

Where Governance and Risk Management Align for Impact

Hard Numbers for Hard Truths: Quantifying Third-Party Breach Risk Through Data Governance

Christine Dewhurst, B.Math, CPA, CISA
Dr. Thomas Lee, BS Physics & EE, MS, PhD Biophysics

DISCLAIMER

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of ISACA or any other co-sponsors. ISACA does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2026 ISACA or its affiliates. The ISACA logo and other trademarks are proprietary. All rights reserved.

Who we are….



Christine Dewhurst

Partner, NSC Tech

CISA, CPA,
B Mathematics,
University of Waterloo
Christine.Dewhurst@nsctech.com



Dr. Thomas Lee

CEO, VivoSecurity

BS Physics & EE
MS, PhD Biophysics
University of Chicago
ThomasL@vivosecurity.com



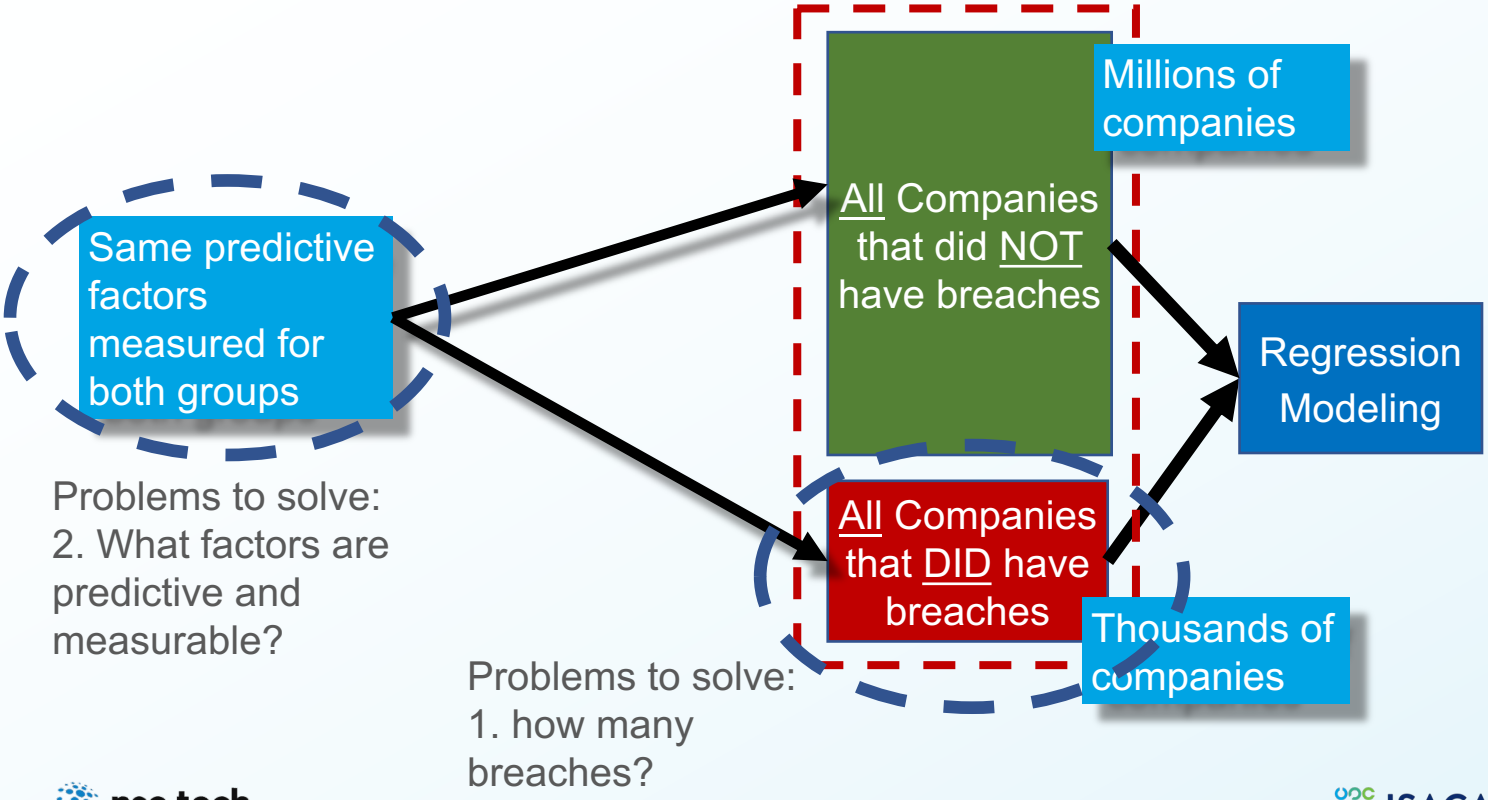
Learning Objectives

1. Learn and explore the math behind every organization – everyone has a measurable exposure curve
2. Governance maturity scales with N
3. How to calculate your organizations and your risk of a data breach...you can’t reduce risk you don't know

How to develop a model for probability

