CHAPTER 4

Strengthen Security Culture Through Communications and Awareness Programs

Human error or misconduct of one kind or another must be either the direct cause or a contributing factor to almost every security breach or outage. Whether it is the user clicking a phishing link, an operator accidentally deleting the corporate directory, a manager approving excessive privileges, a receptionist letting a thief or spy into the building, or an incident responder hitting the snooze button on the wrong malware alarm, the examples are legion.

Security leaders should strive to improve security-related behavior through user awareness and training programs. Sometimes these programs succeed in bettering security-related behaviors, sometimes they don’t. Wouldn’t it be nice to know why? It turns out that people’s behavior is related to a larger issue of security culture, which is itself a part of organizational culture.

Formally adopted security policies, well-defined security governance, and clear security-related roles in the business are prerequisites for a successful security program. But in the background behind the visible security governance and security program machinery is the organization’s security culture. A security culture is the part of an organization’s self-sustaining patterns of behavior and perception that determine how (or if) the organization pursues security. A positive security culture can provide your best opportunity to secure the business; a negative one can be your greatest vulnerability.
“Culture eats strategy for breakfast, lunch, and dinner.”

Peter Drucker, Management Guru

Modern organizational thinking – and marquee schools such as Wharton or Harvard Business School – sees organizational culture as paramount for business outcomes. Hard to define, as likely to change the executive as to be changed, and usually neither all good nor all bad – culture is pervasive in the business.

Security leaders can use communications and awareness programs to gradually enhance security culture throughout the organization as well as improve specific user behaviors such as resisting and reporting phishing messages and becoming good stewards of customer information. Over a period of time, security teams can cultivate a network of influencers throughout the business to create a healthier security culture.

The chapter provides guidance for security leaders on how to

- Address common challenges
- Understand security culture and awareness concepts
- Make enhancing communication a top security team priority
- Use awareness programs to improve behaviors and security culture
- Commit to improving security culture
- Measure and improve

4.1 Address Common Challenges

According to ISACA/CMMI’s 2018 “The Cybersecurity Culture Gap,” 95 percent of global survey respondents identify a gap between their current and desired organizational culture of cybersecurity. Today, organizations face multiple challenges with engaging business units and executives at the strategic level and shifting the business towards a healthier security culture. Ineffective security communication styles can exacerbate these challenges.¹

¹“The Cybersecurity Culture Gap: An ISACA and CMMI Institute Study,” ISACA/CMMI, 2018, accessed at: https://www.isaca.org/-/media/info/cybersecurity-culture-report/index.html
4.1.1 Business Executives Not Engaged at the Strategic Level

The average executive has probably been briefed on, or read about, security threats often but tends to be personally less knowledgeable than the general public about cybersecurity practices and self-assesses his or her business as not being well prepared. Moreover, we previously cited evidence that business executives tend to not consider cybersecurity strategic (see Chapter 2’s section “Cybersecurity Not Considered Strategic”).

According to a KPMG “U.S. CEO Outlook” study, 2 executive awareness of cybersecurity threats is high, but that doesn’t translate to being ready.

- 33% of Chief Executive Officers (CEOs) identified cybersecurity as their top threat to growth.
- 92% can identify new cyber threats (i.e., from the news).
- 89% consider protecting customers’ personal data “hugely important.”
- But only 41% consider their company well prepared to deal with threats.

At the same time, business executives overall have relatively low detailed awareness of basic computer protection, privacy, and physical security according a MediaPro survey:

- 41% of executives’ personal security and privacy survey scores put them in the “at risk” category compared to only 29% of the general population.3

4.1.2 Business Units at Odds with IT and Security

As discussed in Chapter 2’s section “Working at Cross-Purposes,” business leaders may be at odds with IT (and security) for all sorts of reasons – personal, organizational, and political reasons. Disruptive changes to IT and immaturity of security governance or

---

2“US CEO Report,” Lynne Doughtie, KPMG, May 2018, accessed at https://assets.kpmg/content/dam/kpmg/us/pdf/2018/05/kpmg-ceo-outlook-2018.pdf
3“State of Executive Cybersecurity Awareness,” David Self, MediaPro, July 2018, accessed at www.mediapro.com/blog/infographic-executive-cybersecurity/
risk management models contribute to the disconnect. Chapter 7’s section “Address Common Challenges” identifies additional structural difficulties for IT. Namely, digital business strategies often lead to decentralization or fragmentation of IT control as trends such as cloud computing, bring your own device (BYOD), and a new generation of power users devolve application and infrastructure management to business units and/or cloud service providers (CSPs).

In some cases, IT (and security teams) are on board with the growing momentum toward cloud-first strategies and acting as brokers/providers. In others, they are facing a diminishing role as providers of premise-based services with shrinking business unit buy-in. If the business and IT managers or staff perceive any of the following, it can have a corrosive effect on the security culture:

- Central IT hasn’t been effective at providing timely solutions or services (e.g., many days or weeks to fulfill a request for new virtual machines, storage capacity, or application access), lacks an effective cloud strategy, and/or resists the LOBs’ own IT or cloud initiatives.

- Security leaders have acted like the “Department of NO,” failed to offer helpful alternatives and solutions when they identify a problem, or not tried to understand the LOB’s drivers or pain points.

- In large multinational organizations with different geographies, languages, and cultures, some LOBs are not engaged with IT or security programs from the headquarters or some of the meaning of these programs is lost in translation.

