Cyber Resilience Before the Crisis: Proactive Strategies and Funding Pathways for Public Sector Organizations

Webinar Transcript • July 9, 2026

Presented by Michael Paddock, Dr. Liz Shay, and Shannon Day, Grants Office, LLC, with Jason Likens and Felix Alvarez, Rubrik

Sponsored by Rubrik, Inc. • Grants Office, LLC

Welcome and Introductions

Michael Paddock:

Hello, everyone, and thanks for joining us for Cyber Resilience Before the Crisis: Proactive Strategies and Funding Pathways for Public Sector Organizations. I'm Michael Paddock, CEO of Grants Office, and I want to welcome everyone to today's session. We've got a good one. We've heard from a few of our attendees who have said they're really looking forward to what we're presenting today, so welcome to all of you, and we'll look forward to a great session. Before we get too far into it, I want to very much thank our sponsor, Rubrik, for sponsoring today's session and making it possible for us to bring you this information. Big thanks to Rubrik for sponsoring today's session.

You probably saw the housekeeping items in the waiting area before we entered today's session. For those of you who want to have access to the recording, the session is being recorded, and optional materials, including the slide deck, will be available on the resources page immediately after today's session. Kate, our intrepid webcast producer, will be posting updates on that in the chat throughout the course of today's session. So check out the chat, and you can also ask questions in the chat, as the housekeeping message said. Feel free to send in whatever questions you'd like, and we'll get to as many as we can over the course of today's session.

Okay. Cyber Resilience Before the Crisis — as I mentioned, we've got a lot to cover today. We're going to talk about some background on the need for cybersecurity and some of the threats that are out there. We'll hear from some of our friends at Rubrik about those, and then we'll talk about grants for cybersecurity and how to think about cybersecurity in the context of grantseeking. There are certainly grants available for cybersecurity, and there are other grants that can fund cybersecurity — actually, many grants that can fund cybersecurity as part of a larger project. So we'll talk about those, and then a little bit about the Rubrik Grants Support Program. Not to give too much away, but it is a robust grant support program that Grants Office is very happy to be a partner with Rubrik on, and you can get free, no-obligation grants support through that Rubrik Grants Support Program. We'll hear more about that

toward the end, but I just want to give a shout-out to the program before we get started. And then, as I mentioned, with whatever time we have left, we'll go through the questions that have come in up to that point.

I'm joined by a great group of panelists — a really knowledgeable and expert group here. On the left side of your screen, you'll see our cybersecurity experts: Jason Likens, Vice President of Sales Engineering for SLED at Rubrik, and Felix Alvarez, SLED National Practice Manager here for Rubrik. And on the right side of our screen, the Grants Office professionals: Dr. Liz Shay, Senior Grants Development Consultant here at Grants Office, and Shannon Day, also a Senior Grants Development Consultant here at Grants Office. So we've brought in the heavy hitters, and we're looking forward to a great session. Without further ado, I want to pass it over to Jason Likens to talk to us a little bit about some background on cybersecurity and what the needs are. Jason?

Proactive Cyber Resilience in Practice

The Threat Is Real, and Public Sector Is a Primary Target

Jason Likens:

Thank you so much for the time. I really appreciate it. For those listening, my name is Jason Likens. I'm the Vice President of Sales Engineering for Rubrik. Happy to spend some time with you today. We're going to talk a little bit about ransomware, and hopefully I can give you some information that might be relevant or impactful for you guys as we talk about Rubrik as well as our grants program. So let's dive in. When you're looking at ransomware, the first thing we have to do is acknowledge that the threat is incredibly real, and in public sector, we are a prime target.

When you look at some of the numbers across this screen: over 2,000 ransomware attacks on government and educational institutions alone. That figure is from 2023; the most updated figure is well over 3,000 attacks. The average downtime for an attack: 21 days. That's actually really generous. Lately, what I've seen is closer to 45 days, but the average, when we take it across all verticals, is 21 days. Then the cost — there's a cost associated with recovery. That average cost is $2.6 million. That's really big; it's impactful. It's going to cost people their jobs, but it also encompasses fines. A lot of people forget about the different fines for sensitive data and the exfiltration of that data.

There are a lot of things we can talk about in this, but the biggest thing that I want to talk about is the services that get impacted when this happens. We look at school systems that can't teach their students and have to send them home — or, worst case, have to not only send them home but then pay for a LifeLock service because their students' data was compromised; those Social Security numbers were compromised. Here's a real example that happened in a county neighboring mine: they were hit with

ransomware, and their 911 system went down. They couldn't dispatch to help people in need. Hospitals were impacted. Court systems couldn't operate. Another real-life scenario happened out on the coast: a customer was hit by a hurricane, and the ransomware attackers took that as a prime opportunity to hit them with a ransomware attack while they were down. Not only was that big because there was a hurricane going on, but their supervisory control and data acquisition, or SCADA, systems were locked down off the network. They had a part fail, and they didn't realize it because their production system was down; the email relay didn't work.

Those are critical things when we talk about the threats that we're facing out in the world today, and they only get worse.

Reactive Recovery vs. Proactive Resilience

So what we want to do is shift the story and talk about the way that we approach this. If we look at reactive recovery versus proactive resilience, people often ask, what does that mean, and how does that impact me in any meaningful way? Well, it's the difference between reacting after something has happened and being prepared for it, so that when it happens, we have a plan that is tested, that is validated, and that can help us recover quickly, successfully, and without issue.

