Four CISO tribes and where to find them

Version 2.0

Gary McGraw, Ph.D.
Sammy Migues
Brian Chess, Ph.D.

Table of contents

Introduction

If you are a CISO, this work is for you. Turns out that CISOs are humans, and humans sometimes worry about what they're doing and why. They ask questions such as, How do I stack up against my peers? What is it that everyone else does in this role? Am I missing something obvious that everyone else already knows? What can I do to improve my performance? These are just four of the many questions we intend to answer in this work. Our overarching goal is to describe what a CISO does all day and how that work gets organized and executed.

Data matter, especially in computer security. As scientists, we like to gather data and then describe the data we've gathered in a coherent model. This is the approach we took in the BSIMM Project, and it is the same approach we take in this project.

We gathered data in a series of extended in-person interviews with 25 CISOs. The firms we chose to study include ADP, Aetna, Allergan, Bank of America, Cisco, Citizens Bank, Eli Lilly, Facebook, Fannie Mae, Goldman Sachs, HSBC, Human Longevity, JPMorgan Chase, LifeLock, Morningstar, Starbucks, and U.S. Bank. Collectively, our population represents just under 150 years of experience in the CISO role.

Though we knew when we started this project that our results would be data-driven, we had no idea what kinds of things we would uncover. As it turns out, we set ourselves up for some hard work. CISOs are all individuals with modes of operation that have been influenced by long and distinguished careers. We produced an initial version of this report in 2016 based on analysis of data from 12 CISOs. With double the population size (25 CISOs), the current version of the report validates and refines our model.

We identify four distinct approaches to the CISO role, each with unique characteristics and discriminators. We describe the four "tribes" below, with an emphasis on what separates one from another (as opposed to what makes them all the same). Dividing CISOs into tribes leads to some insight with regard to career development and progression. We believe that when CISOs understand their own approaches with reference to others, they will be better informed about their own ways forward.

What we're not going to talk about:

The generic CISO

Sadly, the usual drivel written about the CISO role is put together by people who are not CISOs, have never been CISOs, and may not even know any actual CISOs. That bothers us. Results are often presented as a laundry list of one-size-fits-all items that can be ticked off like merit badges, as though the size of one's list of controls determines the best CISO. We are going to avoid the laundry list approach in this work.

Though we did end up with lists of controls and reams of technical security information in our data, we focus our discussion on other aspects of the CISO role. In particular, we're interested in how the four tribes we have identified differ in executing a security plan, and what the tribes may be able to learn from one another.

In the real world, two major factors are more important than any others when it comes to success in the CISO role: the person and the organization—that is, the personality and experience of the leader, and the culture, security willingness, and resources of the company. The tricky question is whether either of these factors can be changed or evolved in any given situation. Can a zebra change its stripes if it is trapped in the zoo?

Before we set out on our in-person interviews, our approach was to devise a framework for use in guiding the conversations. Of course, in cases like this, the framework itself needs to be based on actual data! As step zero, we conducted a series of phone conversations to gain a basic understanding of main topics, key words, and other ways to divide up the CISO problem space.

We identified three domains that every firm had in common. They are Workforce, Governance, and Controls (or in slightly more hackneyed terms, People, Process, and Technology). These three domains help to organize our results in a meaningful pattern.

The Workforce domain covers people and includes organizational structure, Board interaction, goals/MBOs, and staff development.

The Governance domain covers process and includes metrics, reporting rhythm, budgets, Line of Business interaction, and project management.

Finally, the Controls domain covers technology and includes cyber security frameworks, risk management, network operations, incident response, security features, assessment and vulnerability management, threat intelligence, software security, and vendor control. Of the three domains, the Controls domain ran the largest risk of becoming a laundry list, which, as we mentioned above, was something we set out to avoid.

We also discussed peer groups, role consistency, and evolution of the CISO role with each of our participants.

Using this three-domain CISO framework, our 25 in-person interviews generated lots of real-world data.

WORKFORCE	GOVERNANCE	CONTROLS
Organization Structure	Metrics	Framework
Management	Budget	Vulnerability Management
Staff	Projects	Vendors

Data from real live CISOs

Based on the data we gathered, we identified four groups of CISOs that we call the four tribes. They are:

- Tribe 1: Security as Enabler
- Tribe 2: Security as Technology
- Tribe 3: Security as Compliance
- Tribe 4: Security as a Cost Center

In our model, membership in one tribe is mutually exclusive with membership in other tribes. Each of the 25 CISOs fits into one of these four tribes.

Our working theory is that any CISO will fall into one of these four tribes. Further, knowing what tribe you are in can help you plan to evolve and improve in the most efficient manner.

We will describe each of the four tribes in detail below, but before we do that, we introduce a set of discriminators that can be used to differentiate the tribes.

18 discriminators

What sets apart our four tribes of CISOs? Are there particular aspects of the four tribes that differ from one another in important ways? Can these differences be meaningfully organized? The answer to all three of these questions can be found in what we call discriminators.

Simply put, discriminators can be used to tease apart CISOs from different tribes. And, not surprisingly, discriminators help clarify what makes any particular tribe tick. Finally, discriminators can be used to influence strategy directly and efficiently.

