"Perfect is the Enemy of Good": The CISO's Role in Enterprise Security as a Business Enabler

Kimberly Ruth
kcruth@cs.stanford.edu
Stanford University
USA

Veronica A. Rivera
varivera@stanford.edu
Stanford University
USA

Gautam Akiwate
gakiwate@cs.stanford.edu
Stanford University
USA

Aurore Fass
fass@cispa.de
CISPA Helmholtz Center for Information Security
Germany

Patrick Gage Kelley
patrickgage@acm.org
Google
USA

Kurt Thomas
kurtthomas@google.com
Google
USA

Zakir Durumeric
zakir@cs.stanford.edu
Stanford University
USA

ABSTRACT

Chief Information Security Officers (CISOs) are responsible for setting and executing organizations' information security strategies. This role has only grown in importance as a result of today's increasingly high-stakes threat landscape. To understand these key decision-makers, we interviewed 16 current and former CISOs to understand how they build a security strategy and the day-to-day obstacles that they face. Throughout, we find that the CISO role is strongly shaped by a business enablement perspective, driven by broad organizational goals beyond solely technical protection. Within that framing, we describe the most salient concerns for CISOs, isolate key decision-making factors they use when prioritizing security investments, and surface practical complexities and pain points that they face in executing their strategy. Our results surface opportunities to help CISOs better navigate the complex task of managing organizational risk, as well as lessons for how security tools can be made more deployable in practice.

CCS CONCEPTS

• **Security and privacy** → **Human and societal aspects of security and privacy**; • **Applied computing** → *Enterprise computing*; • **Social and professional topics** → **Socio-technical systems**; *Management of computing and information systems*; • **Human-centered computing**;

KEYWORDS

CISO, security, enterprise, business

ACM Reference Format:

Kimberly Ruth, Veronica A. Rivera, Gautam Akiwate, Aurore Fass, Patrick Gage Kelley, Kurt Thomas, and Zakir Durumeric. 2025. "Perfect is the Enemy of Good": The CISO's Role in Enterprise Security as a Business Enabler. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26-May 1, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 19 pages. https://doi.org/10.1145/3706598.3713895

CHI '25, April 26-May 1, 2025, Yokohama, Japan

ACM ISBN 979-8-4007-1394-1/25/04…$15.00
https://doi.org/10.1145/3706598.3713895

1 INTRODUCTION

Enterprise security is an increasingly impactful issue. Recent headlines reflect the monumental challenges faced by Chief Information Security Officers (CISOs)—executives who head enterprises' information security operations. Attacks include ransomware attacks disrupting operations, incurring hundreds of millions of dollars in losses [8]; nation states spying on executive emails [43]; malicious patches to critical software dependencies [15]; and data breaches that trigger extensive disclosure obligations [26, 32].

The continued success of today's attacks is not for lack of effort or expertise on the part of CISOs, nor for a lack of security investments by enterprises. Indeed, by some measures, security spending is at an all time high [11]. Likewise, prior studies have shown that CISOs take proactive steps such as using risk frameworks to identify process failures [31], leveraging government guidance and threat intelligence [31, 45], and communicating risk to business leaders to secure investment [10]. The tools available to CISOs for endpoint threat detection, cloud monitoring, and more [9, 13, 30, 44] are also increasingly sophisticated. Yet, there remains a disconnect: if the know-how, improved tools, and funding are there, why do such serious enterprise incidents persist?

The research community's understanding of what shapes and limits CISOs' success remains relatively piecemeal. Past work has studied CISO skill sets [21], communication practices [25], and perceptions of technical risk [31] in isolation. However, recent systematization of these studies [36] has noted that our broader understanding of how CISOs operate remains "nascent" and has identified a fundamental gap in our knowledge of the challenges CISOs face. In this work, we attempt to fill this gap by analyzing how CISOs engage with the business environment they operate in. We interviewed 16 current and former CISOs from the technology, finance, healthcare, and higher education sectors to understand:

RQ1: Responsibilities and Threats (Sections 4 and 5). How do CISOs approach obligations around operational risk, compliance requirements, and the business' broader objectives? Where are these obligations in tension? How do they inform CISOs' assessment of top risks?

RQ2: Prioritization and Success Objectives (Section 6). How do CISOs prioritize security investments? How do CISOs weigh technical threat-modeling versus business constraints? How do CISOs measure success and validate their approach?

RQ3: Implementation Challenges (Section 7). What challenges impede CISOs' ability to implement their strategy? How much of the difficulty is due to technical shortcomings versus human or organizational complications?

In considering these questions together, we observed that CISOs framed their role in a more business-centric manner than has been captured by prior work. Our participants consistently described their role as enabling their organization to *intentionally* take on risk in a measured way—such as through new business ventures and product launches—rather than exclusively ensuring operational security. This *business enablement* role underpinned the difficulty of allocating resources and effort amid a complex landscape of constraints, thereby affecting enterprises' security posture. Optimizing for business enablement required complex and often bespoke decision making. Threat modeling was just one input into CISOs' deliberation process: other inputs included externally-driven obligations (from customers, regulators, insurers), internal business constraints (budget, staffing, competing engineering priorities), and other stakeholder requirements (from their board of directors, executive team). Accounting for these business considerations, strategy and prioritization were more art than science, and flawless security was an explicit non-goal due to the unacceptable burden it would impose on the broader organization.

CISOs faced fundamental *organizational* challenges in deploying security mitigations—challenges that the research community can, in fact, help address. Participants lamented difficulties in coordinating security efforts across large, complex, and technically heterogeneous organizations, particularly due to incongruous needs of other stakeholders. Combined with a lack of meaningful metrics on the business value of security controls, this meant CISOs needed to fall back on persuasion, compromise, or simply acceptance of imperfections, as befit the objectives and risk tolerance of the overall business. Security weaknesses primarily persisted, not because they could not technically be fixed, but because the broader business context limited what fixes made sense.

Our work shows how business operations drive both the risks CISOs are tasked with managing and the day-to-day operations that make risk management difficult. We contribute: (1) a novel characterization of CISOs' business enablement perspective, (2) understanding of how this perspective shapes their challenges and decisions, and (3) identification of crucial mismatches between decision factors and how enterprise security solutions are designed. In doing so, we highlight opportunities for researchers to help address enterprises' most pressing security challenges.

2 BACKGROUND AND RELATED WORK

CISOs are senior executives responsible for setting and executing the information security strategy for their organizations [27]. They manage security personnel and oversee activities including conducting risk assessment, defining protective security measures and policies, running employee awareness training, and managing incident response [36]. This requires extensive nontechnical communication in addition to technical background [12]. While there is consensus that CISO effectiveness relies on being placed high in the organizational chart [36] and respected as senior executives [41], there is ongoing debate about best-practice reporting lines; documented cases include reporting to the CIO, CEO, COO, Chief Risk Officer, or general counsel [36].

While prior work has surveyed security management skill sets and professional activities [16, 38], the literature on understanding the CISO role more deeply is limited. Recent systematization has highlighted fundamental open questions about how CISOs operate in their environment: notably, (1) how CISOs navigate their role within the business, and (2) what challenges hinder them in achieving their objectives [36]. Our work addresses these two questions. We summarize related work here and compare our results in Section 8.

Security strategies. Literature about how CISOs direct their security programs is sparse. Prior work on information security governance, not centered on CISOs, has primarily focused on how organizations *should* govern rather than current practices (e.g., [2, 23, 28, 37, 42]). Work on small to medium-sized businesses (SMBs) has found that security professionals' perceived risk level and number of implemented security defenses both increase with company size [22]. Wolf et al. reported that small-business CISOs are underprepared for security threats and uninformed about regulations [45]. Specific to security prioritization, the closest work to ours is from Moore et al. [31] in 2016, who interviewed security managers and executives to investigate how organizations manage security risks and what drives security investments, focusing on technical risk factors such as past attacks, threat intelligence, and maturity frameworks. While we corroborate many of their findings from nearly a decade ago, we also demonstrate how CISOs' prioritization is more complex than managing technical risk, involving a broad array of stakeholder demands from across the business.

Managing friction for individuals. There is a growing body of work examining how security managers, including CISOs, address the friction that security controls create for employees. Early work by Albrechtsen and Hovden in 2009 [1] demonstrated a disconnect between managers' and users' views on security, leading managers to make security decisions that are poorly aligned with what users expect. A decade later, Reinfelder et al. [34] found that security managers care about usability for non-security employees, but organizations do not have the structure for engaging users in the planning process. Ashenden and Sasse [3] interviewed five CISOs in 2013 to investigate how they build credibility and engage with employees. Most recently, Hielscher et al. [17] conducted workshops with CISOs in Switzerland to study their view on human-centered security and argued that they associate it too strongly with awareness training. Other work has shown that security may interfere with employees' jobs and decrease their productivity [18], documented employees' limited capacity for following security policies [4], and discussed how employees' misaligned incentives can manifest differently in different parts of an organization [29]. Our work documents how CISOs' understanding of friction affects their planning processes and ability to deploy solutions, as well as how the friction CISOs face also involves systemic organizational complexity not previously identified.

Communicating upwards. Multiple studies have examined the CISO's managerial relationship with the board and with senior leadership. Da Silva et al. [10] characterized the CISO's role as analogous to that of a soothsayer to a non-expert board audience. Lowry et al. [25] interviewed board members and senior security experts to investigate the perceived effectiveness of board members' security oversight. Other work has documented that CISOs struggle to be taken seriously by other executives and the board of directors [41], and has argued that CISOs receive insufficient upskilling support from senior management [46]. Although our findings are largely consistent with this body of work, we focus more on how CISOs steer their security program within their organizational context, with leadership relationships being one of many factors influencing their strategies and operational challenges.

3 METHODOLOGY

We conducted semi-structured interviews with 16 current or former CISOs. We describe our participants, data collection, analysis strategy, ethics, and limitations.

3.1 Participants and Recruiting

We identified potential participants via professional networking sites, personal connections, and snowball sampling whereby participants facilitated connections to other CISOs. In total, 16 participated: 15 current CISOs and 1 former CISO. All participants had over 10 years of experience in security; nine had over 20 years of experience. Participants had an average of 6.5 years experience as a CISO and 4.3 years in their current organization. Participants oversaw security for a mix of company sectors, sizes, and ownership models (Table 1).

3.2 Data Collection

We conducted semi-structured interviews from June to September of 2023. Each interview involved one participant and 2–3 researchers; interviews lasted 67 minutes on average. We piloted our initial interview script with one CISO (not included in our set of 16) before settling on our final interview script (Appendix C). Prior to interviews, all participants filled out a pre-survey with information about their job role, the size of their security team, core responsibilities, and relevant compliance standards. This helped to prepare interviewers given the limited time available with participants. During our interview, we focused on the following topics:

Risks. The risk landscape they operated in, how their risks differed from other businesses, and how risks changed over time.

Priorities & Success Criteria. How they prioritized risks and available mitigations, factors that influenced their goals and decision making, and assessment of progress or outcomes.

