Independent Insurance Agents of Arkansas
2020 Cyber Rating Bands

Please complete pages 3-5 to bind.
Pages 6-17 contain proposal details.

Evolve MGA, 1752 Lincoln Avenue, San Rafael, CA 94901

5 Reasons Why **Insurance Agencies** Need Cyber Insurance

1

Wire Transfer Fraud "Social Engineering"

Modern day hackers are looking to trick CFO's, CEO's, and even an insurance agency's client into wiring money to fraudulent bank accounts. These attacks usually originate through phishing emails or stolen login credentials. What is the average amount of funds that pass through your agency?

2

Ransomware

Insurance agencies are heavily reliant on technology and client information to perform everyday duties. Ransomware is a malware intended to lock up an agency's data and hold it for ransom. As a result, an attack can cause high forensic costs to restore data and large amounts of lost revenue from business interruption.

3

Reputational Harm

An insurance agent's failure to protect their client's confidential information will not only lead to loss of current clients, it can lead to loss of future clients. A smart insurance agency has adequate reputational harm cover in the event of a security breach to reimburse for that loss of revenue.

4

Personal Funds Protection

Evolve's policy provides protection for the personal bank accounts of Senior Executive Officers in the event that money is wired out of their personal bank accounts while on the work network. Hackers are increasingly targeting businesses and stealing SEO's credentials, resulting in compromised bank accounts.

5

Management Liability

D&O insurance does not adequately contemplate coverage for a cyber triggered management liability claim. Evolve's cyber policy will protect Senior Executive Officers in the event a hacking attack has a lasting impact upon an insurance agency, leading to a cyber triggered management liability claim.

evolve

RATING BANDS: Valid 1/1/20 – 1/1/21

Limit Options: $0 - $5M in Revenue

Prior Year's Revenue	Fee	Deductible	Limit Option:	$250,000	$500,000	$1,000,000	$2,000,000	$3,000,000	$100,000 Crime AP	$250,000 Crime AP	Total Payables (with taxes and fees)
$0 - $500K	$150	$2,500		$650.00	$750.00	$1,000.00	$1,775.00	$2,550.00	$250.00	$350.00	Click Here
$500K - $1M	$150	$2,500			$800.00	$1,025.00	$1,850.00	$2,650.00	$250.00	$350.00	Click Here
$1M - $1.5M	$150	$2,500				$1,050.00	$1,925.00	$2,750.00	$250.00	$350.00	Click Here
$1.5M - $2M	$150	$2,500				$1,075.00	$2,000.00	$2,850.00	$250.00	$350.00	Click Here
$2M - $2.5M	$150	$2,500				$1,100.00	$2,075.00	$2,950.00	$250.00	$350.00	Click Here
$2.5M - $3M	$150	$2,500				$1,125.00	$2,150.00	$3,050.00	$250.00	$350.00	Click Here
$3M - $3.5M	$150	$2,500				$1,150.00	$2,225.00	$3,150.00	$250.00	$350.00	Click Here
$3.5M - $4M	$150	$2,500				$1,175.00	$2,300.00	$3,250.00	$250.00	$350.00	Click Here
$4M - $4.5M	$150	$2,500				$1,200.00	$2,375.00	$3,350.00	$250.00	$350.00	Click Here
$4.5M - $5M	$150	$2,500				$1,225.00	$2,450.00	$3,450.00	$250.00	$350.00	Click Here

1. **Terms subject to an additional $150 Service Fee, which is included in the Total Payable Figures**
2. **Premium subject to an additional 4.0% Arkansas Surplus Lines Tax, applied to the premium and fee, which is included in the Total Payable Figures**
3. Deductible applies to each and every claim, including costs and expenses
4. Base rates include coverage for Media Liability at Full Limits, unless otherwise noted

EVOLVE

Evolve MGA, 1752 Lincoln Avenue, San Rafael, CA 94901

CYBER INSURANCE APPLICATION FORM

This application form is for companies with revenues of less than $50m who are looking for cyber insurance limits of $5m or below.

