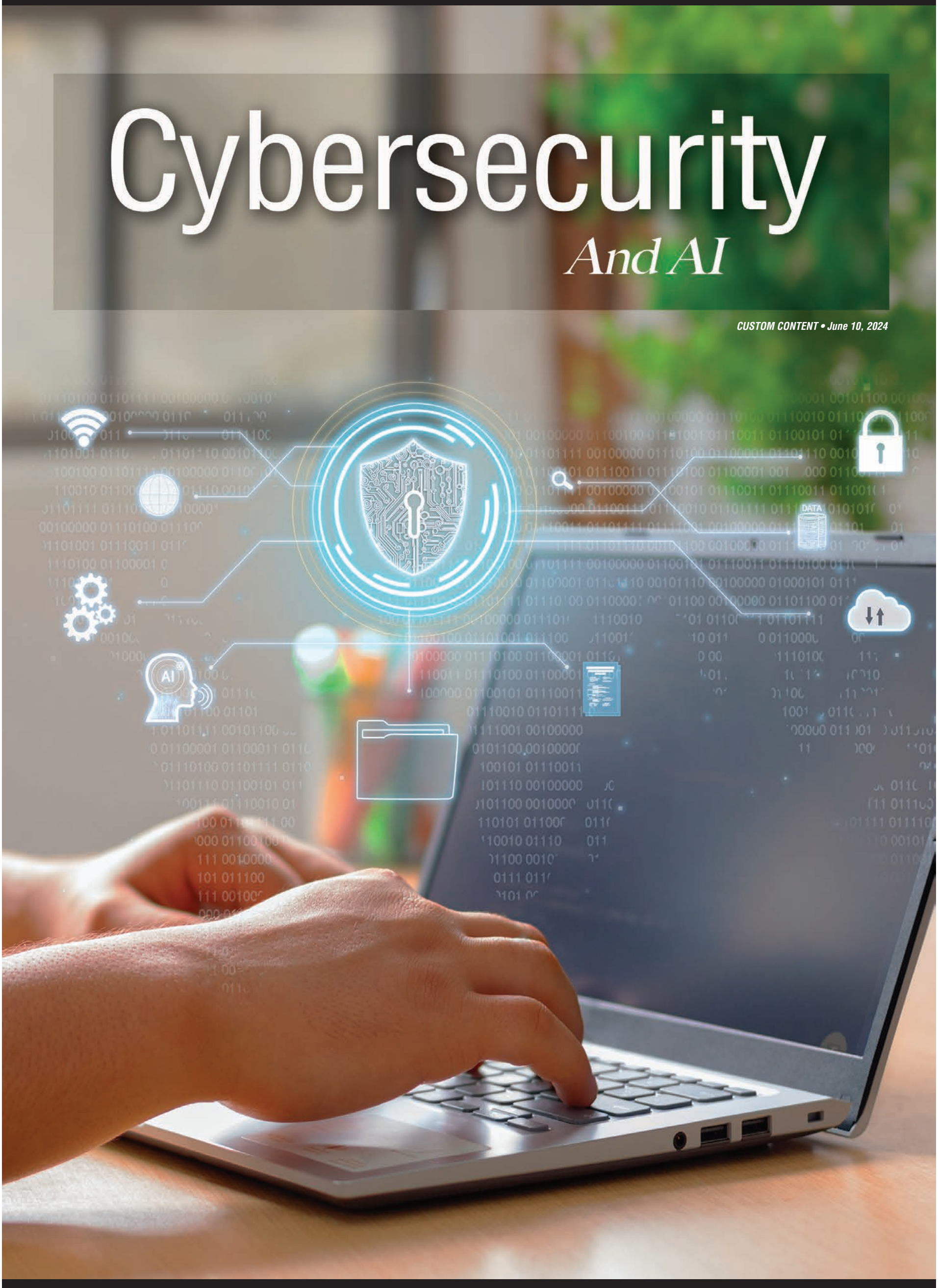
Cybersecurity

And AI

CUSTOM CONTENT • June 10, 2024



CYBERSECURITY AND AI

6 Startup KPIs You Need to Measure

By Withum's Technology and Emerging Growth Services Team

Contact Allen Goh

As funding for technology startups and emerging growth companies face continued pressures, there will be an increased investor due diligence and review of key operating and financial key performance indicators (KPIs). The depth and complexity of startup KPIs can be as simple as a back-of-the-napkin calculation or as complex as a merger of multiple **customer relationship management (CRM) systems** and financial information. No matter the stage of growth, the ability to summarize multiple data points into meaningful metrics is critical to successful financial and operational growth.

