Alaska	Edward M. Deleon Guerrero	N. Mariana Islands
Peni Itula Sapini Teo	American Samoa	Eric Dunning	Nebraska
Michael Conway	Colorado	Marlene Caride	New Jersey
Andrew N. Mais	Connecticut	Mike Causey	North Carolina
Trinidad Navarro	Delaware	Judith L. French	Ohio
David Altmaier	Florida	Glen Mulready	Oklahoma
Colin M. Hayashida	Hawaii	Michael Humphreys	Pennsylvania
Dana Popish Severinghaus	Illinois	Alexander S. Adams Vega	Puerto Rico
Doug Ommen	Iowa	Elizabeth Kelleher Dwyer	Rhode Island
Vicki Schmidt	Kansas	Michael Wise	South Carolina
Sharon P. Clark	Kentucky	Carter Lawrence	Tennessee
Timothy N. Schott	Maine	Jon Pike	Utah
		Mike Kreidler	Washington

NAIC Support Staff: Jane Koenigsman

AGENDA

1. Receive a Proposal for Amendments to the *Property and Casualty Insurance Guaranty Association Model Act* (#540) for Cyber Insurance and Consider Exposing a Request for Model Law Development for Public Comment—*Roger Schmelzer (National Conference of Insurance Guaranty Funds—NCIGF)* — Pg. 1- Attachment One - Proposal; Pg. 81- Attachment Two – Draft MLR
2. Discuss Providing Feedback to Guaranty Funds on Future Uniform Data Standards (UDS) Enhancements—*Laura Lyon Slaymaker (PA)*
3. Consider Adoption of the Memorandum of Understanding for Pre-Liquidation Coordination—*Kevin Baldwin (IL)* — Pg. 83- Attachment Three
4. Discuss Any Other Matters Brought Before the Task Force —*Commissioner James J. Donelon (LA)*
5. Adjournment

Attachment One

Considerations for Insolvency Practitioners presented with Cyber Security Claims

I. Introduction

Cyber security insurance coverage is trending into the admitted market. Consequently, NCIGF anticipates the insurance insolvency resolution system will be presented with claims and other issues related to this coverage. These policy obligations may flow both from standalone cyber policies, endorsements, or from coverages that may be found to exist in commercial general liability and other lines of business typically written for business entities. For this reason, policymakers need to determine how such coverages will be handled should an insurer writing this business become insolvent. While each jurisdiction will need to decide whether, and within what parameters, cyber claims will be covered, we offer for consideration and guidance the attached amendments to the NAIC Property and Casualty Insurance Guaranty Association Act (NAIC Model 540). Policy makers should also consider how such claims will be handled before guaranty funds and associations (hereinafter "guaranty funds") are triggered – for example in a rehabilitation proceeding. Likewise, current insolvency processes and transition to the guaranty funds will need to be changed and enhanced to deal with this unique line of business and especially its demanding claims administration standards. For the purpose of this discussion, we offer the following information:

II. Key Cyber Insurance Facts and Characteristics

1) Cybersecurity ("Cyber") Insurance is a generalized term that covers a range of first-party and third-party policy coverages and benefits. While a policy could include various triggers, typically policy coverage is implicated by an unauthorized access to a computer system and/or by unauthorized access to or use of private or confidential information. Examples could include ransomware, malware, theft or loss of a device, improper disclosure of protected information, and more.

2) Policies often offer a policyholder as a policy benefit the opportunity to engage service providers to investigate a suspected infiltration, to give legal advice about a policyholder's regulatory or statutory reporting and notification obligations, to send notifications, and to give benefits to affected persons, such as credit monitoring. There may be coverage for the services of a ransomware negotiator and for a ransom paid in response to cyber extortion. The policies often include coverages directed to recovering or recreating data or access to data compromised by the incident. They may also afford business interruption coverage. In addition, policies generally provide liability coverage, including the provision of a defense, triggered by specific types of allegations or claims. Some policies contain e-crime coverages

such as social engineering losses, fraudulent instruction losses, etc.

3) There are currently no standardized Cyber Insurance policy forms, but the sample policies we have examined do have many characteristics of P&C insurance. While many descriptions of Cyber Insurance, such as those written by brokers and others promoting such insurance, do not convey this underlying reality, Cyber Insurance policies are similar to other conventional insurance coverage. Some of these similarities are described below.

4) Although Cyber policy forms are not standardized (in contrast to ISO forms, for example), there are trends toward certain common characteristics in these policies, including the following:

   a) Most, if not all, policies are written on a claims-made basis.
   b) Most typically, these policies have aggregate limits, with a current trend toward lower limits.
   c) Often there are sub-limits applicable to certain types of coverage.
   d) Amounts expended under the policy, including defense costs, typically erode the aggregate limits and, where applicable, appropriate sub-limits.
   e) Policies generally include retentions or deductibles to be borne by the policyholder, although a retention may be zero for some coverages, with a current trend toward higher retentions or deductibles.
   f) Generally, policies define all claims or losses arising from the same incident to be a single claim or loss.
   g) Some policies require a policyholder to use incident response (breach response) service providers from a preapproved list of vendors. Others may require prior mutual agreement to the retention of a particular service provider. As to defense counsel under a liability insuring agreement, prior mutual agreement is commonly required.
   h) Policies may vary, including by insuring agreement, as to whether an insurer reimburses a policyholder (meaning the policyholder pays in the first instance) or pays on behalf of a policyholder.

5) Coverages are modular and will vary significantly, even among policies issued by a specific insurer.

6) The range of services paid for by or on behalf of the policyholder are varied and novel as compared to traditional P&C products. The insurer is typically very active in identifying service provider options for the policyholder to consider engaging in terms of appropriate legal representation (including notification obligations), cyber forensic services and other ancillary services needed for regulatory compliance.

7) Another defining characteristic of Cyber Insurance is the required timeline for the insurer's response in the event of a triggering incident. Ideally, a policyholder's first notice of loss is given as soon as possible upon discovery, an insurer's response also must be very quick, and

any appropriate contact with breach counsel, computer forensics, and cyber extortion services vendors is arranged within a short time and with urgency. In summary, the timeline for responding to and servicing the claim is extremely short compared to typical property & casualty claims.

8) A significant benefit of the bargain for some policyholders, particularly small and middle market businesses, is obtaining the insurer's expertise in providing the policyholder access to qualified service providers to engage for the investigation of a cyber intrusion and breach response tactics, as well as legally evaluating and assisting with the complex regulatory compliance often required in such circumstances.

9) Cyber Insurance often covers ransomware extortion payments, even though United States policy strongly discourages such payments. Such payments have potential implications for compliance with OFAC (Office of Foreign Asset Control), sanctions, and perhaps other laws. We understand, however, that insurers do sometimes negotiate and pay such fees. There are also troubling trends shown in the data with implication for this coverage discussion: smaller companies are most frequently victimized by ransomware. We believe this coverage will need to be carefully evaluated in the discussions about Cyber Insurance.

10) The market for Cyber Insurance is dynamic and growing. While larger policyholders often have stand-alone Cyber Insurance policies, for some smaller insureds, Cyber Insurance coverage is more likely to be endorsed on to some other kind of policy, such as a CGL(Commercial General Liability), BOP(Business Owner's Policy), or Professional Liability policy. That said, there are also stand-alone policies for smaller insureds and that approach appears to be expanding. There are also some smaller specialty insurers that write Cyber Insurance coverages in the middle and main street markets.

11) Premium reporting for Cyber Insurance is somewhat uncertain because it is not its own line or classification. This appears to be changing, but the publicly available historical premium and experience data is limited. In general, however, and putting surplus lines Cyber Insurance aside, we believe that premiums for admitted Cyber Insurance generally are currently reported within the guaranty fund's assessable lines. This is an important distinction.

12) Cyber liability claims may also arise from CGL, medical malpractice, legal malpractice, and other commercial lines, sometimes referred to as "silent cyber" coverage.

III. Issues to Consider

Insolvency practitioners should consider the following issues:

1. What are appropriate guaranty fund limits if a jurisdiction decides to cover cyber claims?

While industry loss reporting for Cyber Insurance is not formally administered as such by a rating or advisory agency, the available voluntarily reported data indicates generally that the average claim for small and medium size businesses under these policies would fall within the claim cap (see attached 2021 claims study report). The claims costs for 2020 were materially higher than prior years. It is difficult to predict the future threat landscape and thus future claims costs, as the escalation in attacks is being met with a variety of defensive and mitigation strategies. At this juncture, however, the typical guaranty fund claims caps of $300,000-$500,000 should provide reasonably adequate coverage for most small and medium size businesses in most states. The statutory amendments offered in our revisions to the NAIC Model Act call for only one claim cap per incident.

2. Should the guaranty funds and receivers use vendors established in the policy to provide various services such as breach coaching, notification, forensics, etc.?

Sometimes use of certain vendors is mandated by the policy or accompanying documents. It may make sense for the receivers and guaranty funds to make use of pre-established vendors if they are still available, especially considering the short timelines in play for response on Cyber Insurance claims response. As we are all aware, however, sometimes vendor relationships can be disrupted in a liquidation context. It is thus advisable to expressly maintain the guaranty fund's statutory power to select counsel and service providers and direct the provision of legal and other services. Moreover, receivers should be prepared to address these services in a troubled company context. This issue is likely to require cooperative and innovative solutions.

3. What are considerations for amending guaranty fund acts and potentially other insolvency law that policymakers should take into account? ?

Guaranty fund laws are amended infrequently – any amendment should stand the test of time. Other typical guaranty fund provisions, such as the purpose clause, warranty exclusion, deemer provisions, and fine and penalty exclusions, should be reviewed in order to avoid conflicts with any Cyber Insurance amendments. Policymakers should also review net worth provisions embodied in many guaranty fund acts to ensure that claims payment and services provided on an expedited basis will be properly recovered from high net worth insureds as Cyber Insurance claims will require claims administration on a compressed timeline incompatible with high net worth vetting. As always and given that this coverage is also written on a surplus lines basis, it should be clear that GA coverage extends only to licensed business and does not extend to claims on surplus lines policies.

IV. Conclusion and Request for Collaboration

Finally, we ask that the NAIC and other policymaking bodies who are considering statutory amendments or other measures to address Cyber Insurance claims work with the NCIGF to develop solutions. The NCIGF Legal Committee has spent considerable time studying this

matter and the NCIGF wants to share the benefits of the knowledge acquired with the NAIC and other appropriate stakeholders in order to ensure that appropriate policy claims and claims related services for insurance consumers are not disrupted, thus upholding the insurance promise.

The point of contact for this matter for NCIGF is Barb Cox. Ms. Cox has tremendous resources and expertise available, as well, to assist in this matter.

NAIC Model Laws, Regulations, Guidelines and Other Resources—April 2009

PROPERTY AND CASUALTY INSURANCE GUARANTY ASSOCIATION MODEL ACT

Table of Contents

Section 1. Title

This Act shall be known as the [State] Insurance Guaranty Association Act.

Section 2. Purpose

The purpose of this Act is to provide a mechanism for the payment of covered claims under certain insurance policies, to avoid excessive delay in payment and to the extent provided in this Act minimize financial loss to claimants or policyholders because of the insolvency of an insurer, and to provide an association to assess the cost of such protection among insurers.

Section 3. Scope

This Act shall apply to all kinds of direct insurance, but shall not be applicable to the following:

A. Life, annuity, health or disability insurance;

B. Mortgage guaranty, financial guaranty or other forms of insurance offering protection against investment risks;

C. Fidelity or surety bonds, or any other bonding obligations;

D. Credit insurance, vendors' single interest insurance, or collateral protection insurance or any similar insurance protecting the interests of a creditor arising out of a creditor-debtor transaction;

E. Other than coverages that may be set forth in a cybersecurity insurance policy, insurance ~~Insurance of~~ warranties or service contracts including insurance that provides for the repair, replacement or service of goods or property, indemnification for repair, replacement or service for the operational or structural failure of the goods or property due to a defect in materials, workmanship or normal wear and tear, or provides

reimbursement for the liability incurred by the issuer of agreements or service contracts that provide such benefits;

F. Title insurance;

G. Ocean marine insurance;

H. Any transaction or combination of transactions between a person (including affiliates of such person) and an insurer (including affiliates of such insurer) which involves the transfer of investment or credit risk unaccompanied by transfer of insurance risk; or

I. Any insurance provided by or guaranteed by government.

Drafting Note: This Act focuses on property and liability kinds of insurance and therefore exempts those kinds of insurance deemed to present problems quite distinct from those of property and liability insurance. The Act further precludes from its scope certain types of insurance that provide protection for investment and financial risks. Financial guaranty is one of these. The NAIC Life and Health Insurance Guaranty Association Model Act provides for coverage of some, of the lines excluded by this provision.

For purposes of this section, "Financial guaranty insurance" includes any insurance under which loss is payable upon proof of occurrence of any of the following events to the damage of an insured claimant or obligee:

1. Failure of any obligor or obligors on any debt instrument or other monetary obligation, including common or preferred stock, to pay when due the principal, interest, dividend or purchase price of such instrument or obligation, whether failure is the result of a financial default or insolvency and whether or not the obligation is incurred directly or as guarantor by, or on behalf of, another obligor which has also defaulted;

2. Changes in the level of interest rates whether short term or long term, or in the difference between interest rates existing in various markets;

3. Changes in the rate of exchange of currency, or from the inconvertibility of one currency into another for any reason;

4. Changes in the value of specific assets or commodities, or price levels in general.

For purposes of this section, "credit insurance" means insurance on accounts receivable.

The terms "disability insurance" and "accident and health insurance," and "health insurance" are intended to be synonymous. Each State will wish to examine its own statutes to determine which is the appropriate phrase.

A State where the insurance code does not adequately define ocean marine insurance may wish to add the following to Section 5, Definitions: "Ocean marine insurance" means any form of insurance, regardless of the name, label or marketing designation of the insurance policy, which insures against maritime perils or risks and other related perils or risks, which are usually insured against by traditional marine insurance, such as hull and machinery, marine builders risk, and marine protection and indemnity. Perils and risk insured against include without limitation loss, damage, expense or legal liability of the insured for loss, damage or expense arising out of or incident to ownership, operation, chartering, maintenance, use, repair or construction of any vessel, craft or instrumentality in use in ocean or inland waterways for commercial purposes, including liability of the insured for personal injury, illness or death or for loss or damage to the property of the insured or another person.

Section 4. Construction

This Act shall be construed to effect the purpose under Section 2 which will constitute an aid and guide to interpretation.

Section 5. Definitions

As used in this Act:

[Optional:

A. "Account" means any one of the three accounts created by Section 6.]

Drafting Note: This definition should be used by those States wishing to create separate accounts for assessment purposes. For a note on the use of separate accounts for assessments see the Drafting Note after Section 6. If this definition is used, all subsequent subsections should be renumbered.

A. "Affiliate" means a person who directly, or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with another person on December 31 of the year immediately preceding the date the insurer becomes an insolvent insurer.

B. "Association" means the [State] Insurance Guaranty Association created under Section 6.

C. "Association similar to the association" means any guaranty association, security fund or other insolvency mechanism that affords protection similar to that of the association. The term shall also include any property and casualty insolvency mechanism that obtains assessments or other contributions from insurers on a preinsolvency basis.

Drafting Note: There are two options for handling claims assumed by a licensed carrier from an unlicensed carrier or self insurer. Alternative 1 provides that these claims shall be covered by the guaranty association if the licensed insurer becomes insolvent subsequent to the assumption. Alternative 2 provides coverage only if the assuming carrier makes a payment to the guaranty association in an amount equal to that which the assuming carrier would have paid in guaranty association assessments had the insurer written the assumed business itself. If a State wishes to adopt Alternative 1, it must select Alternative 1 in Section 5D and Alternative 1a or 2a in Section 8A(3). If a State wishes to adopt Alternative 2, it must select Alternative 2 in Section 5D and Q and Alternative 1b or 2b in Section 8A(3).

D. **[Alternative 1]** "Assumed claims transaction" means the following:

(1) Policy obligations that have been assumed by the insolvent insurer, prior to the entry of a final order of liquidation, through a merger between the insolvent insurer and another entity obligated under the policies; or

(2) An assumption reinsurance transaction in which all of the following has occurred:

(a) The insolvent insurer assumed, prior to the entry of a final order of liquidation, the claim or policy obligations of another insurer or entity obligated under the claims or policies: and

(b) The assumption of the claim or policy obligations has been approved, if such approval is required, by the appropriate regulatory authorities; and

(c) As a result of the assumption, the claim or policy obligations became the direct obligations of the insolvent insurer through a novation of the claims or policies

[Alternative 2] "Assumed claims transaction" means the following:

(1) Policy obligations that have been assumed by the insolvent insurer, prior to the entry of a final order of liquidation, through a merger between the insolvent insurer and another entity obligated under the policies, and for which Assumption Consideration has been paid to the applicable guaranty associations, if the merged entity is a non-member insurer; or

(2) Policy obligations that have been assumed by the insolvent insurer, prior to the entry of a final order of liquidation, pursuant to a plan, approved by the domestic commissioner of the assuming insurer, which:

(a) Transfers the direct policy obligations and future policy renewals from one insurer to another insurer; and

(b) For which Assumption Consideration has been paid to the applicable guaranty associations, if the assumption is from a non-member insurer.

(c) For purposes of this section the term non-member insurer also includes a self-insurer, non-admitted insurer and risk retention group; or

(3) An assumption reinsurance transaction in which all of the following has occurred:

(a) The insolvent insurer assumed, prior to the entry of a final order of liquidation, the claim or policy obligations of another insurer or entity obligated under the claims or policies;

(b) The assumption of the claim or policy obligations has been approved, if such approval is required, by the appropriate regulatory authorities; and

(c) As a result of the assumption, the claim or policy obligations became the direct obligations of the insolvent insurer through a novation of the claims or policies.

E. "Claimant" means any person instituting a covered claim, provided that no person who is an affiliate of the insolvent insurer may be a claimant.

F. "Commissioner" means the Commissioner of Insurance of this State.

Drafting Note: Use the appropriate title for the chief insurance regulatory official wherever the term "commissioner" appears.

G. "Control" means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of voting securities, by contract other than a commercial contract for goods or nonmanagement services, or otherwise, unless the power is the result of an official position with or corporate office held by the person. Control shall be presumed to exist if a person, directly or indirectly, owns, controls, holds with the power to vote, or holds proxies representing, ten percent (10%) or more of the voting securities of any other person. This presumption may be rebutted by a showing that control does not exist in fact.

H. "Covered claim" means the following:

(1) An unpaid claim, including one for unearned premiums, submitted by a claimant, which arises out of and is within the coverage and is subject to the applicable limits of an insurance policy to which this Act applies, if the insurer becomes an insolvent insurer after the effective date of this Act and: the policy was either issued by the insurer or assumed by the insurer in an assumed claims transaction; and

(a) The claimant or insured is a resident of this State at the time of the insured event, provided that for entities other than an individual, the residence of a claimant, insured or policyholder is the State in which its principal place of business is located at the time of the insured event; or

(b) The claim is a first party claim for damage to property with a permanent location in this State.

(2) Except as provided elsewhere in this section, "covered claim" shall not include:

(a) Any amount awarded as punitive or exemplary damages;

(b) Any amount sought as a return of premium under any retrospective rating plan;

(c) Any amount due any reinsurer, insurer, insurance pool or underwriting association, health maintenance organization, hospital plan corporation, professional health service corporation or self-insurer as subrogation recoveries, reinsurance recoveries, contribution, indemnification or otherwise. No claim for any amount due any reinsurer, insurer, insurance pool, underwriting association, health maintenance organization, hospital plan corporation, professional health service corporation or self-insurer may be asserted against a person insured under a policy issued by an insolvent insurer other than to the extent the claim exceeds the association obligation limitations set forth in Section 8 of this Act;

(d) Any claims excluded pursuant to Section 13 due to the high net worth of an insured;

(e) Any first party claims by an insured that is an affiliate of the insolvent insurer;

(f) Any fee or other amount relating to goods or services sought by or on behalf of any attorney or other provider of goods or services retained by the insolvent insurer or an insured prior to the date it was determined to be insolvent;

(g) Any fee or other amount sought by or on behalf of any attorney or other provider of goods or services retained by any insured or claimant in connection with the assertion or prosecution of any claim, covered or otherwise, against the association;

(h) Any claims for interest; or

(i) Any claim filed with the association or a liquidator for protection afforded under the insured's policy for incurred-but-not-reported losses.

Drafting note: The language in this provision referring to claims for incurred-but-not-reported losses has been inserted to expressly include the existing intent of this provision and make it clear that "policyholder protection" proofs of claim, while valid to preserve rights against the State of the insolvent insurer under the Insurer Receivership Model Act, are not valid to preserve rights against the association.

I."Cybersecurity insurance", for purposes of this Act, includes first and third party coverage, in a policy or endorsement, written on a direct, admitted basis for losses and loss mitigation arising out of or relating to data privacy breaches, unauthorized information network security intrusions, computer viruses, ransomware, cyber extortion, identity theft, and similar exposures.

Note: This definition is optional.

~~I.~~ J."Insolvent insurer" means an insurer that is licensed to transact insurance in this State, either at the time the policy was issued, when the obligation with respect to the covered claim was assumed under an assumed claims transaction, or when the insured event occurred, and against whom a final order of liquidation has been entered after the effective date of this Act with a finding of insolvency by a court of competent jurisdiction in the insurer's State of domicile.

Drafting Note: "Final order" as used in this section means an order which has not been stayed. States in which the "final order" language does not accurately reflect whether or not the order is subject to a stay should substitute appropriate language consistent with the statutes or rules of the State to convey the intended meaning.

~~J.~~ K."Insured" means any named insured, any additional insured, any vendor, lessor or any other party identified as an insured under the policy.

~~K.~~ L.(1) "Member insurer" means any person who:

(a) Writes any kind of insurance to which this Act applies under Section 3, including the exchange of reciprocal or inter-insurance contracts; and

(b) Is licensed to transact insurance in this State (except at the option of the State).

(2) An insurer shall cease to be a member insurer effective on the day following the termination or expiration of its license to transact the kinds of insurance to which this Act applies, however, the insurer shall remain liable as a member insurer for any and all obligations, including obligations for assessments levied prior to the termination or expiration of the insurer's license and assessments levied after the termination or expiration, which relate to any insurer that became an insolvent insurer prior to the termination or expiration of the insurer's license.

Formatted: Font: 10 pt
Formatted: Indent: First line: 0.5"
Formatted: Font: 10 pt
Formatted: Normal, No bullets or numbering
Formatted: List Paragraph, Indent: Left: 1"
Formatted: No bullets or numbering
Formatted: No bullets or numbering
Formatted: No bullets or numbering

~~L.~~ M. "Net direct written premiums" means direct gross premiums written in this State on insurance policies to which this Act applies, including policy and membership fees, less the following amounts: (1) return premiums, (2) premiums on policies not taken, and (3) dividends paid or credited to policyholders on that direct business. "Net direct written premiums" does not include premiums on contracts between insurers or reinsurers.

~~M.~~ N. "Novation" means that the assumed claim or policy obligations became the direct obligations of the insolvent insurer through consent of the policyholder and that thereafter the ceding insurer or entity initially obligated under the claims or policies is released by the policyholder from performing its claim or policy obligations. Consent may be express or implied based upon the circumstances, notice provided and conduct of the parties.

~~N.~~ O. "Person" means any individual, aggregation of individuals, corporation, partnership or other entity.

~~O.~~ P. ~~"~~Receiver" means liquidator, rehabilitator, conservator or ancillary receiver, as the context requires.

Drafting Note: Each State should conform the definition of "receiver" to the definition used in the State's insurer receivership act.

~~P.~~ ~~"Se~~Q. lf-insurer" means a person that covers its liability through a qualified individual or group self-insurance program or any other formal program created for the specific purpose of covering liabilities typically covered by insurance.

~~Q.~~ R. **[Alternative 2b]** "Assumption Consideration" shall mean the consideration received by a guaranty association to extend coverage to the policies assumed by a member insurer from a non-member insurer in any assumed claims transaction including liabilities that may have arisen prior to the date of the transaction. The Assumption Consideration shall be in an amount equal to the amount that would have been paid by the assuming insurer during the three calendar years prior to the effective date of the transaction to the applicable guaranty associations if the business had been written directly by the assuming insurer.

In the event that the amount of the premiums for the three year period cannot be determined, the Assumption Consideration will be determined by multiplying 130% against the sum of the unpaid losses, loss adjustment expenses, and incurred but not reported losses, as of the effective date of the Assumed claims transaction, and then multiplying such sum times the applicable guaranty association assessment percentage for the calendar year of the transaction.

The funds paid to a guaranty association shall be allocated in the same manner as any assessments made during the three year period. The guaranty association receiving the Assumption Consideration shall not be required to recalculate or adjust any assessments levied during the prior three calendar years as a result of receiving the Assumption Consideration. Assumption Consideration paid by an insurer may be recouped in the same manner as other assessments made by a guaranty association.

Section 6. Creation of the Association

There is created a nonprofit unincorporated legal entity to be known as the [State] Insurance Guaranty Association. All insurers defined as member insurers in Section 5K shall be and remain members of the association as a condition of their authority to transact insurance in this State. The association shall perform its functions under a plan of operation established and approved under Section 9 and shall exercise its powers through a board of directors established under Section 7.

[Alternate Section 6. Creation of the Association

There is created a nonprofit unincorporated legal entity to be known as the [State] Insurance Guaranty Association. All insurers defined as member insurers in Section 5K~~J~~ shall be and remain members of the association as a condition of their authority to transact insurance in this State. The association shall perform its functions under a plan of operation established and approved under Section 9 and shall exercise its powers through a board of directors established under Section 7. For purposes of administration and assessment, the association shall be divided into three separate accounts:

A. The workers' compensation insurance account;

Formatted: No bullets or numbering

Formatted: No bullets or numbering

Formatted: No bullets or numbering

Formatted: No bullets or numbering

Formatted: No bullets or numbering

Formatted: Font: Not Bold

Formatted: No bullets or numbering

B. The automobile insurance account; and

C. The account for all other insurance to which this Act applies.]

Drafting Note: The alternate Section 6 should be used if a State, after examining its insurance market, determines that separate accounts for various kinds of insurance are necessary and feasible. The major consideration is whether each account will have a base sufficiently large to cover possible insolvencies. Separate accounts will permit assessments to be generally limited to insurers writing the same kind of insurance as the insolvent company. If this approach is adopted the provision of alternate Sections 8A(3) and 8B(6) and optional Section 5A should also be used.

Section 7. Board of Directors

A. The board of directors of the association shall consist of not less than five (5) nor more than [insert number] persons serving terms as established in the plan of operation. The insurer members of the board shall be selected by member insurers subject to the approval of the commissioner. Vacancies on the board shall be filled for the remaining period of the term by a majority vote of the remaining insurer members subject to the approval of the commissioner. If no members are selected within sixty (60) days after the effective date of this Act, the commissioner may appoint the initial members of the board of directors. Two (2) persons, who must be public representatives, shall be appointed by the commissioner to the board of directors. Vacancies of positions held by public representatives shall be filled by the commissioner. A public representative may not be an officer, director or employee of an insurance company or any person engaged in the business of insurance. For the purposes of this section, the term "director" shall mean an individual serving on behalf of an insurer member of the board of directors or a public representative on the board of directors.

Drafting Note: A State adopting this language should make certain that its insurance code includes a definition of "the business of insurance" similar to that found in the NAIC Insurer Receivership Model Act.

B. In approving selections to the board, the commissioner shall consider among other things whether all member insurers are fairly represented.

C. Members of the board of directors may be reimbursed from the assets of the association for reasonable expenses incurred by them as members of the board of directors.

D. Any board member who is an insurer in receivership shall be terminated as a boar*d member*, effective as of the date of the entry of the order of receivership. Any resulting vacancies on the board shall be filled for the remaining period of the term in accordance with the provisions of Subsection A.

E. In the event that a director shall, because of illness, nonattendance at meetings or any other reason, be deemed unable to satisfactorily perform the designated functions as a director by missing three consecutive board meetings, the board of directors may declare the office vacant and the member or director shall be replaced in accordance with the provisions of Subsection A.

F. If the commissioner has reasonable cause to believe that a director failed to disclose a known conflict of interest with his or her duties on the board, failed to take appropriate action based on a known conflict of interest with his or her duties on the board, or has been indicted or charged with a felony, or misdemeanor involving moral turpitude, the commissioner may suspend that director pending the outcome of an investigation or hearing by the commissioner or the conclusion of any criminal proceedings. A company elected to the board may replace a suspended director prior to the completion of an investigation, hearing or criminal proceeding. In the event that the allegations are substantiated at the conclusion of an investigation, hearing or criminal proceeding, the office shall be declared vacant and the member or director shall be replaced in accordance with the provisions of Subsection A.

Section 8. Powers and Duties of the Association

A. The association shall:

(1) (a) Be obligated to pay covered claims existing prior to the order of liquidation, arising within thirty (30) days after the order of liquidation, or before the policy expiration date if less than thirty (30) days after the order of liquidation, or before the insured replaces the policy or causes its cancellation, if the insured does so within thirty (30) days of the order of liquidation. The obligation shall be satisfied by paying to the claimant an amount as follows:

(i) The full amount of a covered claim for benefits under a workers' compensation insurance coverage;

(ii) An amount not exceeding $10,000 per policy for a covered claim for the return of unearned premium;

(iii) An amount not exceeding $500,000 per claimant for all other covered claims.

