ordr

VERITEX COMMUNITY BANK

CASE STUDY

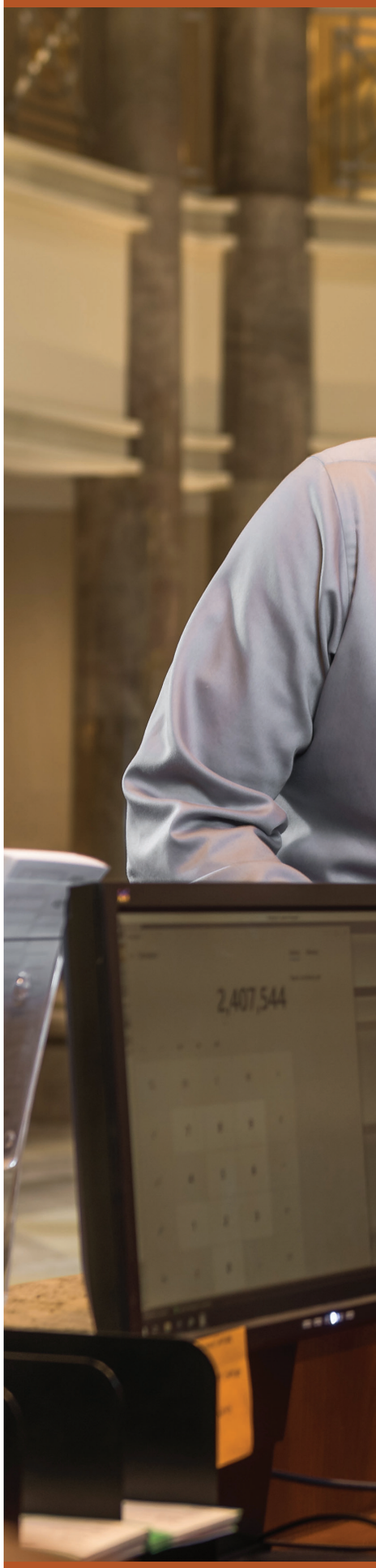
# VERITEX
## COMMUNITY BANK

*Technology and Truth*

# TECHNOLOGY AND Truth

## Veritex Community Bank is on a cybersecurity journey rooted in a Texas-sized commitment to honesty

Truth. It's what's deep in the heart of one of the 10 largest banks headquartered in Texas. Since its inception in 2010, Veritex Community Bank (VCB) has been firmly grounded in truth, transparency, and unwavering integrity. Those same values are the foundation for a cyber technology journey that aims to identify cybersecurity threats and respond to them, protecting and recovering vital information.




The award-winning Dallas-based institution specializes in providing depository and credit services to small and mid-size businesses largely neglected by national banks. VCB operates banking centers in the Dallas-Fort Worth metroplex and greater Houston area.

Bob Ludecke, VCB's Chief Information Security Officer, oversees its Cyber and Information Security Program (CISP). We recently spoke with him about the program and its goals, and the most vital aspects of their efforts. "Ensuring the careful consideration of people, processes, and technology throughout the entire life cycle, from conception to implementation and maintenance, is paramount to preserving our business partners' operational efficiency and guaranteeing the successful functioning of our technology," he said.

Understanding the needs of the business as well as of the customer is essential. "Cyber doesn't drive business, business drives cyber," he said. "I learned this more than 20 years ago when I attended my first Common Body of Knowledge presentation for the newly created Certified Information Systems Security Professional (CISSP) certification, and it stuck."

VCB's customers trust the bank to provide credit, capital storage,

CYBALT™

Cybalt is at the forefront of providing industry-leading **cybersecurity solutions and services** to secure its clients from devastating cyberattacks and enable their digital transformation journey. **Headquartered in the US**, our global delivery model empowers us to serve clients across industries globally. Our approach focuses on delivering **outcome-based services tailored to each client's unique security challenges** and needs. We provide **comprehensive detection, protection, and response** to emerging cyber threats by utilizing a broad array of **cutting-edge cybersecurity platforms, robust processes, and our deep expertise.** In combination with Black Box (www.blackbox.com), **Cybalt** is responsible for providing security solutions and services to the global customers across **30+ countries**.

