Achieving Compliance with NCUA Audit Requirements

Notes Pertaining to this Version (Revised Draft • 09/21/16):

- Changes made to the First Draft to emphasize an asset inventory and authentication are highlighted.
- All comments are welcomed, including suggestions for graphics; questions [???] and requests for specific input are highlighted in yellow.
- Previous notes that remain pertinent:
  - The proposed approach is to write a product-specific problem/solution white paper that could easily (and optionally) be repurposed into a generic contributed article if desired.
  - Intended Audience: Business and Technical Decision-makers at Credit Unions
  - Target Length: 4-6 Pages

Introduction

When asked by a reporter why he robbed banks, Willie Sutton supposedly answered, "Because that's where the money is." If Sutton were alive today, he might prefer to use a PC instead of gun to commit his robberies.

In addition to money, financial institutions also hold valuable member information that makes them a primary target for cyberattack. Among private sector breaches investigated by Verizon in its *2016 Data Breach Investigations Report*, the financial industry ranked second behind only the entertainment industry with 1,368 and 2,707 confirmed breaches, respectively. Of the 2,260 total security incidents with confirmed data loss, the financial industry ranked first with 795 incidents, representing over one-third of the total.

These attacks impose an increasing financial toll on vulnerable financial institutions. According to the Ponemon Institute's *2015 Cost of Cyber Crime Study*, the financial services industry experienced the greatest losses of the 18 different industry sectors studied, with a total average annualized loss of $13.5 million.

To address this growing threat, the National Credit Union Administration (NCUA) has published IT security regulations, and offers a variety of cybersecurity resources and assessment tools. These share two important and related requirements with other regulations, such as those from the Federal Financial Institutions Examination Council and those contained in the Gramm-Leach-Bliley Act. The first requirement is for a complete and accurate inventory of all endpoints authorized to be connected to the network. The second is to ensure that every one of these endpoints is adequately authenticated before being granted network access.

This white paper, intended for both business and technical professionals, outlines some of the challenges credit unions now face implementing adequate cybersecurity, and explains how endpoint and IoT (Internet of Things) connection security—a layer of security that the NCUA itself uses—can help achieve full compliance with the regulations.

[Optional Sidebar???] The *NCUA Audit Survival Guide: How to Pass an IT Audit* by ERM Security notes: "As you probably have noticed, the Federal Financial Institutions Examination Council is increasingly focusing on cybersecurity in its assessments, and you should expect this to continue. In the past, many auditors would skip over the IT portion of an assessment, but that has all changed. Today's focus on cyber assessments means that when the auditors come onsite, they will look under the hood and focus on the cybersecurity plans of your organization."

New Challenges in Cybersecurity

In its Supervisory Priorities for 2016 letter, the NCUA made Cybersecurity Assessment its top priority: "Cybersecurity threats continue to represent significant potential operational risks to financial institutions. Cyberattacks are expected to increase in frequency and severity as worldwide interconnectedness grows and the capabilities to conduct cyberattacks become more sophisticated and easier for criminals or terrorists to obtain. As in 2014 and 2015, NCUA will continue to carefully evaluate credit unions' cybersecurity risk management."

The applicable regulations are contained in *Title 12 (Banks and Banking) Chapter VII (NCUA) Subchapter A (Regulations Affecting Credit Unions) Part 748 (Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance) of the Code of Federal Regulations (CFR)*.

In addition to protecting credit union offices from robberies, burglaries, larcenies and embezzlement, the regulations include this requirement that applies to cybersecurity: "Ensure the security and confidentiality of member records, protect against the anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member."

Additional requirements involve responding to incidents of unauthorized access, assisting in the identification of the persons committing or attempting such actions and crimes, and preventing the destruction of vital records. Specific regulations are outlined in *Part 748 Appendix A (Guidelines for Safeguarding Member Information)* and *Appendix B (Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice)*.