(iv) In no event shall the Association be obligated to pay an amount in excess of $500,000 for all first- and third-party claims under a policy or endorsement providing or that is found to provide cybersecurity insurance coverage and arising out of or related to a single insured event, regardless of the number of claims made or the number of claimants.

Formatted: List Paragraph, No bullets or numbering

Formatted: List Paragraph, Indent: Left: 2", Space Before: Auto, After: Auto, Line spacing: Multiple 1.04

(b) In no event shall the association be obligated to pay a claimant an amount in excess of the obligation of the insolvent insurer under the policy or coverage from which the claim arises. Notwithstanding any other provisions of this Act, a covered claim shall not include a claim filed with the guaranty fund after the final date set by the court for the filing of claims against the liquidator or receiver of an insolvent insurer.

For the purpose of filing a claim under this subsection, notice of claims to the liquidator of the insolvent insurer shall be deemed notice to the association or its agent and a list of claims shall be periodically submitted to the association or association similar to the association in another State by the liquidator.

Drafting Note: On the general subject of the relationship of the association to the liquidator, the working group/task force takes the position that since this is a model State bill, it will be able to bind only two parties, the association and the in-State liquidator. Nevertheless, the provisions should be clear enough to outline the requests being made to out-of-State liquidators and the requirements placed on in-State liquidators in relation to out-of-State associations.

Drafting Note: Because of its potential impact on guaranty association coverage, it is recommended that the legislation include an appropriate provision stating that the bar date only applies to claims in liquidation commencing after its effective date. Drafters should insure that the State's insurance liquidation act would permit, upon closure, payments to the guaranty association and any association similar to the association for amounts that are estimated to be incurred after closure for workers compensation claims obligations. The amounts should be payable on these obligations related to losses both known and not known at the point of closure.

(c) Any obligation of the association to defend an insured shall cease upon the association's payment or tender of an amount equal to the lesser of the association's covered claim obligation limit or the applicable policy limit.

Drafting Note: The obligation of the association is limited to covered claims unpaid prior to insolvency, and to claims arising within thirty days after the insolvency, or until the policy is canceled or replaced by the insured, or it expires, whichever is earlier. The basic principle is to permit policyholders to make an orderly transition to other companies. There appears to be no reason why the association should become in effect an insurer in competition with member insurers by continuing existing policies, possibly for several years. It is also felt that the control of the policies is properly in the hands of the liquidator. Finally, one of the major objections of the public to rapid termination, loss of unearned premiums with no corresponding coverage, is ameliorated by this bill since unearned premiums are permissible claims, up to $10,000, against the association. The maximums ($10,000 for the return of unearned premium; $500,000 for all other covered claims) represent the working group's concept of practical limitations, but each State will wish to evaluate these figures.

(2) Be deemed the insurer to the extent of its obligation on the covered claims and to that extent, subject to the limitations provided in this Act, shall have all rights, duties and obligations of the insolvent insurer as if the insurer had not become insolvent, including but not limited to, the right to pursue and retain salvage and subrogation recoverable on covered claim obligations to the extent paid by the association. The association shall not be deemed the insolvent insurer for the purpose of conferring jurisdiction.

(3) **[Alternative 1a]** Assess insurers amounts necessary to pay the obligations of the association under Subsection A(1) subsequent to an insolvency, the expenses of handling covered claims subsequent to an insolvency, and other expenses authorized by this Act. The assessments of each member insurer shall be in the proportion that the net direct written premiums of the member insurer for the calendar year preceding the assessment bears to the net direct written premiums of all member insurers for the calendar year preceding the assessment. Each member insurer shall be notified of the assessment not later than thirty (30) days before it is due. A member insurer may not be assessed in any year an amount greater than two percent (2%) of that member insurer's net direct written premiums for the calendar year preceding the assessment. If the maximum assessment, together with the other assets of the association, does not provide in any one year an amount sufficient to make all necessary payments, the funds available shall be prorated and the unpaid portion shall be paid as soon as funds become available. The association may exempt or defer, in whole or in part, the assessment of a member insurer, if the assessment would cause the member insurer's financial statement to reflect amounts of capital or surplus less than the minimum amounts required for a certificate of authority by a jurisdiction in which the member insurer is authorized to transact insurance. However, during the period of deferment no dividends shall be paid to shareholders or policyholders. Deferred assessments shall be paid when the payment will not reduce capital or surplus below required minimums. Payments shall be refunded to those companies receiving larger assessments by virtue of the deferment, or at the election of the company, credited against future assessments.

[Alternative 2a] Assess insurers amounts necessary to pay the obligations of the association under Subsection A(1) subsequent to an insolvency, the expenses of handling covered claims subsequent to an insolvency, and other expenses authorized by this Act. The assessments of each member insurer shall be in the proportion that the net direct written premiums and any premiums received for an assumed contract after the effective date of an assumed claims transaction with a non-member insurer of the member insurer for the calendar year preceding the assessment bears to the net direct written premiums and any premiums received for an assumed contract after the effective date of an assumed claims transaction with a non-member insurer of all member insurers for the calendar year preceding the assessment. Each member insurer shall be notified of the assessment not later than thirty (30) days before it is due. A member insurer may not be assessed in any year an amount greater than two percent (2%) of that member insurer's net direct written premiums and any premiums received for an assumed contract after the effective date of an assumed claims transaction with a non-member insurer for the calendar year preceding the assessment. The 2% limitation on assessments shall not preclude a full payment for assumption consideration. If the maximum assessment, together with the other assets of the association, does not provide in any one year an amount sufficient to make all necessary payments, the funds available shall be prorated and the unpaid portion shall be paid as soon as funds become available. The association may exempt or defer, in whole or in part, the assessment of a member insurer, if the assessment would cause the member insurer's financial statement to reflect amounts of capital or surplus less than the minimum amounts required for a certificate of authority by a jurisdiction in which the member insurer is authorized to transact insurance. However, during the period of deferment no dividends shall be paid to shareholders or policyholders. Deferred assessments shall be paid when the payment will not reduce capital or surplus below required minimums. Payments shall be refunded to those companies receiving larger assessments by virtue of the deferment, or at the election of the company, credited against future assessments.

(3) **[Alternate 1b]** Allocate claims paid and expenses incurred among the three (3) accounts separately, and assess member insurers separately for each account, amounts necessary to pay the obligations of the association under Subsection 8A(1) subsequent to an insolvency, the expenses of handling covered claims subsequent to an insolvency and other expenses authorized by this Act. The assessments of each member insurer shall be in the proportion that the net direct written premiums of the member insurer for the calendar year preceding the assessment on the kinds of insurance in the account bears to the net direct written premiums of all member insurers for the calendar year preceding the assessment on the kinds of insurance in the account. Each member insurer shall be notified of the

assessment not later than thirty (30) days before it is due. A member insurer may not be assessed in any one year on any account an amount greater than two percent (2%) of that member insurer's net direct written premiums for the calendar year preceding the assessment on the kinds of insurance in the account. If the maximum assessment, together with the other assets of the association in any account, does not provide in any one year in any account an amount sufficient to make all necessary payments from that account, the funds available shall be pro-rated and the unpaid portion shall be paid as soon thereafter as funds become available. The association may exempt or defer, in whole or in part, the assessment of a member insurer, if the assessment would cause the member insurer's financial statement to reflect amounts of capital or surplus less than the minimum amounts required for a certificate of authority by a jurisdiction in which the member insurer is authorized to transact insurance. However, during the period of deferment no dividends shall be paid to shareholders or policyholders. Deferred assessments shall be paid when the payment will not reduce capital or surplus below required minimums. Payments shall be refunded to those companies receiving larger assessments by virtue of such deferment, or at the election of the company, credited against future assessments. A member insurer may set off against any assessment, authorized payments made on covered claims and expenses incurred in the payment of claims by the member insurer if they are chargeable to the account for which the assessment is made.]

(3) **[Alternate 2b]** Allocate claims paid and expenses incurred among the three (3) accounts separately, and assess member insurers separately for each account, amounts necessary to pay the obligations of the association under Subsection 8A(1) subsequent to an insolvency, the expenses of handling covered claims subsequent to an insolvency and other expenses authorized by this Act. The assessments of each member insurer shall be in the proportion that the net direct written premiums and any premiums received for an assumed contract after the effective date of an assumed claims transaction with a non-member insurer of the member insurer for the calendar year preceding the assessment on the kinds of insurance in the account bears to the net direct written premiums and any premiums received for an assumed contract after the effective date of an assumed claims transaction with a non-member insurer of all member insurers for the calendar year preceding the assessment on the kinds of insurance in the account. Each member insurer shall be notified of the assessment not later than thirty (30) days before it is due. A member insurer may not be assessed in any one year on any account an amount greater than two percent (2%) of that member insurer's net direct written premiums and any premiums received for an assumed contract after the effective date of an assumed claims transaction with a non-member insurer for the calendar year preceding the assessment on the kinds of insurance in the account. The 2% limitation on assessments shall not preclude a full payment for assumption consideration. If the maximum assessment, together with the other assets of the association in any account, does not provide in any one year in any account an amount sufficient to make all necessary payments from that account, the funds available shall be pro-rated and the unpaid portion shall be paid as soon thereafter as funds become available. The association may exempt or defer, in whole or in part, the assessment of a member insurer, if the assessment would cause the member insurer's financial statement to reflect amounts of capital or surplus less than the minimum amounts required for a certificate of authority by a jurisdiction in which the member insurer is authorized to transact insurance. However, during the period of deferment no dividends shall be paid to shareholders or policyholders. Deferred assessments shall be paid when the payment will not reduce capital or surplus below required minimums. Payments shall be refunded to those companies receiving larger assessments by virtue of such deferment, or at the election of the company, credited against future assessments. A member insurer may set off against any assessment, authorized payments made on covered claims and expenses incurred in the payment of claims by the member insurer if they are chargeable to the account for which the assessment is made.]

(4) Investigate claims brought against the association and adjust, compromise, settle and pay covered claims to the extent of the association's obligation and deny all other claims. The association shall pay claims in any order that it may deem reasonable, including the payment of claims as they are received from the claimants or in groups or categories of claims. The association shall have the right to appoint and to direct legal counsel retained under liability insurance policies for the defense of covered claims~~.~~ and to appoint and direct other service providers for covered services.

(5) Notify claimants in this State as deemed necessary by the commissioner and upon the commissioner's request, to the extent records are available to the association.

Drafting Note: The intent of this paragraph is to allow, in exceptional circumstances, supplementary notice to that given by the domiciliary receiver.

(6) (a) Have the right to review and contest as set forth in this subsection settlements, releases, compromises, waivers and judgments to which the insolvent insurer or its insureds were parties prior to the entry of the order of liquidation. In an action to enforce settlements, releases and judgments to which the insolvent insurer or its insureds were parties prior to the entry of the order of liquidation, the Association shall have the right to assert the following defenses, in addition to the defenses available to the insurer:

(i) The association is not bound by a settlement, release, compromise or waiver executed by an insured or the insurer, or any judgment entered against an insured or the insurer by consent or through a failure to exhaust all appeals, if the settlement, release, compromise, waiver or judgment was:

(I) Executed or entered within 120 days prior to the entry of an order of liquidation, and the insured or the insurer did not use reasonable care in entering into the settlement, release, compromise, waiver or judgment, or did not pursue all reasonable appeals of an adverse judgment; or

(II) Executed by or taken against an insured or the insurer based on default, fraud, collusion or the insurer's failure to defend.

(ii) If a court of competent jurisdiction finds that the association is not bound by a settlement, release, compromise, waiver or judgment for the reasons described in Subparagraph (a)(i), the settlement, release, compromise, waiver or judgment shall be set aside, and the association shall be permitted to defend any covered claim on the merits. The settlement, release, compromise, waiver or judgment may not be considered as evidence of liability or damages in connection with any claim brought against the association or any other party under this Act.

(iii) The association shall have the right to assert any statutory defenses or rights of offset against any settlement, release, compromise or waiver executed by an insured or the insurer, or any judgment taken against the insured or the insurer.

(b) As to any covered claims arising from a judgment under any decision, verdict or finding based on the default of the insolvent insurer or its failure to defend, the association, either on its own behalf or on behalf of an insured may apply to have the judgment, order, decision, verdict or finding set aside by the same court or administrator that entered the judgment, order, decision, verdict or finding and shall be permitted to defend the claim on the merits.

(7) Handle claims through its own employees, one or more insurers, or other persons designated as servicing facilities, which may include the receiver for the insolvent insurer. Designation of a servicing facility is subject to the approval of the commissioner, but the designation may be declined by a member insurer.

(8) Reimburse each servicing facility for obligations of the association paid by the facility and for expenses incurred by the facility while handling claims on behalf of the association and shall pay the other expenses of the association authorized by this Act.

(9) Submit, not later than 90 days after the end of the association's fiscal year, a financial report for the preceding fiscal year in a form approved by the commissioner.

B. The association may:

(1) Employ or retain persons as are necessary to handle claims, provide covered policy benefits and services, and perform other duties of the association;

(2) Borrow funds necessary to effect the purposes of this Act in accordance with the plan of operation;

(3) Sue or be sued;

(4) Negotiate and become a party to contracts necessary to carry out the purpose of this Act;

(5) Perform other acts necessary or proper to effectuate the purpose of this Act;

(6) Refund to the member insurers in proportion to the contribution of each member insurer to the association that amount by which the assets of the association exceed the liabilities, if at the end of any calendar year, the board of directors finds that the assets of the association exceed the liabilities of the association as estimated by the board of directors for the coming year.

[Alternate Section 8B(6)

(6) Refund to the member insurers in proportion to the contribution of each member insurer to that account that amount by which the assets of the account exceed the liabilities, if at the end of any calendar year, the board of directors finds that the assets of the association in any account exceed the liabilities of that account as estimated by the board of directors for the coming year.]

Drafting Note: The working group/task force feels that the board of directors should determine the amount of the refunds to members when the assets of the association exceed its liabilities. However, since this excess may be quite small, the board is given the option of retaining all or part of it to pay expenses and possibly remove the need for a relatively small assessment at a later time.

C. Suits involving the association:

(1) Except for actions by the receiver, all actions relating to or arising out of this Act against the association shall be brought in the courts in this State. The courts shall have exclusive jurisdiction over all actions relating to or arising out of this Act against the association.

(2) The exclusive venue in any action by or against the association is in [designate appropriate court]. The association may, at its option, waive this venue as to specific actions.

[Optional Section 8D

D. *(1) The legislature finds:*

(a) The potential for widespread and massive damage to persons and property caused by natural disasters such as earthquakes, windstorms, or fire in this State can generate insurance claims of such a number as to render numerous insurers operating within this State insolvent and therefore unable to satisfy covered claims;

(b) The inability of insureds within this State to receive payments of covered claims or to timely receive the payments creates financial and other hardships for insureds and places undue burdens on the State, the affected units of local government, and the community at large;

(c) The insolvency of a single insurer in a material amount or a catastrophic event may result in the same hardships as those produced by a natural disaster;

(d) The State has previously taken action to address these problems by adopting the [insert name of guaranty association act], which among other things, provides a mechanism for the payment of covered claims under certain insurance policies to avoid excessive delay in

payment and to avoid financial loss to claimants or policyholders because of the insolvency of an insurer; and

(e) In order for the association to timely pay claims of insolvent insurers in this State and otherwise carry out its duties, the association may require additional financing options. The intent of the Legislature is to make those options available to the association in the event that a natural disaster such as an earthquake, windstorm, fire or material insolvency of any member insurer results in covered claim obligations currently payable by the association in excess of its capacity to pay from current funds and current assessments under Subsection A(3). In cases where the association determines that it is cost effective, the association may issue bonds as provided in this subsection. In determining whether to issue bonds, the association shall consider the transaction costs of issuing the bonds.

(2) In the event a natural disaster such as an earthquake, windstorm, fire or material insolvency of any member insurer results in covered claim obligations currently payable by the association in excess of its capacity to pay from current funds and current assessments under Subsection 8A(3), the association, in its sole discretion, may by resolution request the [insert name of agency] Agency to issue bonds pursuant to [insert statutory authority], in such amounts as the association may determine to provide funds for the payment of covered claims and expenses related thereto. In the event bonds are issued, the association shall have the authority to annually assess member insurers for amounts necessary to pay the principal of, and interest on those bonds. Assessments collected pursuant to this authority shall be collected under the same procedures as provided in Subsection 8A(3) and, notwithstanding the two percent (2%) limit in Subsection 8A(3), shall be limited to an additional [insert percentage] percent of the annual net direct written premium in this State of each member insurer for the calendar year preceding the assessment. The commissioner's approval shall be required for any assessment greater than five percent (5%). Assessments collected pursuant to this authority may only be used for servicing the bond obligations provided for in this subsection and shall be pledged for that purpose.

(3) In addition to the assessments provided for in this subsection, the association in its discretion, and after considering other obligations of the association, may utilize current funds of the association, assessments made under Subsection 8A(3) and advances or dividends received from the liquidators of insolvent insurers to pay the principal and interest on any bonds issued at the board's request.

(4) Assessments under this subsection shall be payable in twelve (12) monthly installments with the first installment being due and payable at the end of the month after an assessment is levied, and subsequent installments being due not later than the end of each succeeding month.

(5) In order to assure that insurers paying assessments levied under this subsection continue to charge rates that are neither inadequate nor excessive, within ninety (90) days after being notified of the assessments, each insurer that is to be assessed pursuant to this subsection shall make a rate filing for lines of business additionally assessed under this subsection. If the filing reflects a rate change that, as a percentage, is equal to the difference between the rate of the assessment and the rate of the previous year's assessment under this subsection, the filing shall consist of a certification so stating and shall be deemed approved when made. Any rate change of a different percentage shall be subject to the standards and procedures of [cite appropriate statutory authority for provisions on filing and approval of rates].

Drafting Note: This provision should only be considered by those States that haveserious concerns that circumstances could result in a substantial capacity problem resulting in unpaid or pro rata payment of claims. An association intending to consider this provision should first consult with experienced bond counsel in its State to identify an appropriate State agency or bonding authority to act as vehicle for issuing the bonds. That agency or authority's statute may also have to be amended to specifically authorize these types of bonds and to cross-reference this provision in the guaranty association law. It is possible that in some situations a new bonding authority may have to be created for this purpose.

Regardless of the vehicle used, it is important that the decision-making authority on whether bonds are needed and in what amounts be retained by the association's board.

The extent of additional assessment authority under this subsection has not been specified. When considering the amount of additional authority that will be needed, a determination should be made as to the amount of funds needed to service the bonds. More specifically, consideration should be given to the amount of the bonds to be issued, interest rate and the maturity date of the bonds. The association should be able to raise sufficient funds through assessments to pay the interest and retire the bonds after some reasonable period (e.g. ten (10) years). Subsection D(2) requires the Commissioner's approval before the association can impose an additional assessment in excess of 5%. This is to assure that the additional assessment will not result in financial hardship to the member insurers and additional insolvencies.

The intent of Subsection D(4) is to permit recoupment by member insurers of the additional cost of assessments under this subsection without any related regulatory approval. A State enacting this subsection may need to revise Subsection D(4) so that it conforms to the particular State's recoupment provisions, as well as the provisions on filing and approval of rates.]

Section 9. Plan of Operation

A. (1) The association shall submit to the commissioner a plan of operation and any amendments to the plan of operation necessary or suitable to assure the fair, reasonable and equitable administration of the association. The plan of operation and amendments shall become effective upon approval in writing by the commissioner.

(2) If the association fails to submit a suitable plan of operation within ninety (90) days following the effective date of this Act, or if at any time thereafter the association fails to submit suitable amendments to the plan, the commissioner shall, after notice and hearing, adopt reasonable rules necessary or advisable to effectuate the provisions of this Act. The rules shall continue in force until modified by the commissioner or superseded by a plan submitted by the association and approved by the commissioner.

B. All member insurers shall comply with the plan of operation.

C. The plan of operation shall:

(1) Establish the procedures under which the powers and duties of the association under Section 8 will be performed;

(2) Establish procedures for handling assets of the association;

(3) Require that written procedures be established for the disposition of liquidating dividends or other monies received from the estate of the insolvent insurer;

(4) Require that written procedures be established to designate the amount and method of reimbursing members of the board of directors under Section 7;

(5) Establish procedures by which claims may be filed with the association and establish acceptable forms of proof of covered claims;

(6) Establish regular places and times for meetings of the board of directors;

(7) Require that written procedures be established for records to be kept of all financial transactions of the association, its agents and the board of directors;

(8) Provide that any member insurer aggrieved by any final action or decision of the association may appeal to the commissioner within thirty (30) days after the action or decision;

(9) Establish the procedures under which selections for the board of directors will be submitted to the commissioner;

(10) Contain additional provisions necessary or proper for the execution of the powers and duties of the association.

D. The plan of operation may provide that any or all powers and duties of the association, except those under Sections 8A(3) and 8B(2), are delegated to a corporation, association similar to the association or other organization which performs or will perform functions similar to those of this association or its equivalent in two (2) or more States. The corporation, association similar to the association or organization shall be reimbursed as a servicing facility would be reimbursed and shall be paid for its performance of any other functions of the association. A delegation under this subsection shall take effect only with the approval of both the board of directors and the commissioner, and may be made only to a corporation, association or organization which extends protection not substantially less favorable and effective than that provided by this Act.

Section 10. Duties and Powers of the Commissioner

A. The commissioner shall:

(1) Notify the association of the existence of an insolvent insurer not later than three (3) days after the commissioner receives notice of the determination of the insolvency. The association shall be entitled to a copy of a complaint seeking an order of liquidation with a finding of insolvency against a member company at the same time that the complaint is filed with a court of competent jurisdiction;

(2) Provide the association with a statement of the net direct written premiums of each member insurer upon request of the board of directors.

B. The commissioner may:

(1) Suspend or revoke, after notice and hearing, the certificate of authority to transact insurance in this State of a member insurer that fails to pay an assessment when due or fails to comply with the plan of operation. As an alternative, the commissioner may levy a fine on a member insurer that fails to pay an assessment when due. The fine shall not exceed five percent (5%) of the unpaid assessment per month, except that a fine shall not be less than $100 per month;

(2) Revoke the designation of a servicing facility if the commissioner finds claims are being handled unsatisfactorily.

(3) Examine, audit, or otherwise regulate the association.

Drafting Note: This section does not require periodic examinations of the guaranty associations but allows the commissioner to conduct examinations as the commissioner deems necessary.

C. A final action or order of the commissioner under this Act shall be subject to judicial review in a court of competent jurisdiction.

Section 11. Coordination Among Guaranty Associations

A. The association may join one or more organizations of other State associations of similar purposes, to further the purposes and administer the powers and duties of the association. The association may designate one or more of these organizations to act as a liaison for the association and, to the extent the association authorizes, to bind the association in agreements or settlements with receivers of insolvent insurance companies or their designated representatives.

B. The association, in cooperation with other obligated or potentially obligated guaranty associations, or their designated representatives, shall make all reasonable efforts to coordinate and cooperate with receivers, or

their designated representatives, in the most efficient and uniform manner, including the use of Uniform Data Standards as promulgated or approved by the National Association of Insurance Commissioners.

Section 12. Effect of Paid Claims

A. Any person recovering under this Act shall be deemed to have assigned any rights under the policy to the association to the extent of his or her recovery from the association. Every insured or claimant seeking the protection of this Act shall cooperate with the association to the same extent as the person would have been required to cooperate with the insolvent insurer. The association shall have no cause of action against the insured of the insolvent insurer for sums it has paid out except any causes of action as the insolvent insurer would have had if the sums had been paid by the insolvent insurer and except as provided in Subsection B and in Section 13. In the case of an insolvent insurer operating on a plan with assessment liability, payments of claims of the association shall not operate to reduce the liability of the insureds to the receiver, liquidator or statutory successor for unpaid assessments.

B. The association shall have the right to recover from any person who is an affiliate of the insolvent insurer all amounts paid by the association on behalf of that person pursuant to the Act, whether for indemnity, defense or otherwise.

C. The association and any association similar to the association in another State shall be entitled to file a claim in the liquidation of an insolvent insurer for any amounts paid by them on covered claim obligations as determined under this Act or similar laws in other States and shall receive dividends and other distributions at the priority set forth in [insert reference to Statepriority of distribution in liquidation act].

D. The association shall periodically file with the receiver or liquidator of the insolvent insurer statements of the covered claims paid by the association and estimates of anticipated claims on the association which shall preserve the rights of the association against the assets of the insolvent insurer.

Section 13 [Optional] Net Worth Exclusion

Drafting Note: Various alternatives are provided for a net worth limitation in the guaranty association act. States may choose any of the Subsection B alternatives below or may elect to not have any net worth limitation. Subsection A, which defines "high net worth insured," has two alternates allowing States to choose different net worth limitations for first and third party claims if that State chooses alternatives 1 or 2 to Subsection B. Subsections C, D and E are recommended to accompany any of the Subsection B alternatives. In cases where States elect not to include net worth, States may either omit this section in its entirety or include only Subsection C, which excludes from coverage claims denied by other States' net worth restrictions pursuant to those States' guaranty association laws.

A. For purposes of this section "high net worth insured" shall mean any insured whose net worth exceeds $50 million on December 31 of the year prior to the year in which the insurer becomes an insolvent insurer; provided that an insured's net worth on that date shall be deemed to include the aggregate net worth of the insured and all of its subsidiaries and affiliates as calculated on a consolidated basis.

[Alternate Section 13A

A. (1) For the purposes of Subsection B(1), "high net worth insured" shall mean any insured whose net worth exceeds $25 million on December 31 of the year prior to the year in which the insurer becomes an insolvent insurer; provided that an insured's net worth on that date shall be deemed to include the aggregate net worth of the insured and all of its subsidiaries and affiliates as calculated on a consolidated basis.]

(2) For the purpose of Subsection B(2) [and B(4) if Alternative 2 for Subsection B is selected] "high net worth insured" shall mean any insured whose net worth exceeds $50 million on December 31 of the year prior to the year in which the insurer becomes an insolvent insurer; provided that an insured's net worth on that date shall be deemed to include the aggregate net worth of the insured and all of its subsidiaries and affiliates as calculated on a consolidated basis.

Drafting Note: Alternate Subsection A language should only be considered in cases where a State is considering Alternative 1 or 2 of Subsection B and would like to set different dollar thresholds for the first party claim exclusion provision and the third party recovery provision.

Attachment One
NCIGF Suggested Amendments to Address Cyber Liability Claims August 30, 2022

NAIC Model Laws, Regulations, Guidelines and Other Resources—April 2009

Drafting Note: States may wish to consider the impact on governmental entities and charitable organizations of the application of the net worth exclusion contained in the definition of "covered claim." The Michigan Supreme Court, in interpreting a "net worth" provision in the Michigan guaranty association statute, held that governmental entities possess a "net worth" for purposes of the provision in the Michigan guaranty association statute that prohibits claims against the guaranty association by a person who has a specified net worth. Oakland County Road Commission vs. Michigan Property & Casualty Guaranty Association, 575 N.W. 2d 751 (Mich. 1998).

[Alternative 1 for Section 13B

B. (1) The association shall not be obligated to pay any first party claims by a high net worth insured.

(2) The association shall have the right to recover from a high net worth insured all amounts paid by the association to or on behalf of such insured, whether for indemnity, defense or otherwise.*]*

(3) The Association may also, at its sole discretion and without assumption of any ongoing duty to do so, pay any cybersecurity insurance obligations covered by a policy or endorsement of an insolvent company on behalf of a high net worth insured as defined in Section 13A(1). In that case, the Association shall recover from the high net worth insured under this Section all amounts paid on its behalf, all allocated claim adjusted expenses related to such claims, the Association's attorney's fees, and all court costs in any action necessary to collect the full amount to the Association's reimbursement under this Section.

Note: This revision would only be a consideration in states with a net worth exclusion.

[Alternative 2 for Section 13B

B. (1) The association shall not be obligated to pay any first party claims by a high net worth insured.

(2) Subject to Paragraph (3), the association shall not be obligated to pay any third party claim relating to a policy of a high net worth insured. This exclusion shall not apply to third party claims against the high net worth insured where:

(a) The insured has applied for or consented to the appointment of a receiver, trustee or liquidator for all or a substantial part of its assets;

(b) The insured has filed a voluntary petition in bankruptcy, filed a petition or an answer seeking a reorganization or arrangement with creditors or to take advantage of any insolvency law; or

(c) An order, judgment, or decree is entered by a court of competent jurisdiction, on the application of a creditor, adjudicating the insured bankrupt or insolvent or approving a petition seeking reorganization of the insured or of all or substantial part of its assets.

(3) Paragraph (2) shall not apply to workers' compensation claims, personal injury protection claims, no-fault claims and any other claims for ongoing medical payments to third parties.