If cybersecurity isn’t considered strategic or business units are disengaged, business leaders are less likely to support sustained efforts to improve security culture. This chapter and the book as a whole proposes multiple recommendations to build better bridges to the business and improve the security culture. But first security leaders must look inward, at their organization, themselves, and their communication styles.

4.1.3 Hard to Change Culture

One definition of business culture is “The self-sustaining pattern of behavior that determines how things are done,” and it is further characterized as “An elusively complex entity that survives and evolves mostly through gradual shifts in leadership, strategy,
and other circumstances.” The same authors argue that cultures are hard to change: “Cultures are constantly self-renewing and slowly evolving: What people feel, think, and believe is reflected and shaped by the way they go about their business. Formal efforts to change a culture (to replace it with something entirely new and different) seldom manage to get to the heart of what motivates people, what makes them tick. Strongly worded memos from on high are deleted within hours. You can plaster the walls with large banners proclaiming new values, but people will go about their days, right beneath those signs, continuing with the habits that are familiar and comfortable.”

In my experience, security culture inherits many attributes of the business culture. The good news is that security culture is a smaller problem space, and many security behaviors can be improved through targeted awareness campaigns, process changes, and even user experience (UX) changes to technologies – without changing the core business culture.

### 4.1.4 Ineffective Security Communication Styles

Every security organization has a culture of its own and the opportunity to influence the security culture across the entire organization it serves. An unhealthy business security culture can emerge, however, when the security organization’s subculture is out of line with the broader business culture.

Both the CISO and the security team create the security organization’s subculture. Although a larger security organization will have multiple teams, one or just a few predominant personality archetypes (e.g., the “cop,” “ex-military,” “auditor,” “techie,” or “business school” type) will tend to dominate the security organization and its communication style. If this style is out of line with the business culture (e.g., highly authoritarian in a consensus-oriented culture or vice versa), the security organization is unlikely to be well regarded.

Even without cultural dissonance between the security organization and the business, security leaders tend to find communicating with executives or peer business leaders challenging. Security leaders, even CISOs, serve a nonrevenue-generating function that’s often positioned too low in the organization chart or informal executive pecking orders. They are often the bearers of bad news about incidents, vulnerabilities,

---

4 “Ten Principles of Organizational Culture,” Strategy+Business, February 15, 2016, accessed at www.strategy-business.com/feature/10-Principles-of-Organizational-Culture
deficiencies, and unwelcome regulatory requirements. To top it off, they may lack strong communication skills. An effort to overcompensate and overplay the fear, uncertainty, and doubt (FUD) card can get attention in the short run but lead to a loss of credibility when feared consequences don’t soon materialize.

### 4.1.5 Measuring Culture Is a Soft Science

Security culture is more than awareness, and as a social phenomenon, it is an outlier to both the business financial metrics and the security technical metrics domains. Measuring whether efforts to improve security culture are effective (or that any single awareness and training campaign has succeeded) is important for our ability to understand what works. However, taking such measurements is challenging.

Organizations and practitioners who are unaware of methods to measure security culture may turn to measuring proxies, such as number of attendees and completion rates of awareness training courses. These metrics are not very useful because they only measure (at best) one or two points along a continuum of security behaviors and ignore other cultural attributes.

If the purpose of security awareness training is to improve the overall culture and not just a single behavior (such as reporting phishing messages), then a set of metrics must be devised to measure a broad set of security culture attributes. Unfortunately, there is no ISO or NIST standard for how to do this nor much research to provide empirical evidence that conventional awareness programs are effective. Such efforts that have been made to measure awareness effectiveness typically use only counts or trends of security-related events and incidents.

Measuring incidents in isolation just creates confusion. If more incidents are reported, does that mean security is getting worse or just that incidents are – at last – being reported? Incident metrics alone won’t resolve uncertainty.
Kai Roer, who developed the Security Culture Framework process and has made a career out of security culture projects, explained: “Our process included a measurement phase. But no standard metrics existed. Although we did measure changes, we did not know if they were improvements or not. When we did security culture work as consultants, we also had to consider political factors. Initially there was lot of bias in the measurement.”

In 2015, Roer teamed up with socio-informatics expert Dr Gregor Petritc to create a Norwegian company called CLTRe (pronounced “culture”). CLTRe is a software-as-a-service (SaaS)-based measurement application loaded with the best security culture metrics the two of them could devise. Roer and Petritch also began producing an annual security culture report with industry metrics. In 2019, CLTRe was acquired by the US-based awareness firm KnowBe4, Inc.

In the “Measure and Improve” section, we’ll discuss Kai Roer’s approach to measuring security culture as well as additional strategies.

### 4.2 Understand Security Culture and Awareness Concepts

A security culture is the part of a business culture’s self-sustaining patterns of behavior and perception that determine how (or if) the organization pursues security. It is an amalgamation of perceptions about and behavior toward the business’s own IT and security systems, security policies, and operational security practices or projects. Security culture is not fixed, it is constantly evolving based on people’s experiences and social interactions.

Security culture can impact an organization’s risk levels, compliance posture, and costs or benefits in both positive and negative ways. Business and security leaders ignore it at their own risk, or they can leverage it to get better outcomes.

A security culture strategy is a conscious effort by security and business leaders to transform their de facto security culture into one that’s more conducive to information protection and risk management. The strategy also seeks to sustain security culture at the desired state as the business changes over time.

---

5 “The Security Culture Framework” website, CLTRe, accessed at https://securitycultureframework.net
The way that the security organization communicates and aligns with the business along with user awareness and training programs is a primary tool for improving the security culture. In a healthy security culture, the security team’s communications and the awareness programs have a higher chance of success. Even in a more negative setting, the right communications and awareness messaging carried out over time can help improve the security culture. A stronger security culture will then ease many other cybersecurity challenges.