Key Startup Metrics

While not comprehensive, the following are key startup metrics companies should use to track and monitor growth and proactively identify challenges. Each KPI provides insights that – whether good or bad – create opportunities for corrections and decision-making.

1. Annual Recurring Revenue (ARR)

ARR represents a startup subscription-based revenue on an annualized basis. ARR provides visibility into a startup's sales and growth pipeline. ARR's continued growth is evidently healthy and sustained growth compared to a decline, which can be a red flag.

ARR is calculated by:
– Monthly Reoccurring Revenue (MRR) X's 12 months whereas
– MRR = Number of customers X's average revenue per customer
– For example, if a startup has 50 customers paying an average of $1,000 per month
– 50 customers X $1,000 X's 12 months = $600,000 ARR

2. Customer Churn Rate

Customer churn rate is the percentage of lost customers over a period. While customer churn is expected, an increasing churn rate is evident in customer retention challenges.

The customer churn rate is calculated by:
– (Number of customers lost during a period / Number of customers at the beginning of period) X's 100
– For example, at the beginning of the month, a startup has 50 customers and lost four customers during the month, the churn rate is calculated by
– (4 customers lost in month / 50 customers at the beginning of the month) X's 100 = 8%

3. Customer Acquisition Cost (CAC)

CAC measures how much a startup is spending to obtain new customers. In the early stages of growth, a higher CAC is expected. Still, as time progresses, an incremental decrease is a vital metric to monitor if customer acquisition costs result in returns.

Here is how CAC is calculated:
– Costs for sales and marketing during a period / total number of customers during a period
– For example, if a startup incurred $30k in salaries for the sales team and $10k in marketing material and acquired 5 customers
– ($30k + $10k) / 5 = $8k CAC

4. Payroll as a Percentage of Expenses and Sales

For many startups, their high costs consist of payroll and contractor costs. For pre-revenue companies, measuring payroll costs compared to the total expenses helps identify the amount of payroll and contractor costs compared to the total. A range of 70-80% of total expenditures is typical for startups – the remaining costs are related to SaaS costs, Selling, General and Administrative (SG&A) costs and other operating expenses. A reduction in payroll percentage can suggest that certain operational costs have begun to increase disproportionately and should be investigated.

Payroll as a percentage of expense is calculated by:
– Total payroll and contractor costs / total expenses
– For example, total payroll and contractor costs for a period were $800k, and total expenses were $1 Million ($800k/$1 million = 80%)

For startups who have begun generating revenue, a measurement of payroll compared to total sales helps identify how the growth and changes in headcount costs directly correlate to revenue. The percentage range will vary based on the point in a revenue life cycle and can be defined and measured under multiple fronts.

5. Gross Margin

Gross margins represent a startup's profit from its core revenue generation activity. This excludes SG&A costs such as marketing, rent and other related operating expenses. As a startup scales, the gross margin will likely be negative, which is expected and normal. Continued growth in revenue will create an opportunity to obtain cost efficiencies which can inevitably lead to smaller negative gross margins and eventually positive gross margins.

Gross margin is calculated by:
– Total Revenue – Total Cost of Revenue
– For example, total revenue during a $1.2 million period and total costs were $1.5 million
– $1.2 million – $1.5 million = ($300k) gross margin

6. Cash Runway

Cash runway measures the number of months a company has until its cash runs out. The cash runaway can be calculated using anywhere from a simple calculation of the current cash balance divided by current cash burn (cash expenses less cash revenue), which relies on historical data, or a more complex calculation that depends on the cash flow forecast of cash expenses and revenues when projecting the projected cash burn rate.