Finding the differences between all companies that did and did not experience data breach

We can use regression modelling



How we solved problem 1

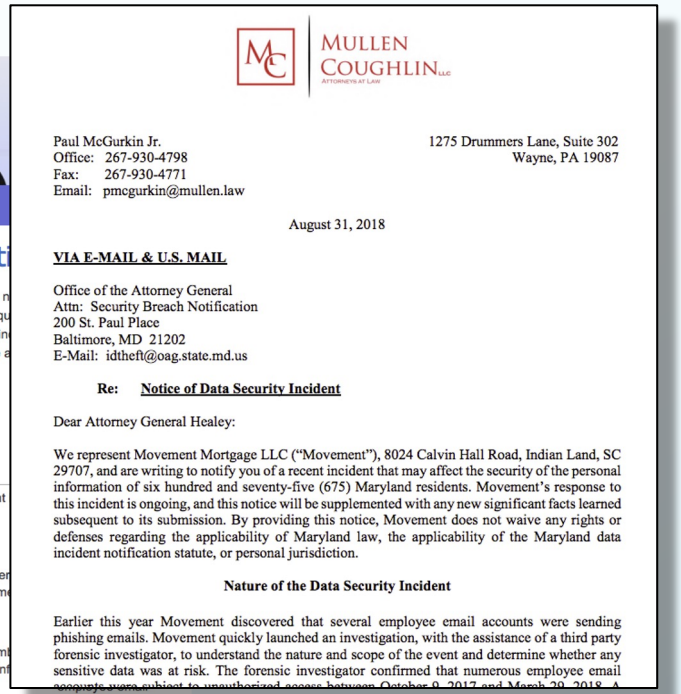
How many data breaches are there?

Maryland is a magic source of data

Company	State	Marylanc	Incident	Data	3rd Party
Ransom Memorial Hospital	KS	2	MO	PHI	No
HealthEquity, Inc. (attachec	UT	46	MO	PHI	Yes
Aflac	GA	78	MO	PHI	Yes
Jemison Internal Medicine,	AL	1	MO	PHI	No
Ohio Living	OH	1	MO	PHI	No
Flexible Benefit Service Co	IL	21	MO	PHI	No
Serene Sedation, LLC	MD	4327	MO	PHI	Yes
DecisionHR Holdings, Inc.	FL	2	MO	PHI	Yes
Michael Gruber, DMD, PA	NJ	14	MO	PHI	No
Arkansas Children's Hospit	AR				
Ebbs, Roberts, Head & Da	NM				
Cambridge Dental Consulti	NV				
Ruben U. Carvajal, MD	NY				
RISE Wisconsin, Inc	WI	2	MO	PHI	No
Dr. Robert Carpenter	TX	3	MO	PHI	No
SureFire, LLC	CA	39	MO	CHD	Yes
Capital Integration Systems	NY	181	MO	PFI	No
The Coca-Cola Company	GA	14	MO	PFI	No
Stein Eriksen Lodge Hotel	UT	5	MO	PII	No
Authentic Recovery, LLC	CA	3	MO	PHI	No
Securus Technologies, Inc.	TX	25	MO	PII	No
The Childrens Mercy Hospi	MO	6	MO	PHI	No