At Cybalt, excellence is ingrained in our DNA. Being assured that their operations are well-protected against cyber threats, our clients confidently navigate today's digital landscape. As their cybersecurity partners, we not only protect their current operations but also prepare them to embrace their evolving digital transformation journey safely.

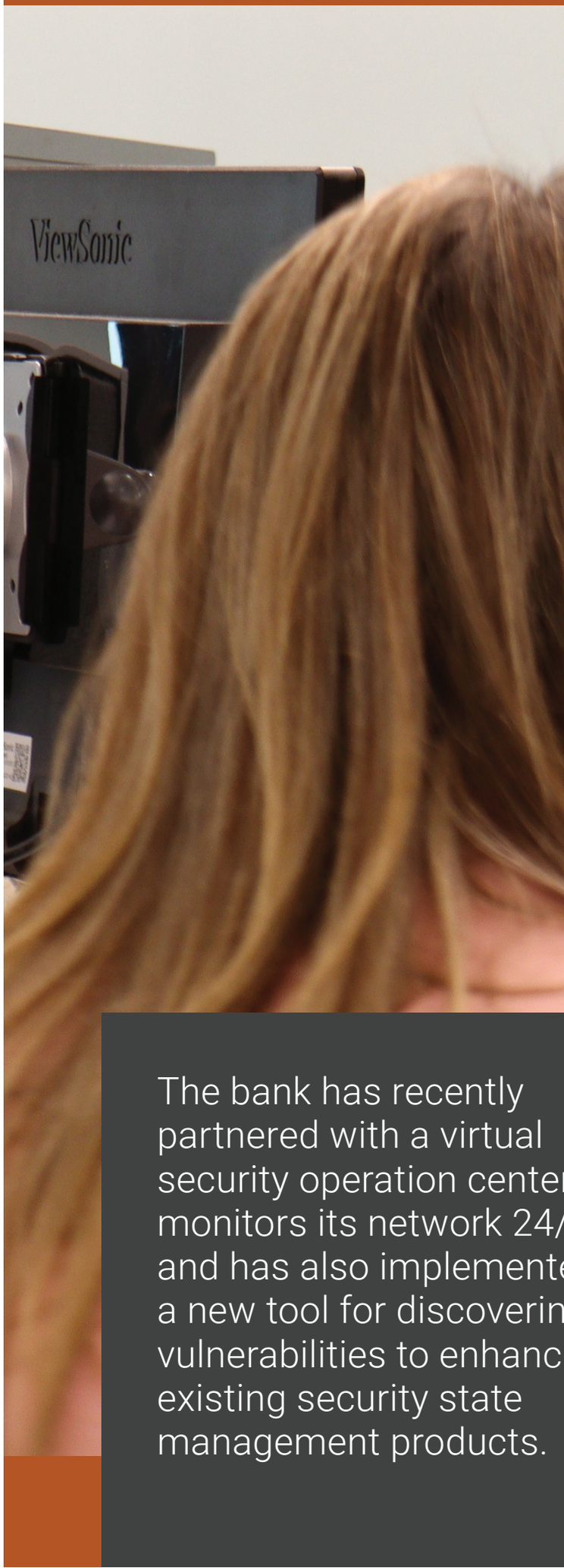
www.cybalt.com

and investment opportunities and to safeguard the cash, capital, and personally identifiable information it collects to do so. Cybersecurity requires that Ludecke's teams understand the origin, processing, transmission, and storage of this information.

"The central reason we have technology is to serve our customers and achieve our strategic goals resulting in shareholder value. That technology is where information is created, transmitted, processed, and/or stored," he pointed out. "Each one of those functions is an opportunity for unauthorized disclosure. Security and IT teams are on the hook to collaborate to make sure that data is secure at each function."