Here is how the cash runway is calculated:
– Total cash balance at the end of the period / Total cash expenses during a period
– For example, total cash expenditures for during a period were $300k, and the ending cash balance for the period was $2.4 Million
– $2.4 Million ending cash balance / $300k cash expenditures = 8 months cash runway

Each startup has unique processes, and KPIs can be calculated in various ways. A trusted CFO partner ensures your startup metrics are consistent and relevant to your company. Withum's CFO Advisory and Outsourced Accounting Systems and Services (**OASyS**) team provides that stress-free solution of a perfectly framed financial picture, saving companies valuable time and money. Every business's needs differ based on their stage in the business lifecycle, so we tailor our services to fit exactly your needs.

We work with businesses of all sizes, from large organizations that prefer not to staff and manage an accounting department, to smaller entities or startups that need a 360-degree approach to direction and support.

Contact us to learn more about our Technology and Emerging Growth Services Practice at www.withum.com/tech.

Withum is a forward-thinking, technology-driven advisory and accounting firm that has a deep level of expertise relating to all of the issues that arise within the technology industry. Tech companies know they need to do more than just manage current trends, they need to anticipate future shifts as well. Withum's Technology and Emerging Growth Services Team's dynamic approach goes beyond traditional accounting services for companies, helping them build toward their goals and innovate for the future.

withum
ADVISORY TAX AUDIT

withum

Accountants Who Talk Tech

Tech companies speak the language of innovation, constantly looking for new and exciting ways to better our world and change the business landscape. At Withum, we go beyond traditional tax and accounting services, providing tech businesses with customized solutions that meet their needs. With deep expertise and over 150 specialized professionals, we don't just know tech, we talk tech.

withum.com/wc-tech

CYBERSECURITY AND AI

Enhanced Cybersecurity Protection with Fortress Checking

Sunwest Bank is the Bank built for Entrepreneurs by Entrepreneurs. This means we offer compressive banking and lending solutions through a team of experienced bankers that value long-lasting relationships and face-to-face service. Over the past fifty years, we have operated with a Fortress Balance Sheet, providing safety and security to our clients while meeting their needs by tailoring solutions to help their businesses grow through all business cycles.

In addition to the turbulent economic times, businesses nationwide are experiencing cybersecurity fraud at an increasing rate. These risks continue to grow as the technology available to hackers and their overall sophistication increases. Because of this, businesses must enhance their cybersecurity protection to keep up. When researching cybersecurity incidents at small and medium-sized businesses, most of the incidents and fraud losses could have been prevented through basic enhancements to system security and processes; however, an outsourced IT firm, internal IT administrator, or other key team members did not implement the necessary controls and training.

In continuing with our culture of providing safety and security to our clients, we have introduced an innovative, new banking product called the Sunwest Fortress Checking Account. This account is embedded with enhanced security tools designed to mitigate the risk of fraud on your bank account. This allows a business owner, CFO, or controller to have the confidence that all their team members are operating with the proper cybersecurity protocols when they interact with their bank, providing a more robust cybersecurity stance than any other bank account the company has.

Nearly all cybersecurity incidents occur because individuals are tricked into providing credentials through social engineering. Common schemes include phishing emails, text messages, or phone calls. Consistently, people are often the weakest link. There are many ways to mitigate this exposure through enhanced security settings, multi-factor authentication (MFA), dual control, ACH, and check fraud mitigation, and cybersecurity training. The Fortress Checking Account mandates and includes all these necessary security protocols and provides a comprehensive cybersecurity training platform from Beauceron Security at no additional cost. This is an institutional-level training platform that banks and Fortune 500 companies use to train their teams and transform them into proactive participants in identifying and resolving day-to-day, front-line cyber threats. This significantly reduces the business's overall exposure to cybersecurity fraud.

With the Fortress Checking Account, you will harden your company's cybersecurity stance to prevent growing cybersecurity threats, enabling you to stay focused on growing your business.