Companies with headquarters
Across all 50 states





We discovered we can predict by state

State	Breaches Reported to Maryland
	Observed
AK	5
AL	10
AR	3
AZ	7
CA	99
CO	15
CT	8
DC	17
DE	4
FL	32
GA	23
IA	5
ID	4
IL	45
IN	15
KS	9
KY	5
LA	2
MA	21
MD	67
MI	11
MN	13
MO	9

State	Breaches Reported to Maryland
	Observed
MS	2
MT	3
NC	22
NE	3
NJ	27
NM	1
NV	1
NY	58
OH	28
OK	3
OR	10
PA	40
RI	4
SC	7
TN	15
TX	55
UT	9
VA	30
VT	2
WA	7
WI	13
WV	2

GDP predicts breaches

State	Breaches Reported to Maryland		GDP	Distance to Maryland	State	Breaches Reported to Maryland		GDP	Distance to Maryland
	Observed	Predicted				Observed	Predicted		
AK	5	-3	51,479	4,273	MS	2	3	109,375	1,018
AL	10	8	211,196	780	MT	3	-1	47,079	1,947
AR	3	4	[illegible]2,704	1,050	NC	22	21	540,497	437
AZ	7	9	[illegible]6,446	2,277	NE	3	3	119,588	1,153
CA	99	97	[illegible]7,601	2,625	NJ	27	26	602,069	179
CO	15	10	345,233	1,663	NM	1	1	94,211	1,861
CT	8	13	264,510	253	NV	1	2	158,302	2,408
DC	17	12	72,461	38	NY	58	62	1,606,601	188
DE	4	13	135,768	74	OH	28	25	645,747	413
FL	32	35	[illegible]76,386	744	OK	3	5	188,632	1,319
GA	23	21	[illegible],608	664	OR	10	4	227,155	2,808
IA	5	6	[illegible],930	1,020	PA	40	34	756,269	101
ID	4	-1	72,294	2,379	RI	4	5	59,306	372
IL	45	30	822,540	702	SC	7	9	221,690	570
IN	15	14	352,273	579	TN	15	13	349,569	703
KS	9	4	159,108	1,254	TX	55	57	1,645,136	1,416
KY	5	8	202,175	610	UT	9	3	164,917	2,086
LA	2	8	235,960	1,126	VA	30	24	510,586	147
MA	21	22	542,979	412	VT	2	3	32,545	478
MD	67	65	399,538	0	WA	7	15	524,323	2,764
MI	11	19	508,905	628	WI	13	12	321,373	789
MN	13	12	350,179	1,109	WV	2	5	74,047	365
MO	9	10	303,763	1,060					

Technology

Agriculture

Oil

Problem 1, SOLVED!

State	Breaches Reported to Maryland		GDP	Distance to Maryland
	Observed	Predicted		
AK	5	52	51,479	0
AL	10	58	211,196	0
AR	3	55	122,704	0
AZ	7	62	326,446	0
CA	99	151	2,797,601	0
CO	15	63	345,233	0
CT	8	60	264,510	0
DC	17	53	72,461	0
DE	4	55	135,768	0
FL	32	86	976,386	0
GA	23	71	563,608	0
IA	5	57	183,930	0
ID	4	53	[illegible]	0
IL	45	80	822,540	0
IN	15	63	352,273	0
KS	9	56	159,108	0
KY	5	58	202,175	0
LA	2	59	235,9[illegible]	0
MA	21	70	542,9[illegible]	0
MD	67	65	399,5[illegible]	0
MI	11	69	508,9[illegible]	0
MN	13	63	350,1[illegible]	0
MO	9	61	303,7[illegible]	