To cohere with our CISO framework, we chunk discriminators into our three domains of Workforce, Governance, and Controls. Each of the 18 discriminators is given a number in Roman numerals (I through XVIII). The Workforce domain encompasses eight discriminators (I–VIII). The Governance domain encompasses five discriminators (IX–XIII). The Controls domain encompasses five discriminators (XIV–XVIII).

I. CISO executive stance

II. CISO-Board relations

III. CISO curation of security message

IV. CISO and compliance

V. Security organization structure

VI. Security career path

VII. Security alignment with business

VIII. Company culture and security

IX. KPIs, KRIs, and metrics

X. Security and crisis

XI. Program management

XII. Budget

XIII. Risk management and technical debt

XIV. Cyber security framework

XV. Security controls

XVI. Vulnerability management, risk, and threats

XVII. Lines of Business alignment

XVIII. SSI measurement

Each of the 18 discriminators can have up to four subentries describing how that particular discriminator is mapped into each tribe. For example, discriminator I is called "CISO executive stance." This discriminator has four subentries, one for each of the four tribes. Each of these subentries is labeled with its associated tribe as follows: T1 = Enabler, T2 = Technology, T3 = Compliance, T4 = Cost Center. For example, I.T1 is the subentry for discriminator I, Tribe 1. Take a quick look at discriminator I, below, and our scheme will become clear.

In some cases, a discriminator does not have a subentry for each of the four tribes. That's because there is no difference between two particular tribes in the case of that discriminator. For example, discriminator II, "CISO-Board relations," has one subentry shared between T1 and T2. When there is no change in a subentry with respect to tribes, that subentry is labeled with all relevant tribes (in some cases, up to three tribes share one subentry).

No individual discriminator alone can be used to categorize a tribe. Tribes are associated with sets of discriminators. In addition, discriminator subentries associated with the four tribes do not always have contiguous boundaries. That is, they may not perfectly describe any individual CISO. For example, the subentries for discriminator II describe just three of all possible types of CISO-Board relationships.

For now, what's most important is understanding each of the 18 discriminators we listed above without worrying too much about subentries. We provide the subentries here so you can refer back to this section later.

Using these 18 discriminators, we discuss the four tribes in some detail.

EIGHT WORKFORCE DISCRIMINATORS

I. CISO executive stance

I.T1 The CISO is a seasoned senior executive. While often having a deep technical past, the CISO focuses much more attention on the business and less on technology.

I.T2 The CISO has a deep technical past and in many cases may still be known primarily for technical work. The CISO has solid business skills, which may still be developing.

I.T3 The CISO is a seasoned senior executive without a deeply technical past. The CISO is often an excellent administrator.

I.T4 The security leader, whose title is likely not CISO but who remains at the top of the security heap, is a technology person.

II. CISO-Board relations

II.T1-T2 The CISO enjoys direct interaction with and influence on both the CEO and the Board.

II.T3 The CISO enjoys direct interaction with the CEO. Board interaction likely includes attendance but not direct education about security.

II.T4 The security leader lacks a collegial relationship with either the CEO or the Board. While the CEO and Board might know the security leader by sight, the security message is filtered through other layers of senior management before it gets to the top.

III. CISO curation of security message

III.T1-T2 The CISO curates Board understanding of security, which is well past a compliance-only view.

III.T3 The CISO does not curate a well-mapped Board understanding of security. Though the Board may understand that compliance alone is insufficient, they remain hazy about security goals.

III.T4 The Board has limited understanding of cyber security, is not being educated, and may be driven by popular press. In many cases, the Board is made aware of security activity without any grounding in actual risk to the firm.

IV. CISO and compliance

IV.T1 The CISO has moved the firm from compliance to commitment.

IV.T2 The CISO has moved the firm past compliance as the goal, but work remains to be done to integrate security into the business.

IV.T3 The firm is finishing up or actively working compliance requirements and has identified the next set of security goals but is not executing against them.

IV.T4 The security program is limited to compliance and is seriously resource constrained.

V. Security organization structure

V.T1 Security organization structure reflects the firm's business focus and is not only technology driven. In the case of global firms, geography often plays a role in organization structure.

V.T2 Security organization structure is built around technical goals and objectives and may not reflect the business focus of the firm, but understaffing is not a problem.

V.T3 Security organization structure is built around technical goals and objectives and may not reflect the business focus of the firm. In addition, understaffing can be a problem.

V.T4 The security organization is understaffed even to achieve compliance.

VI. Security career path

VI.T1 A career path in security is well-defined and includes succession planning and direct executive mentorship. Roles among direct CISO reports are often non-technical.

VI.T2 A career path in security is well-defined and includes succession planning and direct executive mentorship. However, career advancement tends to overemphasize technical security prowess even though there are some direct efforts to teach about the business.

VI.T3 A career path in security is murky and is probably non-technical even though responsibilities are technical.

VI.T4 Security work is tactical in nature, is often only technical, and does not align with obvious career progression.

VII. Security alignment with business

VII.T1 Employee development in security is aligned with the business and includes leadership finishing school (just like the opportunities found outside security).

VII.T2 Employee development in security is not clearly aligned with the business and tends to overemphasize the technical.

