Correspondent Views

BANKERS' BANK OF THE WEST newsletter for community banks

Issue 3 ▪ 2017

PRESIDENT'S MESSAGE

Getting the job done right has never been a solo act

What one Portuguese prince, a German metalworker, and a 19th century British surgeon have in common is hard to reckon at first. But there are similarities—and lessons that can be applied to banking.

In the 1400s, Prince Henry of Portugal—a country bordered only by the Atlantic Ocean and Spain, a much larger and wealthier neighbor—founded an astronomical observatory and the world's first school for teaching science, map charting, and oceanic navigation. Much of the world was still unknown to Europeans at the time, and superstitions had been stifling explorers' ambitions. Henry the Navigator's sailor training school and his financing of bold expeditions paved the way for the Age of Discovery.

Bill Mitchell
BBW President and CEO

It was around this time that Johann Gutenberg, a goldsmith and printer by trade, spent years (possibly as much as a decade) inventing and refining a groundbreaking printing method using metal type. Not much is known about the man himself, but Gutenberg's press made possible the large-scale production of books. As books reached the hands of many more people, big changes in attitudes, politics and cultures followed.

Moving on to the early 1800s: Believing something had to be done to curb the high rate of death from gangrene in surgery patients, physician Joseph Lister took it upon himself to run a series of experiments. He confirmed that micro-organisms cause infection and identified an antiseptic capable of killing those germs. Lister's work led to the practice of washing hands, cleaning wounds, and sterilizing surgical instruments—sharply reducing the infection rate in patients after surgery.

At the center of each of these stories is someone with enough fire-in-the-belly drive and vision to achieve a big goal. They accomplished feats that furthered the greater good in some way.

History books won't mention this, but the work community bankers do furthers the greater good, too. You help families realize their dreams and businesses employ people in the community. You contribute to your local economy directly and indirectly. Any time you volunteer—which most community bankers do regularly—you change your corner of the world for the better.

Something else we share with heroes from the past: Nobody succeeds entirely on his or her own.

The three earlier stories focus on self-starters with plenty of talent. But they were also well-connected. Royal influence, teachers, financiers, and other scientists' discoveries helped tip the scales in their favor.

While financial institutions compete with one another in some ways, we do business in the same "universe" when it comes to the technology infrastructure we use. All financial institutions must pull together to maintain a safe operating environment. No one can go it alone. It's simply in our self-interest to support the collective good by staying educated, working with our industry counterparts and regulators on risk mitigation, and following best practices.

This is doable. And to broaden your educational options, Bankers' Bank of the West will hold a **Conference on Cybersecurity in Community Banking** (page 3) in Denver July 16-18. Geared to community banks, the program will feature roundtables, dual-track sessions, networking opportunities, and speakers with varied and extensive expertise. I urge you to download information (**bbwest.com)** and register ... for the benefit of your bank and the continued well-being of the financial services industry.

TAKING NOTE

ACKNOWLEDGMENTS

At the Bankers' Bank of the West Bancorp Inc. annual shareholder meeting held in April of this year, three directors were recognized for completing their service on the holding company board. BBW staffers add this public thank-you for the wisdom, integrity and commitment these directors brought to their five-year terms:

Byron Maynes, recently retired president of First National Bank in Cortez, Colo.; **Dennis Schardt**, chairman of Exchange Bank in Gibbon, Neb.; and **Kent Shurtleff**, director of Wyoming Community Bank in Riverton, Wyo.

Three newly elected directors were elected to the board during the same meeting. Their names are followed by an asterisk in the list at right. Welcome, gentlemen!

RESOURCES FOR AND ABOUT BANKING

The Industry Analysis section of the FDIC website (**fdic.gov**) provides access to reports, sponsored research papers, historical information, issues analysis, press conference videos, and a plethora of data in various formats including graphs, sortable tables with hyperlinks to institution information, and spreadsheets.

The **Quarterly Banking Profile** published by the FDIC includes a section on community bank performance. In addition to recaps of net interest margin, net income, loan balances, and asset quality movement during the quarter (and at times year-over-year), the section provides hyperlinks to supporting charts and tables.

In the Find More Information window on the right side of the screen, visitors can subscribe to email notifications that indicate when new resources are posted to the site.

FEEDBACK SOUGHT ON AMENDMENT TO REG CC

On May 31, the Federal Reserve Board issued a call for public comments on an additional proposed amendment to Regulation CC aimed at settling burden of proof issues in certain disputes over check forgery. A press release with details is posted to **federalreserve.gov** under the News & Events section. Comments (identified by Docket No. R01564) must be submitted by Aug. 1.

