



# evolve

## Cyber Security Insurance Specialists



Teague  
INSURANCE



# AGENDA:

- Current Cyber Landscape
- Common Misconceptions about Cyber Exposures
- Ransomware Trends of 2023
- Social Engineering & Theft of Funds
- Obligations as a Data Owner
- How can a Business Stay Secure
- Q&A



# WHAT IS EVOLVE MGA?

## Advisen's Cyber MGA of the Year 2020, 2021, & 2022

- Cyber Specialist MGA
  - Standalone Cyber Policies
- Educational Resources (Free Dark Web Scanner, Industry-Specific Whitepapers, Claims Examples, Breach Calculators)
- Broadest Cyber Coverages
- Largest In-House Cyber Claims team (20+ years experience)
- Suite of Free Risk Management Tools available to Policyholders
- **Business Name, Revenue, Website = Dark Web Scan & Pricing**



**Proudly featured in:**



THE WALL STREET JOURNAL



Rough Notes





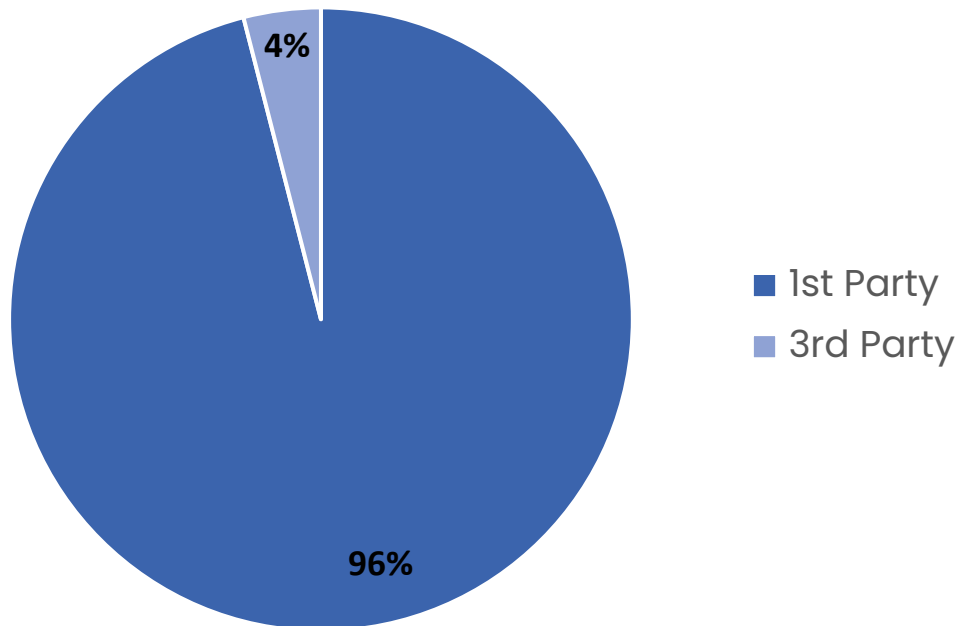
A person wearing a blue hoodie is holding a laptop. The background is a dark blue gradient with vertical columns of white binary code (0s and 1s) floating around. The entire image has a semi-transparent blue overlay.

# STATE OF THE CYBER MARKET

# SO... WHAT IS CYBER INSURANCE?

Protects your intangible assets (data & bank accounts).

## Evolve Claims Payout



## 2022 Evolve Data:

- Process 150+ cyber claims a month
- 60% of claims are Ransomware
- 21% of claims are Social Engineering / theft of funds
- Average cost of Ransomware incident: \$260,000





# WE ARE LIVING IN A DIFFERENT ERA

Average ransom payment in  
Q1 2023?

**\$327,883**

What was the total  
estimated losses in 2022?

ROUGHLY  
**\$10.3 Billion**

What was the total estimated  
loss on (BEC) attacks in 2022?

OVER  
**\$2.7 Billion**

In Q1 2023 companies with less than 1000  
employees experienced:

**Roughly 72.5% of Attacks**



# COMMON CYBER MISCONCEPTIONS

Only tech companies need cyber insurance...

Hackers wouldn't go after a small company like me...

I outsource everything and don't hold any data on my system...

I don't collect sensitive data...

My IT provider takes care of that...



# WHY DO BUSINESSES GET HACKED?

Every industry...

**#1 Cause of  
Cyber Attacks  
is Human  
Error**



**Collects sensitive data**

**Relies on technology**

**Performs financial transactions**

**Has a human workforce**





# RANSOMWARE

1. Phishing Links
2. Vulnerable Software
3. RDP Open Ports



# TARGETS OF RANSOMWARE

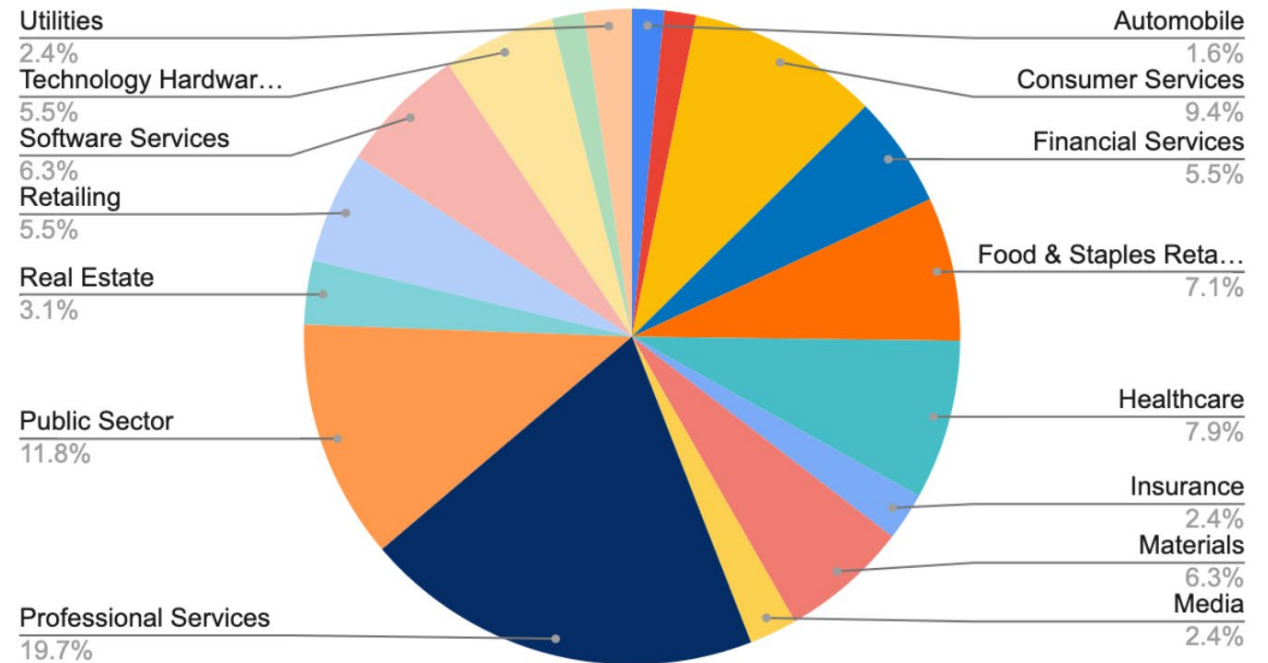
## **By Industry:**

- Public Sector: 12.9%
- Software Services: 12.1%
- Healthcare: 11.3%

## **By Company Size:**

- 1 to 10 Employees: 3.2%
- 11 to 100 Employees: 29%
- 101 to 1,000 Employees: 40.3%

