breachsiren

Breach Intelligence Platform

Real data, right now.

Considering Breach Data to Gain Budget

About Me

Jay Bobo
Founder, Breachsiren

Experience:

- 20+ years in technology
- Nine years in healthcare

Passions:

- Spending time with family
- Helping friends in TPRM reduce their workload with automation & data

Goals For Today

1. Learn to speak the language of the business

1. Use data to build compelling stories about your work

2. Make a perfect pitch for budget

Meet Bob

Bob’s Problem

He’s stressed & overwhelmed.

- Solo practitioner
- Works for a small hospital
- 700 vendors (150 critical)
- Uses Microsoft Excel

Bob’s Wants

More resources!

- Hire a junior person
- Dedicated TPRM tool
- Continuous vendor monitoring (ESG, financial, cyber)

“I can’t manage this myself. The vendors take forever to respond if they respond at all.

I need some help.”

— Bob Rossi

Bob’s Pitch

He prepared a report with…

- # of assessments annually
- A recent study stating regulators are focusing on supplier risk and the % of increased incidents
- The average cost of a breach

“I looked up some of our vendors online and found a website that scans them.

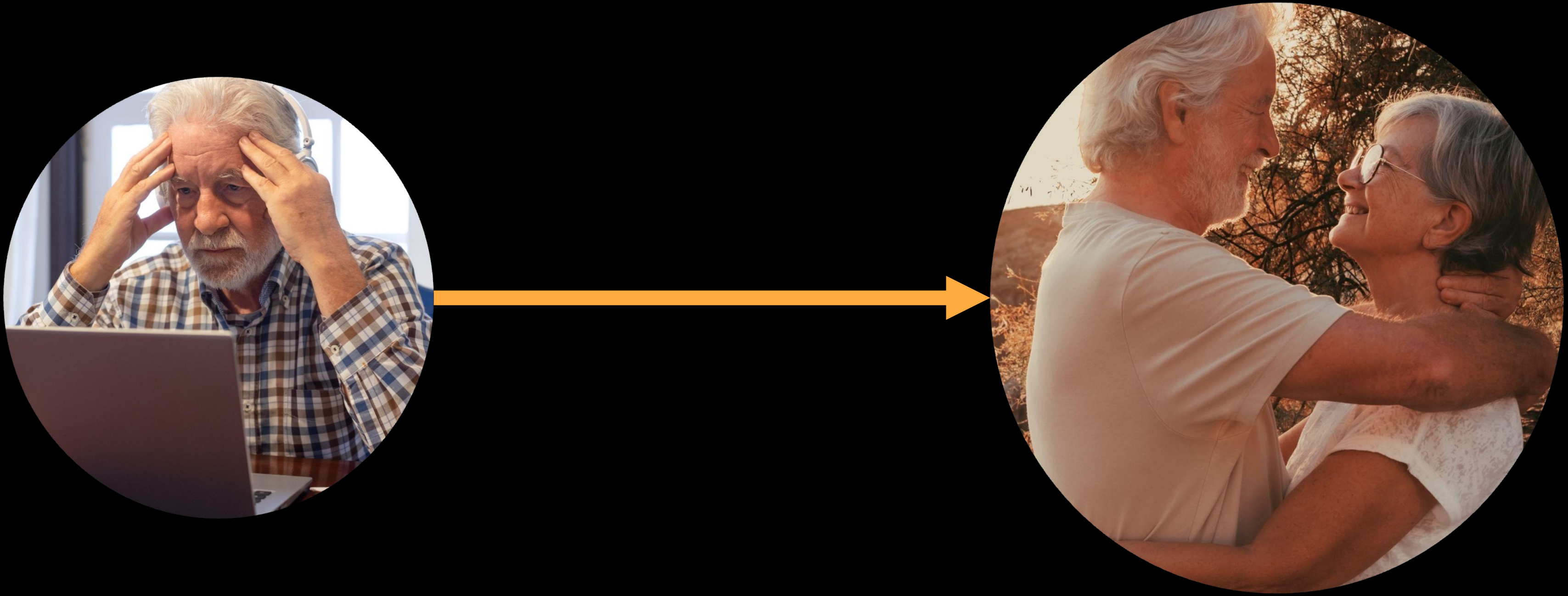
It says they have low risk scores. There could be a real risk to the business.”

— Bob Rossi

The Result

The CISO says…

“I’m sorry. We really appreciate your effort on this, but we don’t have the resources right now. The board is concerned about how our audit deficiencies might be viewed publicly. We need to focus on those this year.”



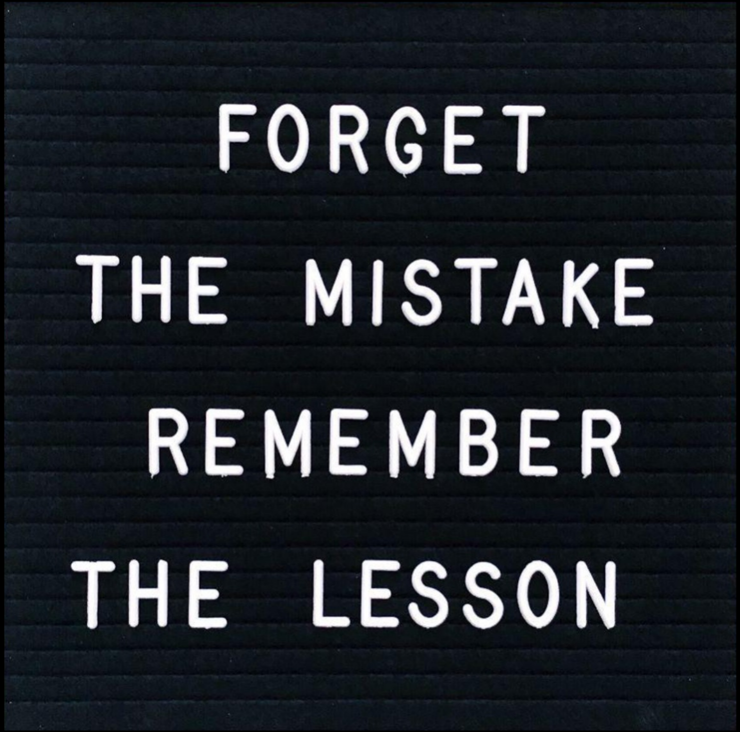
Problem: Bridging the gap

Where did Bob go wrong?

Mistakes!?!

What did he get wrong?

- Didn’t address business needs
- Wrong data
- Lack of support
- Lack of narrative
- Made it easy to say, “No”



FORGET
THE MISTAKE
REMEMBER
THE LESSON

Understanding the gap at work

breachsiren

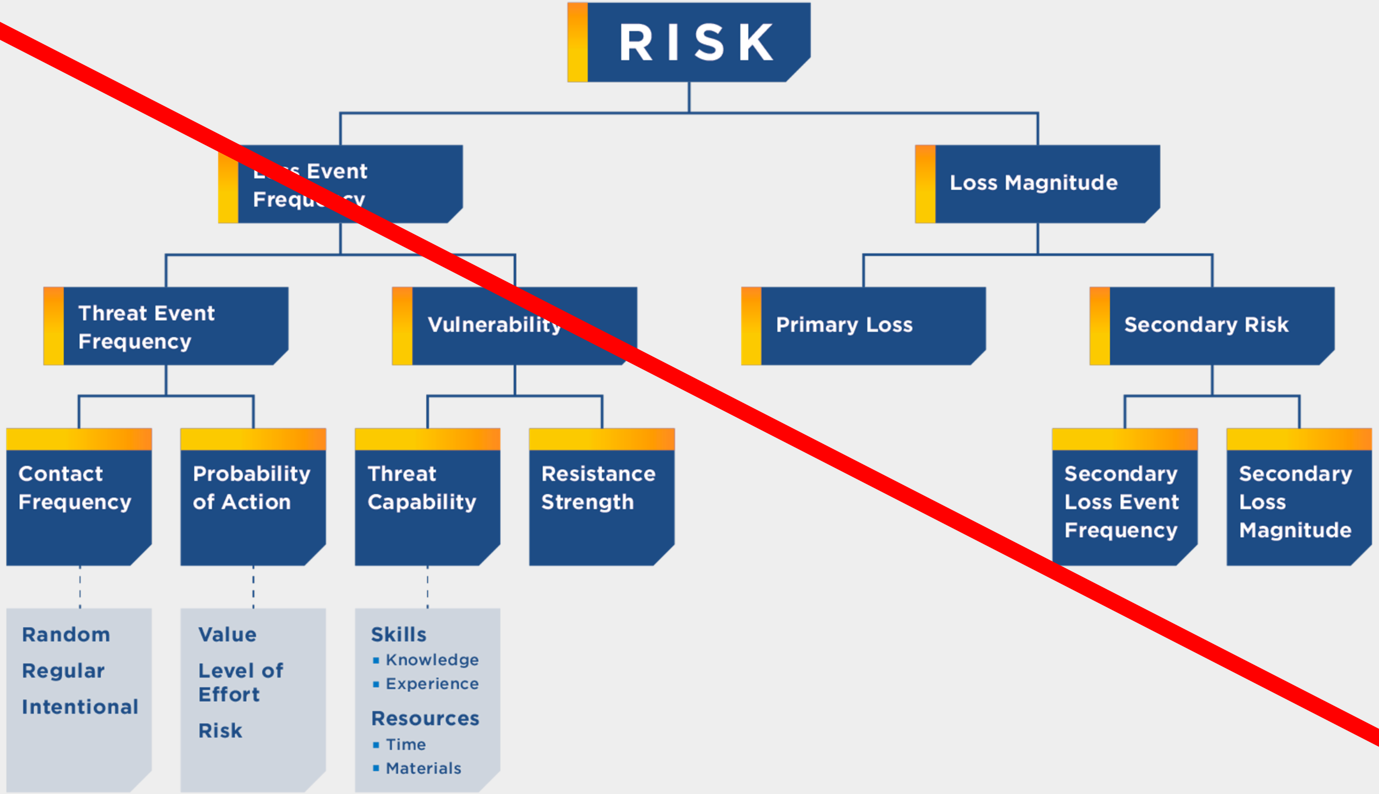
Question:

How do you communicate the value you provide?