What is the Fortress Checking Account?
Sunwest Bank's Fortress Checking Account offers and requires embedded security tools, including Beauceron cybersecurity training, ACH & check fraud mitigation (positive pay), multi-factor authentication (MFA), fraud prevention with wire tokens, and more to protect your business from fraud. As part of this account offering, we also provide the latest cybersecurity training for all your employees.

Why invest in cybersecurity?
The economy has become increasingly digital, which means businesses need to protect themselves digitally the same way they think about physical security. The more difficult it is for a fraudster to gain access to your information and bank accounts, the less likely they are to succeed and will likely seek an easier victim. Therefore, continue to harden your cybersecurity to make your business an unattractive target.

Why is cybersecurity awareness training included?
People are almost always the weakest link in a cybersecurity breach. This is accomplished through very skilled and sophisticated social engineering, which targets owners and employees with emails, texts, links, and phone calls to capture sensitive credentials and then use this information to perpetrate fraud against the business. Fortress Checking includes cybersecurity awareness training from Beauceron Security, at no additional cost, to bolster your team's cybersecurity knowledge and defenses and combat the fact that people are often the primary targets in cyber-attacks.

How do I ensure my team benefits from the cybersecurity training?
Beauceron Security works with banks and Fortune 500 companies throughout North America to enhance their cybersecurity prevention. They have very strong

and intuitive training delivered through their platform and automated emails to test your team's effectiveness in thwarting phishing attempts. This is a state-of-the-art cybersecurity awareness tool to help your team manage cyber risk inside and outside your business at no additional cost. Additionally, implementing a cybersecurity training tool at your business will typically lower your overall cyber insurance premium.

What is Multi-factor Authentication, and why is it important?
Multi-factor authentication is the simplest method to prevent business email compromise and subsequent bank account fraud. Multi-factor authentication requires an additional device to authenticate logging into an account besides the email and password credentials. This prevents a fraudster from gaining access to your email or other accounts without that secondary device (i.e., mobile phone, RSA token, mobile app token, etc.). If this is not required at your business to be enabled by your team members, require it.

How does Positive Pay benefit and protect my business?
Positive Pay is an automated check and ACH prevention tool that helps detect and prevent unauthorized transactions. This tool electronically matches your business's checks with those presented for payment, significantly reducing the risk of fraud. Check and ACH fraud is on the rise, and Sunwest is proactively working with its clients to provide tools that create greater fraud deterrents and protect their businesses' hard-earned capital.

How can Sunwest Bank support my business?
Sunwest Bank is an entrepreneurial business bank with innovative solutions and team members to support your business through various stages of growth. We pride ourselves in providing safety and security to our clients through all economic cycles and the evolving business landscape.

To learn more about Sunwest Bank, the Bank for Entrepreneurs by Entrepreneurs, and our new Fortress Checking Account with embedded cybersecurity protection, visit sunwestbank.com/fortress-checking or scan the QR code on this page.