LIMIT OPTIONS

Desired Limit off Rating Band: **Requested Effective Date:**

Cyber Crime Option: ☐ None ☐ $100K ☐ $250K

CONTACT & COMPANY DETAILS

Please complete the following details for the entire company or group (including all subsidiaries) that is applying for the insurance policy:

Contact Name: Position:

Email Address: Telephone Number:

Company Name: Last Year's Revenue: $

Website: Date Established: M M / D D / YYYY

Full Primary Address:

Primary Industry Sector & Description of Business Activities:

PREVIOUS CYBER INCIDENTS

Please tick all the boxes below that relate to any cyber incident that you have experienced in the last three years (there is no need to highlight events that were successfully blocked by security measures):

☐ Cyber Crime ☐ Cyber Extortion ☐ Data Loss ☐ Denial of Service Attack ☐ IP Infringement

☐ Malware Infection ☐ Privacy Breach ☐ Ransomware ☐ Other (please specify)

If you ticked any of the boxes above, did the incident(s) have a direct financial impact upon your business of more than $10,000? ☐ Yes ☐ No

If yes, please provide more information below, including details of the financial impact and measures taken to prevent the incident from occurring again:

IMPORTANT NOTICE

By signing this form you agree that the information provided is both accurate and complete and that you have made all reasonable attempts to ensure this is the case by asking the appropriate people within your business. Evolve MGA will use this information solely for the purposes of providing insurance services and may share your data with third parties in order to do this. We may also use anonymized elements of your data for the analysis of industry trends and to provide benchmarking data.

Contact Name: Position:

Signature: Date: M M / D D / YYYY

POLICYHOLDER DISCLOSURE NOTICE OF TERRORISM INSURANCE COVERAGE

You are hereby notified that under the Terrorism Risk Insurance Act of 2002, as amended ('TRIA'), that you now have a right to purchase insurance coverage for losses arising out of acts of terrorism, **as defined in Section 102(1) of the Act, as amended:** The term 'act of terrorism' means any act that is certified by the Secretary of the Treasury, in consultation with the Secretary of Homeland Security, and the Attorney General of the United States, to be an act of terrorism; to be a violent act or an act that is dangerous to human life, property, or infrastructure; to have resulted in damage within the United States, or outside the United States in the case of an air carrier or vessel or the premises of a United States mission; and to have been committed by an individual or individuals, as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States Government by coercion. Any coverage you purchase for 'acts of terrorism' shall expire at 12:00 midnight December 31, 2020, the date on which the TRIA Program is scheduled to terminate or the expiry date of the policy whichever occurs first, and shall not cover any losses or events which arise after the earlier of these dates.

YOU SHOULD KNOW THAT COVERAGE PROVIDED BY THIS POLICY FOR LOSSES CAUSED BY CERTIFIED ACTS OF TERRORISM IS PARTIALLY REIMBURSED BY THE UNITED STATES UNDER A FORMULA ESTABLISHED BY FEDERAL LAW. HOWEVER, YOUR POLICY MAY CONTAIN OTHER EXCLUSIONS WHICH MIGHT AFFECT YOUR COVERAGE, SUCH AS AN EXCLUSION FOR NUCLEAR EVENTS. UNDER THIS FORMULA, THE UNITED STATES PAYS 85% THROUGH 2015; 84% BEGINNING ON JANUARY 1, 2016; 83% BEGINNING ON JANUARY 1, 2017; 82% BEGINNING ON JANUARY 1, 2018; 81% BEGINNING ON JANUARY 1, 2019 AND 80% BEGINNING ON JANUARY 1, 2020; OF COVERED TERRORISM LOSSES EXCEEDING THE STATUTORILY ESTABLISHED DEDUCTIBLE PAID BY THE INSURER(S) PROVIDING THE COVERAGE. YOU SHOULD ALSO KNOW THAT THE TERRORISM RISK INSURANCE ACT, AS AMENDED, CONTAINS A $100 BILLION CAP THAT LIMITS U.S. GOVERNMENT REIMBURSEMENT AS WELL AS INSURERS' LIABILITY FOR LOSSES RESULTING FROM CERTIFIED ACTS OF TERRORISM WHEN THE AMOUNT OF SUCH LOSSES IN ANY ONE CALENDAR YEAR EXCEEDS $100 BILLION. IF THE AGGREGATE INSURED LOSSES FOR ALL INSURERS EXCEED $100 BILLION, YOUR COVERAGE MAY BE REDUCED.
THE PREMIUM CHARGED FOR THIS COVERAGE IS PROVIDED IN THE QUOATION ACCOMPANYING THIS NOTICE AND DOES NOT INCLUDE ANY CHARGES FOR THE PORTION OF LOSS COVERED BY THE FEDERAL GOVERNMENT UNDER THE ACT.