Question:

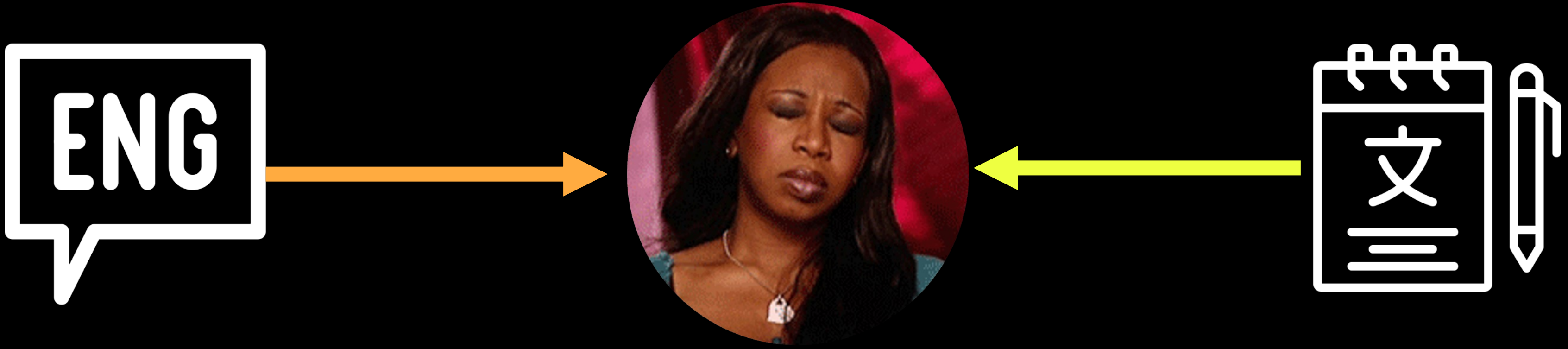
How does your company communicate its value?

breachsiren



RISK

- Loss Event Frequency
  - Threat Event Frequency
    - Contact Frequency
      - Random
      - Regular
      - Intentional
    - Probability of Action
      - Value
      - Level of Effort
      - Risk
  - Vulnerability
    - Threat Capability
      - Skills
        - Knowledge
        - Experience
      - Resources
        - Time
        - Materials
    - Resistance Strength
- Loss Magnitude
  - Primary Loss
  - Secondary Risk
    - Secondary Loss Event Frequency
    - Secondary Loss Magnitude



Problem: Communication

“The human mind is a story processor, not a logic processor.”

— Jonathan Haidt

breachsiren

Our Checklist

Turn mistakes into opportunities!

- **Address business needs**
- Wrong data
- Lack of support
- Lack of narrative
- Made it easy to say, “No”

FORGET THE MISTAKE REMEMBER THE LESSON

Using data to build compelling stories

breachsiren

Question:

What’s wrong with risk rating and threat intelligence tools?

What's
so wrong?

Problem 1

“Organizations should stop using risk scores and risk matrices. There is mounting evidence against (and none for) their effectiveness”

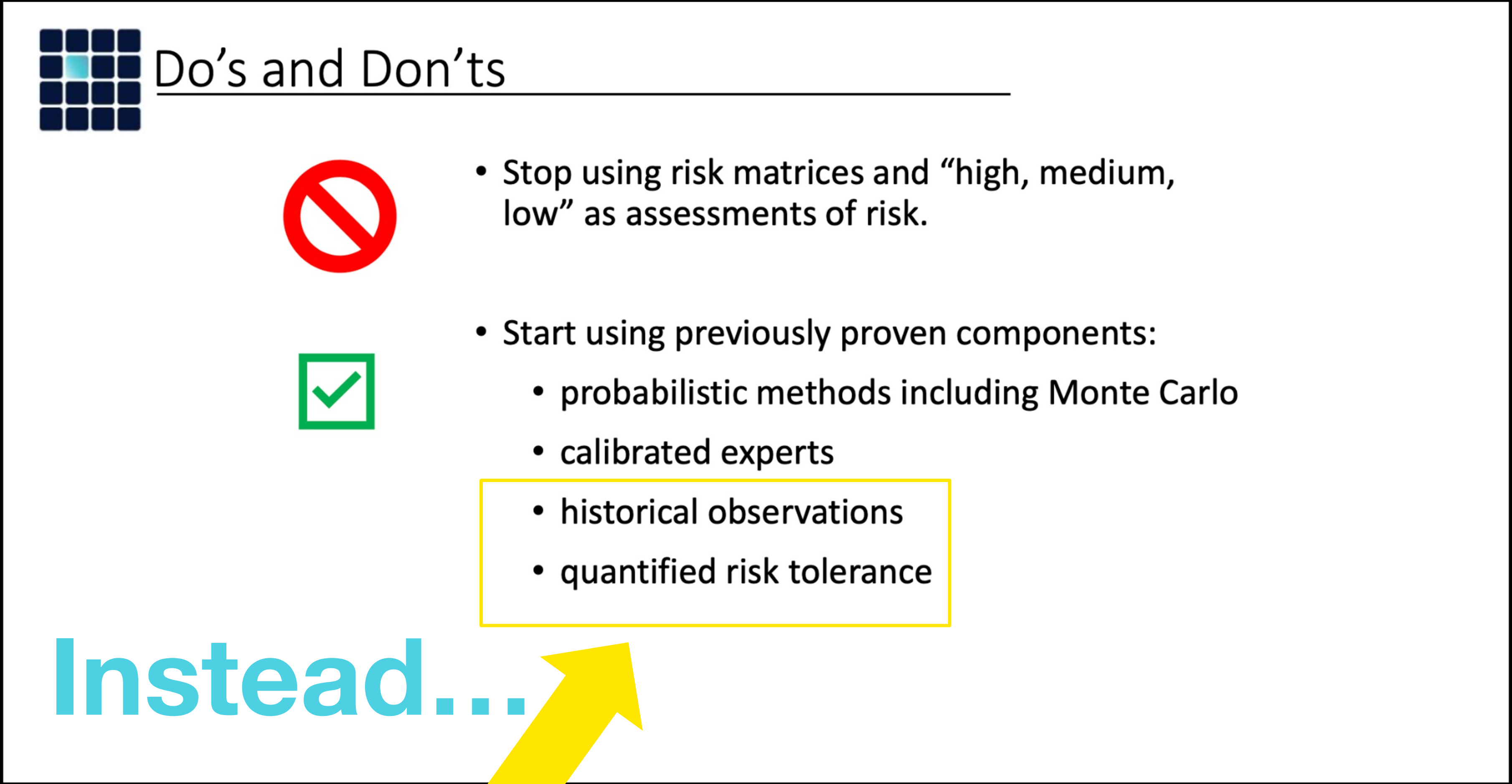
— Doug Hubbard, author of
“How to Measure Anything in Cybersecurity”

Source: https://www.youtube.com/watch?v=bYjPmptlc14

Problem 2

breachsiren

WHEN
WHERE
WHAT
WHO
HOW
WHY



Do’s and Don’ts

🚫

- Stop using risk matrices and “high, medium, low” as assessments of risk.