State	Breaches Reported to Maryland		GDP	Distance to Maryland
	Observed	Predicted		
MS	[illegible]		109,375	0
MT	[illegible]		47,079	0
NC	[illegible]		540,497	0
[illegible]	[illegible]		119,588	0
NJ	[illegible]		602,069	0
NM	[illegible]		94,211	0
NV	1	56	158,302	0
NY	58	108	1,606,601	0
[illegible]	28	74	645,747	0
[illegible]	3	57	188,632	0
[illegible]	10	59	227,155	0
[illegible]	40	78	756,269	0
[illegible]	4	53	59,306	0
[illegible]	7	59	221,690	0
[illegible]	[illegible]	63	349,569	0
TX	55	110	1,645,136	0
UT	9	57	164,917	0
[illegible]	[illegible]		[illegible]86	0
[illegible]	[illegible]		[illegible]45	0
[illegible]	[illegible]		[illegible]23	0
[illegible]	[illegible]		[illegible]73	0
[illegible]	[illegible]		[illegible]47	0

Set distance to zero

Forecast total breaches for state

Total breaches: 2957

Reported to Maryland: 771

Data breaches are so predictable, we can predict them based solely upon economic activity

VivoSecurity nsc tech ISACA IIA

How we solved problem 2

What predictive factors can be measured for all companies

7 Factors that predict data breach & size

and can be measured for all companies

GRC 2026 Conference

People Input Factors	Proxy For…	Impact	Large Breach – > 1M records (7)	Small Breach - > 1M records (7)
CISA / IT (1)	Size of Internal Audit (3rd-line) Certified Information Systems Auditor	Decrease Probability	Very strong, no diminishing return	Strong but, diminishing return
CISSP / IT (2)	Size of InfoSec (2nd-line) Certified Information Systems Security Professional		Very strong, no diminishing return	Strong but, diminishing return
MCSA / IT (3)	Vendor Certifications (1st-line) Microsoft Certified Solutions Associate		Weak	Modest, diminishing return
RHCE / IT (4)	Use of Linux (1st-line) Red Hat Certified Engineer	Increase Probability	Moderate	Moderate
IT Employees (5)	Technical services that require protection		Very Strong	Very Strong
Employees (6)	Attack surface. Accidents, lost devices, malicious insiders & employee turnover		Moderate	Moderate

VIVO VivoSecurity nsc tech ISACA IIA

Modelling observations

- Many other certifications were tried and found to be predictive by themselves, but did not increase the accuracy when combined with CISSP (when collinear or correlated remove from model)
- CISA was different from other cybersecurity certifications, Internal Audit function is key
- Counting employees with certifications was better than simply a count of people in cybersecurity.

An analogy: predicting family size



We might find the amount of milk is a predictor

We might find cereal is also.

But adding cereal does not improve accuracy

We might find diapers is also a good predictor.

Adding diapers is more accurate

This is like the CISSP

Perhaps this is measuring older children

This is like other certs – important but don't improve accuracy

This is like CISA, measuring something different from CISSP

capturing children not yet drinking milk

Best Model Analogy: predicting family size

There are lots of other things in the cart too! These other things are needed for a healthy family.

But all we need to measure is the milk and diapers.

Family Size



What I saw that Dark, Snowy Night…7 Factors



1. Each Company View

By leveraging the model, the probability of a company's data breach is known.

2. Third Party Data Breach View

By leveraging the model, the probability of third-party data breach can be known. Add the up the more the risker!

3. Third Party Data Sharing View

Why are we sharing data with companies that have no CISA & CISSP as they have a higher probability of a data breach?

Governance Maturity Scales with ‘N’

Largest predictor of a Breach
is the number of Third Parties that have your data

Polling Question One

How confident are you that your organization maintains a complete and accurate inventory of third parties that have sensitive data access?

1. Fully confident, comprehensive and validated
2. Largely confident, minor gaps possible
3. Moderately confident, known gaps exist
4. Limited confidence, significant uncertainty
5. No confidence, inventory likely incomplete

Top NA Credit Union - Number of Vendors

Top 10 of 69 Vendors & Their Employee Count

Vendor	Employees
Company 12	74,241
Company 16	60,043
Company 122	59,484
Company 25	44,096
Company 90	17,221
Company 30	14,284
Company 109	9,336
Company 3	10,665
Company 43	7,512
Company 94	6,057

- Biggest risk is number of vendors - Data Surface & Principle of Least Privilege
- There are 69 vendors with 1M+ customer records. This is a major exposure! Why is it so high? Confirm this is correct and if so, action accordingly.
- Village, City, State, Country