When we look at reactive restores, we're discovering those after we're hit. What happens in those scenarios is that you'll get hit with ransomware, and you'll get a pop-up notification, and that's how you figure out something has happened. In a lot of cases, your backups will already have been encrypted. Everything is going to be inaccessible. You're going to be talking about how you have to go rebuild things, and in a lot of legacy environments, that's calling tapes back and hoping those tapes didn't break, hoping they didn't get degaussed, hoping that the data we need is actually on those tapes. The big part of that that gets really scary is that we don't have visibility into the breadth and depth of the attack. We can't identify what's called the blast radius. We don't often know what we were hit by until we've called in the National Guard, in a lot of cases.

The big thing is, in these scenarios, you either have to choose between paying the ransom or rebuilding everything. One thing they don't tell you: even if you pay the ransom, it almost certainly guarantees that you'll get your data recovered — otherwise, the ransomware attackers would never be in business if they never gave you the keys to decrypt everything. But what they don't tell you is that that doesn't mean it's going to work quickly. You're still going to be living in the pain. It also doesn't tell you about phase two of the attack, where they take all that data that they've had access to, and they now exfiltrate that data and sell it on the black and the gray market, compromising your personal information.

So, proactive — this is going to be where we're able to recover faster. We've already planned for what's going to happen, so our backups are immutable. Nothing's able to be touched; nothing's able to be

impacted. We're actively scanning the data, looking for the threats, and when they happen — when changes happen, because they're inevitable — we give you an ability to automate that recovery. You get an ability to scan the data, look for the IOCs — that's the incident of compromise — and you're able to identify what hit you, what you're impacted by, what it's touched, isolate it, and then recover really, really quickly. Now, this philosophy is built on three different pillars. So as we move forward, you're going to see the three pillars of proactive resilience.

Pillar 1 — Protect: Backups Attackers Cannot Touch

In pillar one, we're going to talk about protecting. We need backups that the attackers can't touch. That's the first thing that they're going to do, and I'll give you a real-life story — I'll change the names to protect the innocent. This was a very big company. They had a primary backup environment. They had a disaster recovery backup environment. They even went so far as to have a tertiary environment that they said was off network, and it was their fail-safe. They were compromised. Let's talk about how they got compromised.

First, they didn't have native immutability. It was a bit of a legacy system. They were doing a lot of snaps, a lot of replicating of volume groups, so they weren't immutable. And what happened is the attackers didn't start out by going after the production environment. They went after the DR environment first. They came in through the production front door and said, all right, we're going to leave all of this alone. They went to the DR site over the Network File System, or NFS, protocol between the sites. They got into the DR environment, and they compromised the data that was there. They infiltrated it, they compromised it, and they just sat and waited.

Well, what happened next? A little time goes by, and the customer's got to seed this third offsite copy. They seeded from their DR environment. They opened up the port tunnel that they had to go to this environment, and they replicated the corrupted data from the DR site to the tertiary site, thus corrupting that site's data. Finally, once that was done, the attackers came back up to the production environment and initiated their attack. The customer thought that they were fully protected. They said, we're going to go recover from DR. DR was compromised — again, that native immutability wasn't there. They thought that they had an air gap. They thought they had this tertiary copy offsite that they were going to be able to get to, and everything was going to be fine. But again, because of the access, because they didn't have an ability to lock down that data and it wasn't immutable, that tertiary copy was compromised.

So when they initiated the attack, the customer went to DR; that wasn't accessible. They then said, that's okay, we're going to go to our tertiary copy of data. They went there, and that data was compromised as well. Ultimately, this customer was using a legacy environment that didn't meet the core minimum requirements for protecting that data. As such, they were forced to pay the ransom and

deal with all kinds of fines. Since then, that customer has actually become a Rubrik customer, and they've been great since then.

Pillar 2 — Detect: Know the Blast Radius Before You Recover

The next step — we're going to talk about detection. You have to know the depth to which you have been impacted before you can begin to recover. Otherwise, you risk leaving a breadcrumb trail for the ransomware to re-impact your environment. So what does that mean? All right, we've got to be able to detect anomalies when they happen. We've got to be able to understand what data was actually impacted and where that data lives. Finally, we've got to be able to identify a clean recovery point. And then we've got to be able to actually quarantine the impacted systems and backups so that we don't reinfect ourselves during a recovery.

Now, these are wonderful features that you get with Rubrik, because we are built on this foundation of zero trust, where we can come in and, by default, using some of our Enterprise Edition features, you're able to detect the anomalies. We're doing it at the core level — at a file level, at a hash level of the file. Finally, because we have all of this data and we correlate and look at all that metadata, we can identify that blast radius immediately. It gives us the ability to automate recovery, to orchestrate it. It's going to make your life a lot easier, because things that used to take 21 to 45 days get broken down into a matter of hours. But these are going to be table stakes that you have to think about when you're hit with a ransomware attack — and you 100% will be impacted. It's no longer a question of if; it's when.

The thing that we're seeing is that a lot of customers have that legacy approach where it's the castle and the moat. It's called perimeter detection, perimeter protection: we're going to guard against everything coming in. The problem with that is, as soon as something gets in, it's got full access to everything. Rubrik's a little different. We have a zero-trust methodology. We don't trust anything, including ourselves; we validate, cross-validate, and then, to make it even better, all of the backups on the Rubrik appliance, once they're written, become read-only. Nothing can ever be written and modified by ransomware. That's actually the secret sauce.