ABOUT

Correspondent Views is published by Bankers' Bank of the West for independent community banks in our service area. Downloadable versions are posted to our website. If you prefer to receive newsletters by email, send your request to **info@bbwest.com**.

Headquarters:
Bankers' Bank of the West
1099 18th St., Ste. 2700
Denver, Colorado 80202
303-291-3700 | 800-873-4722

BBW Bancorp, Inc. Board of Directors

Richard J. Fulkerson .... Chairman of the Board
Betzer Call Lausten & Schwartz LLP ▪ Denver, Colo.

Gary Crum* .... Director
Western States Bank ▪ Laramie, Wyo.

Mark Daigle* .... Director
First National Bank ▪ Durango, Colo.

Mike C. Daly .... Director
First State Bank, a Div. of Glacier Bank ▪ Wheatland, Wyo.

John "JV" Evans III.................................. Director
D. L. Evans Bank ▪ Burley, Idaho

Zac Karpf .... Director
Platte Valley Financial Cos., Inc. ▪ Scottsbluff, Neb.

Debbie L. Meyers..................................... Director
Bank Strategies LLC ▪ Denver, Colo.

William A. Mitchell Jr. .... Director
Bankers' Bank of the West ▪ Denver, Colo.

David A. Ochsner .... Director
Commercial Bank ▪ Nelson, Neb.

Roger R. Reiling .... Vice Chairman of the Board
Bankers' Bank of the West (retired) ▪ Denver, Colo.

Dawn M. Thompson................................. Director
First Western Financial, Inc. ▪ Denver, Colo.

Max T. Wake* .... Director
Jones National Bank & Trust Co. Seward, Neb.

Alan D. "Pete" Wilson .... Director
Wray State Bank ▪ Wray, Colo.

ON THE TECH SIDE

Tips and tricks for commonsense patch management

Brandon Minow ▪ Systems Administrator
Bankers' Bank of the West

An often annoying but inevitable fact of our technology-dependent existence (see page 6) is the need to manage patches. To stay organized and efficient, maintain a record of patches deployed. Your log should contain at least:

✓ Software/hardware patch name and version number.

✓ Date the patch was released.

✓ The target computer; user name.

✓ Date the patch was deployed.

✓ Any conflicts with other software on the network.

SCOPE. Remember that workstations, laptops, servers, and mobile devices need to be patched. In addition, regularly check network hardware—like routers, switches, and firewalls.

PREPARATION. It's not safe to assume every patch released by a vendor is safe to deploy. Tech news sites and social media will probably be the first places you'll learn about a patch going bad. Reputable organizations like the SANS Institute typically release an official warning later. It's always a good idea to conduct some research before deploying a patch.

FREQUENCY. Set up your patching routine. Do you want to patch 25% of the servers every weekend? Would you rather do everything once a month—or once per quarter? Document your routine and keep records.

UPKEEP. Audit your environment regularly—once a year at minimum—and remove any unused software and hardware dependencies. Software that is not installed won't need to be patched in the future!

CONFERENCE ON CYBERSECURITY IN COMMUNITY BANKING

July 16-18, 2017 · Denver ▪ Grand Hyatt Downtown

reduced room rate
EXPIRES SOON

REGISTER NOW

Download more information, logistics and registration form at WWW.BBWEST.COM

Select topic outlines

Next Generation Email Defense

John Devenyns, Vice President of Cyber Security Consulting
BAE Systems Applied Intelligence

Attackers keep sending cunningly deceptive messages, and users continue falling for them. John will discuss the current email security threat landscape, share best practices for protecting users from email-borne threats, and explain how big data and machine learning is being used to protect against attacks.

Cybercrime and Hacking Techniques & Prevention

Brett Johnson, Former USA Most Wanted Cybercriminal
AnglerPhish Security

Considered one of the best social engineers in the world (and nicknamed "the original internet Godfather"), Brett served a 7½ year sentence in federal prison. Today he brings a unique grasp of cybercrime and a wealth of knowledge to assist others in staying safe online.

Enterprise Immune System: Using Machine Learning for Next-Generation Cyber Defense

Jesse Hood, Account Executive
Darktrace

Find out how new immune system technologies are being used to learn the "self" of an organization, spot abnormal activity as it emerges, and even take precise, measured actions to curb threats already inside the network—before they become a full-blown crisis.

