ICBA Education

Certification News

December 2023

Quarterly Newsletter for ICBA Certified Community Bankers

Financial Crime Fighters: Unsung Heroes of Banking Security

by Teri Wesley, Thompson Consulting Group, LLC

There are Federal Reserve holidays every banker looks forward to for that extra day off work when banks close. If only every day were a holiday. According to the National Day Calendar, there are 1,500 (more than four each day) "national" holidays. These mostly self-serving holidays that someone made up (or paid the company behind National Day Calendar to promote) are fun and, in some cases, bring awareness to various causes. For example, the first Wednesday in October is National Coffee with a Cop Day, National Online Bank Day is the second Monday in October, International Credit Union Day is the third Thursday in October, and National Hero Day is celebrated October 8th, to name a few. **Did you know that October 26 is "National Financial Crime Fighter Day?"**

Continued on page 2

How I Work with Lisa C. Cronk

Lisa C. Cronk is a Compliance/Audit Control Officer for Lake Elmo Bank in Minneapolis, Minnesota.

Q. Tell us your background/ how you got here.

A. I fell into banking when my eldest child was born. I was looking for something closer to home rather than commuting into the cities for my accounting position at a large public service company. That was over 25 years ago. Since that time, it's been an adventure where I learn something new every day.

Q. Briefly describe how you construct your day for optimal productivity.

A. Each day I research and answer questions like, "can we," "how do we," and "what do we need" for staff, making my days diverse. I also conduct internal audits and reviews of various areas, functions, and departments within the bank.

National Financial Crime Fighter Day was started by financial software providers Bankers Toolbox to recognize the Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) professionals who work tirelessly to protect the financial industry from financial crimes. But for those who work in bank security, every day is financial crime fighter day. Just as our everyday heroes – military, firefighters, police officers – go through rigorous training before they are placed out in the field, bank security officers don't become crime-fighting superheroes overnight.

The Bank Protection Act requires "periodic training and retraining of officers and employees in their responsibilities under the [bank's] security program." Pursuant to section 3 of the Bank Protection Act of 1968 (12 U.S.C. 1882), member banks are required to adopt appropriate security procedures to discourage robberies, burglaries, and larcenies, and to assist in the identification and prosecution of persons who commit such acts. In the late 1980s, the Act's language established very exact minimum standards for vaults, safes, and night depositories:

1. Vaults constructed after Nov. 1, 1973, should have walls, floors, and ceilings of reinforced concrete at **least 12 inches in thickness**. The vault door should be made of steel at least 3.5 inches in thickness or be made of other drill and torch-resistant material. It should be equipped with a dial combination lock, a time lock, and a substantial lockable day gate.
2. Safes constructed after Feb. 15, 1969, **should weigh at least 750 pounds empty** or should be securely anchored.
3. Night depositories constructed after Feb. 15, 1969, should consist of a receptacle chest having cast or welded steel walls, top, and bottom, **at least 1 inch in thickness**, a steel door at least 1.5 inches in thickness with a combination lock, and a chute made of steel that is at least 1 inch in thickness securely bolted or welded to the receptacle and to a depository entrance of strength similar to the chute. Night depositories should be equipped with a burglar alarm and be designed to protect against fishing of deposits.

The bank protection act required an alarm system or other appropriate device for notifying the nearest law enforcement officers of an attempted robbery or burglary. The act also required that the alarm be equipped with an independent source of power, such as a battery backup supply power for at least 24 hours.

The regulation also states that the board shall **designate a security officer** who is responsible for developing and implementing a written security program for the bank's main office and branches that shall:

Continued on page 3

Q. How do you keep track of what you have to do?

A. I love my calendar and electronic files. We use Office 365 within the bank and I love the ability to create tasks so I'm able to track my progress on projects, audits, and reviews.

Q. Take us through a typical workday.

A. I don't know that I have a "typical" day, other than the hours I'm in the building. Each day, or hour for that matter, can bring something new to my "desk." One minute I could be answering or researching how to handle a special deposit account and the next I could be answering a question on a potential loan product, then it could be an online banking question.

