COMMUNITY INSTITUTION & ASSOCIATIONS RISK SUMMARY REPORT

Week of March 5

FINANCIAL SERVICES ISAC

TLP: Green | ACTL: Guarded | PTL: Guarded | Terrorism TL: Elevated | Follow Us

STOP | THINK | CONNECT™

In This Issue

News and Risk Information

Summary:

Below are some of the top news and risks that the Financial Services Information Sharing Analysis Center (FS-ISAC) has observed this week for community institutions (CI).

NEWS

One Suspect Still at Large for Attempted Jackpotting. Banks and credit unions in the Salt Lake City area can rest a little easier now that two more of the seven suspects accused of attempting to jackpot ATMs have been caught. *Fox13* out of Salt Lake City reports that law enforcement arrested one suspect in the middle of jackpotting an ATM, as the machine was spewing out cash; the latest two suspects were arrested after being tracked to a Miami airport, leaving the country. All suspects were from Venezuela and one remains at large.

Banks Battle Retailers Over Proposal to Disclose Consumer Hacks. In the years following the Target breach during the holiday season of 2013, several legislative bills were introduced that would require the same cybersecurity compliance and consumer data breach notification of retailers that are required of banks and credit unions under the Gramm-Leach-Bliley Act (GLBA). After a number of high-profile data breaches last year with delayed public notification, another bill has been proposed that would establish a federal mandate for when and how certain companies, like retailers, notify consumers of a data breach. The newest proposal, though, would exempt financial institutions because of the current GLBA requirements.

Equifax Discloses an Additional 2.4 Million Data Breach Victims. Credit reporting agency Equifax has identified another 2.4 million victims of the 2017 data breach. According to *BankInfoSecurity*, the data was not originally included because only portions of the driver's license number was taken; the state and other key elements of consumer records were not stolen.

Prepaid Card Scammer Caught. An Oklahoma man was charged with multiple felony counts of fraud and conspiracy after stealing or attempting to steal funds from several credit unions and a bank in Nebraska and Kansas. As told by *Credit Union Times*, the man presented "insufficiently funded" Green Dot Visa cards to institution staff and requested cash advances; when advances were declined, the man asked tellers to call a number on the back of the card, which went to a co-conspirator who reported there were sufficient funds on the card. All told, the scammers stole $25,000 from small community institutions.

RISKS

Applebee's Restaurants Suffer Payment Card Breach. POS systems at Applebee's in Alabama, Arizona, Florida, Illinois, Indiana, Kansas, Kentucky, Missouri, Mississippi, Nebraska, Ohio, Pennsylvania, Texas and Wyoming were infected with malware from December 6, 2017 to January 2, 2018. (Some restaurants' infection began on November 23 or December 5.)

This Week's Top Risks

- **Malware, Ransomware, Trojans**
  - Hawkeye keylogger
  - Gozi
  - Pony
  - Trickbot
  - DDoS attacks w/ extortion
  - CannibalRAT
  - GandCrab Ransomware
  - Adobe Flash zero-day vulnerability
- **Physical Security**
  - Two nor'easters hit New England
- **System Vulnerabilities (multiple)**
  - Google Android, Google Chrome, Cisco, TrendMicro, Microsoft
- **Themed Phishing Campaigns**
  - Bank-themed (multiple)
  - Microsoft account-themed
  - "Confirmation of payment"
  - Microsoft Word malspam

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is a non-profit corporation that was established in 1999. FS-ISAC is a member-driven organization whose mission is to help assure the resilience and continuity of the global financial services infrastructure and individual firms against acts that could significantly impact the sector's ability to provide services critical to the orderly function of the global economy. FS-ISAC shares threat and vulnerability information, conducts coordinated contingency planning exercises, manages rapid response communications for both cyber and physical events, conducts education and training programs and fosters collaborations with and among other key sectors and government agencies.

Adobe's Flash: Use in Malspam Campaigns Continue Despite its Decreased Use

Google shared statistics last week that Chrome users who encountered at least one webpage with Flash dropped from around 80% in 2014 to under 8% in early 2018. There are two primary reasons for this: first, since Adobe announced that Flash will no longer be offered or supported by the end of 2020, many web developers have already switched to using HTML5. As well, browsers have begun to require manual Flash initiation on webpages that use it rather than running the content automatically. However, these developments and the reduced usage of Flash have not impacted its go-to status with malicious spammers: a zero-day vulnerability (that was patched last month) is being reported in malspam Microsoft Word documents.

This Week's Threat: Memcached Servers Deliver Explosive DDoS

This Week: Record-breaking distributed denial of service (DDoS) attacks can be avoided

Summary:

Just a few years ago, the idea of a 10Gbps (10 gigabytes per second) DDoS attack was unthinkable. Then, in September 2012 multiple large and mid-sized financial institutions were hit with two 10Gbps DDoS attacks. That series of attacks brought the importance of information sharing for community institutions to light and the term "DDoS" to the public domain.