VII.T3 Employee development in security is aligned with the business.

VII.T4 While there are promotions and title changes, security purview is limited to the technical weeds. Without two-way understanding of and by the business, security staff goals are constrained to the now and do not help prepare them or the firm for the future.

VIII. Company culture and security

VIII.T1-T2 Company culture aligns with security and is partially defined by security.

VIII.T3 Company culture is beginning to align with security at senior executive levels. However, harmonized vision is not yet driven down, sometimes even in the security organization itself.

VIII.T4 Company culture is not conducive to security. Compliance is the one and only currency.

IX. KPIs, KRIs, and metrics

IX.T1-T2-T3 Together with direct reports, the CISO determines which Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) to collect, track, and report.

IX.T4 Metrics tend to be counts of effort. There is little or no evidence of transforming raw data into KPIs/KRIs important to the business.

X. Security and crisis

X.T1 Security has become business as usual. No crisis required.

X.T2 Security is not yet business as usual, though there may be a plan and unity of purpose. A crisis may have been the catalyst for renewed security effort and a change in philosophy.

X.T3 Security is not yet business as usual, and compliance requirements may not be fully accounted for. A crisis may have caused a change in security leadership and the smoke has not yet cleared.

X.T4 Budget may include a pot of money for an anticipated crisis (one allowed per year).

XI. Program management

XI.T1-T2-T3 A Program Management Office (PMO) drives projects forward.

XI.T4 No PMO exists for project management, which is instead handled directly by staff.

XII. Budget

XII.T1 Budget is never an issue, because the Board and senior executives are aligned with the security mission. Funding within the agreed-on security mission is always possible.

XII.T2 Budget is not really an issue, because the Board and senior executives are aligned with the security mission. However, uptake in Lines of Business can be problematic when the firm is not completely aligned with security.

XII.T3 Resources are tight and underinvestment is common. Investment is limited to compliance efforts.

XII.T4 Security is managed like a cost center and is not provided adequate resources. Security apparatus is often paid for by taxing Lines of Business directly.

XIII. Risk management and technical debt

XIII.T1-T2 Security is treated as risk management. Technical debt is understood and accounted for in the risk management paradigm.

XIII.T3 Security is treated as risk management. However, technical debt is not accounted for in the risk management paradigm.

XIII.T4 Security is limited to a compliance exercise. Security has little or no handle on technical debt.

XIV. Cyber security framework

XIV.T1-T2 A cyber security framework (e.g., the NIST framework) is used proactively to drive the security story forward.

XIV.T3 A cyber security framework (e.g., the NIST framework) is used proactively to drive the security story forward. Use of the framework may not be creatively tailored to the business.

VIX.T4 There is no underlying cyber security framework.

XV. Security controls

XV.T1-T2 Top security controls include Identity and Access Management (IAM), use of cryptography, and logging and analysis.

XV.T3 Top security controls, including IAM, use of cryptography, and logging, are still lagging. Projects to improve all three are underway.

XV.T4 Top security controls are in a state of flux at best. IAM may be completely ignored, use of cryptography is haphazard, and logging is weak.

XVI. Vulnerability management, risk, and threats

XVI.T1 The security organization has moved the vulnerability management exercise well past penetrate and patch and is driven by risk.

XVI.T2 The security organization has moved the vulnerability management exercise well past penetrate and patch but is driven by threat instead of risk.

XVI.T3 Vulnerability management is behind the curve, but plans are in the works to address the problem. Threat intelligence and other similar exercises are limited to what is purchased without customization.

XVI.T4 Patch management is the tail that wags the defect management dog. Network security basics may not be in place (think network segmentation).

XVII. Lines of Business alignment

XVII.T1 Lines of Business go along with security requests and do the right thing. This happens even though the requests may not be in their best short-term interest, because they are aligned with the security mission and the security mission is aligned with them.

XVII.T2 Security provides Lines of Business a set of services that may not in all cases be aligned with the business. Because of this, uptake in Lines of Business may vary.

XVII.T3 A past security crisis is being used as a lever to force security into Lines of Business.

XVII.T4 Security is provided as a service to Lines of Business, which may choose to ignore the services entirely. Security advises but probably cannot enforce.

XVIII. SSI measurement

XVIII.T1-T2-T3 The BSIMM is used to measure software security progress.

XVIII.T4 A software security initiative is nonexistent or nascent.

The 18 discriminators and their subentries are reproduced in table form as Appendix A.

Think of discriminators as vectors defining a space. To move from one shape (or tribe) to another, changes in the associated set of discriminators are required (and can be observed and measured). Thus, knowing your discriminators (and your tribe) is the first step in moving forward.

The four tribes

Four groups of somewhat similar firms, which we call tribes, emerged from our analysis of the data. We describe the four groups below. We use the 18 discriminators as a critical aspect of tribe identification.