Pillar 3 — Recover: Services Back Online in Hours, Not Weeks

Now, let's go a little bit deeper and talk about when we're in here recovering your environment and how we do that — how we help you take it back to hours, not weeks. The biggest thing I want everyone to be aware of: identity is the most critical piece, the most important piece in your recovery. So what does identity mean? Active Directory. Entra ID. If those are down, nothing's going to authenticate; you're dead in the water. It has to be the first thing that we recover.

Now, interestingly, I used to be an IT director for an investment firm, long before ransomware was as prevalent as it is today, and we had to recover our Active Directory domain one time. We did an Active

Directory migration. There is about a 300-page document for recovering your Active Directory if it goes down. It is a very manual process, and if you miss one step — congratulations, you have to start over. Now, a lot of people today are using Microsoft 365, or M365, for their mailboxes. If you're doing that, you're authenticating into M365 via your Entra ID. If you're federated and using it at work, where you can access it on your network with your domain credentials, your Active Directory is 100% linked to that Entra ID. So it's really important that you know, if that goes down, you have to recover both. So many people don't have a plan for that. The big thing is, if you have to recover that Active Directory from scratch, be ready to read a 350-page document that's going to take you weeks to get through. And if you don't get through it correctly, you're going to have all kinds of time sync issues, authentication issues, and loss of data. So that's a very manual process.

The beautiful thing with Rubrik, with the application recovery, is there are no manual steps. It's all automated. So when we talk about three ways to recover your Active Directory, think of it largely like the manual process; essentially a point-in-time snapshot recovery — think of trying to do a snapshot from a virtual machine, or VM; or think about using a service that's already got all of that metadata, has already looked at it, and it's just an instant recovery. It's an on-demand restore. And that's what you'll see in that last column: native M365 protection. It's not going to really give you the recovery, but our on-demand and immediate ability to recover that is.

So, a really important takeaway before we move to the next slide. The big thing that I want you to get from that is that Microsoft is a shared services model. They will give you the infrastructure to run, but it's your job to configure it. That's something that a lot of people take for granted, and they don't realize it because it's always there. The problem is, in a ransomware attack — which we're all going to face — that's what they take away. They take away your ability to actually be able to recover. So Microsoft will give you all of the data and give you all of the accessibility to it, but what they won't give you is a recovery of your Entra ID environment.

Organizations Like Yours Are Protecting Citizens Today

So, let's talk about organizations that are very similar to you that are getting protected today. The LA County Registrar: from the time we did a proof of concept, or POC, with them to full implementation was two days. Sensitive data discovery — they thought that they were good. They thought they didn't have any exposures. Two hundred ten million records of their citizens were found. Now, sensitive data could be Social Security numbers, credit cards, any personally identifiable information, or PII, data. That's going to be what we found. The City of Winter Park is out in Florida — a local government with about 30,000 to 35,000 residents. Florida law actually will not allow anybody to pay the ransom. The big thing that they got from us is that we protected their VMware environment, and it didn't matter where

that VM was. It was unified between their on-prem and their cloud. So it didn't matter where the data is; because you're using Rubrik, that data's going to be secured.

All right, as we move on and talk about something a little bit larger — I wanted to show you guys something that scaled, because that's one of the things that we often get asked: well, how does this scale? Now, I had to go a little further away to get it, but let's look at their highway authority. There are 1.9 million vehicles on that road every day. We saved them a ton of money over using the native tools — 16%, in fact — and when you look at an operating budget of 70 million in weekly revenue, we protected that budget and saved them more money on top of it. When you're dealing with figures that are that large, a 16% total cost of ownership savings is substantial. The beauty of that is that money can go back toward other projects that help your citizens, or that help the division that you work with actually be able to pivot. So again, I wanted to show you a couple of options here for different places. We went from the West Coast over to the East Coast, and then I wanted to give you an example of something that was really, really large and had a ton of volume, so we went all the way outside of the US just so I could show you something at big scale.

What Recovery Readiness Looks Like

As we go through, let's talk about preparing for recovery, what that actually looks like, and what it entails. There's a little bit of a checklist here, and I'm not going to read them all to you, but what I do want to do is talk through the plan and the why of these. Again, it's changing the methodology, changing the mindset, and in some cases changing the tools. With that mindset shift, we need backups that are immutable. We need to talk about logical air gapping. This one confuses a lot of people; they're thinking physical air gaps — that was the example I gave you earlier. Well, why is logical any better? Logical's better because you have the ability to control it inside of an environment that can scale. That's really the big difference of why that's better for you guys.

Identity infrastructure — it's got to have its own recovery plan. We're going to talk about a concept called the minimum viable state, or your minimum viable applications. Your identity is your absolute most critical tier-zero application. Without it, you can't get on a Teams call. You often can't authenticate to get your mail, or sometimes to access your home drives if they're on the cloud. We also want to talk about the scale — protecting beyond native. Obviously, M365 and most software platforms are a shared service model. Some of them do give you a little bit of backup protection; the native requirements are very, very low for those. In fact, I encourage you to actually ask them what the native recovery is. Nine out of ten times, they will tell you that, yeah, we're not going to make sure your data's there when you need it. We're going to give you a minimum standard that we see a lot of people use. The one thing I would tell you is that ransomware doesn't care about the minimum standards. They care about just

getting to that data, getting access to it, and then manipulating it to get money from you and your citizens.

All right, recovery. It has to be tested on a regular basis. There's this thing that Netflix does as a company. They run a program, and all it does is run in production and try to go break things. That's how Netflix tests their recoverability and tests their resiliency: they're constantly trying to break something. Now, we can't do that at scale; we can't do that for a lot of our institutions. So what we can do, then, is test, and test thoroughly. A lot of legacy companies — I used to do this years upon years ago — would test a subset of what we thought the critical applications were. We might spin up a single webpage to make sure that our DNS switched over, to make sure that it functioned. What I'm telling you and encouraging you all to do is a deep, deep test — a true test to make sure that everything comes back up, with the interdependencies between all of the different apps.

