INTERVIEW TRANSCRIPT

CLOUD MIGRATION: THE CHANCE TO TRANSFORM SECURITY

Chronicle's Anton Chuvakin on How to Take Advantage of the Opportunity to Redo Cybersecurity

Chronicle
now part of Google Cloud

iSMG
INFORMATION SECURITY
MEDIA GROUP

Chronicle
now part of Google Cloud

Cloud migration isn't just an opportunity to transform business; it's a chance to completely redo the cybersecurity model, says **Anton Chuvakin**, Ph.D., of Chronicle. He explains the business benefits of security transformation for the cloud.

In an interview with Tom Field of Information Security Media Group, Chuvakin discusses:

- The acceleration of cloud adoption;
- Why and how cybersecurity must be redone;
- Issues that are often overlooked in the cloud shared security model.

Chuvakin works on security solution strategy at Google Cloud, where he arrived via Chronicle Security, an Alphabet company acquired by Google in July 2019. He is a recognized security expert in the fields of log management, SIEM and PCI DSS compliance. Until recently, he was a research vice president and distinguished analyst at Gartner for the technical professionals security and risk management strategies team.

A COMMON SECURITY MISTAKE

TOM FIELD: As enterprises have shifted so quickly to the cloud this year, what are some of the common security mistakes you've seen them committing?

ANTON CHUVAKIN: One of the most interesting mistakes that I've seen is copying practices and mistakes from the data center and applying them to the cloud. They go to the cloud and they try to make it as noncloudy as possible, without using any of the security controls and other advantages in the cloud. They treat it as a rented co-location space – as just a place to put their systems.

This means they gain familiarity, and that's an advantage. But many of the positives are never manifest for them. Also, the costs are occasionally quite high, because certain cloud optimizations or cloud storage mechanisms aren't being used, and they store data in the on-premises way while being in the cloud, which is not really known to be cheap. The cloud way is cheap in the cloud, but the on-premises way in the cloud is not. So bringing too much of your legacy from on-premises to the cloud is the main mistake.

WHY REDO SECURITY?

FIELD: You've said that this shift gives enterprises the chance to redo security. Why does it need to be redone?

CHUVAKIN: Lamenting about the state of security is a favorite pastime for most security professionals I've met. The types of challenges that we face today – including ransomware – are not conceptually new. They stem from some of the decisions made in the '80s and '90s.

We need to reduce security from certain fundamentals, but it's impossible because we have technical depth; we have legacy systems; we have other things. But when you move to the cloud in a cloudy way, not in a data center-centric way, you have a chance to drop some of the legacy stuff and lose some of the problems that haunted you before and that still haunt you in the cloud, if you do it wrong.

> “Despite all the things that change in the cloud, the shared responsibility model or joint responsibility model is something that’s forever.”

Dr. Anton Chuvakin
Security Solution Strategy, Chronicle

Dr. Anton Chuvakin (left) with ISMG's Tom Field

BUSINESS BENEFITS OF REDOING SECURITY

FIELD: What are the business benefits of redoing security?

CHUVAKIN: A lot of things would be more streamlined and more tied to the types of workload you are moving. For example, if you are using some data processing workload to the cloud and you are moving it from a system that was written in the '90s that used a big database, some customer-written application, you will have to modify the application to use cloud storage, possibly use modern programming languages, which would improve application security. And you would possibly architect it in a way that fits the cloud, which would increase performance, security, ease of maintenance and a whole bunch of other factors.

There is definitely a cost. It's typically a cost in training and stepping into the less familiar. But the advantages are both on the business side and on the threat reduction side. One other challenge is that compliance aspects weigh on both sides. There are compliance costs and there are compliance benefits, so that part is a little bit tricky.

SHARED SECURITY MODEL

FIELD: It's common to say that the cloud is a shared security model. What is often overlooked when people say that?

CHUVAKIN: Despite all the things that change in the cloud, the shared responsibility model or joint responsibility model is something that's forever. It's not going to change. There will be elements that you control and you would always control as a cloud customer. You would always control and own the accountability. There's no debate about that. We can debate how much of application security, network security, other types of security you'd handle. That's all TBD in the joint responsibility model. But, ultimately, you own the accountability for it. It's not the cloud provider. That is hard to change and perhaps only with significant innovation – something like Google would do – it may change. But, ultimately, that model is forever. The challenge with that model is that people often don't get into enough nuance.