Challenges. The technical and nontechnical challenges they faced when executing on their decisions, pushback from stakeholders, and approaches to resolving challenges.

3.3 Analysis

Our resulting data consisted of 16 transcripts: 11 were manually transcribed from audio recordings where participants consented to recording, while 5 consisted of detailed notes taken during interviews for participants who declined recording but consented to note taking. We followed thematic analysis using a codebook approach [5, 7]. Three researchers iteratively developed a codebook (Appendix D) using inductive and deductive codes, with feedback from the full research team. We selected provisional deductive codes around security controls, harms, threats, and attackers, drawing from frameworks by NIST and threat reports.

The bulk of coding was inductive; we engaged in line-by-line open coding, continuously adding new semantic codes related to factors used in prioritization, success metrics, and challenges across all transcripts while also refining earlier deductive codes. We met regularly to discuss and agree upon changes to the codebook. Three researchers engaged in coding: every interview was assigned to one of the three researchers as primary coder, while one of the remaining two researchers acted as a secondary coder to read and verify correctness of the primary coder's work. In the event of disagreement, the researchers engaged in discussion to arrive at a consensus. As such, we do not report inter-rater reliability.

With this initial set of coded interviews, we iteratively sorted the codes into groups that represent the themes. We followed best practices from Nowell et al. [33] including prolonged engagement with data, capturing memos, and returning to the raw data organically throughout the analysis process. We did not seek (and did not reach) data saturation, in keeping with our thematic analysis lens [6]; however, we did observe eventual stabilization in our top-level inductive themes.

3.4 Ethics

Our study plan was approved by our institution's IRB. Before conducting interviews, we received informed consent from participants to take detailed notes and to share anonymized quotes as part of our research. We offered all participants the option to not be audio recorded, which five participants chose, agreeing to have notes taken by a researcher. Access to recordings and transcripts were protected, being available only to a limited number of researchers directly involved in interview note-taking and coding.

We offered participants a piece of memorabilia (e.g., sweatshirt) as a thank-you gift for participating in the study. To preserve the privacy of our participants, we have not linked the quotes we include to individual participants. We only report firmographics[1] in Table 1 that in combination protect participant identities with an anonymity set of 60 or greater. We have also omitted unique details, phrases, or words to minimize the risk of participants being identified. Additionally, we do not report (nor did we collect any data on) the gender, race, age, or other demographics of our participants.

3.5 Limitations

Our research offers limited generalizablity, as we interviewed only 16 CISOs, some of whom were referred by contacts in our networks or other participants—meaning we may have engaged with just a small cross-section of the CISO population. We also do not offer full coverage of the many business sectors that employ CISOs, nor broad global geographic coverage; all of our participants were from the United States. As with all interview studies, participants may not

[1]"Firmographics" denotes attributes of a company, as demographics does for people.

Participant	Business Sector	Employees	Public	Participant	Business Sector	Employees	Public
P1	Higher education	10K+	No	P9	Technology	1K-10K	Yes
P2	Technology	1K-10K	No	P10	Finance	10K+	Yes
P3	Technology	100-1K	Yes	P11	Technology	1K-10K	No
P4	Finance	1K-10K	No	P12	Health	10K+	No
P5	Technology	100-1K	No	P13	Health	10K+	No
P6	Technology	100-1K	No	P14	Health	1K-10K	No
P7	Technology	1-100	No	P15	Finance	1K-10K	No
P8	Technology	100-1K	No	P16	Finance	10K+	Yes

Table 1: Firmographics of Participants' Companies

have covered all risks or security decision criteria, for any number of reasons including recency bias, believing answers would not be relevant to our research aims, potential concerns of revealing corporate secrets, or corporate practices that may have shone a negative light on their security practices. We believe that even with the limitations above, this study adds important details to how the security community understands the work of CISOs.

4 THE ROLE OF THE CISO

Within their formal role of security strategist, our participants discussed the day-to-day realities of being a CISO: how they enabled organizations to take on new business ventures in a secure way, how they navigated compliance obligations, and how they set a risk posture that best matched their organization's unique constraints.

4.1 Mitigating Risks

All of our participants situated their role within an organization as identifying and mitigating risks—especially existential risks that could cause the organization to cease to function. As one participant framed it, *"it tends to be companies who are existentially threatened by security [that] are very aware of it."* Participants described setting overarching strategy to minimize potential risk, but also to prepare for inevitable breaches: *"any day, any organization can have a bad day and have a major incident."* Participants emphasized the high stakes of operational security, where *"One little hiccup for a company [...] can erode trust very quickly"* and where losing major customers *"would be a death blow."* As we show throughout our work, these high stakes shaped the approach participants took towards security.

4.2 Enabling Business Opportunities

All of our participants underscored that their responsibility was to enable the broader organization to meet its business goals: launching new products, accelerating deliverables, or increasing revenue. Participants emphasized that security alone was an anti-goal and a potential mismatch with the expectations of the research community: *"My job isn't to make us the most secure [...] My job is primarily to help the CEO achieve their business objectives."* Understanding how to enable the business to succeed, while also addressing existential risks, was critical to each participant:

> *"The big disconnect is you can master the subject matter of cybersecurity, but if you don't master the business that the program [...] is operating in, you have completely missed the [point]."*

Within this business paradigm, participants shared how their role was to allow the organization to take on risk in a responsible way, with security enabling new types of business:

> *"The purpose of seatbelts in cars is that cars can go faster [...] Security allows business to expand to new areas. To take new risks with confidence."*

That meant adapting their security strategy as the business evolved: to *"change [your] risk profile because of [where] revenue shifts."* Otherwise, *"risks should not materially change unless your business materially changes."*

4.3 Navigating Compliance

More than half of the participants (10 of 16) discussed how navigating compliance was a core part of their responsibility. Every participant named at least one compliance standard (e.g., CCPA, GDPR, HIPAA) that affected their day-to-day operations. Compliance was also discussed as a precondition for working with certain customers (e.g., European customers may demand ISO 27001; U.S. customers SOC 2 Type II; and federal customers CMMC or FedRAMP). In our pre-interview survey, participants reported a median of four compliance standards that shaped their responsibilities (Appendix A). As one participant succinctly summarized:

> *"What are the compliance requirements that we're going to have to meet? [...] We're going to use that to design a security program."*

While most participants described compliance as providing a "floor" for minimum security standards, it was not a guarantee of security: *"You can be compliant and completely hackable."* Some participants also pointed to the mismatch between compliance and their own business objectives and strategy towards risk:

> *"There are certain CISOs who are more compliance-focused [...] who wouldn't be right for this type of [company]."*

Compliance could also be orthogonal to security at an organization. One participant shared how they obtained unnecessary certifications around payment card industry (PCI) compliance for their business to simply streamline customer engagement:

> *"We are PCI certified. We have no credit card numbers [...] We had several people [customers] who wanted it*

> *because that helps their compliance program when they have to talk to their PCI auditors."*

4.4 Balancing Security, Compliance, and Business

Ultimately, participants described their role as a delicate balancing act of reducing security, privacy, compliance, or other risks without disproportionately hindering the business' main goals. One participant described striking the right balance through a risk–reward paradigm: *"[an organization] is in the business of exploiting the risk–reward paradigm so there is more reward than risk."* This meant prioritizing security only where necessary, given security often incurred a burden: *"You may fix a security problem, but cause processes to slow down or break operationally."*

Most participants embraced a degree of imperfection in their organization's security posture. One explained that for the sake of compromise and forward progress, *"perfect is the enemy of good."* Indeed, perfect organizational security was a viewed as a sign that the organization was spending too much money on security and harming the broader business:

> *"If you're at a 5 [out of 5 on a security rating], you're probably spending too much money on security honestly and you might actually be blocking the business in some cases."*

Striking this balance did not fall solely to CISOs. Participants noted that multiple decision makers—the company's board of directors, other executive staff, and the security organization—were involved in determining which risks were acceptable, which required mitigation, and how to implement improvements. As one participant shared:

> *"In many ways the CISO can't fix things, all we can do is highlight [issues]. We can say, here are the risks that we face and I believe them to be acceptable or unacceptable."*

5 CISO THREAT MODELING

Participants' business-centric goals infused their thinking about risks. When asked about today's risk landscape, participants described their threat model based foremost on how security failures could disrupt their business and profitability. Within this lens, participants brought up longstanding threats (e.g., phishing, zero-days, ransomware) and a rich set of actors who might use them, but shared that the impact of these threats changed based on industry trends or their current operating environment. Participants' perspectives on leading risks were not monolithic; as such, we report breakdowns of the frequencies of which risk dimensions were top-of-mind for participants.

5.1 Business Harms

Our participants viewed minimizing risks to their organization—particularly existential risks—as their top priority. This influenced the way they discussed current risks: participants focused on downstream business consequences more than technical vulnerabilities or attacker capabilities. We discuss the most prominent categories of business harms below.

Operational Continuity. Nearly all participants (14 of 16) described their top risks in terms of operational continuity: interrupted business-critical systems, unavailable support functions (e.g., sales, finance), disaster recovery scenarios, and more. One participant shared how a critical piece of banking infrastructure was brought down by ransomware, resulting in *"enormous financial liability for [reliant banks] that probably lost [them] tens if not hundreds of millions of dollars."* Here, CISOs focused on how security failures might bring down their core infrastructure or dependencies, including through software vulnerabilities, social engineering, misconfiguration, and more.

Brand Reputation & Customer Trust. A majority of participants (10 of 16) worried about the impact an incident would have on their brand and ability to attract or retain customers. As one participant who worked in healthcare stated: *"Our patients trust us to care for them, and they also trust us to care for their data."* Here, CISOs focused on threats to customer data including data breaches, insider risk, misconfiguration, and extortion (e.g., ransomware), among others. But risks also extended to operational data, such as: *"sensitive HR data, legal matters, contracts, [and] code"* that might be embarrassing or create a media cycle if exposed.