TRIBE 1: SECURITY AS ENABLER

The Enabler tribe has a number of salient characteristics. Firms in this tribe have long since evolved the security mission from compliance to commitment. This means a firm's culture prioritizes security and gets compliance as a planned side effect. Even the Board of Directors has moved past compliance and uses a risk management approach to provide oversight. Security is not just a technical problem, and the business-focused approach gets Lines of Business to participate in the security mission. Staff balance between technologists and executives is carefully constructed. Speaking of executives, regardless of whether CISOs in the Enabler tribe have a deep technical past, today they look like their senior executive peers from a business standpoint. Like good senior executives, CISOs in this tribe proactively get in front of the problem both internally and externally by intentionally influencing the standards by which they will be judged.

Workforce discriminators

I.T1 The CISO is a seasoned senior executive. While often having a deep technical past, the CISO focuses much more attention on the business and less on technology.

II.T1-T2 The CISO enjoys direct interaction with and influence on both the CEO and the Board.

III.T1-T2 The CISO curates Board understanding of security, which is well past a compliance-only view.

IV.T1 The CISO has moved the firm from compliance to commitment.

V.T1 Security organization structure reflects the firm's business focus and is not only technology driven. In the case of global firms, geography often plays a role in organization structure.

VI.T1 A career path in security is well-defined and includes succession planning and direct executive mentorship. Roles among direct CISO reports are often non-technical.

VII.T1 Employee development in security is aligned with the business and includes leadership finishing school (just like the opportunities found outside security).

VIII.T1-T2 Company culture aligns with security and is partially defined by security.

Governance discriminators

IX.T1-T2-T3 Together with direct reports, the CISO determines which KPIs and KRIs to collect, track, and report.

X.T1 Security has become business as usual. No crisis required.

XI.T1-T2-T3 A PMO drives projects forward.

XII.T1 Budget is never an issue, because the Board and senior executives are aligned with the security mission. Funding within the agreed-on security mission is always possible.

XIII.T1-T2 Security is treated as risk management. Technical debt is understood and accounted for in the risk management paradigm.

Controls discriminators

XIV.T1-T2 A cyber security framework (e.g., the NIST framework) is used proactively to drive the security story forward.

XV.T1-T2 Top security controls include IAM, use of cryptography, and logging and analysis.

XVI.T1 The security organization has moved the vulnerability management exercise well past penetrate and patch and is driven by risk.

XVII.T1 Lines of Business go along with security requests and do the right thing. This happens even though the requests may not be in their best short-term interest, because they are aligned with the security mission and the security mission is aligned with them.

XVIII.T1-T2-T3 The BSIMM is used to measure software security progress.

Of the 25 firms in our dataset, 5 can be found in Tribe 1.

TRIBE 2: SECURITY AS TECHNOLOGY

One salient characteristic of the Technology tribe is an approach to security not bounded by compliance. Because CISOs in the Technology group started their careers as alpha geeks, their world view tends to overemphasize the technical aspects of security challenges. They bring the technology hammer to bear on every problem first. All that aside, a Technology CISO sets out to be a good business person but has not attained the senior executive gravitas of the Enabler tribe. Learning the business ropes the hard way (that is, through trial and error and raw experience) is an ongoing challenge. Because technologists like to solve hard problems, one common trap for Technology CISOs is to take on the stickiest business challenges themselves. An undersupply of business acumen leads to what we call the "superman syndrome," in which the Technology CISO often gets down in the weeds on a particular problem instead of delegating—for example, weeding through the morning's catch of threat intelligence at 5 a.m. or believing that contributing a tiny bit of revenue to the firm is the best use of time.

Workforce discriminators

I.T2 The CISO has a deep technical past and in many cases may still be known primarily for technical work. The CISO has solid business skills, which may still be developing.

II.T1-T2 The CISO enjoys direct interaction with and influence on both the CEO and the Board.

III.T1-T2 The CISO curates Board understanding of security, which is well past a compliance-only view.

IV.T2 The CISO has moved the firm past compliance as the goal, but work remains to be done to integrate security into the business.

V.T2 Security organization structure is built around technical goals and objectives and may not reflect the business focus of the firm, but understaffing is not a problem.

VI.T2 A career path in security is well-defined and includes succession planning and direct executive mentorship. However, career advancement tends to overemphasize technical security prowess even though there are some direct efforts to teach about the business.

VII.T2 Employee development in security is not clearly aligned with the business and tends to overemphasize the technical.

VIII.T1-T2 Company culture aligns with security and is partially defined by security.

Governance discriminators

IX.T1-T2-T3 Together with direct reports, the CISO determines which KPIs and KRIs to collect, track, and report.

X.T2 Security is not yet business as usual, though there may be a plan and unity of purpose. A crisis may have been the catalyst for renewed security effort and a change in philosophy.

XI.T1-T2-T3 A PMO drives projects forward.

XII.T2 Budget is not really an issue, because the Board and senior executives are aligned with the security mission. However, uptake in Lines of Business can be problematic when the firm is not completely aligned with security.

XIII.T1-T2 Security is treated as risk management. Technical debt is understood and accounted for in the risk management paradigm.

Controls discriminators

XIV.T1-T2 A cyber security framework (e.g., the NIST framework) is used proactively to drive the security story forward.

XV.T1-T2 Top security controls include IAM, use of cryptography, and logging and analysis.

XVI.T2 The security organization has moved the vulnerability management exercise well past penetrate and patch but is driven by threat instead of risk.