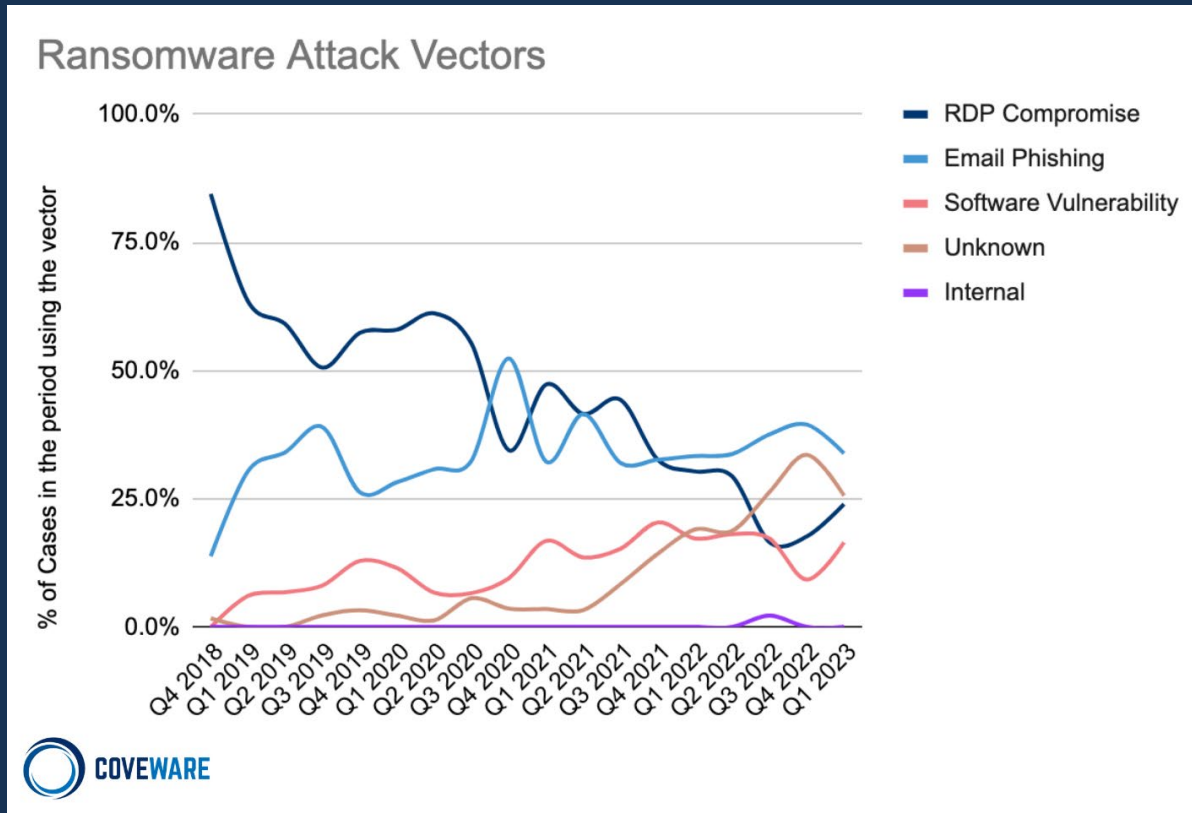
Industries Impacted by Ransomware Q1 2023