Next, we're going to talk about sensitive data. Sensitive data's got to be classified. You've got to be able to track it in your organization. If you can't do that, you have no idea where the data is going or who has access to it — or if there's shadow IT, if a local user is trying to save down a spreadsheet to make their work faster and they forget, and they save a copy locally on the machine, and now you've got sensitive data that's on someone's machine. If you don't have the ability to see that that data has moved around, that is a big risk for you guys.

All right, threat detection. It's got to run against your backup data. You've got to know what's happening. You've got to be able to see inside of those backups and understand if a file's been changed, modified, or even deleted, so that you can take action. This is going to affect your recovery time objectives, or RTOs, and with Rubrik, the beautiful thing is we take those RTOs from weeks and we put them into hours. You're able to recover incredibly quickly.

Your Mission Is to Serve Citizens

So, that being said — this is my last slide we're going to talk about. If your mission is to serve the citizens that you work with, Rubrik's job is to help you make sure that you can serve those citizens. Proactive cyber resilience is not a nice-to-have. It's actually critical for everything that you're going to do. Now, one of the things that we're going to talk about here is that a lot of people that we work with, a lot of people that we interact with, don't necessarily have funding to make this happen. It can be expensive. The number one thing I hear is, this is critical, I completely agree, I need help trying to figure out how to pay for it. Well, that's why we're here today. So we're going to talk, in the next slide — and I'm going to hand it back over — about how you guys can fund the cybersecurity initiatives. That being said, I just want to take a minute to thank you all for the few moments that you had to listen to me. I'll be in the chat if anyone has any questions they want to discuss. Thank you, guys.

Michael Paddock:

Thanks, Jason. And we'll turn it over to Dr. Liz Shay to take it over from here.

Grantseeking for Cybersecurity

Cybersecurity as Part of a Larger Mission-Driven Project

Dr. Liz Shay:

Thanks, Michael, and thank you, everyone. Today, as Jason said, we want to talk a little bit about how cybersecurity can be funded. To start out with, if you've ever tried to search grants for cybersecurity, you might notice that there are relatively few options available, and they usually are pretty strict in a lot of requirements. We're going to talk about the ones that are coming up, but the vast majority of grant funding that is out there is not designed expressly to fund technology, including cybersecurity. Rather, grant opportunities are funded to support mission-driven activities, and the grantmakers are happy to fund technology as part of those larger, comprehensive, mission-driven projects.

So when you're thinking about your cybersecurity needs, think about them in the broader context of your organization. What are you actually enabling through cybersecurity, as well as other technical and non-technical components? Think in the broader context of things like career readiness or professional development, community outreach, campus safety or public safety, transit infrastructure. You're working within that broader context as an organization, so think about cybersecurity as a piece of that bigger picture. When you start to think about this bigger context, it opens up a lot more grant funding opportunities for you, where you will be able to work toward your cybersecurity needs but also toward those broader mission-driven initiatives that your organization is working on.

How to Know if a Grant Is Cyber-Friendly

When we're looking at specific grant programs, more generally, what we're really looking for is: Is a grant cyber-friendly? There are a lot of different ways that we're thinking about this, and here are some recommendations on things that you can be thinking about. First off, the guidance might give you a list of allowable and unallowable costs and eligible activities. We're going to talk about a grant program coming up that lists cybersecurity specifically as an allowable cost inside a larger context. You can also look at things like priority areas. Are there competitive preference priority points, or other kinds of things happening in the priorities or scoring rubric, that lean toward considering cybersecurity as part of a larger comprehensive project? For example, you're really looking at connectivity for distance learning, but cybersecurity plays an important part of that picture to make sure that student data is kept private.

Also look at what's been funded previously. How are you similar, but also a little bit different, from what has already been funded, and how are you aligned with those same kinds of initiatives? And then finally, if you're still unsure, you can always contact the program manager and ask some specific questions. Just make sure you do your homework beforehand. They definitely want to know that you've put in the work to read what they already have available. All of this being said, this is one way to help work toward it. We're going to talk about the Rubrik Grants Support Program coming up, and that also will be able to help you work toward understanding the grants that are cyber-friendly.

Questions for Consideration

To start thinking about some kinds of things that you really should be considering as you are looking at your cybersecurity project within this larger comprehensive context: it's really important to make sure that you are considering allowable costs when you pick a specific grant, as we mentioned, and whether the grant properly aligns with those technology needs. But you also want to think about some other important components of your project. Are there budget limitations on the maximum IT costs that can be included in a particular grant program? And will the grant be able to cover the full cost of an implementation for whatever you're doing? And then finally, are you ready to implement the efforts within the grant's timeline? They often put specific timelines in place for when you can do specific activities. And can you afford to maintain the solution once the grant period ends? That sustainability aspect is very important.

So think about all of these questions as you start to think about your cybersecurity projects within the broader context, and also know that we're going to be returning to these questions when you have conversations as part of the Rubrik Grants Support Program, to make sure that everything is aligned as you're working through grantseeking for your cybersecurity efforts. This is a very high-level overview of how cybersecurity fits into the grant funding landscape, but we're now going to move into looking specifically at what grant programs are out there and what the specific grant funding landscape looks like. For that, I'm going to pass things over to Shannon.