XVII.T2 Security provides Lines of Business a set of services that may not in all cases be aligned with the business. Because of this, uptake in Lines of Business may vary.

XVIII.T1-T2-T3 The BSIMM is used to measure software security progress.

Of the 25 firms in our dataset, 8 can be found in Tribe 2.

TRIBE 3: SECURITY AS COMPLIANCE

Compliance is both a boon and bane for security. The Compliance tribe intentionally leverages compliance requirements to make real security progress. But compliance alone has never kept a bad guy out. That means compliance is both a bare minimum standard that must be reached and a bar that some firms are struggling to get over. In many cases, previous security leadership was replaced at the same time that a compliance regime was imposed from outside (possibly in the wake of a crisis). Historical underinvestment in security, which may have reached crisis proportions, leads these firms to continue to underinvest in security even in the face of compliance requirements. That's because the compliance spending of today is in many cases more than the pre-crisis spending of yesterday. Simply put, they were spending a dime instead of a dollar in the past and are now sanguine in spending a quarter when a dollar is still what's required. CISOs in the Compliance tribe tend not to be deep technologists, but at the same time they tend to have strong managerial and leadership skills. This can lead to a situation in which limited resources are being properly allocated and clear progress is being made, even while technical debt is accumulating.

Workforce discriminators

I.T3 The CISO is a seasoned senior executive without a deeply technical past. The CISO is often an excellent administrator.

II.T3 The CISO enjoys direct interaction with the CEO. Board interaction likely includes attendance but not direct education about security.

III.T3 The CISO does not curate a well-mapped Board understanding of security. Though the Board may understand that compliance alone is insufficient, they remain hazy about security goals.

IV.T3 The firm is finishing up or actively working compliance requirements and has identified the next set of security goals but is not executing against them.

V.T3 Security organization structure is built around technical goals and objectives and may not reflect the business focus of the firm. In addition, understaffing can be a problem.

VI.T3 A career path in security is murky and is probably non-technical even though responsibilities are technical.

VII.T3 Employee development in security is aligned with the business.

VIII.T3 Company culture is beginning to align with security at senior executive levels. However, harmonized vision is not yet driven down, sometimes even in the security organization itself.

Governance discriminators

IX.T1-T2-T3 Together with direct reports, the CISO determines which KPIs and KRIs to collect, track, and report.

X.T3 Security is not yet business as usual, and compliance requirements may not be fully accounted for. A crisis may have caused a change in security leadership and the smoke has not yet cleared.

XI.T1-T2-T3 A PMO drives projects forward.

XII.T3 Resources are tight and underinvestment is common. Investment is limited to compliance efforts.

XIII.T3 Security is treated as risk management. However, technical debt is not accounted for in the risk management paradigm.

Controls discriminators

XIV.T3 A cyber security framework (e.g., the NIST framework) is used proactively to drive the security story forward. Use of the framework may not be creatively tailored to the business.

XV.T3 Top security controls, including IAM, use of cryptography, and logging, are still lagging. Projects to improve all three are underway.

XVI.T3 Vulnerability management is behind the curve, but plans are in the works to address the problem. Threat intelligence and other similar exercises are limited to what is purchased without customization.

XVII.T3 A past security crisis is being used as a lever to force security into Lines of Business.

XVIII.T1-T2-T3 The BSIMM is used to measure software security progress.

Of the 25 firms in our dataset, 7 can be found in Tribe 3.

TRIBE 4: SECURITY AS A COST CENTER

The Cost Center tribe is overwhelmed and underresourced. In most cases, security leadership exists under several levels of executive leadership (and sometimes even middle management) that treat security as a cost center. Security consumes budget but never drives budget creation and in some sense has a thick glass ceiling imposed on it. Without a real executive seat at the table, security is relegated to plumbing, much like the help desk.

Workforce discriminators

I.T4 The security leader, whose title is likely not CISO but who remains at the top of the security heap, is a technology person.

II.T4 The security leader lacks a collegial relationship with either the CEO or the Board. While the CEO and Board might know the security leader by sight, the security message is filtered through other layers of senior management before it gets to the top.

III.T4 The Board has limited understanding of cyber security, is not being educated, and may be driven by popular press. In many cases, the Board is made aware of security activity without any grounding in actual risk to the firm.

IV.T4 The security program is limited to compliance and is seriously resource constrained.

V.T4 The security organization is understaffed even to achieve compliance.

VI.T4 Security work is tactical in nature, is often only technical, and does not align with obvious career progression.

VII.T4 While there are promotions and title changes, security purview is limited to the technical weeds. Without two-way understanding of and by the business, security staff goals are constrained to the now and do not help prepare them or the firm for the future.

VIII.T4 Company culture is not conducive to security. Compliance is the one and only currency.

Governance discriminators

IX.T4 Metrics tend to be counts of effort. There is little or no evidence of transforming raw data into KPIs/KRIs important to the business.

X.T4 Budget may include a pot of money for an anticipated crisis (one per year).

XI.T4 No PMO exists for project management, which is instead handled directly by staff.

XII.T4 Security is managed like a cost center and is not provided adequate resources. Security apparatus is often paid for by taxing Lines of Business directly.