☑

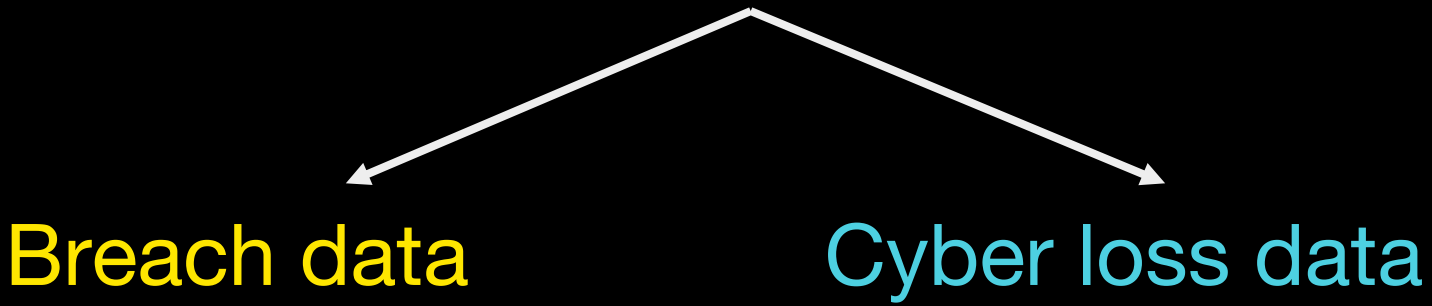
- Start using previously proven components:
    - probabilistic methods including Monte Carlo
    - calibrated experts
    - historical observations
    - quantified risk tolerance

Instead…

“Breakthroughs in science often happen at the intersection of diverse scientific disciplines”

— Dr. Bob Reiter, Bayer

Solution = **Better Data**



Breach data

Cyber loss data

What is breach notification data?

Question:

Are private companies mandated to notify their users if they leak their data?

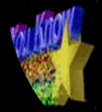
All 50 states and the District of Columbia have laws requiring private businesses, to notify individuals of security breaches of [..] personally identifiable information.”

— National Conference of State Legislatures

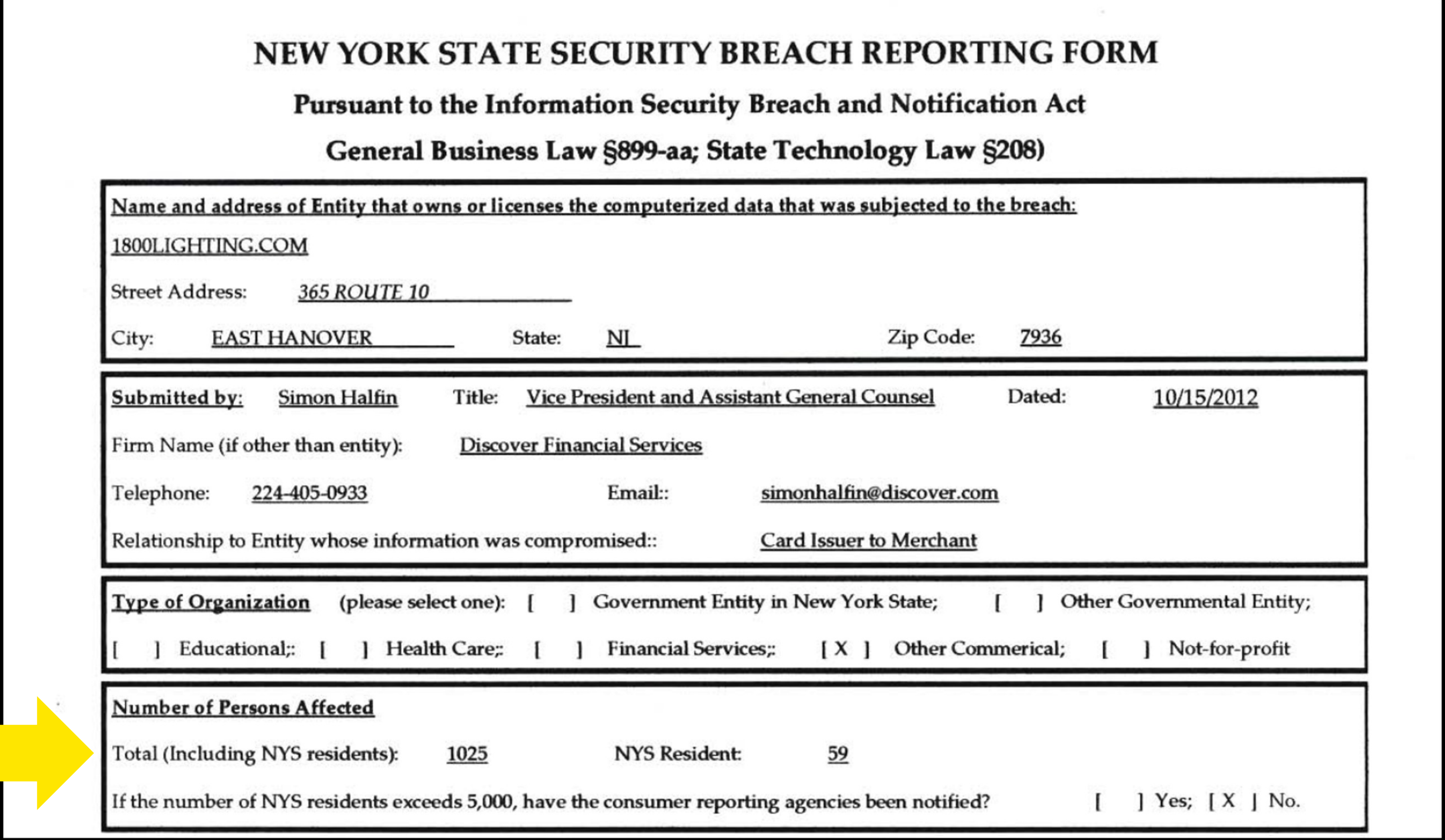
Source: https://www.ncsl.org/technology-and-communication/security-breach-notification-laws

Fun Fact

Things to know…



1. Breach notification laws are regulated at state level
2. 35 states and DC require private companies to notify their Office of the Attorney General
3. 40 states and DC require notification to a credit reporting agency
4. Generally, notification is required for >=1,000 citizens
5. Notification requirements are ASAP to 45 days generally



NEW YORK STATE SECURITY BREACH REPORTING FORM

Pursuant to the Information Security Breach and Notification Act

General Business Law §899-aa; State Technology Law §208)

Name and address of Entity that owns or licenses the computerized data that was subjected to the breach:

1800LIGHTING.COM

Street Address: *365 ROUTE 10*

City: EAST HANOVER State: NJ Zip Code: 7936

Submitted by: Simon Halfin Title: Vice President and Assistant General Counsel Dated: 10/15/2012

Firm Name (if other than entity): Discover Financial Services

Telephone: 224-405-0933 Email:: simonhalfin@discover.com

Relationship to Entity whose information was compromised:: Card Issuer to Merchant

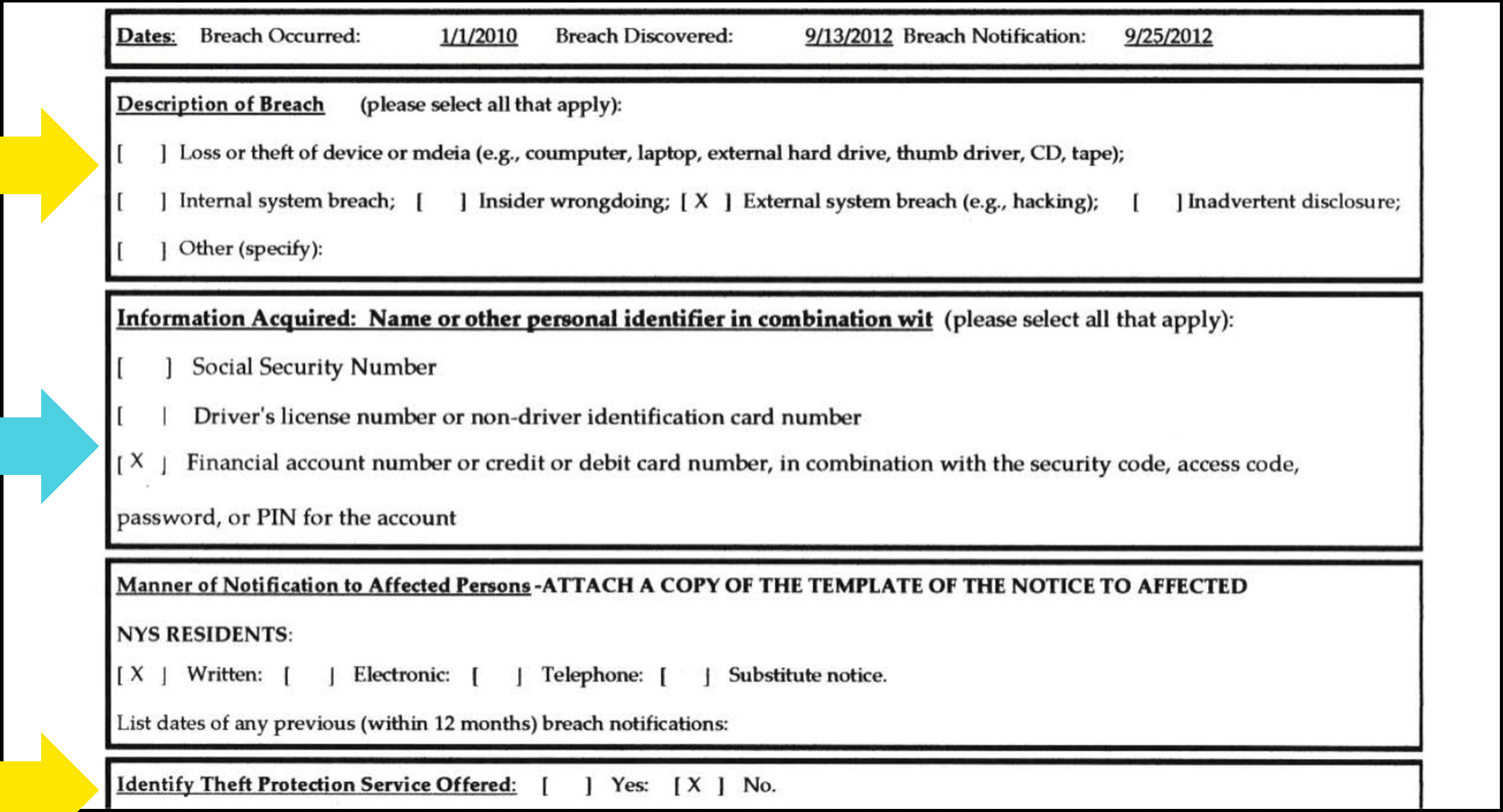
Type of Organization (please select one): [ ] Government Entity in New York State; [ ] Other Governmental Entity;