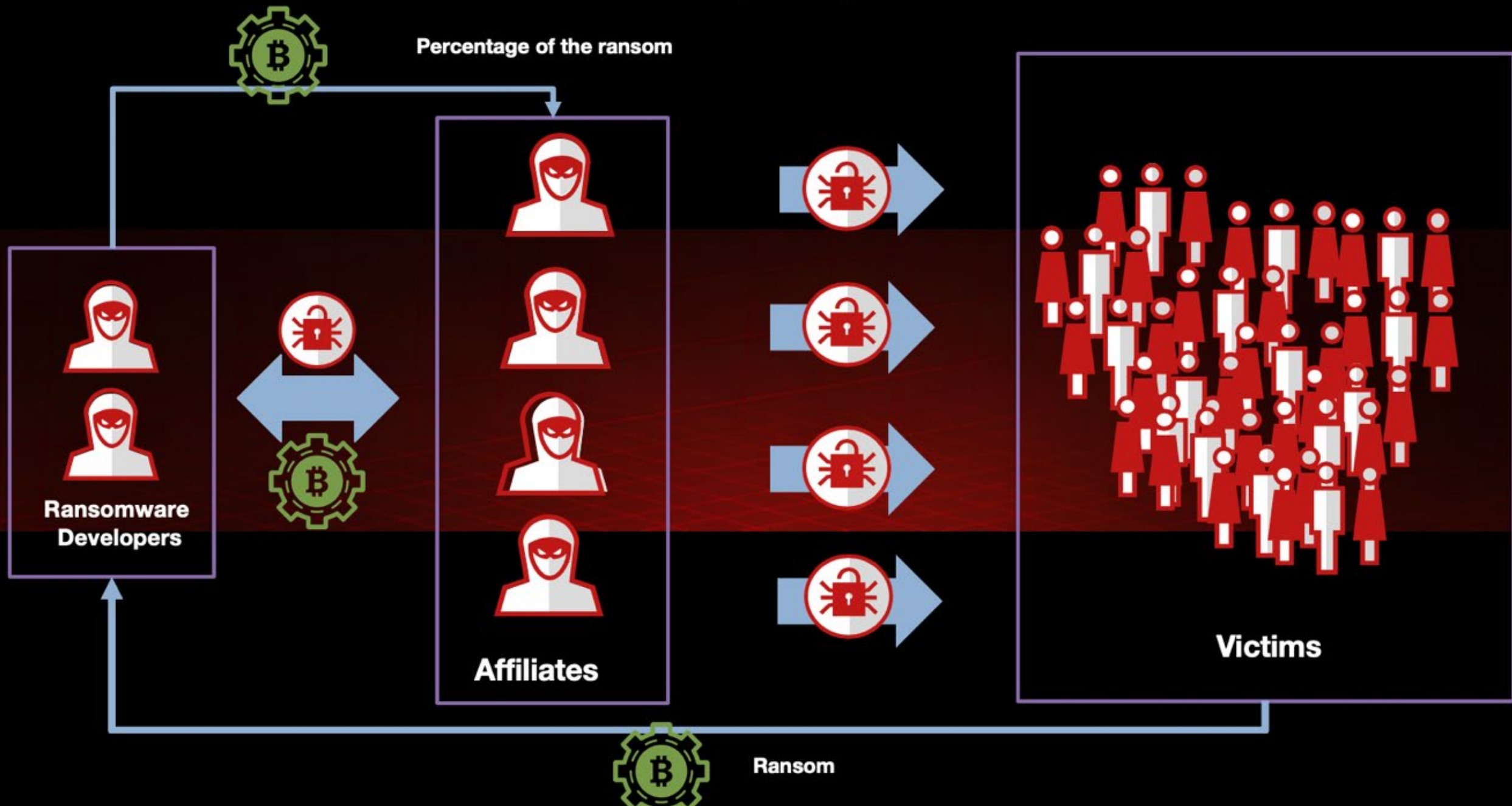
# RANSOMWARE ATTACK VECTORS IN Q1 2023

## Coveware Q1 2023 Report

- Average ransom payment in Q1 2023 was \$327,883
- 86% of ransomware attacks involved the threat to leak exfiltrated data
- Average days of downtime: 25 days
- BlackCat Ransomware variant made up 12.6% of market share



# Gandcrab : Ransomware-as-a-Service (RaaS) Model





# THE DARK WEB

**TOR: developed by  
US Navy for  
anonymous  
communications**

**Online market-  
place / beginning  
and end point for  
hackers**




We wish everyone a Happy Christmas and a Happy New year.

Welcome, highway.

Protect your account using 2FA.

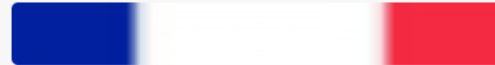
### Featured Stores




 **WVANORANJE'S HIGH QUALITY SHOP**  
Random Offers



 **Hilfiger**



 **Projeccao propose**



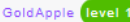
 **TheDutchPastor**



Escrow

4.99 USD

**Kentucky Electricity Bill PSD Template**

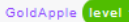
ItemId#627 -  




Escrow

29.99 USD

**EU ID PSD Template Pack (4 Templates)**

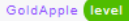
ItemId#831 -  




Escrow

9.99 USD

**1 Million Australia Emails Leads**

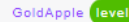
ItemId#1238 -  




Escrow

9.99 USD

**0,76 Million Switzerland Emails Leads**

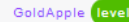
ItemId#1239 -  




Escrow

4.99 USD

**Eon Gas Utility Statement PSD Template**

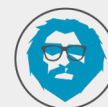
ItemId#1274 -  


# Online Marketplace

# THE COST OF RANSOMWARE

## The Most Common Costs Post Hack Attack:

Ransomware	Cryptocurrency Extortion Demand by Hacker
Funds Transfer Fraud	Average Transaction Size
Forensic Experts	<b>\$500 per Hour</b> <i>(involved on every claim)</i>
Data Breach Attorney	\$500 per Hour
Business Interruption	% of Profit Lost due to Downtime
Dependent Business Interruption	% of Profit Lost due to 3rd Party Provider Downtime
Data / System Reconstruction	\$500 per Hour
Reputational Harm	% of Profit Lost due to Lost Clients
Notification Costs	\$3 per Affected Individual
Fraudulent Theft of Personal Funds	SEO Personal Banking Financial Fraud Loss
Hardware Replacement Costs	Replacement Cost of Computer Hardware
Regulatory Investigation or Fines	Varies Across Federal, State, & Private Bodies
3rd Party Privacy or Network Security Lawsuit	\$500 per Hour (Defense Costs)



# FUNDS TRANSFER FRAUD

## **“Sending Money to the Wrong Place”**

- Senior Executive Officers
- Employees
- Clients
- Vendors

**#1 Cause = Human Error**





# THE COST OF FUNDS TRANSFER FRAUD

## 1. Incident Response

## 2. Funds Loss

*Bank Account #1: The Insured's*

*Bank Account #2: The C-Suite's*

*Bank Account #3: The Client's*

## 3. Reputational Harm

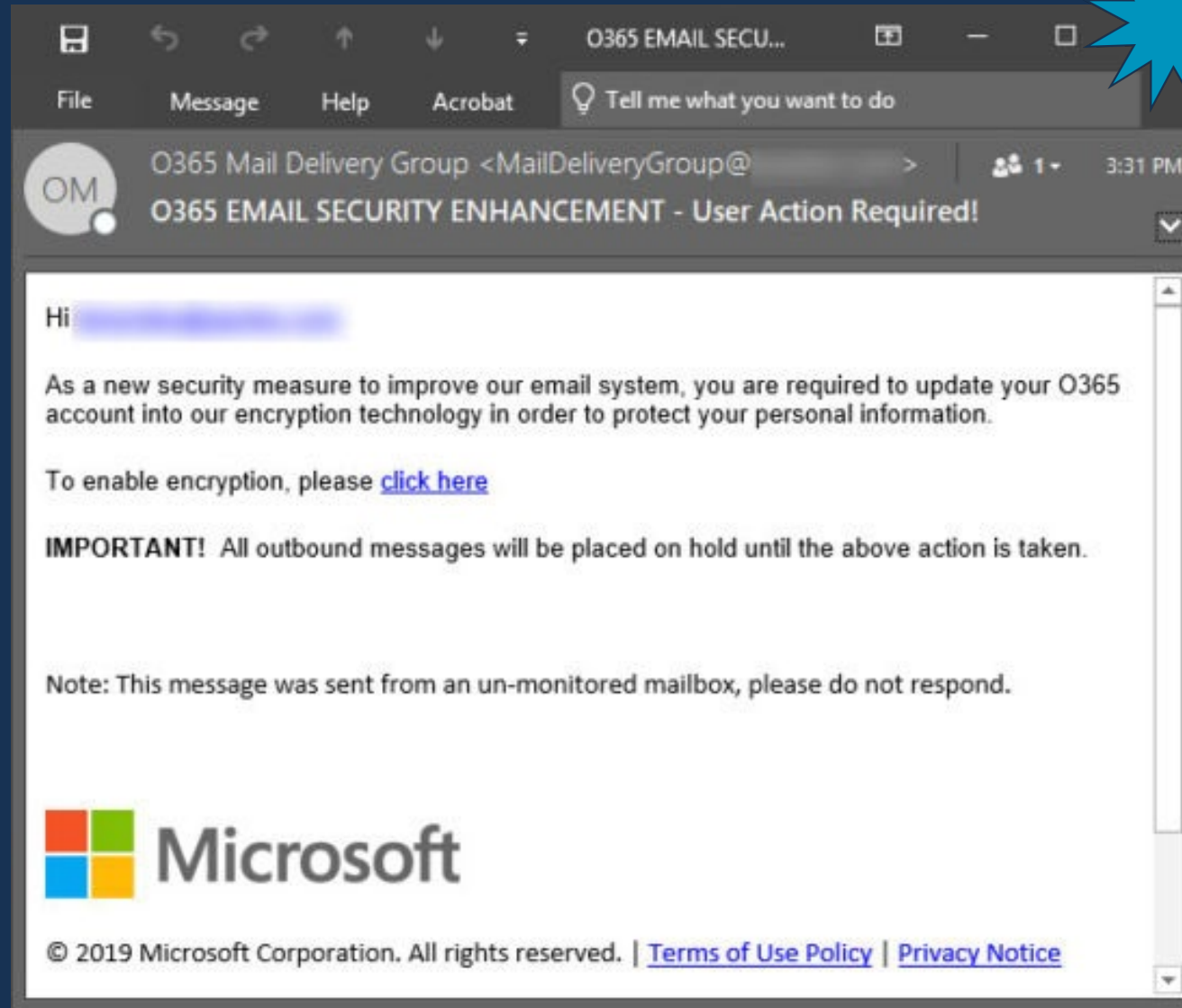
### How to Assess Exposure:

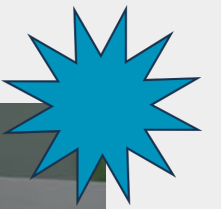
- Average ACH / Wire Transfer?
- Largest Transfer in 12 Months?

\*Base sub-limits start at \$250k



# PHISHING ATTEMPT





## Sign in

Sign in with your Microsoft account to join the family group.

Email, phone, or Skype

No account? [Create one!](#)

[Sign in with Windows Hello or a security key](#) ?

Next



Sign-in options



# HOW HACKERS GET YOU USING SOCIAL ENGINEERING





# DATA BREACHES

Common Causes – Actual or Suspected:

1. Electronic Attack
2. Accidental Disclosure
3. Physical Theft
4. Paper Breach
5. Deliberate Actions of a Rogue Employee



# OBLIGATIONS AS A DATA OWNER

If sensitive information that you are responsible for is lost or stolen, you will most likely **have to notify affected individuals** of the breach and provide credit monitoring services.

When it comes to PII, there are a number of **rules and regulations** about how you collect, use and store that information. If you do not adhere to them, you could face regulatory fines and penalties.

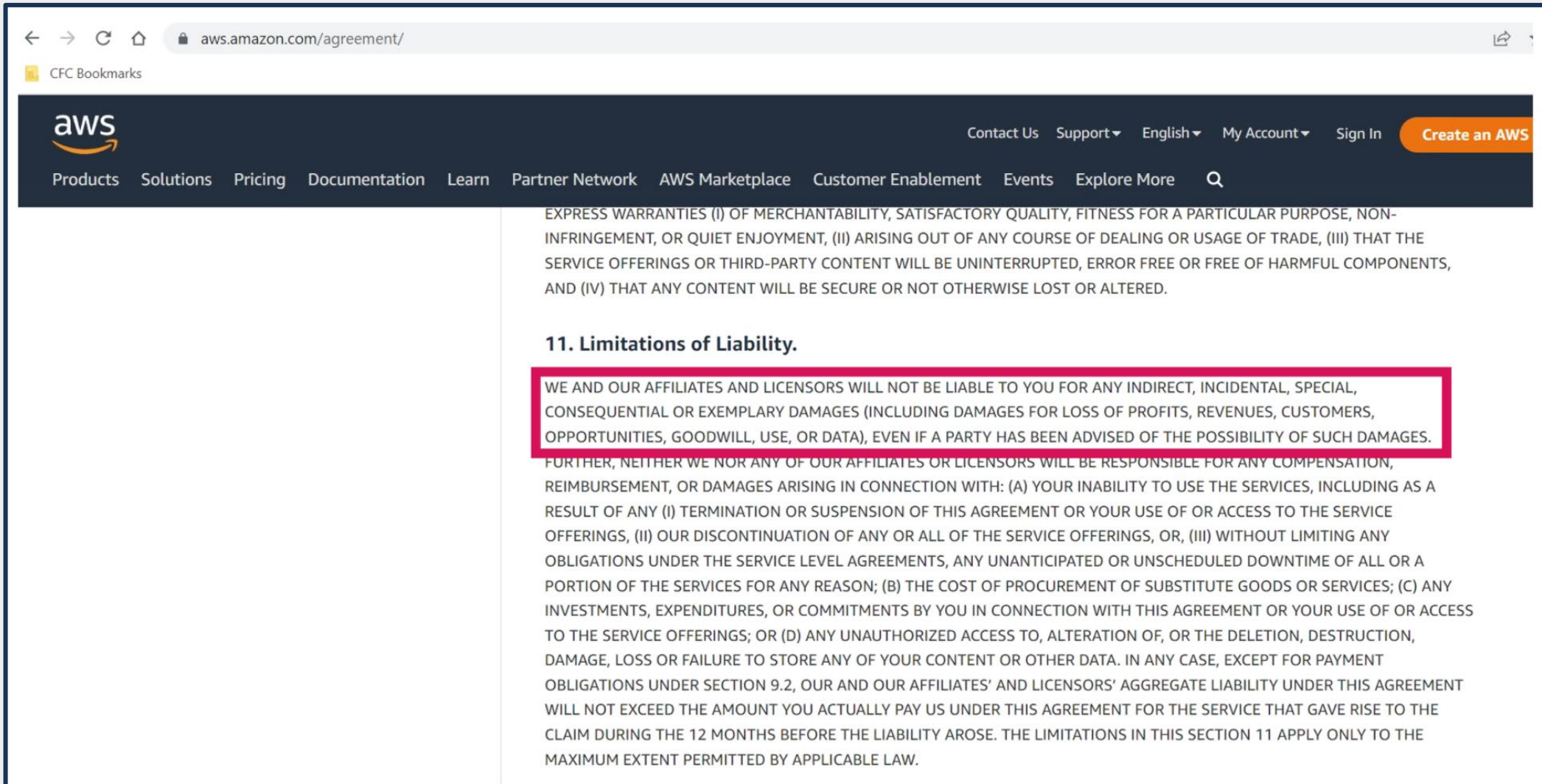
A malicious third party isn't always to blame. Often times, it's as simple as an employee **losing a company laptop**.