Cybersecurity Funding Opportunities

Sources of Grant Funding

Shannon Day:

Thank you, Liz, and thank you, everyone, for joining us. As Liz mentioned, we're going to start to drill down even further. First, we want to look at where grant funding lives. In the United States, grant funding is divided into three major buckets. At the top, we have federal agencies, which offer over $700 billion annually. They really provide the maximum scale, but they also carry the highest compliance and

highest reporting burdens, and they're usually the most competitive. Below that, we have state agencies, which contribute over $100 billion annually. These are critical because states frequently act as pass-throughs for federal funding, but they also often administer state funding programs. And then finally, we have private funding from family, community, and corporate foundations. This totals right around $70 billion annually. These foundations rarely fund heavy municipal infrastructure like cybersecurity, but they are highly agile, and they can be a source for workforce development, training, or educational programs that may have those cybersecurity components.

Federal Sources of Funding

Because the federal bucket is so large, there are 26 grantmaking agencies at the federal level. Many assume that cybersecurity grants only live within homeland security — plus, that's the one we've heard of, which I'm going to touch on very briefly in a minute. But as you see from many of these seals — spanning education, labor, energy, justice, transportation — cybersecurity is pretty much institutionalized. If you're a school district securing student data, you're going to look to the Department of Education. If you're a municipal utility managing a smart grid, that's going to look like the Department of Energy, maybe the Department of Transportation. And of course, if you're a police department expanding your forensics lab, you're going to be looking at the Department of Justice, or DOJ, primarily. The secret to a successful strategy isn't hunting around and, like Liz said, typing in "grants for cybersecurity." It's finding the specific agency that views your cyber vulnerability as a risk to their core mission. So aligning your priorities is key. Similar state agencies are also an excellent resource. A lot of them have the same names, but at the state level.

State and Local Cybersecurity Grant Program (SLCGP)

As I mentioned, we're going to talk briefly about the big boy. Many of you in the field have probably heard of this one. It's the State and Local Cybersecurity Grant Program, or SLCGP. This was established as a $1 billion program under the 2021 Bipartisan Infrastructure Law, and we are now at a crossroads. The original funding sunset last year, though many states are still retroactively administering their allocations, so don't be confused if you are still seeing state deadlines opening. Right now, CISA — the Cybersecurity and Infrastructure Security Agency — is evaluating the success of the program. But there is also a major push from the public sector for more formal reauthorization. We are still waiting, but the House passed the PILLAR Act late last year, early this year, to extend the program for ten years, and a companion bill is pending in the Senate. That one is a little bit shorter.

But again, we're still waiting. And then just last month, in June, a joint coalition, including the National League of Cities, the Conference of Mayors, et cetera, urged the Senate to appropriate $300 million for next year, fiscal year 2027, to avoid that funding cliff when the funding does dry up.

Embedding Cybersecurity in Non-Cyber Grants

So how do we embed cybersecurity into non-cyber, quote unquote, grants? You look for technology-related infrastructure funding, thinking back to that slide that Liz had up. Many public sector grants support cybersecurity if it's baked into a broader tech deployment. For utilities, high-risk targets like water and electricity can leverage Department of Energy and Environmental Protection Agency, or EPA, infrastructure awards to modernize SCADA monitoring systems and prevent grid disruptions. Moving next to transportation: the Department of Transportation and the Federal Highway Administration fund projects to protect rail and bus networks. The ATTAIN grant, for instance — this is a big one. It focuses on smart transportation, advanced transit systems, vehicle-to-vehicle communication protections, and the like. And again, those all live on the network, so they all need to be secure.

And then finally, criminal justice. The justice system depends heavily on sensitive data sharing. DOJ funds things like 911 center upgrades, body-worn camera implementations, smart traffic devices. One example is the Edward Byrne Memorial Justice Assistance Grant, or JAG. This is kind of the big one. This is the premier vehicle for anything in the criminal justice space.

Homeland Security Grant Programs

And then we have homeland security grants. This is where SLCGP lives, but the broader Homeland Security Grant Programs represent a massive, reliable stream of funding. This ecosystem focuses on five core missions. These don't change. They are prevention, protection, mitigation, response, and recovery. Looking closely at the national priority areas — these were the same in 2025 as well — right alongside protecting soft targets and countering terrorism, you will see a dedicated directive: cybersecurity resiliency. So baking a robust cyber defense element into any of these applications makes it more competitive, whether you're applying for the Homeland Security Grant, the Tribal Homeland Security Grant, the Nonprofit Security Grant — which Liz will touch on in a moment — Port Security; I can go on and on. Really, cybersecurity is going to be the through line through those various programs.

Example Funded Project: Law Enforcement JAG

And finally, I want to again talk about JAG a bit — a case study — before I pass you back to Liz. Let us look at the success story. This was a municipal police department that we worked with. I will not name them. They needed to secure their data across the entire justice information sharing continuum, because, again, that information is potentially traveling through the cloud from the police vehicle all the way through the court system. And then they also needed to procure rugged laptops for field use. So their JAG proposal combined those two things. The project won funding because it directly maintained Criminal Justice Information Services, or CJIS, compliance and kept officers securely connected in the field, so they could move out of the back office. They didn't have to return to the office to write their

reports; they could do it right in their vehicle, and they could be available to their community members so they could better serve the community. And with that, I am going to pass things back to Liz again.