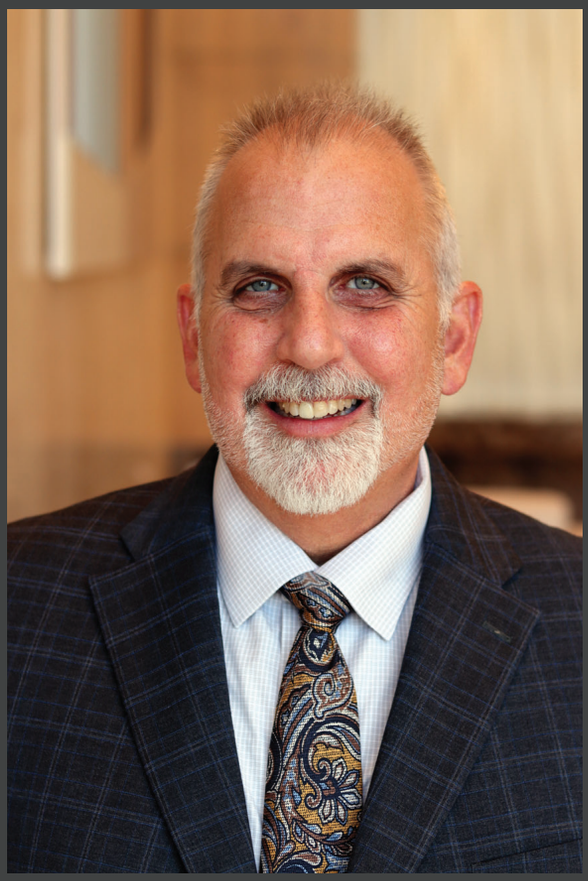
As CISO, it is crucial for Ludecke to understand where the bank's information assets are located, as it allows him to establish appropriate safeguards to effectively ensure their protection. "Additionally, we need the capability to monitor external activity in order to prevent, stop, or contain security events. This helps to avoid potential exposure of our data to unauthorized parties."

The bank has recently partnered with a virtual security operation center that monitors its network 24/7 and has also implemented a new tool for discovering vulnerabilities to enhance existing security state management products. "This tool identifies and categorizes all assets on our network while highlighting any vulnerabilities they may have," he said.




The bank has recently partnered with a virtual security operation cente monitors its network 24/ and has also implemente a new tool for discoverin vulnerabilities to enhanc existing security state management products.

r that
/7
ed
g
e



BOB LUDECKE, VCB'S CHIEF INFORMATION SECURITY OFFICER

"We implemented a software solution that identifies all the devices on our network, categorizing them by the type of device and identifies open vulnerabilities on those devices."

## KEEPING UP WITH THE BAD ACTORS

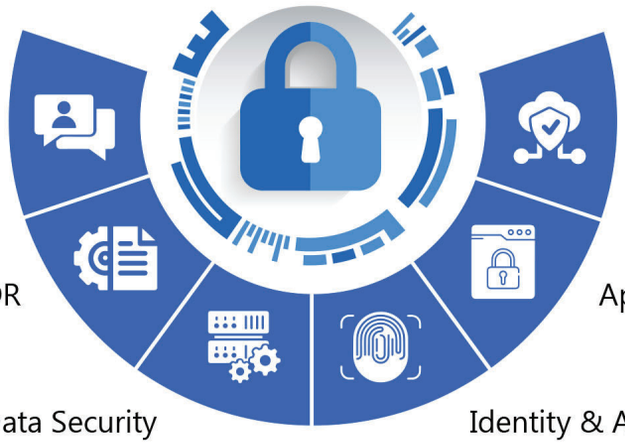
The volume of bad actors and the misuse of technology to attack digital infrastructure continue to increase virtually every hour of every day. VCB's cybersecurity journey includes efforts to educate VCB's business partners on information security and on how to handle sensitive financial information, with the goal of building a human firewall. "This takes time. The bad actors are working 24/7, so we all must be on alert and apply best practices with securing information. The Veritex organization excels at seeking input from my team to address its concerns and implementing process improvements that we recommend," Ludecke said.

When it comes to securing VCB's connected devices, his team needs to know everything that's connected to its network in order to secure them. "We implemented a software solution that identifying all the devices on our network, categorizing them by the type of device and identifies open vulnerabilities on those devices," he said.