XIII.T4 Security is limited to a compliance exercise. Security has little or no handle on technical debt.

Controls discriminators

XIV.T4 There is no underlying cyber security framework.

XV.T4 Top security controls are in a state of flux at best. IAM may be completely ignored, use of cryptography is haphazard, and logging is weak.

XVI.T4 Patch management is the tail that wags the defect management dog. Network security basics may not be in place (think network segmentation).

XVII.T4 Security is provided as a service to Lines of Business, which may choose to ignore the services entirely. Security advises but probably cannot enforce.

XVIII.T4 A software security initiative is nonexistent or nascent.

Of the 25 firms in our dataset, 5 can be found in Tribe 4.

On tribes and evolution

Though we place individual CISOs in particular tribes for this work, boundaries between tribes are not super precise. A CISO's discriminators might be spread across multiple tribes, though as a set they clearly point to a particular tribe in every case observed.

The conceptual distance between tribes varies. Tribe 1 and Tribe 2 share many characteristics and are conceptually close, as demonstrated by discriminator overlap. We have observed that CISOs in both Tribes 1 and 2 can be very effective in their respective organizations.

The discriminators associated with Tribe 3 have little overlap with the discriminators of Tribes 1 and 2. In our view, Tribes 1 and 2 are much closer conceptually than Tribe 3 is to either of them. We have observed in many cases that organizational focus on compliance becomes a habit that's hard to kick. There may not be willingness to go past compliance even after it's attained. The goal becomes the limit.

Tribe 4 discriminators are a unique set. There is no overlap with the discriminators of Tribe 1, 2, or 3. Conceptually, Tribe 4 is way off by itself, further from Tribe 3 than Tribe 3 is from Tribes 1 and 2. We fear that Tribe 4 may be very large, meaning there's plenty of room for security improvement in the world.

Moving between tribes is certainly possible. Moving from Tribe 4 to Tribe 3 may require a crisis, something we see plenty of evidence for in our data. Fortunately, not all firms have to start in Tribe 4. On the other hand, compliance is a common theme in all

security programs in Tribes 1, 2, and 3. The question is whether compliance is a security glass ceiling. Moving from Tribe 3 to Tribe 1 or 2 may be possible, but it does require some heavy lifting. In Tribes 1 and 2, compliance is a side effect of security.

Tribes 1 and 2 are both fine situations to find yourself in as a CISO. Though these two tribes are very similar in appearance, moving from Tribe 2 to Tribe 1 requires earning a seat at the senior executive table.

Using the discriminators to improve

First, a caveat: Changing your tribe may be a nontrivial proposition that requires not only a major shift in firm philosophy but also a distinctly different approach to leadership. Evolving from one tribe to another may not always be possible.

That said, each of our 18 discriminators and its subentries can be used as a roadmap for moving from one tribe to another. Consider discriminator I (reproduced here):

I. CISO executive stance

I.T1 The CISO is a seasoned senior executive. While often having a deep technical past, the CISO focuses much more attention on the business and less on technology.

I.T2 The CISO has a deep technical past and in many cases may still be known primarily for technical work. The CISO has solid business skills, which may still be developing.

I.T3 The CISO is a seasoned senior executive without a deeply technical past. The CISO is often an excellent administrator.

I.T4 The security leader, whose title is likely not CISO but who remains at the top of the security heap, is a technology person.

A Tribe 4 CISO can set out to move into Tribe 2 by moving up the executive food chain. An explicit exercise in leadership development will be required. Indeed, a Tribe 2 CISO may still have work to do to move into Tribe 1 from a business acumen perspective.

Each of the discriminators helps to define a story of possible improvement and tribe evolution.

Eight more things

Eight observations that we see in the data are worth noting and have something to say about the state of security.

Middle management

Lots of security organizations are suffering from a lack of middle management. Incidentally, this is also commonly observed in other technical fields. Senior executive leadership is often strong and present, as are collections of qualified technologists. What's missing is the glue that goes between. If the ranks of senior leadership are to grow, there must be a defined career path from the technical weeds to the executive suite. In addition, execution is hampered by the lack of middle management. There's plenty to learn from CISOs who focus on succession planning and job rotation.

Risk ownership

Crossing the Rubicon from holding all the risk in a firm to identifying, distributing, and managing a firm's risk among all responsible executives is nontrivial. Too many CISOs hold all the risk. Not only is having your head on the chopping block bad for a good night's rest, it really doesn't help your firm either. CISOs should be in the business of risk management, not risk hoarding.

Programs

Security is not just a collection of projects. Strategic vision aligned with the business is easy to sketch on paper, but it remains a real challenge. If your strategic vision is limited to compliance, you need a more appropriate vision.

Talent

There are not enough security people. Acquiring, developing, and retaining a well-oiled security machine requires attention to personnel. Even the top CISOs in the world have a talent problem and invest heavy resources into nurturing their staff. Leadership development is just as important as compensation when it comes to retention. Smart CISOs can kill two birds with one stone, filling the middle management gap and producing highly qualified security executives that want to stick around.

Scale

An approach that works for a team of 10 is unlikely to scale to an army of 10,000. The best CISOs think about scale from day one, just like their counterparts in development and operations. Security processes must evolve at the same pace as the business or risk being left behind.