[ ] Educational;: [ ] Health Care;: [ ] Financial Services;: [X] Other Commerical; [ ] Not-for-profit

Number of Persons Affected

Total (Including NYS residents): 1025 NYS Resident: 59

If the number of NYS residents exceeds 5,000, have the consumer reporting agencies been notified? [ ] Yes; [X] No.



Dates: Breach Occurred: 1/1/2010 Breach Discovered: 9/13/2012 Breach Notification: 9/25/2012

Description of Breach (please select all that apply):

[ ] Loss or theft of device or mdeia (e.g., coumputer, laptop, external hard drive, thumb driver, CD, tape);

[ ] Internal system breach; [ ] Insider wrongdoing; [X] External system breach (e.g., hacking); [ ] Inadvertent disclosure;

[ ] Other (specify):

Information Acquired: Name or other personal identifier in combination wit (please select all that apply):

[ ] Social Security Number

[ ] Driver's license number or non-driver identification card number

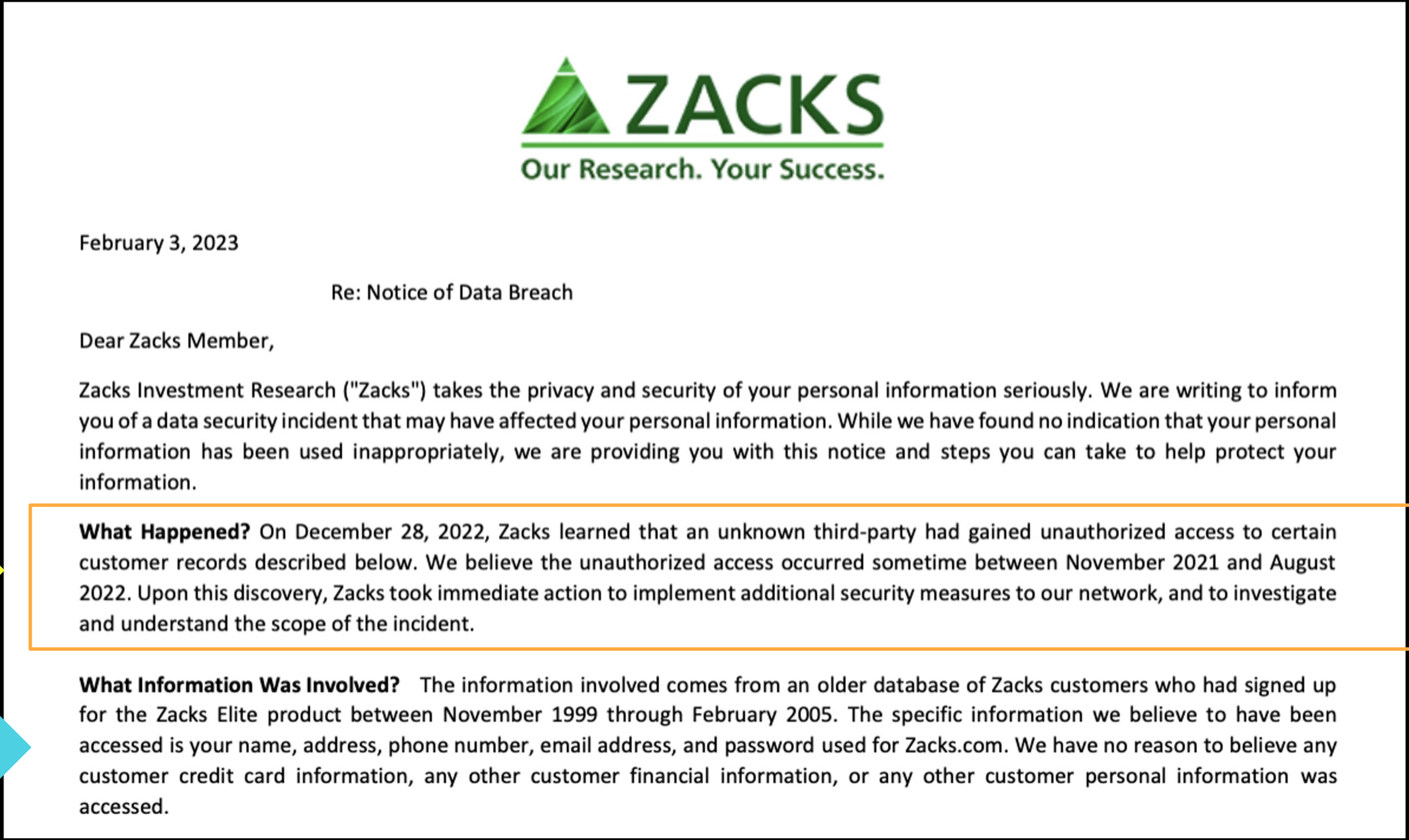
[X] Financial account number or credit or debit card number, in combination with the security code, access code, password, or PIN for the account

Manner of Notification to Affected Persons -ATTACH A COPY OF THE TEMPLATE OF THE NOTICE TO AFFECTED NYS RESIDENTS:

[X] Written: [ ] Electronic: [ ] Telephone: [ ] Substitute notice.

List dates of any previous (within 12 months) breach notifications:

Identify Theft Protection Service Offered: [ ] Yes: [X] No.



ZACKS

Our Research. Your Success.

February 3, 2023

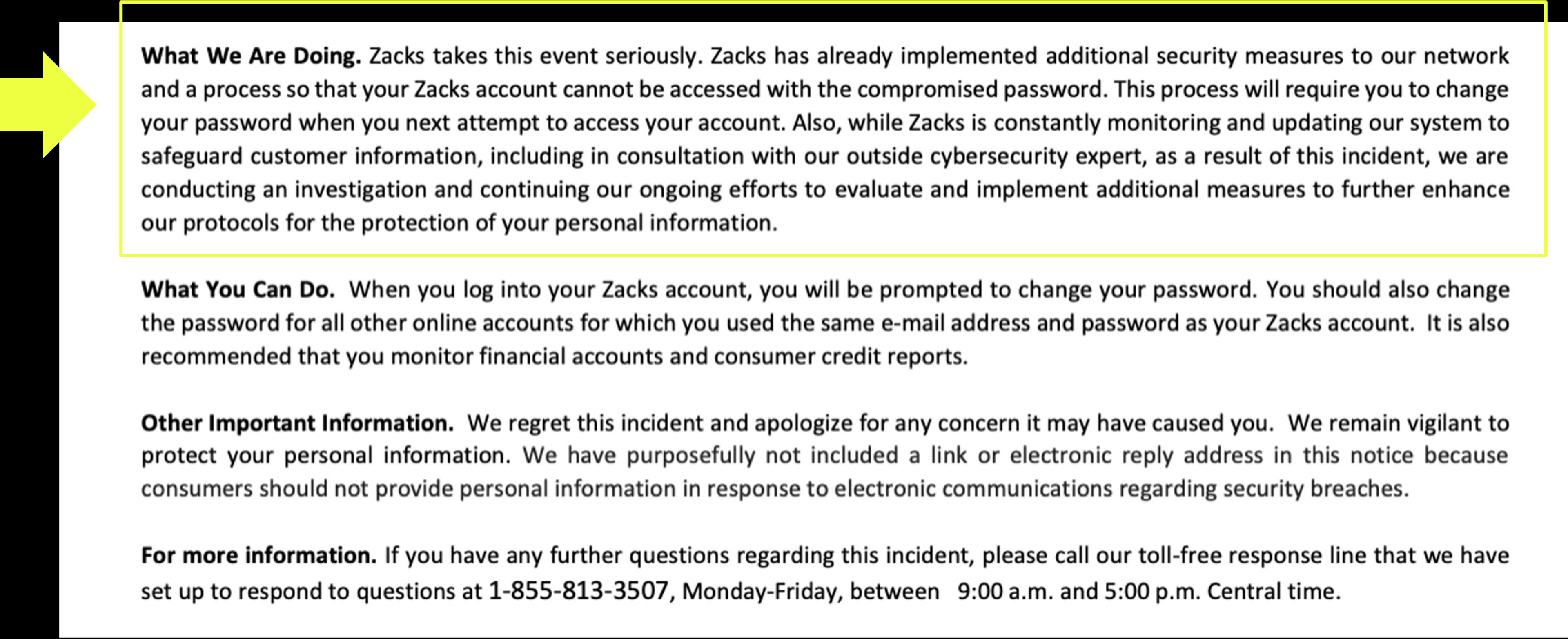
Re: Notice of Data Breach

Dear Zacks Member,

Zacks Investment Research ("Zacks") takes the privacy and security of your personal information seriously. We are writing to inform you of a data security incident that may have affected your personal information. While we have found no indication that your personal information has been used inappropriately, we are providing you with this notice and steps you can take to help protect your information.

