Pearl Meyer MainData GROUP

Should Cybersecurity Metrics be Linked to Executive Pay?

Prepared for WorldatWork

09/26/2024

Adam Kahle
Principal
adam.kahle@pearlmeyer.com
212.407.9593

Brooke Fernandez
VP & General Manager, MDG
brooke.fernandez@pearlmeyer.com
408.762.5274

Introducing Today's Speakers

Adam Kahle

Principal

- Adam is a Principal with the New York office of Pearl Meyer. He has 20 years of combined experience in corporate compensation and consulting. Adam's consulting experience covers a broad range of industries including business services, consumer products, education, energy, financial services, government, healthcare, industrial manufacturing, technology, media and telecommunications, private/joint-venture, retail, transportation, and utilities.
- Previously, Adam served as Head of Global Executive Compensation at Takeda Pharmaceuticals and was an executive pay consultant at Korn Ferry.
- He holds a bachelor's degree from Saint Olaf College and a master's degree in Human Resources and Industrial Relations from the Carlson School of Management.

Brooke Fernandez

General Manager, Main Data Group

- Brooke is the General Manager of Main Data Group (MDG), a provider of executive compensation benchmarking and corporate governance analytics. The MDG team continues to innovate upon a comprehensive proxy database and offers custom research services to top-tier companies and Executive Compensation firms worldwide.
- MDG's mission is to empower executive compensation professionals with meaningful, comprehensive total rewards and corporate governance information through the industry's most cost-effective and easy-to-use data platform.
- She holds a bachelor's degree from UCLA and a master's degree from the Stanford Graduate School of Business.

Agenda

01 Case Study: Microsoft Cybersecurity Incident

02 Key Factors Shaping Cybersecurity Governance Practices

03 Market Prevalence of Cybersecurity in Board Responsibilities and Executive Pay Plans

04 Considerations for Incorporating Cybersecurity Metrics in Executive Pay Plans

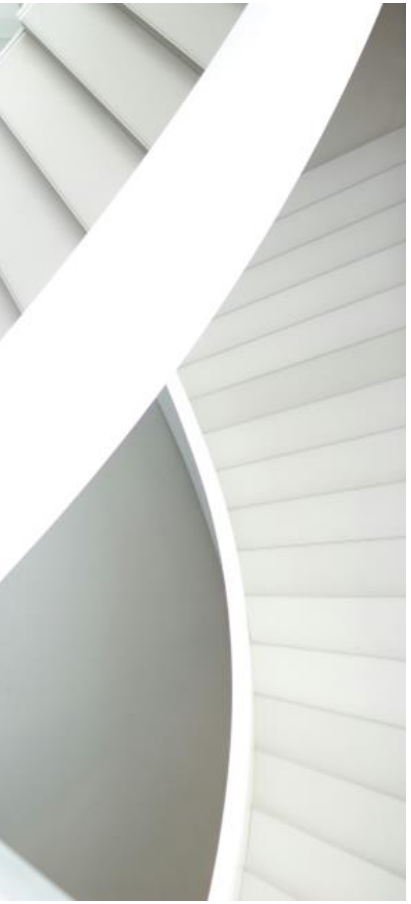
05 Ensuring Cybersecurity Accountability: Key Considerations for Boards and Compensation Committees

06 Roles of Total Rewards Leaders in Advancing Cybersecurity

Broad Reach of Cybersecurity

- Although the title of this presentation includes "Executive Pay", we have focused this presentation more broadly on how all employees, and the Board, can be involved in ensuring protections

Cybersecurity: The Numbers



$10.5tn

Projected 2025 Global Cybercrime Costs[1]

15% y-o-y over a decade

$4.45m

Average Cost of a Data Breach[2]

$15.4m

Average Cost of Insider Threats[3]

Now account for 30% of all data breaches

83%

Phishing Attacks[4]

Percentage of organizations reporting such attacks

79%

Cloud-related Attacks[5]

Percentage of companies experiencing at least one could data breach

3.4m

Cybersecurity Talent Gap[6]

Global shortage of cybersecurity professionals

Sources

1) Cybersecurity Ventures, *2020 Official Annual Cybercrime Report*
2) IBM Security in Partnership with the Ponemon Institution: *IBM Cost of a Data Breach Report (2023)*
3) Ponemon Institute, *Cost of Insider Threats Report (2023)*
4) Proofpoint, *State of the Phish (2023)*
5) Thales, *Cloud Security Report, 2023*
6) (ISC)^2, Cybersecurity Workforce Study, 2023


Pearl Meyer
MainData
GROUP
01
Case Study:
Microsoft
Cybersecurity
Incident

Importance of Cybersecurity

> Cybersecurity is not just about protecting data; it's about protecting the very foundation of our society.

Satya Nadella
Chairman and CEO, Microsoft

Summary of the Microsoft Summer 2023 Cybersecurity Incident

Storm-0558 Background - espionage group linked to the Chinese Government, known for targeting cloud service providers

Incident Overview – Storm-0558 accessed sensitive email accounts, impacting US Gov't officials

Key Failures – company did not detect the breach itself (relied on the Gov't customer to alert them)

Microsoft's Response - Microsoft initiated a full-scale investigation, but company has faced scrutiny for level of transparency, response, etc.

CSRB Recommendations - emphasized the need for stronger cloud security. The report calls for Microsoft and other cloud service providers to implement better logging practices, audit mechanisms, and improved victim notification processes to ensure faster detection and remediation of similar incidents.

Cyber Safety Review Board ("CSRB") Report

+ Provides an in-depth analysis of the cybersecurity incident where the Microsoft Exchange Online mailboxes of 22 organizations, including U.S. government entities, were compromised by a Chinese-linked hacking group called **Storm-0558**

Microsoft’s Response

Company introduced key initiatives to ensure that senior leadership is held accountable for its cybersecurity goals

