Abstract – This document presents a comprehensive analysis of the "2024 Voice of the CISO" report by Proofpoint. The analysis delves into various critical aspects of the report, providing a detailed examination of the challenges and trends faced by Chief Information Security Officers (CISOs) globally.

This analysis provides a high-quality synthesis of the report, offering valuable insights for security professionals and other specialists across various industries. By understanding the challenges and strategies highlighted in the report, professionals can better prepare for the evolving cybersecurity landscape and enhance their organization's security posture. The analysis is particularly useful for those looking to align their cybersecurity efforts with industry best practices and emerging trends.

I. Introduction

The «2024 Voice of the CISO» report by Proofpoint paints a vivid picture of the tumultuous landscape that CISOs have navigated recently After all, dealing with a global pandemic, the chaos of remote work, and record levels of employee turnover was just a walk in the park. Now, with hybrid working becoming the norm and cloud technology expanding the attack surface to unprecedented levels, CISOs can finally relax, right? Wrong.

Cyber threats are more targeted, sophisticated, and frequent than ever. Employees are more mobile, often taking sensitive data with them as they hop from job to job. And let's not forget the generative AI tools that, while promising, have also made it easier for cybercriminals to launch devastating attacks with just a few dollars.

Sure, CISOs are enjoying closer ties with key stakeholders, board members, and regulators. But this newfound proximity only brings higher stakes, more pressure, and heightened expectations. And with flat or reduced budgets, CISOs are expected to do much more with considerably less. In this environment, shortcuts are sometimes necessary, but they can lead to human error—because, of course, everything always goes perfectly when you're under-resourced and overworked.

To better understand how CISOs are navigating yet another high-pressure year, Proofpoint surveyed 1,600 CISOs worldwide. They asked about their roles, outlooks for the next two years, and how they see their responsibilities evolving. The report explores the delicate balance between concern and confidence as various factors combine to ramp up the pressure on CISOs. It delves into the persistent risks posed by human error, the challenges of burnout and personal liability, and the evolving relationship between CISOs and the boardroom.

A. Benefits

- **Comprehensive Data:** The report surveys 1,600 CISOs from organizations with 1,000+ employees across 16 countries, providing a broad and diverse dataset.
- **Current Trends and Challenges:** It highlights key issues such as the persistent vulnerability of human error, the impact of generative AI, and the economic pressures on cybersecurity budgets.
- **Strategic Insights:** The report offers actionable insights and recommendations, such as the importance of AI-powered technologies, improving employee cybersecurity awareness, and the need for robust incident response plans.
- **Board-CISO Relations:** It underscores the improving relationship between CISOs and board members, which is crucial for aligning cybersecurity strategies with business objectives.

B. Limitations

- **Overemphasis on AI:** The report places significant emphasis on AI as both a threat and a solution. While AI's role in cybersecurity is undeniable, the focus might overshadow other critical areas that also need attention.
- **Potential Bias in Self-Reported Data:** The data is self-reported by CISOs, which can introduce bias. CISOs might overstate their preparedness or the effectiveness of their strategies to present a more favorable view of their performance.
- **Focus on Large Organizations:** The survey targets organizations with 1,000 or more employees, which may not accurately reflect the challenges and realities faced by smaller organizations. This focus can limit the applicability of the findings to a broader range of businesses.
- **Economic and Regional Variations:** While the report covers multiple countries, the economic and regulatory environments vary significantly across regions. The findings might not be universally applicable, and regional nuances could be underrepresented.
- **Human-Centric Security:** Although the report emphasizes human-centric security, it might not fully address the complexities of implementing such strategies effectively. The reliance on user education and awareness can be seen as placing too much responsibility on employees rather than improving systemic defenses

C. Methodology

1) Survey Scope

- The survey was conducted by the research firm Censuswide between January 20 — February 2, 2024.

- It surveyed 1,600 Chief Information Security Officers (CISOs) from organizations with 1,000 or more employees across different industries in 16 countries.
- 100 CISOs were interviewed in each of the following markets: U.S., Canada, U.K., France, Germany, Italy, Spain, Sweden, the Netherlands, UAE, Saudi Arabia, Australia, Japan, Singapore, South Korea, and Brazil.