> "We have to make cloud security much more usable, much more default, much more opt-out so that you have to work hard to not have it."

For example, simple, simple, simple control, physical security. It's pretty obvious that it fits on the provider side of the shared model. Nothing contentious. Who owns the guards? Who owns the physical security? The cloud provider, no debate. Now, if you wrote an application and deployed it in the cloud, who owns application security? That is also a no-brainer because it's your code. You wrote it. A small percentage of people assume that the application would be secure because cloud providers are responsible. Well, you wrote the code. Whose code is it? It's yours. That one falls on your side. So, this is a pretty simple case.

Now let's take a tricky case: network security. As a cloud provider, I may give you network security controls that can be arranged in an effective defense against network attacks, but you can potentially either not use them or bring your own controls that you know and deploy them in a way that you are familiar with from on-premises. Now, you built a little island of on-premises in the cloud, and who do you think owns security there? I would say you do, but you would say, "Wait a second. These are your network security controls, and it's your network. Maybe you do." And it becomes contentious.

These situations are resolved very easily, if you are doing it in good faith, if you want to solve the problem. But if people shift into a finger-pointing, blaming mode, these disputes become hairy.

I can pick even more hard-to-argue elements from the joint responsibility matrix. For example: logging. Who gets the logs? Who analyzes them? What kind of insight is derived? There are a lot of very nuanced questions. If I were doing a joint responsibility model, I would stick "both" in certain elements, and it would confuse people. What do you mean by "both"? Whose responsibility is this?

I was just looking at what PCI DSS and the PCI Security Council put together a good number of years ago, and they have a fair number of cells in their matrix that say "both." What does it mean? What do you do? These are the challenges and examples with the joint responsibility model that not enough people have internalized well.

TRANSFORMING SECURITY

FIELD: I accept your premise: Here is the opportunity to transform security. But where do you begin? How do you start this transformation from day one?

CHUVAKIN: Gartner says that 99% of breaches in the cloud are the customer's fault. That's the truth. If you don't believe it, I can show you the fact base. Let's accept that for now. But is this a good thing ethically? Ethically, I would say, "Sure. I give you controls. You do a poor job configuring the controls. You get hacked. It follows the Gartner line that it's your fault. But what can I do to help you not make the mistakes?"

> "Chronicle gives you cloud-native security even if you are not in the cloud."

We can build security in the cloud ... where the client has to do less and whenever a client does things that are wrong security-wise, there would be a lot more friction. Think of it as nudging them away from insecure solutions, securing what we can by default. There's a lot more work that every cloud provider, including us, would have to do to make it a reality. But it has to happen. We have to make cloud security much more usable, much more default, much more opt-out so that you have to work hard to not have it. That is a place to start.

THE CHRONICLE APPROACH

FIELD: Let's bring it back to Chronicle. How are you helping customers to transform security amid their own cloud migration?

CHUVAKIN: One popular misconception about Chronicle is that people assume that it works just to Google Cloud. But in reality, it's the opposite. Chronicle works much better for non-Google Cloud environments because Chronicle was built to serve all customers – on-premises, in Google Cloud, outside of Google Cloud. Chronicle gives you cloud-native security even if you are not in the cloud. As you're transitioning from your on-premises Google Cloud, you would still use it. And you'd still find value in many things we've built. You can stay with your familiar controls from on-premises to the cloud, but those controls aren't legacy controls. They are modern controls built in a cloud way, yet you can use them both in the cloud and in your regular environment. ■

Listen to the full interview: https://www.bankinfosecurity.eu/cloud-migration-chance-to-transform-security-a-15280

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANKINFO SECURITY® CUINFO SECURITY® Just for Credit Unions GOVINFO SECURITY® HEALTHCAREINFO SECURITY®

infoRisk® TODAY CAREERSINFO SECURITY® Data Breach. Prevention. Response. Notification. TODAY CyberEd.io

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io