Penalties & Fines. Several participants (6 of 16) described risk in terms of potential penalties and fines that might be imposed by regulators or via litigation in the event of a security failure. This included *"severe penalties for violating HIPAA"* or *"contract obligations with our customers."* This was a constant source of churn due to updating requirements:

> *"There's no shortage of new privacy laws and regulations out there to keep track of [...] That creates some risk in just trying to keep up with those, and to ensure that we're not missing something."*

The ability for organizations to tolerate such financial losses was business dependent. As one participant framed it, *"Regulators can impose fines, which is not great for a startup."* For others, the financial loss was orthogonal to the real risk: *"As much as actual regulatory or contractual monetary losses [matter], I think the existential part comes from the inability to continue selling the product."*

5.2 Threats and Attack Vectors

Technical threats and attack vectors were subordinate, though salient, considerations for how our participants perceived today's risks (Table 2). Almost all participants (13 of 16) brought up some form of account takeover or social engineering threat whereby an employee with privileged access could be compromised or deceived into transferring funds or taking another unsafe action ("Business Email Compromise"). Changing tactics meant participants had to keep pace with trends: *"Business email compromise is very important now, but it was not important [to us] a year ago."* Software vulnerabilities, both due to zero days and delayed patching, were also a source of concern for participants (11 of 16). One participant framed the complexity of making any progress on this threat:

> *"Just think how much effort there is: [...] training programmers, static analysis tools, dynamic analysis tools, and sandboxing [...] We've got to rebuild everything in*

Threat	Examples	CISOs
Account takeover & social engineering	Phishing, business email compromise, stolen API key, weak authentication	13
Software vulnerabilities	Patching, endpoints, build system, cloud system, apps, zero-days	11
Data breaches & unauthorized access	Unencrypted data, exposed customer data, unauthorized access to data	11
Software supply chain vulnerabilities	Third-party libraries, providers	9
Ransomware & fraud	Ransomware, extortion, fraud	8
Misconfiguration	Private API exposure, missing identity, cloud misconfiguration, overpermissioning	7

Table 2: Top-of-mind Threats for CISOs

safe languages, like Rust or something, but that will take 100 years."

A majority of participants (9 of 16) shared how recent software supply chain attacks—like the SolarWinds breach [14] and the ION Trading ransomware attack [35]—*"put third party risk higher on everyone's concern."* The requirement for CISOs to reason about risk outside their organization posed a significant challenge: *"third party security is a total nightmare and there is no real solution for this that we know."*

Many participants discussed ransomware and fraud (8 of 16) as well as misconfigurations of APIs and cloud infrastructure (7 of 16). The latter often occurred due to new software-as-a-service capabilities with opaque security consequences. As one participant shared:

> *"An engineer forgot to check a box [...] to make this service non-public. And then a whole bunch of important data is publicly exposed [...] I've seen this over and over again, at multiple organizations."*

Given the decades-long experience of all our participants, they emphasized that many threats were not new: *"certainly there are always more advanced threat actors coming along and new techniques, but those are just variations on the same thing that have been playing out for a couple of decades."* But participants recognized that many threats remained unsolved: *"It's the fundamental problems we've been dealing with for decades now. And there's a reason they're still there, because they're not easy to solve."*

5.3 Attackers

Participants rarely centered their discussions of risk around types of attackers. However, when they did discuss adversaries, those that were top-of-mind for participants included insiders intentionally abusing their privileged access (10), nation states (9), cybercriminals with a financial objective (5), and low-technical or spray-and-pray opportunists (4). Several participants highlighted that nation state actors pose risk to their organizations and that *"even the best companies can't offer guarantees against nation states."* The same was true of rogue insiders—*"at the end of the day you have to trust employees,*

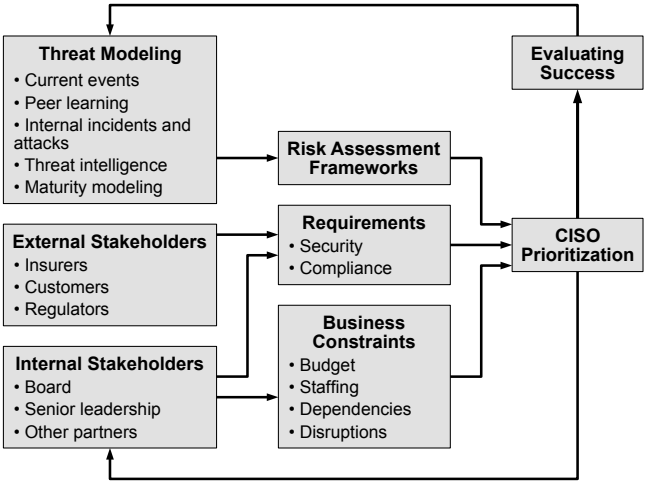

Figure 1: CISOs' Prioritization Process—Participants underwent an instinctual prioritization process based on several classes of inputs. Participants varied in how each component of this process was operationalized.

and trust is a four-letter word in our business"—though some participants discussed meaningful controls they had in place to minimize insider risk: *"We're watching our administrators who can do harm, we do peer reviews and architecture reviews of code that's checked in [...] We have a fairly good handle on [insider risk]."*

6 CISO PRIORITIZATION PROCESSES

The need to address business risk—not just technical risk—complicated how CISOs prioritized security investment. Across our participants, there was no concrete nor consistent process for how CISOs approached this task. Instead, participants emphasized the subjective nature of their role: there was no *"magic formula"* for the judgment calls that they had to make, and their *"judgment is imperfect and imprecise."* Nevertheless, our interviews revealed a structured set of inputs and feedback loops that influenced their decision making (Figure 1). These structures include a means of determining what security controls would reduce their organization's risk profile; a set of stakeholder or business requirements; resource constraints; and evaluation mechanisms to define the success of their program. We discuss each sub-component and ultimately how they influenced a CISO's security strategy.

6.1 Assessing Security Controls

All participants used some assessment of available security controls as a key foundation for prioritization. This foundation enabled them to systematize where they could or should invest in new security mitigations. We observed two structures enabling this thought process: risk assessment frameworks and maturity models. Our participants differed in which of these mindsets they emphasized in their prioritization decisions.

Risk Assessment Frameworks. The majority of participants (12 of 16) described the use of a risk assessment framework, such

as a "risk register," to understand the largest unmitigated risks they faced. This framework typically consisted of a list of risks, their likelihood, their potential impact, and existing controls to mitigate the risk. Scoring and interpretation were subjective. For instance, participants described prioritizing protections based on their company's most important assets—their *"crown jewels"*—while deprioritizing protections on *"either ancillary data or public data."* To reduce uncertainty and stay up-to-date in a shifting landscape, participants frequently relied upon their professional network, including other CISOs, to inform their risk register and scores. This included *"regularly exchanging information on the security problems that they face"* with other security professionals, sharing *"what's working, what's not working"* in terms of mitigations, and how organizations had *"been compromised and ransomwared."* Other signals included lessons from past incidents (both internally and at other organizations), third-party threat intelligence reports, and third-party audits and their recommendations.

Although participants aspired to measure risk quantitatively, this goal remained elusive: *"What is the expected value of fixing versus not fixing this vulnerability? Doing it right now versus pushing it off a week, a month, a year?"* Risk assessment became especially nebulous when vetting third-party entities, in part because *"you're one level removed from it."* Even third party risk management (TPRM) services, which aim to provide objective assessments, *"find a massive number of false positives that are just wasting security professionals' time."*

Maturity Modeling. Half of participants (9 of 16) described using a formal maturity model, such as the NIST Cybersecurity Framework (CSF), to understand the security posture of their organization. Maturity models differ from risk registers in that they focus on an organization's current controls (i.e., defenses), tiers or categories with which to level-set and plan, and a set of recommended best practices to achieve a better security posture rather than attempting to quantify the risks that a specific organization faces. The appeal of these frameworks came partly from a perception of being a *"thoughtful, educated, constructive approach"* and partly from a perceived authoritative source: *"what the government, NIST, recommends."*

Participants valued frameworks like NIST CSF and NIST SP 800-53 as checklists, though warned *"they don't include any standard approach to measurement"* in the framework itself. For instance, one participant scored their maturity per NIST CSF subcategory and aggregated those scores into an overall maturity report. Another assigned importance and implementation-completeness weights to controls in a maturity spreadsheet in order to derive a single overall risk score. Maturity modeling can be resource-intensive, though, and *"takes a long time"* when there are hundreds of check-boxes to assess against. This meant occasionally relying on an external, third-party assessor to implement the process, but these assessors also returned with subjective recommendations:

> *"Your identity [posture] is medium security because you've got MFA here, but you don't have it here. Or your security operations is low maturity because you actually don't have a dedicated SecOps leader."*

6.2 Stakeholder Requirements

Beyond available security controls, participants also had to weigh specific requirements from other stakeholders and external obligations (e.g., compliance and insurance requirements) in order to support the business.

Compliance. While CISOs were typically responsible for implementing compliance programs, compliance was a choice commonly made by the business rather than the CISO. One participant from a regulated industry explained that senior leadership allocated security budget first to compliance and contractual agreements; *"Then, if you can get additional money to manage your risk, you're doing a good job."* Another explained how they prioritized processes over tactical investments, as that was what regulators monitored:

> *"You're not going to get dinged [...] because you had a defect or a vulnerability or someone inappropriately accessed data. You're going to get dinged if you didn't know about it and you didn't have controls that were effectively operating in place."*

Participants had mixed opinions on the influence of compliance as a positive force for security. Half of participants believed that compliance made security easier or was closely aligned with security, and that standards *"result in overall much more disciplined security practice."* But compliance came with a cost: half of participants also believed that compliance slowed down security, or was insufficient to guarantee security. One participant explained that without *"purist"* security leaders designing the program, *"you might just be pulling down what NIST and SOC is telling you what to do—operational people. You won't have a good program."* Another argued that the industry's reliance on SOC 2 ignores the evidence of it not working: *"I think there's a gap between what the standards allow and the level of care we would expect based on the number of breaches that we see from third parties."*

Insurance Policies. Some participants included obtaining cyberinsurance coverage among their priorities. This entailed determining what insurers required to acquire and maintain coverage as well as implementing changes to minimize premiums: *"You can imagine the gamut of different cybersecurity controls, and they ask you what do you do, and then they digest that and then they form a subjective opinion on the strength of your controls."* This could involve a back-and-forth with insurers on whether requirements were realistic: *"[Insurers asked] 'We need to know that you are addressing critical vulnerabilities within 24 hours. Can you attest to that?' I said no, nobody can."*

Customers. Customers—particularly for business-to-business (B2B) companies—also made security demands of our participants. Here, CISOs viewed their ability to help their organization close deals by satisfying customer security requirements as part of their success. This meant at times rapidly re-architecting security systems: *"[If a] new customer has a need that's not presently being met within the product, [we look at] what compliance implications are there, what privacy implications are there, what do we need to close [the deal]."* Some customer needs were client-specific, non-standard compliance requirements. For example, one participant described implementing manual log analysis for a government contract since

automated log analysis was prohibited. If a business promised a security control, *"then you actually have to [implement] them."*

Board and Senior Leadership. Participants described how they engaged in a *"compromise conversation with the board"* and other high-level leaders. Particularly at public companies, the board of directors shaped their organization's risk appetite and spending decisions. These conversations resulted in making business tradeoffs between security risk and other forms of business opportunities:

> *"We want to do this risky thing—that's risky from a cyber point of view—but it's going to help mitigate this other risk, a patient safety risk or a financial risk."*

To conduct these conversations, participants needed to educate the board and senior leadership on how participants thought about risk, while building business cases that aligned with the overarching goals of the business. As one participant shared: *"a lot of the work we do is educational, it's not always technical"*. In the best case, this resulted in improvements in budget and other resource constraints (Section 6.3). However, participants were cautious in what they asked for in order to not be dismissed as *"crying wolf."* This tension was exacerbated by the lack of a data-driven *"harmonized way of expressing risk"* to non-expert business leaders. In such scenarios, participants found more success in arguing for security budget by pointing to gaps in their maturity model, rather than discussing a risk register.

