tripwire

WHITE PAPER

# How to Be a Successful Cybersecurity Leader in the 2020s

## Building a Strong and Forward-Looking Security Culture

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

**You and your security team have a lot on your plate. It's crucial to keep your organization's network protected by maintaining a security program that minimizes risk, and it's you and your team's responsibility to execute this.**

**This effort has only become more complicated as we've entered into a new decade. With the dramatic shift to many of us working from home in 2020—and many organizations choosing to keep things that way long term—some of the well-established methods and processes your team may have been using need to be adapted to the new virtual workplace.**

As we start this new decade, you want to make sure that you are setting yourself up for success as a security leader. You can do this by intentionally communicating cybersecurity strategies and initiatives to all employees and promoting safe and secure business practices to curate a cybersecurity culture within your organization—while on top of that, building a well-rounded, flexible, and productive IT/IS team to execute your security goals.

## A Decline in Organizations' Security Focus

Cisco recently did a study that highlighted a concerning trend that organizations' leaders have not been putting as much of an emphasis on security as they have in the past. Eighty-nine percent of respondents, dropping seven percent from the past four years, said their executive leadership considered security to be a high priority. On a similar note, 90 percent of respondents shared their employer's executive teams established clear metrics for evaluating the organizations' security programs, which is six percent lower than last year.[1]

There are  a multitude of reasons for this decline. One reason is a disconnect or lack of communication between the organization's security team and the rest of the organization. Going one step beyond that, it may be that the disconnect is between the security team and the executive team. Let's take a look at how improving this communication can improve the organization's outlook on security.

## Gain Executive Support

In order to successfully build, sustain, and promote your organization's cybersecurity program, you will need to have executive buy-in. Cybersecurity should be presented as a business risk, not minimized to merely an IT problem. By not emphasizing the necessity of a strong security program, it can be easy for your efforts to be pushed aside by the executives and the rest of the organization.

As a CISO or other security leader, you must work with executives to show the value of a strong cybersecurity posture—translate the initiative into clear points outlining the mission and strategy that executives will want to get behind. Christina Morillo, Sr. Product Manager, Security at Marqeta, highlights the need for executive buy-in:

*"Foundationally, the main factors when building a cybersecurity program are executive buy-in and sponsorship. These include clear lines of accountability and responsibility. Without executive buy-in, sponsorship and support, your initiatives will fall flat. A program of this magnitude must start from the top down. Defining the mission and strategy, clearly articulating and documenting the why and the what as well as aligning this to business risk minimization will help to gain leverage and buy-in across all stakeholders."*

Having executive sponsorship on your security initiatives will give you the momentum to push the project forward and give it more visibility across the organization. This will help you build a cybersecurity culture. Security often comes from the top and flows down. The push to build a cybersecurity culture should be done intentionally—such as allocating time during company-wide meetings to promote this initiative, sharing best practices and discussing how cybersecurity aligns with the business's objectives.

## Cybersecurity Is Everyone's Job

So why is it so important to build a cybersecurity culture? It's because everyone plays a role in keeping their organization secure. There are efforts that every employee can and should make to keep themselves and the organization protected from risks and vulnerabilities. Nigel Sampson, Alegeus' Head of Information Security, shares why having a cybersecurity culture is so important:

*"Getting the organization to understand the importance of information security (IS) as well as leveraging best practices and training is key to communicating their role and responsibility when it comes to information security. They need to get the message that just because there is an information security department doesn't mean that those team members are solely responsible for information security. Each employee has a part to play in the information security program."*

Employees should be well-informed about what they can do to stay protected. Executive sponsorship is crucial—because when you have executives behind you, you will have the platform to

share this information with the rest of the organization.

On top of that, as a security leader, it's important to make sure that complicated security issues are shared in simple verbiage that the whole company can understand. While cybersecurity is everyone's job, not everyone is a cybersecurity engineer. Ron Solano, Data Security Officer at OptumInsight of UnitedHealth Group shares:

*"While it's important to understand technical issues, the CISO needs to translate that into easy-to-understand communications."*

A big responsibility of being a security leader is being able to effectively communicate. A CISO, or someone in a related role, should be able to speak to the value of security and discuss risk management with anyone—from the security team to the CEO to the receptionist.

## Learn More

To learn more about how you can build a cybersecurity culture across your organization, be sure to check out ***Cybersecurity is Everyone's Job***, a publication of the NICE Workforce Management subworking group of the National Institute of Standards and Technology (NIST).

## Adjusting to Remote Work

The shift to working at home has likely shaken up how you and your team do your jobs. You've needed to adjust to the influx of employees logging onto the network every day. You've had to take extra and/or different precautions to make sure this is being done securely.