4.2.1 Your Greatest Vulnerability?

Thought leader Edgar Schein once said about business culture in general: “If you do not manage culture, it manages you, and you may not even be aware of the extent to which this is happening.” Likewise, security culture can make or break a security program.

In fact, the root cause of many security breaches is not technology, but a “people” vulnerability such as an employee being tricked by a phishing message or other social engineering exploits into giving away credentials or installing malware. In other cases, a failure to follow a process, such as change control, is the culprit. Often, multiple things go wrong. A breach rarely is, and in fact should not be, caused by just one vulnerability.

Consider your own organization’s security culture, and ask yourself what would happen in the following “day in the life of a security program” examples:

- When budgeting comes around and the CISO presents a reasonable plan, but the CFO criticizes “unnecessary expenses”
- When the development manager waives the security design review because the project is behind schedule
- When the Agency Director demands immediate firewall rule changes that could expose taxpayer databases to the Internet
- When a potential breach is discovered for the business’s French customers’ data, there’s no detailed response plan, and the CISO goes to the Chief Counsel with a warning about 72-hour General Data Protection Regulation (GDPR) breach notification requirements
- When a mutating zero-day virus has been reported at three sites, and the CISO recommends shutting down the network to affected regions with critical business applications
When the VP of Sales receives a demand from the company’s largest account in Dubai for contact information on all attendees at a recent business conference, even though sharing this personal data was not in the conference agreement and could violate compliance regulations.

When faced with an apparent no-win choice between business and security values, what will the management team do? Will it reason through the issues to find the least-bad choice or brainstorm a third way out, learn from the experience, and update company policies to clarify similar circumstances in the future? Or will a series of unproductive meetings end with escalation to the CEO, bad choices, acrimony, and blaming? How did the organization get to this point?

FINANCIAL SERVICES COMPANY HEAD OF INTERNAL AUDIT’S STORY

“Since more than 80% of the company’s applications were custom developed, the global Chief Technology Officer (CTO) played a critical role. In conversation, it was clear to me that, the CTO understood the need for secure application development and the underlying risks. However, he felt that development organizations did not have additional budget to incorporate these practices and capabilities.

I recall attending a meeting with the CTO and senior engineering and development executives to get them aligned on the urgent need for secure development and operating practices for their transaction processing systems. Surprisingly, the development executives were vigorously resistant: ‘Why can’t engineering take care of security? We are development and we need to focus on building product quickly – our focus is on writing code that is fast, optimizes the user experience, and enables us to get features to market quickly.’

To help the CTO further understand the risk, I asked a question: ‘So across the infrastructure, is traffic encrypted?’ No one seemed to have a definite answer and after substantial discussion, the conclusion, was: ‘No.’ I continued: ‘Then where is the data security coming from if confidential transaction data travels are over public spaces and physical pipes?’ Much to my surprise, the application development and infrastructure security teams started pointing fingers at each other instead of taking ownership and working the problem together. At this point I could see the CTO was losing interest in this topic. There were more important things to do.
My next stop was to brief the CEO. At the end of a long and very interactive discussion with the CEO, which included the CTO who sat quietly appearing non-committal, I summarized ‘We are not secure. And the central issue is that each technology team is saying that security is not a priority requirement for them and needs to be provided at another layer or by another team.’ The CEO’s response was lukewarm. The CEO felt that the CTO was doing enough. The recurring subtext seemed to be: ‘Yeah, we know we are highly regulated and while certain processes may not appear to be great, nothing bad has happened – ever! We’re going to be ok.’

Eventually, the company experienced a serious data breach, where vulnerable applications were exploited early in the kill chain.

The unfortunate event was not surprising. I have seen this storyline play out so many times across a variety of companies and industries. Complacency results from diffused accountability and a decision culture that discourages responsibility for risk taking across teams and the management layers of a company. It becomes difficult to encourage informed decisions and a calibrated sense of urgency in a culture that is sclerotic, overconfident, and focused on constraints rather than solutions.”

Anonymous

The preceding story illustrates multiple problems. Security-related roles, responsibilities, and accountabilities were unclear, and the CEO placed a low priority on security. Thus, IT, development, and executive management failed to support deploying even such a basic control as data-in-transit encryption. The last paragraph of the story explains in the head of internal audit’s own words why the company’s woes with security stemmed from a cultural problem.

4.2.2 Or Your Best Opportunity?

When security issues loom, the business’s fate may hinge on a ripple of knee-jerk reactions preprogrammed into the security culture. We’ve highlighted the possibility of failures – the things you want to avoid. Let’s also consider how a healthy security culture can help an organization avert security failures in most cases and respond well or recover quickly even from serious incidents. Is your organization ready? Do the leaders and staff really value security? Do they realize that it requires teamwork between security
and business functions and what role they are to play? Do they buy into the policies they’re expected to observe and know what principles to consider when pressed to make a difficult decision?

Maybe not all that – yet. There probably is no perfect security culture out there. But there are plenty of good models that leading organizations can aspire to:

- **Active executive oversight:** Executives aren’t just going through the motions to review a quarterly report and react only when findings or incidents are too serious to ignore. Instead, at least a chosen few are actively meeting and discussing cybersecurity with security leaders from time to time and helping the rest of the executive team and the Board exercise oversight. The CEO or another top executive works with the security leadership to understand and prioritize the business impact of security risks and projects.