In October 2016, another unthinkable scenario occurred when hundreds of thousands of Internet-of-Things (IoT) devices were infected with Mirai malware and used to launch a massive 1.2Tbps (terabytes per second) DDoS attack against Dyn, a domain name service (DNS) provider. That attack caused interruptions of highly-used sites like Amazon, Etsy, Starbucks, Netflix and PayPal to name just a few.

At the time, a 1.2Tbps DDoS attack seemed impossible, other-worldly and, in a way, terrifying.

Records Are Made to be Broken

In just five short early-2018 days, the 1.2Tbps Dyn attack seemed old-fashioned. Last week, the highly-used software development platform GitHub sustained a 1.3Tbps DDoS attack. While this may not seem like a huge increase, the method was alarming.

Five days after the GitHub attack, and with heads still reeling, the 1.3Tbps record was broken with a 1.7Tbps attack against a US service provider, unnamed at this point. (For those still somewhat unimpressed, 1.7Tbps = 1700Gpbs, which is 170 times the amount financial institutions faced a scant five and a half years ago).

A New Vector and a New Message

These new DDoS attacks use Memcached servers available on the Internet to stage redirection/amplification attacks. The purpose of a Memcached server (memory cached) is to cache frequently used data to improve internal access speeds they are generally implemented in an internal data center and should only rarely be available on the Internet.

However, there are an estimated 50,000 to more than 100,000 vulnerable Memcached servers on the internet.

To stage DDoS attacks using these servers, attackers send a spoofed request (redirection) to the Memcached servers for a large amount of data (amplification). When the Memcached servers respond, they send the troves of data to the spoofed IP address, which is the victim's external IP or website. This flood of information bogs down the services of the receiving site.

One new, final twist is that the DDoS attack against GitHub contained an extortion note (aka ransom) in the data being delivered from the Memcached servers.

Risks to Organizations:

- Unnecessary ports, protocols or services on a firewall or other server or appliance is a pathway for multiple types of attack.
- DDoS attacks cause business interruptions that can affect an institution's reputation and transactions; as well, DDoS attacks can be staged to obfuscate more dangerous activity like illicit wire transfers. Finally, regulators are to be notified when such an attack is staged against a community institution.

Remediation:

- Block UDP traffic from Port 11211, the port used for communication from Memcached servers.
- If your institution has them, remove Memcached servers' access to the Internet.
- Conduct an internal DDoS risk assessment to determine the value of contracting with a DDoS mitigation provider; as well, plan and practice for a DDoS attack so all parties know their roles in the event of attack.

Google Chrome Vulnerabilities Patched

Multiple alerts have been issued regarding a vulnerability in Google Chrome that could allow arbitrary remote code execution. In the worst cases, sensitive information could be compromised, security restrictions could be bypassed to perform unauthorized actions, or a denial of service condition could be caused. Chrome released an updated version of its browser, 65.0.3325.146, for Windows, Mac and Linux. NCCIC/US-CERT encourages users and administrators to review the Chrome Releases page and apply the necessary update.

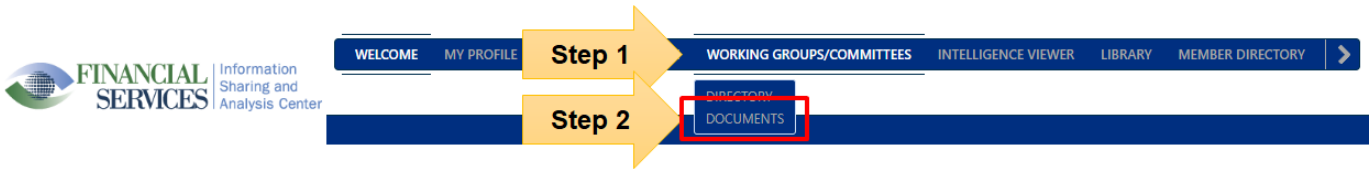
Tip of the Week: Portal Changes

FS-ISAC's Portal has been updated, learn how to find what you're looking for

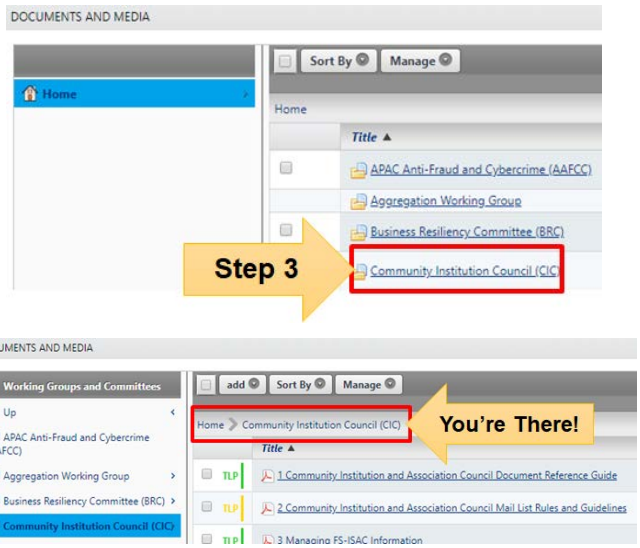
Summary:

FS-ISAC's Portal has gone through some changes and we want to be sure that are able to locate the documents that you need.