If you outsource your data storage to a third party and that third party is breached, you will still likely be **responsible for notifying affected individuals** and dealing with subsequent regulatory actions.

**Cyber insurance covers the range of costs associated with data breaches**, like notifying affected individuals and your responsibilities under different regulations.



# AWS STANDARD CONTRACT LANGUAGE



The screenshot shows the AWS Standard Contract Language page. The browser address bar displays 'aws.amazon.com/agreement/'. The AWS logo is in the top left, and navigation links like 'Contact Us', 'Support', 'English', 'My Account', 'Sign In', and 'Create an AWS' are in the top right. A search bar is also present. The main content area is divided into two columns. The left column contains a list of links: Products, Solutions, Pricing, Documentation, Learn, Partner Network, AWS Marketplace, Customer Enablement, Events, and Explore More. The right column contains the contract text. A pink box highlights the following text: 'WE AND OUR AFFILIATES AND LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, REVENUES, CUSTOMERS, OPPORTUNITIES, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.'

EXPRESS WARRANTIES (I) OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, (II) ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE, (III) THAT THE SERVICE OFFERINGS OR THIRD-PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, AND (IV) THAT ANY CONTENT WILL BE SECURE OR NOT OTHERWISE LOST OR ALTERED.

## 11. Limitations of Liability.

WE AND OUR AFFILIATES AND LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, REVENUES, CUSTOMERS, OPPORTUNITIES, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

FURTHER, NEITHER WE NOR ANY OF OUR AFFILIATES OR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE THE SERVICES, INCLUDING AS A RESULT OF ANY (I) TERMINATION OR SUSPENSION OF THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS, (II) OUR DISCONTINUATION OF ANY OR ALL OF THE SERVICE OFFERINGS, OR, (III) WITHOUT LIMITING ANY OBLIGATIONS UNDER THE SERVICE LEVEL AGREEMENTS, ANY UNANTICIPATED OR UNSCHEDULED DOWNTIME OF ALL OR A PORTION OF THE SERVICES FOR ANY REASON; (B) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; (C) ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY YOU IN CONNECTION WITH THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS; OR (D) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR CONTENT OR OTHER DATA. IN ANY CASE, EXCEPT FOR PAYMENT OBLIGATIONS UNDER SECTION 9.2, OUR AND OUR AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY UNDER THIS AGREEMENT WILL NOT EXCEED THE AMOUNT YOU ACTUALLY PAY US UNDER THIS AGREEMENT FOR THE SERVICE THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS BEFORE THE LIABILITY AROSE. THE LIMITATIONS IN THIS SECTION 11 APPLY ONLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.



# (PCI) PAYMENT CARD INFORMATION EXPOSURES

## PCI Fines, Penalties & Assessments

1. Card Reissuance: **\$3 - \$10**
2. Fraud: **Subject to 100%**
3. PCI Fine/Penalty: **\$5,000 - \$500,000**

## Additional Costs

- Card payments are immediately halted
- PCI forensic analyst assesses breach
- Legal advice
- Reputation damaged – loss of current + future customers
- Public relations firm hired
- Class action from breached customers

PCI Data Security  
Standard Board



VISA



# Cost of Losing 5,000 & 15,000 Records

How many records were exposed?

What type of data was exposed?

Is this the organization's first breach?  
☒ Yes ☐ No

Was the data stored in a centralized system/location?  
☒ Yes ☐ No

Is fraud expected?  
☒ Yes ☐ No

Is a class action lawsuit expected?  
☐ Yes ☒ No

Does your organization currently have data breach coverage?  
☒ Yes ☐ No

**CALCULATE**

\$160,000

INCIDENT INVESTIGATION

\$44,125

CUSTOMER NOTIFICATION / CRISIS MANAGEMENT

\$107,900

REGULATORY FINES & PENALTIES

\$0

PCI

\$0

CLASS ACTION LAWSUIT

\$312,025

TOTAL COST

\$62

PER RECORD COST



evolve

How many records were exposed?

What type of data was exposed?

Is this the organization's first breach?  
☒ Yes ☐ No

Was the data stored in a centralized system/location?  
☒ Yes ☐ No

Is fraud expected?  
☒ Yes ☐ No

Is a class action lawsuit expected?  
☐ Yes ☒ No

Does your organization currently have data breach coverage?  
☒ Yes ☐ No

**CALCULATE**

\$164,000

INCIDENT INVESTIGATION

\$92,375

CUSTOMER NOTIFICATION / CRISIS MANAGEMENT

\$122,050

REGULATORY FINES & PENALTIES

\$0

PCI

\$0

CLASS ACTION LAWSUIT

\$378,425

TOTAL COST

\$25

PER RECORD COST

A person wearing a blue long-sleeved shirt is holding a tablet computer. The background is a dark blue gradient with vertical columns of white binary code (0s and 1s) floating around. A semi-transparent blue rectangle covers the top half of the image, and the text is centered in white at the bottom.

# Cyber Security Best Practices

# WHAT ARE UNDERWRITERS LOOKING FOR?

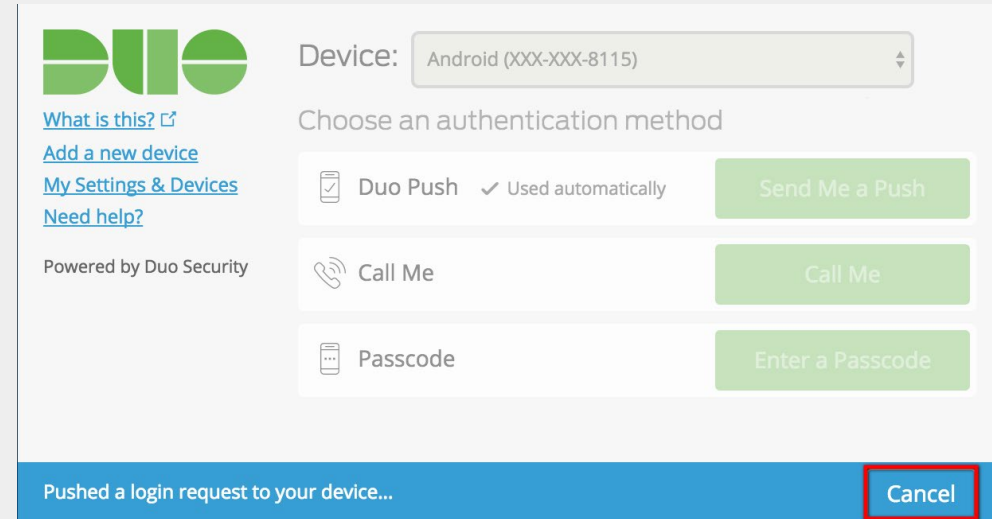
1. Multi-Factor Authentication (MFA)
  - On All Employee Email Accounts
  - For Remote Access to Network
  - For Privileged User Accounts (i.e. IT Admin)
2. Offline Backups or Cloud Back-Ups Secured by MFA
3. Endpoint Detection & Response Solution (EDR)
4. Network Monitoring Solutions
5. Employee Training & Phishing Simulations
6. Email Filtering Software
7. Regularly Updating Computer Systems & Carrying Out Critical Patches / No End-of-Life / Legacy Software



