COMMUNITY BANKER UNIVERSITY®
powered by ICBA

Newsletter for Audit, Compliance, Security, IT, Credit Analyst, Lending, and BSA Officers

Summer 2017

CERTIFICATION NEWS

TECHNOLOGY

Ransomware: Hackers Target Middle Market

By Alain Marcuse

Recent ransomware incidents have made global headlines, with a wave of unprecedented attacks infecting companies worldwide. While many banks and their small to mid-sized business customers think they are not a target for cyberattacks and are too small to interest hackers, the opposite is actually true. The ransomware threat is very real and risks are more prevalent for smaller companies than larger organizations because of differences in the depth of resources and education.

Ransomware typically spreads through extensive email campaigns sent by a hacker, and does not target a specific business. If a user clicks on a link or attachment, a malware program launches that locks a computer's screen with a message communicating that files have been encrypted. That message also presents a ransom note, detailing the amount necessary (typically via bitcoin) to unlock files before they are permanently destroyed. This amount often increases over time, for example doubling after three days.

*See **Ransomware**, page 2*

PROFESSIONAL PROFILE

Get to Know Samantha L. White, an ICBA Certified Banker in Mississippi

By Shirley Ringhand

Samantha L. White is assistant vice president, compliance and CRA officer at Merchants & Farmers Bank in Holly Springs, Miss. She became a Certified Community Bank Compliance Officer in 2007 and a BSA/AML Professional in 2012.

*See **Profile**, page 3*

Fact Check
Merchants & Farmers Bank

Headquarters: Holly Springs, Miss
Retail offices: Byhalia, Miss., Hickory Flat, Miss. and Ashland, Miss.
Bank asset size: $100 million
Number of bank employees: 36
Number of staff in auditing and BSA/AML: Four
Website: www.mandfbankshs.com

2017 CERTIFICATION CALENDAR ►

Audit Institute (Week 1)
- Sept. 11-15; Minneapolis

Audit Institute (Week 2)
- Sept. 18-22; Minneapolis

Annual Current Issues/ Certification Conference
- Sept. 25-28; Minneapolis
- Oct. 23-26; Baltimore

Bank Security Institute
- Sept. 10-13; Minneapolis

BSA/AML Institute
- July 31-Aug. 2; Chicago
- Nov. 13-15; San Diego

Community Bank IT Institute
- Aug. 7-11; Minneapolis

Compliance Institute
- June 11-16; Baltimore
- Oct. 1-6; Minneapolis

Consumer Lending Institute
- Sept. 17-20; Minneapolis

Commercial Lending Institute
- Oct. 1-6; Minneapolis

Credit Analyst Institute
- Aug. 20-23; Nashville

Ransomware *Continued from page 1*

Ransomware has become the most widespread security threat facing middle market companies, growing exponentially due to its simplicity of execution and its potential to collect large ransoms from victims. While traditional hacking is difficult, ransomware kits can be inexpensively purchased on the black market and require no technical skills. With large attacks launched indiscriminately, victims come directly to the attacker, rather than the hacker having to seek out targets, infiltrate systems, and locate and sell data.

Traditional hacking is often perceived as targeting large companies, but ransomware turns that structure on its head. Since ransomware is not a targeted crime, smaller companies - including community banks - are more vulnerable to attacks, because they typically have less sophisticated incident response, security awareness and system patching processes in place.

While the threat is very real, middle market companies can easily implement four key defenses to protect critical systems and files, and effectively counter ransomware threats.

Security awareness
Simply speaking, an educated staff is your best defense. A custom security awareness program helps your employees understand ransomware risks, what to look for and how to respond. The program should be continuous and updated to include new threats, tested with regular social engineering exercises, and engaging enough to help ensure widespread user adoption.

Patch management
The next line of defense against ransomware is to prevent infection should a user click on a malicious link. Symantec data recently found that 75 percent of breaches leverage exploits where a patch is available, and 78 percent of scanned websites exhibited known vulnerabilities.

Therefore, your organization should develop a comprehensive inventory of systems and applications in your environment, as well as a program to identify, prioritize and apply patches to software. Be sure to consider applications such as Microsoft Office, Flash and Java in addition to operating systems and antivirus programs.

Therefore, your organization should develop a comprehensive inventory of systems and applications in your environment, as well as a program to identify, prioritize and apply patches to software. Be sure to consider applications such as Microsoft Office, Flash and Java in addition to operating systems and antivirus programs.

System backups
Unfortunately, hackers and their methods are becoming increasingly sophisticated, and harmful emails and websites can look very legitimate. You must be prepared with robust data backup programs to address a ransomware attack if it happens to you. A comprehensive program includes data mapping to identify what and where data is, ensuring that backups are complete and offline from the network, and comprehensive, regular testing protocols to ensure the data can be restored.

Incident response planning
Decisions on whether to pay a ransom and how to respond should not be made in the middle of a crisis. Accordingly, an incident response plan and team must be established. The team should include a law firm, digital forensics professionals and public relations resources. Your plan should be tested and updated on a regular basis through tabletop exercises.

In addition, your organization should proactively decide on a stance toward paying ransom. Many middle market companies are setting up a bitcoin wallet in advance, as a precaution. Establishing a bitcoin account can take up to a week, and internal protocols can extend that timeline, creating a delay that could result in increased ransom or the outright loss of critical files.