“You cannot Breach IT if you do not Share IT”

What is included?	What is not included?
• CRM Platform • Banking Platform • Credit adjudication • Identity & Access management • API’s • HR Platform • Credit Score Checks • Share Management	• Data encrypted in transit/in use or obfuscated • Office supply company • Paper shredder

Customer Insights

- First engagement many organizations do not know how many vendors data is shared
- Maturity is correlated to size and Industry regulation
- Many smaller companies than larger

How to calculate your organizations and your risk of a data breach

You cannot reduce risk you do not know

Likelihood of Data Breach



Customer Insights

- Over 100K companies evaluated, normal distribution
- Add them up! Each vendor has a probability of a data breach
- Average is 0.07%
- No bad vendor
- Over 0.17% is a Tail Vendor
- Probability is N * 0.07%

Polling Question Two

Would you be comfortable sharing your customer data with a third party that has no certified cybersecurity professionals or clearly inadequate staffing?

1. Yes
2. Probably
3. Unsure
4. Probably not
5. No

Top 10 NA Credit Union - No CISA or CISSP

GRC 2026 Conference

Sample 10 of 150 vendors with no CISA or CISSP's

Vendor	Employees
Company 1	4,765
Company 2	1,079
Company 6	674
Company 11	526
Company 13	522
Company 14	454
Company 15	451
Company 18	389
Company 20	369
Company 21	341



Of your 150 vendors, there are 59 vendors with no CISSP's, and 68 vendors with no CISA. Is the Credit Union comfortable with this?



Appear to have no Cyber Security or Internal Audit function.



Village, City, State, Country

ISACA | IIA

How many CISA's and CISSP's should a Third Party must have to share data?