2) Industry Representation:

- IT, technology, and telecoms (42%)
- Manufacturing and production (14%)
- Financial services (12%)
- Retail (8%)
- Business and professional services (6%)
- Public sector (5%)
- Healthcare (3%)
- Education (3%)
- Media, leisure, and entertainment (3%)
- Transport (2%)
- Energy, oil/gas, and utilities (2%)

3) Company Size:

- 1,000 — 2,500 employees (48%)
- 2,501 — 5,000 employees (33%)
- 5,001 or more employees (19%)

4) Research Standards:

The research is in alignment with the MRS Code of Conduct and ESOMAR principles, ensuring adherence to industry standards and ethical practices.

II. Heightened Concerns But Growing Confidence

A. Increased Risk Perception:

- **Material Cyber-attack Risk:** Over two-thirds (70%) of CISOs feel at risk of a material cyber-attack in the next 12 months, a slight increase from 68% last year and significantly higher than 48% in 2022.
- **Likelihood:** 31% of CISOs rate the risk of a significant attack as «very likely,» up from 25% in 2023.

B. Geographical Concerns:

- **Most Concerned Regions:** CISOs in South Korea (91%), Canada (90%), and the US (87%) are the most concerned about experiencing a material cyber-attack.
- **Optimistic Regions:** Brazil's CISOs are the most optimistic, with only 45% fearing an attack.

C. Industry-Specific Concerns:

- **High-Risk Industries:** Education (86%), transport (77%), and retail, healthcare, and public sector (all 74%) lead in cyber-attack concerns.

D. Awareness vs. Preparedness:

- **Awareness:** While 70% of CISOs feel at risk, only 43% believe their organization is unprepared to cope with a targeted cyber-attack in 2024, an improvement from 61% in 2023 and 50% in 2022.
- **Preparedness Gap:** The gap between awareness and preparedness remains a concern, highlighting a disconnect between recognizing risks and being ready to address them.

E. Top Threats:

- **Ransomware:** 41% of CISOs see ransomware as the leading threat in the next 12 months.
- **Other Threats:** Malware (38%), email fraud (36%), cloud account compromise (34%), insider threats (30%), and DDoS attacks (30%) are also significant concerns.

F. Regional Threat Focus:

- **Ransomware:** Top concern in Japan (64%), UK (51%), Sweden (49%), and the Netherlands (49%).
- **Email Fraud:** Major concern in Saudi Arabia (50%), Australia (46%), Germany (46%), Canada (42%), the Netherlands (42%), and Japan (42%).

III. Human Error: The Persistent Vulnerability

A. Human Error as the Biggest Vulnerability:

- 74% of CISOs consider human error to be their organization's biggest cyber vulnerability, up from 60% in 2023 and 56% in 2022.
- However, only 63% of board members agree that human error is the biggest vulnerability, suggesting CISOs need to better communicate this risk to the board.

B. Employee Negligence as a Key Concern:

- 80% of CISOs see human risk, including employee negligence, as a key cybersecurity concern over the next two years, up from 63% in 2023.
- This sentiment was most strongly felt in France (91%), Canada (90%), Spain (86%), South Korea (85%), and Singapore (84%).

C. Employee Awareness vs. Capability:

- 86% of CISOs believe their employees understand their role in defending the organization, with 45% strongly agreeing.
- CISOs still feel that employees pose an enormous risk, implying that while employees understand their responsibilities, they lack the necessary skills, knowledge, and tools to effectively defend against threats.

D. Adoption of AI-Powered Capabilities:

- 87% of CISOs are looking to deploy AI-powered capabilities to protect against human error and block advanced human-centric cyber threats.
- Industries leading the adoption include retail (81%), IT, technology, and telecoms (89%), and education (88%).

E. Regional and Industry Variations:

- CISOs in Saudi Arabia (84%), Canada (83%), and France (82%) are most concerned about human error being their organization's biggest cyber vulnerability.