Security Milestones

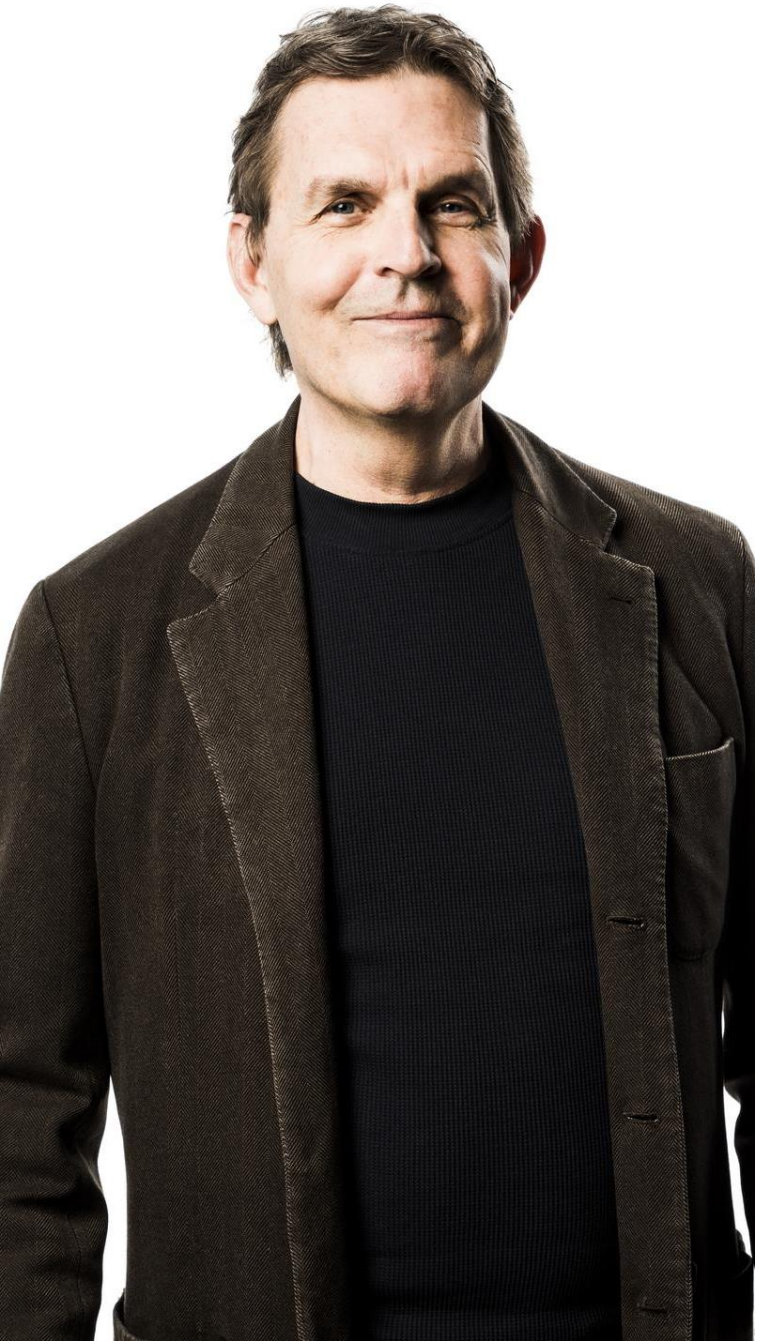
+ Part of the executive team's compensation is now tied to meeting security goals and milestones. This applies to all senior leaders, with cybersecurity becoming a critical component of their performance evaluations starting in fiscal year 2025

Secure Future Initiative

+ Microsoft launched the Secure Future Initiative to address gaps in cybersecurity and increase security across all products. The performance of executives is measured based on their progress in implementing security improvements across six key pillars, including protecting identities, networks, and engineering systems

Regular Reviews

+ Microsoft’s leadership team reviews cybersecurity progress on a weekly basis, and updates are provided to the Board of Directors quarterly. Additionally, this performance is now a key factor in hiring and promotion decisions across the company



> We are making security our top priority at Microsoft, above all else—over all other features(…) We will mobilize the expanded SFI pillars and goals across Microsoft and this will be a dimension in our hiring decisions. In addition, we will instill accountability by basing part of the compensation of the company's Senior Leadership Team on our progress in meeting our security plans and milestones

Charlie Bell
EVP, Microsoft Security

Pearl Meyer
MainData GROUP

Key Factors Shaping Cybersecurity Governance Practices

02

Key Factors Shaping Cybersecurity Governance Practices

Regulatory and Compliance Requirements (e.g., GDPR for the EU and NIST for the USA)

Evolving Threat Landscape (e.g., ransomware, phishing, and nation-state threats)

Board-Level Accountability (cybersecurity is a strategic business issue)

Technological Advancements (e.g., cloud computing, AI, IoT, remote work)

Risk Management and Incident Response (frameworks that prioritize cyber risks)

Collaboration and Information Sharing (between private sector, government, and industry)

Employee Awareness and Training (human error remains a vulnerability)

Third-Party Risk Management (reliance on external partners presents risks)

Why is this important?

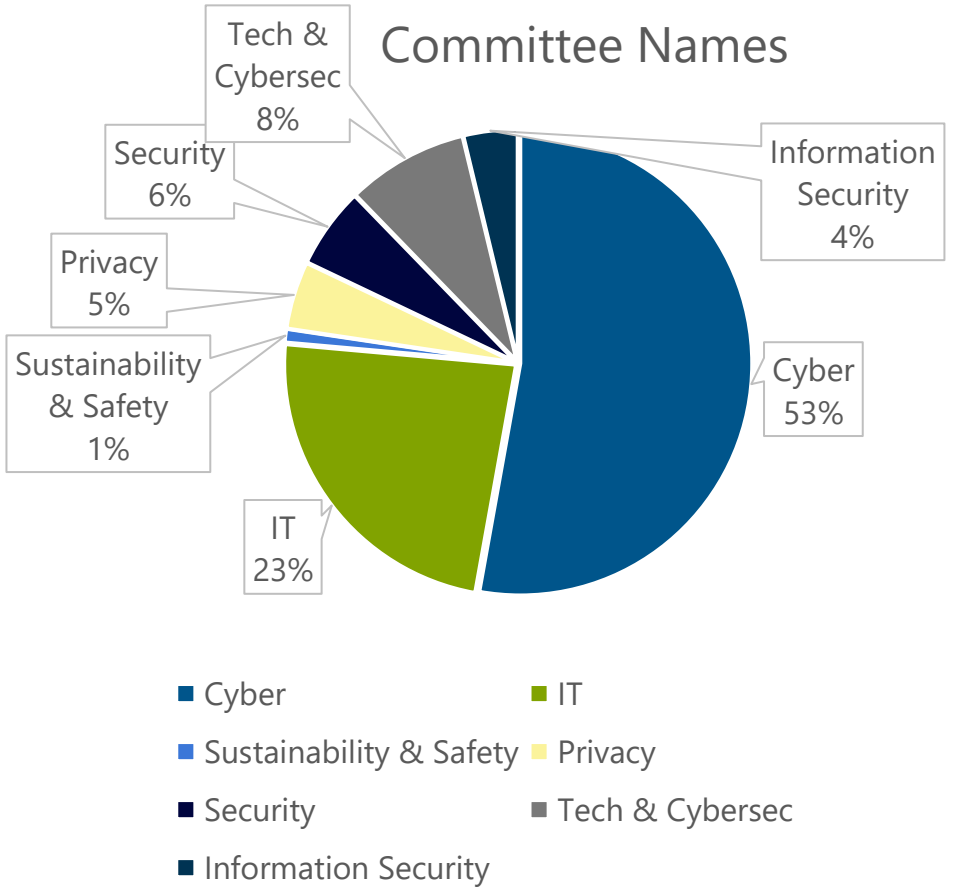
+ These factors collectively shape how organizations implement cybersecurity governance to protect their assets, data, and reputation in an increasingly digital and interconnected world.