People Centric Actuarial Tables

7 Factors that predict data breach & size

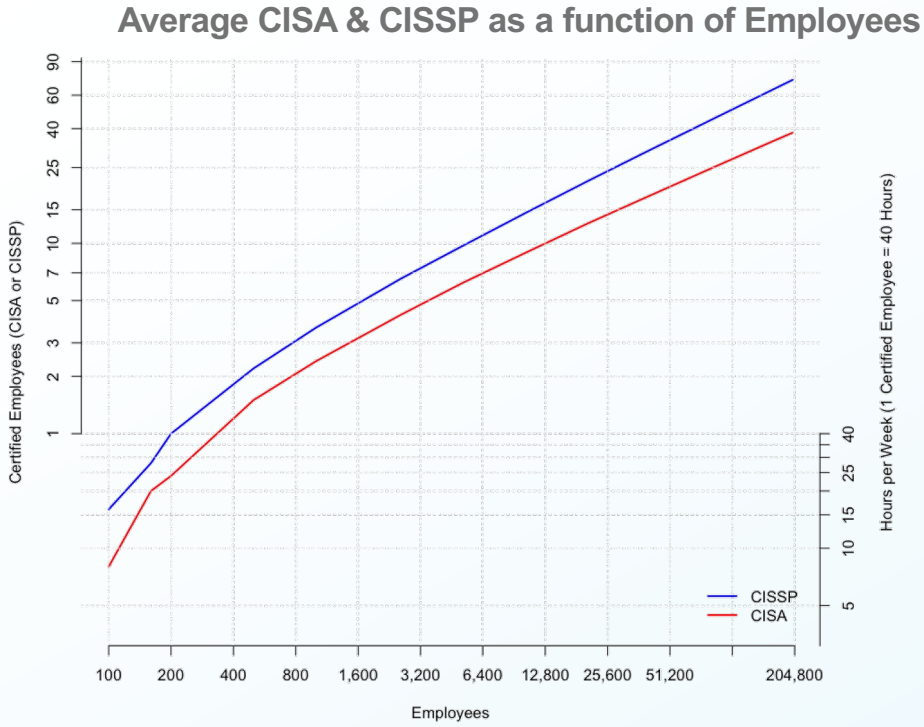
and can be measured for all companies

GRC 2026 Conference

People Input Factors	Proxy For…	Impact	Large Breach – > 1M records (7)	Small Breach - > 1M records (7)
CISA / IT (1)	Size of Internal Audit (3rd-line) Certified Information Systems Auditor	Decrease Probability	Very strong, no diminishing return	Strong but, diminishing return
CISSP / IT (2)	Size of InfoSec (2nd-line) Certified Information Systems Security Professional		Very strong, no diminishing return	Strong but, diminishing return
MCSA / IT (3)	Vendor Certifications (1st-line) Microsoft Certified Solutions Associate		Weak	Modest, diminishing return
RHCE / IT (4)	Use of Linux (1st-line) Red Hat Certified Engineer	Increase Probability	Moderate	Moderate
IT Employees (5)	Technical services that require protection		Very Strong	Very Strong
Employees (6)	Attack surface. Accidents, lost devices, malicious insiders & employee turnover		Moderate	Moderate