Despite its explosive growth, many organizations may not fully understand the potential for ransomware infections within their systems. However, while middle market organizations are at an increased risk for these attacks, implementing proven defense measures can increase awareness, prevent attacks and effectively respond to potential incidents.

Alain Marcuse *(alain.marcuse@rsmus.com) is director of security, privacy, and risk services at RSM US LLP*

Profile, **continued from page 1**

What makes a community bank different from the largest banks?
White: The hometown atmosphere and the opportunity for our customers to get to know bank staff. Community bankers listen closely and respond quickly—a luxury not afforded by larger banks.

What makes you most proud of your bank?
White: The dedication and hard work of the staff. A great group of team players.

How did you find your way into banking?
White: I was formerly an administrative assistant for a public school and I needed a change. I quickly found that banking was the career for me.

Tell us your biggest and best accomplishment.
White: Completing Compliance and BSA/AML Institutes through ICBA that helped me advance my career at Merchants & Farmers Bank.

What do you like best about the work you do?
White: Working behind the scenes and really learning the intricate parts of banking. Also, helping fellow coworkers understand the laws and regulations for the success of the bank.

What's your best advice to a new bank employee?
White: Be a team player and do not be afraid of change. Seize positive opportunities when they are presented.

Shirley Ringhand *(shirley.ringhand@icba.org) is vice president of certification, seminars and the Bank Director Program at ICBA's Community Banker University*

Compliance Dates to Remember

Effective Date	Regulatory Change
Oct. 3, 2017	Military Lending Act (MLA) effective date for credit cards
Oct. 19, 2017	Mortgage Servicing Rules amendments effective date
Jan. 1, 2018	HMDA final rule effective date for provisions related to institutional and transactional coverage, data collection, recording, reporting, and disclosure; Lenders will collect the new information in 2018 and report it by March 1, 2019
April 1, 2018	Prepaid Card Rule effective date
May 11, 2018	Must comply with Bank Secrecy Act customer due diligence requirements (beneficial owner rule)

Have additional questions? Community Banker University staff members are happy to assist you. Contact us at 800-422-7285.

FinCEN Proposes Changes to the DoEP form

On June 13, 2017, the Financial Crimes Enforcement Network (FinCEN) published in the Federal Register a Notice and Request for Comments on a proposed update and renewal of the collection of information through the Designation of Exempt Person (DoEP) report used to designate eligible customers as exempt from CTR reporting requirements.

FinCEN is proposing to remove the reference to "Document Control Number", which is no longer in use, and add a country field to accommodate reporting from U.S. territories in Part II following current item 11, and part III following the current item 23.

Written comments are welcome and must be received by FinCEN on or before Aug. 14, 2017.

Flood Insurance Update

The House Financial Services Committee began marking up a set of flood insurance bills on June 15, 2017. The committee is considering seven bills that would overhaul the National Flood Insurance Program.

Not to be outdone by the House, the Senate Banking Chairman Mike Crapo (R-Idaho) and ranking member Sherrod Brown (D-Ohio) released a draft bill for a six-year reauthorization of the National Flood Insurance Program, which is set to expire Sept. 30.

ICBA is currently working with both the House and Senate to ensure a timely reauthorization without a lapse in the program. Compliance and lending staff are encouraged to keep an eye on this flood activity in the coming months.

ICBA
Independent Community Bankers of America®
PO Box 267
Sauk Centre, MN 56378
(800) 422-7285
RETURN SERVICE REQUESTED

2017 Annual Current Issues Certification Conference

Sept. 25-28; Minneapolis, Minn. • Oct. 23-26; Baltimore, Md.

Don't wait. Register today for this important conference! Designed for participants in ICBA's Auditing, Compliance, Bank Security, IT and BSA/AML certification programs, and other interested bankers, the agenda for this four-day conference is based on surveys completed by participants and topics relevant to community bank professionals. It's a great training and networking opportunity if you are in need of continuing education or just looking to be updated on key issues facing community banks today.

DAILY SCHEDULE

7:30 – 8 am	Registration
8 am – 4 pm	Program
Noon – 1 pm	Lunch

DAY ONE —
MONDAY, SEPT. 25 / OCT. 23
Auditing Issues

DAY TWO —
TUESDAY, SEPT. 26 / OCT. 24
Lending Compliance Issues

DAY THREE —
WEDNESDAY, SEPT. 27 / OCT. 25
Deposit Compliance and Bank Secrecy Act

DAY FOUR —
THURSDAY, SEPT. 28 / OCT. 26
Fraud, Physical Security, CyberSecurity & Technology

ICBA Member Fee:
Four-Day Conference: $1,295
Three-Day Conference: $995
Two-Day Conference: $695
One-Day Conference: $395

Nonmember Fee:
Four-Day Conference: $1,845
Three-Day Conference: $1,295
Two-Day Conference: $895
One-Day Conference: $495

Nonbanker Fee:
Four-Day Conference: $2,195
Three-Day Conference: $1,495
Two-Day Conference: $995
One-Day Conference: $595

For more information go to www.icba.org/education or call 800-422-7285.