Pearl Meyer
MainData GROUP

Market Prevalence of Cybersecurity in Board Responsibilities and Executive Pay Plans

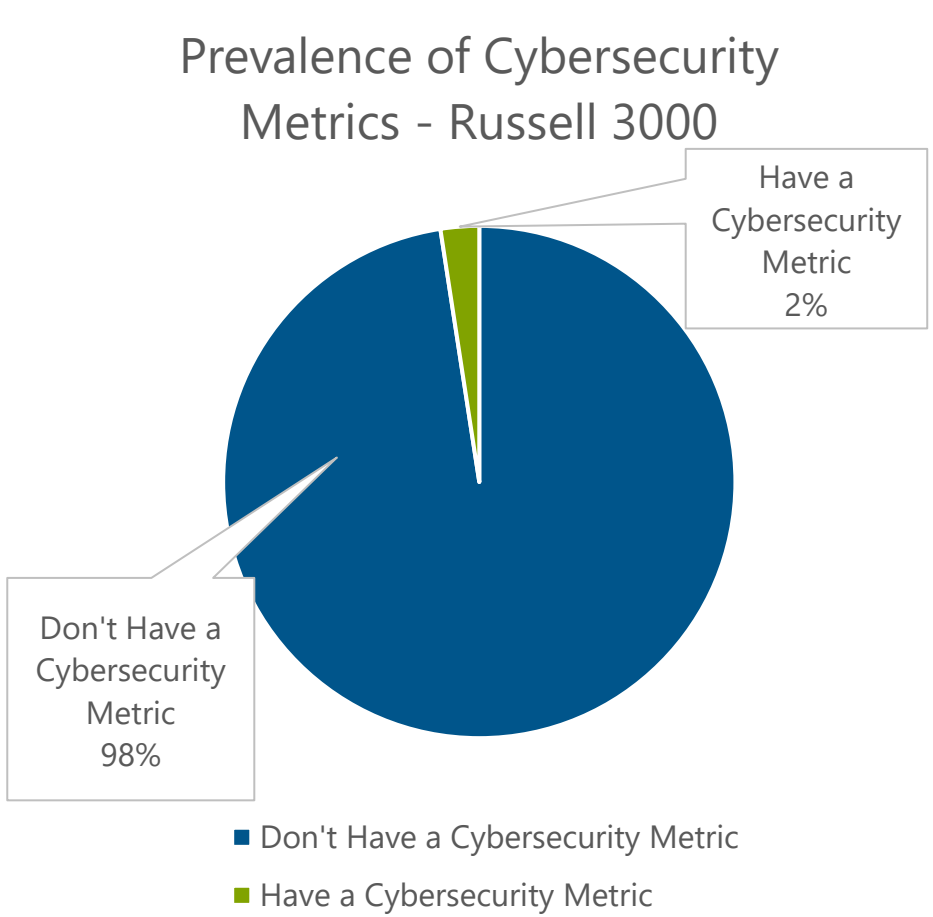
03

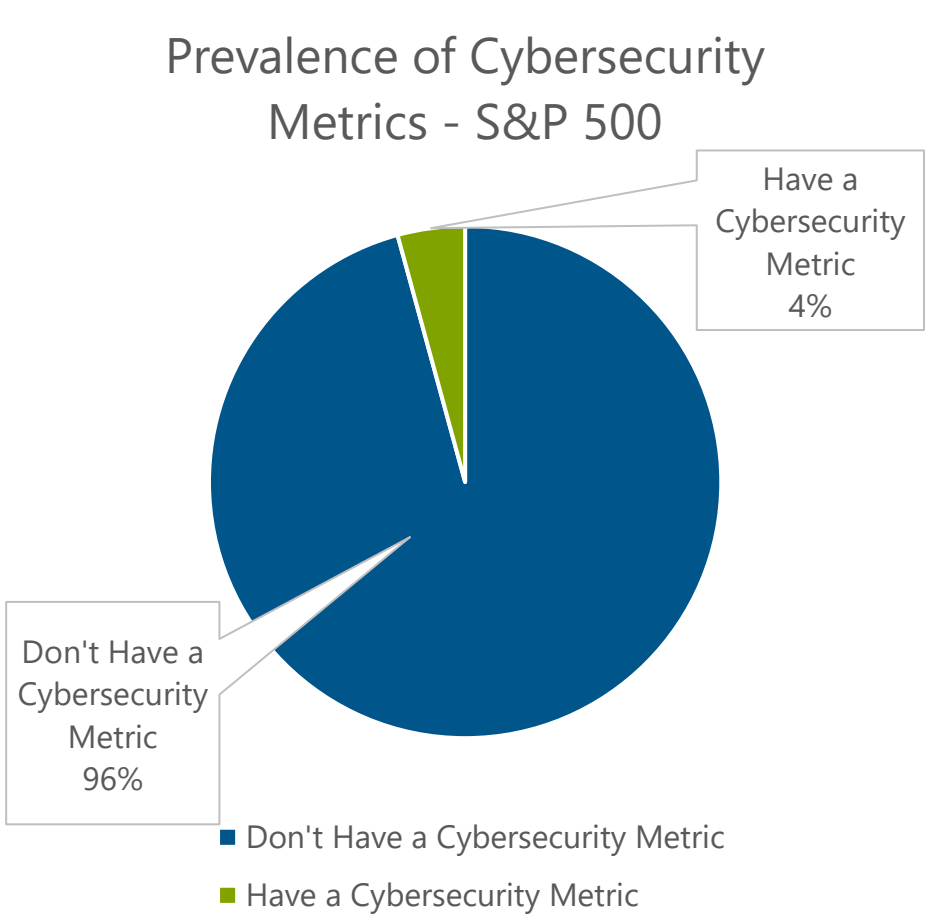
Committees and Subcommittees with Cybersecurity Oversight Responsibility