Carson Lappetito
President, Sunwest Bank

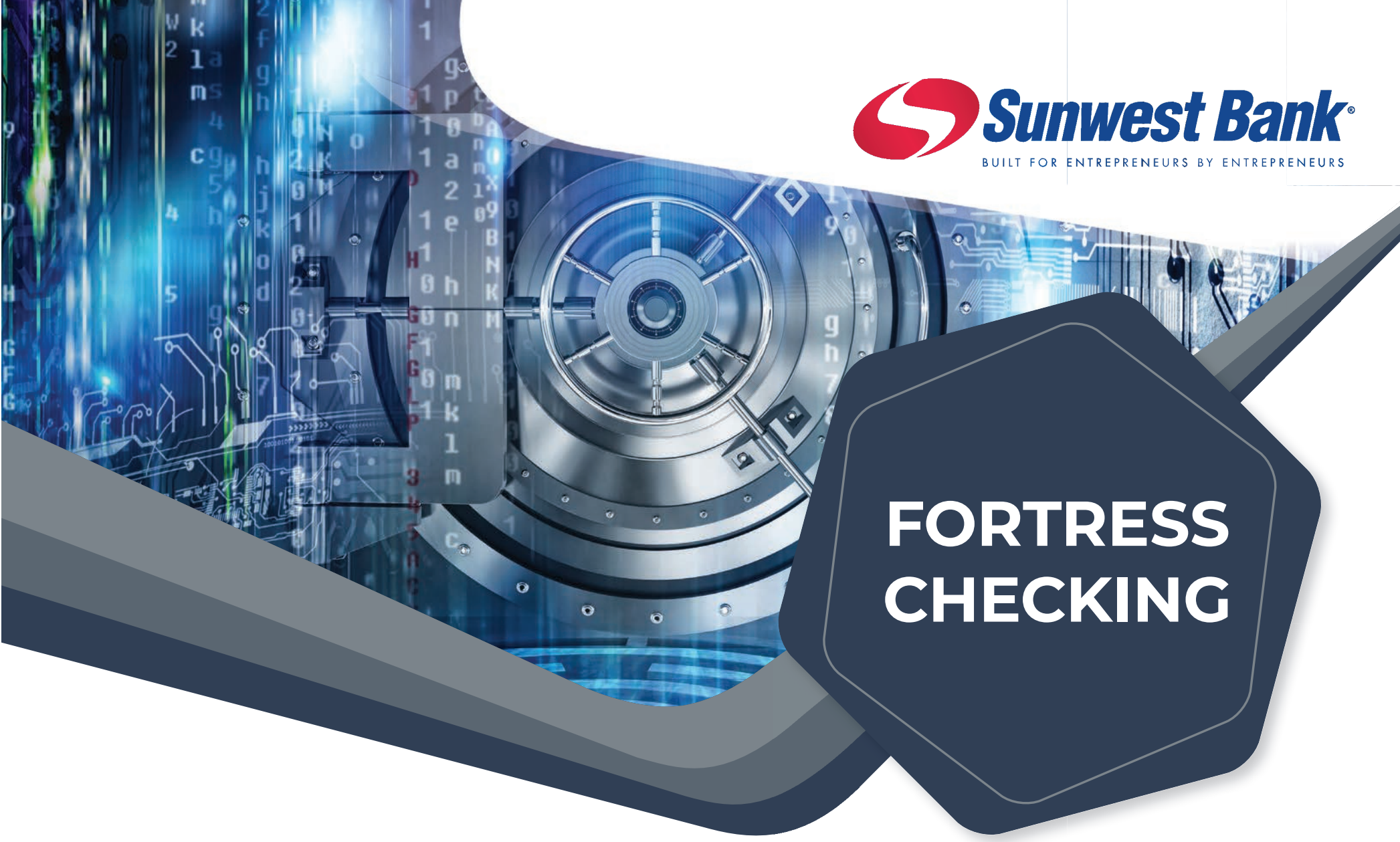
Carson Lappetito serves as the President and Director of Sunwest Bank. As the President of Sunwest Bank, Mr. Lappetito manages the banks day-to-day operations, which now has nearly $3.3 billion in assets. During his tenure, the bank has grown significantly and transformed itself into a regional business bank through M&A, enhancing the customer experience, and building innovative technology.

Sunwest Bank
BUILT FOR ENTREPRENEURS BY ENTREPRENEURS

Balance Requirement to waive Service Charge and Per Item Fees: $100,000 Avg Balance. Minimum Opening Balance: $100,000. Exclusive Benefits: Positive Pay and Cybersecurity Training Included. Up to 100 checks paid, 15 deposits, and 200 items deposited. Service Charge: $39.99. Check Paid Charge: $.30 Each. Deposit Charge: $1.50 Each. Checks Deposited Charge: $.15 Each.
**Available to Business Clients only*

Sunwest Bank®

BUILT FOR ENTREPRENEURS BY ENTREPRENEURS



FORTRESS CHECKING

Protect Your Business. Protect Your Money.

Multi-Factor Authentication | Positive Pay | Cybersecurity

Sunwest Bank's Fortress Checking Account provides enhanced security and tools to mitigate the risk of fraud to your business. We provide positive pay to mitigate check and ACH fraud as well as require MFA for all users accessing the account. In cybersecurity, people are still the main target in cyber attacks, so we provide the latest cybersecurity training to all your employees as part of this account offering.