(4) The association shall have the right to recover from a high net worth insured all amounts paid by the association to or on behalf of such insured, whether for indemnity, covered policy benefits and services, defense or otherwise.*]*

(5) The Association may also, at its sole discretion and without assumption of any ongoing duty to do so, pay any third-party claims or cybersecurity insurance obligations covered by a policy or endorsement of an insolvent company on behalf of a high net worth insured as defined in Section 13A(2). In that case, the Association shall recover from the high net worth insured under this Section all amounts paid on its behalf, all allocated claim adjusted expenses related to such claims, the Association's attorney's fees, and all court costs in any action necessary to collect the full amount to the Association's reimbursement under this Section.

Formatted: Font: Not Italic
Formatted: Indent: First line: 0"
Formatted: Font: Not Italic
Formatted: List Paragraph, No bullets or numbering
Formatted: Condensed by 0.15 pt
Formatted: Indent: Hanging: 0.5", Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 2 + Alignment: Left + Aligned at: 1.5" + Indent at: 1.5"
Formatted: Condensed by 0.15 pt
Formatted: Condensed by 0.15 pt
Formatted: Condensed by 0.15 pt

Note: This revision would only be a consideration in states with a net worth exclusion.

[Alternative 3 for Section 13B

B. The association shall not be obligated to pay any first party claims by a high net worth insured.*]*

C. The association shall not be obligated to pay any claim that would otherwise be a covered claim that is an obligation to or on behalf of a person who has a net worth greater than that allowed by the insurance guaranty association law of the State of residence of the claimant at the time specified by that State's applicable law, and which association has denied coverage to that claimant on that basis.

D. The association shall establish reasonable procedures subject to the approval of the commissioner for requesting financial information from insureds on a confidential basis for purposes of applying this section, provided that the financial information may be shared with any other association similar to the association and the liquidator for the insolvent insurer on the same confidential basis. Any request to an insured seeking financial information must advise the insured of the consequences of failing to provide the financial information. If an insured refuses to provide the requested financial information where it is requested and available, the association may, until such time as the information is provided, provisionally deem the insured to be a high net worth insured for the purpose of denying a claim under Subsection B.

E. In any lawsuit contesting the applicability of this section where the insured has refused to provide financial information under the procedure established pursuant to Subsection D, the insured shall bear the burden of proof concerning its net worth at the relevant time. If the insured fails to prove that its net worth at the relevant time was less than the applicable amount, the court shall award the association its full costs, expenses and reasonable attorneys' fees in contesting the claim.

Section 14. Exhaustion of Other Coverage

A. (1) Any person having a claim against an insurer,, shall be required first to exhaust all coverage provided by any other policy, including the right to a defense under the other policy, if the claim under the other policy arises from the same facts, injury or loss that gave rise to the covered claim against the association. The requirement to exhaust shall apply without regard to whether the other insurance policy is a policy written by a member insurer. However, no person shall be required to exhaust any right under the policy of an insolvent insurer or any right under a life insurance policy.

(2) Any amount payable on a covered claim under this Act shall be reduced by the full applicable limits stated in the other insurance policy, or by the amount of the recovery under the other insurance policy as provided herein. The association shall receive a full credit for the stated limits, unless the claimant demonstrates that the claimant used reasonable efforts to exhaust all coverage and limits applicable under the other insurance policy. If the claimant demonstrates that the claimant used reasonable efforts to exhaust all coverage and limits applicable under the other insurance policy, or if there are no applicable stated limits under the policy, the association shall receive a full credit for the total recovery.

[Alternative 1 for Section 14A(2)(a)

The credit shall be deducted from the lesser of:
(i) The association's covered claim limit;
(ii) The amount of the judgment or settlement of the claim; or
(iii) The policy limits of the policy of the insolvent insurer.*]*

[Alternative 2 for Section 14A(2)(a)

The credit shall be deducted from the lesser of:
(i) The amount of the judgment or settlement of the claim; or (ii) The policy limits of the policy of the insolvent insurer.*]*

Formatted: Indent: Left: 2", No bullets or numbering

(b) In no case, however, shall the obligation of the association exceed the covered claim limit embodied in Section 8 of this Act.

(3) Except to the extent that the claimant has a contractual right to claim defense under an insurance policy issued by another insurer, nothing in this section shall relieve the association of the duty to defend under the policy issued by the insolvent insurer. This duty shall, however, be limited by any other limitation on the duty to defend embodied in this Act.

(4) A claim under a policy providing liability coverage to a person who may be jointly and severally liable as a joint tortfeasor with the person covered under the policy of the insolvent insurer that gives rise to the covered claim shall be considered to be a claim arising from the same facts, injury or loss that gave rise to the covered claim against the association.

(5) For purposes of this section, a claim under an insurance policy other than a life insurance policy shall include, but is not limited to:

(a) A claim against a health maintenance organization, a hospital plan corporation, a professional health service corporation or disability insurance policy; and

(b) Any amount payable by or on behalf of a self-insurer.

(6) The person insured by the insolvent insurer's policy may not be pursued by a third-party claimant for any amount paid to the third party by which the association's obligation is reduced by the application of this section.

B. Any person having a claim which may be recovered under more than one insurance guaranty association or its equivalent shall seek recovery first from the association of the place of residence of the insured, except that if it is a first party claim for damage to property with a permanent location, the person shall seek recovery first from the association of the location of the property. If it is a workers' compensation claim, the person shall seek recovery first from the association of the residence of the claimant. Any recovery under this Act shall be reduced by the amount of recovery from another insurance guaranty association or its equivalent.

Drafting Note: This subsection does not prohibit recovery from more than one association, but it does describe the association to be approached first and then requires that any previous recoveries from like associations must be set off against recoveries from this association.

Section 15. Prevention of Insolvencies

To aid in the detection and prevention of insurer insolvencies:

A. The board of directors may, upon majority vote, make recommendations to the commissioner on matters generally related to improving or enhancing regulation for solvency.

B. At the conclusion of any domestic insurer insolvency in which the association was obligated to pay covered claims, the board of directors may, upon majority vote, prepare a report on the history and causes of the insolvency, based on the information available to the association and submit the report to the commissioner.

C. Reports and recommendations provided under this section shall not be considered public documents.

Section 16. Tax Exemption

The association shall be exempt from payment of all fees and all taxes levied by this State or any of its subdivisions except taxes levied on real or personal property.

Section 17. Recoupment of Assessments

Drafting Note: States may choose how they wish to allow member insurers to recoup assessments paid by selecting one of three alternatives for Section 17.

[*Alternative 1 for Section 17*

A. Except as provided in Subsection D, each member insurer shall annually recoup assessments it remitted in preceding years under Section 8. The recoupment shall be by means of a policyholder surcharge on premiums charged for all kinds of insurance in the accounts assessed. The surcharge shall be at a uniform percentage rate determined annually by the commissioner that is reasonably calculated to recoup the assessment remitted by the insurer, less any amounts returned to the member insurer by the association. Changes in this rate shall be effective no sooner than 180 days after insurers have received notice of the changed rate.

B. If a member insurer fails to recoup the entire amount of the assessment in the first year under this section, it shall repeat the surcharge procedure provided for herein in succeeding years until the assessment is fully recouped or a de minimis amount remains uncollected. Any such de minimis amount shall be collected as provided in Subsection D of this section. If a member insurer collects excess surcharges, the insurer shall remit the excess amount to the association, and the excess amount shall be applied to reduce future assessments in the appropriate account.

C. The amount and nature of any surcharge shall be separately stated on either a billing or policy declaration sent to an insured. The surcharge shall not be considered premium for any purpose, including the [insert all appropriate taxes] or agents' commission.

D. A member may elect not to collect the surcharge from its insureds only when the expense of collecting the surcharge would exceed the amount of the surcharge. In that case, the member shall recoup the assessment through its rates, provided that:

(1) The insurer shall be obligated to remit the amount of surcharge not collected by election under this subsection; and

(2) The last sentence in Subsection C above shall not apply.

E. In determining the rate under Subsection A for the first year of recoupment under this section, under rules prescribed by the commissioner, the commissioner shall provide for the recoupment in that year, or in such reasonable period as the commissioner may determine, of any assessments that have not been recouped as of that year. Insurers shall not be required to recoup assessments through surcharges under this section until 180 days after this section takes effect.*]*

[*Alternative 2 for Section 17*

A. Notwithstanding any provision of [insert citation to relevant tax and insurance codes] to the contrary, a member insurer may offset against its [insert all appropriate taxes] liability the entire amount of the assessment imposed under this Act at a rate of [insert number] percent per year for [insert number of years] successive years following the date of assessment. If the assessment is not fully recovered over the [insert number of years] period, the remaining unrecovered assessment may be claimed for subsequent calendar years until fully recovered.

Drafting Note: States may choose the number of years to allow an insurer to offset an assessment against the insurer's premium tax liability.

B. Any tax credit under this section shall, for the purposes of Section [insert citation to retaliatory tax statute] be treated as a tax paid both under the tax laws of this State and under the laws of any other State or country.

C. If a member insurer ceases doing business in this State, any uncredited assessment may be credited against its [insert all appropriate taxes] during the year it ceases doing business in this State.

D. Any sums that are acquired by refund from the association by member insurers and that have been credited against [insert all appropriate taxes], as provided in this section, shall be paid by member insurers to this State as required by the department. The association shall notify the department that the refunds have been made.*]*

[*Alternative 3 for Section 17*
The rates and premiums charged for insurance policies to which this section applies shall include amounts sufficient to recoup a sum equal to the amounts paid to the association by the member insurer less any amounts returned to the member insurer by the association. Rates shall not be deemed excessive because they contain an additional amount reasonably calculated to recoup all assessments paid by the member insurer.*]*

Section 18. Immunity

There shall be no liability on the part of, and no cause of action of any nature shall arise against a member insurer, the association or its agents or employees, the board of directors, or any person serving as an alternate or substitute representative of any director, or the commissioner or the commissioner's representatives for any action taken or any failure to act by them in the performance of their powers and duties under this Act

Section 19. Stay of Proceedings

All proceedings in which the insolvent insurer is a party or is obligated to defend a party in any court in this State shall, subject to waiver by the association in specific cases involving covered claims, be stayed for six (6) months and such additional time as may be determined by the court from the date the insolvency is determined or an ancillary proceeding is instituted in the State, whichever is later, to permit proper defense by the association of all pending causes of action.

The liquidator, receiver or statutory successor of an insolvent insurer covered by this Act shall permit access by the board or its authorized representative to such of the insolvent insurer's records which are necessary for the board in carrying out its functions under this Act with regard to covered claims. In addition, the liquidator, receiver or statutory successor shall provide the board or its representative with copies of those records upon the request by the board and at the expense of the board.

Chronological Summary of Actions (all references are to the Proceedings of the NAIC).

1970 Proc. I 218, 252, 253-262, 298 (adopted).
1972 Proc. I 15, 16, 443, 477-478, 479-480 (amended).
1973 Proc. I 9, 11, 140, 154, 155-157 (amended).
1973 Proc. II 18, 21, 370, 394, 396 (recoupment formula adopted).
1979 Proc. I 44, 46, 126, 217 (amended).
1981 Proc. I 47, 50, 175, 225 (amended).
1984 Proc. I 6, 31, 196, 326, 352 (amended).
1986 Proc. I 9-10, 22, 149, 294, 296-305 (amended and reprinted).
1986 Proc. II 410-411 (amendments adopted later printed here).
1987 Proc. I 11, 18, 161, 421, 422, 429, 450-452 (amended).
1993 Proc. 2nd Quarter 12, 33, 227, 600, 602, 621 (amended).
1994 Proc. 4th Quarter 17, 26, 566, 576, 579-589 (amended and reprinted).
1996 Proc. 1st Quarter 29-30, 123, 564, 570, 570-580 (amended and reprinted).
2009 Proc. 1st Quarter, Vol I 111, 139, 188, 288-317 (amended).

NetDiligence®

CYBER CLAIMS STUDY

2021 REPORT

OUR SPONSORS

RSM

experian

GUIDEWIRE CYENCE

Beckage
Legally Focused. Technology Driven.

Contents

Introduction

Welcome to the eleventh annual NetDiligence® *Cyber Claims Study*. Each year the study has grown, from fewer than 100 claims in 2011 to almost 6,000 claims in 2021. This large number of claims has allowed us to explore the data more thoroughly and produce the most comprehensive report ever. Growth continues in the number of claims submitted, as well as the in categories of the data analyzed.

This report includes incidents that occurred during the five-year period 2016–2020. A total of 5,797 claims was analyzed. By comparison, the sixth Cyber Claims Study, published in 2016, analyzed fewer than 200 cyber insurance claims. While many of the categories over the last five years have remained the same, the data has changed, sometimes dramatically.

By the Numbers

- 5,797 claims analyzed, arising from incidents that occurred during 2016–2020
- 3,000 new claims collected in 2021, from incidents occurring from 2018–2020
- 1,423 claims analyzed arising from incidents occurring in 2020·
- 99% of claims ($537M in total) from Small to Medium Enterprises (SMEs) with less than $2 billion in annual revenue
- 1% of claims ($727M in total) from Large Companies with more than $2 billion in annual revenue
- Almost 1,500 claims due to ransomware, 55% of which occurred in 2019 and 2020
- 557 ransomware claims which provide both the ransom demand and the total incident cost

To present more accurate pictures of the business impact of cyber events on smaller versus larger organizations, findings for SMEs are often presented separately from findings for large companies[1].

Preliminary Observations

- As has been the case since the first *Cyber Claims Study* was published eleven years ago, there are enormous variances in the magnitude of the loss data. The smallest claims are less than $1,000 and the largest are over $120M. The numbers of records exposed range from 1 to over 300M.
- There are often dramatic differences between the numbers for SMEs and Large Companies – multiples of 10x, 50x, or more. The biggest Large Company in the dataset (over $30B in annual revenue) is approximately 2.7 million times larger than the smallest organization (less than $15K in annual revenue). The average Large Company in the dataset ($11B in annual revenues) is more than 130 times larger than the average SME ($84M).
- As will be discussed in the report, there is no clear correlation between the size of an entity and the magnitude of a cyber-related loss. Sometimes a smaller organization will experience a very expensive claim (>$100M) and a large organization will have a claim so small (less than $5,000) that it makes one wonder why the claim was filed in the first place. In fact, the most expensive incident during the five-year period occurred at an SME.

With Appreciation

We want to sincerely thank the cyber insurers listed on page 28 for their support of this report and their dedication to industry education. Many of them have contributed to this research every year for 10 years. Without their support this educational report would not be possible.

Suggestions

If you have ideas or requests for next year's study, please let us know. Send us your thoughts at cyberclaims@netdiligence.com.

[1] Given the small number of claims for Large Companies, analysis is not always meaningful and so findings are usually presented for SMEs only.

Key Findings

Company Size

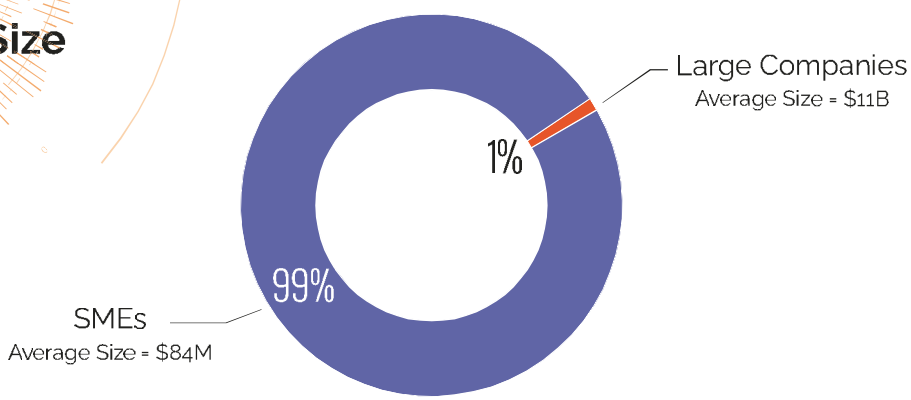

Figure 1

Average Costs for All Claims

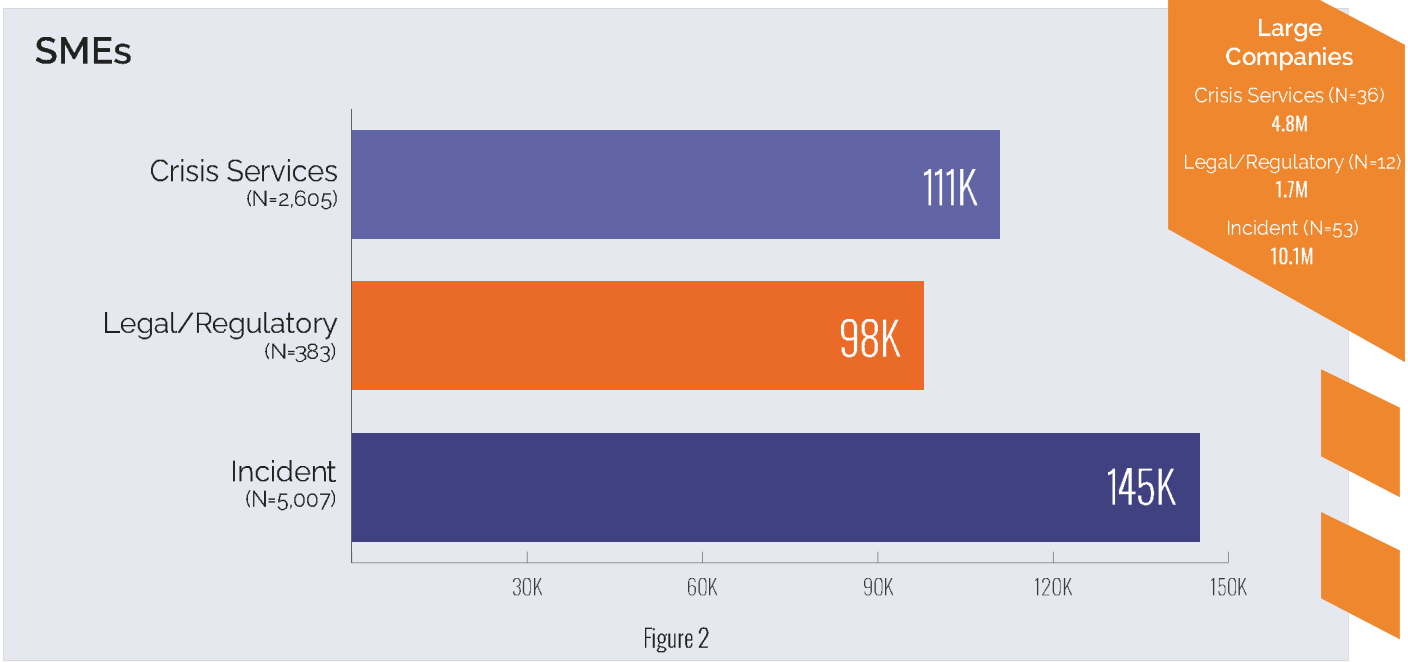

Figure 2

TERMS

Breach Coach®

A qualified data security and privacy attorney who provides legal guidance for cyber incident response.

Incident Cost

Because the proportion of "recordless" events is so large, we replaced the term "breach" with "incident". The term Incident Cost in this report means the aggregate total of all types of costs/expenses associated with the incident.

Crisis Services Costs

Costs associated with responding to the breach event. These costs include, but are not limited to, Breach Coach counsel, forensics, notification, credit/ID monitoring, and public relations.

Legal Costs

Legal and regulatory expenses incurred due to the event. These costs include, but are not limited to, lawsuit defense, lawsuit settlement, regulatory action defense, and regulatory fines.

Self-Insured Retention (SIR)

The dollar amount that the insured organization had to pay before the insurer paid anything on the claim. In this study, the SIR is included in Breach Costs.

Small to Medium Enterprise (SME)

Categorized in this study as organizations with less than $2 billion in annual revenue.

Large Company

Categorized in this study as organizations with $2 billion or more in annual revenue.

All findings are for the five-year period 2016–20120 unless otherwise noted.
NetDiligence and Breach Coach are registered trademarks of Network Standard Corporation, dba NetDiligence.

 Version 1.0

Average Costs for Ransomware

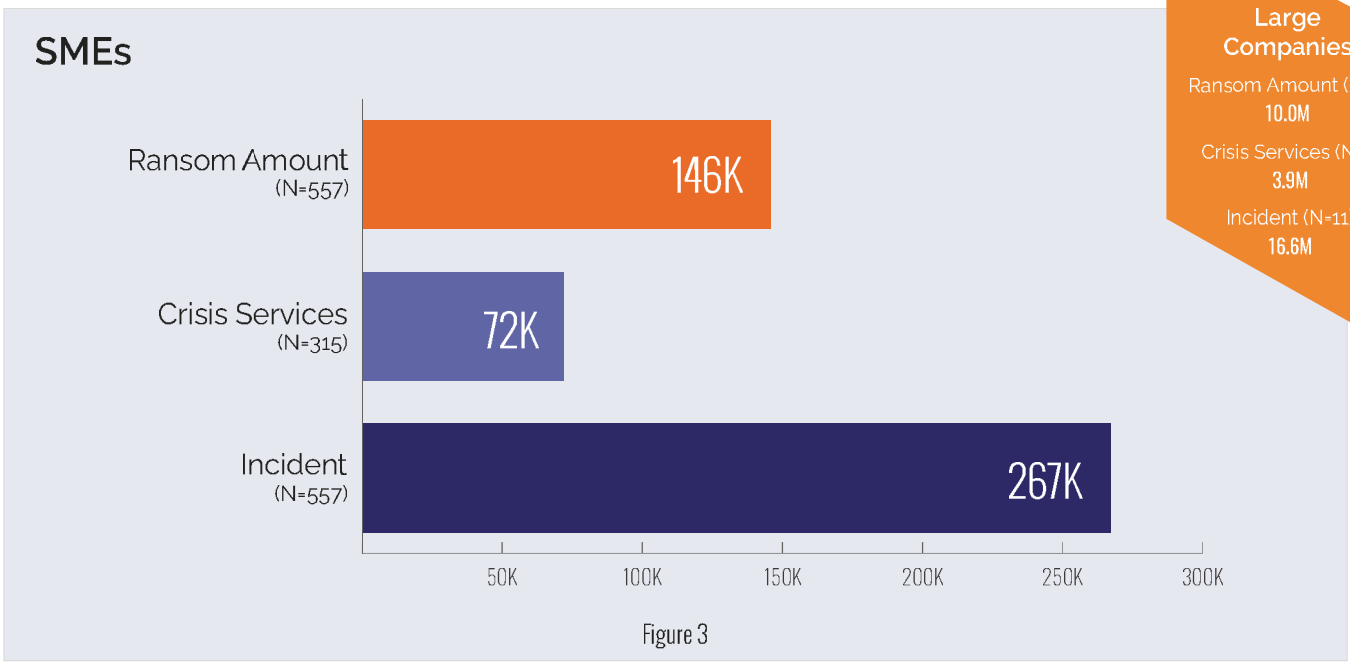

Figure 3

Ransomware is not slowing down or letting up. Readiness is a necessary lifeline to survive in this Cyber-demic environment. Experian® Reserved Response is the only program that offers a proven path forward that delivers live drills, a scalable infrastructure, and a guarantee to mitigate brand damage, customer migration, regulatory scrutiny, and executive termination because of a failed data breach response.

Michael Bruemmer
Experian® Data Breach Resolution

Average Costs for Business Interruption

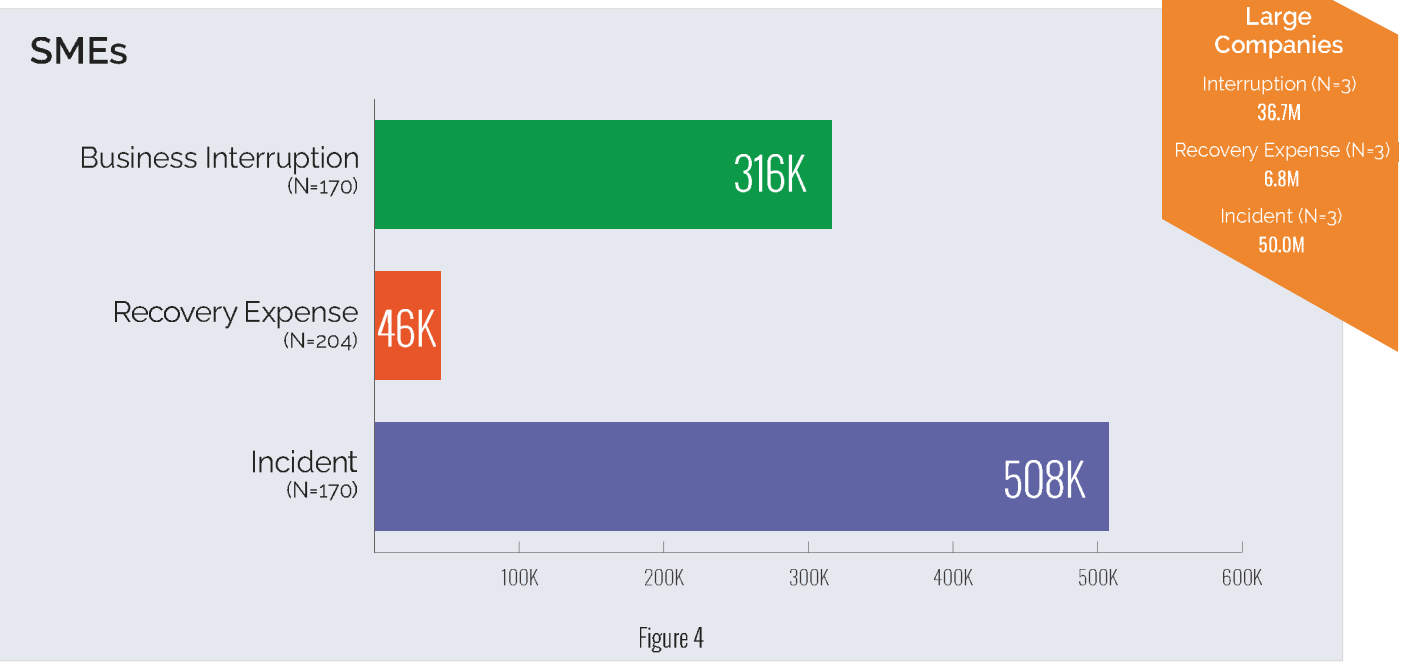

Figure 4

The significant upward trend in BI claims and costs demand risk prevention guidance throughout the policy lifecycle: from initial binding/renewal, through to continuous monitoring during the policy period, and finally with the collection of more robust incident claims data that relates back to frontend risk control guidance.

Erin Kenneally
Guidewire, Director, Cyber Risk Analytics

Business Sector

Top 5 by Number of Claims – SMEs

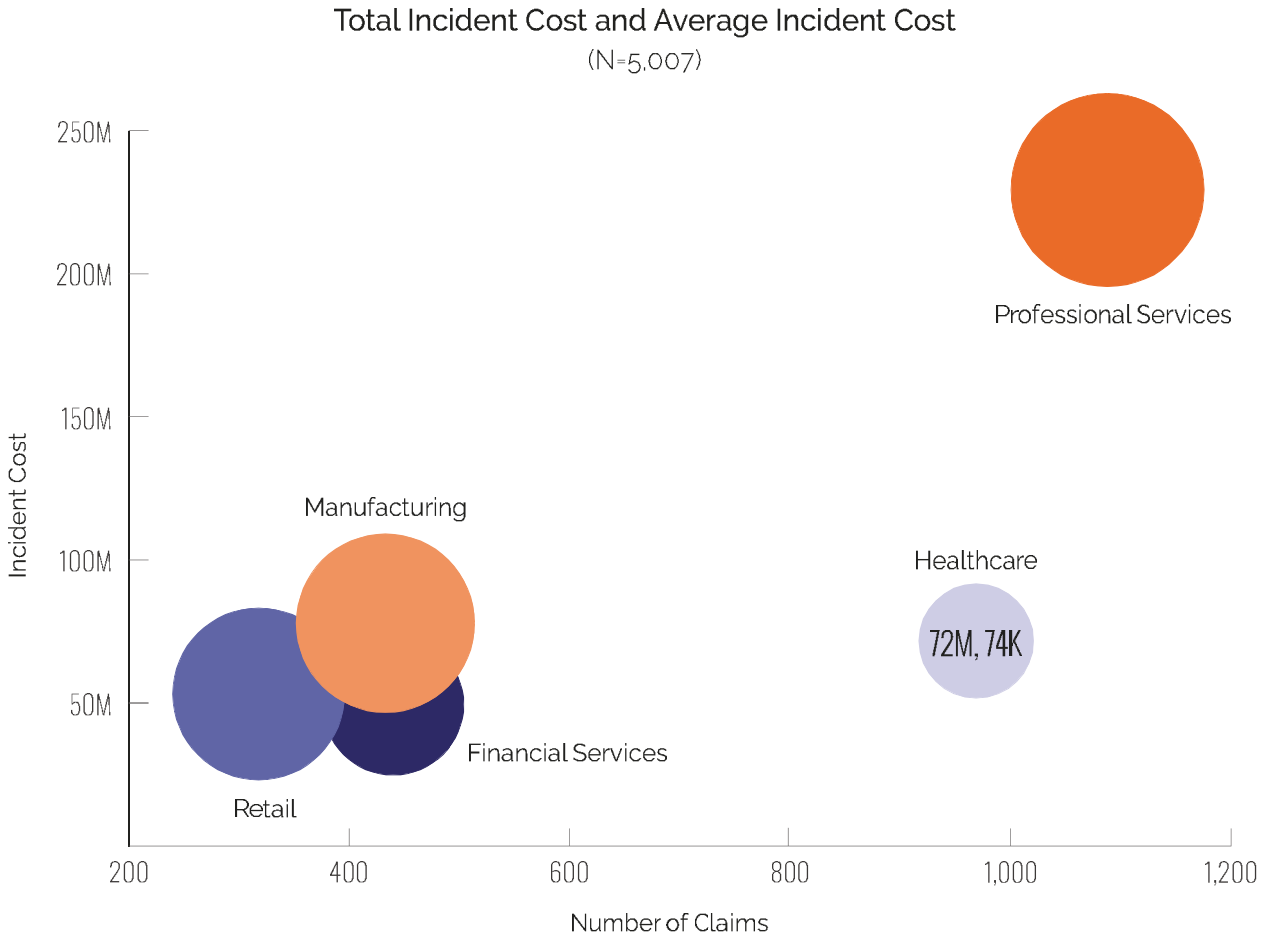

Figure 5

Every enterprise must consider its ability to withstand cyberthreats, comply with an increasingly complicated constellation of state, federal, and international regulations, and prepare to respond to incidents now..