- **Coordinated management:** A cross-functional cybersecurity coordination group (such as a security steering committee at larger businesses) is in place. It is sponsored from the executive level, and the committee chair dedicates quality time to it. Although not every security issue bubbles up to the group, those that do to get resolved through principles-based deliberation, as much as possible to the benefit of both business and security.

- **Engaged stakeholders:** Business and security leaders or staff perform their security and risk management roles – such as data owner, data steward, risk owner – with the right mix of empowerment and control. A network of informal partnerships between security and business functions complements the official organizational structures and processes.

- **Supportive workforce:** End users are aware of the awareness program and often apply its advice or training to their work and personal computing activities. They tend to understand that security rules and policies are there to protect the business and themselves. They appreciate the security department’s efforts to “make the secure way the easy way” through tools such as password managers and mobile device management. They often report suspicious emails or other indicators of compromise to the security team.
4.2.3 Attributes of Security Culture

Earlier, we defined security culture as an organization or group’s amalgamation of perceptions about and behavior toward its own IT and security systems, security policies, and operational or social security practices and projects.

Figure 4-1 illustrates the interrelationship of perceptions and behavior with other security culture components as described in the report “Security Culture 2018: Measure to Improve.” Observe that in a security culture, attitudes, norms, cognition, and communication shape perception and behavior. Group perceptions and behavior create better or worse security outcomes. Each component of culture can be measured and has complex interactions with the other components.

---

6“Security Culture 2018: Measure to Improve,” CLTRe AS, Kai Roer, 2018, accessed at https://get.clt.re/report
Observe how the inputs and impacts (or outputs) of security culture form a feedback loop in Figure 4-1. The book “CISO Soft Skills” (discussed in Chapter 2) analyzes the security program and security culture using system theory. In the authors’ model and this one, negative inputs degrade the system, producing negative outputs and a vicious circle that degrades the culture. Positive inputs and outputs do the opposite. All security cultures have a mix of positive and negative attributes and flows.

4.2.4 Security Culture Styles

Security culture in an organization is part of the larger business culture and needs to align with it. Figure 4-2 depicts various organizational culture concepts which are helpful for security leaders to understand.
General business culture can, according to the Harvard Business Review’s “The Culture Factor’s” research, be understood in terms of eight distinct cultural styles that fall along two dimensions: how people interact and how they respond to change. In another model, Hofstede Insights analyzes organizational cultures along six dimensions, including whether they are means oriented or goal oriented, internally or externally driven, easygoing or strict in work discipline, local vs. professional, open vs. closed, and employee oriented or work oriented. Hofstede also provides tools organizations can use to measure their cultures.

National cultures can be compared in many ways and must be considered as well as the general business culture in determining which security culture strategies and governance models (e.g., centralized, decentralized, and matrixed) will be effective. For example, organizations in a country typified by a high power distance are likely to have

---

7“The Culture Factor,” Harvard Business Review, January–February 2018 Issue, accessed at https://hbr.org/2018/01/the-culture-factor

8“Organizational Culture,” Hofstede Insights, accessed at https://hofstede-insights.com/models/organisational-culture/

9“How Power Distance Influences Leadership,” Florida Tech Online Blog, accessed at www.floridatechonline.com/blog/psychology/how-power-distance-influences-leadership/
better results with a centralized, prescriptive leadership approach, while organizations in a country with a low power distance may align better with a decentralized or matrixed organization’s consensus- and collaboration-based processes.

In addition to national cultures, distinct **occupational subcultures** for executives/managers, office/administrative staff, developers, and other groups exist in almost all but the smallest organizations. Technology and IT services companies have many “white-collar” knowledge workers and developers. Health care has doctors and nurses; educational institutions have professors and teachers. Organizations in retail, manufacturing, utilities, and transportation have large numbers of “blue-collar” workers staffing factories, facilities, stores, or field operations. Government, financial services, and business services industry organizations have their own unique mixes of blue-collar and white-collar functions. The desired security cultural traits and the awareness methods to instill them may vary between these occupational subcultures, and the differences should be considered in deciding where a more prescriptive and where a more flexible and collaborative security culture strategy, governance, and communications approach would be optimal.

Some businesses – such as Chevron, Google, and Southwest Airlines\(^\text{10}\) – have a business culture that is **clearly defined** and intentionally cultivated in a consistent manner, some do not. One can look at an organization’s vision statement, or mission, to see if it calls out or implies a business culture style. If not, security leaders should look for other clues as to which of the cultural styles the organization seeks to follow.

**Multinational businesses** sometimes attempt to superimpose a global business culture vision over operating units in different countries; this scenario may dovetail with matrixed business, IT, and security governance (see Chapter 3). Or, local subsidiaries may be encouraged to operate with distinct national or local organizational cultures.

**Other considerations:** Organizational culture research doesn’t identify a perfect culture, since the efficacy of culture is relative to the goals of the organization. However, much is written about the (numerous) dysfunctional organizational cultures including one short piece from the Hofstede Insights.\(^\text{11}\) Business leaders often identify and discuss culture issues on their own and may be in the middle of a culture change project.