	I hereby elect to purchase coverage for acts of terrorism for the prospective additional premium stated in the quotation provided to me.
	I hereby elect to have coverage for acts of terrorism excluded from my policy. I understand that I will have no coverage for losses arising from acts of terrorism.

Policyholder/Applicant's Signature

Print Name

Date

LMA9104
12 January 2015

For Evolve, TRIA is included at no additional premium - please still elect if you would like to have this coverage included in your policy.

EVOLVE

Date of Issue: TBD

DISCLOSURE TO SURPLUS LINE INSURED

FORM SL-3

THE UNDERSIGNED ACKNOWLEDGES THAT HE/SHE HAS BEEN INFORMED THAT THE INSURANCE RISK FOR WHICH HE/SHE DESIRES COVERAGE HAS BEEN PLACED PURSUANT TO THE SURPLUS LINE INSURANCE LAW; AND THAT HE/SHE UNDERSTANDS THAT THE INSURANCE COMPANY'S RATES AND FORMS ARE NOT SUBJECT TO REVIEW BY THE ARKANSAS INSURANCE DEPARTMENT; THAT THE PROTECTION OF THE ARKANSAS PROPERTY AND CASUALTY GUARANTY ACT DOES NOT APPLY TO THE POLICY WRITTEN PURSUANT TO THE SURPLUS LINE INSURANCE LAW; AND THAT A TAX OF 4% IS REQUIRED BY LAW TO BE COLLECTED ON ALL SURPLUS LINE INSURANCE PREMIUMS.

_____ _____

DATE SIGNATURE OF INSURED

_____

FIRM REPRESENTED, IF APPLICABLE

_____

Address

_____

_____

Telephone Number

_____

Email Address

(REV. 4/06)

LIMITS OF LIABILITY AND DEDUCTIBLES

Insuring Clauses 1 – 3 are Subject to an Each and Every Claim Limit:		
Insuring Clause 1: Cyber Incident Response (Separate Tower - Mirrors Policy Limit)		
Section A: Incident Response Costs	Full Limits, ($0 Deductible – *applies to this Section only*)	
Section B: Legal and Regulatory Costs	Full Limits	
Section C: IT Security and Forensic Costs	Full Limits	
Section D: Crisis Communication Costs	Full Limits	
Section E: Privacy Breach Management Costs	Full Limits	
Section F: Third Party Privacy Breach Management Costs	Full Limits	
Section G: Post Breach Remediation Costs	$50,000 subject to a maximum of 10% of all sums **we** have paid as a direct result of the **cyber event** ($0 Deductible – *applies to this Section only*)	
Insuring Clause 2: Cyber Crime		
Section A: Funds Transfer Fraud (Social Engineering)	$100,000	$250,000
Section B: Theft of Funds Held In Escrow	$100,000	$250,000
Section C: Theft of Personal Funds	$100,000	$250,000
Section D: Extortion	Full Limits	
Section E: Corporate Identity Theft	$100,000	$250,000
Section F: Telephone Hacking	$100,000	$250,000
Section G: Push Payment Fraud	$50,000	
Section H: Unauthorized Use of Computer Resources	$100,000	$250,000
Insuring Clause 3: System Damage and Business Interruption		
Section A: System Damage and Rectification Costs	Full Limits	
Section B: Income Loss and Extra Expense	Full Limits, sub-limited to $1,000,000 in respect of **system failure**	
Section C: Additional Extra Expense	Sub-limited to 10% of the Overall Limit, Maximum Sub-limit of $100,000	
Section D: Dependent Business Interruption	Full Limits, sub-limited to $1,000,000 in respect of **system failure**	
Section E: Consequential Reputational Harm	Full Limits	
Section F: Claim Preparation Costs	$25,000, ($0 Deductible – *applies to Section F only*)	
Section G: Hardware Replacement Costs	Full Limits	

