CUSTOMER Q + A

ST. LUKE'S HEALTH SYSTEM

St Luke's Health System unites mission-critical data and boosts organizational efficiency with RSA Archer

AT-A-GLANCE

Challenges

- St Luke's holds large volumes of data about its IT environment, much of it in the form of lists, which are saved across disparate systems
- It regularly carries out risk assessments but had no easy way of tracking findings and saving results
- It needed to centralise all its data to make it easier for business users to access and mine for insights

Results

- The frustration and inefficiency of chasing data has been eliminated. Users can now make fast business decisions, based on the latest information
- RSA Archer's flexibility means the IT team can experiment with different usage models, easily adapting and optimizing them to ensure the best possible fit with the organization's needs

"RSA Archer has helped us evolve from an organization where we're constantly trying to chase data and information and the resulting frustration and inefficiency that stems from that. Now we have a source of record where employees can access data and more quickly consume it and make decisions based on it."

REID STEPHAN, DIRECTOR OF IT SECURITY, ST LUKE'S HEALTH SYSTEM

St Luke's

RSA

As the only Idaho-based, not-for-profit health system, St. Luke's Health System is a vital part of the community, with local physicians and boards committed to furthering the organization's mission "to improve the health of people in our region." Each St. Luke's Health System hospital is nationally recognized for excellence in patient care, with prestigious awards and designations reflecting the exceptional care that is synonymous with the St. Luke's name.

Please tell us about yourself and your organization

Reid Stephan (RS): I'm Reid Stephan, I'm the director of IT security for St. Luke's Health System. We are the state's largest private employer and Idaho's only not-for-profit health system.

Dustin Aldrich (DA): My name's Dustin Aldrich, I'm an IT security analyst at St. Luke's.

What GRC challenges were you facing?

RS: At St. Luke's we love lists. When I got here we had lists of servers, end-point devices, applications and locations. They all lived in different spreadsheets on different shared drives and we have some SharePoint here as well, but there was nothing that tied them all together at a high level and let people draw points of connection.

DA: In the past we have done a lot of risk assessments in IT, in fact we would have one every couple of years. We would do the assessment, we would get the results, we would talk about it for a little bit and it would end up being saved in a Word document on some shared drive somewhere.

How have you addressed these challenges?

RS: We've implemented the RSA Archer GRC tool. We've used the Enterprise Management module to help us to import all the disparate data from our many lists and centralize it, so that users can make logical connections.

We're currently in the process of deploying the Policy module as well. Our current environment is such that if we're asked to respond to the question of our HIPAA compliance posture it's really more of a qualitative kind of a gut feeling response. There's some validity to that but it's hard to defend and it's hard to benchmark and track progress against. With the Policy module we can establish our control objectives, set tests for those objectives, and send out questionnaires to have the owners of the different controls actually self audit. This then lets us attach a quantifiable measurement to our compliance. So we can take a particular service line and produce a percentage of HIPAA compliance and then also provide a gap analysis of what's remaining, to get them fully compliant with the HIPAA rule.

DA: We've also used the Risk Management module of Archer to run a risk assessment. We loaded it into the tool and generated a risk register, with a list of problems that rolled up into those risks. Then we were able to take each of those problems, assign them to an owner and say 'Are we going to mitigate them or are we going to accept them?'

What results have you achieved with RSA Archer?

RS: I think one of the most positive outcomes of using RSA Archer is that it's helped us to evolve from an organization or an environment where we're constantly trying to chase data and information and the resulting frustration and inefficiency that stems from that. Now we have a source of record where employees can go to access data and more quickly consume it and make decisions based on it. So it's not only improved efficiency, but it's also really helped to improve morale. It's eliminated a lot of frustration and finger pointing that had occurred in the past when you had single points of failure with a custodian who owned a single piece of data that wasn't widely available to the entire organization.

I think one of the advantages that we experience from RSA Archer is its flexibility. We can try things and experiment and go down a path a way, and if we find that it's not quite working the way we thought it's very easy for us to back out, to course-correct on the fly with really very little resource cost or impact. I think that helps us from an internal organizational perspective of trying to be the best we can, to deliver the best patient care, to make the best use of our resources and to really adapt and adjust to shifting market demands and changes.

DA: It's eliminated bottlenecks. It has enabled us to get access to information where before we had to find out where the information was. We had to reach out to the person and we had to communicate back and forth through emails, and now it's more of a self-service model. They know where the information they need is, they can log right into it, get their information and move on, and there's no question about 'Is this current? Is this accurate?'

One use case we have is our application list. Prior to implementing RSA Archer we would have one individual who was responsible for updating and sharing that information. That process was very inefficient because he was doing other things, and it would take

sometimes days to get information back as a result of that. Now we are able to get that information to those people immediately. There is no administrative burden associated with it and those people can now spend that time focusing on other more efficient activities and effective uses of those resources.

How does Archer help you meet your compliance goals?

HIPAA is really the regulatory requirement that we have to attest to. HIPAA does not give a lot of detail as to what IT security needs to do. It just makes general statements like 'Protect your information'. We can go to a framework that is a lot more prescriptive and gives us a lot more detail on how we can really accomplish that task, such as NIST. Archer enables us to map those two together, so whenever we attest to NIST we can also simultaneously attest to HIPAA.

What impact has the project had on your organization?

RS: I was at a meeting last week with our CIO and he made the comment that a year ago when we started our journey to stand up a risk management program, it was a topic that he felt he was responsible for but it wasn't exciting for him. But he said in that meeting that now risk management is one of the things that he enjoys most about his job, that he's in Archer at least every other day and he enjoys being able to look at how we're progressing, where the trouble spots are, having that accountability to then go and have conversations with stakeholders as necessary, and it's one of his favourite parts of our security program.

RSA Archer has also given us the gift of perspective. It's allowed us to take a top-down or bottom-up perspective and show people how a system strategy or business objective is supported by an underlying risk management item. They can see how Archer and IT support what they want to accomplish for the health system. Conversely, you can take an IT employee who has an action plan and they can drill up and see how the work they're doing directly contributes to that business objective or to that system strategy. In the past that was kind of murky and it was hard for folks to understand how those points connected at times.

What advice would you give to others embarking on a similar project?

RS: One of the things that we learned as we've deployed the RSA Archer tool is that a great benefit for us was to take it in very digestible segments. We just deployed two modules initially, which allowed us time to establish a good foundation, and become very proficient in how we used those modules. It also gave us time to really be methodical in planning out our long-term strategy and approach, to fully round out our GRC solution and the pace and the order of the additional modules that we wanted to deploy.

DA: One of the lessons that I would impart to other users of the RSA Archer tool would be to really focus on getting those quick wins. The way you identify where those quick wins for your organization would be is by really thinking about where your pain points are, and when you identify where your pain points are and you focus on resolving those pain points, adoption happens very quickly.

The other thing is to make sure that when you engage with Professional Services, you give them something to focus on. Often, organizations look to Professional Services to lead, while Professional Services are looking to the organization to lead. Really it's up to the organization to really instruct them on what they need accomplished, and by identifying those pain points and focusing on those quick wins that is really going to speed up the process by which you implement the tool.

To view the full video interview, go to http://www.emc.com/link

ABOUT RSA

RSA's Intelligence Driven Security solutions help organizations reduce the risks of operating in a digital world. Through visibility, analysis, and action, RSA solutions give customers the ability to detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, prevent IP theft, fraud and cybercrime. For more information on RSA, please visit www.RSA.com.

CONTACT US

To learn more about how RSA products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller — or visit us at www.RSA.com

www.emc.com/rsa

RSA