Jennifer Beckage
Founder, Beckage

Cause of Loss

Top 5 by Number of Claims – SMEs

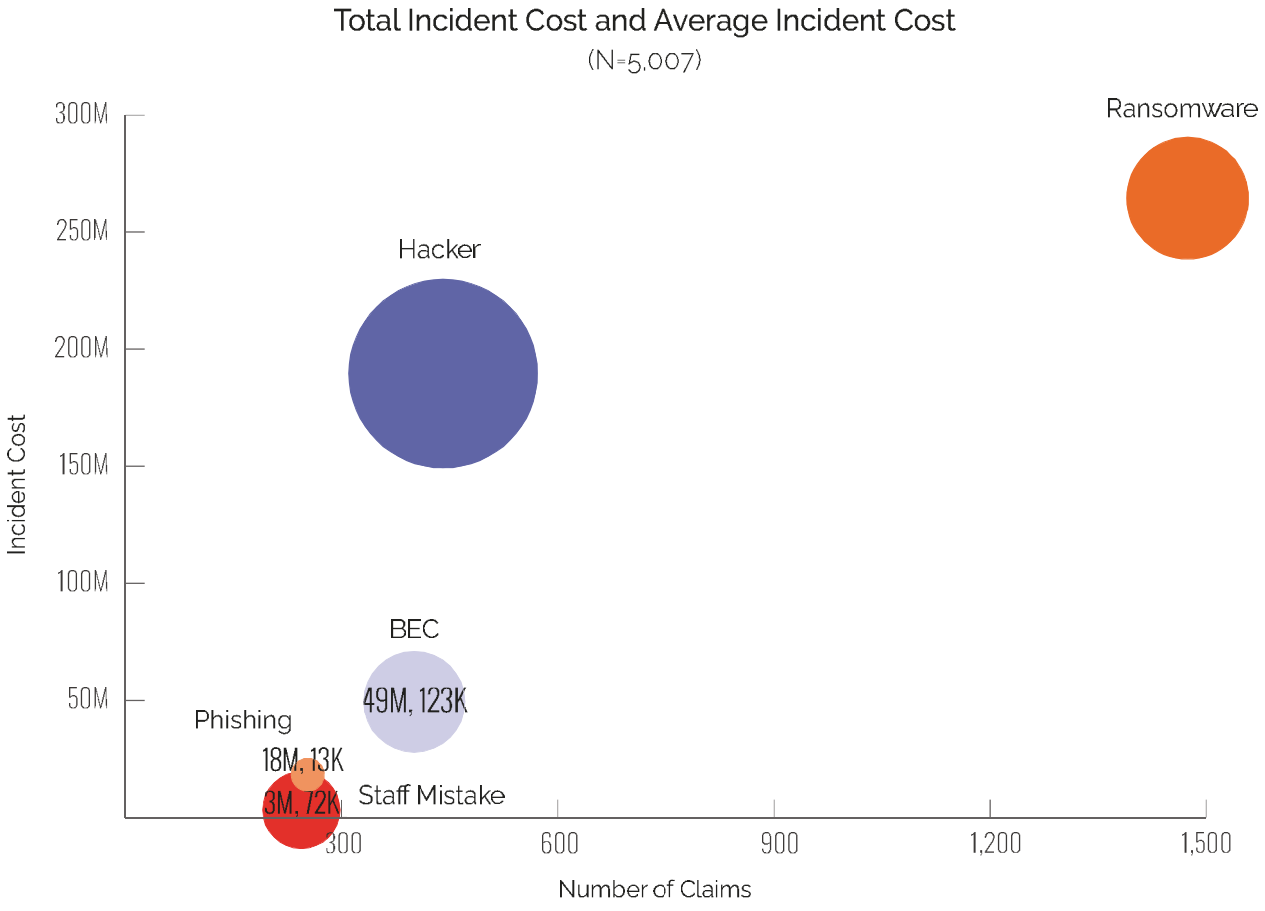

Figure 6

An Overview of the Data

The claims analyzed in this study come from organizations of all sizes, the smallest with less than $15K in annual revenue and the largest with $30B. As indicated earlier, the dataset is overwhelmingly weighted with claims from smaller companies. This can dilute the findings for large companies, while large companies can function as outliers that skew the findings for small organizations.

For that reason, the dataset has been divided into two categories based on the size of the insured entity. Organizations with less than $2B in annual revenue have been defined as Small to Medium Enterprises (SMEs), while those with greater than $2B in annual revenue have been defined as Large Companies.

A large percentage (64%) of study participants provided estimates of the annual revenue of the insured entities. Analysis of this data provides the following company demographics:

- SMEs: annual revenue ranged from less than $15K to $1.9B. The average was $84M.
- Large Companies: annual revenue ranged from $2B to more than $30B. The average was $11B.

These companies represent more than 18 business sectors.

For SMEs, the top five sectors as defined by number of claims were:

- Professional Services
- Healthcare
- Financial Services
- Manufacturing
- Retail

For Large Companies, the top five sectors as defined by number of claims were:

- Healthcare
- Technology
- Financial Services
- Retail
- Education

Additional analysis by Business Sector and Revenue Size appear later in this report.

Claims by Year of Event

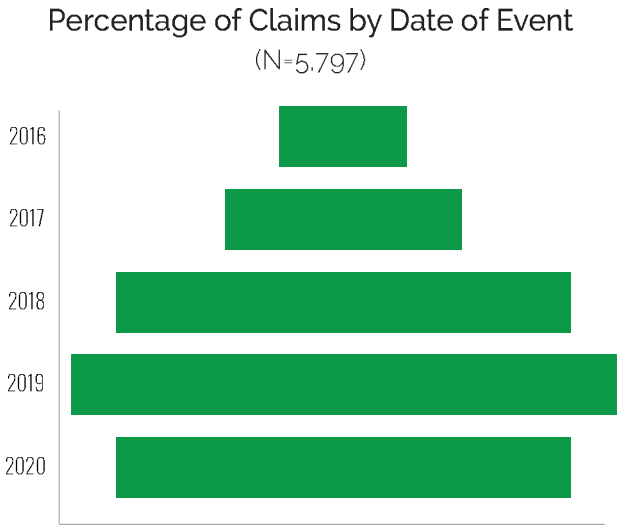

Figure 7

The scope of this study is 5,797 incidents that occurred from 2016-2020. The distribution of claims over this five-year period is depicted in Figure 1. The number of claims collected and analyzed per year has increased from almost 400 in 2016 to over 1,700 in 2019 and 1,400 in 2021.[2]

Crisis Services and Incident Costs

For all organizations, Crisis Services costs ranged from less than $100 to more than $120M. Incident cost, inclusive of Self-Insured Retention (SIR), ranged from less than $1,000[3] to more than $120M. The averages were influenced by some very expensive claims. At SMEs, there were six claims in 2017 with total incident cost of more than $5M, one of which exceeded $100M. At Large Companies, there were ten claims ranging from $15M to $100M.

At SMEs, Crisis Services costs in 2020 averaged $113K (ranging from less than $100–$2.1M). Total incident cost averaged $286K ($1K–$7.6M). For the five-year period, Crisis Services costs averaged $111K (ranging from less than $100–$120M). The average incident cost during this time frame was $165K (ranging from less than $1,000–$120M).

[2] New claims are collected for incidents that occurred during the previous three calendar years. For the 2021 study, these were incidents in 2018, 2019, and 2020.
[3] A few claims for less than $1K were excluded from the analysis.

For all organizations, Crisis Services costs ranged from less than $100 to more than $120M.

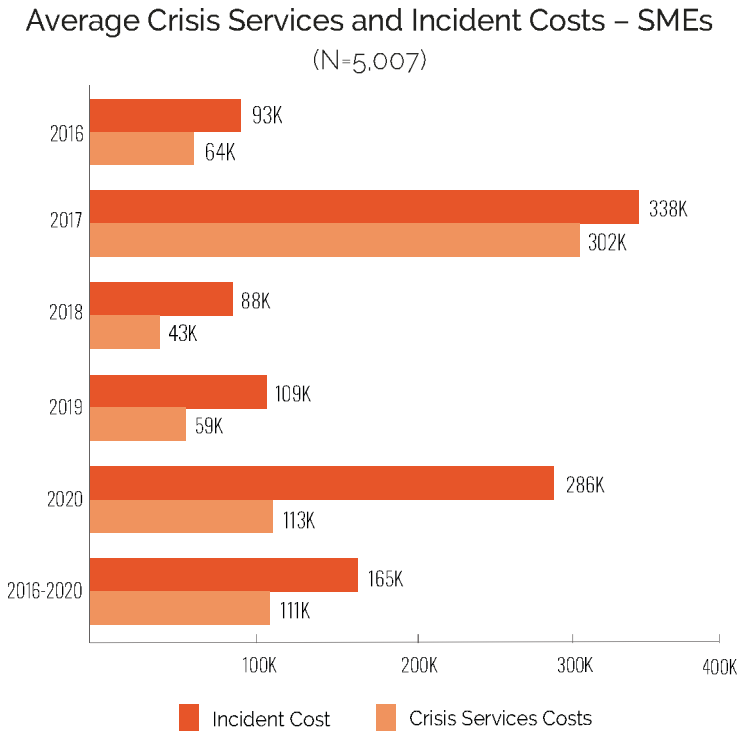

Figure 8

For Large Companies in 2020, Crisis Services costs averaged $2.3M (ranging from less than $5K–$7.3M). The average incident cost in 2020 was $10.4M ($55K– $55M). Over five years, the average was $7.6M (ranging from less than $5K–$100M).

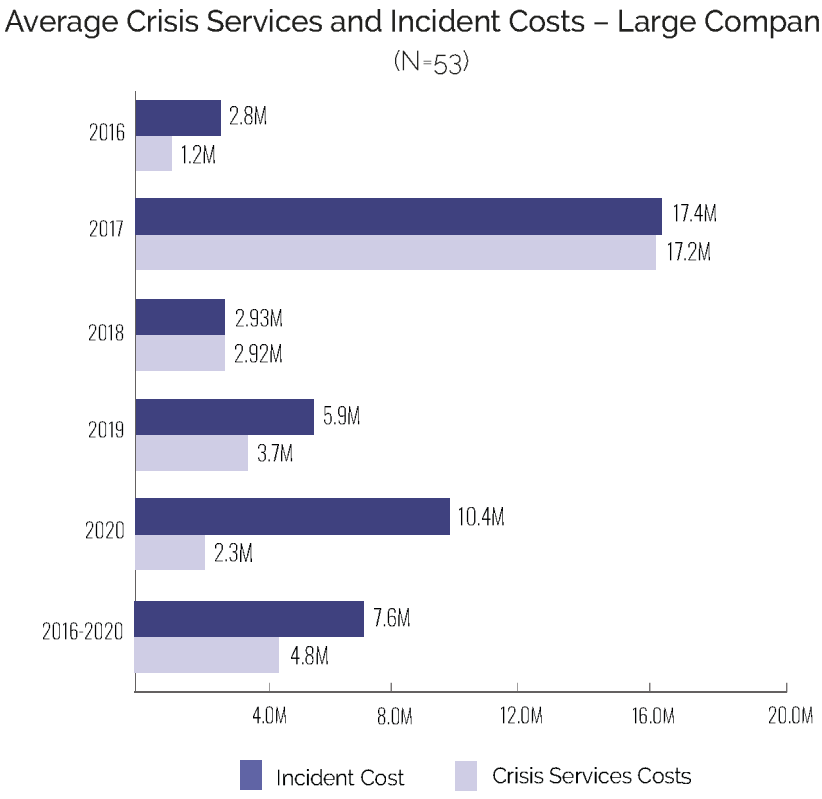

Figure 9

The following two graphs depict Crisis Services costs as a percentage of total incident cost. These percentages are quite variable, going from 39% to 89% for SMEs and from 22% to 100% for Large Companies. The extent to which Crisis Services costs are a significant component of total incident cost is entirely dependent upon the nature of the incident. Many ransomware and banking fraud incidents do not utilize Crisis Services, whereas complex hack and malware/virus incidents often incur significant Crisis Services costs.

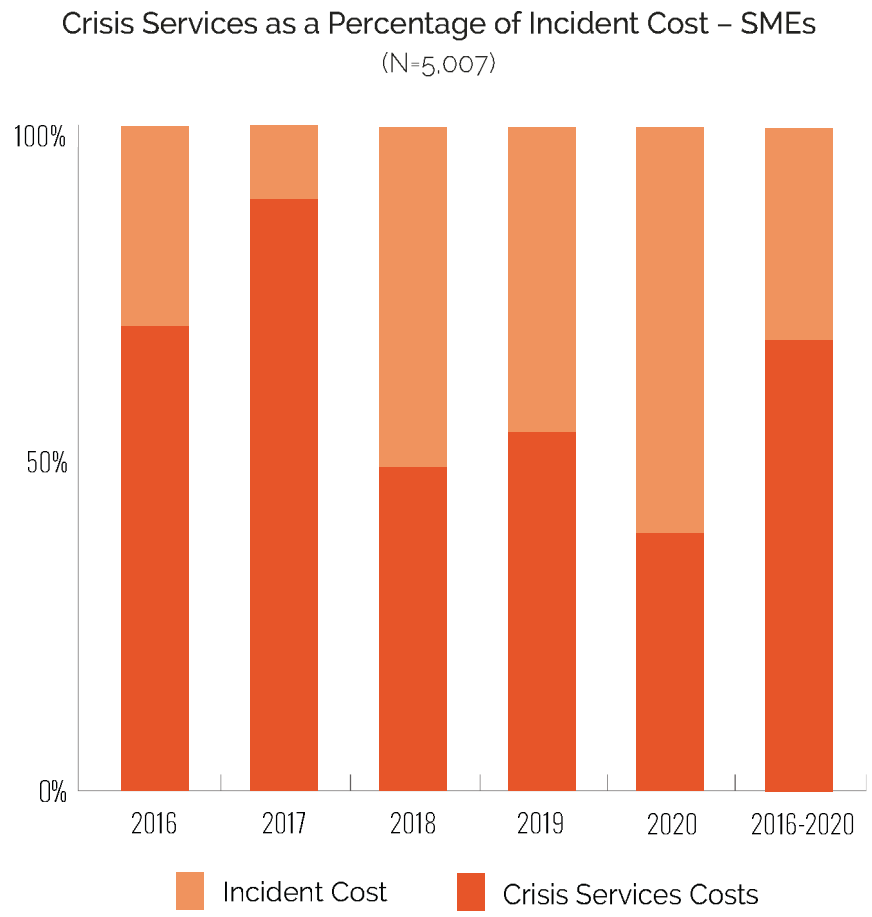

Figure 10

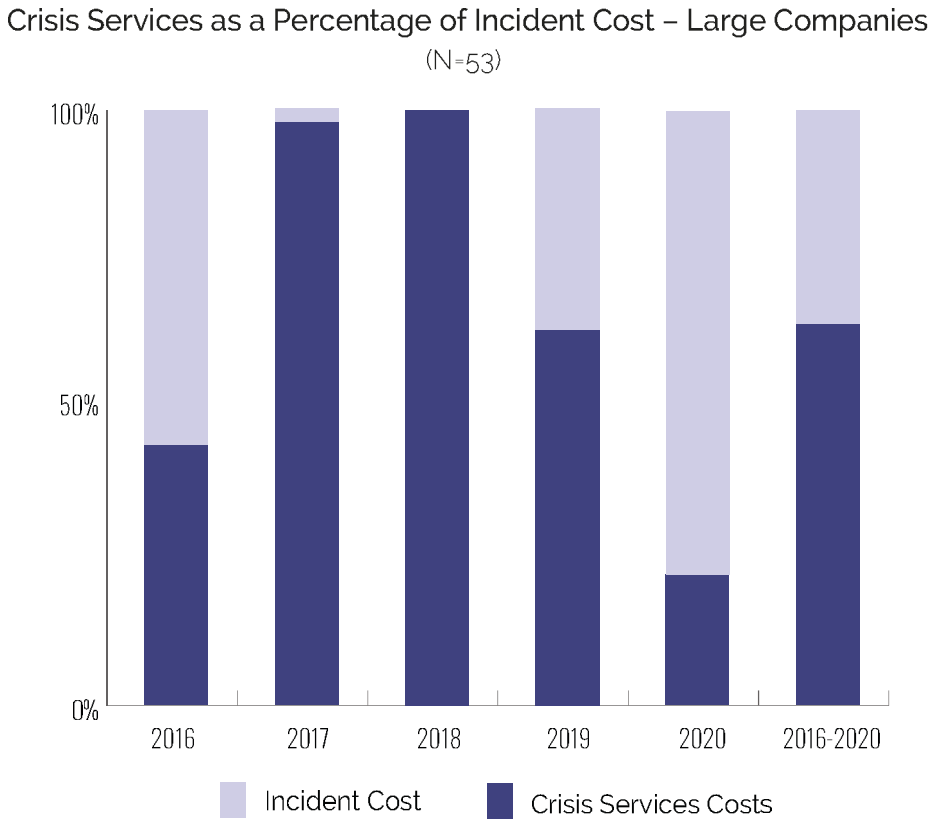

Figure 11

Distribution of Crisis Services Costs

The following graphs depict the year-by-year average individual Crisis Services costs for SMEs, as well as the year-by-year and five-year percentage distribution of individual Crisis Services costs[4] for both SMEs and Large Companies. Incidents that expose records usually have significant costs in all categories. Ransomware and wire transfer fraud events often have no forensics, monitoring, or notification costs.

Figure 6 displays the average cost of each individual crisis service. Forensic services and Other crisis services have the highest average in each of the five years.

At SMEs, the percentage of forensics and legal guidance costs is fairly uniform, ranging from 47%–53% for forensics and 17%–27% for legal guidance. Monitoring costs are negligible and notification costs range from 1%–11%.

At Large Companies, the distribution of Crisis Services costs can be quite variable and heavily dependent upon not only the type of incident but also one or two mega-events.

[4] Forensics costs typically include the cost of incident response services. However, when the victim organization engages an incident response company to negotiate and pay a ransom, forensics costs will sometimes include the cost of the ransom. Other crisis services costs typically include public relations costs. However, some insurers put ransom amounts and even data recovery in this category.

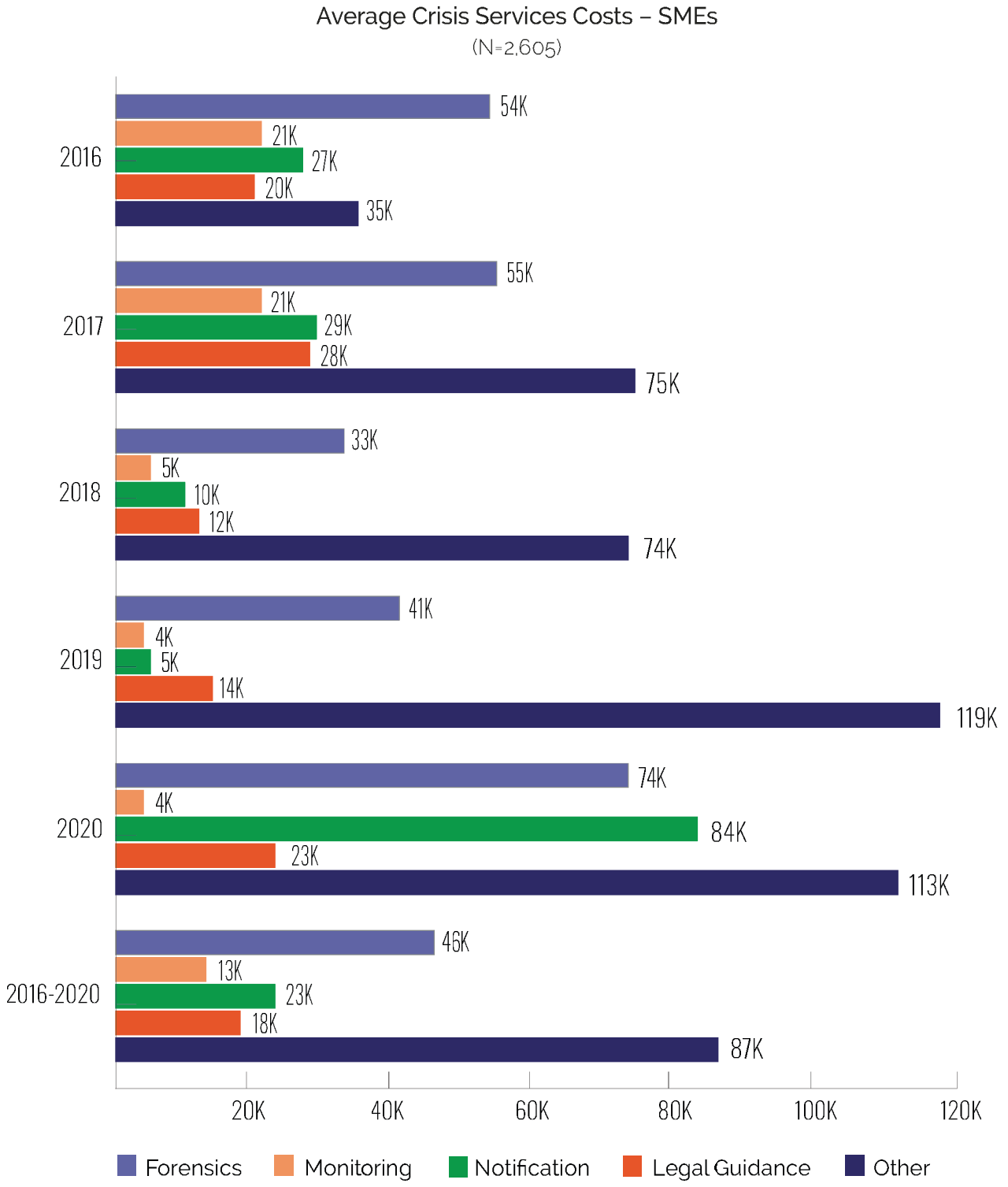

Figure 12

[4] Forensics costs typically include the cost of incident response services. However, when the victim organization engages an incident response company to negotiate and pay a ransom, forensics costs will sometimes include the cost of the ransom. Other crisis services costs typically include public relations costs. However, some insurers put ransom amounts and even data recovery in this category.

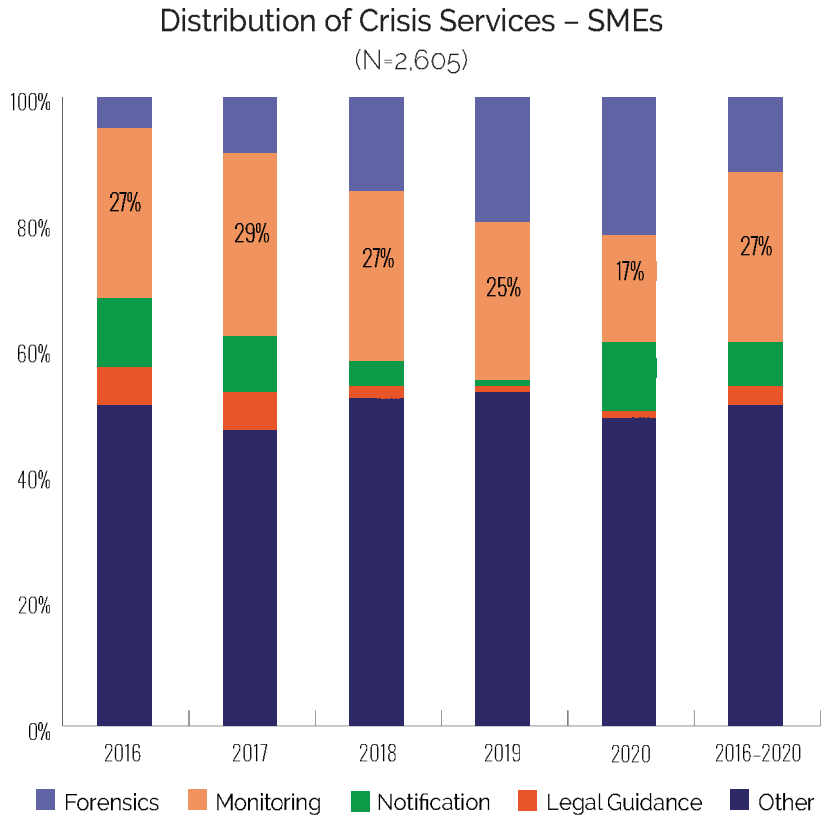

Figure 13

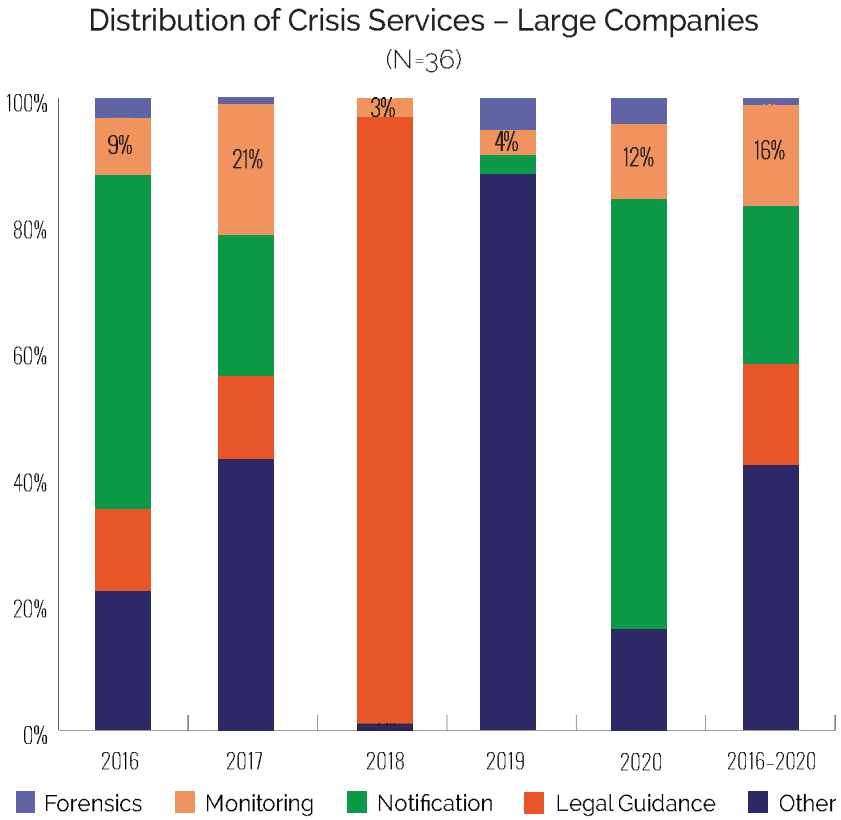

Figure 14

Business Interruption and Recovery Expense

SMEs

Of the 5,716 claims at SMEs, 170 included costs for business interruption (BI) and 204 included costs for recovery expense. Only 49 claims incurred both BI and recovery expense.

Overall, BI costs in 2020 averaged $446K ($3,500-$3M). The total incident cost for these claims averaged $898K ($25K-$3.1M). For the five-year period, the average BI costs were $316K (<$150 to $10M). Total incident cost averaged $508K ($4K to $17.5M). In 2020 and over five years, the average incident cost with BI is significantly higher than the overall average incident cost for the same periods.

Ransomware incidents accounted for 79% of the claims with a business interruption loss, followed by malware/virus (9%) and hacking (5%) incidents. The remaining claims (7%) were due to rogue employees, system glitches, and other/unknown causes of loss.