Insuring Clauses 4 – 7 are Subject to an Aggregate Limit:	
Insuring Clause 4: Network Security & Privacy Liability	
Section A: Network Security Liability	Full Limits, including **costs and expenses**
Section B: Privacy Liability	Full Limits, including **costs and expenses**
Section C: Management Liability	Full Limits, including **costs and expenses**
Section D: Regulatory Fines	Full Limits, including **costs and expenses**
Section E: PCI Fines, Penalties and Assessments	Full Limits, including **costs and expenses**
Insuring Clause 5: Media Liability	
Section A: Defamation	Full Limits, including **costs and expenses**
Section B: Intellectual Property Rights Infringement	Full Limits, including **costs and expenses**
Insuring Clause 6: Technology Errors and Omissions	
Technology Errors and Omissions	No Cover Provided
Insuring Clause 7: Court Attendance Costs	
Court Attendance Costs	$100,000 Limit, in the aggregate ($0 Deductible – *applies to this Section only*)

The chosen policy limit and retention shown on Page 1 apply to the Insuring Clauses and respective sections unless otherwise indicated.

CAVEMAN SPECIAL AMENDATORY CLAUSE

Attaching to Policy #:
The Insured:
With Effect From:

HOW MUCH WE WILL PAY

It is understood and agreed that the following amendments are made to the Declarations page:

1. The time period shown as the "WAITING PERIOD" in the Declarations page is deleted in its entirety and replaced with the following:

   6 hours

2. The following **INSURING CLAUSE** is added:

   CRIMINAL REWARD COVERAGE

Aggregate limit of liability:	USD50,000	in the aggregate
Deductible:	USD2,500	each and every claim

3. The following **SECTION** is added to **INSURING CLAUSE 4** in the Declarations page:

   SECTION F: CONTINGENT BODILY INJURY

Aggregate limit of liability:	USD250,000	in the aggregate, including **costs and expenses**
Deductible:	USD2,500	each and every claim, including **costs and expenses**

It is further understood and agreed that the following amendments are made to the Policy:

1. The following **INSURING CLAUSE** is added:

   INSURING CLAUSE: CRIMINAL REWARD COVERAGE

   We agree to reimburse **you** any reasonable sums necessarily incurred with **our** prior written agreement to pay any person or organization, other than:

   a. any external or internal auditor of the **company**; or

   b. any individual or organization who manages or supervises the individuals stated in a. above;

   for information not otherwise available which directly results in the arrest and conviction of any person or organization who is committing or has committed any illegal act directly relating to a claim covered under **INSURING CLAUSES 1**, **2**, **3** or **4**.

2. The following **SECTION** is added to **INSURING CLAUSE 4**:

   SECTION F: CONTINGENT BODILY INJURY

   We agree to pay on **your** behalf all sums which **you** become legally obliged to pay (including liability for claimant's costs and expenses) as a result of any **claim** arising out of **bodily injury** caused as a direct result of a **cyber event** affecting **your computer systems** first discovered by **you** during the **period of the policy**.

We will also pay **costs and expenses** on **your** behalf.

However, **we** will not make any payment under this Section for which the **you** are entitled to indemnity under any other insurance, except for any additional sum which is payable over and above the other insurance.

3. Part a. of **INSURING CLAUSE 3** (**SECTON A**) is deleted in its entirety and replaced with the following:

   a. **third party** contract staff or overtime costs for **employees** to rebuild **your** data, including the cost of data re-entry or data re-creation;

4. The following **DEFINITION** is added:

   "Bodily injury" means
   death, bodily injury, mental injury, illness or disease.