6.3 Resource Constraints

Participants' resource constraints set by the business—like budget and staffing—also affected their prioritization. One participant explained that *"by and large, the security problems that lead to companies being compromised have known technical solutions,"* but that expense and labor held companies back. We discuss constraints further in Section 7, and focus here on the context of prioritization.

Budget. Limited budgets, and the fact that security is typically accounted as a *"cost center,"* led CISOs to grapple with difficult questions of *"when should you spend and when should you stop spending and when are you done?"* Participants reported needing to build *"effective business cases"* to senior leadership in order to justify investments, such as support of the business' revenue streams. This could mean maximizing the utility of an existing investment, rather than moving to a new security control even if it presented better (but more costly) protection:

> *"Leverage every toy that you have purchased to its fullest, before moving on to another toy."*

Other participants *"lead with the compliance requirement"* when arguing for funding a desired initiative since *"you can't question it."* These budget limitations caused some participants to simply truncate their priority list.

Staffing. Many participants indicated that talent shortages affected what they could accomplish. Hiring people with the *"right skills, mission focus, and collaboration focus"* was challenging in large part because securing an organization was a technically multifaceted endeavor. Ultimately, participants tried to address their top risks *"within the rate limit imposed by there being a limited number of people on certain teams."* Staff availability was especially pertinent when deciding whether to build solutions in-house or to use an external product or service:

> *"It's going to be difficult to get new staff to build things yourself, so anytime you're making that decision to build in-house, you're probably going to have to stop doing something in order to find the resources to go fully build something."*

Dependencies. Participants were reliant on other teams—like product engineering, reliability engineering, or IT—to deploy and manage security mitigations. Participants rarely had direct authority over these organizations, and thus they had to navigate teams who had *"their own priorities"* and *"misaligned incentives"*:

> *"I'm rolling software out in environments that I don't own [...] I have to roll these out in IT-owned environments, or engineering-owned environments, or dev-ops owned environments."*

To do so, participants reported needing to *"have a feel for organizational will"* and to *"find things that would compel someone to do the work."* For example, participants explained that they sought opportunities to align security with other initiatives, which can help increase velocity for cross-functional efforts:

> *"If we're already doing something to upgrade a certain part of our infrastructure for reasons unrelated to security, we may choose to prioritize the security investment there."*

Disruptions. In line with participants' role of enabling business objectives, participants prioritized security decisions based on the minimal disruption it would cause to the organization. Even if an effective security control existed, participants considered its impact on velocity: *"Anytime you implement a control in the organization you have some impact on productivity."*

For example, one participant discussed how removing employees as administrators of their own devices and establishing privileged access management could prevent attacks, but simultaneously prevent network engineers who needed admin-level features when diagnosing or configuring devices to complete their job. Organization-wide disruptions required making *"sure that the senior leadership of all the groups who are going to lose potentially hours of productive work time [...] understand the urgency."*

6.4 Making Prioritization Decisions

After weighing all the factors—from risk modeling, stakeholder and external requirements, and resource constraints—CISOs decided how best to prioritize where to invest in improving security. Many CISOs noted this process was *"not super scientific."* One participant, after describing a long list of decision factors including maturity, compliance, and threat intelligence, added:

> *"But I don't want you to walk away thinking [there's] more structure than it is. Ultimately, it's pretty heavily driven by the judgment of folks—we think we've hired some really strong experts—and that judgment drives the decision-making."*

Decisions hinged on constructive engagement with stakeholders, as they *"try to work with the rest of the company to find how we move forward."* As one participant shared, prioritization was *"just*

a subjective call, but it's a collective subjective call." Participants viewed their decisions through a lens of strategic tradeoffs. They aspired to long-term thinking, despite pursuing short-term gains at times. This meant long time horizons: often year-long planning, but as far ahead as *"24, 36 months down the road."*

Participants tried to stick to their decision, unless *"suddenly something will come through a channel that'll require you to drop everything and just refocus."* While pivoting was often a necessity—*"clean up on aisle 13 constantly"*—participants emphasized the need to maintain stable and forward progress on decisions, while working in parallel to respond to incidents or crises.

6.5 Evaluating Success

CISOs described using an assortment of quantitative metrics, tests, and qualitative criteria to evaluate their programs and to identify future improvements. Despite participants relying on metrics to inform their judgment, several participants pointed out a large gap in their ability to measure what was important: *"The things that you really want to know, we don't know how to measure."* To get around this, participants evaluated performance—and thus success—from a variety of incomplete vantage points.

Passive metrics. Many participants described the importance of visibility into the company's systems and security operations. CISOs used *"a portfolio of different operational metrics"* to monitor their environments and feed back into their risk assessment. The specific monitoring and metrics that CISOs mentioned varied widely; we provide here a few illustrative examples. One participant measured *"how many spam are we stopping, how many phishing messages get caught by our email gateway"* to judge program success. Another measured *"how long it takes us from the point at which a patch is released to when is it applied across the environment, how complete is that deployment"* to inform assessment of risks from vulnerabilities. A third measured *"mean time to respond, mean time to recover"* to assess their incident response capabilities. Finally, a software maker watched for *"an uptick in quarter-to-quarter high and critical [bugs]"* in their product development lifecycle to judge whether they needed to reevaluate their development security tooling.

Metrics were also used for demonstrating security posture to external stakeholders. For instance, one participant mentioned using the number of *"people [who] have completed their security awareness training"* to appease auditors. Although appealing, these granular metrics could be misleading when not crafted thoughtfully. One participant called out potential interpretation issues:

> *"People make bad decisions because they have bad metrics, and they don't understand that the thing they're doing and the thing they think they're doing are not the same thing."*

This participant gave an example where counting components migrated to a new authentication system did not communicate actual risk reduction due to the differing importance of components.

Testing. Participants described a range of proactive testing strategies to assess their security program. For some participants, test results provided a feedback loop to inform their risk assessments. Red teaming and penetration testing were the most common; one participant described a variant in which they *"defanged"* ransomware samples and ran them against their defenses. These approaches resulted in metrics such as detection rate, speed, and which layers of defenses fired. However, penetration testing reports were taken with a grain of salt:

> *"It's really easy to write pen test reports. Just hire a bunch of morons. You're like 'whoa, there was nothing found!' Finding nothing is usually a bad thing and usually means you have bad pen testers."*

Participants also described using bug bounties to more continuously test their controls, while also gaining access to a broader set of security experts:

> *"We can invite the security research community in to work with us on a continuous basis and not just work once a year with a pen test firm [...] Bug bounty researchers tend to have more time and motivation to look for the things that slip through the cracks."*

Participants considered audit reports to be part of their evaluation strategy, either leveraging audits opportunistically or seeking out audits voluntarily. These audits had embedded scores discussing *"how many findings and the severity of those findings."*

Outcomes. Besides proactive testing, participants also discussed reactive success criteria around incidents, in part because *"outcomes are very easy to measure"*—as long as you look for incidents. One participant discussed their process:

> *"If we did get breached [...] was it some risk that we didn't anticipate, or was it a risk that we had accepted, sort of understanding the causes. So that's ultimately the success criteria, but that doesn't help you in day-to-day decision-making."*

Translating incident outcomes to business outcomes was challenging. One participant discussed retroactively reasoning about lost business: *"Did you lose that customer because they were unhappy with the last two years of service, or did you lose them because of the incident?"* Measuring outcomes thus carried limitations, as with other metrics.

Project progress. Partly due to difficulties measuring security efficacy, some participants defined success simply around the deployment progress of initiatives, completion of best practices, or the security habits and behaviors in their organization. One participant reasoned:

> *"You've got the age old issue in security of, how do you quantify something that doesn't happen? How do you quantify the incidents that you avoided because you had good practices? Well I don't pretend to be able to do that. I do find it important to track our progress on major projects."*

However, progress towards major milestones could not validate the original choice of a security control.

Business metrics. In line with participants' ultimate goal of business enablement, some participants described evaluating the success of their security program in terms of profits and losses. Questions they contemplated included *"are we making money"* and *"is security and privacy enabling us to sell more deals."* Other participants assessed whether their security team members were *"happy with their jobs."* This was meaningful to the operational success of

the organization, as *"if we lose like 2 or 3 security engineers, we're screwed."*

6.6 Prioritization Summary

Revisiting the CISO prioritization process, we find that CISOs' support of the business manifests as multifaceted and imprecise decision-making. Participants weighed technical assessments of viable security controls against multiple business considerations, including externally-forced requirements from regulators, insurers, and customers, as well as day-to-day business constraints like budget, staffing, competing priorities, and how disruptive controls might be to the organization. CISOs made these prioritization decisions in conjunction with other business stakeholders, including the board of directors, executives, and their engineering teams, but ultimately the decisions were subjective. This was in part due to our participants' reliance on a constellation of imperfect—but directional—signals like monitoring, audits, red teaming, or top-level business metrics that helped create a feedback loop on whether decisions were effective. Finally, while CISOs attempted to stick to their priorities once established for a year, incidents, emerging threats, or shifting business needs could require course correction, and thereby a reallocation of precious security resources.

7 DEPLOYING SECURITY

As described in the last section, CISOs' ability to pursue risk-reducing security measures was directly affected by the difficulty of operationalizing those measures. Exploring the sources of this difficulty, we find that *business operational complexities* were a more significant impediment to security rollouts than were technical limitations of security tools themselves. Participants explained that *"by and large, the security problems that lead to companies being compromised have known technical solutions,"* but that the expense and labor of deployment was *"administratively burdensome"* and held companies back—so much so that rather than wrestling with an incompletely or improperly deployed protection, it was easier to simply buy a new tool *"to compensate for failed deployments of existing technology."* Deployment issues led to long time horizons:

> *"At least in my experience, I think it takes like a good year to get something implemented once you plan it out and start standing it up."*

Incomplete and delayed deployments led to direct impacts on the organization's security: *"We meant to build more, typically, when we don't catch something."*

In this section, we describe the business complexities hindering security that CISOs must nevertheless support and navigate. While we discuss several specific desired controls in context with pain points, a list of commonly used classes of controls is provided in Appendix E.