What Happened? On December 28, 2022, Zacks learned that an unknown third-party had gained unauthorized access to certain customer records described below. We believe the unauthorized access occurred sometime between November 2021 and August 2022. Upon this discovery, Zacks took immediate action to implement additional security measures to our network, and to investigate and understand the scope of the incident.

What Information Was Involved? The information involved comes from an older database of Zacks customers who had signed up for the Zacks Elite product between November 1999 through February 2005. The specific information we believe to have been accessed is your name, address, phone number, email address, and password used for Zacks.com. We have no reason to believe any customer credit card information, any other customer financial information, or any other customer personal information was accessed.



What We Are Doing. Zacks takes this event seriously. Zacks has already implemented additional security measures to our network and a process so that your Zacks account cannot be accessed with the compromised password. This process will require you to change your password when you next attempt to access your account. Also, while Zacks is constantly monitoring and updating our system to safeguard customer information, including in consultation with our outside cybersecurity expert, as a result of this incident, we are conducting an investigation and continuing our ongoing efforts to evaluate and implement additional measures to further enhance our protocols for the protection of your personal information.

What You Can Do. When you log into your Zacks account, you will be prompted to change your password. You should also change the password for all other online accounts for which you used the same e-mail address and password as your Zacks account. It is also recommended that you monitor financial accounts and consumer credit reports.

Other Important Information. We regret this incident and apologize for any concern it may have caused you. We remain vigilant to protect your personal information. We have purposefully not included a link or electronic reply address in this notice because consumers should not provide personal information in response to electronic communications regarding security breaches.

For more information. If you have any further questions regarding this incident, please call our toll-free response line that we have set up to respond to questions at 1-855-813-3507, Monday-Friday, between 9:00 a.m. and 5:00 p.m. Central time.

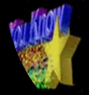
Takeaways

1. Breach notifications are **real data**. They are the Who, What, Where and When.

1. Not notifying impacted users = you’re breaking state law!

1. Breach notification data can be used to ensure vendors, clients and partners are being truthful

   If you’re paying for risk/threat intelligence data but real data isn’t included, what are you really paying for?



What is loss data?

Question:

How would you identify the true financial cost of a data breach?

Anthem®

IMPACT

DON'T DO THIS

$2.5 million - Security consultants (ie. security firm Mandiant)

$115 million - Security improvements

$31 million - Notification to public and affected individuals

$112 million - Free credit monitoring and identity protection services

$31 million - Class-action legal fees

$39.5 million - Multi-state settlement in 2020

$16 million - October 15, 2018 paid record HIPAA settlement with OCR

$115 million - June 23, 2018 class-action settlement

+

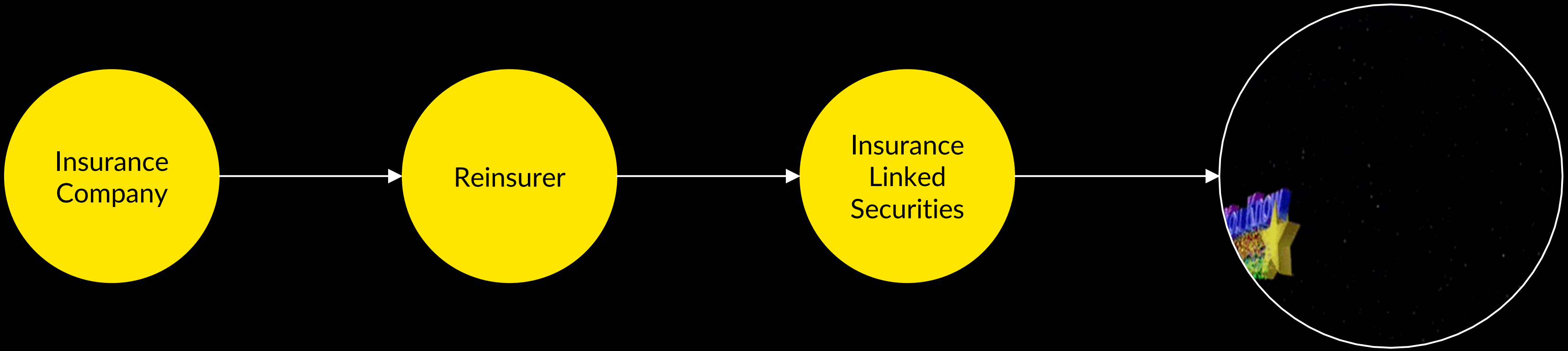
$$$ - other legal costs, higher insurance premiums, etc

At least **$462 million dollars**

*Data compiled from independent incident assessments, Anthem annual reports, DOJ indictment and state insurance commissioner reports.

Why is this important…

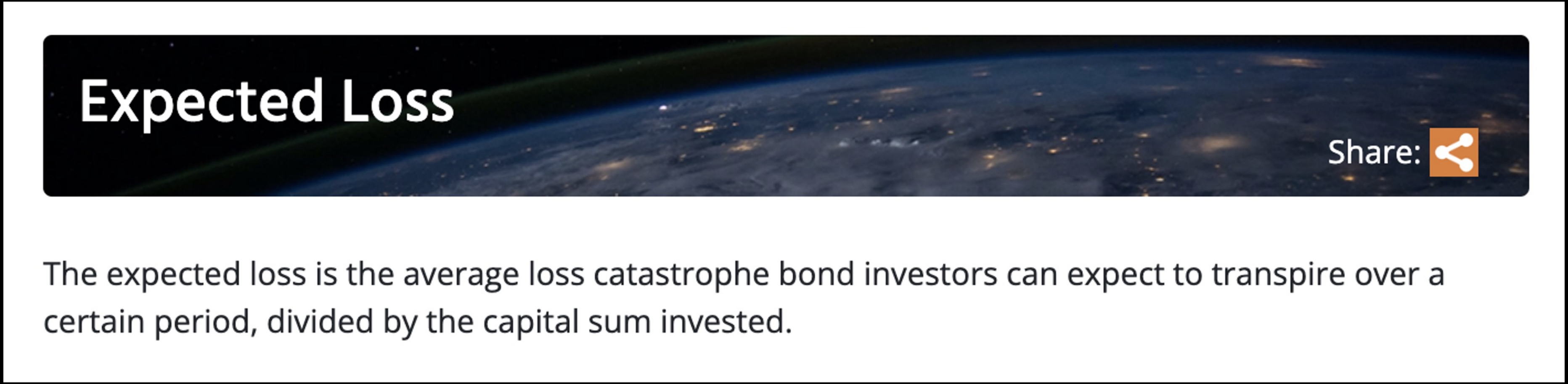
It’s your insurers job to know how much it will cost them if your company has a breach because of **risk transfer**.



Insurance Company

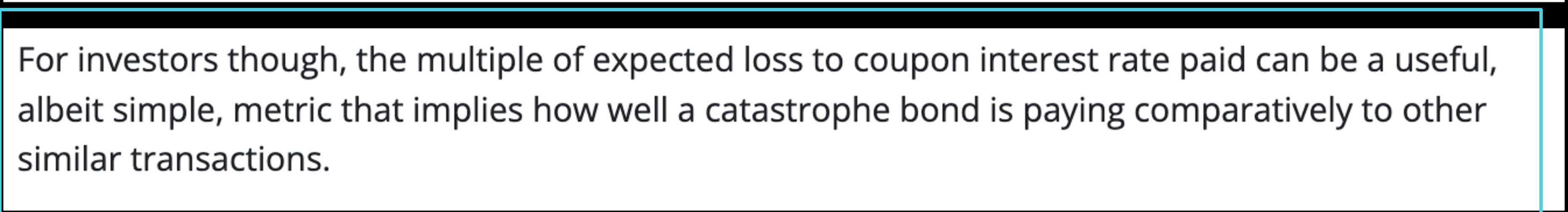
Reinsurer

Insurance Linked Securities



Expected Loss

The expected loss is the average loss catastrophe bond investors can expect to transpire over a certain period, divided by the capital sum invested.