5. The "Bodily injury and property damage" **EXCLUSION** is deleted in its entirety and replaced with the following:

   arising directly or indirectly out of:

   a. **bodily injury**; or

   b. tangible property damage.

   However, part a. of this Exclusion will not apply to:

   a. **INSURING CLAUSES 4** (**SECTIONS A**, **B** and **C** only) and **5** for any **claim** as a direct result of mental injury or emotional distress; and

   b. **INSURING CLAUSE 4** (**SECTION F** only).

6. Where "10%" is stated in the "Associated companies" **EXCLUSION** it is deleted in its entirety and replaced with "15%".

7. Where "60 days" is stated in the "Extended reporting period" **CONDITION** it is deleted in its entirety and replaced with "90 days".

8. Where "20%" is stated in the "Mergers and acquisitions" **CONDITION** it is deleted in its entirety and replaced with "25%".

SUBJECT OTHERWISE TO THE TERMS AND CONDITIONS OF THE POLICY

EVO 4.0 Coverage Cheat Sheet

Insuring Clause 1: Cyber Incident Response (1st Party)

Mirrors Policy Limit, Unlimited Re-instatement

Section A: Incident Response Costs — **USD 1,000,000** *each and every claim*

Free, 24/7 access to a technically trained cyber incident manager ($0 deductible) for advice on how to quickly stop a claim.

Section B: Legal and Regulatory Costs — **USD 1,000,000** *each and every claim*

Payment of the hourly billables of a specialist data breach attorney needed to legally navigate federal, state, and private privacy regulations (including notification costs).

Section C: IT Security and Forensic Costs — **USD 1,000,000** *each and every claim*

Payment of the hourly billables of a specialist computer forensic expert needed to stop and contain an attack.

Section D: Crisis Communications Costs — **USD 1,000,000** *each and every claim*

Payment of the hourly billables of a specialist data breach public relations firm needed to reduce damage to your brand and mitigate the loss of customers.

Section E: Privacy Breach Management Costs — **USD 1,000,000** *each and every claim*

Payment of the additional costs to comply with privacy regulations, including credit monitoring and identity restoration.

Section F: Third Party Privacy Breach Management Costs — **USD 1,000,000** *each and every claim*

Payment of 3rd party additional costs to comply with privacy regulations, including credit monitoring and identity restoration required by contract.

Section G: Post Breach Remediation Costs — **USD 50,000** *each and every claim*

Payment of the costs to comply with HIPAA security risk assessments ($0 deductible, betterment).

Insuring Clause 2: Cyber Crime (1st Party)

Unlimited Re-instatement

Section A: Funds Transfer Fraud *(insured's bank account)* — **USD 250,000** *each and every claim*

Reimbursement of unauthorized electronic funds transfer from a social engineering attack, including the voluntary departure of funds.

Section B: Theft of Funds Held in Escrow *(customers' money in transit)* — **USD 250,000** *each and every claim*

Reimbursement for electronic theft of 3rd party funds temporarily held in your bank account.

Section C: Theft of Personal Funds *(SEO bank accounts)* — **USD 250,000** *each and every claim*

Reimbursement to a senior executive officer for a personal financial loss (or identity theft costs) when the company's network security is compromised.

Section D: Extortion — **USD 1,000,000** *each and every claim*

Reimbursement for any ransom paid (usually cryptocurrency) after a ransomware attack.

Section E: Corporate Identity Theft — **USD 250,000** *each and every claim*

Reimbursement to the Insured for their financial loss due to a fraudulent third party impersonating the business' electronic identity.

Section F: Telephone Hacking — **USD 250,000** *each and every claim*

Reimbursement of the increased phone bill costs resulting from unauthorized calls or misused bandwidth.

Section G: Push Payment Fraud *(3rd party bank accounts)* — **USD 50,000** *each and every claim*

Reimbursement of the cost to indemnify existing customers that experience a financial loss caused by fraudulent electronic communication.