7.1 The Need to Minimize Friction and Breakage

Disruptions to organizational function were antithetical to CISOs' business objectives and CISOs worked hard to minimize disruptions: *"we're not on mission if we're going to break something."* Participants most often described receiving pushback when security added friction to everyday job activities or risked breaking other systems or workflows. This pushback was not merely annoyance, but concern about impacts to critical functions of the business:

> *"Sales people are not usually the ones who are like, 'you know what I'm really happy you did? Lock down my Salesforce access.' This is not a thing that sales people generally say."*

Even seemingly simple interventions like patching systems required guardrails to minimize potential impacts. One participant described how they waited to patch on-premise systems until limited maintenance windows so customers would not be affected. The participant also described needing senior leadership buy-in for an emergency Outlook upgrade to fix a severe vulnerability, due to the vast number of employees *"who are going to lose potentially hours of productive work time."* In some cases, business agility needs made adequate security impossible. One participant described how customer support tooling, by design, requires extensive access to customer data:

> *"What's hard is there are queues to build case-driven logic to prevent customer support reps to poke around other unrelated data, but there are teams that feel almost deputized and want access to everything. Can't trigger a case that says 'investigate thing that includes 500 accounts,' can't reel in where I go look. Customer support tooling is never strong enough to prevent abuse."*

Engineering teams were particularly prone to disruption by security efforts. While CISOs were keen to introduce controls such as "shift left" code security protections and OSS vetting processes that helped engineers write more secure code, doing so hurt productivity: *"We make money by building things. I don't want to slow our team down."* As a result, CISOs could not expect developers *"to adopt some central tool that is not sufficiently well baked."* Further, security teams often relied on IT and engineering teams to roll out protections across the organization, which introduced substantial implementation delays:

> *"You might be asking to deprioritize something that's got the potential to make money for something that's going to cost us more money. And so it'd be a difficult argument to have."*

Several participants discussed application allowlisting and privileged access management solutions—those that restrict what software can execute on a machine and who can administer it—as particular points of friction. While effective against attacks, these interventions also hindered people's jobs, such as network engineers who needed admin-level features when diagnosing or configuring devices. Participants took differing approaches to this tradeoff. One described mitigating this point of friction with a highly responsive approval process that placed a high burden on the security team: *"[the engineers] need access to the software now. Not in half an hour, not in a couple hours, but now."* Another simply decided not to implement it in the foreseeable future since it was *"an administrative nightmare [that was] nearly impossible."* A third participant struck a compromise using an *"admin-by-request"* process.

Where possible, participants minimized risk of breakage using extensive *"empirical testing"* of upgrades and workflows. This could involve careful consultation with experienced security staff and

potentially affected teams, using the *"collective wisdom of the organization"* to de-risk rollouts. One participant lamented the laboriousness of empirically assessing upgrade compatibility. Another described a cross-team collaborative test:

> *"People were like, 'I'm worried that if we lock this down then we're going to have trouble with somebody who's on call.' And I was like [...] let's go test the on-call workflows, and we'll put you on call and make sure that there's a secondary who's available."*

In addition, sometimes participants entirely avoided security practices where the risk of failure was too high. One participant reported foregoing realistic simulations of a Gmail outage: *"If there could be more time, if there could be an easier way to do that and have confidence that things could come back online, that would definitely be a plus."*

7.2 Effort to Convince and Incentivize Others

Where friction or risk of breakage was inevitable in pursuit of security efforts deemed crucial, CISOs relied on extensive nontechnical efforts to persuade others to accept the security change anyway.

As other teams were not directly rewarded for secure practices, CISOs sometimes described convincing others that security was beneficial for those other teams' primary objectives. For instance, one participant convinced developers to adopt more proactive product security measures by arguing that spending more time on security early in the software launch cycle meant spending less time on incident response later. At the senior leadership level, getting buy-in hinged on *"build[ing] effective business cases."* One participant described a time when they successfully convinced the board and executive team to prioritize security by discussing various business risks and how security was the fiscally responsible thing to do for two reasons: marketing dollars depended on security because *"people need to feel safe with our platform to engage with it"*; and by not spending enough on security to meet federal regulator requirements, the organization would incur a financial penalty.

In the absence of aligned incentives, CISOs worked to creatively construct new incentives. Some participants reported using gamified per-division scorecards for *"creating accountability for security across the organization"*—though this required senior leadership buy-in for enforcement to be effective. Others described making compromises and constructing *"win-win"* arrangements:

> *"We actually relaxed our password restrictions such that if you enroll and if you use a Yubikey for your password management for MFA, then we're not going to require you to cycle your password on a regular basis [...] and we have better effective security all around."*

Even all of the above efforts were not enough. Participants described the importance of relationship-building for getting buy-in from stakeholders, where CISOs *"have to build credibility and trust in order to not have folks fight you."* Partly, this meant being cautious about what they asked for:

> *"when you come in practical, you know, you're not the one that's kind of crying wolf all the time. You're saying, 'this is real, I need it done,' and people listen and go off and do it."*

Partly this also meant building an organizational culture of security and educating other stakeholders, by means such as periodic memos and appearances at all-hands meetings. as well as in meetings with the board. *"I talk about our first line of defense is you. Everyone in the room."* Tangible case studies helped soften pushback. In response to a simulated phishing test, one participant explained:

> *"one of our accountants come[s] up to us and says, 'I don't like you doing this test to us. You are trying to trick us and we are in the middle of a really busy season' [...] I looked at her and go, you know, the test for you isn't scheduled for another 3 days. That wasn't the test. That was an actual attack [...] So it was like a light bulb going off."*

7.3 Lack of Comprehensive Visibility

Gaining visibility into business systems and operations was a constant battle for CISOs, who could not secure what they did not know existed. As individuals in the business pursued their goals, they precipitated changes in the business—both nontechnical, such as personnel turnover, and technical, such as new infrastructure. Reporting these changes to the security team was typically not on path for these other stakeholders' goals, and thus did not always occur consistently. This posed a fundamental problem for CISOs since they reported needing a complete perspective of an organization's devices, services, and environments. In reality, achieving this level of visibility was an unsolved challenge:

> *"there's always an element that you just don't know about, you can't know about. At any organization over a few dozen people you just start to lose track of some of the things that your company or employees are doing."*

Although business processes often existed to loop in the security team, they did not necessarily cover all security-relevant changes, and they could fail due to human error. One participant explained how a rushed HR application deployment was only brought to the security team's attention after it went live:

> *"I was like, hey, why are we emailing plaintext passwords? Where's two-factor authentication? [...] The process stipulates, well, this person should be educated well enough to know what the end state is, wasn't; the process is supposed to make sure that IT is involved, they weren't; when you go to test, right, you should have a reasonable sized test group with a diversity of positions around the company, it wasn't."*

Participants shared there was rarely a good starting point for enumerating all of an organization's assets:

> *"IT may have a list of endpoints, but 10 out of 10 times that I've ever looked at an IT department, and I said 'Can you show me your asset management list?' that list is always wrong. 100% of the time."*

Furthermore, achieving completeness was not a one-and-done endeavor. One participant explained that when employees leave the company, *"not everybody returns all the equipment, so you don't know whether you've lost it or whether it's still out there."* Another described completeness challenges with implementing privileged access management:

> *"There are a lot of pieces of software that we just didn't know about that our employees are using, for legitimate business purposes, and making sure that we find all of those, understand what they are, categorize them, catalog them, keep that catalog maintained, that does take a lot of work."*

Data governance, including data minimization, was one particular endeavor that CISOs pointed out as challenging on this front. Not only did they need to catalog all their data and where it was, but also they needed to establish who owned it, which was difficult to determine: *"It's the shared data pools that lack ownership and responsibility. [...] To unwind who should see it is very difficult because you don't have a central custodian."*

Visibility issues also arose when other branches of the business adopted new technologies that were incompatible with preexisting security tooling, such as containers and embedded/IoT systems: *"security folks are behind the education curve of like the DevOps folks who are kind of building this environment out [...] as new tech comes out, those who are engineers and want to build are going to go play with the new tech and the security folks need to catch up."*

7.4 Difficulties Navigating Heterogeneous Environments

Business operations and continuous changes also led to significant heterogeneity in CISOs' technical and operating environments. As business enablers, CISOs had limited agency to oppose the forces that resulted in heterogeneity, despite their repercussions for security deployability.

Participants' ability to deploy solutions was inherently complicated by the complexity of their systems and cross-service dependencies:

> *"The more homogeneous your technology is, the better chance you have of managing the risk [...] the more you have to deal with international regulations [...] the more legacy you have. Those are the things that fundamentally create difficulties in your environment."*

These difficulties were compounded at scale:

> *"You've got hundreds of thousands of devices [...] where each employee probably has multiple devices [...] and not everybody's connected to the network all the time."*

This patchwork of environments also meant that even if participants had a comprehensive list of devices, installing endpoint protections or patching systems remained tedious: *"there's very rarely an easy button to roll out agents across the whole fleet of the organization."*

Business circumstances played a significant role in driving heterogeneity. Participants from the health and education sectors attributed their heterogeneous environments in part to the specialized and/or disparate technology needs in their line of work. Business merger and acquisition (M&A) decisions also led to bringing in disparate technology leading to *"tech and security debt"*:

> *"you might buy a business because it's a commercial fit, but you may not necessarily join the technologies, so you end up with potentially parallel technology environments that are providing broadly the same services [...] there are lots of different business nuances that make it difficult to standardize, and so you end up with this replication of different tech stacks across the environment, all of which need to be protected, and operated."*

As a result, participants noted high costs for replacing systems—*"the things that require burning down the most terrible things in production, those always take longer than anything else"*—and expressed only limited agency in pushing to homogenize environments. Commonly, they instead sought to *"put protective padding"* around old or dangerous infrastructure, as well as spent effort managing exceptional cases:

> *"it's a web application and the URI during normal operation contains SQL statements in it. Which, anyone who's done web app pen testing is like, this should never happen, right, this is what attackers do when they want to enumerate your database [...] So we've kind of had to back out protections on that application in that area, because we know that they're legitimate."*

Security efforts thus benefited greatly from preexisting homogenization efforts: *"if you have a weak central CIO and a largely distributed [authority structure] ... then the CISO's job is almost impossible."*

7.5 Insufficient Staff Capacity to Manage Complex Systems

The proliferation of systems in a complex organization led to an immense amount of human labor for security teams, far exceeding their precious staff's capacity. Participants discussed being overwhelmed by the sheer scale of logs and environment configurations they had to interpret, and not being able to do so: *"We're dealing with billions of events, all the time."* Obligations to protect containerized environments could result in *"a massive amount of data, sometimes too much for an individual to even be able to parse and understand,"* due to the number of additional components involved.