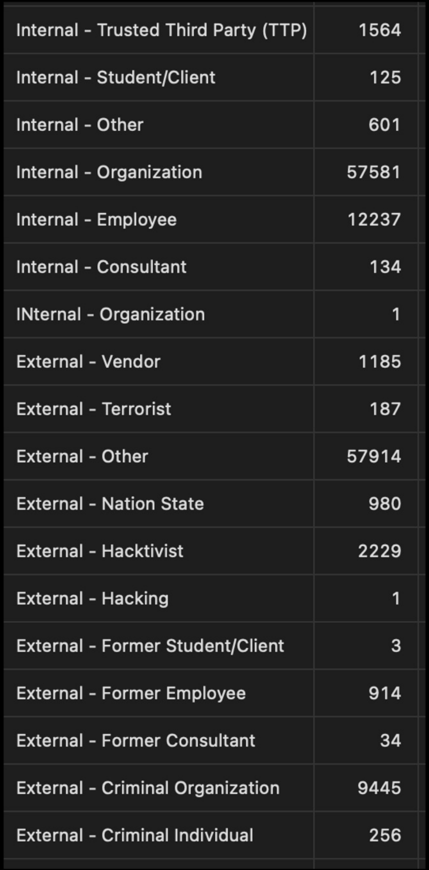


For investors though, the multiple of expected loss to coupon interest rate paid can be a useful, albeit simple, metric that implies how well a catastrophe bond is paying comparatively to other similar transactions.

Source: https://www.artemis.bm/glossary/expected-loss/

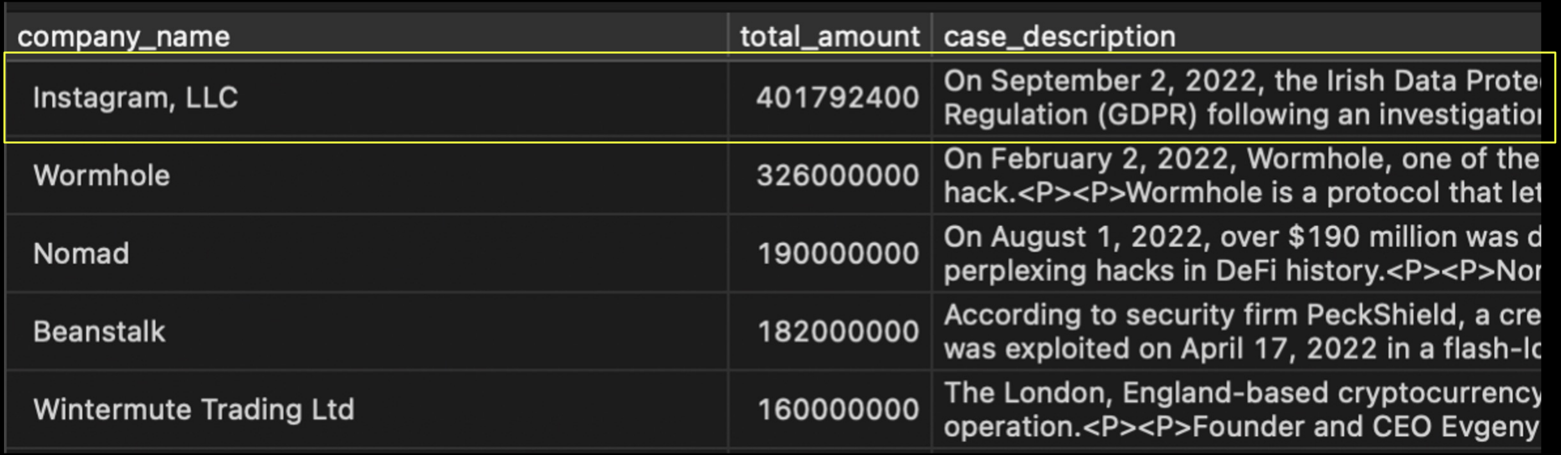
WE NEED TO GO DEEPER

Fields

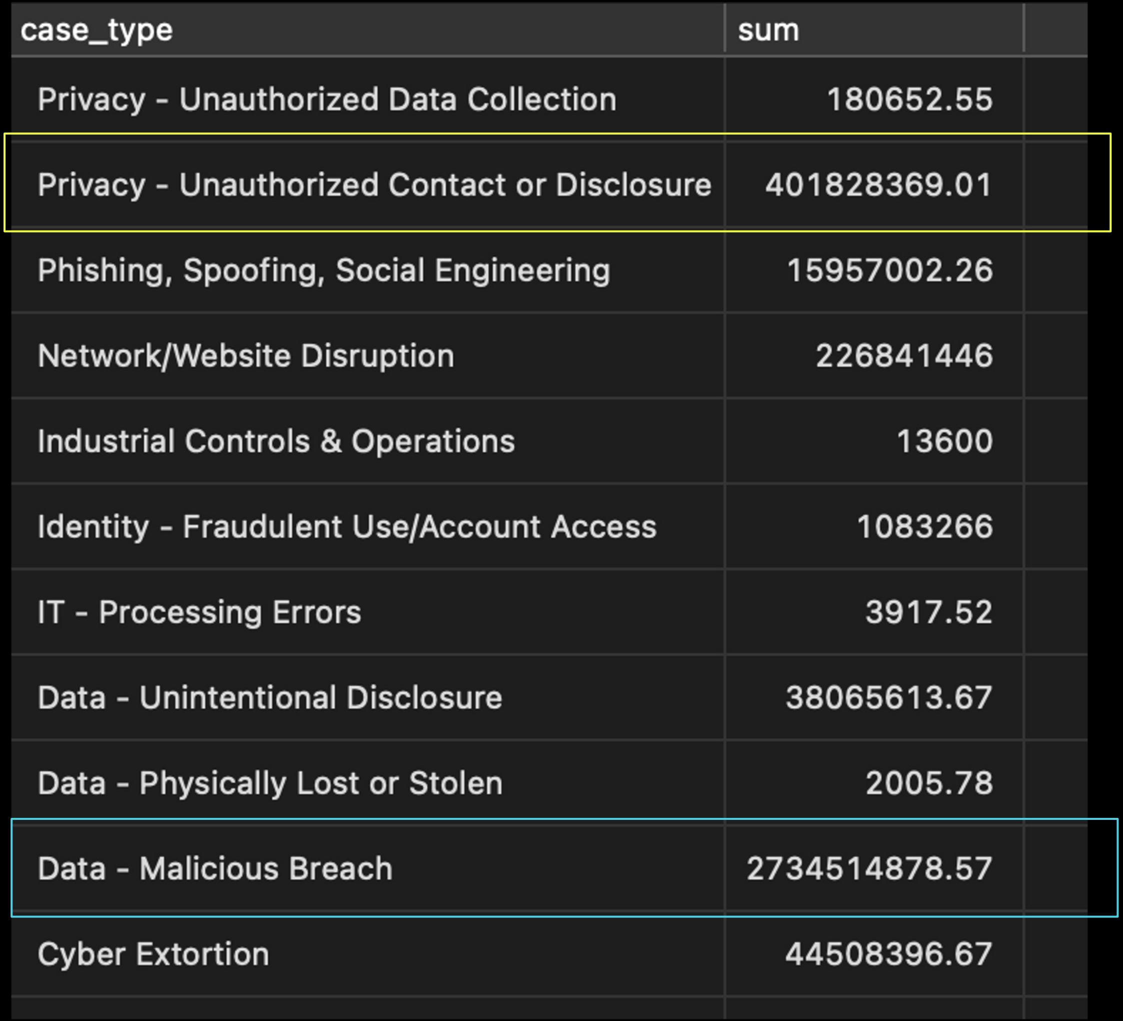


Internal - Trusted Third Party (TTP)	1564
Internal - Student/Client	125
Internal - Other	601
Internal - Organization	57581
Internal - Employee	12237
Internal - Consultant	134
INternal - Organization	1
External - Vendor	1185
External - Terrorist	187
External - Other	57914
External - Nation State	980
External - Hacktivist	2229
External - Hacking	1
External - Former Student/Client	3
External - Former Employee	914
External - Former Consultant	34
External - Criminal Organization	9445
External - Criminal Individual	256

- Company and industry identifiers
- External or internal caused loss including employee, vendor/consultant, terrorist, criminal organization, etc
- Actor vectors, proximate + secondary causes, compromised data sources, types, and affected counts
- Settlement amounts, legal fees, fines, restitution