- Industries with the highest concern about human error include education (89%), media, leisure, and entertainment (85%), and the public sector (78%).

IV. Data Protection and Insider Threats

A. Reduction in Data Loss:

- Fewer than half (46%) of global CISOs reported a material loss of sensitive information in the past 12 months, down from 63% last year.

B. Geographical Variations:

- South Korea (77%), Canada (61%), France (58%), and Germany (57%) reported higher rates of sensitive data loss compared to the global average.

C. Industry-Specific Data Loss:

- Education (68%), financial services (54%), and media, leisure, and entertainment (54%) sectors were most affected by sensitive data loss.

D. Causes of Data Loss:

- Negligent insiders or careless employees were blamed for 42% of data loss incidents.
- Other significant causes included external attacks (40%) and malicious or criminal insiders (36%).
- Additional factors included system misconfiguration (27%) and lost or stolen devices (28%).

E. Employee Turnover and Data Loss:

- 73% of CISOs said that employees leaving their organization played a role in data loss events.
- A concern around data loss due to job switchers has decreased from 82% last year, it still remains an issue.

F. Impact of Data Loss:

- The consequences of data loss included financial loss (43%), post-attack recovery costs (41%), and loss of critical data (40%).

G. Mitigation Strategies:

- To combat data loss, CISOs are focusing on educating employees about security best practices (53%) and using cloud security solutions (52%).
- Other measures include deploying data loss prevention (DLP) technology (51%), endpoint security (49%), email security (48%), and isolation technology (42%).

H. Future Priorities:

- 87% of CISOs agree that information protection and data governance are top priorities, a significant increase from previous years.
- The adoption of DLP technology has surged, with 51% of CISOs now using it, up from 35% last year.
- 81% of CISOs believe their data is adequately protected, up from 60% in 2023.

V. The Cyber Realities for a CISO in 2024

A. Generative AI:

- **Security Risks:** 54% of CISOs believe generative AI poses a security risk to their organization.
- **AI**: While AI can aid cybercriminals by making attacks easier to scale and execute, it also provides defenders with real-time insights into threats, which traditional methods cannot match.
- **Top Concerns:** ChatGPT and other generative AI models are seen as significant risks, followed by collaboration tools like Slack and Teams (39%) and Microsoft 365 (38%).

B. Economic Impact:

- **Economic:** 59% of CISOs agree that current economic conditions have negatively impacted their organization's ability to resource cybersecurity budgets.
- **Regional Impact:** CISOs in South Korea (79%), Canada (72%), France (68%), and Germany (68%) feel the economic impact most acutely.
- **Budget:** Nearly half (48%) of CISOs have been asked to cut staff, delay backfills, or reduce spending.

C. Priorities and Strategies:

- **Priorities:** Improving protection and enabling business innovation remain top priorities for 58% of CISOs.
- **Employee Cybersecurity Awareness:** Improving employee cybersecurity awareness has become the second-highest priority, indicating a shift towards human-centric security strategies.

D. Board Relations:

- **Alignment with Board:** 84% of CISOs now see eye to eye with their board members on cybersecurity issues, up from 62% in 2023.
- **Board-Level Expertise:** 84% of CISOs believe cybersecurity expertise is required at the board level, reflecting a significant increase from previous years.

E. Challenges and Pressures:

- **Unrealistic Expectations:** 66% of CISOs believe there are excessive expectations on their role, a continued increase from previous years.
- **Burnout:** More than half (53%) of CISOs have experienced or witnessed burnout in the past 12 months, although there is a slight improvement with 31% reporting no burnout, up from 15% last year.
- **Personal Liability:** 66% of CISOs are concerned about personal, financial, and legal liability, with 72% unwilling to join an organization without directors and officers (D& O) insurance or similar coverage.

VI. Strengthening Board-CISO Relations

A. Improved Alignment:

- **Increased Agreement:** 84% of CISOs now report seeing eye to eye with their board members on cybersecurity issues, a significant increase from 62% in 2023 and 51% in 2022.
- **Industry Variations:** The highest levels of agreement are seen in healthcare (91%), transport (88%), and energy, oil/gas, and utilities (81%).