Trends in Cybercrime

Isaac Barnes, Assistant to the Special Agent in Charge
United States Secret Service

Hear about the types of cybercrimes occurring on the national level and the profiles of varied groups and individuals responsible for them. Also learn about the Colorado Electronic Crimes Task Force, a collaborative "ecosystem" of organizations and people committed to cybersecurity.

Emerging Cybersecurity Threats and Risks

Ron D. Hulshizer, Managing Director-IT Risk Services
BKD, LLP

Ron will talk about current and ongoing threats and risks in the banking cybersecurity world, discuss the weakest link in cybersecurity, review regulatory hot buttons for banks, and present the top ten best practices banks should consider to help manage risk.

This conference is made possible through the support of sponsors: **BAE Systems · Darktrace**

Blazing-the-trails concept extends to the sharing of knowledge and expertise

The education lineup for BBW's 2017 Bank Card Conference in Black Hawk, Colo., consisted of ten large-group presentations and two optional training sessions—a full agenda to be sure.

The speakers at the May 3-5 event took on a variety of topics, cited data from many sources, and brought unique perspectives to card-related advancements, studies and issues. One theme that surfaced often and prominently throughout the program was fraud.

Several presenters touched on that theme in relation to their specialized topic, each attacking fraud from a different angle. They pointed out what to watch for, analyzed data on breaches, shared tools and tactics for mitigating losses, and shed light on the contemporary hacker's mindset and tactics, among other things.

The net effect of these layered perspectives was a clear and memorable message—namely, fraud is ever-present in the marketplace, within our country and throughout the world.

Speaker **Jim Foster** (PULSE) identified escalating fraud as one of today's top macro debit trends. He noted that the share of debit losses attributable to specific points of compromise is shifting over time.

Brett Johnson, a former fraudster and current cybercrime educator, offered an expert view of current-day hazards—some of the more notable crime types being card not present, account takeover, prepaid debit cards and bank drops, and synthetic fraud. In addition, he discussed a dozen nefarious tools used by criminals and a number of weaknesses they commonly exploit.

Also the program were topics unrelated to fraud. **Evan Abbott**, Mountain States Employers Council, spoke about creating accountability within an organization's culture.

STAR Network's **Brian DuCharme** referenced census data and consumer/business studies to identify key advantages that local businesses enjoy over national chains. He shared seven examples of specific, easy-to-execute, low-cost strategies for building loyalty and leveraging the strengths of businesses within the community.

Many thanks to all of the 2017 conference speakers, sponsors and participants who made the event a success. See you next year!

Preliminary comments on the recent update to the Cybersecurity Assessment Tool

On May 31, the Federal Financial Institutions Examination Council (FFIEC) issued an update to the Cybersecurity Assessment Tool.

Changes have been made to the following:

- In the **Cybersecurity Maturity** section, management can respond to declarative statements with **Y**es, **N**o, or **Y(C)**, the last of which indicates "yes, with compensating controls." This is significant because while many institutions may not meet the specific requirement of the statement in a domain, some do have controls in place that perform the same function.
- **Appendix A** has been totally revised. Each area of Baseline in the Cybersecurity Maturity is now mapped to a corresponding piece of the FFIEC IT Examination Handbook booklets.

These things were not changed:

- **Inherent Risk Profile** remains the same with respect to the way it is quantified; the matrix to determine the level of Cybersecurity Maturity needed is unchanged as well.
- Cybersecurity Maturity question quantity has not changed.

More in-depth information will be made available by compliance firms and by Bankers' Bank of the West. Contact Anne Benigsen, First VP – Information Security & Technology for BBW, to find out more: **info@bbwest.com**.

Business and consumer trends show it's a small world after all

Debbie Wendt, SVP–Operations
Bankers' Bank of the West

Even Americans who love their jobs—you're one of them, no doubt—usually look forward to getting out and about each summer. Some venture farther than others. The National Travel and Tourism Office (**tinet.ita.doc.gov**) reports that 2016 spending by U.S. citizens on international travel—for business and pleasure —to every region of the world exceeded prior-year spending. By providing essential international services at competitive prices, BBW helps community banks keep up with the growing needs of retail and business customers alike.

The **International Currency** template on BIDS allows you to arrange shipment of currency orders to any of your branches. After you complete the fields for currency type, name of the customer requesting the currency, and amount needed, the screen will return the rate for the currency type chosen and convert to the US Dollar amount. More than 90 currencies are available, and most currency orders placed by 3 pm Mountain Time are delivered the next day.