Q. What tools/software/ resources can't you live without?

A. Office 365 and Teams give me the ability to manage, track, and access my projects, tasks, and research from various electronic devices.

Q. Can you share a problem/ challenge you're working on or trying to solve?

A. The big compliance challenges we face right now regard how to meet the requirements of Section 1071 without impacting our customers and the changes to CRA. From an internal audit standpoint, another challenge is meeting the financial statement audit requirements and testing of controls.

Q. What's the best advice you have for other people in your role?

A. Don't take any of the challenges or issues personally and assure management and staff that you are there to support them. Our job as compliance

i. **Establish procedures for opening and closing** for business and for the safekeeping of all currency, negotiable securities, and similar valuables at all times.
ii. **Establish procedures that will assist in identifying persons** committing crimes against the institution and that will preserve evidence that may aid in their identification and prosecution. Such procedures may include but are not limited to maintaining a camera that records activity in the banking office; using identification devices, such as prerecorded serial-numbered bills, or chemical and electronic devices; and retaining a record of any robbery, burglary, or larceny committed against the bank.
iii. **Provide for initial and periodic training** of officers and employees in their responsibilities under the security program and in proper employee conduct during and after a burglary, robbery, or larceny; and
iv. **Provide for selecting, testing, operating, and maintaining** appropriate security devices, as specified in paragraph (c)(2) of this section.

The current language found in 12 CFR 208.61 – Bank Security Procedures Section (C)(2) is broader in scope today than it was in the 80s and makes no effort to provide technical design specifications for vaults, safes, or electronic surveillance systems. Instead, it says under Security Devices that banks shall have, at a minimum, the following security devices:

1. **A means of protecting cash and other liquid assets**, such as a vault, safe, or other secure space.
2. **An alarm system or other appropriate device** for promptly notifying the nearest responsible law enforcement officers of an attempted or perpetrated robbery or burglary; and
3. **Such other devices as the security officer determine to be appropriate**, taking into consideration: the indigence of crimes against financial institutions in the area, the amount of currency and other valuables exposed to robbery, burglary, or larceny, the distance of the banking office from the nearest responsible law enforcement officers; the cost of the security devices; other security measures in effect at the banking office; and the physical characteristics of the structure of the banking office and its surroundings.

Over the years, the role of bank security officers has undergone significant changes due to advancements in technology, evolving threat landscapes, and shifting customer expectations. **Here are just a few key ways their role has transformed:**

Continued on page 4

officers and internal auditors is to identify the risks and recommend controls that would reduce those risks. When I was starting out in this business, I had someone tell me that my job was to locate the potholes in the road and to make suggestions on how to fix them.

Q. What are you currently reading?

A. I am currently reading "True Believer" by Jack Carr. I love a good mystery thriller.

Q. Who are the people who help you get things done?

A. Everyone. It is definitely a team effort. Supervisors, managers, and the doers of whichever function I'm reviewing are the real experts that can answer my questions or show me how they are utilizing the systems in their day-to-day job functions.

Q. What is your favorite thing about the Annual Current Issues Certification Conference?

A. I love the Annual Certification Conference. The networking and sharing of knowledge are the biggest draw to me. I love being able to talk with everyone about which systems they are using and how they are using them for their own processes. The wealth of knowledge and willingness to share and brainstorm possible controls or procedures for given situations is so helpful for this department of one.

Q. How has your designation affected your career/ role at the bank?

A. The designation helps demonstrate the ability and willingness of an individual to be a lifelong learner, along with the desire to achieve a higher standard of excellence in a field.