# MULTI-FACTOR AUTHENTICATION (MFA)

## On All Email Accounts + Remote Access to Network + Privileged User Accounts (IT Admin)

- Microsoft 365 → turn on in settings
- Microsoft 2013 or newer → turn on “Modern Authentication for Office 2013”
- Legacy Systems → use outsourced/third party MFA providers
  - TierPoint
  - Duo Mobile
  - Okta
  - Symantec VIP



The image shows the Duo Security authentication interface. On the left is the Duo logo and links: "What is this?", "Add a new device", "My Settings & Devices", and "Need help?". Below these links is the text "Powered by Duo Security". On the right, there is a "Device:" dropdown menu showing "Android (XXX-XXX-8115)". Below this is the heading "Choose an authentication method". There are three options: "Duo Push" (with a checkmark and "Used automatically"), "Call Me", and "Passcode". Each option has a corresponding green button: "Send Me a Push", "Call Me", and "Enter a Passcode". At the bottom, a blue bar contains the text "Pushed a login request to your device..." and a red-outlined "Cancel" button.





## Offline Backups

- Instruct IT personnel to back up business critical data to external hard drive once per month which is disconnected from the internet.

## Cloud Back-Ups Secured by MFA

- Drop Box
- AWS
- Egnyte



# ENDPOINT DETECTION AND RESPONSE

**Combines continuous monitoring of endpoints and response analytics.**

- Activity that is flagged to be suspicious is then automatically removed or contained.
- Endpoint = any device that can communicate back & forth with a network (cellphones, individual computers, servers, etc)



# EMPLOYEE AWARENESS TRAINING & PHISHING SIMULATIONS



**Human Error is the #1 Cause of Cyber Attacks**

**Employees = Weakest Link in an Organizations IT Security Chain**

Training programs designed to increase employees' security awareness. For example, programs can focus on how to identify potential phishing emails.

**Phishing Simulations** = Fake Phishing emails sent to employees on a monthly basis. Those who click on the fake link are prompted to a series of e-learning videos.

**\*Evolve offers Free employee Awarenesssss Training & Phishing Simulations for Policyholders**



# EMAIL FILTERING SOFTWARE

Software used to scan an organization's inbound and outbound email messages and place them into different categories, with the aim of filtering out spam and other malicious content.

- Mimecast
- Barracuda
- SpamTitan
- Proofpoint
- Graphus





# CARRYING OUT CRITICAL PATCHES / NO END OF LIFE OR LEGACY SOFTWARE

## **Software Vulnerabilities have been an increased cause of Ransomware Attacks**

Instruct IT Personnel to check & carry out critical patches from technology/software providers every 2 weeks or as soon as possible

Ensure No End-of-Life (EOL) Software or Legacy Software is Used

- If so, we recommend decommissioning or segregating their end-of-life (EOL) software

Examples:

- Windows 7 or Windows 8 Operating Systems
- Microsoft Exchange Server 2010
- Adobe Acrobat 2015

**\*Evolves Claims team pushes notifications to policyholders if we catch wind of a new vulnerability for a specific software.**



# SOCIAL ENGINEERING PREVENTATIVE ACTIONS

## Call Back Procedure's

- Picking up the phone and calling (over a verified telephone number) the company or person requesting the funds transfer to confirm that the request is legitimate.
- Verified telephone number **does not** include numbers found in the email containing the request, but rather the phone number listed on the vendor's website, or a number that is confirmed via an internal resource.

## Dual Signature Authorization

- Have a two-signature verification process with two senior executive officers involved.
- For example, if you are performing a wire transfer over \$10,000, then two assigned officers must review and sign off on it before further action is taken.

## Phishing Training

Phishing Simulations allow the organization to create fake phishing email campaigns which are sent to staff members.

Human error is currently the highest cause of cyber related claims.

## Multi Factor Authentication (MFA or 2FA)

In order to prevent hackers from obtaining access to emails, we highly recommend utilizing Multi-Factor Authentication (MFA) when logging into email related accounts and applications that require a username and password.

This is one of the most successful methods of preventing hackers from using brute force attacks, in which they run a program that rallies through a series of passwords until one works.



# CYBERSECURITY IMPLEMENTATION

## **Minimum cybersecurity controls**

are required by the entire marketplace  
**to purchase cyber insurance.**

Evolve's Cybersecurity Partners:

1. Oversee Timely Cybersecurity Implementations
2. Are Significantly Discounted



Evolve's Cybersecurity Partnerships Solve Minimum Cyber Underwriting Requirements



# CYBERSECURITY IMPLEMENTATION CONT.

## Broker Benefits:

- Meet insurance deadlines to bind coverage
- Save time shopping the cybersecurity market for vendors
- Educate clients on cybersecurity controls that mitigate risk

## Client Benefits:

- Improve cybersecurity posture to prevent or mitigate the cost of a cyber attack
- Professional cybersecurity expertise & oversight throughout implementation
- Exclusive Evolve discounted pricing on top tier cybersecurity products & services
- Meet cyber insurance requirements to purchase coverage

## Minimum Cybersecurity Controls:

Multi-Factor Authentication (MFA)

Endpoint Detection & Response (EDR)

Legacy Software Decommissioning

Next Gen Antivirus & Firewall Software

Malicious Email Filtering

Employee Phishing Training

Data Back Up Solutions

Network Monitoring Software

Vulnerability Scanning & Patch Management

Penetration Testing

Security Information & Event Management (SIEM)

Security Operations Center (SOC)

Evolve's Cybersecurity Partnerships Solve Minimum Cyber Underwriting Requirements





# CYBER SECURITY BEST PRACTICE RESOURCES

- *Technology Implementation*
- *TierPoint MFA Implementation*
- *Secure Your Business: 5 Easy Steps*
- *Multi-Factor Authentication Instructional PDF's*
- *Secure Your Home Office – 5 Free Easy Steps*
- *Security Controls Glossary of Terms*



## Secure Your Business: 5 Easy Steps

Directions: Management should ask their IT department to review the minimum security standards highlighted below and report back on any security vulnerabilities that could be implemented across the entire organization.