Section H: Unauthorized Use of Computer Resources — **USD 250,000** *each and every claim*

Reimbursement of the additional costs associated with a fraudulent third party using your business' computer systems for cryptojacking (bitcoin mining) or botnetting (the use of your computer to launch an attack on a 3rd party).

Insuring Clause 3: System Damage and Business Interruption (1st Party)

Unlimited Re-instatement

Section A: System Damage and Rectification Costs — **USD 1,000,000** *each and every claim*

Reimbursement of the hourly billables of current employees' overtime costs or specialist consultants to rebuild your computer systems and data including the cost of re-creating data from scratch.

Section B: Income Loss and Extra Expense — **USD 1,000,000** *each and every claim*
USD 1,000,000 is the maximum limit for system failure

Reimbursement of lost income during a computer system outage (lasting longer than 8 hours) as a direct result of a hack attack or system failure.

Section C: Additional Extra Expense — **USD 100,000** *each and every claim*

Reimbursement for operating costs in addition to normal operating expenses to source products and services from alternative sources to meet contractual obligations after a hack attack or system failure.

Section D: Dependent Business Interruption — **USD 1,000,000** *each and every claim*
USD 1,000,000 is the maximum limit for system failure

Reimbursement of lost income after a 3rd party technology provider or supply chain partner (via endorsement) resulting from a hack attack or system failure.

Section E: Consequential Reputational Harm — **USD 1,000,000** *each and every claim*

Reimbursement of lost income after the loss of current or future customers post hack attack.

Section F: Claim Preparation Costs — **USD 25,000** *each and every claim*

Payment of the hourly billables of a forensic accountant needed to assess lost income ($0 deductible).

Section G: Hardware Replacement Costs — **USD 1,000,000** *each and every claim*

Payment of the cost of replacing damaged computer hardware or tangible equipment post hack attack (must be more cost efficient than fixing damaged software).

Insuring Clause 4: Network Security & Privacy Liability (3rd Party)

Policy Aggregate Limit

Section A: Network Security Liability — **USD 1,000,000** *in the aggregate, including costs and expenses*

Payment for the defense and settlement of a lawsuit resulting from transmission of malware to a 3rd party's computer systems.

Section B: Privacy Liability — **USD 1,000,000** *in the aggregate, including costs and expenses*

Payment for the defense and settlement of a lawsuit resulting from a breach of sensitive information entrusted to you (PII, PHI, credit card info, confidential corporate info, etc.).

Section C: Management Liability — **USD 1,000,000** *in the aggregate, including costs and expenses*

Payment for the defense and settlement of a lawsuit made against a Senior Executive Officer (Director or Officer) as a result of a hack attack.

Section D: Regulatory Fines — **USD 1,000,000** *in the aggregate, including costs and expenses*

Payment of any fines and penalties resulting from a regulatory investigation (any government or professional body) post hack attack."

Section E: PCI Fines, Penalties and Assessments — **USD 1,000,000** *in the aggregate, including costs and expenses*

Payment of fines, penalties, and/or PCI assessments (card re-issuance & 100% of the fraud) requested by your acquiring bank or payment processor post credit card breach.

Insuring Clause 5: Media Liability (3rd Party)

Policy Aggregate Limit

Section A: Defamation — **USD 1,000,000** *in the aggregate, including costs and expenses*

Payment for the defense and settlement of a lawsuit claiming defamation or emotional distress arising out of your businesses' media content.

Section B: Intellectual Property Rights Infringement — **USD 1,000,000** *in the aggregate, including costs and expenses*

Payment for the defense and settlement of a lawsuit claiming an infringement of intellectual property or misappropriation of content arising out of your businesses' media content.

Insuring Clause 6: Technology E&O (3rd Party)

Policy Aggregate Limit **USD 1,000,000** *in the aggregate, including costs and expenses*

Payment for the defense and settlement of a lawsuit resulting from any act, error, or omission in the provision of your businesses' technology services.