Once you are at the portal login page, authenticate using MFA credentials. Once you are logged in, select the "**Working Groups/Committees**" tab. A drop-down menu will appear; select "**Documents**."



Looking at the Documents and Media section, select Community Institution Council (CIC). Within this folder you'll find a tremendous amount of workpapers.



Regardless of whether you are a community bank or credit union, these papers are available for download and can be modified to meet your institution's policies or practices.

Within the CIC folder are subfolders. There are page numbers at the bottom of the webpage. Currently there are five webpages with 89 folders full of information available for your use.

We've attempted to put them in order by type. For example, you may require a checklist for ATM Jackpotting; one of the folders will be named ATM Jackpotting. Inside there you will find a checklist and other material for your use.

Looking for a policy? Visit the "Sample Policies" folder and you will find a wide arrange of documents.

Looking back at the menu at the top of the page, you'll see a "Library" tab. This will take you to a general documentation area. Members will most likely be interested in the "Member Services" folder where you can access the Automated Cybersecurity Assessment Tool (ACAT). Member points-of-contacts can access the "Membership Guide" and other tools to assist you in getting the most of your membership.

As you will note, there are other links you can take advantage of on the navigation bar. You can submit threats you want to share via the "Member Submission." Perhaps you are looking for a contact at another institution regarding a money mule; go to "Member Directory" and search for the institution or member name. To research FS-ISAC Analysis reports, go to the "Intelligence Viewer" where you can search by tracking ID number or keyword and download results.

If you have any ideas on how we can make your portal experience better, please let Member Services know at admin@fsisac.com.

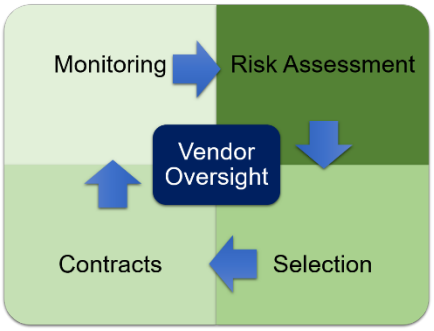
Vendor Oversight: Risk Management

Vendor oversight is amongst community bank and credit union regulator focus

Summary:

In part three, we will discuss the importance of risk management when outsourcing technology services. Risk management is the process of identifying, measuring, monitoring, and managing risk. Risk exists whether your institution maintains information and technology services internally or elects to outsource them. Regardless of which alternative you choose, your management is responsible for managing risk in all outsourcing relationships. Accordingly, institutions should establish and maintain an effective risk management process for initiating and overseeing all outsourced operations. An effective risk management process involves several key factors:

- Establishing senior management and board awareness of the risks associated with outsourcing agreements to ensure effective risk management practices;
- Ensuring that an outsourcing arrangement is prudent from a risk perspective and consistent with the business objectives of the institution;
- Systematically assessing needs while establishing risk-based requirements;
- Implementing effective controls to address identified risks;
- Performing ongoing monitoring to identify and evaluate changes in risk from the initial assessment; and
- Documenting procedures, roles/responsibilities and reporting mechanisms.



Risk Management incorporates these ongoing activities.

Before signing a contract, management should:

1. Ensure the contract clearly defines the rights and responsibilities of both parties;
2. Ensure the contract contains adequate and measurable service level agreements;
3. Ensure contracts with affiliates clearly reflect an arms-length relationship and that costs and services are at least as favourable to the institution as those available from a non-affiliated provider;
4. Choose the most appropriate pricing method for the financial institution's needs;
5. Ensure the contract does not contain provisions or inducements that may have a significant, adverse effect on the institution;
6. Engage legal counsel to review the contract; and
7. Evaluate foreign-based third-party service providers considering the guidance found in this section and in Appendix C, Foreign-Based Third-Party Service Providers.

The above process focuses on risk elements specifically associated with outsourcing, but today many small organizations require products to compete with peer and larger financial institutions. Financial institutions must understand the complex nature of arrangements with outside parties and ensure adequate due diligence for the engagement of the relationships and ongoing monitoring.

Regardless of whether the financial institution's control procedures are manual or automated, internal controls should address the areas of transaction initiation, data entry, computer processing, and distribution of output reports. These control considerations apply to these products. The FFIEC provides resources for supervising technology service providers as well as retail payment systems, with which each institution should familiarize themselves.

Next week we shall discuss performing risk assessments.

Questions:

If you have any questions about this week's report, please contact Community Institution & Associations. Content provided for internal use by FS-ISAC members. Copyright owners retain all copyrights to material referenced.

Member Services:
admin@fsisac.com
Toll-Free: 877-612-2622 – prompt 1 Outside US: 1 571-252-8517

FS-ISAC Analysis Team:
IAT@fsisac.com
Toll-Free: 877-612-2622 – prompt 2

For more TLP White about FS-ISAC information, follow us on Twitter @FSISAC and join the discussion on LinkedIn.