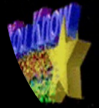


company_name	total_amount	case_description
Instagram, LLC	401792400	On September 2, 2022, the Irish Data Prote Regulation (GDPR) following an investigatio
Wormhole	326000000	On February 2, 2022, Wormhole, one of the hack.<P><P>Wormhole is a protocol that let
Nomad	190000000	On August 1, 2022, over $190 million was d perplexing hacks in DeFi history.<P><P>Nor
Beanstalk	182000000	According to security firm PeckShield, a cre was exploited on April 17, 2022 in a flash-lo
Wintermute Trading Ltd	160000000	The London, England-based cryptocurrency operation.<P><P>Founder and CEO Evgeny



case_type	sum
Privacy - Unauthorized Data Collection	180652.55
Privacy - Unauthorized Contact or Disclosure	401828369.01
Phishing, Spoofing, Social Engineering	15957002.26
Network/Website Disruption	226841446
Industrial Controls & Operations	13600
Identity - Fraudulent Use/Account Access	1083266
IT - Processing Errors	3917.52
Data - Unintentional Disclosure	38065613.67
Data - Physically Lost or Stolen	2005.78
Data - Malicious Breach	273514878.57
Cyber Extortion	44508396.67

Things to know…



1. Cyber loss data is used purely for underwriting purposes not continuous monitoring of actual breaches as reported to regulators

1. It is occasionally the Why but always the How Much of our story.

2. Identify the REAL cost of a breach from an insurers POV

1. Enrich your risk tools for better storytelling

Solution(s)

↓

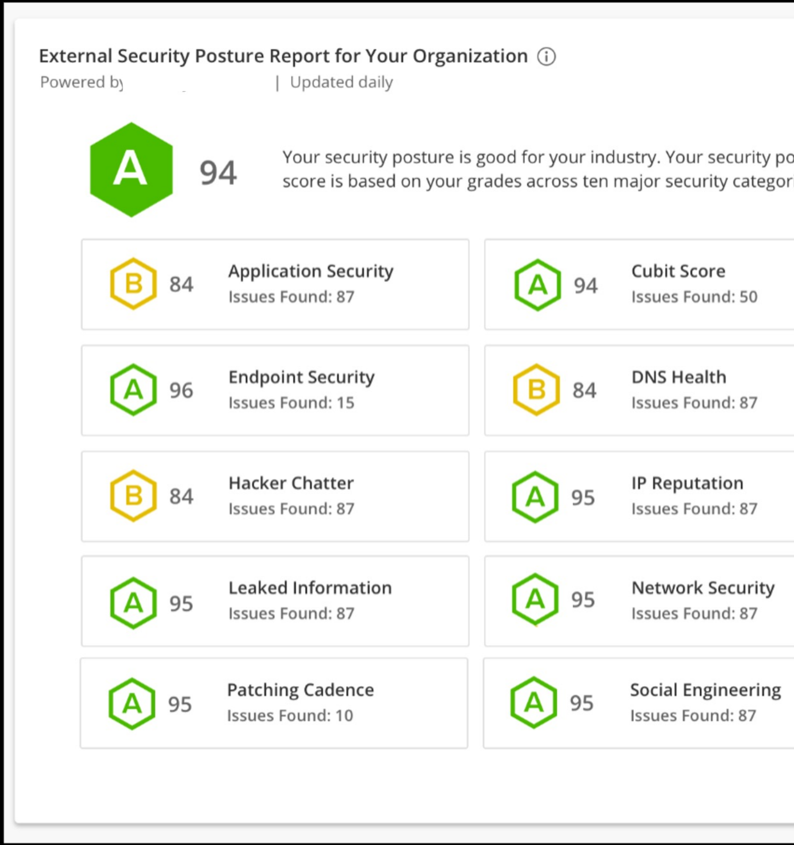
Third Party Risk

(continuous monitoring)

Vendor X - High Risk

What story do we want to tell?

- What letter grade would another vendor assign them?
- What would their theoretical credit score be?
- What security issues are in their external facing sites?



External Security Posture Report for Your Organization ⓘ

Powered by [redacted] | Updated daily

A 94 Your security posture is good for your industry. Your security po score is based on your grades across ten major security categor

B	84	Application Security Issues Found: 87	A	94	Cubit Score Issues Found: 50
A	96	Endpoint Security Issues Found: 15	B	84	DNS Health Issues Found: 87
B	84	Hacker Chatter Issues Found: 87	A	95	IP Reputation Issues Found: 87
A	95	Leaked Information Issues Found: 87	A	95	Network Security Issues Found: 87
A	95	Patching Cadence Issues Found: 10	A	95	Social Engineering Issues Found: 87

Vendor X - High Risk

An alternative story:

- How many breaches have been reported to a regulator?
- Have they reported a breach but not told us?
- Did they report something different than what was shared with us?
- **How much did their breaches cost them and/or other parties?**

Which story is better?

A 💩 story:

- Vendor X has a risk rating of A-
- They have websites that don’t enforce HTTPS
- The vendor is mentioned in an unnamed forum on the dark web
- The range of industry losses is $500k-7m

A 😎 story:

- Vendor X reported three breaches last year
- They informed us of 1/3
- They lost the data due to phishing
- The total loss amount was $20m USD

We can answer other questions too…

A 😎 story:

- **Likelihood:** How many hospitals reported a breach last year?
- **Impact:** What was actual average cost of a breach for a hospital

Impact

x Likelihood

Risk

😎

Our Checklist

Turn mistakes into opportunities!

- Didn’t address business needs
- **Get the right data**
- Lack of support
- Lack of narrative
- Made it easy to say, “No”

Common misconceptions

Statement: We don’t have enough data!

Blackjack

How do we win?

- We do not have perfect information about the deck.
- **Are there systems for making good decisions without complete information?**

Statement:

Reputational damage can’t be measured!

Susie’s Lemonade

Maybe awesome, maybe not!

- Her competitor Little Johnny tells the whole neighborhood that Susie puts rat poison in her lemonade.
- **How would we measure reputational damage to Susie?**

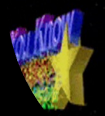
Influencing the influencer

breachsiren

Question:

Have you ever heard someone ask for less resources?

Things to remember…



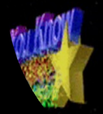
1. Acknowledge the business needs first
2. Identify the personal impact to your leader
3. Know when your request may be invalid or poorly timed
4. State your willingness to be a good team player
5. Help with prioritization

Establishing Allies

Who else is impacted?

- What's the impact of your work on finance, legal and the business?
- Are you a bottleneck for others?
- Has your company had a prior audit finding for TPRM?

Things to remember…



1. Ask your peers how they're impacted
2. Have them advocate for you directly or indirectly (testimonial)
3. Craft your pitch together
4. **Solve your problem by solving theirs first**

Our Checklist

Turn mistakes into opportunities!

- Didn’t address business needs
- **Wrong data**
- **Gather support**
- Lack of narrative
- Made it easy to say, “No”

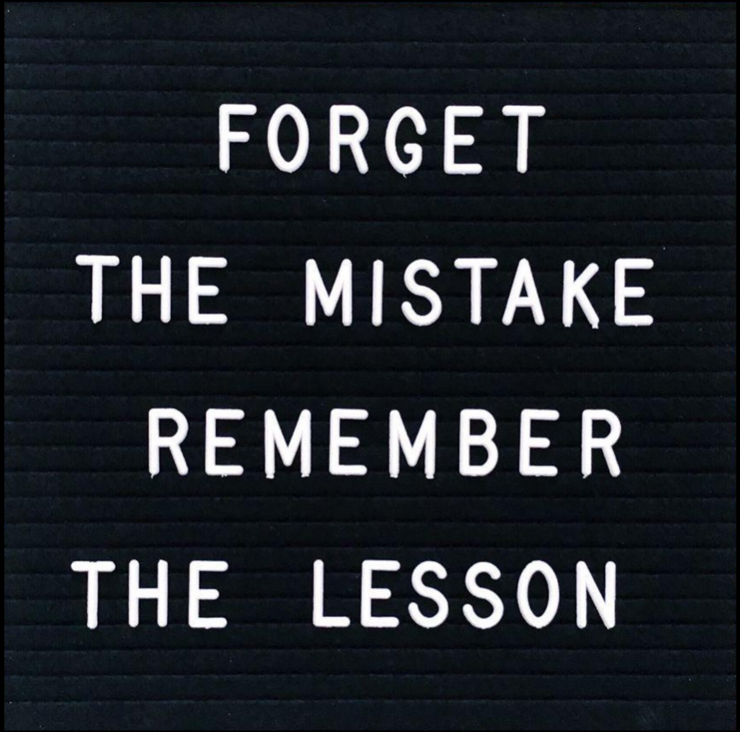
Getting it right the second time!

breachsiren

Our Checklist

Turn mistakes into opportunities!

- Didn’t address business needs
- **Wrong data**
- Lack of support
- Craft your narrative
- **Make it easy to say, “Yes”**



FORGET
THE MISTAKE
REMEMBER
THE LESSON

“I understand the board is concerned our audit deficiencies may impact our share price so they’ve been putting a lot of pressure on you to find a resolution.”