\(^{10}\)“10 Examples of Companies With Fantastic Cultures,” Sujan Patel, *Entrepreneur*, August 2015, accessed at [www.entrepreneur.com/article/249174](http://www.entrepreneur.com/article/249174)

\(^{11}\)“Ask an Expert: 6 Signs That Your Organisational Culture Is Not Working?,” Hofstede Insights, accessed at [https://news.hofstede-insights.com/news/2018/06/15/ask-an-expert-when-an-organisational-culture-is-not-working](https://news.hofstede-insights.com/news/2018/06/15/ask-an-expert-when-an-organisational-culture-is-not-working)
4.3 Make Enhancing Communication a Top Security Team Priority

Security culture and awareness campaign outcomes are shaped by the whole message that businesspeople get from the security organization. Security leaders can address the challenge described in the section “Ineffective Security Communication Styles” by understanding how businesspeople perceive both the security organization’s occupational subculture and the messages they’re receiving and by improving communications in the following ways:

- Cultivate a collaborative and supportive communication climate with business leaders, managers, and staff to encourage open interaction. Communicate with the expectation that stakeholders will be the supportive colleagues you need them to be.

- Be mindful of the audience and tailor messages appropriately. Don’t use highly technical language that might lose businesspeople. Use examples businesspeople can understand. Keep presentations as brief and actionable as possible while providing supporting material.

- Couch negative messages as an opportunity for improvement rather than criticizing or casting blame.

- Discover positive points and include them in the message; there will almost always be something stakeholders are already doing well, some area where they have improved, or positive intentions they have expressed. Give stakeholders public credit for any help they provide, even in small things.
• Also accentuate the positive by communicating with a sense of efficacy, as advised in Chapter 2’s section “Earn Trust and Cooperation from Users.” Stakeholders will respond well if offered an easy or achievable way to improve or reduce risk.

• Be respectful of stakeholder’s time. Prepare for meetings with stakeholders in advance to minimize the amount of information gathering required during meetings. Take note of the information learned from stakeholders and make it available to security team colleagues to avoid repetitive requests.

The following generalized example proposes a good way to frame briefings of security issues or calls to action for stakeholders. Note the focus on teamwork done in advance of the briefing to show the security organization’s collaborative approach.

**COMMUNICATION TIP FOR CISO EXECUTIVE BRIEFING**

• **Begin with a realistic take:** We may have some bad incidents, audit findings, or negative third-party assessments. There’s a lot of red (risk) on this chart.

• **Map to business impact:** Here’s how our risk scenarios relate to your core business functions. Here’s what happened to some of our peers.

• **Emphasize teamwork that’s gone into finding a solution:** Here are some ways we can (or already have) work with business teams to come up with a new approach (e.g., strategy, policy, technology upgrades, budget).

• **Focus on business outcomes:** This is how the new approach could protect or recover your core business functions or performance metrics. Here’s how the required work would affect you.

• **Set realistic expectations:** Even with the new approach, there are still some risks we must live with. However, by working together we can greatly reduce our risk and have a defensible strategy. Any and all questions welcome!
All communications involve three components: the content, the relationship between the parties, and the organizational structure that frames the relationship and content. As we discussed in Chapter 2’s section “Clarify Security-Related Business Roles,” having a clear definition of roles and responsibilities can help many aspects of the security culture. Better security governance structures and security communication efforts are mutually supportive.

As noted in section “Security Culture Styles,” security leaders must be mindful of the business culture as they seek to communicate with stakeholders. Communicating effectively across multinational business cultures in large organizations requires a sustained team effort as suggested in the following CISO stories.

**COMMUNICATION TIP FOR MULTINATIONAL IT AND SECURITY TEAMS**

**CISO Stories of Building a Multinational Security Culture**

“You have to travel and get in front of the international business units. Face to face meetings, continual reiteration that you are building the security program for them and with them, not ‘just because.’ Understand and work with different culture’s communication styles. I found that in India they don’t want to say no, you have to get to the reasons why something would not make sense and work with those issues. Sometimes this means learning more about the customers of your customers.

Once the relationships existed, I was able to cross-fertilize know how on international weekly calls among security staff – e.g. Australia is having audit findings, here’s how Sao Paolo’s team handled that issue. If they’ve done something and been rewarded for it, they will value it.”

Michael Everall, CISO

“We realized we needed to tell people what we were doing as a team (everything from the network architecture on up); we made a list of 50 initiatives and prioritized 10 with champions assigned to develop presentations. When they travelled, they had to present one of that 10 to the local site. I told staff that I wouldn’t sign their expense reports unless they made a presentation, and I would personally add an extra ½ day to my trips for the presentation and open house Q&A. This was really appreciated, and we learned a lot.”

Paul Simmonds, CISO
Recognition of the need for security leaders and CISOs to improve soft skills has been growing for some time. The average CISO in 2020 is almost certainly a better communicator than his or her counterpart in 2010. But it hasn’t been enough – yet – to improve cybersecurity-business alignment and cybersecurity outcomes against the rising bar of threats, regulations, and business needs. CISOs can take the following steps to improve the security organization’s business communications:

- Make improving security-related communications a top priority.
- Provide communication training, measure communication skills, and hire effective communicators within the security organization.
- Recruit security champions within the business’s sales and marketing teams to provide additional coaching or training on communication skills for key security managers and staff.
- Obtain commercial communications training, coaching, and tools. Offer these enablers both to members of the security organization and to members of security-related functions such as compliance.
- Use the communication tips provided here for executive briefings and international teams. Collect a library of such tips for other situations.