Cybersecurity Measures Tied to Executive Compensation are a Rarity

We will start to see this shift over the next few years



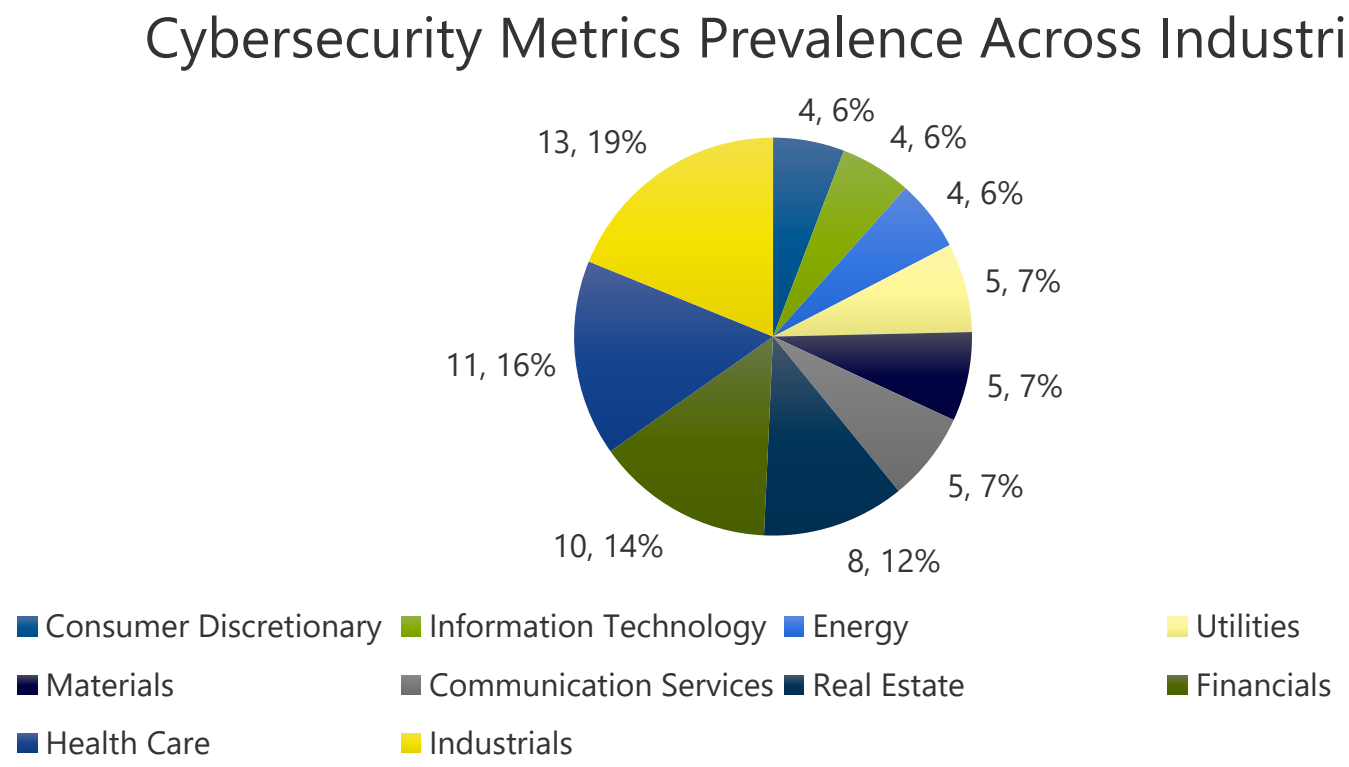


Cybersecurity still emerging as a comp metric

+ We think this is simply because boards are still thinking about/digesting how to manage this risk area