Created by Ordr, the solution delivers visibility and security for connected devices from traditional IT devices to the newer and more vulnerable Internet of Things, and operation technology (OT). It discovers every device, profiles its risk and behavior, maps all communications, and protects it with automated policies. VCB is using Ordr not only to inventory the devices that they have in the network, but also support their cybersecurity hygiene program - such as identifying devices running outdated operating systems.

# Securing Clients at the Speed of Innovation

## Our Portfolio




**Consulting** Services

**Transformation** Services

**Managed** Services

- Tailor-made Solutions
- Platform Agonistic
- Cloud-first Offerings
- Automation Powered
- Globally Scalable
- Skilled & Certified Talent

**In this era of Generative AI-armed threat actors, it's imperative for enterprises to strategically advance their cybersecurity defenses and fortify themselves from increasingly sophisticated and damaging cyberattacks.**

- Khiro Mishra, CEO - Cybalt

A Q&A with

# BOB LUDECKE

SVP & CISO of Veritex Community Bank

## TELL US A LITTLE ABOUT YOURSELF AND YOUR JOURNEY TO WHERE YOU ARE TODAY?

I grew up in the Tampa, St. Petersburg area, and my journey started off with my first computer job at a savings and loan organization in Florida. While the organization succumbed to the S&L crisis at the time, it was a good introduction to the industry. After graduating with my criminal justice degree, I worked in a variety of different roles – helpdesk, systems analyst, compliance and audit manager – at various technology providers. I then moved the family to New York to take on a role as the Information Risk Lead at JP Morgan Chase. After a couple of years in New York, I decided to move to Texas for the warmer weather. I led risk management and governance teams at companies like Fidelity Investments and Citi here in Texas before joining Veritex Community Bank. I've been CISO at Veritex since 2021.

On a personal note, I've been married to my lovely wife for 30 years and we have four daughters, one grandson, one granddaughter, and one granddaughter on the way.

## YOU HAVE A LOT OF EXPERIENCE IN TECHNOLOGY AND RISK MANAGEMENT POSITIONS, HOW HAVE THESE ROLES HELPED YOU GET TO A CISO POSITION?

The main skills these roles have taught me is how to work with people to get things done. A lot of what I do as a CISO is influencing and collaborating with a lot of very smart people. Cybersecurity isn't just about protecting the business; cybersecurity must be an enabler to help drive the business forward.

## WHAT ARE THE CYBERSECURITY CHALLENGES W/ THE EXPLOSIVE GROWTH OF CONNECTED ASSETS IN FINANCIAL SERVICES?

The biggest challenge is visibility. You can't protect what you don't know about. Depending on the size of your organization, there may be tens of thousands to hundreds of thousands of connected assets, ranging from laptops and mobile devices, networking equipment and IP phones to Internet of Things (IoT) and Operational Technology (OT) like elevator control systems, video surveillance cameras and alarm systems that are critical to running the business. These connected assets may run outdated operating systems, default passwords, or have vulnerabilities that increase your attack surface.

"Cybersecurity isn't just about protecting the business; cybersecurity must be an enabler to help drive the business forward."

## WHAT GUIDANCE DO YOU HAVE FOR CISOS & SECURITY LEADERS TO SECURE THESE DEVICES?

Within the financial services industry, there is a lot of governance. Having a solution like Ordr that can identify every "thing" on the network including IoT and OT devices that are particularly challenging to categorize is important. Next, focus on cyber hygiene; determine which assets are running outdated operating systems, which assets have critical vulnerabilities that need to be patched. Finally, we also use Ordr for device-based threat detection. We've been able to identify issues before being notified by our virtual SOC.

I would also add that automation is important. When you're dealing with high volume of cyber assets, make sure to select a solution that will integrate with your existing vulnerability workflows, and can optimize your resources by automating tasks like discovering and categorizing assets, alerting when new assets connect to the network and triggering a scan, or generating policies to secure certain devices.