4.4 Use Awareness Programs to Improve Behaviors and Security Culture

Awareness programs can be targeted to improve specific security-related behaviors for defined audiences. They can also be used in a strategic effort to improve security culture. Figure 4-3 diagrams three dimensions of an optimal user awareness and training program.
NOTE  I could have written a whole book on user awareness and training programs. Instead, I’ve limited discussion to the programs’ goals and strategies that support security culture and business alignment. Fortunately, there’s another book that’s highly complementary to the notion of driving a healthy security culture through the awareness program. Perry Carpenter’s “Transformational Security Awareness”\textsuperscript{12} gets much deeper into tactics and I’ll refer to it herein.

\[\text{Figure 4-3. Dimensions of User Awareness and Training Programs}\]

4.4.1 Promote More Secure Behavior

Today’s users work online in a minefield of malware, ransomware, social engineering, and insecure devices, applications, and networks. Some primary purposes for awareness programs are to improve users’ understanding of cyber threats to themselves and the business as well as teach them to practice basic security hygiene against those threats. Role-based awareness and training can also be deployed to IT, development, and other business areas to reduce human or technical vulnerabilities and/or promote regulatory compliance.

\textsuperscript{12}“Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors,” Perry Carpenter, John Wiley and Sons, Inc., 2019.
Some of users’ most common insecure practices are

- Failing to be vigilant enough to ignore or report potential phishing messages
- Falling for other social engineering tricks
- Selecting weak passwords or not changing default passwords
- Sharing accounts with colleagues, friends, and family members
- Telecommuting unsafely (using insecure Wi-Fi, leaving devices unlocked or unattended)
- Disabling security controls on a device
- Installing or using unauthorized applications
- Using obsolete software or unpatched software
- Revealing potentially sensitive information in personal interactions or on social networks
- Falling afoul of industry-specific compliance issues such as protecting customers’ personal information

Security leaders (with the support of the business) should use the full array of security program instruments to promote more secure behavior including policy, processes, awareness programs, and tools that either prevent insecure behavior or discourage it. An even better approach is to make secure behavior the path of least resistance; for example, multifactor authentication obviates the need to create highly complex passwords and change them frequently.

### 4.4.2 Target Awareness Campaigns and Training Initiatives

Awareness program leaders can identify which kinds of insecure practices are most prevalent or serious for the business by

- Running vulnerability scans for top areas of user-related vulnerabilities, such as weak passwords
- Interviewing the organization’s most knowledgeable user-facing staff in incident responder, help desk support, and HR roles to identify security topics on which users need help
Reviewing relevant audit findings (such as privileged administrators sharing passwords to service accounts in an unauthorized or ad hoc manner)

Surveying users or supervisors in the target populations

For further prioritization, the types of insecure practices can be correlated and prioritized for different audiences. Work environment factors to consider are the users’ business roles, hardware and software, IT-related roles, relevant risk scenarios, and defensive controls already in place. Find out whether different populations of users can

- Telecommute and use BYOD solutions
- Browse the Web relatively freely and connect to personal web-based mail from their work device
- Have local administrative privileges on their work device
- Get access to personal or sensitive information
- Administer IT systems or applications

Awareness program leaders can then identify a small number of audience types and tailor awareness messaging and training. For example, at a retail company, one might target all employees and full-time contractors for phishing training and phishing simulation testing. However, only office workers with devices would be trained on device security hygiene. Only administrative staff and store managers would be trained on consumer privacy regulatory compliance during an initial awareness campaign.

Having selected the target behaviors and populations, identify specific awareness/training objectives, audiences, messages, and medium(s). Note that IT staff and developers might merit awareness and training on some of the same issues as end users, but the messages and training content could vary. For example, both end users and IT staff could be cautioned against sharing accounts. IT staff could also be advised of acceptable organization-standard account sharing workarounds such as password vaults for break glass access but cautioned to adhere to policies against granting excessive privileges to colleagues or end users.

[13]“How to Design a PAM Break Glass Process,” Dan Blum, Security Architects LLC, January 2020, accessed at https://security-architect.com/how-to-balance-assurance-and-availability-in-pam-systems/
Larger organizations under medium or high security pressure should have a group dedicated to awareness training and a communications organization providing content preparation and delivery. In smaller organizations, or organizations lacking staff dedicated to awareness and communication, the security leader responsible for the program should consult with internal marketing staff and/or supervisors to learn which mediums (e.g., videos, email newsletters, lunch and learn sessions, posters, etc.) would be most effective for each audience.

“We try to follow the good practice of sending a positive message in awareness programs. Our awareness program leader believes that if you teach people how to be secure in their personal lives, that translates to business benefit because the basic literacy applies to everybody. Also, teaching awareness this way raises attendance at events.”

David Sherry, CISO Princeton University

In “Transformational Security Awareness,” Carpenter repeatedly emphasizes the need to work with human nature, not against it. People tend to resist doing things that are difficult, awkward, or require change. We tend to quickly forget about 90% of our training unless it is reinforced through use. Carpenter writes that instilling knowledge and awareness is like “an exercise in cutting through the noise and slipping past the brain’s defenses” to motivate users, give them the ability, and continually prompt them do the right thing. Facing this challenge, it is generally best to automate the desired task or behavior whenever possible.

Awareness professionals must adjust content and tactics to the following user behavior groupings: Those motivated and able to perform a duty, those motivated but not able, those able but not motivated, and those with neither motivation or ability. That’s how deep security user awareness and training can get into behavioral science, multimedia content development, and attention management. Carpenter notes: “Being a security expert doesn’t naturally transfer to communicating security-related information to people outside the field.” Therefore, in my experience, successful awareness programs rely heavily on non-technical people with a background in marketing, education, or communications to work with technical experts.
4.4.2.1 Special Considerations for Work at Home, or Bring Your Own Device (BYOD) Programs

In 2020, COVID-19 forced many organizations to greatly expand teleworking and BYOD programs. As part of expanded remote access, employees in many cases require more latitude to browse the web free of restrictions or protections from proxies or firewalls. Hackers have moved to exploit newly vulnerable users and their organizations leading to increases in fraud and abuse.