BBW facilitates corporate **Wires** and offers a consumer wire transfer solution that automatically generates consumer disclosures as required by Dodd-Frank. More than 70 currencies are available; some restrictions apply. Templates are available on BIDS for sending recurring wires, helping you to ensure accuracy, maintain consistency, and save time.

Draft Orders—issued on accounts in the beneficiary's country—are available in a variety of currencies. BBW's operations specialists are available by phone or email (**ops@bbwest.com**) to provide you with information on specific currencies and restrictions that might apply.

Whether your summer destination is nearby or far-flung, make happy memories ... and be safe!

ACH Audit: Two-Part Course (each 90 minutes)

Led by WesPay Payments Association Trainers*

This webinar training will review every ACH participant's audit points, providing specific information on how to properly test for compliance, and suggest "sound practices" to be incorporated into existing policies and procedures. The review of compliance with ACH audit requirements has been identified as a key priority for examiners under guidelines published by the Federal Financial Institutions Examination Council (FFIEC).

PART ONE	June 22 (Thurs.)	1^{00} pm Mountain	2^{00} pm Central
PART TWO	June 30 (Fri.)	1^{00} pm Mountain	2^{00} pm Central

* These sessions have been scheduled for BBW customers. Email ops@bbwest.com for enrollment & pricing info.

2017 OPERATIONS CONFERENCE: the next five years

BANK to the future

August 23 & 24 ▪ Denver ▪ Marriott Gateway Park

Change is rapid and unstoppable in the modern bank operations environment. By anticipating and adapting to those shifts, you can pave the way for success.

This conference will explore some key changes expected over the coming five years. Speakers will discuss where we're headed on payments, regulatory requirements, the demographics (and expectations) of customers and other stakeholders—and offer a fresh take on galvanizing tomorrow's workforce to carry community banking forward.

PREVIEW OF TOPICS (subject to change)
Evolution of the Payments System
Vendor Management as an Audit Requirement
Customer Succession Planning
Panel: What Millennials Look for From a Financial Services Provider and Employer
Internally Developing Staff at All Levels

Registration to begin soon. For updated information, visit NEWSROOM/EVENTS at **BBWEST.COM**

LEARNING MOMENTS

WCry: Don't shed tears … instead, adhere to best practices

Anne Benigsen, CISSP ▪ First VP – Info Security & Technology
Bankers' Bank of the West

So the talk of the tech community since May has been the WannaCry (WCry) ransomware attack, which exploited critical vulnerabilities in Windows computers. In reaction, anti-malware and anti-virus companies have been pushing their big-ticket wares, and a glut of pricy webinars concerning the threat have sprung up.

Let's start with some **facts** about the incident:

- WCry coul**d** be the largest coordinated ransomware attack in history.
- It originated with the National Security Agency, which did not inform Microsoft of the exploit. The exploit was discovered by a hacker group known as Shadow Brokers.
- An estimated 200,000+ computers in more than 150 countries were stricken.
- A kill-switch, discovered by chance, stopped the attack before it could impair critical systems around the world.

Moving on to a few **lesser-known details**:

- Old operating systems weren't the ones primarily infected. Over 98% of the affected machines were Windows 7. (Microsoft did provide a patch for all operating systems Windows Vista Plus and Windows Server 2008 Plus.)
- It not only held computers and data for ransom; WCry also installed a backdoor, Double-Pulsar, which had to be removed as well.
- Most if not all victims who paid the ransom did **not** get their files decrypted.
- The hackers reportedly made less than $100,000 off WCry.

And finally, the **best preventive** techniques:

- Don't click on links in spam emails or those that appear even remotely suspicious.
- Patch software and hardware regularly.

That's it. This stunningly short list of easy-to-implement tactics can stop most malware, ransomware, and other malicious cyber-hazards.

The WCry incident illustrates why social engineering tests are important. It's why you should never roll your eyes when told to be careful about phishing emails. And it's why doing those patches—even though they take some time and require a reboot—is a must. As long as you consistently follow both preventive tactics, most malware will never get a foothold.

If you have related questions or want to know more, contact Anne at **303-291-3700**.

PATCHING TIPS: PAGE 3

1099 18th Street ▪ Suite 2700
Denver, Colorado 80202

CYBERSECURITY
CONFERENCE **UPDATE** (p. 3)
reduced room rate
EXPIRES SOON