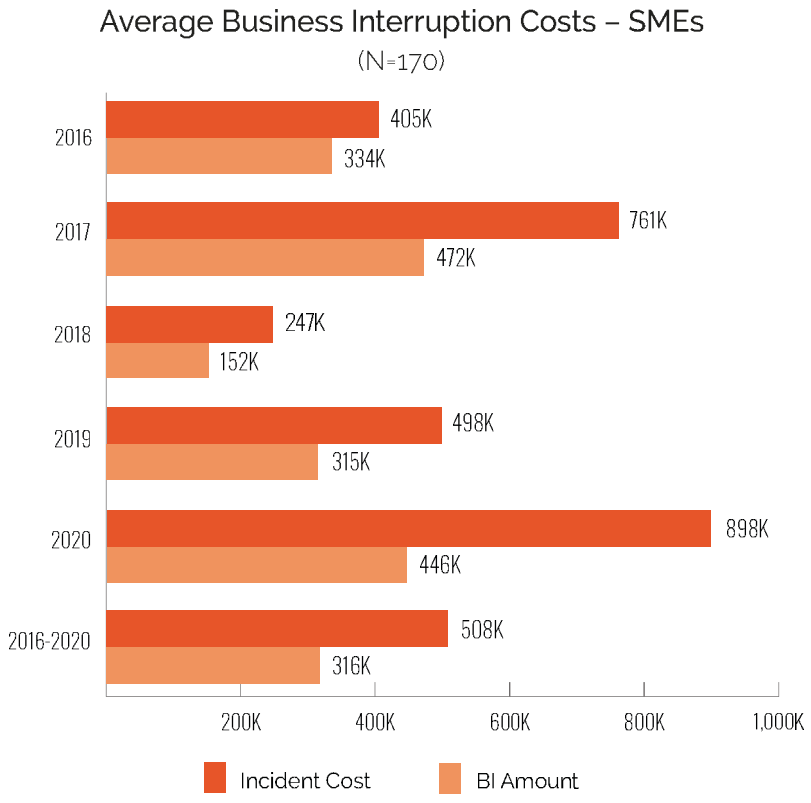

Figure 15

Recovery expense in 2020 averaged $103K (less than $1,700–$1.6M). The total incident cost for these claims averaged $412K ($8K–$1.7M). For the five-year period, these costs averaged $46K (less than $200– $1.6M). The five-year average incident cost for a claim with recovery expense was $181K ($1,500–$3.9M).

Ransomware incidents accounted for 81% of the claims with a recovery expense loss, followed by hacking (7%) and malware/virus (5%) incidents. The remaining claims (7%) were due to rogue employees, staff mistakes, system glitches, and other/unknown causes of loss.

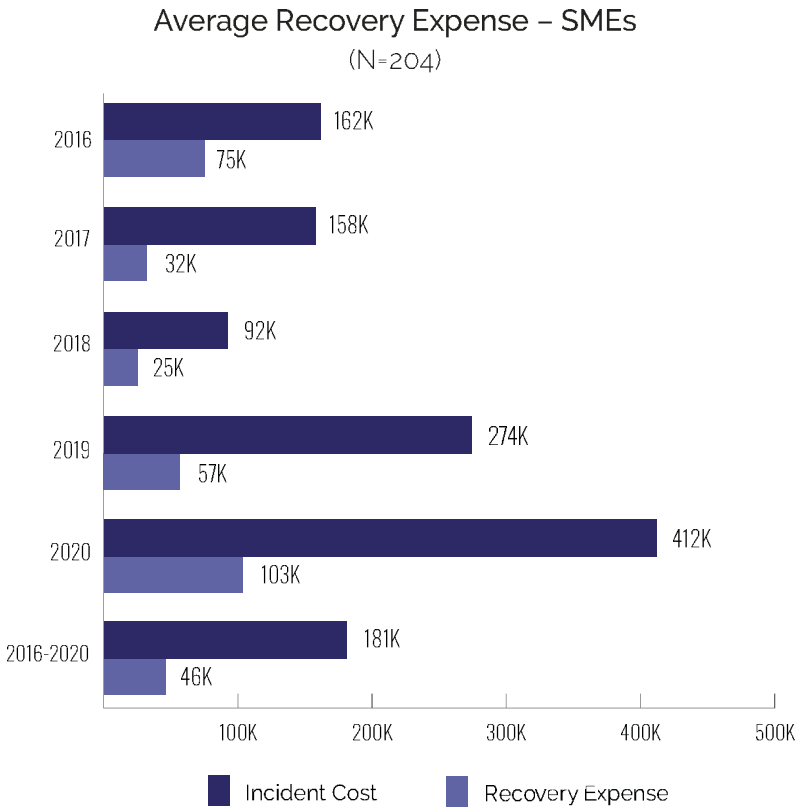

Figure 16

Large Companies

There were only five Large Company claims that included BI and/or recovery expense. Three of these involved ransomware, one involved malware, and one very large claim was caused by a system glitch/network outage. In 2020, these claims averaged a BI loss of $25M. The total incident cost averaged $35M. Over five years, the BI loss averaged $37.7M and the total incident cost averaged $50M. In 2020, the average recovery expense was $133K and the average total incident cost was $4M. The five-year incident amounts were $6.8M and $29.3M, respectively.

Legal Costs

In this year's report, we have combined the four categories of litigation cost—Legal Damages Defense, Settlement, Regulatory Defense, and Regulatory Fines—into a single category of Legal Costs.

There were 385 claims for legal costs from SMEs. In 2020, these costs ranged from less than $500 to $5.2M (average=$411K). Over five years, these costs ranged from less than $100 to $6.8M (average=$98K). At Large Companies, there were 13 claims for legal costs. In 2020, the total costs ranged from $500K to $8M (average=$4.2M) and the five-year costs ranged from less than $2K to $8M (average=$1.6M).

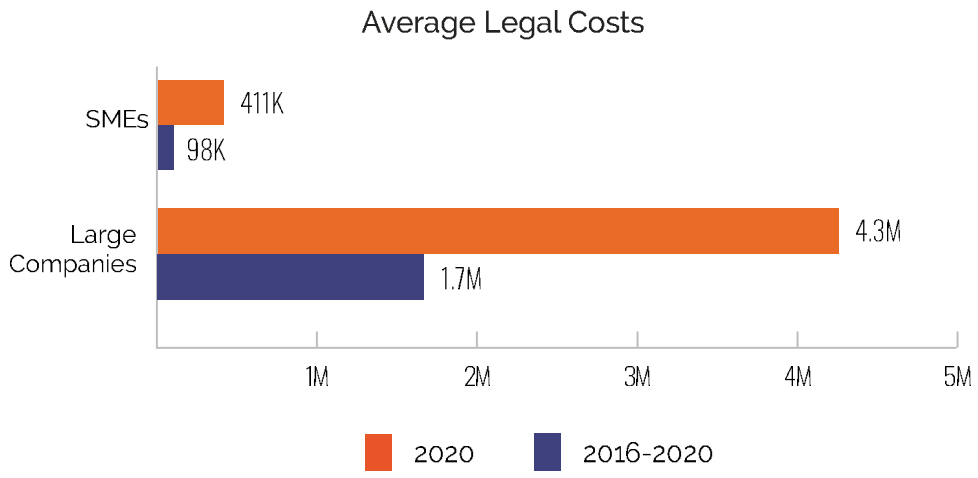

Figure 17

Exposed Records

Of the 5,797 claims in the dataset, 895 were for incidents that constituted some form of a data privacy incident, and thus exposed records. The total number of records exposed in these incidents was greater than 1.1 billion. The numbers of records exposed per claim ranged from a single record to over 300 million records. Incidents at SMEs accounted for 872 of these claims and 355 million records. Incidents at Large Companies accounted for 23 claims and 724 million records.

Incidents at Large Companies exposed, on average, 85 times more records than incidents at SMEs.

The average number of records exposed varies substantially from year to year for both SMEs and Large Companies. This is primarily because mega-incidents drive up the averages. In 2017 and 2020, incidents at SMEs exposed far greater numbers of records than in each of the other years. In 2018 and 2019, incidents at Large Companies exposed far greater numbers of records than in other years.

Figure 12 shows the average number of records exposed. These averages are dramatically different for SMEs and Large Companies. For the five-year period, incidents at Large Companies exposed, on average, 85 times more records than incidents at SMEs.

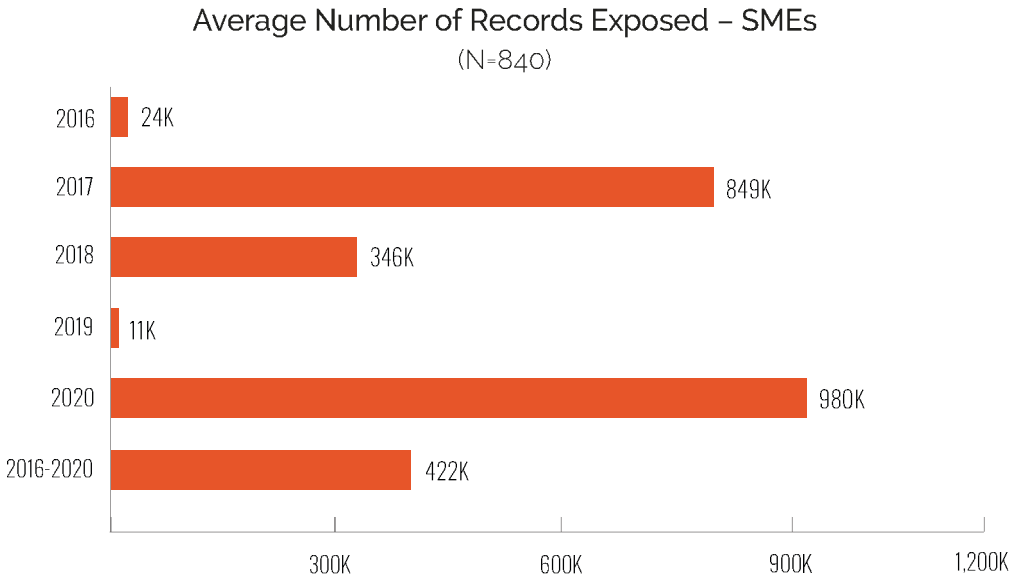

Figure 18

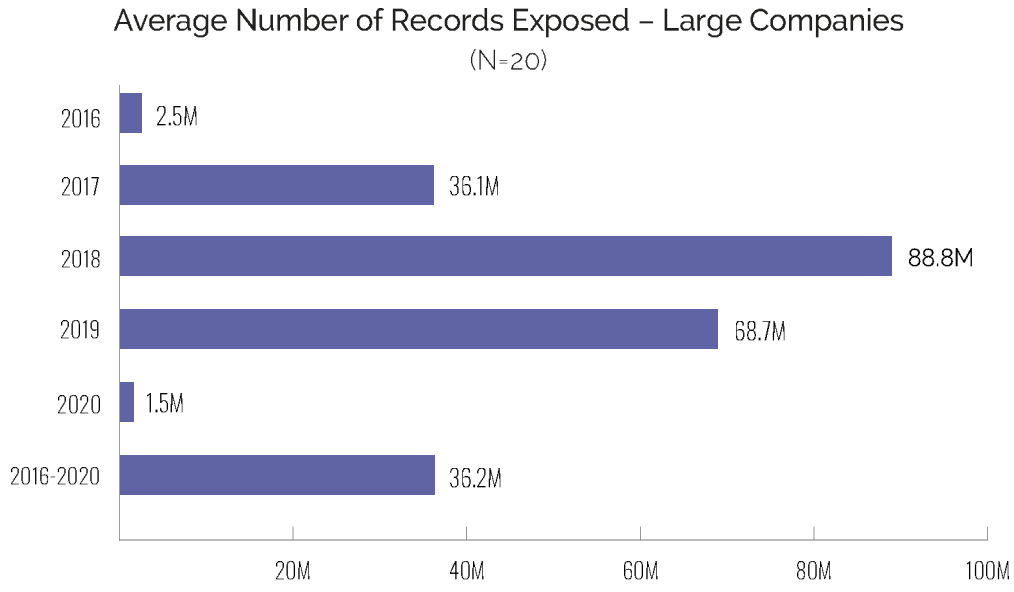

Figure 19

Recordless Claims versus Claims with Exposed Records

"Recordless" claims are incidents that do not expose records. Ransomware, wire transfer fraud, business email compromise (BEC), and distributed denial of service (DDoS) account for most of these incidents. In last year's report, recordless incidents accounted for 55% of claims in 2019 and 39% of claims over five years. In this year's report, these incidents account 70% in 2020 and 37% of claims over five years. This large increase in the proportion of recordless incidents is primarily due to the increased number of ransomware claims in 2020.

Figure 20

Criminal vs Non-Criminal Activities

Criminal incidents include:

- Hacking
- Ransomware
- Malware/virus
- Social engineering
- Business email compromise (BEC)
- Phishing
- Distributed denial of service (DDoS) attacks
- Stolen devices
- Theft of money by wire transfer
- Banking/ACH fraud

Non-criminal events include:

- Staff mistakes
- Mishandling of paper records
- Improper disclosure
- Lost laptops
- Programming errors
- System glitches
- Legal actions

Since 2016, the proportion of claims caused by criminal activities has ranged from a high of 83% to a low of 69%. The proportion of claims caused by non-criminal activities decreased from 28% in 2019 to 17% in 2020.

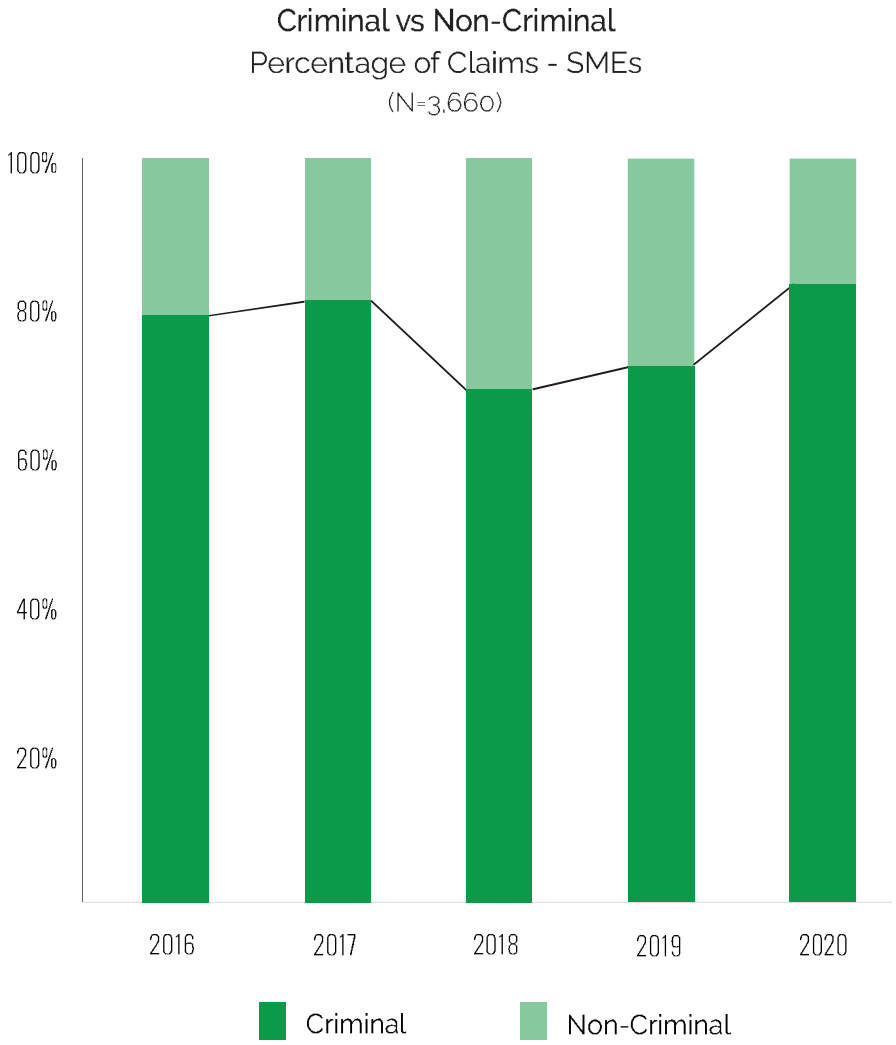

Figure 21

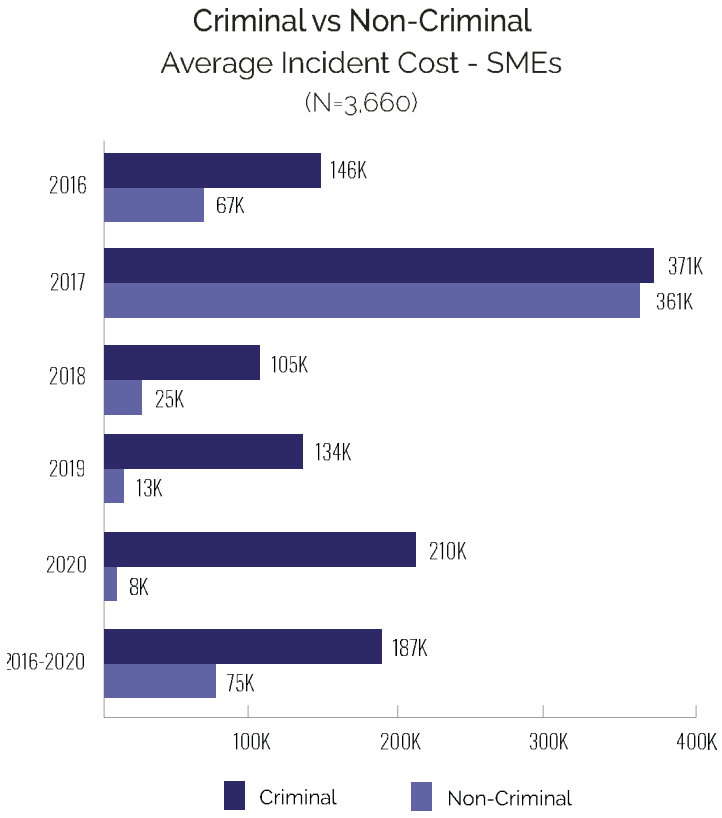

Figure 22

Average Incident and Crisis Services costs, as well as the average number of records exposed, were all dramatically higher for criminal events.

Criminal vs Non-Criminal – SMEs

Time Period	Impact	Type of Activity	Minimum	Average	Maximum	Total
2020 Criminal (N=611) Non-Criminal ((N=25)	Records Exposed	Criminal	3	1M	30M	33.3M
		Non-Criminal	0.4K	4K	8.5K	8.9K
	Crisis Services	Criminal	0.1K	116K	2.1M	23M
		Non-Criminal	0.1K	8K	26K	41K
	Incident Cost	Criminal	1K	210K	7.5M	128.4M
		Non-Criminal	1K	9K	64K	233K
2016-2020 Criminal (N=3,241) Non-Criminal ((N=419)	Records Exposed	Criminal	2	519K	143M	347.7M
		Non-Criminal	2	40K	1.8M	6.8M
	Crisis Services	Criminal	0.1K	97K	120.2M	41.1M
		Non-Criminal	0.1K	19K	540K	5.6M
	Incident Cost	Criminal	1K	187K	120.2M	606.3M
		Non-Criminal	1K	75K	17.5M	31.6M

Table 1

Self-Insured Retentions (SIRs)

The dataset contains 3,520 claims from SMEs that reported a value for SIR. Over five years, the size of SIR ranged from $0 to $10M. In 2020, SIR at SMEs ranged from $1K to $250K. The maximum SIR in 2020 dropped to $250K, from $350K in 2019 and $500K in 2018.

Self-Insured Retentions (SIRs) – SMEs

	Claims	Minimum	Average	Maximum
2020	908	1K	14K	250K
2016–2020	3,520	0	28K	10M

Table 2

The following chart displays the average SIR for each of the previous five years as well as the five-year average. Since 2017, there has been a dramatic decrease in the average SIR.

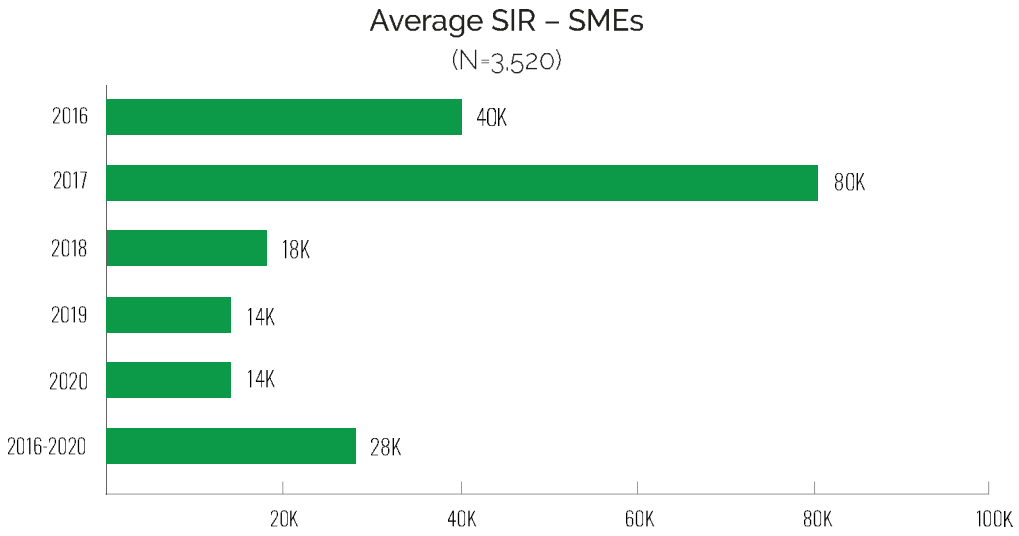

Figure 23

Topics of Special Interest

Company Size and Loss Magnitude: Does Size Really Matter?

Four years ago, we began asking study participants to provide an estimate of the annual revenue of each claimant. At present, we have this data for about 65% of claims.

One of the questions we have tried to answer is whether there is a clear correlation between the size of the claimant organization and the magnitude of the cyber-related loss.

As the graphs below show, the short answer is no. For SMEs, there is really no correlation at all (R2<0.0992). For large companies, there is some, but not much, correlation (R2<0.3364). One of the largest incidents in the dataset occurred at a small enterprise and one of the smallest at a very large one.

There are probably many reasons for this, most importantly the equalizing effect of cheaper and more powerful hardware. Other factors include the omnipresence of the internet, the availability of fast, inexpensive connectivity, and massive amounts of cheap storage in the cloud and on premises. Instead of a relatively small number of targets to exploit, in 2021 almost everyone on the planet has become a potential target to exploit.

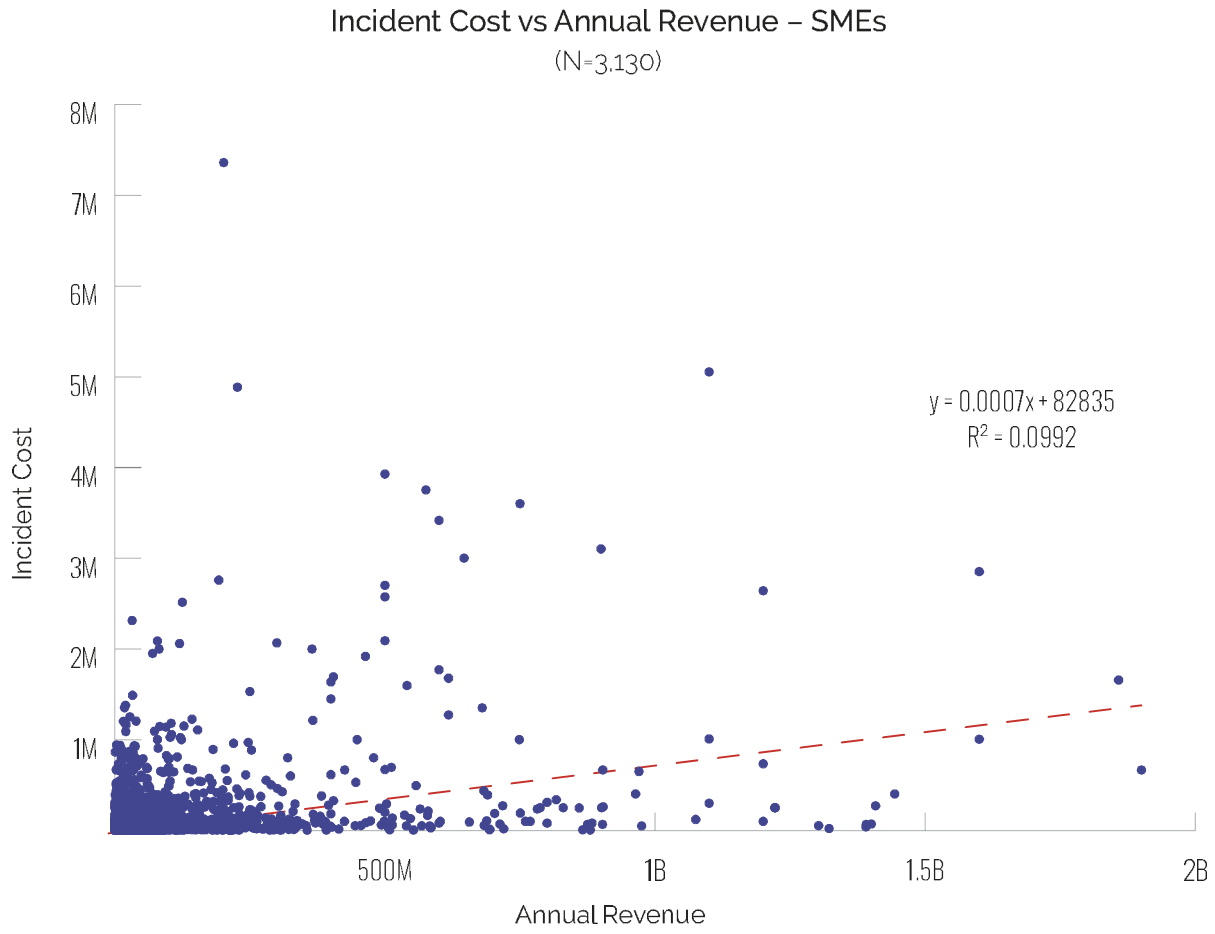

Figure 24

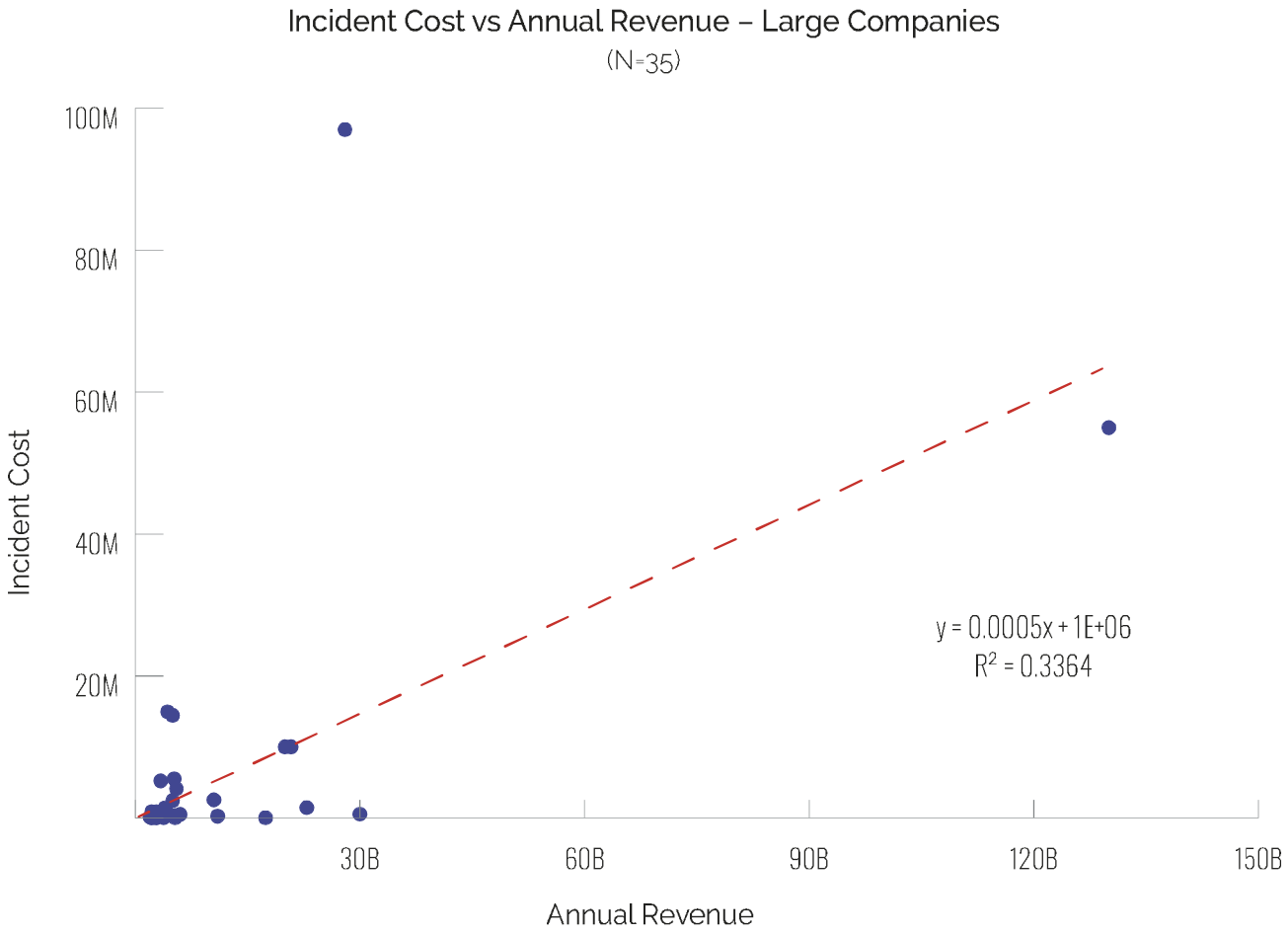

Figure 25

Top Causes of Loss at SMEs

As measured by the number of claims over five years, the top five causes of loss at SMEs were:

- Ransomware
- Hackers
- Business email compromise
- Staff mistakes
- Phishing

Losses in these five categories accounted for 70% of claims and 80% of total incident cost ($525M). For metrics on all sectors, please see the graphs and tables in the appendices.