## WHAT KEEPS YOU UP AT NIGHT?

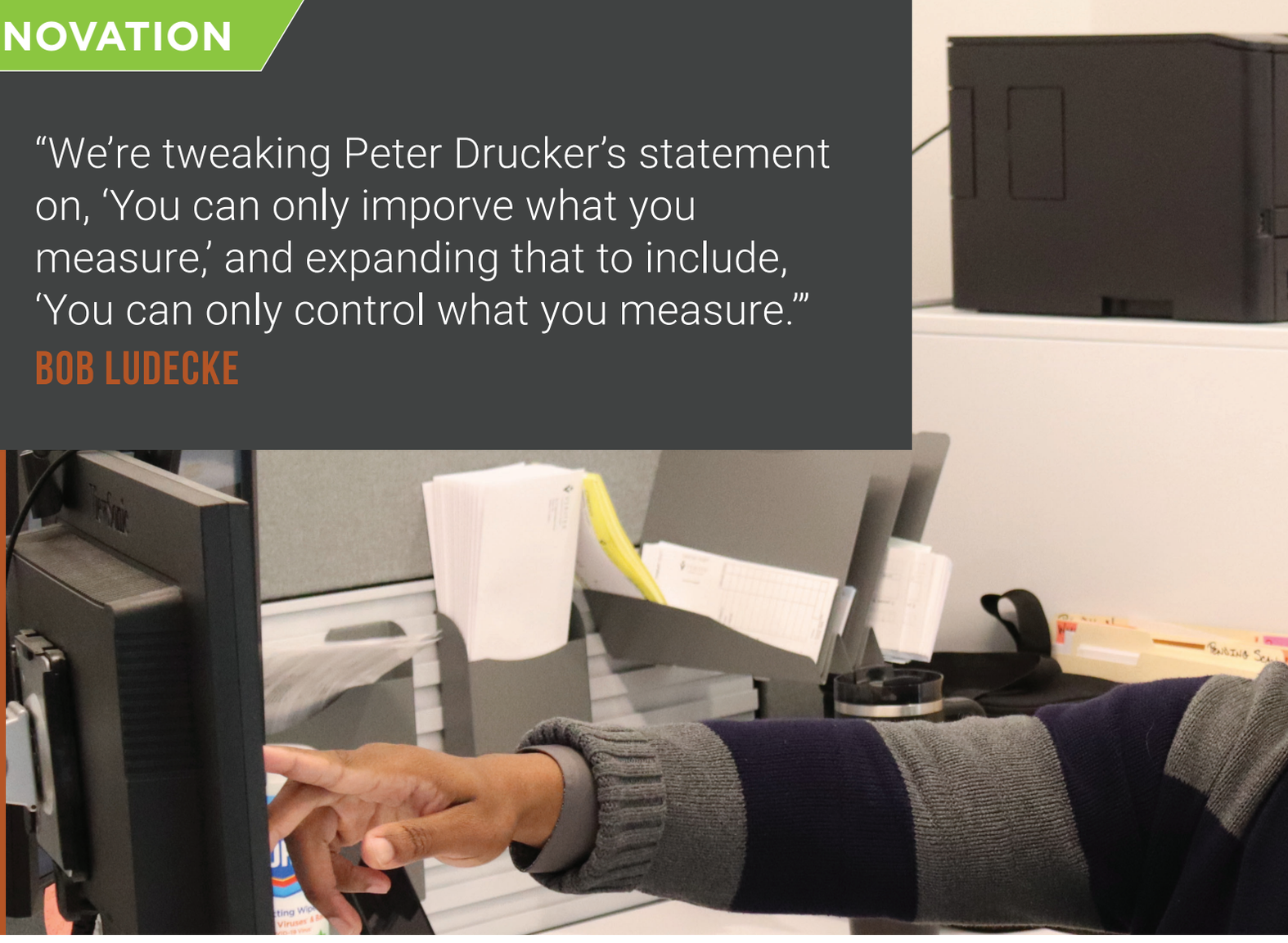
The bad actors don't go to sleep, they are working 24-7, and this means we must stay vigilant. People are our most important asset but at the same time they can also become our biggest risks. I need to make sure our teams and partners are properly trained on cybersecurity and know not to click on phishing emails or share their passwords. At the same time, I need to trust in our virtual SOC, the cybersecurity tools we have invested in and an architecture where we design security controls to prevent as much as possible. Finally, there are the internal processes. We continuously test our processes and tools with table top exercises, and penetration testing so we can be prepared.