Fraud

Most CISOs don't own fraud control. Among the 25 CISOs we observed, only 2 of them had anything to do with fraud control. Simply put, fraud is beyond the scope of the security organization even when there is an active fraud control approach at the firm.

SOCs

Almost all the CISOs in our study have a security operations center (SOC). Though the trend seems to be that many SOC duties are outsourced, many firms are bringing them in-house. Sometimes SOC duties are split between a vendor and staff. Even within the Enabler tribe, SOC execution is not carried out the same way by all firms.

Vendor control

No organization, no matter what tribe it is in, has solved the vendor control problem. Interestingly, vendor control is on everybody's radar.

Now what?

We've learned a bunch about CISOs, and we hope you have too. Everywhere we've been so far, we've seen great interest in what CISOs actually do, why they do it, and how they can do it better. Occasionally, groups of like-minded CISOs get together, especially if they all are from the same vertical or geography. This is an encouraging trend that we support. In the best of all possible worlds, the model we describe can provide not only a common vocabulary but also a basis for further discussion and professionalization.

Please share this work with all the CISOs you know. If you're a CISO yourself and you want to be involved in our science project, get in touch. Everyone is welcome.

Appendix A

The following is a table representation of the discriminators.

- (T1) Tribe 1: Security as Enabler
- (T2) Tribe 2: Security as Technology
- (T3) Tribe 3: Security as Compliance
- (T4) Tribe 4: Security as a Cost Center

T1	T2	T3	T4	LABEL	DISCRIMINATOR
WORKFORCE					
CISO executive stance					
✓				I.T1	The CISO is a seasoned senior executive. While often having a deep technical past, the CISO focuses much more attention on the business and less on technology.
	✓			I.T2	The CISO has a deep technical past and in many cases may still be known primarily for technical work. The CISO has solid business skills, which may still be developing.
		✓		I.T3	The CISO is a seasoned senior executive without a deeply technical past. The CISO is often an excellent administrator.
			✓	I.T4	The security leader, whose title is likely not CISO but who remains at the top of the security heap, is a technology person.
CISO-Board relations					
✓	✓			II.T1-T2	The CISO enjoys direct interaction with and influence on both the CEO and the Board.
		✓		II.T3	The CISO enjoys direct interaction with the CEO. Board interaction likely includes attendance but not direct education about security.
			✓	II.T4	The security leader lacks a collegial relationship with either the CEO or the Board. While the CEO and Board might know the security leader by sight, the security message is filtered through other layers of senior management before it gets to the top.
CISO curation of security message					
✓	✓			III.T1-T2	The CISO curates Board understanding of security, which is well past a compliance-only view.
		✓		III.T3	The CISO does not curate a well-mapped Board understanding of security. Though the Board may understand that compliance alone is insufficient, they remain hazy about security goals.

			✓	III.T4	The Board has limited understanding of cyber security, is not being educated, and may be driven by popular press. In many cases, the Board is made aware of security activity without any grounding in actual risk to the firm.
CISO and compliance					
✓				IV.T1	The CISO has moved the firm from compliance to commitment.
	✓			IV.T2	The CISO has moved the firm past compliance as the goal, but work remains to be done to integrate security into the business.
		✓		IV.T3	The firm is finishing up or actively working compliance requirements and has identified the next set of security goals but is not executing against them.
			✓	IV.T4	The security program is limited to compliance and is seriously resource constrained.
Security organization structure					
✓				V.T1	Security organization structure reflects the firm's business focus and is not only technology driven. In the case of global firms, geography often plays a role in organization structure.
	✓			V.T2	Security organization structure is built around technical goals and objectives and may not reflect the business focus of the firm, but understaffing is not a problem.
		✓		V.T3	Security organization structure is built around technical goals and objectives and may not reflect the business focus of the firm. In addition, understaffing can be a problem.
			✓	V.T4	The security organization is understaffed even to achieve compliance.
Security career path					
✓				VI.T1	A career path in security is well-defined and includes succession planning and direct executive mentorship. Roles among direct CISO reports are often non-technical.
	✓			VI.T2	A career path in security is well-defined and includes succession planning and direct executive mentorship. However, career advancement tends to overemphasize technical security prowess even though there are some direct efforts to teach about the business.
		✓		VI.T3	A career path in security is murky and is probably non-technical even though responsibilities are technical.
			✓	VI.T4	Security work is tactical in nature, is often only technical, and does not align with obvious career progression.
Security alignment with business					
✓				VII.T1	Employee development in security is aligned with the business and includes leadership finishing school (just like the opportunities found outside security).
	✓			VII.T2	Employee development in security is not clearly aligned with the business and tends to overemphasize the technical.