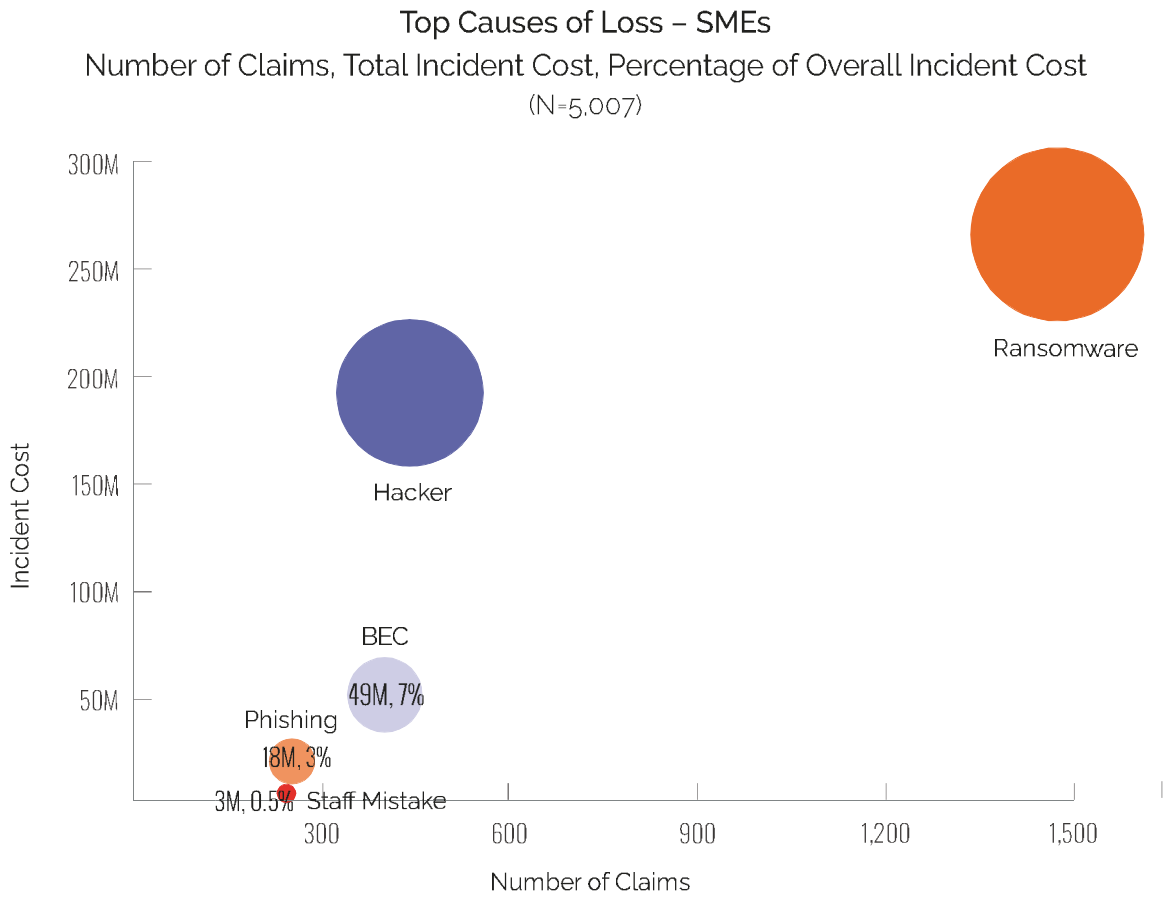

Figure 26

Ransomware

As we all know, ransomware claims have snowballed since 2018–2019. From year to year, the NetDiligence data shows a significant increase in the number of ransomware claims and in the costs of ransomware incidents. From reading the news about events at Colonial Pipeline, Kaseya, the NBA, and many other entities, we know that things have become even worse in 2021[5].

Ransomware accounts for the largest number of claims in the five-year data (N=1,474). Ransom demands and total incident cost average $146K (less than $200–$3.7M) and $179K ($1K–$20M), respectively.

Ransom amounts and incident cost were provided for only a subset[6] of claims (N=557). We have focused on these claims because we believe that they provide a better understanding of the claims experience. When viewed in this way, the average ransom amount and range of incident cost do not change, but the average incident cost is substantially higher.

This year's report further confirms the growing impact of ransomware attacks on both small to medium businesses and large organizations. Based on what we're seeing in the marketplace, ransomware threats are only becoming more frequent, and threat actors are becoming more sophisticated by leveraging criminal business models like Ransomware-as-a-Service (RaaS). We expect these numbers to continue to trend in an upward direction unless organizations focus on putting appropriate defensive controls and processes in place.

Tauseef Ghazi
National Leader, Security and Privacy Risk Consulting, RSM

[5] NetDiligence has not yet collected data for incidents in 2021.
[6] See the methodology section for a discussion of missing and mismatched data.

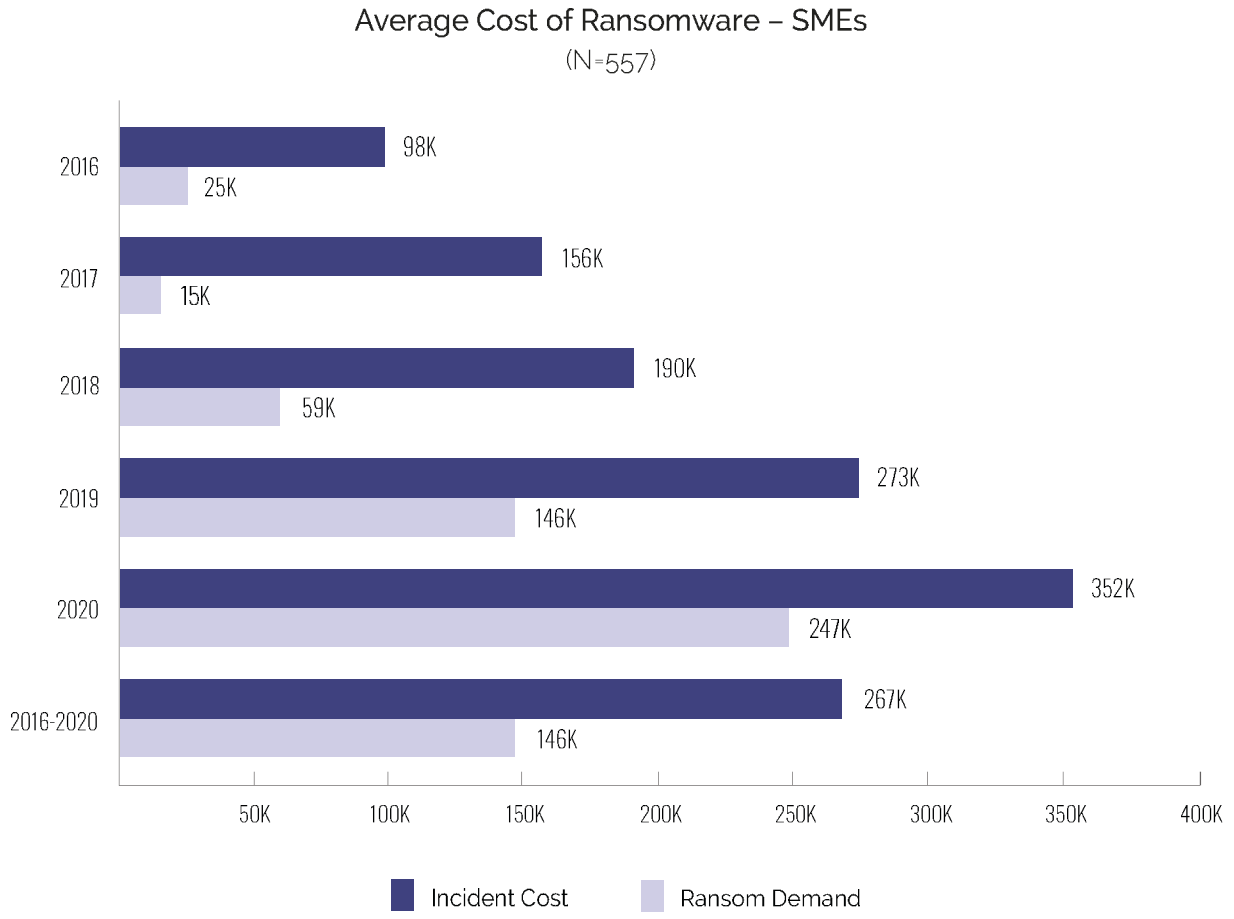

Figure 27

Some victim organizations choose not to pay a ransom. What happens then? Sometimes, but not very often, backups have not been infected and sufficient recovery is possible. Some organizations just bite the bullet and perform a data recovery process. Increasingly, victims elect not to pay ransoms because there is a good chance that the decryption keys will not work.

There is a small subset of claims which noted that the victim chose not to pay a ransom demand. For most of these, we do not know what the ransom demand was because it was not paid and therefore was not provided. The total incident cost for these events averaged $308K ($15K–$2.1M) in 2020 and $247K ($2.5K–$6.6M) over five years (not much less than the averages in Figure 21).

As noted above, ransomware incidents accounted for 79% of the claims with a business interruption loss. BI costs in ransomware incidents in 2020 ranged from $3,500–$3M and averaged $489K. The total incident cost of these incidents ranged from less than $25K–$3.1M and averaged $975K. BI costs over five years ranged from less than $200–$5.1M and averaged $275K. Total incident cost ranged from $4.6K–$6.6M with an average of $433K.

Ransomware incidents accounted for 81% of the claims with a recovery expense loss. Recovery expense in ransomware incidents in 2020 ranged from $1,700–$613K and averaged $107K. The total costs of these incidents ranged from less than$8K–$1.7M and averaged $427K. Recovery expense over five years ranged from less than $200–$613K and averaged $49K. Total incident cost ranged from less than $1,500–$3.9M with an average of $181K.

The increasing frequency and loss magnitude caused by ransomware incidents is a huge concern for insurers and organizations. NetDiligence has published two Spotlight reports on ransomware (2020 and 2021), and will very likely publish another one in the near future.

Top Affected Sectors

As measured by the number of claims over five years, the following sectors accounted for 70% of claims and 74% of total incident cost ($535M):

- Professional Services
- Manufacturing
- Healthcare
- Technology
- Retail
- Financial Services

These sectors have been at the top of the list for many years now because they represent valuable and easy targets for criminals. The graph below provides a look at the frequency and magnitude of claims as well as the percentage of the aggregate SME incident cost. For metrics on all sectors, please see the appendices.

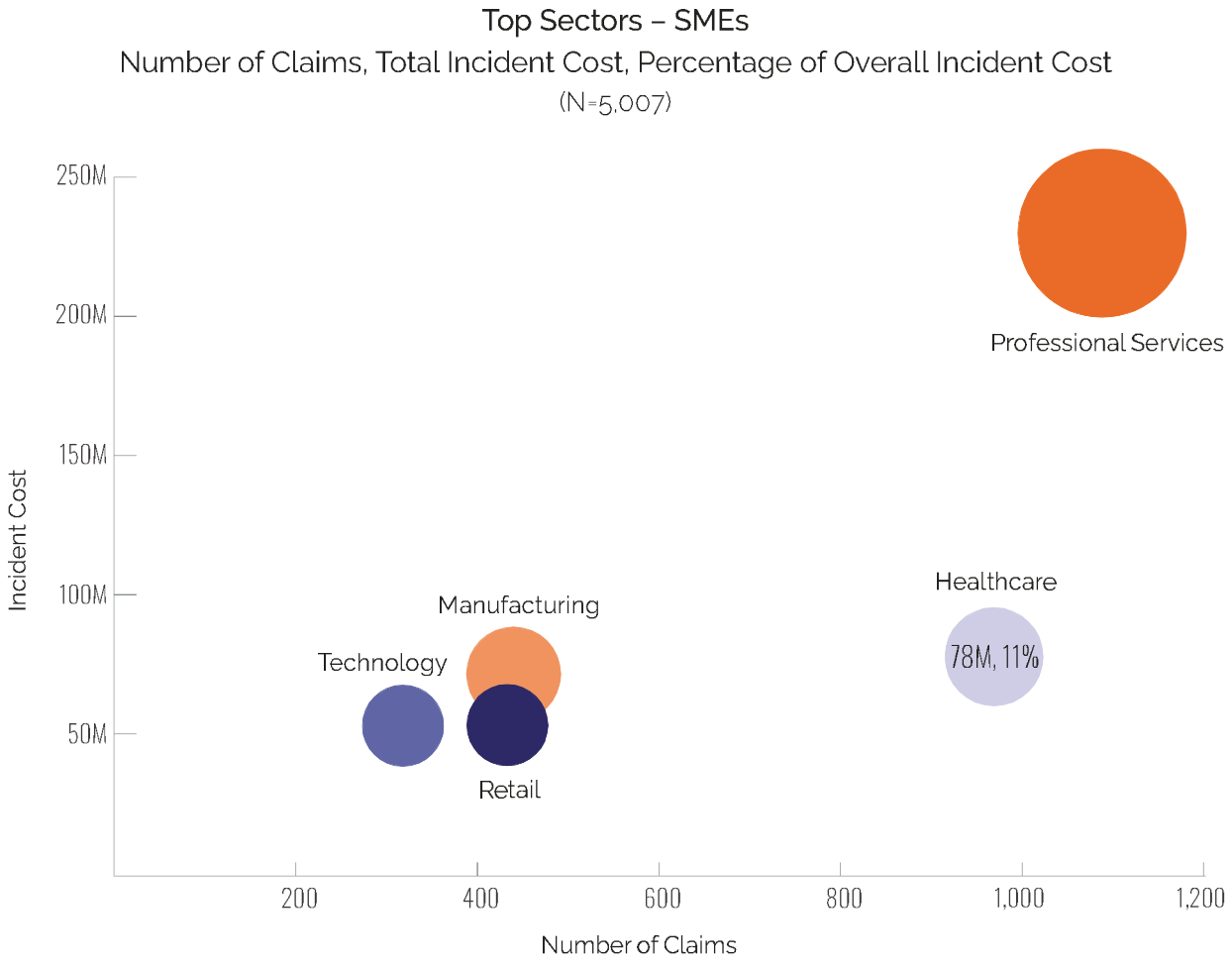

Figure 28

Claims from Public Entities

The average Public Entity claim for Crisis Services costs in 2020 was $76K ($7K–$236K). The average incident cost was $239K. The corresponding five-year averages were $95K (less than $200–$790K) and $156K ($1.8K–$1.4M), respectively.

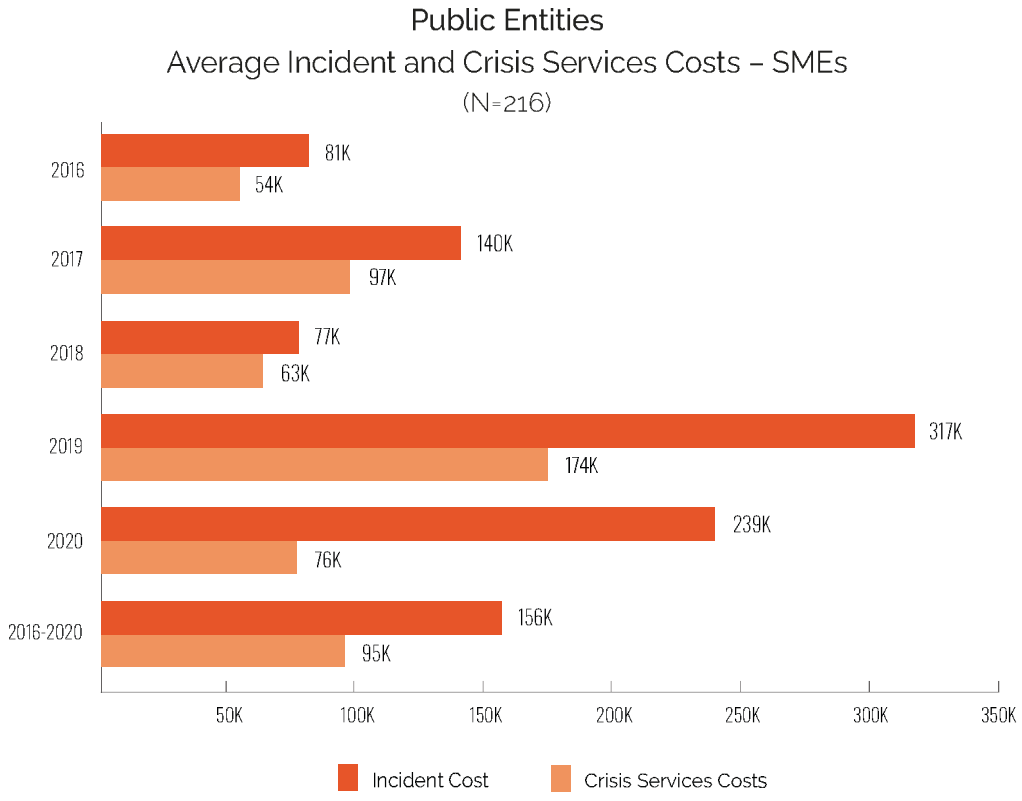

Figure 29

Public Entities
Top Causes of Loss 2016-2020 – SMEs

Cause of Loss	Claims	Average Incident Cost
Ransomware	72	157K
Hacker	23	83K
Staff Mistakes	16	17K
Business Email Compromise	14	200K

Table 3

Claims from Canada

The average Canadian claim for Crisis Services in 2020 was $144K (from less than $100–$1.1M). The average incident cost was $310K ($1.1K–$2.1M). The corresponding five-year averages were $163K (less than $100–$3.8M) and $237K ($1.1K–$3.8M), respectively.

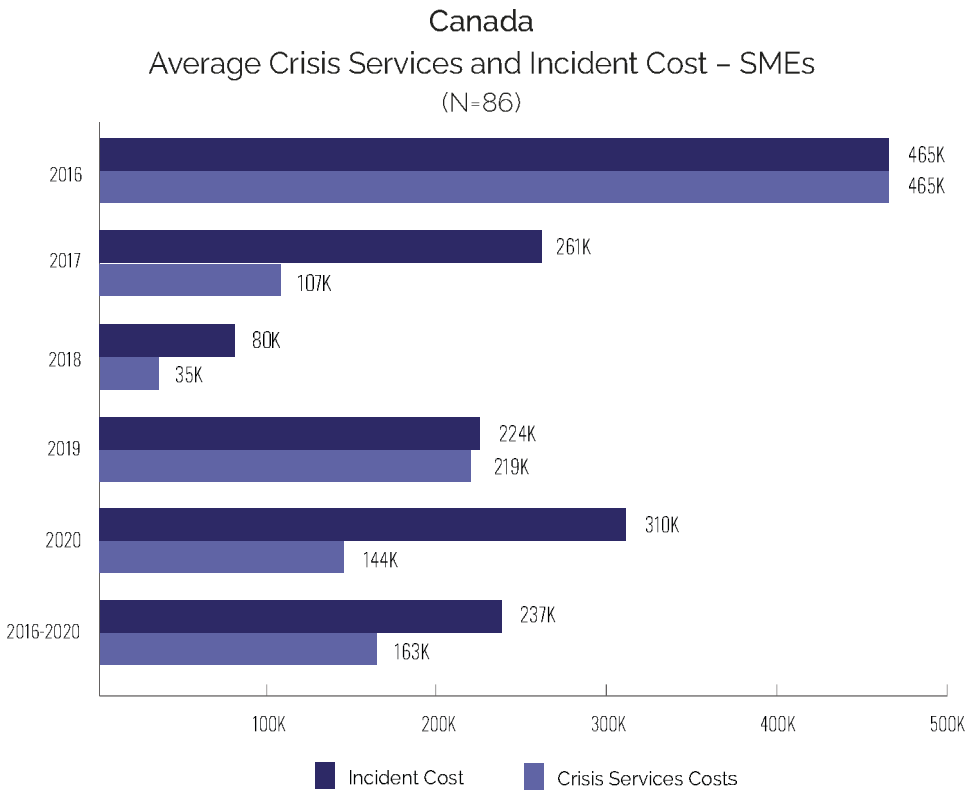

Figure 30

Canada
Top Causes of Loss 2016-2020 – SMEs

Cause of Loss	Claims	Average Incident Cost
Ransomware	33	393K
Business Email Compromise	17	178K
Hacker	10	115K
Staff Mistake	6	23K

Table 4

7 Canadian claim amounts were provided in CAD. These amounts were converted to USD as of December 31st of the year of each incident.

Conclusion

With this eleventh edition of the Cyber Claims Study, NetDiligence continues to raise the bar for presenting and understanding comprehensive loss analysis for cyber insurers and other key stakeholders. For eleven years, these studies have represented the gold standard in the cyber insurance space and, arguably, in the entire cybersecurity space. No other studies provide more or better evidence-based information.

This year's study includes more data and more targeted findings than ever before including the first data analysis of Canadian claims. 3,000 new claims were submitted this year, an almost 50% increase over last year. These were added to an existing dataset of over 2,700 claims. The result has been a comprehensive, representative, and objective dataset of cyber claims incidents, including their causes and monetary impacts.

As more and more insurers and brokers have participated in this study and shared even more claims and more information about each claim, the value of the study has continued to increase. For the benefit of the industry overall, all underwriters are encouraged to participate in next year's NetDiligence study. All participating insurers are encouraged to share a larger percentage of their cyber claims, especially those for companies with more than $2B in annual revenue. As participation in the study expands in these two ways, its findings will be richer and more representative of changing market conditions.

Insurance Industry Participants

Over the years, many insurance companies have contributed claims data for this study. We thank them all, as without their participation this study would not be possible. Special thanks go to the following companies for contributing a significant number of new claims for analysis and inclusion in the 2020 study.

AXA XL

Beazley

Berkley Cyber Risk

CFC Underwriting

Chubb

Great American Insurance

Hiscox

Markel

Philadelphia Insurance Companies

QBE

Sompo International

Swiss Re

Tokio Marine HCC

Travelers

United States Liability Insurance

Insurers: We invite you to join this elite group of participating companies. We'll be starting next year's study in January. Contact us at cyberclaims@netdiligence.com.

Appendices

Revenue Size

Analysis of claims by annual revenue size of the claimant has been an important part of every NetDiligence study. The graphics below provide insight into the proportion of claims in the dataset for each company size grouping.

As was mentioned previously, SMEs (companies with annual revenue less than $2B) account for 99% of the claims analyzed, and 61% of total incident cost. Large Companies (companies with annual revenue greater than $2B) account for only 1% of the claims analyzed but 39% of total incident cost.

Percentage of Claims by Revenue Size
SMEs – 2016–2020
(N=5,716)

Figure 31

Incident Cost by Revenue Size
SMEs – 2016–2020

	Claims	Minimum	Average	Maximum	Total	Rank*
Nano-Rev (<$50M)	2,651	1K	88K	6.7M	232.8M	4
Micro-Rev ($50M-$300M)	971	1K	172K	7.5M	167.4M	3
Small-Rev ($300M-$2B)	223	3K	478K	7.4M	106.7M	1
Unknown	1,162	1K	189K	120.2M	220.0M	2

*Rank based on Average Incident Cost

Table 5

Average Crisis Services Costs by Revenue Size

SMEs – 2016–2020

	Forensics	Monitoring	Notification	Legal Guidance	Other	Total Crisis	Rank*
Nano-Rev (<$50M)	35K	11K	14K	15K	45K	53K	4
Micro-Rev ($50M-$300M)	64K	26K	43K	33K	116K	110K	3
Small-Rev ($300M-$2B)	120K	27K	66K	44K	143K	209K	1
Unknown	43K	8K	12K	10K	177K	189K	2

*Rank based on Total Crisis Services Cost

Table 6

Business Sector

Claims are categorized into one of 18 sectors. As has been the case for many years, claims from the Professional Services, Healthcare, Financial Services, Manufacturing, and Retail sectors provide over 65% of the SME claims in the dataset.

The graphic below shows the percentage of SME claims by sector for 2016–2020.

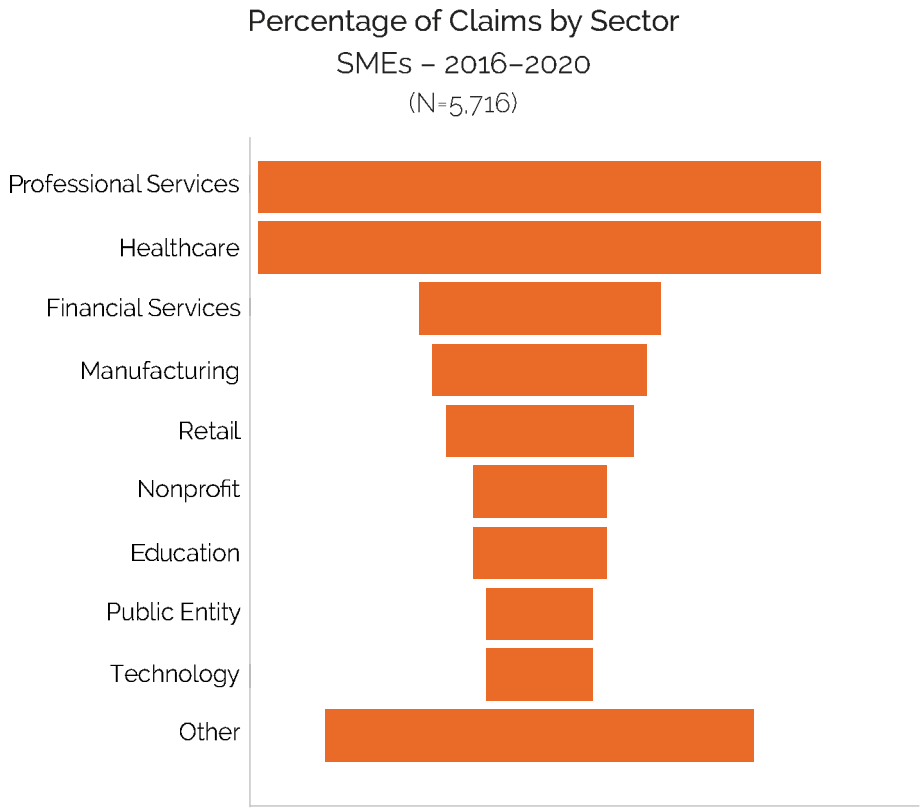

Figure 32

The following two tables list important metrics for claims in each sector. Table 7 provides a summary of total incident cost. Table 8 provide a summary of Crisis Services costs.

Incident Cost by Sector
SMEs - 2016-2020

Sector	Claims	Minimum	Average	Maximum	Total	Rank*
Education	229	1K	118K	1.5M	27.1M	10
Energy	20	11K	89K	390K	1.8M	15
Entertainment	20	4K	110K	548K	2.2M	13
Financial Services	440	1K	112K	5.0M	49.4M	11
Gaming & Casino	6	18K	202K	532K	1.2M	6
Healthcare	969	1K	74K	6.6M	71.6M	16
Hospitality	86	2K	159K	2.6M	13.7M	9
Manufacturing	433	1K	180K	20.0M	77.9M	7
Media	37	2K	214K	2.5M	7.9M	4
Nonprofit	271	1K	65K	1.2M	17.6M	17
Other	580	1K	104K	4.9M	60.4M	14
Professional Services	1,088	1K	211K	120.2M	229.3M	5
Public Entity	216	2K	111K	1.4M	24.1M	12
Restaurant	23	2K	63K	376K	1.4M	18
Retail	318	2K	167K	7.5M	53.2M	8
Technology	180	2K	296K	7.4M	53.4M	3
Telecommunications	25	4K	300K	2.3M	7.5M	2
Transportation	66	1K	412K	17.5M	27.2M	1

*Rank is based on Average Incident Cost

Table 7

Average Crisis Services Costs by Sector

SMEs - 2016-2020

Sector	Forensics	Monitoring	Notification	Legal Guidance	Other*	Total Crisis Services	Rank**
Education	64K	9K	38K	22K	128K	99K	7
Energy	52K		6K	10K	65K	70K	10
Entertainment	32K	92K	3K	33K		64K	13
Financial Services	41K	10K	13K	21K	61K	68K	11
Gaming & Casino	132K		6K	31K	3K	159K	3
Healthcare	34K	20K	26K	10K	83K	36K	18
Hospitality	79K	18K	36K	33K	28K	101K	6
Manufacturing	34K	7K	8K	23K	40K	77K	9
Media	34K		86K	22K		52K	16
Nonprofit	47K	13K	6K	15K	46K	55K	15
Other	44K	4K	11K	12K	188K	58K	14
Professional Services	35K	8K	11K	15K	85K	271K	1
Public Entity	46K	19K	20K	20K	97K	95K	8
Restaurant	30K	7K	16K	18K	85K	48K	17
Retail	104K	14K	47K	33K	121K	134K	4
Technology	73K	45K	83K	32K	88K	129K	5
Telecommunications	89K	1K	22K	204K	37K	241K	2
Transportation	73K	8K	3K	14K	0K	66K	12

* Includes public relations, data restoration, and sometimes ransom payment, and fraudulent wire transfer
**Ranking is based on Average Crisis Services

Table 8

Cause of Loss

Claims in the dataset are classified by 24 distinct causes of loss. As the graphs below show, ransomware, hackers, BEC, staff mistakes, and phishing were the leading causes of loss for 2016–2020.