Now that many organizations are working remotely, it has become more important than ever to promote a cybersecurity culture. Employees are exposed to more risk working from their home offices, therefore putting your organization at more risk. According to BusinessWire, 94 percent of cybersecurity professionals are more concerned about security, and 89 percent said that their job has become more difficult since this shift to working from home[2]. It is more of a challenge to keep systems secure and compliant, and there is an increased threat of ransomware or phishing attacks.

On top of that, the way the team goes about doing this work and problem solving is different. You can no longer walk a few steps over to a colleague's desk to quickly brainstorm a solution to a problem. A replacement to a physical piece of equipment isn't just in a closet down the hall. You and your team have had to adapt to instant messaging as means of communicating, have gotten more comfortable with getting on the phone to hash things out, and planning ahead when it comes to handling things that need to be done physically on-premises.

Further easing these hurdles, again, can come from executives' intention of addressing these challenges for their security team. Dr. Grigorios Fragkos, CISO, discusses the impact this has made on his organization:

*"... [T]he leadership's commitment to cybersecurity made a huge difference. The early decision to invest in OPEX, focus on a dynamic design and flexibly expandable architecture, have strategic partnerships in place and develop a clear distribution of responsibilities paid off. All these early decisions allowed the cybersecurity team to enable different types of business requests in a secure manner."*

Wile the shift to working from home was done out of necessity, this will likely be a more common situation for many employees or even entire organizations for years to come. It is worth it to invest in and rebuild processes that work with this new normal.

## Build and Manage a Strong Team

As a security leader, you know how important it is to have a strong team. A strong team means that it is built up of intelligent, flexible, and diverse people.

Especially since many IT teams have needed to adjust their processes to adapt to this decade's new remote workplace, it is beneficial to have smart members that don't all think the same way, so the team can creatively problem-solve these unique challenges. Christian Toon, CISO at Pinsent Masons LLP, believes that diversity is something that the industry should be putting more of an emphasis on.

*"A big problem with this is that we lack diversity in our industry that can help bring about positive change. (There's a reason it's known as a 'God complex' and not a 'Goddess complex.') Organizations try to hire in a particular template, and it inhibits them from becoming more effective around cybersecurity. If the security team looks like the security leader, there's a problem."*

Additionally, to have a strong team, you need to ensure that your team is as productive as they can be, giving them the flexibility they need working from home and making an effort to make sure they are not getting burnt out. Employees each have unique working styles and different personal situations; it's even more important to accept that as working from home has become the norm. How one person on the team works to be the most productive may not be the same as for others, so allowing team members to find their own rhythm is not only helpful for preventing employee burnout, but will also help the team be at its most efficient.

Another way to prevent burnout is to intentionally make the effort to still keep your company culture. Dianne Kelley, CTO at Microsoft, highlights the value of collaboration, whether it's about work or just socializing:

*"Remote work can be an engaging, collaborative experience when teams brainstorm in video meetings, iterate documents and projects in shared workspaces, and track progress in ongoing chat threads. And having a bit of fun matters, too! To keep remote workers connected, consider virtual group activities like a weekly brown bag lunch, happy hour, or a book/movie discussion club. Find a way to replicate water-cooler comradery in the virtual world."*

Your organization has likely made efforts to find the virtual equivalent of eating lunch with coworkers in the break room. Be sure to not forget about these efforts as the work from home lifestyle begins to feel more normal.

## Summary

The start of a new decade is a great time to take a look at your strategies, priorities, and processes as a security leader. The dramatic shift to many of us working from home will have a big impact on the workplace for years to come, so adjusting to this will be crucial to you and your team's success. No matter what your office looks like, you should focus on building a strong security team and curating a cybersecurity culture within your organization. Both of these will help you accomplish your cybersecurity goals in the 2020s and beyond.



## Sources


1 "Securing What's Now and What's Next: 20 Cybersecurity Considerations for 2020." Cisco, Cisco Cybersecurity Report Series, 2020, www.cisco.com/c/dam/en/us/products/collateral/security/2020-ciso-benchmark-cybersecurity-series-feb-2020.pdf

2 "Tripwire Survey: 94% of Cybersecurity Professionals More Concerned About Security in Wake of COVID-19." Business Wire, 13 May 2020, www.businesswire.com/news/home/20200513005006/en/Tripwire-Survey-94-Cybersecurity-Professionals-Concerned-Security

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
**Connect with us on LinkedIn, Twitter and Facebook**


WPSCL1a 2011