## ANY FINAL GUIDANCE?

Technology only gets you so far. I would encourage everyone to also focus on building relationships with senior leaders and lower levels. The role of the CISO has become very broad. It's important to influence cybersecurity behavior and build "human firewalls". Talk to senior leaders in business language, about the risks and costs of not doing something. I regularly report to the board of directors, and the metrics on how we are doing, I'm telling a story with my metrics.

Finally, life is short; have fun with what you're doing. Veritex has great people and culture, and I have a great team. it's a great place to work.

> "We're tweaking Peter Drucker's statement on, 'You can only imporve what you measure,' and expanding that to include, 'You can only control what you measure.'"
>
> **BOB LUDECKE**



Insights on vulnerabilities for IoT and OT devices also complement their traditional vulnerability management solutions. "This was a very good investment."

According to Ludecke, using Ordr's device-centric threat and anomaly detection, VCB has also been able to detect and quickly address issues, even before being notified by their virtual SOC. This has helped the team accelerate response.

To ensure that VCB's connected devices are properly configured and maintained, the organization shifted left, which means having security assurances at the earliest stages of the life cycle.

"This is important to drive hardening standards across the technology stack before deployment. Leveraging industry standards as a baseline is a great first step." Having tools in place to measure compliance to the industry standard is also critically important. "We're tweaking Peter Drucker's statement on, 'You can only improve what you measure,' and expanding that to include, 'You can only control what you measure,'" he added.

As you'd expect, robust policies and procedures are in place to govern the use of connected devices.

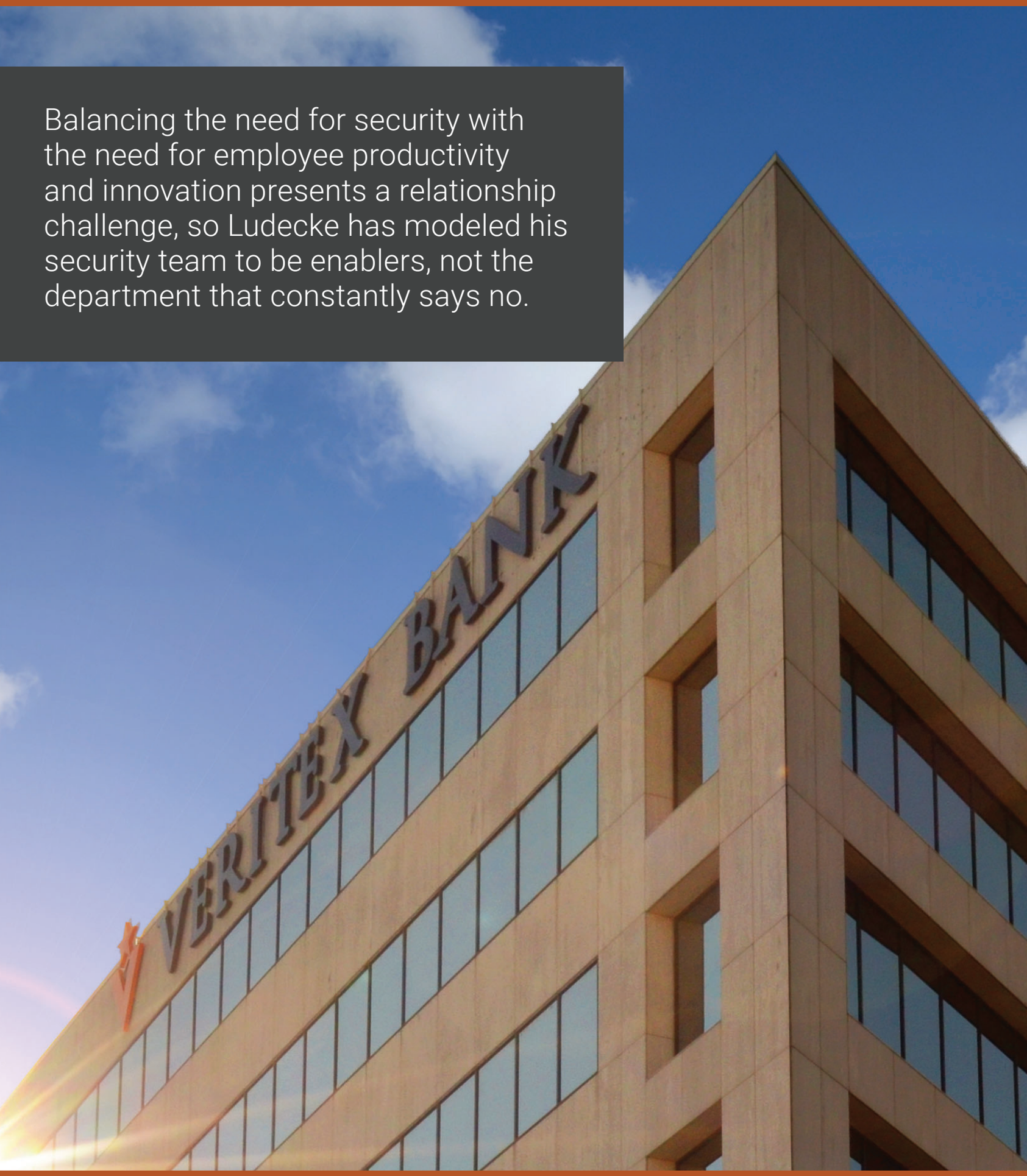
"We transitioned to a new policy taxonomy for cyber and information

