COMMUNITY BANKER UNIVERSITY®
powered by ICBA

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

Fall 2017

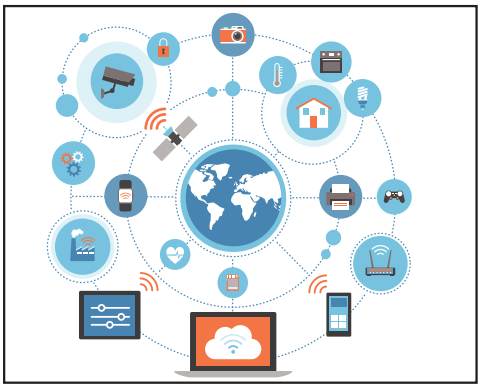
CERTIFICATION NEWS

TECHNOLOGY

Internet-Connected Devices + Lack of Oversight = Hacking Made Easy

By Alex Becker

Spurred by cheap Wi-Fi technology and eager businesses, the number of everyday household products with internet connectivity has exploded in recent years. These devices, collectively coined the Internet of Things (IoT), have a multitude of helpful applications. But due to the rise of global cyber threats, many experts worry that some manufacturers are rushing products to market without proper security standards in place.



Here's how the exploitation works

Take for instance, an internet-connected camera that consumers can use to view a video feed of Fido while they're on vacation or away at work. This same camera can be used by hackers to exploit security vulnerabilities into an IT network. Some cameras even have an online management interface, which gives easy access to the camera's feed for the consumer, but also to anyone who knows the device's weakness.

*See **Hacking Made Easy**, page 2*

PROFESSIONAL PROFILE

Get to Know Catrena Thompson, an ICBA-Certified Banker in Tennessee

By Shirley Ringhand

Catrena Thompson is a compliance officer and internal auditor at Citizens Savings Bank & Trust Co. in Nashville, Tenn. She became a Certified Community Bank Compliance Officer and BSA/AML Professional in 2015. In 2017 she became a Certified Community Bank Internal Auditor.

*See **Profile**, page 3*

Fact Check
Citizens Savings Bank & Trust Co.

Headquarters: Nashville, Tenn.
Retail offices: Three and one LPO/DPO
Bank asset size: $107 million
Number of bank employees: 38
Number of staff in auditing and BSA/AML: One
Website: www.bankcbn.com
Taglines/Motto: Over 100 Years of Promises Kept!

2018 CERTIFICATION CALENDAR

Audit Institute (Week 1)
- April 23-27; Kansas City, Missouri
- Sept. 10-14; Minneapolis, Minnesota

Audit Institute (Week 2)
- April 30-May 4; Kansas City, Missouri
- Sept. 17-21; Minneapolis, Minnesota

Annual Current Issues/ Certification Conference
- Sept. 24-27; Minneapolis, Minnesota
- Oct. 22-25; TBD

Bank Security Institute
- Sept. 9-12; Minneapolis, Minnesota

BSA/AML Institute
- May 15-17; Minneapolis, Minnesota
- July 30-Aug. 1; Kansas City, Missouri
- Nov. 14-16; Dallas, Texas

Compliance Institute
- Feb. 25-Mar. 2; Dallas, Texas
- June 10-15; Minneapolis, Minnesota
- Sept. 30-Oct. 5; Nashville, Tennessee

Commercial Lending Institute
- Aug. 19-24; Minneapolis, Minnesota

Consumer Lending Institute
- Sept. 16-19; Minneapolis, Minnesota

Credit Analyst Institute
- April 15-18; Minneapolis, Minnesota
- Nov. 4-7; Dallas, Texas

IT Institute
- Aug. 6-10; Minneapolis, Minnesota

Hacking Made Easy *Continued from page 1*

Compromised IoT devices can be controlled to build a network of "bots" to perform large scale distributed denial of service (DDoS) attacks on their targets. A DDoS attack is when the attacker commands the "botnet" to send large amounts of data to the victim's online server to render it inaccessible due to traffic overflow. As the number of IoT-connected devices surges (Gartner predicts 20 billion such devices by 2020), the popularity of botnet attacks on IoT devices will increase as well.

Government oversight gaining steam

A bipartisan group of U.S. senators recently introduced legislation to combat IoT insecurity, titled the Internet of Things (IoT) Cybersecurity Improvement Act of 2017. This legislation would define standards for internet-connected devices sold to government agencies. In its current form, the bill would require vendors to contractually state that the devices being sold to the government are patchable, do not contain any known vulnerabilities, utilize standard protocols and do not contain any hard-coded passwords.

The stipulated requirements are relatively basic security principles, which helps to illustrate the current security expectation surrounding IoT devices. The legislation does not cover standards for products sold to businesses and consumers outside of the federal government space.

How organizations should respond

Even if this legislation passes, there is still no widespread effort to ensure the devices are being implemented securely when they are installed in a business setting. Organizations will continually face competitive pressure to integrate these devices into their workflow. How to manage integration largely depends on having a robust cybersecurity posture.

Organizations with a mature security posture may already have regular procedures in place that identify weaknesses in new devices and harden the system before they are put into production. As more devices are introduced to their network, organizations without a robust IT security practice may struggle to handle the associated security implications.

If you haven't already, start building up your security framework in anticipation of this wave of technology. At a basic level, you should take measures to assess new devices for insecure configurations such as default passwords, outdated service versions and known vulnerabilities, so that these devices do not introduce security vulnerabilities into your environment. Then, once you have a device up and running, be sure to avoid the "set it and forget it" mindset.