To assist member credit unions in complying with these regulations, the NCUA worked with other agencies of the Federal Financial Institutions Examination Council (FFIEC) to produce a Cybersecurity Assessment Tool and offers a Cybersecurity Resources Page its Website.

The multiple layers of defense-in-depth network security provisions employed by credit unions to comply with NCUA regulations—including firewalls, user authentication and network access controls, intrusion protection and data loss prevention systems, anti-virus software, and others—have proven to be reasonably effective. But the frequent reports of successful attacks and breaches demonstrate that while these security provisions are all necessary, they are no longer sufficient. Indeed, according to Verizon's 2016 Data Breach Investigations Report, "No locale, industry or organization is bulletproof when it comes to the compromise of data."

A significant cybersecurity challenge faced by all organizations today, including credit unions, involves the expansion of the attack surface based on the growing number of devices now being connected to networks. Perhaps the most notorious are the Bring Your Own Device (BYOD) smartphones and tablets employees now use to work both at home and in the office. But the growth in network-attached devices also includes Voice over IP (VoIP) phones, printers, document scanners, security cameras, HVAC controls and many other "things" in the so-called Internet of Things (IoT). Every one of these endpoints should be identified in the asset inventory (including the BYODs) and authenticated before being granted authorized access.

How big is the problem of such device proliferation? The Air Academy Federal Credit Union (see sidebar) found that it had over 5,000 endpoints on its network that spans 10 locations, including two data centers. After installing an endpoint and IoT connection security solution, most organizations report finding substantially more networked endpoints than estimated—often more than twice as many.

Not only are many of these endpoints completely unknown to the IT department and, therefore, not in the inventory, many lack the ability to be authenticated by traditional network access control provisions, or to be protected by traditional PC-based security software. Such a lack of endpoint visibility—and, therefore, lack of connection control—makes it difficult to comply with NCUA cybersecurity regulations, and that can become rather obvious during the audit.

[Mini Case Study Sidebar] **Air Academy Federal Credit Union**

Since its founding in 1955, the Air Academy Federal Credit Union has grown to nearly 43,000 members worldwide with total assets of almost $500 million. AAFCU wanted a solution that exceeded the compliance requirements for semi-annual NCUA audits, and after an exhaustive evaluation, found it in the Beacon endpoint and IoT connection security suite. Beacon now provides real-time visibility and behavioral monitoring of all connected devices across the credit union's entire network of eight branches and two data centers. AAFCU also uses Beacon to detect and prevent MAC spoofing.

Getting into Compliance with Endpoint and IoT Connection Security

The Cybersecurity Assessment Tool notes that cybersecurity controls can be preventive, detective or corrective. The Beacon endpoint and IoT connection security suite from Great Bay Software provides all three capabilities.

More specifically, the Beacon Endpoint Profiler and Beacon Endpoint Enforcement products help comply with these specific provisions included in Appendix A to Part 748 Section III (Development and Implementation of Member Information Security Program) Paragraph C1 (Manage and Control Risk):

- Access controls on member information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing member information to unauthorized individuals who may seek to obtain this information through fraudulent means
- Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into member information systems

- Response programs that specify actions to be taken when the credit union suspects or detects that unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies

The Beacon suite provides a separate layer of security that is purpose-built to address the vulnerabilities created by the many intelligent devices being deployed on networks. This layer of protection includes four separate but complementary capabilities:

- *Detecting* every device on the network and assigning it an identity in a profile
- *Onboarding* every device securely using critical factors in its profile
- *Monitoring* the network to detect when any device is exhibiting uncharacteristic behavior
- *Enforcing* access restrictions as needed to thwart an attempted breach

Detect All Devices

Eliminating any vulnerability begins with visibility, and that requires detecting and identifying every single endpoint on the network. Beacon Endpoint Profiler is designed to find all IT, IoT and other devices automatically, without any exceptions and without requiring an agent or any special software running on any device. This ensures the credit union's ability to comply with the requirement to have an up-to-date and comprehensive inventory of all devices, systems and equipment authorized to connect to the network.