Example Funded Project: Education NSGP

Dr. Liz Shay:

Thanks, Shannon. As another example, looking at the education side of the house, the Nonprofit Security Grant Program is a very popular program to support cybersecurity-rich initiatives happening for private K-12 and higher education entities. As an example, we worked with a private, nonprofit, religious K-12 school, and they needed to make sure that they were not at risk for cyber terrorism. It's something that is definitely a concern for them, given their religious nature, and they wanted to make sure that they could protect their student data and protect their faculty and staff data, to make sure that everything was safe and there were no risks associated with anyone attending the school. For this particular project, they also did a risk assessment on the physical security side of things and did come across needing some cameras and door access as well.

So as a whole, the well-rounded project considered both physical and cybersecurity to prevent these kinds of potential religious-based terroristic attacks. Now they're better prepared, and they can include all of those components in their grant application to meet these current gaps in their security and make sure that they're no longer able to be a target.

Distance Learning and Telemedicine Grant Program (DLT)

As we transition from the homeland security funding and move into the next section, this is the Distance Learning and Telemedicine Grant Program, or DLT. This particular grant program is the one that I mentioned earlier as being a grant that specifically calls out cybersecurity as an allowable cost. However, the purpose of the grant is not cybersecurity. The goal of this particular grant program is to expand educational opportunities and health care services out to rural Americans, and it supports this programming through the use of a variety of different technologies. So there is audiovisual, or AV, and teleconferencing included, networking, cybersecurity — all of these things are critical to these kinds of projects. For this particular program, when I say rural, I really mean communities of under 20,000, but often we see these kinds of projects led by urban institutions — either institutes of higher education or health care services — to be able to provide their services out to these rural Americans.

This program had a deadline just a couple of weeks ago, so now is a really good time to start thinking about the next cycle. Are you working on a distance learning or telemedicine project that impacts rural Americans? That's definitely a good thing to be thinking about, and to get engaged with the Rubrik Grants Support Program to talk about it some more.

Example Funded Project: Education

For this program, as an example of a project — we have this kind of conversation quite a bit — this is with an urban institute of higher education, in this case a university, and they wanted to be able to provide real-time dual enrollment courses for high schools and colleges in rural spaces. So they were able to provide some of those specialty courses that otherwise could not be taught out in these rural spaces — things like calculus, some advanced science, those kinds of courses that the students wanted to take but that it is not sustainable to hold an entire class for out in those rural areas. Their particular project included AV and teleconferencing technology for the classrooms at all the locations. They also included some networking for the rural locations so that they would have sufficient bandwidth to be able to receive these real-time educational experiences.

And then finally, they included cybersecurity to protect all of that project equipment and all those connections, to make sure that it was a secure connection and that the students could participate safely and actively in this particular set of coursework. So with that, now you have a sense of some of the kinds of things going on in the federal space. I'm going to pass things back to Shannon to talk about state funding.

Examples of State Funding

Shannon Day:

Thank you, Liz. We're playing ping-pong. So, state funding. Again, I mentioned it earlier that it is the second main source of grant funding. On the left, you'll see a snapshot of state-funded grants. These are just examples; obviously, I can't cover all of your states. But Florida, for example, does run its own cybersecurity grant in addition to the federal SLCGP program. We are seeing more states doing this. They planned for that federal funding to sunset, so we are seeing states start to pick up the slack. So make sure you keep an eye on your state. And as we've discussed, you don't want to stop at just cyber funding. First, you can start with your Department of Justice. I put links on the right of your screen to find out those administering agencies. These are the agencies that administer pass-through funding through the Department of Justice — JAG is an example — and through the Department of Homeland Security — the State Homeland Security Grant Program or SLCGP are examples. This is a place to get you started.

Finally, I want you to think creatively, because there will be other state agencies, and you don't want to miss out. If, again, you just look for the keyword "cybersecurity," you may only come up with old results, inaccurate results, et cetera. So consider other state agencies whose priorities align with your organization's, like Departments of Commerce, Departments of Transportation, Education, et cetera.

Example Funded Project: New York Local Government Efficiency Program

And I want to talk about another project description: the New York Local Government Efficiency Program. On paper, this program exists to develop cost-saving, shared regional service delivery. It's an efficiency and consolidation grant, not an IT security grant, so it will not show up on your radar if you're just looking for cybersecurity grants. But a smart applicant successfully requested funding for technology upgrades by tying robust cybersecurity integrations directly into protecting a shared, multi-jurisdictional water and wastewater management system. By framing cybersecurity as the essential backbone of a critical shared regional utility, they checked the boxes the state was looking for, and they got their project funded. This is how you transform a standard tech request into a winning, holistic proposal.

Writing a Compelling Narrative

How to Pick a Grant: Start with the Project

And again, winning grants requires shifting our mindset a little bit, away from what we want to buy and toward what the funder wants to achieve. So over the next few minutes, we're going to look at the strategic framework you need to adopt to pick the right grant, align your mission, and organize your internal documentation. First up, we want to ask ourselves these three questions. What are your precise technology needs? Be granular. Are you securing endpoint devices or deploying immutable data backups? Identify the exact technical gap. Don't be vague. Next, what mission-driven activities does this enable? Funders don't fund software licenses; they fund outcomes. Does this keep dispatch lines live during an incident? Does it ensure public utility records remain tamper-proof? Focus entirely on the human and operational capabilities.

And now, finally, how do you align your mission with the funder's? Every grant has a legislative intent. Whether it's federal, state, or foundation, they all have an intent behind them. Your job is to build the bridge between your local project outcomes and their macro-level goals. And sometimes you are going to be hammering that square peg into the round hole, and it is not going to fit. That's when it's time to move on and look for another grant.