B. Board-Level Expertise:

- **Cybersecurity Expertise:** 84% of CISOs believe that cybersecurity expertise should be required at the board level, up from 62% in 2023.
- **Regional Differences:** CISOs in Saudi Arabia (95%), Brazil (92%), Germany (90%), and UAE (90%) report the highest levels of agreement with their boards.

C. Board Concerns:

- **Top Concerns:** CISOs believe that their boards are most concerned about disruption to operations (44%), loss in revenue (44%), and reputational damage (43%) in the event of a material cyber-attack.
- **Country-Specific Concerns:** Concerns vary by country, with some regions prioritizing different aspects of the impact of cyber-attacks.

D. Factors Behind Improved Relations:

- **Post-Pandemic Influence:** Many CISOs have maintained their place at the table post-pandemic, influencing wider business strategy.
- **Communication:** CISOs have taken steps to speak the language of the boardroom, translating security concerns into potential business impacts.

E. Enduring Integration:

- **Long-Term Change:** The integration of CISOs into the boardroom is seen as an enduring enhancement strategy, necessary for success in the modern digital era.

VII. Unrelenting Pressure on CISOs

A. Increased Expectations:

- **Unrealistic Demands:** 66% of CISOs believe there are excessive expectations on their role, a continued increase from 61% in 2023 and 49% in 2022.
- **Global Variations:** The highest levels of perceived excessive expectations are in Saudi Arabia (88%), UAE (87%), and South Korea (75%).

B. Burnout:

- **High Incidence:** More than half (53%) of CISOs have experienced or witnessed burnout in the past 12 months.
- **Improvement:** There is some progress, with 31% of CISOs reporting no burnout, up from 15% last year.
- **Regional Differences:** CISOs in South Korea (72%), Sweden (63%), and Australia (62%) are most likely to have experienced or witnessed burnout.

C. Personal Liability Concerns:

- **Legal and Financial Risks:** 66% of CISOs are concerned about personal, financial, and legal liability, up from 62% in 2023.
- **Insurance Coverage:** 72% of CISOs would not join an organization without directors and officers (D& O) insurance or similar coverage against financial liability in the event of a successful cyberattack.
- **Industry Concerns:** CISOs in manufacturing and production (75%), financial services (74%), and retail (68%) feel most strongly about the need for such insurance.

D. Impact of High-Profile Cases:

- **Influence of Legal Cases:** High-profile legal cases, such as the SEC charges against a SolarWinds CISO, have heightened concerns about personal liability.

E. Ongoing Challenges:

- **Resource Constraints:** CISOs continue to face challenges with flat or reduced budgets, making it difficult to meet the growing demands and expectations placed on them.

VIII. Conclusion

A. Increased Concern but Improved Preparedness:

- More CISOs are concerned about a material cyber-attack in the near future.
- Fewer CISOs feel unprepared, indicating greater confidence in their defensive measures.

B. Closer Relationships with Stakeholders:

- CISOs report closer relationships with key stakeholders and the boardroom.
- This change highlights the growing recognition of the CISO role at the highest organizational levels and the importance of cybersecurity.

C. Ongoing Challenges:

- **Employee Turnover:** Continues to be a critical concern, with job leavers posing a sustained risk of data loss across all sectors.
- **Adoption of DLP Technology:** Many CISOs have adopted Data Loss Prevention (DLP) technology and invested in employee education to mitigate this risk.

D. Evolving Threat Landscape:

- **Familiar Threats:** Ransomware and Business Email Compromise attacks remain significant concerns.
- **Emerging Technologies:** AI poses new challenges but also offers potential solutions.

E. Human-Centric Security:

- People and their behaviors continue to pose the greatest ongoing risk to organizations.
- Many CISOs are investing more in human-centric approaches, leveraging AI to help mitigate human error.

F. CISO Role Challenges:

- **Personal Liability:** Growing concern around personal liability.
- **Expectations:** Increasing numbers of CISOs report excessive expectations, burnout, and higher budgets.
- Addressing these issues is crucial to ensure CISOs are equipped for their roles now and in the future.