To operate transparently, Beacon Endpoint Profiler employs a variety of standard techniques to detect whenever a device connects to a network, including a "MAC notification" or a "link-state" trap from an Ethernet switch, or whenever any device requests an IP address, such as via the Dynamic Host Configuration Protocol (DHCP). These events can all be detected using commonly-deployed traffic monitoring and management provisions, such as packet inspection, NetFlow, SNMP (polling/traps), as well as via integrations with commonly-available third-party data sources, such as Active Directory.

Detecting devices connected to the network is relatively straightforward. The more meaningful and difficult aspect of endpoint profiling involves identifying and categorizing appropriate behavior for the many different devices. For this aspect of profiling, Beacon has amassed the industry's most comprehensive Warehouse of Context® that provides contextual insight on every device listed in the IEEE's official MAC (Media Access Control) address registry. The Beacon Warehouse of Context contains over 1200 pre-defined endpoint profiles that Beacon uses to determine the identity and categorize the behavior of all devices found on the network. The assignment of these profiles employs a combination of vendor data and other identity values, including behavior, and each profile is continuously assessed to either confirm or change it to maximize the level of certainty.

Onboard All Devices Securely

MAC addresses have another critical role to play during onboarding: authenticating those devices that lack an agent or supplicant required for IEEE 802.1X authentication and some network access control (NAC) systems. When onboarding non-authenticating endpoints, most NAC solutions provide a means for granting access based on a pre-approved list of MAC

addresses. Access control is normally enforced at the point of network access, which is inevitably a port on a switch (where Wi-Fi access points also connect) through support for a feature like Cisco's MAC Authentication Bypass (MAB). When a port is unable to authenticate a newly-connected device using 802.1X, it will attempt to authenticate the device using its MAC address as the equivalent of a username/password credential.

Because Beacon Endpoint Profiler knows the MAC address and identity of all attached devices, each can be granted a pre-determined level of network access, which might initially be limited to a restrictive network segment. Once the device's profile is fully and accurately determined, it can be moved automatically to its designated network segment. All devices that are not pre-approved are either blocked from gaining any access or placed in "quarantine" in an isolated virtual LAN (VLAN), depending on the credit union's security policy.

It is important to note the Beacon endpoint and IoT connection security suite enables administrators to assign network access privileges with full knowledge of what each device is and, therefore, what its legitimate functions should be during onboarding. The result is a much more granular and secure method of using MAC authentication to establish and enforce access privileges and/or restrictions.

> [Sidebar] **Blocking Access by Rogue Devices**
>
> Most people, including credit union employees, now have home networks configured with Ethernet hubs and Wi-Fi routers. It's easy to do, so the employee might think, "What could be the harm in setting up a similar "cubicle area network" at work for personal or business use?" The networking equipment and any devices connected might seem harmless to the employee, but each creates an additional vulnerability. Beacon Endpoint Profiler detects every such device connected to the network, and if the MAC address is not on the approved list, access will be blocked. [Is this true for both an Ethernet hub and Wi-Fi router???]

Monitor All Device Behavior

The profile in the Beacon Endpoint Profiler is what identifies what each device is and how it should behave on the network. The Beacon Endpoint Enforcement system then continuously monitors network communications to detect any unusual or non-conforming behavior that might be symptomatic of an internal or external attack, or a malware infection.

Because the profiles for any device can be made quite restrictive, attempts to perform certain functions or access specific resources are relatively easy to detect. For example, a device with a proprietary operating system suddenly identifying as a general-purpose PC would indicate a potentially threatening change in its behavior. Even more threatening would be a device attempting to upload files via an outbound FTP (File Transfer Protocol) session, or trying to access a controller or a switch via the Telnet or Secure Shell (SSH) protocols.

Enforce Access Security

The Beacon Endpoint Enforcement system offers administrators a choice of both manual and automatic enforcement actions. At a minimum, the system is usually configured to issue an alert whenever a new device that has not been pre-approved attempts to connect to the network, or

when an approved device's identity changes in certain ways. Manual intervention is then required to further investigate the incident and take corrective action as warranted.