- **Emphasis on Cybersecurity:** With the rise of online banking and digital transactions, bank security officers now play a critical role in ensuring robust cybersecurity measures are implemented. They are responsible for safeguarding sensitive financial data, detecting, and responding to cyber threats, and regularly updating security protocols.
- **Enhanced Physical Security:** Despite the growing importance of digital security, physical security remains vital for banks. Today's bank security officers have embraced advanced surveillance systems, access control technologies, and biometric authentication methods to protect physical premises, cash handling areas, and ATMs.
- **Threat Intelligence and Risk Assessment:** Bank security officers now use advanced analytics tools and threat intelligence platforms to proactively identify potential risks. They conduct comprehensive risk assessments, evaluate vulnerabilities, and develop strategies to mitigate emerging threats.
- **Collaborative Approach:** Bank security officers now work closely with law enforcement agencies, regulatory bodies, and cybersecurity firms to gather intelligence, share information, and maintain up-to-date knowledge about evolving threats and best practices.
- **Crisis Response and Incident Management:** Bank security officers are trained to respond swiftly and effectively to security incidents, ranging from physical threats to cyberattacks. They coordinate emergency preparedness drills, develop incident response plans, and collaborate with internal stakeholders to minimize disruptions and ensure customer safety.

The role of these financial crime fighters has become more proactive, encompassing both physical and digital security domains. Ongoing training is more essential than ever for today's bank security officers. Well-trained security officers are crucial to ensuring the safety and security of your banks, customers, and the bank's assets. Through comprehensive training programs, officers gain a deep understanding of physical security, cybersecurity, fraud prevention, crisis management, and risk assessment techniques. In addition, training helps security officers and related staff member stay up to date with the latest security technologies and systems used in the banking industry. This includes surveillance systems, access control systems, intrusion detection systems, and cybersecurity tools.

The most effective training fosters teamwork, collaboration, and communication skills that are all necessary for coordinating efforts with other staff members, law enforcement agencies, and third-party security providers. Don't put your security officer out in the field without the crucial training that ensures they are well-equipped with the knowledge, skills, and awareness required to address diverse security challenges, comply with regulations, and prioritize customer safety. It is an ongoing process that helps security officers stay prepared and adaptable in an ever-changing security landscape.

ICBA Annual Current Issues Certification Conference

A four-day conference that focuses on key issues and trends related to auditing, BSA/AML, regulatory compliance, and security and fraud.

Day 1: Auditing issues
Day 2: Lending & Deposit Compliance issues
Day 3: BSA/AML issues
Day 4: Fraud & Physical Security issues

Register now for enlightening presentations, insightful Q&A, plus the opportunity to learn from and engage with your peers and instructors. Attend one day or all four to stay in the know and earn live CPE to maintain your certification.

Sept. 23-26
Nashville, TN

Oct. 21-24
Livestream

2024 Certification Calendar

Stay current and earn CPE to maintain your certification.
Check out our in-person and livestream options for 2024.

Certification Institutes			ICBA Member	Non-Member	Non-Banker
Audit Institute	May 14–16 & 21–23*	Livestream	$3,299	$4,199	$4,799
	Sept. 8–13	Bloomington, MN			
Bank Security Institute	Feb. 27–29	Livestream	$1,699	$2,199	$2,699
	Aug. 27–29	Bloomington, MN			
BSA/AML Institute	May 7–9	Bloomington, MN	$1,699	$2,199	$2,699
	Aug. 6–8	Livestream			
	Nov. 5–7	Dallas, TX			
Commercial Lending Institute	Aug. 18-23	Bloomington, MN	$2,299	$2,999	$3,999
Compliance Lending Institute	Feb. 25–March 1*	Dallas, TX	$2,899	$3,799	$4,699
	June 4–6 & 11–13*	Livestream			
	Oct. 6–11	Bloomington, MN			
Consumer Lending Institute	Sept. 24–26	Livestream	$1,699	$2,199	$2,699
Credit Analyst Institute	April 16–18	Livestream	$1,699	$2,199	$2,699
	Aug. 11–14	Dallas, TX			
IT Institute	Sept. 29–Oct. 3	Dallas, TX	$2,699	$3,599	$4,499
Risk Management Institute	TBA	Bloomington, MN	$1,699	$2,199	N/A

***Indicates an Institute is split over two weeks.*
If you wish to test for certification, the testing fee is $500 in addition to the registration fee.

Newsletter Sponsored By: ICBA Education