security," he revealed. Policy is applicable to the workers and authorizes standards, which are more focused in a particular area of security. Policies and standards are similar in that they tell what is required. Next, VCB has process control manuals that describe in detail how the control is managed, enforced, and measured. "For each standard, we have a corresponding process control manual. Measures are in place to track compliance."

To educate its employees about the importance of cybersecurity, VCB has annual training requirements that each employee or contractor is required to take, and Ludecke's team gives monthly staff briefings to help staff members understand their responsibilities, best practices to follow, or reminders to be diligent on emerging patterns. "Tiger team penetration testing provides awareness to our employees of the importance of securing all information, whether paper or digital, in their workspaces. Phishing campaigns are conducted to advise our employees on the different schemes threat actors are actively using."

The CISP team closely collaborates with vendors and key partners, too. "Weekly check points are critical for ensuring our

Balancing the need for security with the need for employee productivity and innovation presents a relationship challenge, so Ludecke has modeled his security team to be enablers, not the department that constantly says no.



collective success and fostering a sense of collaboration within our community at Veritex. We pride ourselves on being more than just a company — we are a tight knit family," he noted. "My team is critically important to the success of the CISP. I could not have asked for a better team or better management that fully supports me and the program."

Balancing the need for security with the need for employee productivity and innovation presents a relationship challenge, so Ludecke has modeled his security team to be enablers, not the department that constantly says no. "The relationship is key to ensure that we are promoting the idea of a human firewall. Our business partners handle information, and they are on the front lines. Therefore, it is best to have the business partners be well versed in how to perform their jobs securely. This takes time but is worth the effort."

Ludecke invoked Drucker's adherence to accurate measurement as the ultimate truth. "Metrics indicate if things are working by showing progress toward strategic goal fulfillment. They also provide opportunities to make certain that programs are optimized and are operating as efficiently as possible," he said.

It's clear VCB's commitment to veracity isn't just a portmanteau. "The corporate culture is impressive, and, to be honest with you, I didn't know places like Veritex existed. I am incredibly blessed to be at this institution and serve as its Chief Information Security Officer." ■

POWERED BY

BOSS MAGAZINE

8214 Westchester Drive
Suite 800, Dallas, TX 75225

Ph: 972.349.6200

**www.veritexbank.com**