Industrials and Healthcare Industries are the Early Adopters

We will start to see this shift over the next few years

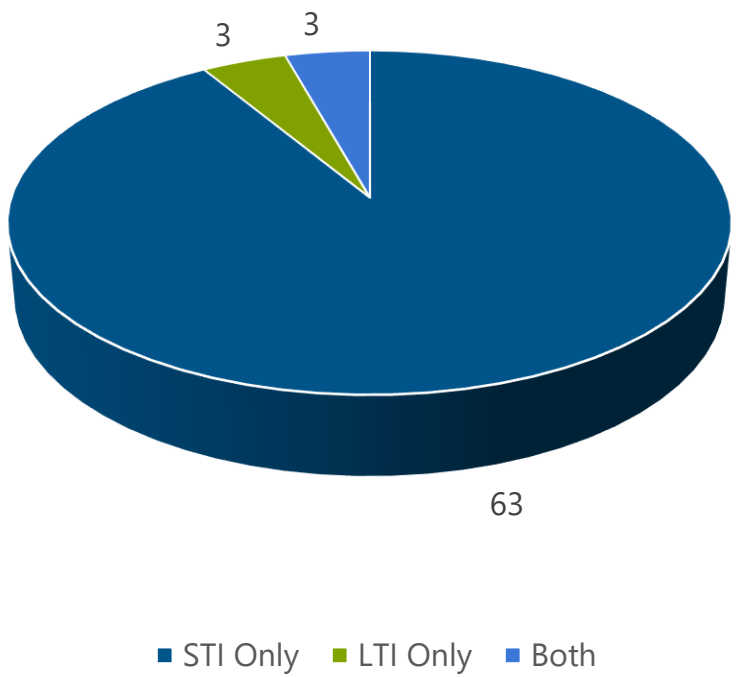


Data Set is Thin

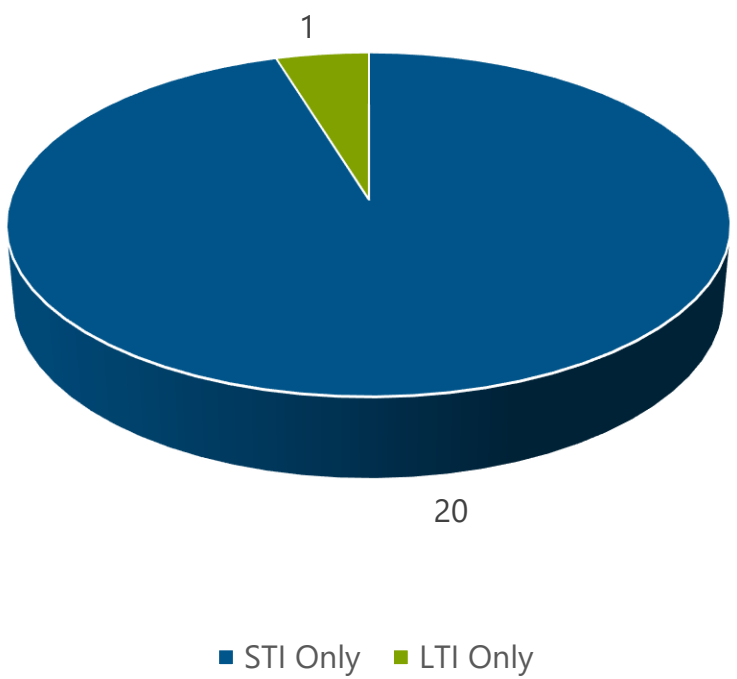
- We were surprised to see this – we anticipated technology /IT to be the clear leader here
- Proxy season is still underway – we have ~ 3 more months of filings
- MSFT hasn't filed yet they file in October typically

Cybersecurity Measures are Predominantly Tied to Short-Term Incentive Plans

Use of STI vs LTI in Cybersecurity metrics across the Russell 3000



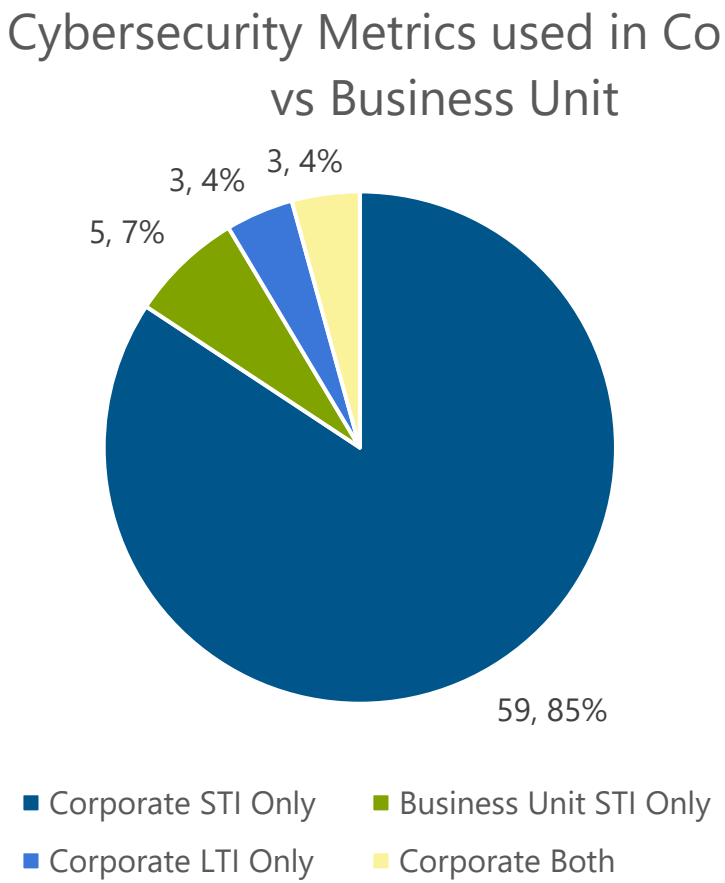
Use of STI vs LTI in Cybersecurity metrics across the S&P 500



Potential Shift to Long-Term?

+ Although most companies are currently using cybersecurity metrics in the STI plan, as cybersecurity should be a long-term focus, we would expect to see more companies implement metrics in LTI plans in the future

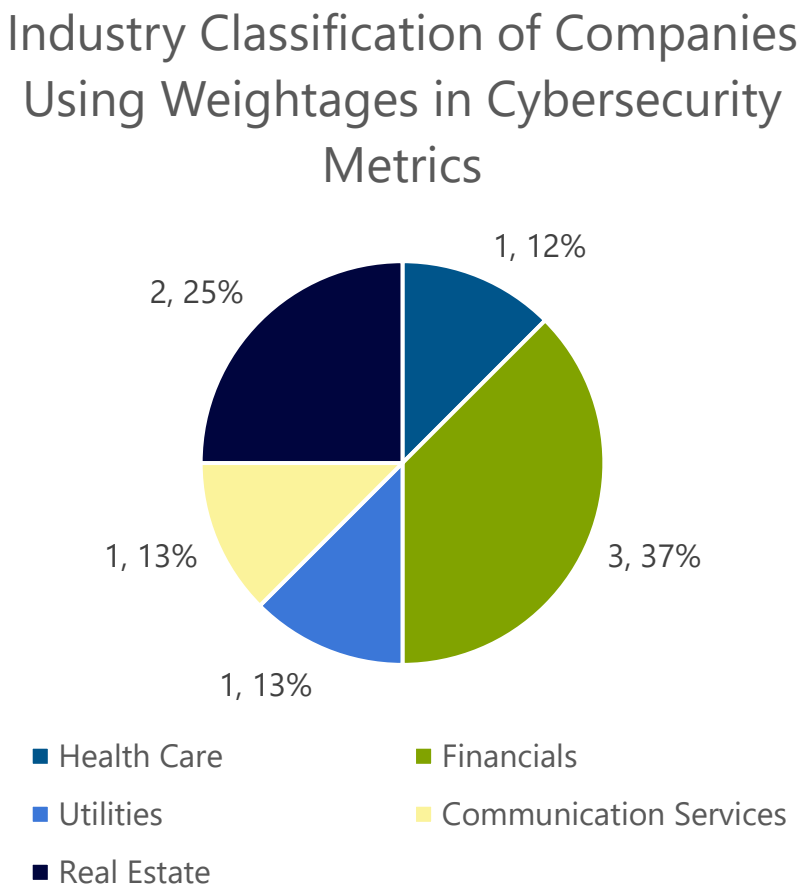
Cybersecurity: Corporate vs. Business Unit Measurement