— Bob Rossi

Bob’s Pitch

He presented…

- How he and his peers can address the audit deficiencies of the CISO
- The financial impact of the riskiest most critical vendors for small hospitals in his region with the likelihood of occurrence

Short Hills Hospital

An alternative story:

- Their vendor had a breach of their patient data
- They were also fined by US Department of Health for lack of adequate risk management practices according to the resolution agreement
- The total loss amount was $20m USD

Bob's Pitch

He ended his pitch with three options...

- **Good:** Are we open to accepting TPRM risk so we can put it on-hold. That would let me focus my full attention on the audit?
- **Better:** Should we automate our monitoring of low risk vendors for $45k and spend that time on audit response?
- **Best:** Can we hire a junior third party risk management analyst at $75k, I'll train that person so that I can help with the audit?

“I’ve discussed this plan with account management and they would like to know if we’re willing to accept the risk and put TPRM on-hold this year as it’s a big bottleneck for them.”

— Bob Rossi

The Result

The CISO says…

“Thanks for this. Account Management reached out to me already. I’m not willing to accept the risk but I’d like to learn more about the other options you presented.

Our Checklist

Turn mistakes into opportunities!

- □ Address business needs
- □ Get the right data
- □ Gather support
- □ Craft your narrative
- □ **Make it easy to say, “Yes”**

> “CISOs need to translate the cybersecurity request for funds into the language of the rest of the organization”
>
> — Doug Hubbard, author of “How to Measure Anything in Cybersecurity”

Solution

Source: https://www.youtube.com/watch?v=bYjPmptlc14

What Have We Learned?

1. Speak the language of the business

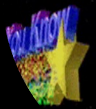
1. Build compelling stories about your work

2. Made a “perfect” pitch for budget

Recommendations & Tools

breachsiren

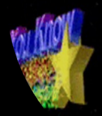
Recommendations…



- For communications & relationship building:
  - *Radical Candor* by Kim Scott
  - *How to Win Friends* by Andrew Carnegie
  - *Influence* by Robert Cialdini
  - MEDDIC Sales Qualification Framework

- For storytelling:
  - *How to Tell a Story* by Scott Simon (NPR)
  - Why Storytelling Works: The Science

Recommendations…

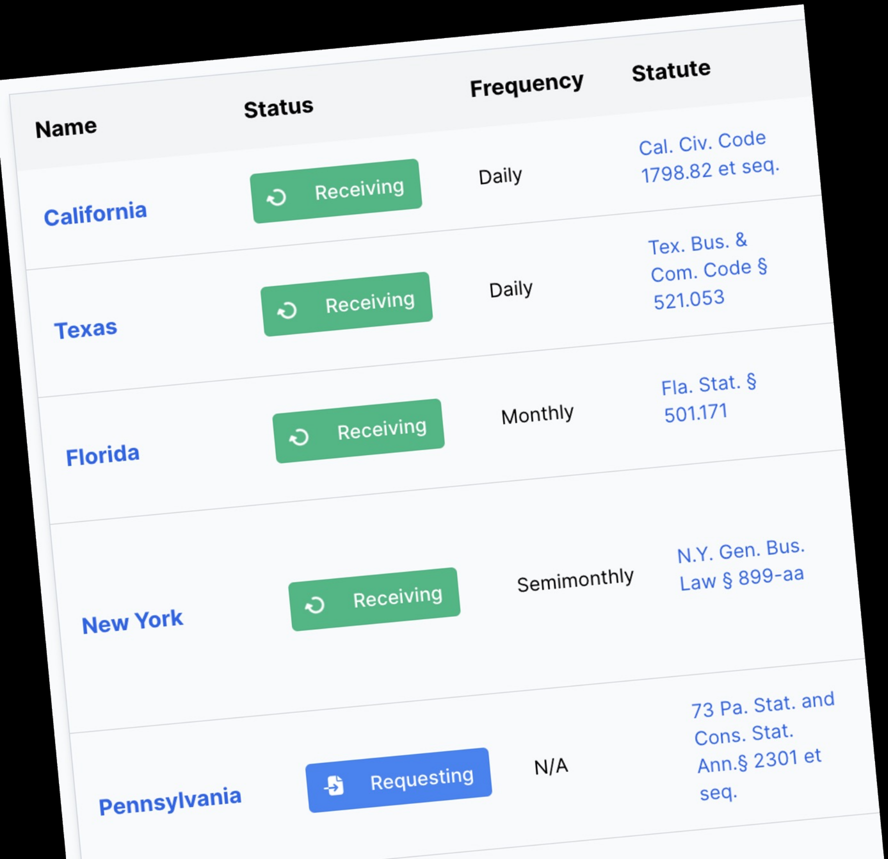


- For cyber loss data:
  - Verisk, IHS Markit, Zywave, breachsiren.com

- For breach notification data:
  - Vcdb, breachsiren.com

- Risk quantification:
  - “How to Measure Anything in Cybersecurity Risk” by Doug Hubbard
  - *FAIR Blog: Shopping for Cyber Loss Data* by Allison Seidel

What We’re Doing At BreachSiren

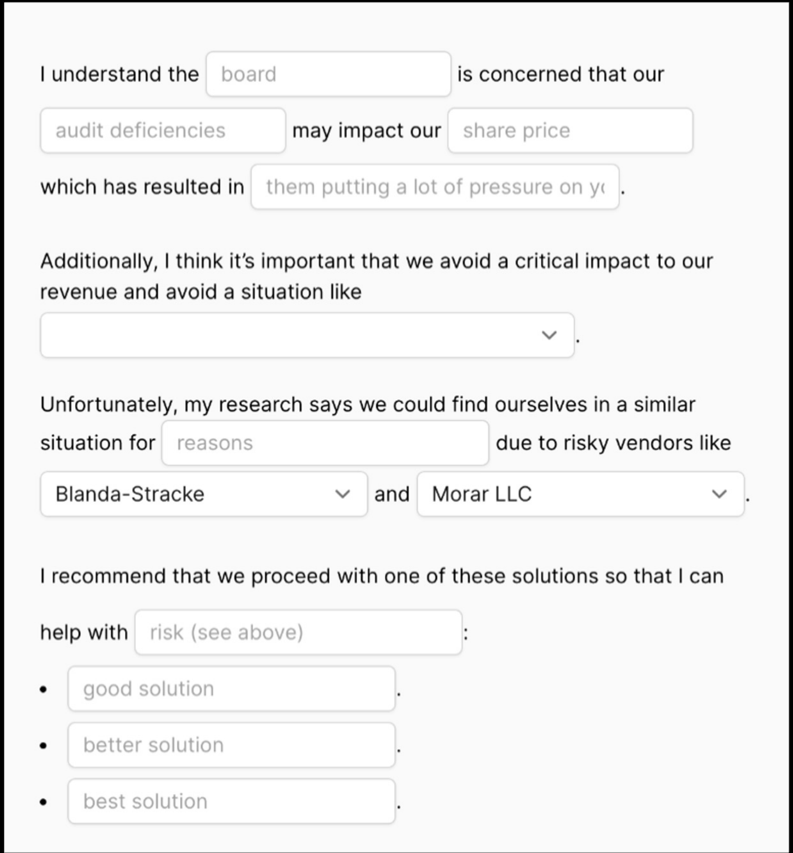


Name	Status	Frequency	Statute
California	Receiving	Daily	Cal. Civ. Code 1798.82 et seq.
Texas	Receiving	Daily	Tex. Bus. & Com. Code § 521.053
Florida	Receiving	Monthly	Fla. Stat. § 501.171
New York	Receiving	Semimonthly	N.Y. Gen. Bus. Law § 899-aa
Pennsylvania	Requesting	N/A	73 Pa. Stat. and Cons. Stat. Ann.§ 2301 et seq.

- Learn what your vendors are reporting to federal, state and industry regulators
- Thirty-six sources include:
  - HHS, OCC, HIBP, FTC, *SEC (December)
  - CA, TX, FL, NY, IL, OH, NC, MA, NJ, MD, DE, ME…
- Downloadable audit reports

breachsiren

What We’re Doing At BreachSiren



I understand the [board] is concerned that our [audit deficiencies] may impact our [share price] which has resulted in [them putting a lot of pressure on y].

Additionally, I think it’s important that we avoid a critical impact to our revenue and avoid a situation like

[⌄].

Unfortunately, my research says we could find ourselves in a similar situation for [reasons] due to risky vendors like [Blanda-Stracke ⌄] and [Morar LLC ⌄].

I recommend that we proceed with one of these solutions so that I can help with [risk (see above)]:

- [good solution].
- [better solution].
- [best solution].

- Know how much vendors have paid in fines and settlements
- Storyteller Prompts
    - Budget Requests
    - Team Value

breachsiren

“You’re not a cost center, you’re a value center. Your value is helping your senior leaders sleep better at night.”

— Tom Garrubba, Echelon Risk + Cyber

breachsiren

Breach Intelligence Platform

Real data, right now.

Fin

breachsiren.com