Although it’s generally preferable to limit users’ vulnerability through automated technical controls, such as blocking ports on a device, it isn’t always possible to do that in a BYOD environment where controls require more user discretion, or user cooperation, to operate.

As organizations seek to stabilize home office security and (in many cases) to continue supporting remote work over the long haul – users’ security awareness becomes even more strategic to business success. Security leaders can take the opportunity to partner with business and IT functions concerned with improving staff’s digital literacy and proficiency, which are also a cybersecurity concern.

4.4.3 Coordinate Awareness Messaging with Managers and Key Influencers in Target Audiences

Business people are more likely to be influenced by awareness and training if their managers and executives support the program.

> To maximize the chance of success, security leaders need to gain buy-in for awareness, training, or security culture improvement programs, in advance from the managers or executives of the target groups.

Security leaders responsible for the awareness program should establish relationships with business or LOB executives, gain their trust, and seek their buy-in and support for the strategic use of awareness programs.
“The attitude, behavior and messaging related to security from the CEO (and other executives) is critical. Just having the CEO wear a badge whenever appearing on an all-employee video sends a message.”

Christopher Carlson, Information Security Writer and Adviser

Once management is supportive, role- or audience-specific awareness and training doesn’t necessarily require an over-sized budget. The awareness program can reach out to influencers in the organization as well as security team members and IT staff to get some assistance. Consider using customizable curricula with a “train the trainer” approach. Engage experienced staff to introduce, explain, or add context to generic or third-party training content for their colleagues.

Coordinate security communications to the business with IT computer support and applicable corporate administration functions (HR, legal) or LOBs. Align instructions on how to perform basic or role-specific security duties with corresponding security processes.

Involving IT or business-level staff in customizing role-specific training or awareness content not only builds the library of training materials but is also more engaging and memorable to the staff themselves. Role-specific training can be tied to corresponding security processes, such as how should

- An executive sign off on a risk acceptance memorandum
- A data steward evaluate a Sales Department request for releasing customer information to a partner
- A system administrator request access for a third-party vendor to troubleshoot a critical system

See Chapter 6’s Table 6-3 to identify which control domains engage which business functions. Consider training needs for managers and staff in the roles needed to implement each control domain according to the organization’s security or business processes. As the awareness program builds a network of key influencers throughout the organization, its ability to create a healthy security culture grows.
4.5 Commit to Improving Security Culture

Business and security leaders in organizations with a healthy security culture tend to accept and approve of requirements for awareness programs and security governance. They seek to move the organization from being one that performs tactical awareness and training projects to one that intentionally defines and measures security culture targets as a way to achieve its security vision, drive its security strategy, and meet its security objectives.

A long-term commitment to improve security culture could operate on a few different points of the continuum between purely tactical compliance–driven awareness programs and strategic, full-on security culture transformation programs. Note that strategic commitment could take the following forms:

- Establish formal security culture teams, projects, and process methodologies. ENISA’s “Cyber Security Culture in Organizations” report\(^1\) proposes a “do it yourself” model for such a program.
- Engage a management consultant specializing in driving business change and who has experience working with IT and security programs.

I’m guessing that the majority of those reading this, however, don’t have the mandate for a full-on transformation program or funding for the additional project team that would be required. The good news is that what I propose in the sections “Make Enhancing Communication a Top Security Team Priority” and “Use Awareness Programs to Improve Behaviors and Security Culture” are about midway along the continuum between a tactical and strategic approach. Although they require and deserve some additional funding and management priority, they shouldn’t require additional teams of resources in the typical organization.

Awareness and training efforts to strategically improve security culture can be built in an iterative manner and therefore be accessible to almost any security organization in almost any business. The main prerequisite is to enrich the awareness and training program to be a bit more strategic, enhance security-related communications, and measure aspects of the security culture along with the results.

---

\(^{1}\)“Cyber Security Culture in Organisations,” European Union Agency for Network and Information Security (ENISA), November 2017, accessed at [www.enisa.europa.eu/publications/cyber-security-culture-in-organisations](http://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations)
of these efforts. As described in section “Measure and Improve,” the awareness and communications programs can periodically measure and assess the as-is culture and security posture, select departments or audiences for awareness projects, and perform them. Then measure the results and adjust or sustain those activities, practices, or communications that are successful. At a later stage as awareness and communications programs mature, the business could choose to begin a full-on security culture improvement initiative.

4.6 Measure and Improve

Because security culture is multifaceted and full of subtleties, businesses can benefit by developing, choosing, and monitoring culture metrics. Due to staff turnover and continual changes in security policies, technologies, regulations, and the business, security culture and user awareness program effectiveness should be measured at least once every two years. Security leaders can pursue any (or all) of three suggested approaches to measure security culture–related information over time:

- Measure security-related communications effectiveness.
- Measure security awareness program effectiveness.
- Measure culture comprehensively to determine whether a security culture program is effective.