In the context of detection and response, participants underscored that many tools were ineffective without constant monitoring—*"If you just deploy [EDR] and then walk away, you've wasted a whole lot of money"*—but that it was important to not overwhelm the security staff triaging leads. This challenge extended to cloud-based protections that might charge participants based on the volume of logs processed or alerts generated: *"it is potentially the most expensive [solution] depending upon how we deploy it, and we have to deploy it in a way that doesn't overload us with alerts, also doesn't generate a very large bill."* Reducing noise and spurious alerts was viewed as an imperative: *"I think that's the key to having some kind of sanity in the security world."* However, tuning the alerting thresholds was challenging, with one participant wanting *"better and easier visibility for non-security staff to really take a look at those logs and operations that are happening, and really try to identify known good baselines."*

While participants underscored the value of automating processes to cut through noise and lower expenses, automation was not without its share of labor costs. Participants praised infrastructure-as-code to reduce manual configuration effort, but noted that infrastructure code still needed to be vetted *"to identify potential misconfigurations."* Automation also wasn't a one-and-done initiative either:

> *"it's sort of a never-ending journey because your controls aren't fixed in time, like they evolve, and so you need to make sure your automation evolves with them."*

Furthermore, some tasks such as IAM configuration updates, incident response processes, and governance routines resisted automation: *"The same problem that has [always] existed in identity is still plaguing us: trying to figure out who should have access to what. [...] That's pretty resource-intensive from just a knowledge and understanding perspective."* Configuration tasks could also require input from other branches of the organization. IAM in particular drew fire: one participant described difficulties chasing down the evolving identity/role information they needed, *"because you have to talk to people and they don't know, so then you have to discover."* Another participant described an application onboarding process where *"every application team has to provide information to the access management group, to say [...] here is the logical functional activity that each entitlement within my application governs"*; as well as an access control review process that *"happens on a quarterly basis for every staff member that works for a manager for every access."*

7.6 Summary: Deployability

Business enablement for CISOs required both reducing business risks and accommodating the business operations that made risk reduction measures difficult. Navigating both was a difficult challenge: CISOs needed to roll out security interventions to a complex and incompletely-documented environment, using the limited manual labor available to them, while minimizing friction to other organizational divisions and reducing risk of breakage. These challenges could be further exacerbated by an organization's line of business, scale, and decentralized control. While CISOs had a mostly clear grasp of the security controls they most desired to implement, these organizational deployment challenges severely limited the pace of adoption, suggesting opportunities for more organizationally informed design.

8 DISCUSSION

In this work, we showed how CISOs' goals of enabling their businesses drive the risks they worry about, the complexity of their decision-making, and the difficulty in deploying solutions. Grounded in our findings, we provide takeaways for the research community and directions for future work.

8.1 Fundamental Problems Remain Unsolved

Many of the attacks that CISOs worried about—like account takeovers, software vulnerabilities, and misconfigurations—are not new. Rather, our participants described evolution of the same problems that have plagued them for years and noted that proposed solutions failed to address those problems in complex, real-world environments. In some cases, new attack variants required small modifications to procedures; in others, these escalations caused significant shifts in corporate security posture, such as overhauling multifactor authentication tooling once attackers began bypassing weak second factors like SMS.

Given that CISOs expressed a solid grasp of what it takes to solve security problems technically, it is tempting to write off many of these attacks as solved problems, where there are no interesting research questions left, simply deployment. However, solutions have, in part, been difficult to deploy because they fall short in accounting for the complexities of real-world environments and business constraints. We call on the research community to study and engage with the translational gap between seemingly "solved" problems and the challenges that practitioners face securing complex environments.

8.2 Business Needs Shape Security Posture

Throughout our analysis, we find that business enablement underpins CISOs' risk perceptions, decision-making, success criteria, and deployment constraints. This perspective serves as a useful lens through which to interrogate why fundamental security challenges persist. One aspect of business enablement that we explore is the impact of business stakeholders and their requirements on CISOs' prioritization process. Although we corroborate prior work's identification of many threat modeling inputs [31], including maturity frameworks, past attacks, threat intelligence, and peer learning, we also show that business factors such as compliance and customer demands play a larger role than previously identified. Our participants articulated the insufficiency (and sometimes counterproductive nature) of compliance for security, and yet many integrated it deeply into their decision-making processes regardless, due to its business importance. In light of complementary work exploring coverage gaps [28, 40] and security flaws [39] in existing compliance standards, we as a research community should consider compliance to be an underappreciated—and perhaps underperforming—lever for driving behavior, and a worthy target of study.

Our work is not the only one to consider tensions between security and the business. Prior literature agrees that understanding and communicating in the language of the business is key to CISOs working effectively with senior executives and boards [36]. Partly this can be viewed as a necessity due to the leadership team's lack of security expertise [10, 25], or as a means of building legitimacy in the eyes of these stakeholders [41]. We go one step further and posit that business emphasis is not simply a veneer that CISOs adopt when communicating with the board and the executive team, but a philosophy that permeates how many CISOs operate. Indeed, our participants were keenly aware of their business enablement role, including the importance of accounting for other business stakeholders' inputs and minimizing friction for the organization. As technology designers attempting to improve security, it is thus imperative that we engage with this business perspective and design for the broader business context rather than solely technical risk reduction.

8.3 Research Frontiers in Organizational Friction

Our interviews surfaced challenges that CISOs experienced while implementing security controls. Recent work has taken valuable steps towards addressing some of these issues with improved enterprise security tools, such as reducing false positives for alerts [19, 20] and identifying pain points for adopting passwordless authentication [24]. A growing body of academic literature has also focused on human-centered elements of enterprise security, including how security friction interferes with individual employees'

jobs [1, 4, 18, 29, 34] and how CISOs attempt to address this by engaging with employees [3, 17].

Yet, these are just single aspects of what makes deploying security solutions challenging in practice. Across our interviews, the obstacles to improving security that CISOs most frequently described stem from organizational behavior. CISOs must attempt to align incentives within the organization, educate and negotiate with many stakeholders, balance competing priorities under budgetary and staffing constraints, and influence a complex and evolving technical and organizational landscape where they do not always have much control. In particular, many of our participants' implementation challenges stemmed from security being necessarily secondary to the objectives of the business. This priority obliged CISOs to avoid business disruption, operate with limited resources, and accommodate the business taking calculated risks, even when this undermined perfect security. As we reframe the role CISOs have not just in security posture, but also within the organizational landscape, we can better understand their constraints and decision-making rationale.

Thus, enterprise security tools need to consider systemic *organizational friction*—the tensions resulting from misaligned incentives, internal power structures, and competing requirements that hinder enterprise security mitigations—in their design. Organizational friction may be an interesting design space for usable security. We might draw on usable security's history of centering users in the design and development of secure systems to better align different stakeholders' incentives in these tools. For the broader academic security community, assessing how solutions are adopted and deployed within organizational contexts and how adoption varies across sectors can help improve tool use and influence organizational security for the better.

8.4 Designing for Deployability

Our participants' discussion of their objectives and challenges implicate concrete, cross-cutting organizational factors that hinder or slow the adoption of security measures. Given these factors that we identify, we encourage designers to consider the *deployability* of their solutions, accounting for the operations of the broader business rather than just the security team in isolation.

To this end, we identify a set of design lessons to consider when exploring potential security interventions, based on the challenges our participants faced:

Engage with stakeholders. Participants described highly cross-functional security efforts, requiring involvement from teams with varied non-security needs—from site reliability and product engineering to HR and customer support. There is thus a rich opportunity for designers to evoke others' needs and and build for collaboration: Who are the business stakeholders who are implicated in risk and/or affected by change? How might the proposed security intervention be placed on (or become) the shortest path for others' workflow? Can it serve as a win-win to help others achieve their goals, rather than relying on the CISO cajoling them into cooperation? Or, does it demand less involvement from these other stakeholders in the first place?

Assess work requirements. Participants articulated how human labor, both within and beyond the security team, drove up costs and delays for security rollouts. Designers should document parameters such as: How much manual and/or automatable work does the proposed intervention require, both to implement (e.g., sweeping upgrades to legacy infrastructure) and to maintain/operate (e.g., monitoring a deluge of alerts)? What level of skill does this work require (e.g., security engineering training vs. basic self-taught IT experience)? What business functions does this work impose upon, and are they included as stakeholders in the design process? Does the intervention make some preexisting workload or cost unnecessary?

Account for complexity. Participants described how problems of decentralized control, constant change, and scale of infrastructure vastly complicated deployment. These factors suggest practical criteria for evaluating a proposed intervention: What preexisting knowledge (e.g., up-to-date asset inventory or access requirements) does it assume the security team has? What business changes (either technical or nontechnical) could affect solution efficacy, and how are those changes accommodated? How does the solution scale to infrastructures that are not just large, but heterogeneous?

Create a safety net. Participants worried about business disruptions due to the changes they initiated. Designers might thus consider: What systems, services, or functions are affected by a proposed intervention? What is the business consequence if a mistake or unintended consequence materializes (e.g., causing work stoppage or delays in a critical business area)? How might those enumerated possibilities be avoided or tested for, and how would the change be rolled back reliably if needed?

Define success. Participants described multifaceted signals they used to learn—and demonstrate to others—that their efforts were effective. Designers might thus ask: What metrics, tests, or qualitative observations would meaningfully accompany the proposed intervention as evaluative signals? What business conversations or decision-making could those signals facilitate or inform, both with internal and external stakeholders? How much additional effort is required to gather those success signals?

Outline the business case. Ultimately, participants underscored the need to view security in service of the overall business. In that context, designers have an opportunity to engage with CISOs' problems holistically: How does the proposed intervention interact with the assessment frameworks, stakeholder demands, and constraints that CISOs use to decide what is important? What business objectives (e.g., reducing incident-driven losses, improving customer satisfaction, or meeting compliance obligations) could it enable?

Building solutions that are less expensive and less difficult to deploy, and that are rooted in business needs and priorities, can help close the translational gap for organizational security. We hypothesize that there may be outsized benefits of this approach for organizations that are not as well resourced or whose business models do not make security as easy to argue for. Engaging with stakeholders to define realistic deployability parameters and develop solutions that meet them is a promising direction for improving enterprise security in practice.

9 CONCLUSION

Chief Information Security Officers (CISOs) play a crucial role in shaping the information security strategy of their organization.

Through 16 semi-structured interviews with current and former CISOs, we surfaced how CISOs conceptualize their role as business enablers, and how fulfilling this role is more complex than simply maximizing technical protection. We showed that CISOs' foremost focus on business success underpinned their risk perceptions, complicated their decision-making, and shaped their success criteria. Furthermore, we found that supporting the business meant accommodating systemic organizational complexities and operations that today's security tools struggle to account for, and that imperfections in security posture were an expected consequence. Taken together, these results serve as a call for the research community to consider a wider range of business and organizational realities in designing security solutions for enterprises.

ACKNOWLEDGMENTS

We thank Art Sturdevant, Grant Ho, Keith Brautingam, Olga Livingston, Stefan Savage, and members of the Stanford Empirical Security Research Group for helpful discussions during the formation of this study. We additionally thank Carrie Gates for assisting with participant recruitment, our anonymous pilot participant, and the anonymous reviewers for their feedback. We thank Tara Holliday, Lata Nair, and Opeta Henderson for their help with logistics, and Parker Ruth for graphic design assistance. This work was supported in part by a Sloan Research Fellowship, by an NSF Graduate Research Fellowship DGE-1656518, and by the National Science Foundation under Grant Number #2319080. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

[1] Eirik Albrechtsen and Jan Hovden. 2009. The information security digital divide between information security managers and users. *Computers & Security* 28, 6 (2009), 476–490.

[2] Sultan AlGhamdi, Khin Than Win, and Elena Vlahu-Gjorgievska. 2020. Information security governance challenges and critical success factors: Systematic review. *Computers & security* 99 (2020), 102030.