Gather Existing Documents: Operational Readiness

Let's talk about operational readiness. As Liz said, DLT just closed, so now is a great time to start thinking about these components. You can gather these at any time. Grant application windows are notoriously short — generally 30 to 45 days, sometimes 60 days if you're lucky. If you wait until an announcement to gather all these components, you're not going to be successful, and you're going to stress yourself out. So first, on the upper left of your screen, we have financial documents. Gather your operating budgets for the past three to five years, your formal audited financial statements, vendor quotes —

those are going to be needed for your budget — and a list of current or pending funding sources, because, again, the funder wants to know not only how you have funded this project up until now, but how you will sustain it after the grant has expired. Next, upper right, we have your description: your formal mission statement, your vision, your value statements. Have them ready, on company letterhead or organization letterhead. Also an org chart; that is often required as part of a grant application.

Next, on the lower left, we have your designation. Are you a 501(c)(3)? If so, you want your nonprofit designation letter. Are you a company or municipality? You want your Employer Identification Number, or EIN, or your other active registrations, your business registration numbers. Also, you want to register in grant portals. Do you have your System for Award Management, or SAM, registration? Do you have your Grants.gov registration? And then finally, over to the right, these "as required" materials. These are things that aren't necessarily required for every grant application, but they are required for a lot, so it is better to have them and not need them than to need them and not have them, because these often take the longest to secure. Anything working with partners is going to take a longer time. Getting memoranda of understanding, or MOUs, letters of support, or resumes for key project personnel — you want to have those now, because they don't necessarily expire.

So you want to have them now; you want to have those stakeholders involved in the project now. So, again, when the grant application opens, you are not running around in a fire drill. And again, I will pass things back over to Liz to take us home.

Project-Specific Pieces

Dr. Liz Shay:

Thanks, Shannon. Now that we have the information that you need for any grant application, we want to talk about the information that you need for a specific grant application. Once you've started putting together your specific project and the specific grant that you're aiming for, you're going to need a bit of information. First off, you're going to need a need statement. This is going to be related to your mission and also related to where you currently have gaps that you're seeing. Oftentimes, this is going to include more details than just something like "we need cybersecurity." It's more going to be about "we want to ensure connectivity for rural Americans to educational experiences," giving a lot of detail on that kind of front.

You're also going to want to have a description of your activities, your goals, and your objectives. These are all going to be related to one another, but basically, it gives you a description of what you're going to do, why you're going to do it, and what the impact of those activities is. And then finally, you're going to need data. This is going to be data that relates to identifying the gaps that you're currently seeing, and also data that relates to your goals and outcomes and being able to measure the success of your project. Right now, the more data, the better, and you can always cut things out as you prepare a specific

application, but make sure that you have all the information that you're going to need as you start to put pen to paper.

Draft Your Story

When you draft your story, the components that we've talked about up until now give you all of the key details, but you want to also make sure that you're answering the key questions about your project. First of all, who is your organization, and why is it best positioned to be able to address the particular need that you have identified? You also want to think about what this project will require in terms of the equipment, the personnel, and the planning — so cybersecurity will be a piece of that, but what are the other components that come into play? And then you also want to think about where it's going to take place; it could be more than one place, in that sense. When will your project occur, and how long is it going to take to complete, in alignment with the specifics of a particular grant program on that kind of timeline? You want to be able to say why this project is the best option to solve the problem that you have identified, for the reviewers.

And then think about how this project will fit within the context of your community's needs, and the related question: How does this fit within the context of the grantmaker's goals? So make sure that you can answer all of these questions as you're starting to prepare your application plans.

Major Budget Components

As you move into even more levels of detail, you're going to have several major budget components, and you want to make sure that you have considered all of these things and their applicability for your particular project. First off are going to be things related to people. So you might have salaries, fringe benefits, or contractors involved for implementation, or things like that. You're also going to have some things, meaning equipment — so that's more expensive, longer-use pieces of technology or other items that you might need — and then materials and supplies. These are smaller, shorter-lifespan kinds of things, such as paper and pens. And then think about the facilities that you're going to be using and make sure that those are available and ready.

Then you may have some other categories as well. This is things like travel, if you're going to need to go someplace to be able to talk about the work that you're doing, be trained on the work that you will be doing, or something along those lines. You might have some subcontracts that come into play with organizations you're collaborating with, in the case of partners, or with entities who will be helping you in other ways. And then your indirect costs — your kind of management, administration, facilities types of costs, more generally, for your organization. Typically, these come into play the most in the federal space, but some other grantmakers also allow them on your particular project.

The Importance of Alignment

And then finally, as you're thinking about all of your project components, make sure that everything aligns very clearly. Your project narrative — that's answering all those who, what, when, where, why, and how kinds of questions that describe your project with your activities, goals, and objectives — make sure that that is aligned with your budget. Make sure that the expenses make perfect sense for the things that you're actually going to be doing. And then make sure that your budget justification, which is a narrative component that describes all of the pieces in your budget, also aligns very carefully with this. You explain everything that's in your budget, and you explain how everything in your budget aligns with your activities, goals, and outcomes. All of these pieces must play very well together, and definitely an important component of that is making sure that you have outside sets of eyes to make sure that all of these collaborations are happening and all of this alignment is happening. So with that, I'm going to hand things off to Felix to talk about the Rubrik Grants Support Program.