CYBERSECURITY TRAINING SOFTWARE

Partnered with Beauceron Security to provide state-of-the-art cybersecurity awareness training available to all employees, at no additional cost.

DIGITAL AND MOBILE BANKING WITH MFA

Delivers one-time passcodes (OTP) to a specialized, secure phone application in order to authenticate user access when conducting wire and ACH transactions.

POSITIVE PAY

Integrated and automated check and ACH fraud solutions to provide greater fraud deterrents and mitigate risk to your business.

FRAUD PREVENTION WITH WIRE TOKENS

Delivers one-time passcodes (OTP) to a specialized, secure phone application in order to authenticate user access when conducting wire transactions.

Balance Requirement to waive Service Charge and Per Item Fees: $100,000 Avg Balance. Minimum Opening Balance: $100,000. Exclusive Benefits: Positive Pay and Cybersecurity Training Included. Up to 100 checks paid, 15 deposits, and 200 items deposited. Service Charge: $39.99. Check Paid Charge: $.30 Each. Deposit Charge: $1.50 Each. Checks Deposited Charge: $.15 Each.

**Available to Business Clients only*

STRENGTH // SECURITY // SOLUTIONS

www.sunwestbank.com 800.330.9890

EQUAL HOUSING LENDER

Member FDIC

CYBERSECURITY AND AI

Coming to America—European-style Comprehensive AI Legislation

By Sharon R. Klein, Alex C. Nisenbaum, and Karen H. Shin

Just as Europe pushed comprehensive privacy laws to America through the GDPR, European principles in the EU AI Act, enacted in March, are now in the United States. Colorado has become the first U.S. state with comprehensive artificial intelligence ("AI") legislation, SB 24-205 (the "Act"), effective February 1, 2026. The Act is a harbinger of comprehensive AI legislation that will dominate the U.S. landscape. Over a quarter of U.S. states have proposed AI legislation including California, which is currently drafting regulations on automated decision-making.

The Act applies to all developers and deployers of high-risk AI systems that do business in Colorado, even non-profits, and protects all Colorado residents ("consumers"), including employees. Similar to the EU AI Act, Colorado takes a risk-based approach. "High-risk AI systems" are any AI system that when deployed makes, or is a substantial factor in making, a consequential decision. "Developers" develop or intentionally and substantially modify an AI system, while "deployers" buy and deploy a vendor's high-risk AI system.

The Act follows several principles of the EU AI Act, including transparency, preventing algorithmic discrimination, and imposing differing obligations for developers and deployers.

Developers Versus Deployers

Both developers and deployers of high-risk AI systems must use reasonable care to protect consumers from any algorithmic discrimination and report such discrimination to the Colorado Attorney General within 90 days of discovery. The Colorado Attorney General can audit both developers and deployers.

Developers must:

- Make available a **general statement** describing the reasonably foreseeable uses and known harmful or inappropriate uses of the high-risk AI system and **documentation** that includes certain disclosures.
- Provide information to **assist deployers in completing impact assessments.**
- Provide a **notice** on its website including certain disclosures of high-risk AI systems developed or intentionally and substantially modified by the developer.

Deployers must:

- Implement and maintain a **risk management policy and program** regarding algorithmic discrimination.
- Complete an**impact assessment** annually and within 90 days after any intentional and substantial modification to the high-risk AI system is made available. The impact assessment must be retained for three years following the final deployment of the high-risk AI system.
- Annually**review** the deployment of each high-risk AI system so that there is no algorithmic discrimination.
- Provide **notices to consumers** containing specific disclosures.
- Provide consumers certain **rights** where the high-risk AI system makes or is a substantial factor in making a consequential decision that is adverse to the consumer.

The push to use AI and the corresponding influx of regulations affects all companies. The required assessments and other documentation fall heavily on AI developers but all companies using high-risk AI systems are subject to increased regulatory scrutiny and should analyze their exposure now to this new trend.