[3] Debi Ashenden and Angela Sasse. 2013. CISOs and organisational culture: Their own worst enemy? *Computers & Security* 39 (2013), 396–405.

[4] Adam Beautement, M. Angela Sasse, and Mike Wonham. 2008. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop*. Association for Computing Machinery, New York, NY, USA, 47–58.

[5] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. https://doi.org/10.1191/1478088706qp063oa

[6] Virginia Braun and Victoria Clarke. 2021. To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales. *Qualitative research in sport, exercise and health* 13, 2 (2021), 201–216.

[7] Virginia Braun and Victoria Clarke. 2022. Conceptual and design thinking for thematic analysis. *Qualitative psychology* 9, 1 (2022), 3.

[8] Kevin Collier. 2023. Cyberattack cost MGM Resorts about $100 million, Las Vegas company says. https://www.nbcnews.com/business/business-news/cyberattack-cost-mgm-resorts-100-million-las-vegas-company-says.

[9] Crowdstrike. 2024. The leader in endpoint security. https://www.crowdstrike.com/platform/endpoint-security/.

[10] Joseph Da Silva and Rikke Bjerg Jensen. 2022. "Cyber security is a dark art": The CISO as Soothsayer. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2, Article 365 (Nov. 2022), 31 pages.

[11] Gartner. 2023. Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024. https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024.

[12] Marilu Goodyear, Holly T. Goerdel, Shannon Portillo, and Linda Williams. 2010. Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers. *Available at SSRN 2187412* (2010).

[13] Google. 2024. Overview of Event Threat Detection. https://cloud.google.com/security-command-center/docs/concepts-event-threat-detection-overview.

[14] Rohan Goswami. 2023. SEC sues SolarWinds over massive cyberattack, alleging fraud and weak controls. https://www.cnbc.com/2023/10/31/solarwinds-defrauded-investors-about-cybersecurity-sec-alleges.html.

[15] Andy Greenberg and Matt Burgess. 2024. The Mystery of 'Jia Tan,' the XZ Backdoor Mastermind. https://www.wired.com/story/jia-tan-xz-backdoor/.

[16] Husam Haqaf and Murat Koyuncu. 2018. Understanding key skills for information security managers. *International Journal of Information Management* 43 (2018).

[17] Jonas Hielscher, Uta Menges, Simon Parkin, Annette Kluge, and M. Angela Sasse. 2023. "Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security. In *USENIX Security*. USENIX Association, Anaheim, CA, 2311–2328.

[18] Jonas Hielscher, Markus Schöps, Uta Menges, Marco Gutfleisch, Mirko Helbling, and M. Angela Sasse. 2023. Lacking the Tools and Support to Fix Friction: Results from an Interview Study with Security Managers. In *Symposium on Usable Privacy and Security (SOUPS 2023)*. USENIX Association, Anaheim, CA, 131–150.

[19] Grant Ho, Mayank Dhiman, Devdatta Akhawe, Vern Paxson, Stefan Savage, Geoffrey M Voelker, and David Wagner. 2021. Hopper: Modeling and detecting lateral movement. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 3093–3110.

[20] Grant Ho, Aashish Sharma, Mobin Javed, Vern Paxson, and David Wagner. 2017. Detecting credential spearphishing in enterprise settings. In *26th USENIX security symposium (USENIX security 17)*. USENIX Association, Vancouver, BC, 469–485.

[21] Val Hooper and Jeremy McKissack. 2016. The emerging role of the CISO. *Business Horizons* 59, 6 (2016), 585–591.

[22] Nicolas Huaman, Bennet von Skarczinski, Christian Stransky, Dominik Wermke, Yasemin Acar, Arne Dreißigacker, and Sascha Fahl. 2021. A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises. In *USENIX Security*. USENIX Association, 1235–1252.

[23] Allen C Johnston and Ron Hale. 2009. Improved security through information security governance. *Commun. ACM* 52, 1 (2009), 126–129.

[24] Leona Lassak, Elleen Pan, Blase Ur, and Maximilian Golla. 2024. Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication. In *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Philadelphia, PA, 7231–7248.

[25] Michelle R. Lowry, Anthony Vance, and Marshall D. Vance. 2021. Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity. *Available at SSRN 4002794* (2021).

[26] Stuart Madnick. 2024. What's Behind the Increase in Data Breaches? https://www.wsj.com/tech/cybersecurity/why-are-cybersecurity-data-breaches-still-rising-2f08866c.

[27] Sean Maynard, Mazino Onibere, and Atif Ahmad. 2018. Defining the strategic role of the Chief Information Security Officer. *Pacific Asia Journal of the Association for Information Systems* 10, 3 (2018), 3.

[28] Henock Mulugeta Melaku. 2023. A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy* 3, 3 (2023), 327–350.

[29] Uta Menges and Annette Kluge. 2024. Contrasting and Synergizing CISOs' and Employees' Attitudes, Needs, and Resources for Security Using Personas. In *2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 456–472.

[30] Microsoft. 2024. Microsoft Defender for Cloud. https://www.microsoft.com/en-us/security/business/cloud-security/microsoft-defender-cloud.

[31] Tyler Moore, Scott Dynes, and Frederick R Chang. 2016. Identifying How Firms Manage Cybersecurity Investment. In *Workshop on the Economics of Information Security*. 1–27.

[32] Lily Hay Newman. 2023. Okta's Latest Security Breach Is Haunted by the Ghost of Incidents Past. https://www.wired.com/story/okta-support-system-breach-disclosure/.

[33] Lorelli S Nowell, Jill M Norris, Deborah E White, and Nancy J Moules. 2017. Thematic analysis: Striving to meet the trustworthiness criteria. *International journal of qualitative methods* 16, 1 (2017), 1609406917733847.

[34] Lena Reinfelder, Robert Landwirth, and Zinaida Benenson. 2019. Security Managers Are Not The Enemy Either. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–7.

[35] Harry Robertson. 2023. ION brings clients back online after ransomware attack. https://www.reuters.com/technology/ion-starts-bring-clients-back-online-after-ransomware-attack-source-2023-02-07/.

[36] Zeynep Sahin and Anthony Vance. 2025. What do we need to know about the Chief Information Security Officer? A literature review and research agenda. *Computers & Security* 148 (2025), 104063.

[37] Stef Schinagl and Abbas Shahim. 2020. What do we know about information security governance? "From the basement to the boardroom": towards digital security governance. *Information & Computer Security* 28, 2 (2020), 261–292.

[38] Zahoor Ahmed Soomro, Mahmood Hussain Shah, and Javed Ahmed. 2016. Information security management needs more holistic approach: A literature review. *International journal of information management* 36, 2 (2016), 215–225.

[39] Rock Stevens, Josiah Dykstra, Wendy Knox Everette, James Chapman, Garrett Bladow, Alexander Farmer, Kevin Halliday, and Michelle L Mazurek. 2020. Compliance Cautions: Investigating Security Issues Associated with US Digital-Security Standards. In *NDSS*.
[40] Rock Stevens, Faris Bugra Kokulu, Adam Doupé, and Michelle L Mazurek. 2022. Above and Beyond: Organizational Efforts to Complement US Digital Security Compliance Mandates. In *NDSS*.
[41] Anthony Vance, Michelle Lowry, and Zeynep Sahin. 2022. Taking a Seat at the Table: The Quest for CISO Legitimacy. In *International Conference on Information Systems*.
[42] Merrill Warkentin and Allen C Johnston. 2016. IT governance and organizational design for security management. In *Information security*. Routledge, 46–68.
[43] Tom Warren. 2024. Microsoft 'senior leadership' emails accessed by Russian SolarWinds hackers. https://www.theverge.com/2024/1/19/24044561/microsoft-senior-leadership-emails-hack-russian-security-attack.
[44] Wiz. 2024. Detect, Investigate, and Respond to Cloud Threats. https://www.wiz.io/lp/nb-cdr-b.
[45] Flynn Wolf, Adam J. Aviv, and Ravi Kuber. 2021. Security Obstacles and Motivations for Small Businesses from a CISO's Perspective. In *USENIX Security*. USENIX Association.
[46] Moti Zwilling. 2022. Trends and challenges regarding cyber risk mitigation by CISOs—A systematic literature and experts' opinion review based on text analytics. *Sustainability* 14, 3 (2022), 1311.

A COMPLIANCE PROGRAMS

CISOs commonly referenced SOC 2 Type II (13/16), PCI DSS (10/16), and GDPR (10/16) as well as the NIST CSF (12/16), NIST 800 series (9/16), and CIS (7/16) frameworks (Figure 2). Although compliance requirements are often thought of as industry-specific, we observed these requirements often affect other organizations too. For example, financial institutions, an educational institution, and a SaaS company indicated that they are beholden to HIPAA.

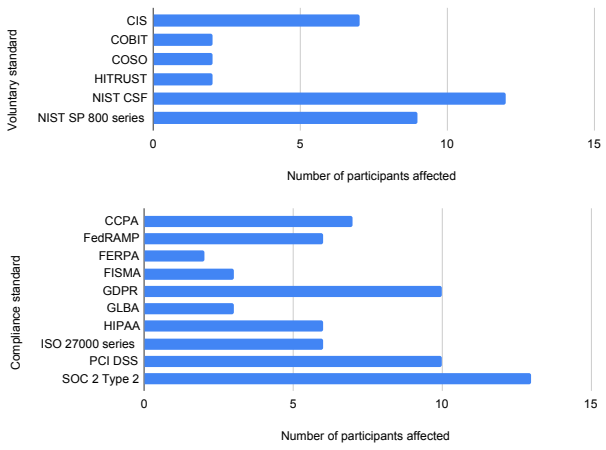

Figure 2: Voluntary and compliance standards affecting participants' day-to-day activities.

B PRE-INTERVIEW SURVEY QUESTIONS

B.1 Background Information

The questions below will help us set up for your interview. We appreciate you taking a minute to answer them in advance.

1. What is your job level? (Mark only one)
   - CISO or equivalent head of security
   - VP or equivalent direct report to C-suite
   - Director or equivalent senior management
   - Other:
2. How many years of experience do you have in security? (Mark only one)
   - 1 – 5
   - 6 – 10
   - 11 – 15
   - 16 – 20
   - More than 20
3. How many people work in the security group that you lead? (Mark only one)
   - 1 – 20
   - 21 – 50
   - 51 – 100
   - 101 – 200
   - 201 – 500
   - 501 – 1000
   - More than 1000
4. Which of the following are you responsible for in your current role? (Check all that apply)
   - Operational security (e.g., protecting customer or user data, preventing ransomware)
   - Product security
   - Physical security (e.g., facilities, data centers)
   - Privacy
   - Compliance
   - Other:
5. What security standards or compliance programs affect your day-to-day operations? (Check all that apply)
   - CCPA
   - CIS
   - COBIT
   - COPPA
   - COSO
   - FAIR
   - FedRAMP
   - FERPA
   - FISMA
   - GDPR
   - GLBA
   - HIPAA
   - HITRUST
   - ISO 27000 series
   - NIST CSF
   - NIST SP 800 series
   - PCI DSS
   - PIPEDA
   - SOC 2 Type 2
   - N/A (this is not my job scope)
   - Other:
6. Is there anything you'd like to clarify about any of your responses?