Rubrik Grants Support Program

Felix Alvarez:

Thank you, Liz. First, I want to thank Jason for walking us through what true cyber resilience looks like before, during, and after a cyber event. Thank you to Grants Office. They just covered an incredible amount of valuable and important information on grant funding opportunities, project alignment, and building competitive grant applications. They've shown us that there are more funding opportunities available than most organizations realize. What we at Rubrik have seen is that the challenge isn't that funding doesn't exist. The challenge is having those dedicated resources who can research grants, match projects to funding opportunities, interpret eligibility requirements, and assist with grant applications.

If you're like most organizations listening today, you're probably thinking, okay, this was great information, but where do we even begin? We don't have the time, resources, or bandwidth to truly navigate the grants review and application process. Or, yes, we definitely have a grants team available within our organization, but we're dealing with competing interests, so they're also helping the food service people, the facilities people, everything else. That's exactly why Rubrik invested in creating something different: a value-add grant support program that's no cost, no obligation to existing, new, or possible future customers. We wanted to remove as much of that burden as possible.

Pillar 1: Funder Prospecting Research

Our first pillar of this grant support program falls under funder prospecting. Maybe you already know you need cyber resilience. You know your backups need modernization; maybe you're looking at protecting M365, or recovering Active Directory, or improving ransomware recovery, but you don't

know what grants might align, or even where to start. That's where we begin and work with you through the first step of the grant support program. This first step is to connect you with grants consultants within Grants Office who are experts and understand cybersecurity projects and grants that align with those projects, and they will help research funding opportunities that specifically align to your technology needs.

Pillar 2: Project Development Consultation

The next pillar is project development consultation. Jason talked about protecting public services before, during, and after a cyber event. We know that grants don't fund technology; they fund outcomes. That's why this next step is so important and critical to assisting you in navigating this complex process. Our consultants, who are now your dedicated resource, help translate your cybersecurity initiative into the type of mission-focused project that grant funders are looking at. For example, Liz and the team talked about many of the other projects that kind of align, but examples of these projects center around operational resilience, continuity of services, protection of citizen services, disaster recovery, critical infrastructure protection — the list goes on and on and on.

Pillar 3: Proposal Review and Editing Support

And then finally, we get to pillar three, and that is proposal review and editing support. Once you've identified the right grant opportunity by working with your individual resource at Grants Office — again, that's free, no cost, no obligation — once you've identified that right grant opportunity, you're not left on your own. Whether your team simply wants another set of expert eyes reviewing a proposal or help providing suggested edits, our team is there to increase your chances of submitting the strongest application possible.

What I love personally about this program is that I come from the public sector; I spent 20 years on that side of the house. This is a comprehensive and value-added grant support program with no obligation, no cost, nothing for you to sign to go through the process, no terms and conditions for the program. We want to help public sector organizations navigate what can often be a very complex process. In closing, Jason challenged us today to think differently about cyber resilience. Grants Office showed us that funding may already exist for many of those projects. What Rubrik is trying to do is bridge the gap between those two conversations, because protecting your community shouldn't be limited by not knowing where to find funding or where to begin, or not having the resources to pursue it. If today's discussion sparked an idea for a cybersecurity initiative you're trying to fund, we at Rubrik and Grants Office would love the opportunity to help you navigate that. Thank you, everyone, for joining us today, and I'll pass it back off to Michael.

Q&A Session

Michael Paddock:

Thanks, Felix, and what a great call to action that was. Thanks to all of our speakers — really great information today. Okay, we have just a couple of minutes for a couple of quick questions.

Audience Questions

Q1: I'm in IT, and many grants seem to require non-IT involvement. Who should I talk with at my organization to make progress?

Michael Paddock:

I want to start with Liz. The first question is: I'm in IT, and it seems like a lot of grants are going to require non-IT involvement. Who should I talk with at my organization to make progress on this?

Dr. Liz Shay:

Great question. It definitely is going to require a team effort at any organization to be able to pursue these kinds of grant opportunities, but it's also that great opportunity to further your mission-driven activities along with your technology needs. The best people to talk to — start out with those that you already have a good relationship with, but also think about the folks who handle finance, who are in charge of your mission-driven activities. In the education space, for example, we see a lot of curriculum development specialists or leads for particular grades or departments at colleges. Those are the kinds of folks that tend to be involved in grantseeking already for non-technology initiatives, so being able to collaborate with them to broaden the scope of what's being considered is a really good opportunity.

Q2: How should people get started with the Rubrik Grants Support Program?

Michael Paddock:

Great, thanks. And then one for Felix. You mentioned the Rubrik Grants Support Program. I just want to clarify: How should people get started with that? Is there an email?

Felix Alvarez:

Appreciate it. You can reach out to me at my email, felix.alvarez@rubrik.com, but be assured we're going to be following up with everybody with our website link and with a PDF flyer, so you'll get a follow-up as part of this conversation, and we'll make sure to follow up with you as well.

Closing

Michael Paddock:

Fantastic. Thank you so much. Thank you to our presenters — Felix Alvarez, who we just heard from, Jason Likens, Dr. Liz Shay, and Shannon Day — for sharing a ton of great information and insights with us today, and thanks to all of you for your participation in today's session. I hope you found this a valuable use of your time, and we'll see you next time on a future Grantscast. Have a great day, everybody.

— End of Transcript —

Grants Office, LLC • empowering communities • Recorded July 9, 2026

About This Transcript

This transcript was generated using Webex's automatic caption feature and subsequently reformatted with the assistance of artificial intelligence. While we make every effort to ensure accuracy, errors may remain. If you notice a discrepancy, we welcome your corrections — please reach out to education@grantsoffice.com.

Live sign language interpretation is available upon request for future Grantscast® events. To request an interpreter or learn more about accessibility accommodations, please contact accessibility@grantsoffice.com.