Insuring Clause 7: Court Attendance Costs (3rd Party)

Policy Aggregate Limit **USD 100,000** *in the aggregate*

Reimbursement of the costs to attend court in connection with a claim covered under this policy. ($0 deductible).

How much could a data breach cost me?

click here

What can I do to help prevent a cyber attack?

click here

What are the most common cyber claims?

click here

EVOLVE

5 FREE $5,000 VALUE Risk Management Services

Evolve has teamed up with specialist security experts to help strengthen, improve, and protect your organization. Each Evolve policyholder has the benefit of using the following services at no additional cost:

BITSIGHT

VULNERABILITY ASSESSMENT

Bitsight's full report provides the technical insight to strengthen any organization's security. Your IT department can look to improve areas where there are low scores.

NINJIO

SECURITY AWARENESS VIDEO TRAINING

4 minute "gamified" video episodes on real breaches that train your employees on how to avoid falling victim to hack attacks. Insured receives service for free for up to 25 employees.

INTENTIONAL PHISHING

PHISHING OUT CYBER THREATS

This phishing tool will intentionally try to trick your employees to "click" on suspicious links. Once clicked, the employee will be prompted through an online e-training course to prevent a future attack.

INCIDENT RESPONSE PLAN BUILDER

BUILD A STRONG INCIDENT RESPONSE PLAN

Do you have a cyber breach incident response plan in place? If not, our incident response experts will help you build a robust plan that can effectively reduce the impact of a cyber event.

SKURIO

I-SPY YOUR INFORMATION

The Skurio breach monitoring service continually searches the dark web for information specific to your organization and alerts you in real time to possible breaches of your data. This proactive approach helps you minimize the fallout from a variety of cyber incidents.

For access, please email:

RISKMANAGEMENT@EVOLVEMGA.COM

CLAIMS EXAMPLES

"There are two types of companies: those who have been hacked and those that will be."

Robert Mueller, FBI Director 2012

The CFO of an insurance brokerage in Virginia discovered that a fraudulent third party had compromised his computer and was attempting to wire money out of the brokerage's bank account. Upon forensic review, it was determined that the hacker had gained access to confidential information such as social security numbers and sensitive financial information.

In late 2017, a mid-sized insurance agency found that malicious links were being sent internally as well as to their clients from their Human Resources department. It was discovered that one of their employee's Office 365 accounts had been compromised and the malicious emails had been sent to everyone on their contact list. The employee immediately changed their O365 credentials. However, forensics was still needed to determine how the perpetrator had accessed the system and whether PII had been stolen or compromised.

A small insurance agency in Northern California experienced a ransomware attack while there office was closed for the weekend. While the malware initially accessed their systems on Friday, it didn't lock them down until the weekend. The agency's IT department identified the ransomware attack on Sunday. The agency decided not to pay the ransom and immediately began work on removing the malware. Upon removal, roughly 30% of data was still corrupted and a few computers were not usable. The insured accrued about $50,000 in costs for recovery of data and computer restoration.

An insurance agency received an email from a wholesale broker asking them to forward payment for a policy that recently bound. The employee who received the email overlooked that this was a fraudulent request and was being transferred into an account that the agency had never remitted payment to. Upon completion of the transfer, the agency quickly learned they were victim of a social engineering / funds transfer fraud scam and had transferred $42,000 to an unintended recipient.

The CFO of an insurance brokerage in California received their phone bill and was surprised to see it priced at $18,000 for the month, whereas their bill is normally well under $1,000. The agency quickly learned they were included in a widespread telephone hacking scheme that affected numerous businesses. Hackers set up a phone number where if called, the caller would be charged $3 per minute. Hackers then tapped into the broker's VOIP (voice over internet protocol) phone system and racked up a massive phone bill over the course of a few weeks.

COST ANALYSIS

What does it cost your business when 100,000 records are breached?

S AN FRANCISCO | LONDON | LOS ANGELES

750 BATTERY STREET, 7TH FLOOR, SAN FRANCISCO, CA 94111
415.257.2170
PATRICK@EVOLVEMGA.COM
WWW.EVOLVEMGA.COM