Automatic enforcement actions often accompany the issuance of an alert, especially for behavior that is deemed to be threatening. Examples include, in order of increasing severity, requiring the device to re-authenticate, quarantining it in an isolated and restrictive VLAN, or blocking its access entirely by sending a request to the switch to shut down the port.

Stopping a "MAC Attack"

MAC spoofing is a simple technique that is capable of circumventing certain network security provisions, including segmentation and isolation with VLANs and firewalls that are commonly used to comply with NCUA regulations. Changing a device's MAC address is actually quite easy, and software is readily available on the Internet to enable anyone or any malware subroutine to do so. It should come as no surprise, then, that this technique is regularly employed by hackers during attempts to gain unauthorized access.

An attack usually begins with malware that monitors network traffic for valid MAC addresses. The hacker could just make up a MAC address, but access would be blocked immediately by Beacon's MAC authentication provisions. Such monitoring activity normally goes undetected because the device is merely listening to legitimate traffic.

The threat escalates when the malware spoofs a valid MAC address and attempts to access resources on the network. This traffic can, of course, be detected by a variety of means, including those employed by the Beacon endpoint and IoT connection security suite.

Here is a typical sequence of events leading to an endpoint profile change based on device identity. Note how the profile change is made as soon as the spoofed device attempts to access networked resources:

- The malware changes the MAC address on a PC to that of a known printer
- This change causes the PC to disconnect from and reconnect to the network
- Using its "new" MAC address, the PC (now a "printer") issues a DHCP request to get a new IP address
- Beacon sees the DHCP request as a normal event and authenticates the "printer" (based on information contained in the asset inventory) for access to the same VLAN as the server containing the member database
- When the "printer" begins to communicate, NetFlow sends information about the traffic to Beacon
- Because "printers" should not be initiating communications with servers, Beacon changes the device's profile
- The profile change causes Beacon to generate an alert and, if so configured, to initiate an enforcement action to block access

[Mini Case Study Sidebar] **Randolph-Brooks Federal Credit Union**

Randolph-Brooks Federal Credit Union has more than 335,000 members throughout Texas and total assets exceeding $4 billion, ranking it in the Top 25 of nearly 7,700 financial cooperatives. RBFCU

simply wanted a tool to enable network administrators to have a complete inventory of all devices connected to the networks at its 35 facilities, and chose Beacon Endpoint Profiler for its powerful detection capabilities and ease of use. But after discovering Beacon's full potential, the network security team now uses the suite to help comply with cybersecurity regulations.

Conclusion

NCUA cybersecurity regulations are at once detailed and vague. The dozens of pages outline what needs to be done, but not how to do it in a compliant manner. The result is tremendous flexibility and unnerving uncertainty for the IT department. Will the multiple layers of traditional defense-in-depth security provisions be sufficient? Could the department fail to pass an audit based on discovery of a single endpoint unknown to the staff?

The Beacon endpoint and IoT connection security suite is purpose-built to help eliminate the vulnerabilities being created by the proliferation of networked devices. Working in concert with the existing network infrastructure, Beacon builds the device inventory by immediately detecting and adding any endpoints that are not already included, authenticates each endpoint according to its profile and the security policy during onboarding, continuously monitors their activity to identify uncharacteristic behavior that might be symptomatic of an attack, and takes immediate enforcement action to thwart a breach as it is occurring.

Even the most meticulous of auditors is likely to be satisfied, if not impressed, with the powerful capabilities afforded by this additional layer of security—especially after being reminded that the NCUA uses Beacon to secure its own network.

To learn more about how Beacon Endpoint Profiler and Beacon Endpoint Enforcement can help you comply with NCUA regulations and pass cybersecurity audits, please visit Great Bay Software on the Web at www.greatbaysoftware.com.

# # #