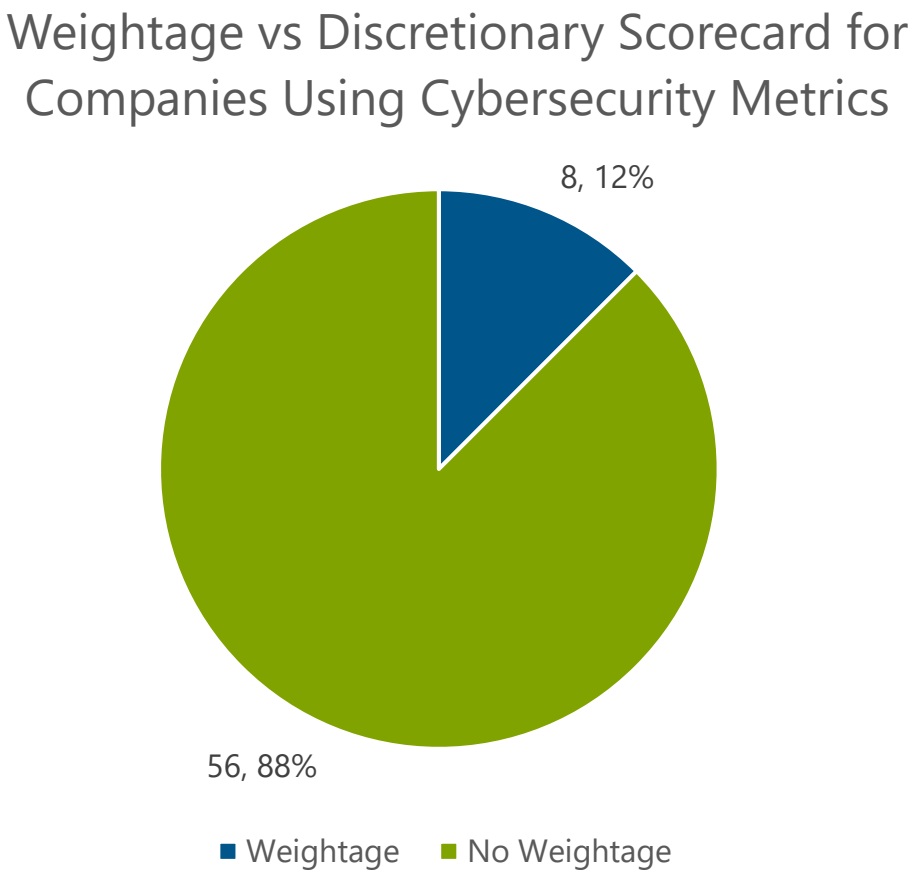


Mostly Corporate

+ Although most companies measure cybersecurity metrics in the STI plan on a corporate-wide basis, some organizations (n=5) measured it at the BU level

Unweighted, Short-Term Incentive Measures are the Currently the Measure of Choice for tying Cybersecurity Measures to Performance






Pearl Meyer
MainData
GROUP
Considerations for Incorporating Cybersecurity Metrics in Executive Pay Plans
04

Incorporating Cybersecurity in Executive Incentive Programs

Top 10 Key Considerations

Aligning Metrics with Business Objectives

Measurable and Clear Cybersecurity Metrics

Balanced Approach Between Risk Management and Innovation

Inclusion of Both Proactive and Reactive Measures

Long-Term Focus

Cross-Departmental Collaboration

Regulatory Compliance and Avoidance of Fines

Incorporating Cybersecurity into Risk Management

Incident Response and Recovery

Transparency and Reporting

An example of using a weighted STI measure to manage cyber risk

Example 1

Annual Incentive Plan

Mr. Funck's target bonus of 115% was not changed in 2023. Based on performance in 2023, Mr. Funck received a bonus in February 2024 which was calculated as follows:

GOAL	2022 RESULTS ACHIEVED	GOAL WEIGHT	2023 GOAL MEASUREMENT			2023 RESULTS ACHIEVED	GOAL SCORE
			THRESHOLD	TARGET	MAXIMUM		
FINANCIAL METRICS(1)							
Adjusted Sales(2)	$44.80B	10%	$40.00B	$40.24B	$40.50B	$40.44B	13.8%
Adjusted Diluted EPS	$5.34	20%	$4.30	$4.40	$4.50	$4.44	24.0%
Free Cash Flow	$7.8B	10%	$4.8B	$5.0B	$5.2B	$5.1B	11.5%
STRATEGIC METRICS(3)							
Goal (10% weight): Execute milestones related to supply chain continuity and capital structure. **Result:** Achieved							10.0%
Goal (12.5% weight): Develop and execute plans to manage cybersecurity and economic risks. **Result:** Achieved							12.5%
Goal (7.5% weight): Develop and execute integration plan for Cardiovascular Systems Inc. **Result:** Achieved							7.5%
Goal (5% weight): Implement a global guided buying platform. **Result:** Mostly Achieved							3.75%
Goal (10% weight): Implement key IT infrastructure initiatives. **Result:** Mostly Achieved							7.5%
HUMAN CAPITAL METRICS							
Goal (15% weight): Meet talent, succession planning, and diversity targets. **Result:** Achieved							15.0%
						Total	105.55%

(1) Adjusted Sales exclude the impact of foreign exchange on actual sales relative to the goal target. Adjusted Diluted EPS is diluted earnings per common share from continuing operations excluding specified items. Free Cash Flow equals Operating Cash Flow less acquisitions of property and equipment.

(2) Set based on expected market growth of the businesses and markets in which we compete. To achieve target payout, market share must increase.

(3) Target not disclosed for competitive reasons.

+ **https://www.sec.gov/Archives/edgar/data/1800/000130817924000182/abt4257331-def14a.htm**

ABBOTT LABS

+ 2023 Proxy
+ Page 42
+ Contains both Cybersecurity and IT measures
+ Weights the measure @12.5%
+ Gives results of whether measure was achieved or not – this is not just a simple discretionary measure

An example of using a weighted STI measure to manage cyber risk

Example 2

"*Operating Objectives.*" A 20% target weight is assigned to the Company's operating objectives measure, set forth in the table below. The Compensation Committee believes that the operating objectives further long-term reliability and foster environmental sustainability. The levels of performance units are earned as follows:

Operating Objectives (5% weight for each objective below)	Performance Goals		
	Minimum	Target(1)	Maximum
Diversity and Inclusion Work Plan	< 3	4	6
Cyber Security Work Plan Milestones/Tasks	<4	5	7
Clean Energy and Electrification Work Plan Milestones/Tasks	< 2	3	5
Reliable Clean City Electric Transmission Projects	< 6	8	10
Payout Relative to Target (%)	0	100	150

Footnote:

(1) The MD&C Committee approves the annual work plan objectives. Performance results are based on average achievement of each work plan over the three-year period. For the Diversity and Inclusion Work Plan, the Cyber Security Work Plan and the Clean Energy Electrification Work Plan, the target approved by the Compensation Committee for 2023 applies to the second year of the three-year performance period for the 2022 performance units and the third year of the three-year performance period for the 2021 performance units.