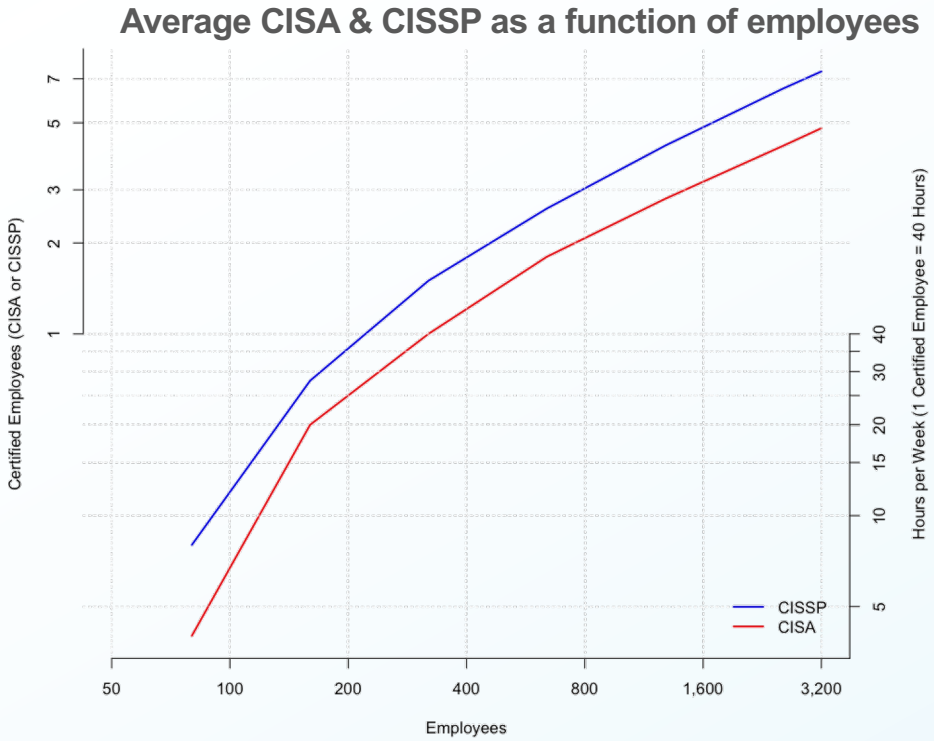
VIVO VivoSecurity nsc tech ISACA IIA

People Centric: Overcoming SOC2 Overload



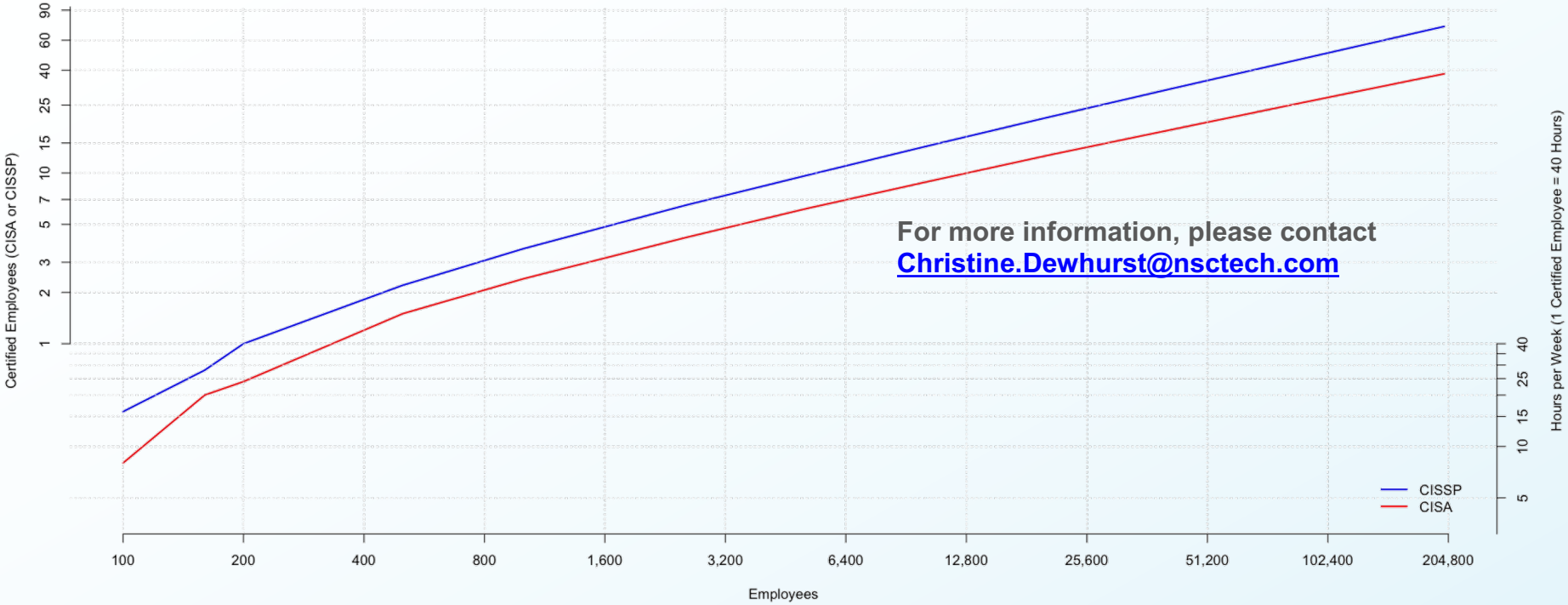
8 Large Business'	Emp (6)	CISA (1)	CISSP (2)
Car rental	86,885	10	20
Insurance	60,043	36	25
Financial tech.	51,591	78	159
Insurance	57,022	48	23
Auto insurance	44,096	28	52
Equifax	20,720	39	85
Cloud-based HR	10,665	12	7
Financial technology	10,712	16	30

People Centric: Overcoming SOC2 Overload



11 Small Business	Emp (6)	CISA (1)	CISSP (2)
Federal Reserve Bank of SF	2,928	31	32
Financial tech services	1,646	1	1
Financial service tech	770	0	1
Mortgage closure tech	723	1	3
Platform technologies	674	0	0
Collection service	526	0	0
Mortgage services platform	522	0	0
Auto buying service	369	0	0
Financial statement services	196	0	0
Payment mgm't solutions	71	0	0
Law firm	41	0	0

People Centric Actuarial Table



Learning Objectives

1. Learn and explore the math behind every organization - everyone has a measurable exposure curve
2. Governance maturity scales with N
3. How to calculate your organizations and your risk of a data breach...you can’t reduce risk you don't know

Want to continue the conversation….

GRC 2026 Conference

ISACA

SJSU COLLEGE OF INFORMATION, DATA AND SOCIETY

Information Risk Management Laboratory

Center for Artificial Intelligence and Cybersecurity



Articles & Papers

- ISACA Article Submitted, ***The Risk That Nobody Owns: A Human Capacity Framework for Governing Aggregate Third-Party Breach Exposure,*** 2026
- White Paper: Calculating the Probability of a Third-Party Data Breach, 2025
- Assessing the Effectiveness of Third-Party Risk Management using Quantitative Models, 2022

VIVO VivoSecurity nsc tech ISACA | IIA

GRC 2026 Conference

Thank you!

We value your feedback, please complete the session survey and share your thoughts with us.

VIVO VivoSecurity nsc tech ISACA IIA