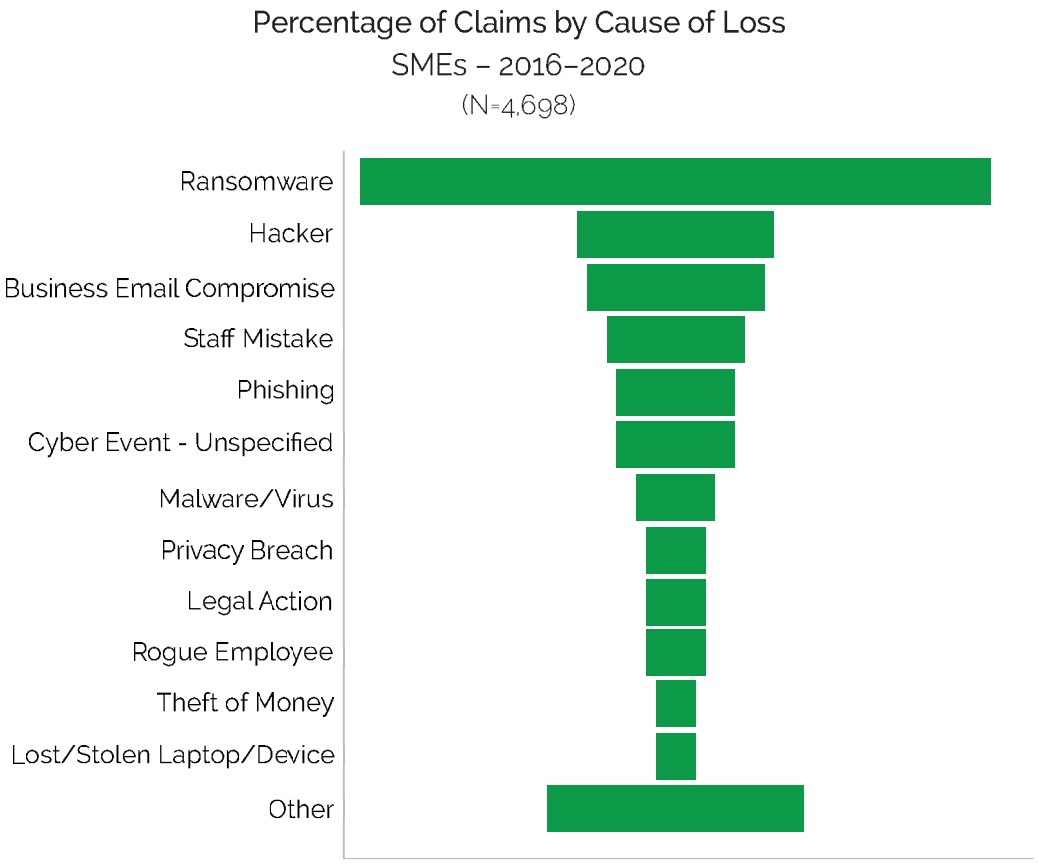

Figure 33

The following two tables tell the story for incident and Crisis Services costs based on cause of loss.

Incident Cost by Cause of Loss
SMEs - 2016-2020

Cause of Loss	Claims	Minimum	Average	Maximum	Total	Rank*
Business Email Compromise	401	1K	123K	3.4M	49.4M	8
Cyber Event (unspecified)	160	2K	100K	860K	15.9M	11
Hacker	441	1K	430K	120.2M	189.5M	2
Legal Action	52	3K	90K	661K	4.7M	13
Lost/Stolen Laptop/Device	69	1K	57K	1.5M	3.9M	18
Malware/Virus	168	2K	160K	6.9M	26.9M	7
Negligence	4	5K	63K	121K	253K	16
Paper Records	28	1K	40K	650K	1.1M	20
Phishing	253	1K	72K	666K	18.2M	14
Privacy Breach	33	1K	13K	51K	415K	25
Programming Error	16	4K	348K	3.6M	5.6M	3
Ransomware	1,474	1K	179K	20.0M	264.4M	5
Rogue Employee/ Malicious Insider	136	1K	91K	2.5M	12.4M	12
Social Engineering - All	716	1K	114K	3.4M	81.8M	9
Staff Mistake	244	1K	13K	284K	3.2M	24
System Glitch	13	4K	1.5M	17.5M	19.5M	1
Theft of Hardware	44	1K	16K	100K	0.7M	23
Theft of Money	54	1K	102K	1.1M	5.5M	10
Third Party	8	5K	33K	76K	264K	21
Trademark/Copyright Infringement	8	12K	166K	468K	1.3M	6
Unauthorized Access	1	20K	20K	20K	20K	22
Wire Transfer Fraud	58	9K	289K	1.9M	16.8M	4
Wrongful Data Collection	3	5K	42K	86K	126K	19
Other	377	1K	58K	2.8M	21.9M	17
Unknown	974	1K	69K	2.0M	67.3M	15

*Rank based on Average Incident Cost

Table 9

 Version 1.0

Average Crisis Services Costs by Cause of Loss
SMEs - 2016-2020

Cause of Loss	Forensics	Monitoring	Notification	Legal Guidance	Other*	Total Crisis Services	Rank**
Business Email Compromise	42.7K	15K	13K	30K	88K	79K	8
Cyber Event (unspecified)	43.1K	1K	8K	8K		50K	13
Hacker	44.5K	12K	43K	30K	28K	398K	1
Legal Action	24K	3K	7K	17K	67K	39K	16
Lost/Stolen Laptop/Device	20K	10K	73K	14K	117K	46K	14
Malware/Virus	105K	2K	30K	32K	116K	142K	2
Negligence	6K	1K	20K	24K		41K	15
Paper Records	16K	3K	4K	11K	20K	13K	22
Phishing	46K	20K	10K	17K	24K	56K	12
Privacy Breach	17K	1K	2K	5K		16K	21
Programming Error	37K	300K	278K	21K		123K	3
Ransomware	45K	20K	19K	12K	102K	72K	9
Rogue Employee/ Malicious Insider	64K	5K	7K	34K	19K	57K	11
Social Engineering–All	42K	16K	12K	25K	91K	71K	10
Staff Mistake	51K	7K	6K	5K	4K	10K	23
System Glitch	78K	2K	81K	40K	54K	87K	6
Theft of Hardware	8K	0K	1K	4K	50K	7K	24
Theft of Money	18K	0K	18K	14K		30K	18
Third Party	23K	36K		12K	1K	28K	19
Trademark/Copyright Infringement				91K		91K	4
Wire Transfer Fraud	15K	5K		15K	141K	91K	5
Wrongful Data Collection				80K		80K	7
Other	15K	8K	6K	9K	83K	19K	20
Unknown	22K	6K	1K	11K	34K	32K	17

* Includes public relations, data restoration, and sometimes ransom payment, and fraudulent wire transfer
**Ranking is based on Average Crisis Services

Table 10

Type of Data

For incidents that expose data, it is important to understand the type of data that was exposed or stolen. Statutes in each state of the United States, the GDPR in the European Union, and laws in many other countries require notification and other actions when certain types of data have been exposed.

Personally Identifiable Information (PII), Private Health Information (PII), and PCI data (payment cards) are the three types of data familiar to most people. However, claims can be classified with 13 other types of data, including non-card financial, other non-public, W-2 specific data, and trade secrets.

Because a large percentage of incidents (ransomware, DDoS, and wire transfer fraud) do not expose records at all, a new category was created in 2018 to capture these incidents. This category is "files-critical". An example of an incident with "files-critical" data would be a ransomware event that locked a database, system, or network deemed essential.

The chart below depicts the percentage of claims for each data type. The tables provide summary statistics for incident and Crisis Services costs.

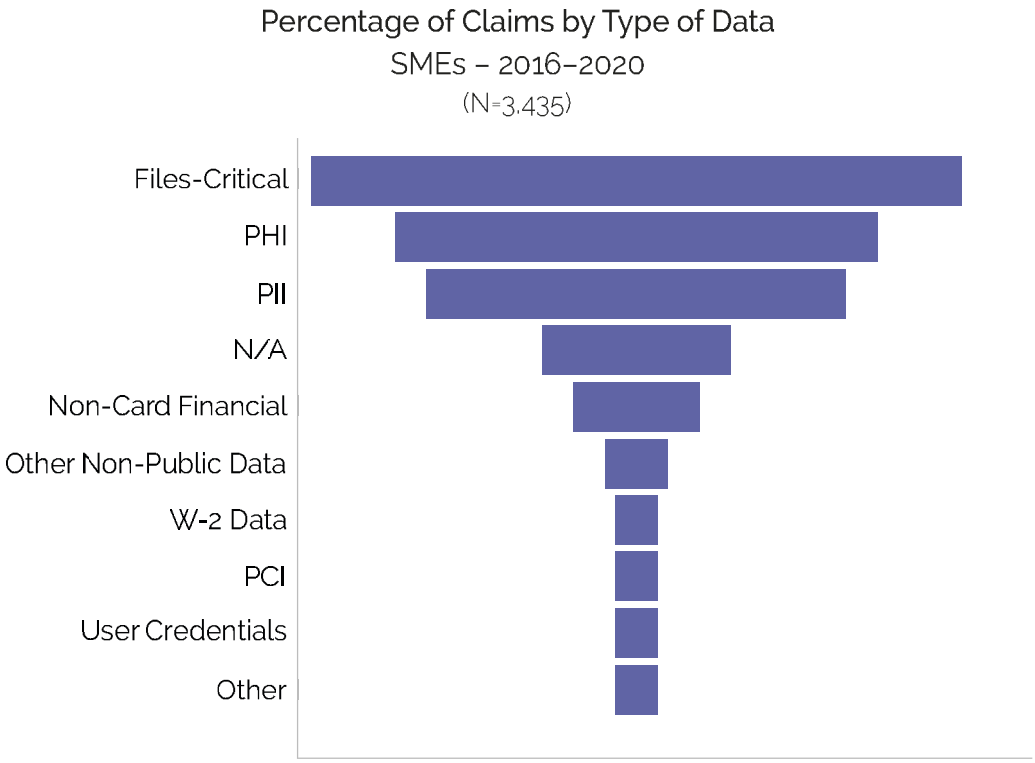

Figure 34

Incident Cost by Type of Data
SMEs - 2016-2020

Type of Data	Claims	Minimum	Average	Maximum	Total	Rank*
DDoS	5	4K	85K	183K	427K	10
Email (unspecified)	14	3K	78K	200K	1.1M	11
Files-Critical	1,023	1K	231K	20.0M	236.1M	5
Intellectual Property	20	3K	178K	1.2M	3.6M	6
N/A	304	1K	91K	1.9M	27.7M	9
Non-Card Financial	193	1K	764K	120.2M	147.5M	1
Other	11	6K	386K	1.1M	4.2M	2
Other Non-Public Data	82	2K	154K	3.1M	12.6M	8
PCI	76	2K	340K	6.9M	25.9M	3
PHI	627	1K	64K	2.1M	40.0M	13
PII	538	1K	156K	7.5M	83.8M	7
Trade Secrets	4	4K	59K	208K	237K	15
Unknown	1,966	1K	63K	2.8M	124.2M	14
User Credentials	59	1K	231K	3.9M	13.6M	4
User Online Tracking	1	25K	25K	25K	25K	16
W-2 Data	84	2K	68K	294K	5.7M	12

*Rank based on Average Incident Cost

Table 11

Average Crisis Services Costs by Type of Data
SMEs -2016-2020

Type of Data	Forensics	Monitoring	Notification	Legal Guidance	Other*	Total Crisis	Rank**
DDoS	38K			8K	4K	36K	14
Email (unspecified)	38K		2K	38K	157K	156K	3
Files-Critical	53K	22K	23K	17K	95K	88K	8
Intellectual Property	130K			28K	521K	148K	4
N/A	32K	5K	4K	10K	45K	42K	13
Non-Card Financial	28K	8K	13K	20K	114K	974K	1
Other	63K			4K	276K	146K	5
Other Non-Public Data	41K	3K	1K	41K	18K	57K	11
PCI	189K	11K	28K	50K	175K	218K	2
PHI	45K	20K	35K	12K	85K	49K	12
PII	57K	11K	27K	32K	79K	94K	6
Trade Secrets	40K			54K		57K	10
Unknown	26K	3K	10K	7K	89K	27K	15
User Credentials	73K	15K	18K	29K	45K	92K	7
User Online Tracking	15K				10K	25K	16
W-2 Data	46K	29K	11K	20K	9K	57K	9

* Includes public relations, data restoration, and sometimes ransom payment, and fraudulent wire transfer
**Rank based on Average Crisis Services

Table 12

Ransomware-as-a-Service (RaaS): A new business model for cyber criminals

Threat actors are selling their ransomware secrets to less sophisticated criminals, resulting in an explosion of new cyberattacks.

by RSM

Ransomware has become the most significant cybersecurity threat today, impacting large multinational organizations to the smallest of entities. A ransomware attack represents a low-risk, high-reward opportunity for criminals, as little effort is required to access sensitive information and demand bounties that can significantly harm businesses—especially small- to medium-sized companies. The RSM US Middle Market Business Index 2021 Cybersecurity Special Report found that 42% of middle-market executives know of a company that has been a target of a ransomware attack, and 11% of executives indicated that they experienced more than one attack in 2020. In the current environment, inaction is not an option, and companies must take proactive steps to address expanding and evolving ransomware risks.

To add to the evolving threat landscape, cyber criminals have taken advantage of the exponential growth of Ransomware-as-a-Service (RaaS), a service model where sophisticated threat actors develop and sell ransomware platforms to other threat actors. Now, cyber criminals no longer need to be highly technical to launch a cyberattack into an organization, so ransomware attacks are rapidly increasing.

How does the RaaS model work?

- The RaaS model provides the purchaser with extensive training, reference materials and malicious code that can be used to launch a ransomware attack. Here are some key takeaways for understanding how RaaS works:
- RaaS providers typically use several different purchase models:
    - Subscription: The RaaS provider receives a predetermined cryptocurrency payment for a finite period of usage.
    - Affiliate: The RaaS provider receives a recurring fee plus a percentage of the ransom payment.
    - Purchase: The RaaS provider sells a "kit" to the purchaser.
- The attacks leverage well-established hacking tools (i.e., Mimikatz), while employing current vulnerability and penetration testing tools (i.e., Cobalt Strike).
- These attacks are designed to not only exploit well-known, existing vulnerabilities, but also take advantage of new zero-day vulnerabilities.
- Threat actors have developed elaborate social engineering and intelligence-gathering methods with the intention of causing significant devastation for a victim when a ransomware attack is launched.

How to protect your organization from ransomware attacks

The reality is that ransomware will continue to be an ongoing threat to organizations, and there is no way to completely remove the risk of ransomware. However, the following actions can help reduce the potential success of an attack:

- **Stay informed about new vulnerabilities**: The National Institute of Standards and Technology (NIST) published information to help protect against threats and recover from a potential ransomware attack. In addition, the US-CERT—CISA regularly posts updates on new vulnerabilities and attacker tactics, techniques and procedure (TTP) trends.
- **Make sure you have backups**: It is important to have backups not just for business continuity and disaster recovery, but also to be able to restore critical data if a ransomware attack occurs. The

trusted, age-old 3-2-1 backup rule will help protect backups from attackers. Don't forget that attackers also work nights, weekends and holidays, so you should have regular and frequent backups.

- **Implement advanced endpoint detection and antivirus protection**: While attackers use established TTPs, they are also attacking new vulnerabilities and constantly updating their toolset. Have a robust and properly configured defense system in place to identify and minimize potential attacks before they gain traction and impact your environment.
- **Have an incident response plan**: Develop a strategy that outlines how your organization will respond if you suffer an attack. A ransomware situation is a chaotic event; the longer it takes you to respond to an attack, the more costly it will be.

Ransomware has always been a concern, but the rapidly changing threat landscape is increasingly impacting companies of all types and sizes. Every organization should create a security approach that includes strategies to both prevent and remediate ransomware attacks. A strong security plan can limit financial exposure and reduce downtime.

About RSM

RSM is the leading provider of audit, tax and consulting services focused on the middle market, with nearly 13,000 professionals in 83 U.S. cities and four locations in Canada. It is a licensed CPA firm and the U.S. member of RSM International, with 48,000 people in more than 120 countries. For more information, visit https://rsmus.com/.

The Cyber-Demic: Why Data Breach Preparedness Is in Hyperdrive, How We Got To Herd Inevitability and The Only Path Forward.

by Experian®

There's no polite way to say this, so I'll make it plain.

The threat of a ransomware cyberattack is not only real; it's here and causing damage by the second, with no end in sight. At this stage of the lawless pay-or-else game, no organization is safe from the devastating financial impacts, regulatory issues, and brand damage of this malware-driven virus. Despite best efforts to prevent it from rising, like the rampant Delta variant, ransomware is raging out of control, posing extreme risks and breaching unsuspecting and unprepared barriers.

What We Know

In the first half of 2021 alone, we saw a 102% increase in ransomware attacks from the year before, according to data released from the cybersecurity firm, Check Point Software. As three cybersecurity threat reports put it, "Attackers have doubled down on ransomware and phishing –with some tweaks—while deep fakes and disinformation are set to become major threats in the future." Even more troubling, with data compromises up 38% over the first quarter of 2021, the Identity Theft Resource Center predicts that if the trend continues, the year could end with data compromises reaching an all-time high.

The hard truth: we are beyond the tipping point of herd inevitability.

Getting hit by a ransomware attack can be summed up in two words: when and how. Gone are the days of "if." Studies and reports show that more ransomware events are happening, and the costs to respond to them are increasing. The outlook is not positive, but there is light in the tunnel.

The Only Path Forward is Preparedness

Ransomware is ripping through all industries, stressing systems, and causing brand harm. Every entity must be ready to unleash an agile and effective response to protect its reputation, customers, and future in these unpredictable times.

At Experian, we've seen the impact of attacks play out firsthand. So far this year, we're up to 6,000 breaches serviced, up nearly 1,000 from 2020. Having managed more than 55,000 breaches over almost 20 years, we also see ransomware attacks getting more complex. Here's what we know:

1. **It's taking 20% longer to execute** a consumer response.
2. **Hackers are getting more sophisticated** in their payment scheme, demanding double extortion money: a first fee to access the data and another to keep it off the dark web. Sometimes they get bolder and ask for three disbursements. The stakes are higher from a company response point of view, too, with ransomware attacks requiring more complex involvement from multiple resources, from crisis public relations and legal to forensics and the C-suite.
3. **All of this activity adds up** in additional costs to plan for and respond to events. In the end, it amounts to higher regulatory fines, customer flight, and brand damage.

Experian handles many data breach cases, and we know that 7 of 10 breaches involve ransomware. As highlighted in this year's Cyber Claims Study, our work also confirms that an organization's size doesn't mean, by any account, that their claim will be small. We also learned that spending on preparedness could save money, and more, in the long run.

Proper preparedness is the only path forward because, again, an attack is just a matter of time.

With Experian® Reserved Response, cyber insurers can be ready, not hasty. With policy costs up 15-17%, being prepared means saving money; 25% less if consumer response is needed. With major providers exiting cyber policies, insurers can benefit from Experian's referral model for lower costs. Being prepared with Experian also means getting:

- Guaranteed Service: Our program includes built-in penalties for missing incident response SLAs
- Speed and Custom Responses: You won't get cookie-cutter service with our 24/7 dedicated U.S.-based call center support
- Yearly Readiness Planning and Live Drills: A ransomware attack is no time to wing it. Our clients are prepared to respond rapidly.
- Small Business Solutions: Guaranteed solutions for affected populations of up to 1 million

Data Breach Response

- Notification: Quickly notifies affected individuals within federal and any state data breach laws. Includes letters and address verification.
- Enhanced Call Center: Dedicated, 24/7 U.S.-based call center support to service impacted customers.
- Identity Protection: Offers Experian IdentityWorks® to help customers maintain security and peace of mind.
- Identity Restoration: U.S.-based Fraud Resolution Agent to guide customers through recovery.

Ransomware is here for the long haul. Experian Reserved Response and Data Breach Resolution are the best ways to fight it.

About Experian® Data Breach Resolution

Experian® Data Breach Resolution, powered by the nation's largest credit bureau, is a leader in helping businesses prepare for a data breach via the proprietary Experian® Reserved Response program and also mitigate consumer risk following breach incidents. With more than nineteen years of experience, Experian has successfully serviced some of the largest and highest-profile data breaches in history. The group offers swift and effective incident management, notification, call center support and fraud resolution services while serving millions of affected consumers with proven credit and identity protection products. For more information, visit www.experian.com/databreach and follow us on Twitter @Experian_DBR.

Hiding in Plain Sight: Towards Now-Gen Cyber Risk Underwriting

by Erin Kenneally, Director, Cyber Risk Analytics, Guidewire

Risk Underwriting Self Help: Closing the Data & Analytics Feedback Loop

Take a gander at any report, paper or article on the state of cyber insurance during its entire multi-decade existence and you'll find at least one universal bellyaching: there is a lack of incident loss data upon which to reliably assess insurance risks and calculate premiums.

Myth busted: the problem is not lack of data, rather, it is under-extraction of insights from the actuarial data that has been generated around cyber incidents. Specifically, there is a facet of incident data that promises to drive better underwriting but which insurers have left on the proverbial cutting room floor: post-incident digital forensics.

Heretofore the industry has mined incident data monolithically and superficially for its firmographics and insurable impacts, which in turn have bounded risk selection and pricing. The industry has overlooked a key data and analytical feedback loop whose closure would move insurers beyond the self-perpetuated actuarial Groundhog Day. Digital forensics & incident response (DFIR) data about incident attack vectors and controls deficiencies collected in the post-incident claims process will evolve the quality of risk correlation and causation and enrich the frontend underwriting of cyber risk.

The Tail Wagging the Dog: Legal Privilege

There are two main dynamics that impede inclusion of DFIR data into the actuarial record and stifle improved underwriting: misaligned insurer-law firm data governance, and disjointed business process.

Cyber carriers are positioned to collect DFIR data and utilize it to inform frontend risk underwriting yet remain largely abstracted from the data because of how they structure the incident response process. Insurers cover the cost of forensic incident response in the wake of breaches and govern the relationship between policyholders and response firms.

Significantly, however, cyber insurers commonly appoint law firms to manage the incident response functions and workflow. This practice strategically and deliberately leverages attorney-client privilege or work product doctrine to prevent third party liability and E&O exposure that may arise if causal details from the DFIR report were otherwise discoverable during litigation proceedings. The goldmine of who, what, when, where, why, and how that is extracted in the DFIR process is nevertheless often left entombed within the ore of firmographic and loss figures associated with the claim.

The economic justification for deferring to avoidance of potential liability cost to the detriment of continuous-loop analytics and ex ante risk reduction has grown frail. Wielding attorney-client privilege to shield access to DFIR data is a vestige of an era when cyber policies were liability-centric and losses were driven by third party litigation following a data breach.

Present day losses and risk transfer needs of cyber compromised companies are skewing more heavily toward business income, interruption (BI) and recovery costs that flow from technical compromise, largely as a result of the ransomware epidemic.

Disjointed Insurance Business Processes

The business process issue for many cyber insurers is not a function of authority over IR data, but rather, structuring and processing more robust claims data to inform underwriting. So even if carriers were to exercise their governance authority to acquire better data from the IR process, the cyber incident details, metadata, and more granular forensics may not be integrated into legacy database schema and tables to close the loop with front-end risk analyses.

Unhiding What's in Plain Sight

While there is variability across IR documentation, the lack of carrier-driven standards and the expanded role of insurers in proactive risk reduction argue that smart engineering of IR data for claims should take a cue from infosec industry data standards. Innovative infosec and DFIR firms are embracing the VERIS and Mitre ATT&CK frameworks, so it's logical that these should be the connective tissue for carriers who seek to effectuate that learning and insight.

If IR and claims are classified in this way an underwriter considering a cyber policy application can consult its corpus of VERIS/ATT&CK-classified claims to augment its assessment of likelihood and severity of the applicant's cyber losses.

Now-Gen Cyber Underwriting: Building a More Robust Cyber Risk Playbook

Now-generation cyber underwriting requires going beyond indemnifying, pooling, and diversifying risks at the policy level to proactively managing insureds' cyber risk at the technical and governance levels.

Continuously looping backend DFIR data for frontend underwriting offers many advantages, including: reduced risk visibility bias, certainty of semantic and syntactic standards, harnessing untapped claims insights, closing the gap between pricing and value, and enhanced understanding of controls efficacy.

About Guidewire

Guidewire is the platform P&C insurers trust to engage, innovate, and grow efficiently. We combine digital, core, analytics, and AI to deliver our platform as a cloud service. More than 400 insurers, from new ventures to the largest and most complex in the world, run on Guidewire. For more information, contact us a info@guidewire.com.

GUIDEWIRE
CYENCE

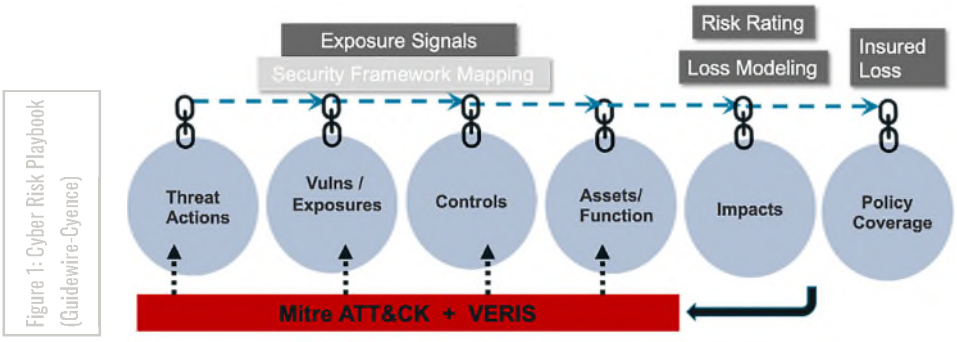

Figure 1: Cyber Risk Playbook (Guidewire-Cyence)

For the full version of this article, see:
https://success.guidewire.com/Whitepaper-HidinginPlainSightTowardsNow-GenCyberRiskUnderwriting_Registration.html

This year's study demonstrates that every enterprise must consider its ability to withstand cyberthreats

by Beckage

With the exponential rise in cybercrimes and new national attention to ransomware, the eleventh edition of NetDiligence's Cyber Claims Study is more relevant than ever. Since 2011, this survey has provided unparalleled insight into the shifting cybersecurity landscape. The analysis of almost 6,000 claims in this year's study serves as a stark reminder of the growth in cyberthreats in recent years, and the expansion of attacks across industry sectors and businesses of all sizes.

At Beckage, our data security and privacy professionals rely on this study for its evidence-based assessment of the trends in the field where we are working on a day-to-day basis. Each year, the study offers a wide lens, capturing the experience of businesses and organizations of all sizes, similar to the clients that we guide through data security incidents. Its analysis of past claims allows us to analyze and assess what's coming next.

This year, the study reflects the well-documented increase in cybercrimes and provides a critical analysis that enterprises of every size should carefully consider. Cyber incidents have not just increased in number, the number of exploited small- and medium-sized enterprises (SMEs) has also vastly expanded. Smaller business size does not translate into fewer consequences, as the study found no clear correlation between the size of a claimant organization and the magnitude of loss related to the incident.

When NetDiligence began this crucial study in 2011 with an analysis of less than 100 cyber claims, there were fewer threats, and many small businesses were less reliant on e-commerce, cloud storage, and constant connectivity to manage and grow their business operations. Now, nearly every organization has become a potential target for exploitation and no company should expect that its size can provide insulation from attacks.

In today's economy, SMEs are often just as reliant on well-connected business ecosystems as large corporations. Accelerated by the COVID-19 pandemic, SMEs need to leverage virtual communication platforms and remote access. Many are sophisticated in their use of personal data, and thus may store large amounts of sensitive information in the cloud or on premise. At the same time, SMEs may not perceive the need for resources to harden their data security environment and compliance programs.

The findings of this year's study demonstrate that every enterprise must consider its ability to withstand cyberthreats, comply with an increasingly complicated constellation of state, federal, and international regulations, and prepare to respond to incidents now.

The study's analysis does not, however, focus only on the challenges that exist or the threats that continue to grow. Instead, it's assessment of the most prevalent incidents can help SMEs prioritize a roadmap to increasing their data security posture and privacy policies.

Importantly, the study found that 70% of claims and 80% of total incident costs for SMEs resulted from just five categories of incidents: ransomware, other hacker attacks, business email compromise, staff mistakes, and phishing. Among these, ransomware was the most prevalent incident for SMEs, accounting for 79% of claims with a business interruption loss and 81% with a recovery expense loss.