CONSOLIDATED EDISON

- 2023 Proxy
- Page 63
- Details how the measure is achieved
- Details the weighting range

- **https://www.sec.gov/Archives/edgar/data/1047862/000114036124019096/ny20018645x1_def14a.htm**

An example of using a weighted STI measure to manage cyber risk

Example 3

2023 ANNUAL CASH INCENTIVE PERFORMANCE METRICS

The determination of 2023 annual cash incentive plan awards for the named executive officers was based on the achievement of certain performance measures approved by the Compensation Committee (and ratified by the Board) as described below. Given the strategic transformation of the Company to a pure play multifamily REIT, the Compensation Committee focused on delivering key strategic milestones that will be instrumental in creating long-term value for shareholders in addition to objectives linked to shorter term financial results. The objectives described below were designed to reward the achievement of significant corporate goals including NOI growth; the disposition of non-strategic assets; reductions in Core G&A; the attainment of ESG goals; and improvement of the Company's cybersecurity posture.

METRIC	WEIGHT	THRESHOLD	TARGET	MAXIMUM	ACTUAL RESULT	OUTCOME
Same Store NOI	20 %	5.8 %	6.8 %	7.8 %	17.6 %	Maximum
Office and Land Sales (in $M)	20 %	$50M	$125M	$200M	$206M	Maximum
Core G&A (in $M)	15 %	$38M	$35M	$33M	$34.8M	Between Target and Maximum
ESG (out of 3)[1]	10 %	1 out of 3	2 out of 3	3 out of 3	3	Maximum
Increase Cybersecurity Rating[2]	5 %	55	65	75	95	Maximum
Individual Performance	30 %	1	3	5	5	Maximum

(1) The plan contemplated the following ESG Goals:
(i) Measure residents' Scope 3 emissions (energy usage) for 35% of the portfolio
(ii) Increase spend from minority / women owned suppliers in the multifamily portfolio by $1.5M (20%)
(iii) Implement Resident ESG Awareness program across >75% of the properties
(2) Based on Center of Internet Security (CIS) benchmark.

The pages that follow describe the above-referenced Company Goals/Tasks that were approved by the Compensation Committee (and ratified by the Board), including the reasons these objectives were selected; the rationale for the designated hurdles; and the results achieved and the corresponding payouts earned. Thereafter, we disclose the Compensation Committee's considerations relating to the individual performance of each of the Company's NEOs as of December 31, 2023.

+ **https://www.sec.gov/Archives/edgar/data/924901/000092490124000031/vre-20240429.htm**

VERIS RESIDENTIAL

+ 2023 Proxy
+ Page 34
+ Details how the measure is achieved
+ Details the weighting range
+ Details the results of the plan


Pearl Meyer
MainData
GROUP
05
Key Considerations for Boards and Compensation Committees

Ensuring Cybersecurity Accountability: Key Considerations for Boards and Compensation Committees

Top 10 Key Considerations

Establishing Governance and Oversight Structures

Setting Clear Cybersecurity Expectations

Tying Cybersecurity to Executive Accountability

Demanding Regular Cybersecurity Reporting

Fostering a Risk-Aware Culture

Ensuring Adequate Cybersecurity Investment

Conducting Cybersecurity Risk Assessments

Compliance with Regulations and Standards

Preparing for Cybersecurity Incidents

Ensuring Cybersecurity Insurance Coverage


Pearl Meyer
MainData
GROUP
06
Roles of Total Rewards Leaders in Advancing Cybersecurity

The Role of Total Rewards Professionals in Advancing Cybersecurity

Exec Comp

- Total Rewards professionals help design compensation plans that tie executive pay to cybersecurity performance. This includes setting measurable cybersecurity goals, such as incident response time, compliance with security policies, and reducing vulnerabilities. They ensure that part of the executives' bonuses or long-term incentives are linked to achieving these cybersecurity objectives.
- By incorporating cybersecurity metrics into executive incentives, Total Rewards professionals emphasize the importance of security as a strategic priority for the organization.
- Executive compensation consultants can provide context on peer group and broader industry trends as it relates to adoption of cybersecurity metrics.

EE Incentives

- TR professionals can be involved in designing incentive programs that reward employees for following cybersecurity best practices. This can include bonuses for employees who complete cybersecurity training or successfully report security incidents.
- For cybersecurity professionals specifically, Total Rewards experts may design specialized incentive structures to retain and motivate talent with competitive pay packages, performance bonuses, and equity compensation linked to the success of the company's cybersecurity initiatives

Culture

- TR professionals contribute to building a culture of cybersecurity by aligning rewards and recognition programs with security awareness. Recognizing employees who demonstrate a strong commitment to cybersecurity through secure behaviors encourages a company-wide focus on security.
- They can also help to integrate cybersecurity values into the overall employee value proposition, making it clear that the company takes security seriously and expects all employees to do the same.

Compliance

- TR professionals ensure that executive and employee compensation programs comply with cybersecurity-related regulations. This includes aligning compensation structures with compliance requirements, such as data protection laws (e.g., GDPR) or industry standards (e.g., NIST frameworks), and ensuring that any cybersecurity failures affecting compliance are reflected in compensation adjustments.

The Role of Total Rewards Professionals in Advancing Cybersecurity

Continued

Talent

- In collaboration with HR, Total Rewards professionals design competitive compensation packages to attract and retain top cybersecurity talent, which is in high demand. This includes offering market-competitive salaries, benefits, and career development opportunities specifically targeted at cybersecurity professionals.
- They also ensure that benefits such as ongoing cybersecurity training and professional certifications are supported through the company's reward and development programs.

Communication

- Total Rewards professionals ensure that there is clear communication around how cybersecurity achievements or failures impact compensation. Transparency in linking rewards to security performance fosters accountability and ensures that all employees understand the role cybersecurity plays in their compensation and overall career advancement.