4.6.1 Measure Your Ability to Improve Security-Related Communications

What if some of security culture’s woes are self-inflicted (see the “Ineffective Security Communication Styles” section)? Why then it would be useful to measure the progress and effect of efforts to apply the guidance in the “Make Enhancing Communication a Top Security Team Priority” section. CISOs can

- Make a list of recent security communications to stakeholders via briefings, meetings, email announcements, newsletters, posts, and important informal contacts. Have an objective party or audience member rate each on a scale of 1–5 for clarity, fitness for audience (i.e., business or IT), positivity, efficacy, and other desirable attributes. Track these ratings over time.
CHAPTER 4  STRENGTHEN SECURITY CULTURE THROUGH COMMUNICATIONS AND AWARENESS PROGRAMS

- Self-assess and ask key team members to self-assess communication skills.
- Get feedback from stakeholders after briefings.

Set targets for improvement based on the data and measure again after a period of time.

### 4.6.2 Measure the Effectiveness of Security Awareness Programs

We can often measure the effectiveness of programs to promote more secure behavior by analyzing IT artifacts before and after awareness or training campaigns. Examples include events in logs, device or account security configuration settings or passwords, and test results such as the output from phishing simulations. In some cases, one must get creative about identifying IT artifacts that are outcomes of the behavior, such as the number of files flagged for containing sensitive data outside authorized repositories. Still other behaviors don’t produce IT artifacts but must be measured by human observation.

For other attributes of the security culture (see Figure 4-1) we can measure norms and attitudes through user surveys, and cognition or compliance through testing and observation.

### 4.6.3 Measure Security Culture Comprehensively

Some of the industry insights provided in this chapter might not have been realized were it not for *The Security Culture Report 2018.*\(^{15}\) The results from the report demonstrate the value of being able to measure security culture. Repeating measurements at the organization level enables businesses to understand how their security culture improves or worsens over time and fine-tune awareness, training, and other programs to correct course as needed. Improvements in culture can also be cited in audit or compliance reports as evidence that “people and process” controls are operating effectively.

The CLTRe toolkit\(^{16}\) measures the attributes of security culture listed in Figure 4-1: attitudes, cognition, communication, compliance, norms, and behavior.

---

\(^{15}\)“Security Culture 2018: Measure to Improve,” CLTRe AS, Kai Roer, 2018, accessed at [https://get.clt.re/report](https://get.clt.re/report)

\(^{16}\)CLTRe website, CLTRe (a KnowBe4 subsidiary), accessed at [https://get.clt.re/the-cltre-toolkit/](https://get.clt.re/the-cltre-toolkit/)
4.7 Call to Action

The core recommendation for security leaders from this chapter is to improve security culture through awareness and communications programs as follows:

- Seek executive support for making security culture improvement a strategic objective.
- Devise ways to promote, prioritize, and target awareness programs to improve security culture as well as problematic security behaviors.
- Coordinate awareness messaging and other communications with the executives or managers of the target audiences.
- Focus on role-specific training as well as basic user-related awareness issues such as the vulnerability to phishing messages.
- Target security communications as needed to applicable audiences or groups.
- Obtain support from influencers in target audience, especially for role-specific programs.
- Evaluate how the security organization communicates with businesspeople, and measure how well the communication is received.
- Measure the success of awareness programs and other efforts to improve security culture.
- Measure improvements in security-related communications.

Action – Make a quick assessment of the state of the organization’s security culture, communications, and awareness programs.

Ask yourself the following short set of questions and score the answers in the Success Plan Worksheet's Section 3, Table 3. Base your score on whether you would answer most of the questions with a strong “no” (1), a strong “yes” (5), or something in between.

1. Do business executives prioritize and support cybersecurity (i.e., consider it strategic)?

17“Rational Cybersecurity Success Plan Worksheet,” Dan Blum, Security Architects LLC, May 2020, accessed at https://security-architect.com/SuccessPlanWorksheet.
2. Do business, IT, and development managers provide resources to security projects and help enforce security policies?

3. Do security team members have positive relationships and communications with business stakeholders?

4. Does the security organization treat communicating with IT and business leaders as being a top priority?

5. Are security leaders incentivized to
   a. Maintain regular communication with IT and business leaders in their functional area?
   b. Improve their communication skills and those of their team members?

6. Does the security organization have a user awareness function sized to the business?

7. Does the user awareness and training function
   a. Communicate in an efficacious manner (“we can do this,” “here’s how others have been [safe, successful]”)?
   b. Target awareness programs to specific audiences?
   c. Coordinate programs with the audiences’ leadership?
   d. Provide role-specific training?
   e. Recruit champions among the target audiences and “train the trainers”?
   f. Provide information or free tools that will help staff and their families improve cybersecurity at home?
   g. Coordinate with the marketing organization’s internal communications program?
   h. Use innovative and entertaining communications mediums, products, or services?
8. Does the security leadership or awareness program itself measure whether awareness and training programs are improving
   a. Security-related behavior?
   b. Attitudes and perceptions about the security program?
   c. Understanding of policies, tools, and procedures (cognition and compliance)?
   d. Compliance audit results?

**Action – Define 1–3 improvement objectives for security culture**

Note improvement objectives in Section 4, Table 5b, of the worksheet. The following are examples of security culture–related improvement objectives:

- Continuously maintain the stakeholder engagement table as part of an ongoing personal or team project (especially in larger organizations).
- Assess your communication style or habits and improve at least one practice.
- Get the security team to assess group communication styles or habits and improve at least one practice.
- Create and manage at least one practice for user awareness and training improvement (e.g., task key team members to collect feedback from 1–3 business or IT stakeholders on security-related communications).
- Prepare an informal briefing on security culture (using this chapter as a resource) and present or discuss it with at least one of your business or IT executive sponsors.

Don’t limit yourself to these examples. Look for improvement objectives that fit the gaps and priorities you’ve identified for your business.