### 1. Secure Ransomware Threat

**Ransomware's biggest threat to your organization is destroying essential data to operate. Back up, encrypt, and secure logins.**

- ✓ Cloud Storage: [Locally Back Up Data \(NAS\)](#)
- ✓ CRM Data & Email Data: [Back Up Data in the Cloud](#)
- ✓ Local Data: [Encrypt Windows | Mac & Back Up Windows | Mac](#)
- ✓ Enable Multi-Factor Authentication on Critical Operating Systems:
  - ✓ CRM: [SalesForce Authenticator](#)
  - ✓ Email: [Microsoft Authenticator](#)
  - ✓ Cloud Storage: [DUO Authenticator](#)

### 2. Secure Employees

**Control employee security standards on the corporate level.**

- ✓ Set Up a Corporate Password Manager: [LastPass](#)
  - ✓ Require Generated Security Passwords
  - ✓ Ensure Employees have a "Strong" Security Score
  - ✓ Do Not Allow Passwords to be Saved in Web Browser
- ✓ Automatically Block Malicious Websites: [Require DNS Blocker](#)
- ✓ Require Ad Blockers on Web Browsers: [AdBlock](#)
- ✓ Implement Mandatory Monthly Software Updates
  - ✓ Anti-Virus, Microsoft Office, Computer, and Phone Software

### 3. Secure Phishing Threat

**Purposely phish employees, set up a security gateway, and stop hackers from impersonating your emails.**

- ✓ Run Monthly Phishing Tests on Employees: [CyberRiskAware](#)
  - ✓ Send Violations Reports to Management
- ✓ Stop Incoming Phishing Threats: [Security Gateway Providers](#)
- ✓ Stop Outgoing Phishing Threats: [Set Up DMARC](#)

### 4. Secure Company Website

**Identify & correct security faults on your website.**

- ✓ Add SSL/TLS Encryption: [ImmunWeb](#)
- ✓ CMS Vulnerabilities & Website Compliance: [ImmunWeb](#)
  - ✓ Update CMS Plugins
  - ✓ Update Web Server Software & HTTP Headers
  - ✓ Ensure Regulatory Compliance (GDPR, PCI)

### 5. Secure Bank Accounts & Fund Transfers

**Secure bank access & require transfer security protocols.**

- ✓ Enable Multi-Factor Authentication for Bank Login
  - ✓ Use a Bank Tokenized Keyfob (highest level of security)
- ✓ On New Transfers, Require Call Back Procedure Prior to Transfer
- ✓ Require a 2<sup>nd</sup> Internal Signature on Transfers Over a Certain Minimum Dollar Threshold (E.G. - \$10,000.00)

**evolve**

Visit [www.evolveimga.com](http://www.evolveimga.com) for more information.



# Evolve MGA

## Security Controls Glossary

### Application whitelisting

A security solution that allows organizations to specify what software is allowed to run on their systems, in order to prevent any nonwhitelisted processes or applications from running.

### Antivirus

A product that can detect and prevent malicious software on computers, laptops and other tech devices.

### Asset inventory

A list of all IT hardware and devices an entity owns, operates or manages. Such lists are typically used to assess the data being held and security measures in place on all devices.

### Brute force attack

A method whereby threat actors submit multiple password attempts in rapid succession until they successfully gain entry into business networks.

### Cloud

A virtual space on the internet used for storing digital resources instead of on local computer networks. Clouds can be public, private or hybrid, each with pros and cons. Examples include Google Drive, Apple iCloud, Netflix, Amazon Web Services (AWS), Dropbox and Microsoft OneDrive.

### Custom threat intelligence

The collection and analysis of data from open source intelligence (OSINT) and dark web sources to provide organizations with intelligence on cyber threats and cyber threat actors pertinent to them.

### Cyber

Relates to or characteristic of the culture of computers, information technology, and virtual reality

### Cyber attack

An unauthorized attempt by hackers to damage, destroy, alter or exploit a computer network, system, or employees.

### Cybercrime

Extortion by phishing, ransom attacks, social engineering or losses caused by malware or DDOS.

### Cyber event

Actual or suspected unauthorized system access, electronic attack or privacy breach.

### Cyber insurance

Cyber insurance exists to help protect businesses against the threat of cybercrime.

### Cyber security

The technologies, processes and controls used to protect and support information technology (IT).

### Cyber threat analysis

The dedicated team typically provided by a cyber insurer to help detect, prevent and stop cyber attacks from affecting businesses before they fall victim.

### Database encryption

Where sensitive data is encrypted while it is stored in databases. If implemented correctly, this can stop malicious actors from being able to read sensitive data if they gain access to a database.

### Data loss prevention

Software that can identify if sensitive data is being exfiltrated from a network or computer system.

### DDoS mitigation

Hardware or cloud based solutions used to filter out malicious traffic associated with a Distributed Denial of Service (DDoS) attack, while allowing legitimate users to continue to access an entity's website or web-based services.

### DMARC

An internet protocol used to combat email spoofing – a technique used by hackers in phishing campaigns.

### DNS filtering

A specific technique to block access to known bad IP addresses by users on your network.

### Email filtering

Software used to scan an organization's inbound and outbound email messages and place them into different categories, with the aim of filtering out spam and other malicious content.

### Employee awareness

Training programmes designed to increase employees' security awareness. For example, programmes can focus on how to identify potential phishing emails.

### End user device

Any computer or mobile device used by the end customer.

### Endpoint protection

Software installed on individual computers (endpoints) that uses behavioral and signature based analysis to identify and stop malware infections.

### Extortion

A crime involving an attack or threat of an attack coupled with a demand for money or some other response in return for stopping or remediating the attack.

### Firewall

Hardware solutions used to control and monitor network traffic between two points using predefined parameters.

### Incident response

An organized approach involving technical, legal and claims expertise to address and remediate a cyber incident. These are typically offered by a cyber insurer as the full suite claims service.

### Incident response plan

Action plans for dealing with cyber incidents to help guide an organization's decision-making process and return it to a normal operating state as quickly as possible.

### Intrusion detection system

A security solution that monitors activity on computer systems or networks and generates alerts when signs of compromise by malicious actors are detected.

### Malware

Includes viruses, trojans, worms or any code or content that could have an adverse impact on organizations or individuals.