Risk Mitigation

- By aligning compensation incentives with cybersecurity risk management, Total Rewards professionals help promote a risk-aware culture across the organization. They can incorporate cybersecurity risk mitigation into broader risk management frameworks, ensuring that rewards and incentives align with minimizing security risks.
- Consider having your executive compensation consultant include the cybersecurity program as part of its annual Compensation Risk Assessment provided to the Compensation Committee

Retention of Cybersecurity Talent

- Cybersecurity professionals are in high demand, and retaining top talent is crucial for maintaining a strong security posture. Total Rewards professionals can design specialized retention programs aimed at keeping key cybersecurity personnel engaged and motivated. These might include:
- Retention Bonuses
- LTI: Offering equity compensation or deferred bonuses tied to long-term cybersecurity projects or security improvement milestones.
- Recognition Programs: Creating recognition programs that reward cybersecurity employees for their contributions, such as successful threat mitigation or innovative security solutions.

Cybersecurity Resources for Management and Directors

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

CYBER SAFETY REVIEW BOARD

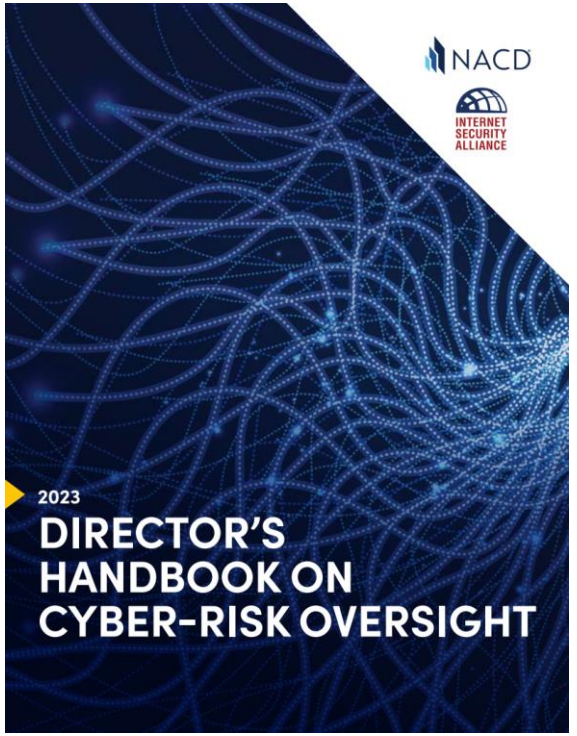
Review of the Summer 2023 Microsoft Exchange Online Intrusion

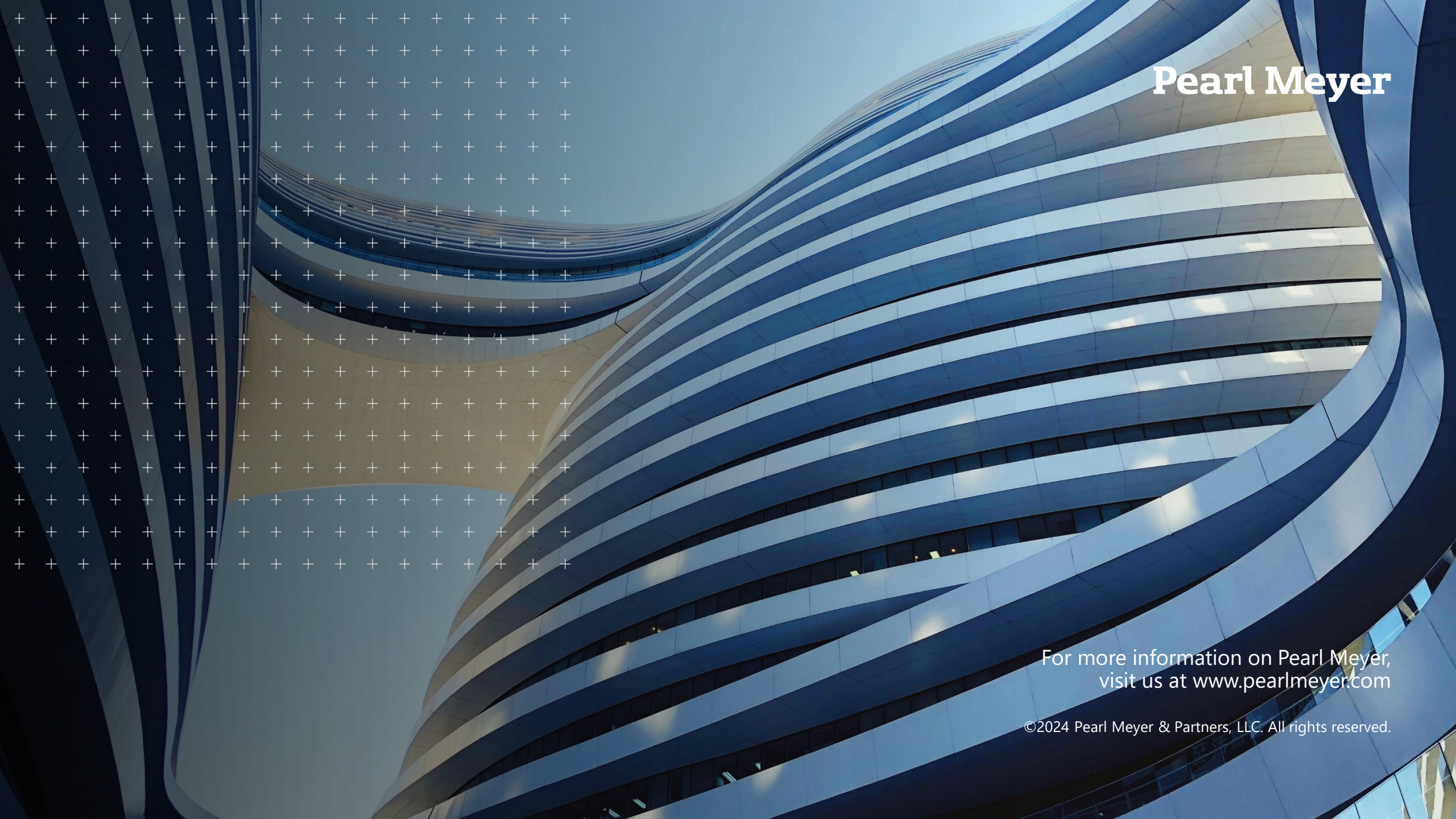
March 20, 2024
Cyber Safety Review Board

Pearl Meyer

Cyber Security, AI, and Data Science Salary Survey

2024 Prospectus





Pearl Meyer

For more information on Pearl Meyer,
visit us at www.pearlmeyer.com