public sector leaders are constantly seeking smarter ways to improve their cybersecurity posture amid the growing number of daily cyberthreats and to meet the needs of a workforce that has been working almost entirely remotely for the past four months because of the COVID-19 pandemic.

While digital tools and artificial intelligence provide better analytics and visibility across agency networks, executives still struggle to prioritize security risks and responses across the overall environment.

One way to build a stronger cybersecurity strategy, and align resources more effectively, is to require a greater security awareness and engagement across all the major lines of business, says Sajed Naseem, Chief Information Security Officer for New Jersey Courts.

It is important that organizations establish a balance between risk mitigation and completely securing systems. This will depend on the business case. For example, public websites containing public information are expected to have risks mitigated, while systems with confidential data are expected to be secured, Naseem says.

But to get there, public agencies need a cybersecurity framework to spell out the areas of risk that are most important. Those risk areas are the ones that support the continuity of the mission, the security of critical assets, minimal liabilities and positive growth.

Properly defining a framework is where many organizations fall short, says Naseem. If a cybersecurity framework is built and managed only within the security team, not only will they fail to gain buy-in from agency executives, but they may also misunderstand the organization’s most vulnerable systems as they look to mitigate risks.

Naseem, who leads security initiatives for New Jersey’s judiciary, with close to 750 physical court locations and networks and 50,000 devices. The systems directly serve 100,000 attorneys, 25,000 police officers and 10,000 staff members, as well as the public.

But the challenges his team faced throughout the COVID-19 pandemic have reinforced for him why getting executive buy-in is a critical component for successful security program. Because of meaningful executive engagement before the crisis, when priorities shifted, his department received the additional resources it needed to address increased risks from the surge in employees relying on home networks to proceed with their casework.

Evaluate risks

Even before the COVID-19 pandemic, Naseem and his team had been working to better understand risk within the organization. Their approach welcomed judicial stakeholders to collaborate with the security team on a strategy that defined high risk focus areas.

One of the first areas of modernization was the court’s records management system and other applications to process documentation. Naseem explains that because the judicial system already has predefined rules for which documents are public or confidential, the CISO’s team worked with the courts’ lawyers to make sure it understood these rules in exactly the same way as the judicial departments.

The effort to establish better cybersecurity and risk management practices required building a cybersecurity framework.
to clearly define language across the organization. And that broke down into two fundamental objectives for the court. “Some technologies need to be secured and others need to have risks mitigated, depending on the business case,” he explains.

However, Naseem shares that in his experience executives tend to have a difficult time with the question of how to prioritize risk, which means that they aren’t focusing on the right issues.

Ask the fundamental questions

Agencies that struggle to build a holistic cybersecurity framework can probably trace problems back to not being able to clearly communicate the business risk of security to decision-makers within the organization, Naseem says.

When the courts began to address fundamental questions about the goals of the mission, Naseem’s security team and key stakeholders from across lines of business worked together to answer fundamental questions about their security objectives before having any discussions about technology, budget and resources.

They leaned on guidance from resources like the National Institute of Standards and Technology’s (NIST) Cybersecurity Framework (CSF). NIST CSF is a great place to start when building a cybersecurity governance program. It creates a common, quantified risk measurement for all government agencies. And by removing the subjectivity, it helps an organization manage cybersecurity risk more systematically.

Additionally, the courts looked at incorporating a model known as the CIA triad — confidentiality, integrity, availability — a security strategy to protect data on multiple fronts. This strategy is especially important for a system like the New Jersey Courts that is trusted to protect the personal information of children and victims of crime.

To address building a culture of cybersecurity readiness and performance for information security among agency leaders, Naseem and his colleague described other key questions that can often be tough to answer, such as:

- Is the organization’s leadership investing in information security?
- Is the security program more than just cybersecurity tools?
- Does the information security team have autonomy and authority?
- Does the organization have coordinated and measurable information security and cybersecurity awareness programs?
- Are all relevant decision-makers involved in the organization’s cyber-incident-response program?

Naseem shares how involving key stakeholders early on established relationships and helped the security team greatly when it needed to shift focus after the pandemic hit.

Additionally, with so many priorities for the organization, it helps to identify a handful of risk areas — or a “risk register” — to focus on in order to maximize resources against the most urgent threats. Naseem’s office updates these in an actionable guide that is distributed across the organization. And with the help of cybersecurity readiness and performance metrics that measure knowledge, behavior and attitude among employees, the security team is able to apply qualitative and quantitative measurements to these risk factors.

Be ready to pivot if needed

When the physical offices shut down and employees began working in a virtual environment from home, all agencies had to double-down on cybersecurity. Naseem recalls how the shift to work from home left his team asking, “how do you take largely in person service and make it remote?” Suddenly, the top risk areas had to get reprioritized.
Move cybersecurity forward

The CISO role is now a business-focused one, with electronic issues being related to physical issues. So CISOs need to exhibit leadership while being data-driven.

Those who can define a measure of cyber risk can demonstrate the ongoing value of security to executives. For example, establishing a baseline to define risk; or focusing on the speed of incident closure — not just the incident count.

Using tools that provide a single, unified dashboard and update key metrics in real time is the best data-linked approach to help articulate the organization’s current cybersecurity posture.

According to Forrester, these modern governance, risk and compliance platforms can better equip organizations to meaningfully use artificial intelligence, machine learning and predictive analytics to include disparate data and identify patterns and irregularities.

Experts recommend that a modern risk management tool should also include some key protections such as secure authentication, encryption, data loss prevention, network access control and incident response.

Learn how to advance your mission with data-driven insights.

This report was produced by FedScoop and underwritten by Galvanize.

"A lot of responsibility for cybersecurity problems is still at the local operational level"
- Sajed Naseem -

"We were looking at how to handle work with technology and paid special attention to any distractions at home that could interfere with online court proceedings," Naseem says. Because the judiciary’s executive leadership already was supportive of and engaged in implementing the cybersecurity framework, they were able to quickly shift priorities and budgets to meet the new needs.

At the outset of the shift to support a remote workforce, court committees began to look at any disparities or anything that is in a computer that can change the way a court proceeding is happening.

"For example, when using a video platform if one party is playing ambient music in the background, they will always show up number one on the screen. These scenarios can shape the way people see things," explains Naseem.

Tap into leadership

Building a cybersecurity framework and identifying metrics requires the right mix of people at the table, even when that table is a virtual one. This is why even large agencies need to identify those with leadership qualities at both headquarters and regional offices.

For the New Jersey Courts’ 750 locations, Naseem explains that it was imperative to tap into those individuals at local offices who knew more about the processes pertaining to those sites.

“A lot of responsibility for cybersecurity problems is still at the local operational level,” says Naseem, who says the headquarters office needs to allow each outlying office to communicate its needs in order to set effective priorities.

When working on a holistic strategy, there needs to be “a distinction within an organization between leadership and management,” he says. A quality he looks for in leaders are those who — when times get tough — focus on how to improve the productivity of the organization, not just manage a team doing their routine work to “keep the railroad running.”