		✓		VII.T3	Employee development in security is aligned with the business.
			✓	VII.T4	While there are promotions and title changes, security purview is limited to the technical weeds. Without two-way understanding of and by the business, security staff goals are constrained to the now and do not help prepare them or the firm for the future.
				Company culture and security	
✓	✓			VIII.T1-T2	Company culture aligns with security and is partially defined by security.
		✓		VIII.T3	Company culture is beginning to align with security at senior executive levels. However, harmonized vision is not yet driven down, sometimes even in the security organization itself.
			✓	VIII.T4	Company culture is not conducive to security. Compliance is the one and only currency.
				GOVERNANCE	
				KPIs, KRIs, and metrics	
✓	✓	✓		IX.T1-T2-T3	Together with direct reports, the CISO determines which Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) to collect, track, and report.
			✓	IX.T4	Metrics tend to be counts of effort. There is little or no evidence of transforming raw data into KPIs/KRIs important to the business.
				Security and crisis	
✓				X.T1	Security has become business as usual. No crisis required.
	✓			X.T2	Security is not yet business as usual, though there may be a plan and unity of purpose. A crisis may have been the catalyst for renewed security effort and a change in philosophy.
		✓		X.T3	Security is not yet business as usual, and compliance requirements may not be fully accounted for. A crisis may have caused a change in security leadership and the smoke has not yet cleared.
			✓	X.T4	Budget may include a pot of money for an anticipated crisis (one allowed per year).
				Program management	
✓	✓	✓		XI.T1-T2-T3	A Program Management Office (PMO) drives projects forward.
			✓	XI.T4	No PMO exists for project management, which is instead handled directly by staff.
				Budget	
✓				XII.T1	Budget is never an issue, because the Board and senior executives are aligned with the security mission. Funding within the agreed-on security mission is always possible.

	✓			XII.T2	Budget is not really an issue, because the Board and senior executives are aligned with the security mission. However, uptake in Lines of Business can be problematic when the firm is not completely aligned with security.
		✓		XII.T3	Resources are tight and underinvestment is common. Investment is limited to compliance efforts.
			✓	XII.T4	Security is managed like a cost center and is not provided adequate resources. Security apparatus is often paid for by taxing Lines of Business directly.
Risk management and technical debt					
✓	✓			XIII.T1-T2	Security is treated as risk management. Technical debt is understood and accounted for in the risk management paradigm.
		✓		XIII.T3	Security is treated as risk management. However, technical debt is not accounted for in the risk management paradigm.
			✓	XIII.T4	Security is limited to a compliance exercise. Security has little or no handle on technical debt.
CONTROLS					
Cyber security framework					
✓	✓			XIV.T1-T2	A cyber security framework (e.g., the NIST framework) is used proactively to drive the security story forward.
		✓		XIV.T3	A cyber security framework (e.g., the NIST framework) is used proactively to drive the security story forward. Use of the framework may not be creatively tailored to the business.
			✓	XIV.T4	There is no underlying cyber security framework.
Security controls					
✓	✓			XV.T1-T2	Top security controls include Identity and Access Management (IAM), use of cryptography, and logging and analysis.
		✓		XV.T3	Top security controls, including IAM, use of cryptography, and logging, are still lagging. Projects to improve all three are underway.
			✓	XV.T4	Top security controls are in a state of flux at best. IAM may be completely ignored, use of cryptography is haphazard, and logging is weak.
Vulnerability management, risk, and threats					
✓				XVI.T1	The security organization has moved the vulnerability management exercise well past penetrate and patch and is driven by risk.
	✓			XVI.T2	The security organization has moved the vulnerability management exercise well past penetrate and patch but is driven by threat instead of risk.
		✓		XVI.T3	Vulnerability management is behind the curve, but plans are in the works to address the problem. Threat intelligence and other similar exercises are limited to what is purchased without customization.

			✓	XVI.T4	Patch management is the tail that wags the defect management dog. Network security basics may not be in place (think network segmentation).
Lines of Business alignment					
✓				XVII.T1	Lines of Business go along with security requests and do the right thing. This happens even though the requests may not be in their best short-term interest, because they are aligned with the security mission and the security mission is aligned with them.
	✓			XVII.T2	Security provides Lines of Business a set of services that may not in all cases be aligned with the business. Because of this, uptake in Lines of Business may vary.
		✓		XVII.T3	A past security crisis is being used as lever to force security into Lines of Business.
			✓	XVII.T4	Security is provided as a service to Lines of Business, which may choose to ignore the services entirely. Security advises but probably cannot enforce.
SSI measurement					
✓	✓	✓		XVIII.T1-T2-T3	The BSIMM is used to measure software security progress.
			✓	XVIII.T4	A software security initiative is nonexistent or nascent.

THE SYNOPSYS DIFFERENCE

Synopsys offers the most comprehensive solution for building integrity—security and quality—into your SDLC and supply chain. We've united leading testing technologies, automated analysis, and experts to create a robust portfolio of products and services. This portfolio enables companies to develop customized programs for detecting and remediating defects and vulnerabilities early in the development process, minimizing risk and maximizing productivity. Synopsys, a recognized leader in application security testing, is uniquely positioned to adapt and apply best practices to new technologies and trends such as IoT, DevOps, CI/CD, and the Cloud. We don't stop when the test is over. We offer onboarding and deployment assistance, targeted remediation guidance, and a variety of training solutions that empower you to optimize your investment. Whether you're just starting your journey or well on your way, our platform will help ensure the integrity of the applications that power your business.

For more information go to www.synopsys.com/software.

SYNOPSYS®

185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com