### Managed service provider

A third party organization that provides a range of IT services, including networking, infrastructure and IT security, as well as technical support and IT administration.

### Mobile device encryption

Encryption involves scrambling data using cryptographic techniques so that it can only be read by someone with a special key. When encryption is enabled, a device's hard drive will be encrypted while the device is locked, with the user's passcode or password acting as the special key.

### Multi-factor authentication (MFA/2FA)

Where a user authenticates themselves through two different means when remotely logging into a computer system or web based service. Typically a password and a passcode generated by a physical token device or software are used as the two factors.

### Network

Two or more computers linked to share electronic communications, resources and file exchanges.

### Network monitoring

A system, utilising software, hardware or a combination of the two, that constantly monitors an organization's network for performance and security issues.

### Next-generation firewalls

Software or hardware solutions that combines traditional firewall technology with additional functionality, such as encrypted traffic inspection, intrusion prevention systems and anti-virus.

# GET A COMPREHENSIVE CYBER POLICY



- **Will provide both proactive and reactive responses**
- **Most offer free risk management services**
- **A **Cyber Specialist** Claims Team**





# evolve

## How We Can Help





# THREE MAJOR COMPONENTS

**Pre-Breach Risk  
Management  
Services**

**Broad Cyber  
Coverage**

**Expert Claims  
Handling**



# EVOLVE MOBILE APP

## Notify Claims Instantly:

- Suffering an incident? Trigger an immediate call-back from our experienced team of responders

## Turn on Tools:

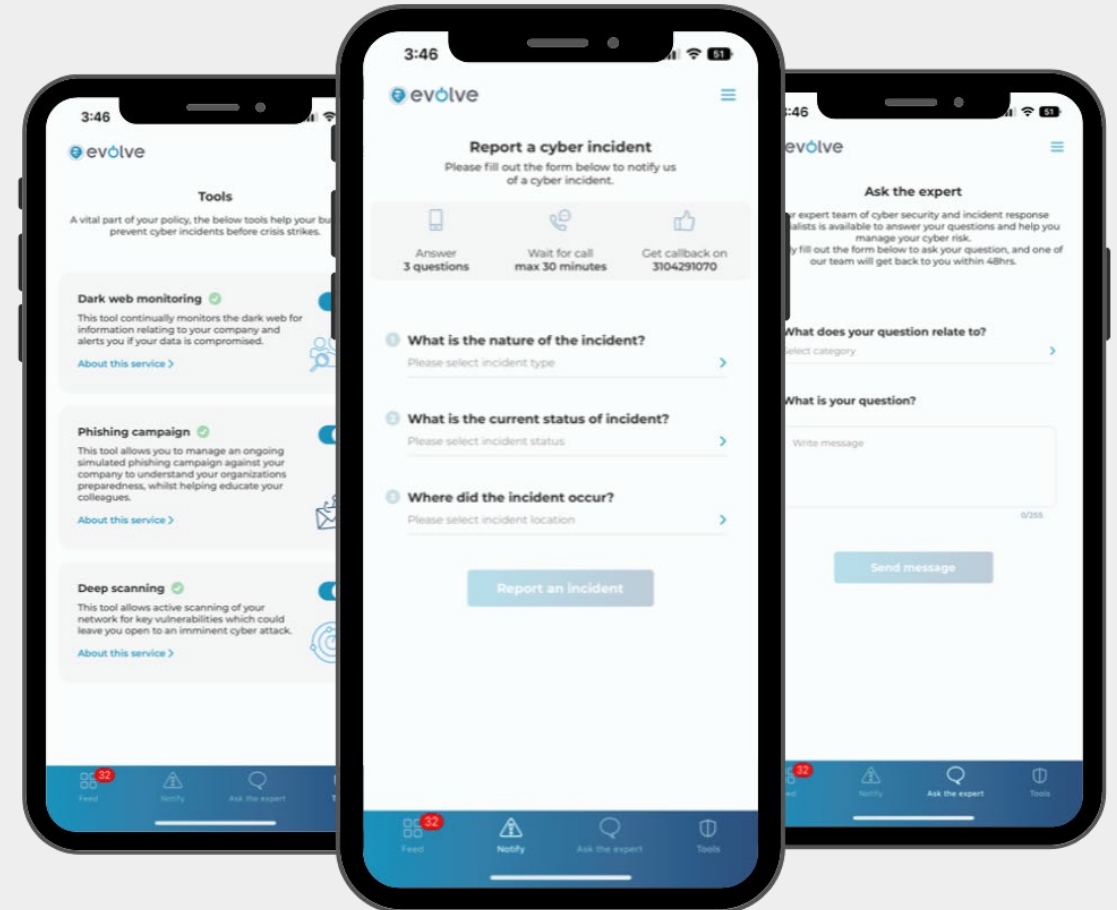
- Activate tools like Deep Scanning and Dark Web Monitoring which identify vulnerabilities before they lead to an attack

## Stay Ahead:

- Get critical, time-sensitive alerts pertaining specifically to your business sent straight to your phone

## Ask an Expert:

- Access our specialist technical team for help with risk mitigation, best practices and more



# CYBERSECURITY

**\$7,500 MARKET VALUE**

## Risk Management Services

### Cybersecurity Vendors

Evolve MGA policyholders get free access to the following "cybersecurity specialist" vendors.

#### DARKTRACE

##### Identify & Prevent Cyber Attacks

Darktrace's artificially intelligent cybersecurity technology identifies & prevents cyber attacks on your organization in real time, autonomously shutting down hackers by monitoring your organization's entire digital footprint, including data wherever it resides (cloud, SaaS, email, endpoints, IoT, & physical systems).

#### BLACKFOG

##### Threat Intelligence Report

BlackFog will provide your organization with a Threat Intelligence Report to spot any malicious activity, including existing ransomware, over a 7-day period.

To access, email: [riskmanagement@evolvemga.com](mailto:riskmanagement@evolvemga.com)

#### NINJIO

##### Employee Cybersecurity Training

Ninjio will send your employees 4-minute, gamified videos on real types of cyber attacks and how to prevent falling victim to them.

#### CONTROL CASE

##### Privacy Compliance Audit

Control Case provides a 40-minute consultation to identify if your organization's sensitive information complies with foreign, federal, state, & private privacy regulatory laws.



# CLAIMS HANDLING

- **One of the Largest In-House Cyber Claims Team in the World**
  - 40 located in Austin, TX
  - 50 located in London, U.K.
- 20+ Years of Cyber Claims Experience
- 150+ Claims Handled per Month

24/7 Breach Hotline  
+ \$0 deductible

Cyber Claims Panel Providers:





Teague  
INSURANCE

# evolve

## Questions?

