For almost a decade, the cyber community has said it's all about the data. The systems, the networks and the hardware devices are important, but if you can secure the data, you are protecting your organization's most important asset, beyond people of course.

Federal News Radio Executive Editor Jason Miller dove deeper into this issue and others during the panel discussion, "Cybersecurity vs. Data Security: Government's Two-Pronged Challenge," in recognition of National Cybersecurity Awareness Month. Guests included Ann Barron-DiCamillo, director of the Homeland Security Department's US-CERT; Bill Lay, the State Department's deputy chief information officer for Information Assurance and chief information security officer; Dr. Ron Ross, a fellow at the National Institute of Standards and Technology and Eddie Garcia, chief security architect in the Office of the CTO at Cloudera.

Many organizations, agencies and the private sector spend much of their resources on cybersecurity. And with the recent data breaches at the Office of Personnel Management, Target, JP Morgan Chase and a host of other large organizations, are agencies and companies focusing on the wrong issues?

If you look at recent legislation, it's focused on information security, whether it's the federal information security management act or the cyber information sharing protection act or a host of other bills.

Then what is cybersecurity and how does it relate to data security?

Some say cybersecurity is about behaviors and activity while data security is about information.

Other experts say cybersecurity has been viewed as a means to data security, but can the reverse can also be true?

When talking about data security, what should agencies focus on? How does data hygiene, data analytics and other security approaches to data protection apply?

On the issue of data security vs. cybersecurity, Ross said, "I think that you can find differences in the definitions, but I think they're very much related," he said. "I've never been able to separate information security from the actual system where that information is processed, stored and transmitted.

“So when we talk about protecting information, it has to be the case that you have to protect the system where that information lives. And so when you talk about behavior versus information, it’s always been about processes, people and technologies.”

From an operational standpoint, the Lay agreed with Ross in that it’s difficult to separate data security and cybersecurity.

“You have to take a full-spectrum approach,” he said. “It’s not just focused on the technology; it’s not just focused on ‘is your data secure?’”

“The people portion is huge,” Lay continued. “Especially with our attack vectors changing, the skill sets are always maturing and becoming obsolete. It’s a moving target for all of us.

“The goal for IT is to enable an organization – in our cases, a federal agency or department – to do its mission. We’re there because of the mission, the mission’s not there because of the IT.”

Barron-DiCamillo added that because agencies can’t protect everything, it’s important to focus on what matters most, such as personally identified information and other sensitive data.

“So I think from an incident response perspective, we’re really seeing a shift across departments and agencies, critical infrastructure partners, state, local, tribal territorial partners, and international constituents to really focus on what matters most,” she said.

“Identify your high-value assets within your networks and ensure that those get the priority protections because it’s such a large attack surface that we’re all trying to focus on with limited resources, with not enough skilled practitioners doing this job,” Barron-DiCamillo added.

On the industry side of the discussion, Garcia said many organizations that have implemented traditional data security tools are lacking the necessary user behavior component.

“Big data platforms enable us to look at data from different ways, taking into consideration other pieces of information that we couldn’t do before,” Garcia said. “This gives us a new perspective and insights that we couldn’t detect before.”

Garcia went on to note organizations can now see a person that has access to data, but also detect if that person uses the data in a way inconsistent with previous behavior.

“We can now say, ‘Why is he looking at this data? Why is he downloading these files?’” Garcia said. “So there’s a different behavior for that user and can lead you to ask, ‘Well, has his account been compromised? Is that the reason? Or is he planning to leave the organization and started downloading files onto his thumb drive? So looking at these other pieces of information – data points – will allow you to do better security analytics.”

Lay later noted the difficulties of identifying such inconsistencies.

“It really becomes a big data challenge,” he said. “In the past we had different groups of individuals with different skill sets looking at different types of data, whether it was security logs off of routers and switches, whether it was profiles coming off of a Microsoft or Linux server or another group that might be looking at how our desktop computers are configured.

“Now since it is more of a full-spectrum approach, we’ve got to do a much better job correlating and combining the information,” Lay continued. “One, to eliminate the millions of false positives that ensue, and two, being able to pull out that kernel of information that shows, OK, there’s some kind of nefarious activity here that we need to explore further. So, it’s basically finding a needle in a whole field of haystacks and it’s quite the challenge.”

Barron-DiCamillo likened it finding “a needle in a stack of needles.”

“I think for a long time there’s been a bit of a disconnect between the data and how it’s used,” she said. “I think CDM is a data source but can also be that conduit between a lot of the different data sources that we’re seeing from an incident response perspective.

“We’re seeing things that are evolving in the wild, things that are evolving from vulnerabilities and from other attack vectors,” Barron-DiCamillo added. “So CDM’s an ability for us to say, ‘OK, adversaries are leveraging this exploit. Who across the departments and agencies have an exposure to that vulnerability?’ And CDM gives us a good understanding on where we need to prioritize limited resources associated with prioritization of patches, prioritization of mitigation

techniques around certain environments to ensure that those attack vectors that we see being leveraged in the wild are not going to be successful.”