Based on prior experience and resources like this study, data security and privacy professionals at firms like Beckage have insight regarding what threats are most likely to occur, can assist organizations in preventing incidents before they happen, create business continuity and response plans to minimize loss, and guide SMEs strategically through each step following an incident.

While the headlines often focus on the incident facing large organizations like Colonial Pipeline or JBS Foods, the NetDiligence's Cyber Claims Study goes much deeper. Its findings again demonstrate the prevalence of threats for enterprises across all industries, regardless of size – and the need for every organization to incorporate data security as a fundamental business priority.

About Beckage

Beckage is a women-owned law firm focused on technology, data security, and privacy. Our attorneys counsel clients on matters pertaining to data security and privacy compliance, litigation and class action defense, incident response, government investigations, technology intellectual property, and emerging technologies. Our lawyers are technologists, tech business owners, CISAs, CISOs, former regulators, and certified privacy professionals. Learn more at Beckage.com.

Beckage
Legally Focused. Technology Driven.

About NetDiligence®

NetDiligence® is a leading provider of Cyber Risk Readiness & Response services. We have been providing cyber risk management services and software solutions to the cyber insurance industry, both insurers and policyholders, since 2001.

Our Cyber Risk Summit conferences and our cyber advisory groups function as information exchange platforms for insurers, legal counsel, and technology specialists. This community of experts serves as the vanguard in the fight against cyber losses. We listen and learn from them. That's why our services support our insurance partners and their policyholders both proactively for cyber readiness and reactively for incident response.

Breach Response Solution with Mobile App

Breach Plan Connect® is a securely hosted solution designed to help senior managers plan for, oversee, and coordinate their organization's response to a cyber incident. Breach Plan Connect comes pre-loaded with a comprehensive incident response plan template that can be easily customized. It also includes a free mobile app for convenient access and alternative means of communication if company systems are compromised.

Risk Management Portal for Insurers

The eRiskHub® is a white-label cyber risk management portal that helps both insurers and their clients combat cyber losses. This Software-as-a-Service (SaaS) offering provides tools and resources to help clients understand their exposures, harden their cyber defenses, and respond effectively to a cyber incident. Our mobile-friendly, flexible platform can be branded, customized, and delivered to any domain. Plus, it's scalable! Start small and increase your license as you grow. You can also add content for other geographic regions as you expand globally.

Cyber Risk Assessments

NetDiligence's QuietAudit® cyber risk assessments give organizations a 360-degree view of their people, processes, and technology, so they can reaffirm that reasonable practices are in place; harden and improve their data security; qualify for network liability and privacy insurance; and bolster their defense posture in the event of class action lawsuits. We offer network vulnerability scans and consultant-led assessments that are tailored to meet the unique needs of small, medium, and large organizations in all business sectors. A variety of automated online self-assessment surveys are also available for underwriting loss control and vendor risk management.

On-Site & Virtual Cyber Programs

The leading networking events for the cyber industry, NetDiligence conferences are attended by thousands of cyber insurance, legal/regulatory, and security/privacy technology leaders from all over the world. Each event features programming curated by cyber professionals and focused on current and emerging concerns in the ever-changing cyber landscape. We traditionally host five on-site conferences per year, in Philadelphia, Santa Monica, Toronto, London, and Bermuda.

Contact Us

For more information, visit us at netdiligence.com, email us at management@netdiligence.com or call us at 610.525.6383.

NetDiligence®

About the Study

Contributors

Risk Centric Security, Inc.

A special thank you also goes to Heather Goodnight-Hoffmann, cofounder and President, and Patrick Florer, cofounder and Chief Technology Officer of Risk Centric Security, who performed the data collection and data analysis, and provided material support in the writing and editing of the report. Risk Centric Security offers research, analysis, and reporting services, as well as state-of-the-art quantitative risk analysis and training for risk and decision analysis. For more information, visit www.riskcentricsecurity.com.

Other

We would also like to acknowledge the following individuals for their contributions to this annual study:

- Heather Osborne – Director of Global Events & Programming, NetDiligence
- Sharon Lyon – Publisher, NetDiligence

For more information, visit us at netdiligence.com, email us at management@netdiligence.com or call us at 610.525.6383.

Methodology

For this study, we invited the major underwriters and carriers of cyber insurance to submit claims information based on the following criteria:

- The incident occurred in 2018, 2019, or 2020.
- The claimant organization experienced a loss covered by a cyber or privacy liability policy.

Invitations to submit data were sent to 144 individuals at 87 organizations in the United States, Canada, and the United Kingdom. From this group, 21 individuals representing 19 organizations provided 3,000 analyzable new claims, using the proprietary NetDiligence® claims data collection worksheet.

The 2021 report also includes data from NetDiligence® studies published in 2017-2020, representing 2,797 incidents that occurred in 2016, 2017, 2018, and 2019. After the elimination of claims that were less than $1,000, the combined dataset included 5,060 incidents, each one, a data Incident insurance claim. This number represents a 50% increase in the number of analyzable claims compared to last year.

There were 5,580 claims in the dataset from American organizations, 163 claims from Canadian organizations, and 25 claims from organizations in the United Kingdom. There were also a small number of claims (N=23) from organizations in Australia, Germany, India, Ireland, Mexico, South Africa, Sweden, and organizations with a global footprint. The country was not specified in 6 claims.

When factoring in SIRs, we were able to calculate total Incident cost to-date for 5,060 (100%) of the claims in the dataset in which the total loss was less than or equal to $1,000. Of these claims, 860 (17%) specified the number of records exposed (greater than one record) and 2,641 claims (52%) included an accounting of Crisis Services costs. The number of claims reporting records decreased somewhat last year due to the large number of claims for incidents that did not expose records (ransomware, social engineering, BEC, etc.). The overall percentage of claims reporting records decreased by nine percentage points (26% to 17%) for the same reason.

For the first time, we did not calculate per-record costs. Per-record cost has been a controversial metric since it was introduced more than 10 years ago by the Ponemon Institute. In previous reports, we presented per-record costs as percentiles of the total distribution of per-record costs: averages from 100%, 95%, 90%, and 80% of the claims for which a per-record cost could be calculated. We have found that even this approach is not useful. Consequently, we no longer provided this analysis.

4,874 (84%) of the claims in the full dataset (N=5,797) were flagged as closed, 907 (15.7%) as open, and 16 (0.3%) as unknown claim status. 3,293 (56.8%) of the claims were for primary coverage, 32 (0.6%) for excess coverage, and 2,472 (42.6%) had an unknown, but most likely primary, coverage level.

There were 1,322 claims in the full dataset for which the revenue size of the organization was unknown. After comparing the distribution of their incident cost to those of SMEs and Large Companies, the decision was made to include these claims in the SME group.

Readers should keep in mind the following:

- Our sampling, although large, is a subset of all incidents. Some of the data points are lower than other studies because we focus on claim payouts

and total costs for specific incident-related expenses and do not factor in other financial impact, including in-house investigation and administrative expenses, customer defections, opportunity loss, etc.

- The NetDiligence data collection form includes approximately 50 fields per claim. Half of these fields captures demographic information: incident date, country, company size, sector, cause of loss, type of data, and incident description, etc. The other half captures loss data: SIR, Crisis Services including forensics, monitoring, notification, legal counsel, and other crisis services, legal costs and regulatory fines, PCI fines, business interruption loss and recovery expense, and total payout and incident cost.

- We have a significant issue of missing data, for the following two reasons.

  1. Not every claim involves each of the data elements that we ask for. For example, ransomware and staff mistake claims do not usually involve exposed records, whereas most hacking and malware/virus claims do; wire transfer fraud claims do not involve ransoms, and often do not incur any Crisis Services costs.

  2. Not every participant can or does provide us with every data element we ask for. The output format of many insurers' claims systems is not always easily aligned with our data collection form.

  This means that we often have to perform subset analyses in which we calculate results in what we describe as an "apples-to-apples" approach. Two of these kinds of analyses involve ransomware and business interruption. The ransomware example follows:

  - We have over 1,500 ransomware claims but know the ransom demand for fewer than 600 of these. The average 5-year incident cost for these 1,500 claims is $179K. However, when you include only the 600 claims for which the ransom is known, the average 5-year incident cost rises to $267K. If you further limit the analysis to ransomware claims with a business interruption loss, the total 5-year incident cost rises to $432K.
  - So, what is the incident cost of a ransomware event? All three answers are correct. The one you choose depends upon the question you are trying to answer.

- There is no attempt here to consider whether claims associated with the same incident appear more than once in the dataset. Given the fact that claims are anonymized when they are sent to us, there is no possible way for us to know this. We believe that the number of duplicated claims, though not zero, is very small.

- We are not privy to the terms of the cyber insurance policies governing the claims provided to us. Apart from SIR, we have no insight into specific exclusions, limits, or sub-limits that might be involved. For this reason, the reader is advised to consider the costs reported as a lower bound; i.e., we know that a given Incident cost at least $X, but cannot say how much more cost (than this amount) was actually incurred.

- Having said that, beginning in 2017, we asked respondents to provide us with an estimate of the total costs of the incident, including amounts that were excluded due to policy provisions. While a few participants in 2017 provided these estimates, a greater number of participants have done so since then, thereby increasing our ability to understand the true costs of an incident.

- Most claims submitted were for total insured losses and so included self-insured retentions (SIRs), which ranged from $0 to $10 million.

- In statistical terms, our sample is a "convenience" sample, which means that we have taken the data we have been given and have described it. We cannot make any statements about "significance" or "non-significance".

It is important to note that approximately 16% of the claims submitted for this study remain 'open'. Therefore, aggregate costs as presented in this study include "payouts to-date" and "incident cost to-date". It is virtually certain that additional payouts will be made on some of the claims in the dataset and therefore

REQUEST FOR NAIC MODEL LAW DEVELOPMENT

This form is intended to gather information to support the development of a new model law or amendment to an existing model law. Prior to development of a new or amended model law, approval of the respective Parent Committee and the NAIC's Executive Committee is required. The NAIC's Executive Committee will consider whether the request fits the criteria for model law development. Please complete all questions and provide as much detail as necessary to help in this determination.

Please check whether this is: ☐ **New Model Law** **or** ☒ **Amendment to Existing Model**

1. **Name of group to be responsible for drafting the model:**

   Receivership Law (E) Working Group of the Receivership and Insolvency (E) Task Force to complete the drafting.

   Note that Model #540 is currently being amended to address restructuring mechanisms, per the request for model law development adopted by NAIC Executive (EX) Committee on August 11, 2022. The Task Force hopes to consider the adoption of further amendments for this request within a similar timeframe.

2. **NAIC staff support contact information:**

   Jane Koenigsman
   jkoenigsman@naic.org
   816-783-8145

3. **Please provide a brief description of the proposed new model or the amendment(s) to the existing model. If you are proposing a new model, please also provide a proposed title. If an existing model law, please provide the title, attach a current version to this form and reference the section(s) proposed to be amended.**

   - ***Property and Casualty Insurance Guaranty Association Model Act (#540)***

   As presented by the National Conference of Insurance Guaranty Funds (NCIGF), cyber security insurance coverage is trending into the admitted market. Consequently, NCIGF anticipates the insurance insolvency resolution system will be presented with claims and other issues related to this coverage. These policy obligations may flow both from standalone cyber policies, endorsements, or from coverages that may be found to exist in commercial general liability and other lines of business typically written for business entities. For this reason, policymakers need to determine how such coverages will be handled should an insurer writing this business become insolvent. While each jurisdiction will need to decide whether, and within what parameters, cyber claims will be covered, we offer for consideration and guidance recommended amendments to the NAIC Property and Casualty Insurance Guaranty Association Act (NAIC Model 540). Policy makers should also consider how such claims will be handled before guaranty funds and associations (hereinafter "guaranty funds") are triggered – for example in a rehabilitation proceeding. Likewise, current insolvency processes and transition to the guaranty funds will need to be changed and enhanced to deal with this unique line of business and especially its demanding claims administration standards.

4. **Does the model law meet the Model Law Criteria?** ☒ **Yes** **or** ☐ **No** **(Check one)**

   (If answering no to any of these questions, please reevaluate charge and proceed accordingly to address issues).

   a. **Does the subject of the model law necessitate a national standard and require uniformity amongst all states?** ☒ **Yes** **or** ☐ **No** **(Check one)**

      If yes, please explain why:

      This proposed change is needed to ensure cyber insurance policyholders in all states are provided with guaranty fund coverage for this trending line of business.

   b. **Does Committee believe NAIC members should devote significant regulator and Association resources to educate, communicate and support this model law?**

☒ **Yes** **or** ☐ **No** **(Check one)**

5. What is the likelihood that your Committee will be able to draft and adopt the model law within one year from the date of Executive Committee approval?

☒ **1** ☐ **2** ☐ **3** ☐ **4** ☐ **5** **(Check one)**

High Likelihood **Low Likelihood**

Explanation, if necessary:
NCIGF has provided a proposal of suggested amendments for consideration. Proposed amendments include a definition of cyber insurance, coverage limitations and updates to other references.

6. What is the likelihood that a minimum two-thirds majority of NAIC members would ultimately vote to adopt the proposed model law?

☒ **1** ☐ **2** ☐ **3** ☐ **4** ☐ **5** **(Check one)**

High Likelihood **Low Likelihood**

Explanation, if necessary: See previous discussion.

7. What is the likelihood that state legislatures will adopt the model law in a uniform manner within three years of adoption by the NAIC?

☒ **1** ☐ **2** ☐ **3** ☐ **4** ☐ **5** **(Check one)**

High Likelihood **Low Likelihood**

Explanation, if necessary:

At this juncture, the amendments being considered are simple and because they have the potential to address future policyholder protection for this line of business, we believe such changes will be widely supported by all parties.

8. Is this model law referenced in the NAIC Accreditation Standards? If so, does the standard require the model law to be adopted in a substantially similar manner?

No reference in Accreditation Standards.

9. Is this model law in response to or impacted by federal laws or regulations? If yes, please explain.

No.

BACKGROUND OF THE

MEMORANDUM OF UNDERSTANDING

When a property & casualty insurer is liquidated, our regulatory system mitigates the adverse effects on policyholders and claimants through the state insurance resolution system. This system includes the coordinated management of the liquidation and wind down of the insurance company, in accordance with the state's receivership laws, and the payment of statutorily defined "covered claims" by the state guaranty fund system. In today's technological world, the insurance financial regulators, insurance receivers and the guaranty funds need advance planning for the transition from a troubled insurance company to liquidation.

This model Memorandum of Understanding ("MOU") is flexible and can be tailored the individual state insurance department and the specific troubled property and casualty insurer situation.

The MOU is intended to be used to facilitate transitional planning and preparation, starting when a troubled property and casualty insurer faces a material risk of being liquidated as insolvent[1]. Such a liquidation creates various obligations for the insurance receiver and triggers the guaranty funds' statutory duties to pay "covered claims." One goal of this transitional planning is to ensure that the guaranty funds are prepared and have the appropriate information necessary to assume their statutory duties to protect policy claimants promptly upon liquidation. Another important goal of this early estate planning process is to facilitate the receiver's duties upon liquidation, which include transition of claims to the guaranty funds, marshalling the remaining company assets and resolving claims against the insurer.

This planning process necessarily involves the sharing of confidential information about the troubled company that is protected by statutory confidentiality and privilege provisions. The parties sharing such information intend that it stay confidential and privileged and that no such protection be waived. This MOU is intended to document an agreement to that effect. The parties are the (1) Commissioner, (2) the insurance receiver if appointed (and who may be added later) or a standing insurance receivership office, if applicable, (3) the potentially triggered guaranty funds, and (4) the National Conference of Insurance Guaranty Funds ("NCIGF").[2] If separate from a state's receivership office, the state's insurance financial regulatory office could also be a party to the MOU, as the MOU can be tailored to the specific state.

The MOU provides that all non-public planning information provided to the guaranty funds under it shall be kept confidential, with the protective mechanism to maintain confidentiality spelled out. Specifically, confidential information initially may only to be shared with NCIGF and guaranty fund staff, agents, and counsel and, importantly, *may only be used for purposes of planning for liquidation of the troubled company.* Confidential information will not be shared with industry representatives who sit on or participate in a guaranty fund's Board of Directors until such time as the information is necessary for the Board to discharge statutory duties or consider or take for official action. Confidential information received by the Insurance Commissioner pursuant to its examination authority, which based upon NAIC Model 390 typically is "confidential by law and privileged, shall not be subject to [insert open records, freedom of information, sunshine or other appropriate phrase], shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action," is as shared agreed to retain such privileged status, particularly given the common interest of the parties in the MOU in facilitating the

[1] This model MOU is intended for use with only property and casualty receiverships. Life and health guaranty associations utilize confidentiality, and joint and common interest agreements, to gain access to information in the event of receivership, when necessary.

[2] See https://www.ncigf.org/. In general, the legal relationships between the troubled company and the regulatory authorities will be governed comprehensively by appropriate statutes and regulations in the state insurance code, thus generally there is no need for the troubled company be a party to the MOU. There may be, however, considerations in particular cases where it would be prudent to add the troubled company as a party, particularly if slow or incomplete compliance with disclosure and reporting requirements are an issue. For example, additional enforcement mechanisms could be added and troubled company cooperation with the prospective receiver and the guaranty funds could be spelled out in more detail.

prospective liquidation proceedings and the insurance resolution mechanism. As further protection for the privileged status of such confidential information, the guaranty funds are obligated under the MOU to defend against any attempt to discover any confidential or privileged information shared with them and to notify the other parties to the MOU of discovery or disclosure request.

The proposed MOU is a template that contains the essential terms of a confidential information sharing agreement and can easily be customized to address specific issues that may arise in the course of addressing troubled company concerns and in planning for liquidation.

MEMORANDUM OF UNDERSTANDING

This Memorandum of Understanding ("MOU") is among the [state] Department of Insurance ("DOI"), the [Receiver of the insolvent company – if appointed] and the [guaranty fund in the state of domicile of the troubled company, the other insurance guaranty funds which have executed this agreement (collectively "Guaranty Funds") and the National Conference of Insurance Guaranty Funds.(NCIGF)

Definitions:

1.1 "Agreement" or "MOU" refers to this Memorandum of Understanding;

1.2 "Confidential Information" refers to any:

a) documents, data or other information relating to any domestic insurance company in the State of [state] where the Commissioner has determined that the financial condition of such company creates a material risk of Liquidation that are not publicly available or public records, whether written or not, including but not limited to claims files and data; financial analyses, modeling and projections; trade secrets, technical processes and know-how; agency agreements, arrangements, accounts, proposals, lists, and other information; policyholder lists and information; costs and pricing information; internal procedures, strategies and plans; and computer programs;

b) work product or other information regarding any such Company that is confidential and/or privileged;

c) communications between the Parties regarding any potential or pending legal actions involving any such company that is a threat to such companies' solvency; and

d) specifically contemplates information received by the Insurance Commissioner pursuant to its examination authority [insert state adoption of NAIC Model Law 390], which is "confidential by law confidential by law and privileged, shall not be subject to [insert open records, freedom of information, sunshine or other appropriate phrase], shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action."

1.3 "Evaluation Material" refers to all information, oral or written, including but not limited to Confidential Information as defined herein, that is furnished to Guaranty Funds or NCIGF under the terms of this Agreement, and all analyses, compilations, studies, or other materials prepared by Guaranty Funds or NCIGF containing or based in whole or in part upon such information. "Evaluation Material" includes but is not limited to information on the financial condition of the company, information data systems utilized and condition of the data, location of data files, involved third party administrators, UDS test files that may be created, policy forms – especially those for unique or complex lines of business, company organization charts, claims counts and liability amounts by line and by state, and lists of cases in trial, attorney contacts and any other information appropriate to enable the Guaranty Funds to fulfill their statutory duties upon liquidation. This material shall be updated from time to time as appropriate.

1.4 "Company or Companies" refers to any domestic property and casualty insurance company in the State of [state]where the Commissioner has determined the financial condition of such company creates a material risk of Liquidation.

1.5 "Commissioner" refers to the Commissioner of Insurance of the State of [state].

1.6 "Party" and "Parties" refer to the Commissioner, the Receiver, if appointed, the signatory Guaranty Funds and the NCIGF.

1.7 "Receivership Court" refers to the [court with jurisdiction over the receivership]

1.8 "Receivership" refers to the rehabilitation or liquidation of any domestic insurance company in the State of [state].

1.9 "Receiver" refers to [name of deputy receiver if appointed]or any of his or her successors.

1.10 "Covered Claim" shall have the same meaning as contained in the applicable statutes of the Guaranty Funds.

II. Recitals

2.1 The Commissioner is responsible for the financial regulation of Companies. From time-to-time the financial condition of one or more of such Companies creates a material risk of Liquidation.

2.2 Should a Receivership occur of a Company, the Commissioner may appoint a special deputy receiver who will be responsible for the handling of such Receivership.

2.3 If the Receivership of a Company includes an order of liquidation with a finding of insolvency or if other statutory requirements are met, the Guaranty Funds will have the responsibility for the payment of "Covered Claims" arising from such Receivership.

2.4 The Parties agree that in order to properly prepare for any Receivership, to provide for a smooth transition to liquidation should it become required, and in order to avoid delay in the payment of "Covered Claims," it is essential to share Confidential Information among them with respect to any Company the Commissioner determines is at material risk of Liquidation.

2.5 It is agreed by the Parties that, subject to the Commissioner's discretion, the Commissioner can freely consult with the Receiver (if appointed), the Guaranty Funds, and NCIGF, with respect to any Company, including but not limited to, the dissemination of Confidential Information and Evaluation Material as defined herein. It is understood that such consultations are to be held in strictest confidence and the Commissioner may, in his or her discretion, withhold the name of the Company being discussed from the Guaranty Funds and the NCIGF.

2.6 The Guaranty Funds have determined that in order to protect consumers and to better fulfill their mission (*see* cite to applicable Guaranty Funds' statutes) it is necessary and proper for them to enter into this Agreement and likewise it is necessary and proper for the NCIGF, as a membership organization that supports the Guaranty Funds in their mission, to enter into this Agreement. The DOI and Receiver have determined that this Agreement enables them to better serve the insurance consumers in [involved states] and to better protect them from the adverse consequences of a Company liquidation.

III. Use and Treatment of Evaluation Material

3.1 Subject to the terms of this Agreement, the Commissioner and Receiver will grant the Guaranty Funds and NCIGF access to Evaluation Material as they determine is appropriate. The Evaluation Material shall be used by the Guaranty Funds and NCIGF to determine potential obligations of the Guaranty Funds, prepare for the possible assumption of such obligations, and to perform such

statutory obligations in the event they become obligated to pay "Covered Claims" under policies of insurance issued by a Company. The Guaranty Funds and NCIGF shall be allowed to copy such Evaluation Material for their own use consistent with the terms of this Agreement.

3.2 The Guaranty Funds and the NCIGF agree to maintain the confidentiality of all Evaluation Material provided to them, and of any privileges with respect to such information. The Guaranty Funds and the NCIGF agree not to disclose any Evaluation Material to any person or entity, except as expressly provided herein.

3.3 The Guaranty Funds and the NCIGF may share Evaluation Material with their respective counsel, consultants or agents as they deem necessary, provided that such persons agree to comply with terms of this Agreement, including but not limited to the remedies provided under Part IV. In the event of a breach of this Agreement by any person to whom Evaluation Material has been provided, the Party or Parties providing such information shall also remain liable for the breach.

3.4 The Guaranty Funds and the NCIGF agree that no Evaluation Material shall be provided to any insurance companies or the owners, directors, officers, employees, agents, representatives, or affiliates of any insurance companies, except as necessary to discharge statutory duties, for official action or consideration by the Board of Directors.

3.5 In the event that the Guaranty Funds or the NCIGF are served with process seeking the production of Evaluation Material, including but not limited to a subpoena or order of a court of competent jurisdiction, an investigation by a government entity, or discovery demand issued in connection with any action, the Guaranty Funds and NCIGF, as appropriate, shall notify the Commissioner and Receiver in writing as promptly as practicable. The Guaranty Funds and NCIGF, as appropriate, shall take reasonable actions to protect the confidentiality and, if applicable, the privileged status of such information, unless otherwise requested by the Commissioner or the Receiver. If a protective order or other remedy is not obtained prior to the date that compliance with the request is legally required, the Guaranty Funds and the NCIGF, as appropriate, will furnish only that portion of the Evaluation Material or take only such action as is legally required.

IV. Remedies

4.1 The Guaranty Funds and the NCIGF agree that money damages would not be a sufficient remedy for a breach of this Agreement, and that the Commissioner or Receiver shall be entitled to equitable relief, including injunctive relief, as a remedy for such breach. Such remedy shall be in addition to all other remedies available at law or in equity, and shall not be deemed the exclusive remedy for a breach of this Agreement. Any action to enforce this Agreement shall be brought in the [appropriate court for the proceeding].

4.2 In the event of an action alleging a breach of this Agreement, the prevailing party shall be entitled to reimbursement for its reasonable attorney's fees. Any attorney's fees awarded to the Guaranty Funds or the NCIGF shall be handled as an administrative expense in the proceeding, subject to [cite to applicable law]. Any attorney's fees awarded to the Commissioner or Receiver shall be paid from the Guaranty funds and NCIGF's funds, and shall not be submitted as a claim in the proceeding.

4.3 No failure or delay by any Party in exercising any right, power or privilege shall operate as a waiver thereof. Any exercise of a right, power or privilege shall not be considered to preclude any other or further exercise thereof.

4.4 There shall be no liability on the part of the Commissioner or Receiver or the Company(ies) to the Guaranty Funds or NCIGF relating to or arising from the Evaluation Material or any other documents, material, information or communications provided under this Agreement.

V. Warranties and Representations

5.1 The Commissioner, the Guaranty Funds, and the NCIGF to the extent consistent with their statutory and other obligations, shall in good faith cooperate and communicate promptly with each other with respect to the performance of their duties under this Agreement.

5.2 The Guaranty Funds and the NCIGF represent that they have the authority to enter into this Agreement and fulfill their obligations under this Agreement.

5.3 Each undersigned person represents that he or she is authorized to sign this Agreement on behalf of the Party he or she represents.

5.4 The Guaranty Funds and the NCIGF understand and acknowledge that the Commissioner or Receiver makes no representations or warranties as to the accuracy or completeness of any Evaluation Material provided under this Agreement.

5.5 The Guaranty Funds and NCIGF understand and acknowledge that the Evaluation Material may include information furnished by consultants, access to which will require additional agreements with such consultants.

VI. Termination

6.1 This Agreement may be terminated at any time by agreement among the Parties or by any single Party in writing with 30 days' notice, provided that all Evaluation Material obtained prior to such termination shall remain confidential, unless otherwise agreed by the Parties, and except as otherwise provided by law. Further, this Agreement shall be terminated upon a determination in writing by the Commissioner or the Receiver that the Company no longer presents a material risk of Liquidation.

6.2 The Guaranty Funds and the NCIGF are permitted to use Evaluation Material in the manner and for purposes described herein until delivery by the Receiver or Commissioner of a written notice specifying the date of termination of this Agreement. Upon a liquidation order wherein one or more Guaranty Funds are triggered this Agreement shall terminate in all respects without the obligation to destroy Evaluation material or maintain it as confidential.

6.3 Except as provided in Paragraph 6.2, in the event of a termination of this Agreement, the Guaranty Funds and NCIGF shall immediately undertake to destroy all Evaluation Materials, and all copies, summaries, analyses and notes of the contents or parts thereof, and shall provide an affidavit attesting to the destruction of all such Evaluation Materials being provided to the Receiver, if appointed, and the Commissioner within 30 days after termination, and no part thereof shall be retained by the Guaranty Funds or NCIGF in any form without the prior written consent of the Commissioner or Receiver.

VII. Miscellaneous Provisions

7.1 Nothing in this Agreement shall be deemed to create an attorney-client relationship between any Party's counsel and any other Party.

7.2 This Agreement shall be governed by and construed in accordance with the laws of the State of [state of domicile of the insolvency].

7.3 This Agreement may be executed in multiple counterparts, each of which shall be deemed an original for all purposes, and all of which together shall constitute one and the same instrument.

7.4 This Agreement shall be effective upon the date signed by each party and shall also apply to any and all Evaluation Material that has previously been shared between the Parties.

7.5 All communications under this Agreement shall be in writing and shall be sent by email to the addresses specified below. A copy of any such notice shall also be personally delivered or sent by either first class registered or certified U.S. Mail, return receipt requested, postage prepaid, or by a bonded mail delivery service, to the address set out below:

The Commissioner:
[name, address, phone, email address]

The Receiver:
[name, address, phone, email address]

Guaranty Funds:

[list of contact information for signatory funds]

7.6 The Parties agree to meet periodically, at least annually, to discuss issues arising under this Agreement and its implementation with respect to any specific Company.

[SIGNATURES OF PARTIES ON FOLLOWING PAGES]

IN WITNESS WHEREOF, the Parties have executed this Agreement on this ____ day of _____, 2019:

Commissioner

By: _____
Its: _____
Date: _____

Receiver (if appointed)
By: _____
Its: _____
Date: _____

NCIGF:

By: _____
Its: _____
Date: _____

Guaranty Fund:

Separate signature pages may be appropriate.