How we can help

It is clear from recent events across the globe that organizations must take security into their own hands when incorporating third-party internet-connected devices into their network. Before you hook up a device, or to understand your readiness for the IoT wave, engage a professional to conduct a cybersecurity assessment and gain a thorough understanding of your network's security.

***Alex Becker** is a senior IT security consultant at CliftonLarsonAllen.*

Compliance Dates to Remember

Effective Date	Regulatory Change
Jan. 1, 2018	Effective date for final rule implementing changes to the Home Mortgage Disclosure Act (HMDA)
Jan. 1, 2018	Effective date for annual dollar threshold adjustments for Regulation Z
April 1, 2018	Effective date for final rule implementing requirements for prepaid accounts (Regulation E & Regulation Z)
May 11, 2018	Compliance date for FinCEN's beneficial ownership rule

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

***Profile*, continued from page 1**

What makes a community bank different from the largest banks?
The relationship that you develop with the people in your community and the opportunity to see firsthand the impact that you make.

What makes you most proud about your bank?
I am most proud that we are the oldest black-owned minority bank in the country. We've been helping our community for 113 years.

How did you find your way into banking?
A friend offered me a position as a loan processor. I accepted it, and I've been growing in banking ever since.

Tell us your biggest and best accomplishment.
In banking my biggest accomplishment has been earning my graduate degree in banking.

What do you like best about the work you do?
The opportunity to be impactful in our community. I love the feeling when a deal closes, and you have provided someone an opportunity to buy a home, start a business or build a community center. It makes me feel like I have made a meaningful difference.

What is your bank's customer-service philosophy?
Treat your external as well as your internal customers with respect and service you would want provided to you.

What's your best advice to a new bank employee?
Pay attention to detail.

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

Flood Insurance Extension Signed Into Law and New Legislation Pending

On Sept. 8, 2017, legislation extended the National Flood Insurance Program (NFIP) through December 8, 2017. The NFIP was set to expire on September 30, 2017. This action by lawmakers was merely a short-term extension in order to help emergency funding for areas affected by the recent hurricanes.

A long-term extension is currently being considered by lawmakers. As of November 14, 2017, the House voted 237-189 to reform and reauthorize the National Flood Insurance Program for five years. House passage of the 21st Century Flood Reform Act (H.R. 2874) sends the debate to the Senate.

If a longer-term extension of the NFIP is not finalized by December 8, 2017 and the NFIP lapses, we are hopeful the regulatory agencies will issue new guidance as to how to proceed with managing flood loans, or refer community banks to informal guidance previously issued by the regulatory agencies.

It is important to note that prior to the Biggert Waters Flood Insurance Reform Act of 2012, the NFIP was extended on a short-term basis multiple times and the program lapsed on four occurrences. At the time of NFIP lapse, the regulatory agencies issued informal guidance to institutions. In all instances, lenders were permitted to continue making loans subject to the flood requirements without flood insurance during the period when the NFIP was not available. Lenders were still required to make timely flood determinations, complete and provide accurate notices to borrowers, and comply with other parts of the flood regulations. Lenders were requested to have a system in place to ensure that flood policies were obtained as soon as available following NFIP reauthorization. Lenders were also reminded that safety and soundness considerations were still required when making all loan decisions.

Awareness of the changes and status of the NFIP coverage will be key for all community bank compliance officers as 2017 comes to a close. Given that loans secured by properties located in flood areas are a focus of most compliance examinations being prepared for a potential lapse in the NFIP can help reduce stress and confusion among bank staff.

Stay tuned for regulatory updates in the ICBA NewsWatch Today e-newsletter! To view past issues of NewsWatch Today or to subscribe visit www.icba.org/news/latest-news/newsletters.

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

Changes to CPE Requirements for Certified BSA/AML Professional Designation Coming

The continuing professional education (CPE) requirement for a Certified BSA/AML Professional (CBAP) designation is changing from 15 to 20 CPE credits effective Jan. 1, 2019.

Regulatory expectations, strict examiner scrutiny and heightened financial trends continue to increase since 2007, when the BSA/AML Certification Program was first introduced. To ensure all individuals maintaining the CBAP designation remain on the pulse of industry issues and emerging trends, the ICBA Certification Board recommended and approved an increase to 20 CPE credits. The board also approved adding BSA/AML curriculum to the Community Banker University portfolio and as such, ICBA will begin adding new BSA/AML CPE opportunities early next year.

As a reminder, participation in this certification program requires that you meet the described CPE credit requirements. You are required to complete at least 20 CPE credits in each two-year maintenance period. This change is effective with all two-year maintenance periods beginning Jan. 1, 2019, and thereafter.

I. Acceptable CPE Activities:
   - Live seminars or conferences must account for at least half of your CPE credits each two-year cycle. (10 credits). You will earn one CPE credit for every 50 minutes of classroom instruction for qualified seminars.
   - Webinars, computer based training, online courses, videos, DVDs and all other self-study courses related to the common body of knowledge can account for a maximum of half of the required CPE credits per cycle. (10 credits).

II. Reporting CPE Credits to Community Banker University.
   - You must report your completed CPE credits to Community Banker University in your online certification portfolio.

CPE credits cannot be reported more than once, and you cannot use them toward more than one certification unless directed by Community Banker University.