Sharon R. Klein, Alex C. Nisenbaum, and **Karen H. Shin** are members of Blank Rome's Orange County office and Privacy, Security & Data Protection team. Sharon is chair of the office and co-chair of the national practice team. She can be reached at sharon.klein@blankrome.com or 949.812.6010.

BLANKROME

Technologent®

LET'S MOVE FORWARD 2024

OUR WEBSITE

WHERE TECHNOLOGY MEETS INTELLIGENT INNOVATION

ENTERPRISE IT SOLUTIONS & SERVICES

- **GENERATIVE AI**
- **DATA** management
- **MODERN CLOUD** & hybrid infrastructure
- **CYBERSECURITY**
- **AUTOMATION**
- **SERVICES** professional financial service provider (XaaS)

technologent.com

@technologent

CYBERSECURITY AND AI

How to Recover From the Financial Fallout of a Cyberattack

Imagine a mid-sized, Orange County-based technology company thriving in its competitive market. Busy with success, the company neglected to prioritize cybersecurity measures. This oversight proved costly when sophisticated cybercriminals hacked into their systems, holding critical accounting data and backup records for ransom. Business operations ground to a halt, and the company faced a chaotic blend of financial, operational and reputational challenges.

For business owners, the nightmare of a data breach is real and costly, with average losses reaching $1.3 million in 2023, according to IBM's Cost of a Data Breach Report. These costs are attributable to business disruptions, revenue loss because of system downtime, the expense of losing and acquiring customers and the impact of the breach on reputation and trust. This doesn't include additional costs related to paying ransom or potential legal fees and fines.

Accounting professionals play a crucial role in quantifying and responding to the financial impact of cyber breaches using forensic accounting to trace losses and strategize effective recoveries. Their involvement is key.

Here are the ways accounting experts are utilized to help businesses recover from a cyberattack:

• **Insurance Claims:** With a deep understanding of insurance policies and the specifics of cyber incidents, accounting professionals can spearhead the complex claims process. They ensure all losses are accurately documented and that claims are submitted in compliance with policy requirements, maximizing reimbursement potential.

• **Forensic Accounting and Fraud Investigation:** Forensic accountants are instrumental in uncovering and investigating any fraudulent activities and transactions. This is critical evidence for legal action or insurance claims.

• **Restoring Financial Processes and Controls:** Accounting professionals assist in re-establishing secure payment processes, restoring financial data integrity and redesigning internal controls to help avoid future threats.

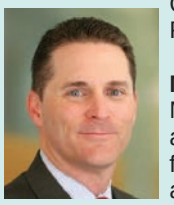
• **Financial Planning and Risk Management:** Accounting professionals advise on resource allocation to bolster cybersecurity measures, adjust financial forecasts to consider a cyberattack's long-term impact and integrate cyber risk management into larger organizational strategies.

• **Compliance and Reporting Requirements:** Following a cyberattack, accounting experts ensure compliance with relevant regulations and reporting requirements, mitigating legal and regulatory risks.

• **Creating a Resilient Outlook:** Accounting professionals perform post-incident reviews to uncover valuable lessons, offer guidance on enhancing cyber insurance coverage and contribute to the creation of comprehensive business continuity and disaster recovery plans.

The financial aftermath of a cyberattack can be as devastating as the attack itself. Accounting professionals are vital in helping businesses recover from cyberattacks, ensuring financial stability and safeguarding against future threats.

Marc Blythe, CPA, CGMA, Founder & President
Marc brings over 30 years of expertise in accounting and financial reporting for various companies. Before starting Blythe Global Advisors, he was an Assurance/Audit Partner at Ernst & Young.



Matthew Snow, CPA
Matthew is a seasoned executive in accounting, auditing and finance, helping firms with accounting issues, financial reporting and internal controls. He previously served as an Assurance/Audit Partner at Ernst & Young.

About Blythe Global Advisors
BGA is a finance and accounting consultancy with 15 years of experience in enhancing client revenue, reducing costs, and increasing profitability through expert advisory services.

BLYTHE GLOBAL ADVISORS
FILLING THE GAP IN ACCOUNTING AND FINANCIAL EXPERTISE®
15TH ANNIVERSARY