C INTERVIEW PROTOCOL

C.1 Risks

[IF they didn't fill out the background survey:] Walk through the pre-interview survey questions.

(1) What are the biggest security risks you think currently face your organization?
(2) How do you think your top risks differ from those of other organizations?
(3) **[IF business outcomes:]** What are the attack vectors you're most worried about that could cause those business outcomes?
(4) **[IF attack vectors:]** What are the business outcomes you're most worried about as a result of those attack vectors?
(5) **[IF vague risk / threat:]** What are the attack vectors that you think could lead to [that risk, say large data breach]
(6) What are some of the biggest risks on the horizon that you're concerned about?
(7) Which risks are you prioritizing right now, and why?
(8) What are the lower priority risks that you'd get to if you could but can't in the near term?
(9) How often does your risk prioritization change?
(10) **[IF they change often]** What's driving those changes? **[ELSE]** What makes those risks such a constant presence for you?
(11) Do you have periodic times, annually say, where you re-evaluate all of this?
(12) What's an example of an event (that you can remember) where something happened that shifted your prioritization?

C.2 Priorities

(1) What past initiatives have you implemented that have had the biggest impact on your current security posture?
(2) What are the most exciting or important ongoing initiatives you're working on to address your highest priority risks moving forward?
(3) **[IF answers all center around processes]** What about in terms of technologies or infrastructure?
(4) **[IF answers all center around technologies]** What about in terms of processes or procedures?
(5) Which of your current initiatives are most challenging or resource-intensive? What makes these things challenging?
(6) What initiatives do you want to launch but can't? Why?
(7) How do you prioritize/triage security initiatives?
(8) How do you balance tactical, short-term initiatives vs. strategic, long-term initiatives? (e.g., how hard is it to set aside resources for longer-term initiatives? What proportion of time or budget is dedicated to various planning horizons?)
(9) **[IF they mention outsourcing security functions to external vendors]** How do you decide what security functions to build in-house vs. buy from an external vendor?
(10) Where do you draw the line for "good enough"? How do you decide what's unimportant?
(11) How do your security priorities differ from other organizations?
(12) **[IF responsible for compliance]** You mentioned you're also responsible for compliance. How does compliance fit into your overall security strategy?
(13) **[ELSE]** What's your relationship with compliance like and how does compliance interact with your overall security strategy?
(14) **[IF responsible for privacy]** You mentioned you're also responsible for privacy. How does privacy fit into your overall security strategy?

C.3 Success Metrics

(1) What are your success criteria?
(2) Are there other parties, such as auditors, insurance providers, or customers, that influence your success criteria?
(3) How do multiple of these stakeholder priorities interact/conflict?
(4) Who do you report to, and what are the pros/cons of that?
(5) How do you measure or track success?

C.4 Challenges

(1) What are some of the biggest roadblocks to executing your security mission? (Money, talent shortage, etc.)
(2) What organizational constraints / roadblocks are most significant for you being successful in your security mission?
(3) Where do you get pushback when you're trying to roll out an initiative, and why?
(4) What about the infrastructure you're running? What challenges does your tech setup present?
(5) What technologies or processes are you most excited about to address your challenges?
(6) Do you think that the security community is solving (or working on solving) the problems that are pressing to you?
(7) In the next 3-5 years, do you think it will become easier or harder to achieve security outcomes? Why?

C.5 Information Sources

(1) Who do you think is getting security right (e.g., other CISOs)?
(2) What other organizations or sources of information influence your thinking about this space (analysts, federal advisories, etc.)?
(3) What kind of level-setting or information-gathering are you able to do from information shared by peers and other security leaders?

C.6 Closing

Is there anything else on your mind that you'd like to share with us before we wrap up?

D CODEBOOK

Here we include the list of high-level codes we applied to participant quotes, along with summarized definitions of each. Codes were not mutually exclusive.

Codes related to risks.

- What puts them at risk: Why attackers may want to target this organization (e.g., resources, security posture)
- Explicit thoughts about risk framing: How they define risk
- Business concerns: Risks framed around impact to the business (e.g., financial loss, business continuity, reputational damage, ransomware/extortion)
- Attack vectors: Risks framed around attacker tactics or exploitation of weaknesses (e.g., phishing, endpoint compromise, exposed cloud-stored data, third party compromise)

- Attacker's identity: Risks framed around who the attacker is (e.g., automated low-skilled attackers, nation-states, insiders)
- Future of security risks: Changes, and frequency of changes, in the risk landscape

Codes related to the shape of CISOs' approach.

- Perspectives on the CISO role: Reflections on their philosophy or approach (e.g., relationship to the business, no magic formula, finding win-wins)
- Decision factors around risks: Decision-making inputs around risks, threats, or weaknesses (e.g., current attacks, risk register, peer consensus, likelihood/impact assessment, information sources)
- Decision factors around practicality: Decision-making inputs around the practicality or implementability of solutions (e.g., cost and time to implement, friction for business, efficacy)
- Decision factors around stakeholders: Decision-making inputs around stakeholders they try (or don't try) to please (e.g., rest of executive team, auditors, customers)
- Technical solutions: Technical initiatives that they think are or were helpful for security (e.g., passwordless authentication, EDR, bug bounty, automation)
- Nontechnical solutions: Nontechnical initiatives that they think are or were helpful for security (e.g., team restructuring, policy development, vetting new employees, awareness training)
- How or why they use solutions: What factors make their chosen solutions desirable or effective (e.g., risk reduction, allocation of labor, ease of implementation)
- Devil in the details: Why implementing solutions is easier said than done (e.g., alert volumes, integration challenges, vendor ecosystem complaints)

Codes related to compliance.

- Impact on security: How security and compliance relate to each other (e.g., closely aligned, orthogonal, subset relationship)
- Perspectives on compliance program: Elaborations on their approach to compliance
- Specific mentions: Discussions of particular compliance standards (e.g., FIPS, NIST CSR, PCI, SOC 2)

Codes related to success criteria.

- What success criteria: Quantitative or qualitative success criteria they use (e.g., metrics, scorecards, project progress, support of business objectives)
- How or why certain success criteria: What needs these success criteria are fulfilling (e.g., visibility, accountability, alignment with business vision)
- Challenges with success criteria: What makes tracking or measuring success difficult (e.g., hard to quantify, uncertainty)

Codes related to org dynamics.

- How they work with others: Strategies for interpersonal or cross-team interactions
- Power distribution challenges: Challenges related to who controls what in the org (e.g., decentralized structure, not owning environments, reporting relationships)
- Business challenges: Challenges related to interfacing with business priorities, operations, or finances (e.g., budgeting, talent pool, incentives)
- Cultural challenges: Challenges related to how people perceive the CISO's initiatives or messaging (e.g., resistance to change, developer culture, communication challenges with leadership)

Other codes.

- Privacy: Comments on privacy
- Perceptions of other orgs: Perceived differences or other observations around orgs or sectors other than their employer
- Other: Long tail of participant comments

Security Control	Examples	CISOs
Detection & Response	Scanning, endpoint detection and response (EDR), anti-virus (AV), logging, monitoring, threat intel, incident response	16
Vulnerability Patching & System Hardening	Patching, sandboxing, code reviews, penetration testing, key management, network segmenting, vendor audits, application whitelisting	15
Identity & Access Management	Two-factor, zero-trust, least privilege, access control	13
Non-technical	Training, hiring, governance, policy, on-call processes	13

Table 3: Top-of-mind Security Controls for CISOs

E COMMONLY USED SECURITY CONTROLS

The individual security controls CISOs selected to implement were business- and context- dependent, with a long tail that is challenging to enumerate. Zooming out, however, we characterize the general classes of our participants' favored security controls. We present a breakdown of the most popular, top-of-mind classes of security controls in Table 3. Below, we describe the motivation behind selecting these controls and control-specific challenges.

Detection and Response. Every participant discussed implementing security controls that allowed them to have visibility across their device fleet and environment to log, detect, and respond to threats:

> *"The space we operate, you can't see it, you can't touch it, you can't smell it, you can't hear it, [...] Logging for*

> *data collection is your eyes and ears of what's going on around you."*

Popular tools included end point detection and response (EDR), anti-virus (AV), network traffic scanning, and numerous other technologies. Participants discussed developing processes around these tools to ingest third-party threat intelligence to trigger alerts, or building investigation tools to respond to potential security failures.

Vulnerability Patching and System Hardening. Nearly every CISO (15 of 16) discussed being inundated with work associated with patching systems, catching misconfigurations, and maintaining basic service hygiene. Keeping pace was a constant challenge:

> *"The volume of vulnerabilities that are being disclosed and the challenges of maintaining the health and hygiene of [our] perimeter is an ongoing challenge, which is just a constant drain of resources, and a constant source of risk."*

Multiple participants noted the never-ending stream of vulnerabilities that they need to patch: *"It's all clean, rinse, repeat. It's like digging a ditch and someone is kicking dirt in it the whole time. You patch today, and you will have to patch again later."*

Identity & Access Management. A majority of participants leveraged identity and access management (IAM) as part of their security strategy (13 of 16). This included enacting least privilege for accounts, enabling two-factor, configuring service access, and more. Participants shared that, with the emergence of cloud infrastructure, software-as-a-service, and zero-trust, IAM was becoming increasingly important due to the loss of network perimeter:

> *"As more orgs lose their perimeter, identity is the thing we focus on to make sure security controls are adequate."*

However, participants pointed out that *"identity and access management is very challenging for organizations."* In particular, participants pointed at the interoperability challenges of onboarding and configuring IAM for multiple, distinct third-party services: *"The same problem that has [always] existed in identity is still plaguing us: trying to figure out who should have access to what. [...] That's pretty resource-intensive from just a knowledge and understanding perspective."*

Non-Technical Controls. A majority of participants mentioned some form of improving non-technical or governance controls within their security strategy (13 of 16). Examples included writing policies, hiring additional security staff, training employees company-wide on security processes, and more. Participants recognized the difficulty of effective employee training:

> *"[It's] a known thing that you just always have to invest in [education] [...] I think we can all be honest and say that we know most people don't pay much attention to [training] videos, so what are the ways that we can actually get the information that our employees need to be aware of from a security perspective into their hands in a way that actually sticks?"*

Automation. While not a direct security control, four participants noted investment in automating their security processes to reduce manual work: *"The highest value activities are activities that can be automated."* This was often out of necessity: *"Can processes be made more efficient to serve those purposes and [lower] expenses?"* Here, participants discussed promising recent advances in artificial intelligence that were helping them scale:

> *"Process automation is something we didn't have a lot of, it's relatively new in cyber. [...] Now I have a system with an AI attached that does log review. [It] can go through a billion logs in a few hours, where a human would have to prioritize which logs to look at and it might take all week."*