Secure Guard Consulting

20 Cybersecurity Controls Every Community Bank Should Implement

Kaushal Kothari
Secure Guard Consulting
(515) 229-5674
kkothari@sgcsecure.com
www.secureguardconsulting.com

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

- About Me
  - Certified Ethical Hacker
  - Former FDIC IT Examination Analyst
  - 20+ years of technology experience
- Audit
  - Internal Security Assessment
  - External Security Assessment and External Penetration Testing
  - Cybersecurity / IT General Controls Review
  - Social Engineering (phishing, phone, etc.)

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

- *Cybersecurity is a constant, never ending and always changing moving target. Keeping up to date and on top of security controls can be a daunting task.*
- *20 key cybersecurity controls that every community bank should implement.*

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

1) Domain Registrar and 2) DNS

- Domain Registrar
  - You register a domain (e.g., amazon.com) through Domain Registrars.
  - Examples Registrars include GoDaddy.com, Network Solutions
  - Find yours: https://www.whois.net/
- Name Servers
  - At the domain registrar, every domain must enter two pieces of information called the name servers.
  - Name Servers tell everyone where to look for DNS records of the domain.
- DNS – Domain Name System
  - Sometimes stored at the registrar, sometimes elsewhere
  - Find yours: https://mxtoolbox.com/DNSLookup.aspx
  - Specifies A Records: Instead of memorizing 67.225.130.234 (or typing https://67.225.130.234/), it's easier to type https://secureguardconsulting.com
  - Specifies MX Records – where incoming email should go to.
  - https://dnsspy.io/
- Implement 2 factor authentication to both of these, or at a minimum, monitor any changes using some automated method.

Secure Guard Consulting

(515) 229-5674
kkothari@sgcsecure.com

- Anti-Spear Phishing Controls
- Kaushal Kothari <kkothari@sgcsecure.com>
- Kaushal Kothari <asdf@kfjlqetf.kz>

(515) 229-5674
kkothari@sgcsecure.com

3) Sender Policy Framework (SPF)

- SPF stands for Sender Policy Framework, a record on the DNS which specifies what IP address, IP address ranges, and/or domains can send email on the domain's behalf.
- Make a list of all the domains the bank owns.
- For the domain that is used to send outbound email, identify if an SPF record is already created or if one doesn't exist by searching for it (https://mxtoolbox.com/spf.aspx).
- If one exists, ensure the record is correct and make sure it's a hard fail (-all)
- If one doesn't exist:
  - Gather IP addresses that are used to send email. For example
    - Web server
    - Online Banking
    - Exchange Server or wherever email is hosted
  - Then use this information to create an SPF record:
    - https://mxtoolbox.com/SPFRecordGenerator.aspx
- v=spf1 mx a include:_spf.hostedemail.com include:mail1.pcsbanking.net -all
- For domains the bank owns that do not send email, the SPF record should indicate no one can send email from this / these domain(s) and should be set to a hard fail. Here's an example record for a non-sending domain:
  - v=spf1 –all
- Publish your SPF records to their respective DNS

Secure Guard Consulting

(515) 229-5674
kkothari@sgcsecure.com

4) DomainKeys Identified Mail (DKIM)

- DKIM works by attaching a digital signature to the header of an email message. The header is generated by the outgoing mail server and is unique to the domain hosted on the server. The receiving mail server can check the header against a public key stored in the sending server's DNS record to confirm the authenticity of the message.
- If DKIM isn't set up, https://www.sparkpost.com/resources/tools/dkim-wizard/
- For domain used to send outbound email
  - Choose a DKIM selector
  - Generate a public-private key pair
- Store private key securely
- Publish the selector and public key by creating the DKIM TXT record
- Attach the token to each outgoing email.
- For domains the bank owns that aren't used for outbound email, there is **NOT** a need for a DKIM record.

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

5) Domain Message Authentication DMARC

- Implement a DMARC record for all domains the bank owns.
- Look up your DMARC: https://mxtoolbox.com/dmarc.aspx
- If no DMARC, then generate a DMARC: https://mxtoolbox.com/DMARCRecordGenerator.aspx
  - v=DMARC1; p=quarantine; rua=mailto:skothari@ironshieldweb.com; ruf=mailto:skothari@ironshieldweb.com; fo=1:d:s; pct=100
- Best to have both SPF and DKIM, but if only SPF, then it's still ok. DMARC works by saying, if SPF checks pass **OR** DKIM checks pass, then DMARC checks pass.

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

6) Spam Filters

- Make sure the bank's spam filters are checking DMARC records. Or, at a minimum, performing SPF checks **AND** taking action on them.

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

7) Disable Web Based Email

- Either disable web-based email entirely, or restrict web-based email to only those who need it, and
  - for those who need it, enable 2FA
  - Implement country level blocks also, if option is available.
- Utilize app passcodes for other mobile devices.

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

8) Manage User Access

- As a financial institution, we should know who has access to what.
- Manage user access across all systems.

	A	B	C	D	E	F	G	H	I
1		Core System	Atm	Compliance One	Online Banking Admin	Wire Transfer	ACH	Network	Web Filtering
2	person1					20000 limite			
3	person2								
4	person3								
5	person4								
6	person5								
7	person6								
8	person7								
9	person8								
10	person9								
11	person10								

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

9) Vendor Management – Enhanced Due Diligence

- Apply your standards to your network support vendor; and any vendor with remote login capability.
  - How often are they patching their networks?
  - Are they reviewing their firewall rules periodically?
  - How often are they doing information security training?
  - Are they running simulated phishing campaigns and other social engineering attacks?
  - https://secureguardconsulting.com/templates/SecurityControlsQuestionnaire.docx

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

10) Information Security Training

- Train your users, at a minimum, quarterly.
- Run simulated phishing campaigns internally.
  - Generic monthly
  - Targeted quarterly
- KnowBe4 isn't a replacement for traditional training (e.g., onsite information security presentation).
  - Have your employees put themselves in the hacker's role.
  - Then have them create phishing attacks.
- Utilize something like Spoof Card (https://www.spoofcard.com/) to demo phone attacks.
- Banners at the top of emails work for about a month. Consider rotating them from the top of an email to the subject line and back again each month.
- Note on KnowBe4:
  - Disable sending links in reminders for training
  - If PhishAlert, disable sending emails to KnowBe4

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

11) Simple Wire Transfer Hack

- Hackers have figured out that banks with more than 1 branch will often have wire transfers initiated and verified at the main location.
- In-person wire transfers from branch locations are often emailed or faxed to the main location.
  - Both of these methods are subject to spoofing.
- Hackers have gotten a hold of wire transfer forms, made them look like in-person wire transfers, and either by email or fax, spoofed them to the main location.
- Do a callback to branches when receiving wire transfers, or use some other authenticated system to verify authenticity.

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

12) Password Managers

- Identify a password management solution and extend it to all bank personnel.
  - KeePass
  - Password Safe
  - LastPass
  - Thycotic

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

13) 2 Factor Authentication (2FA)

- Establish project to enable 2 factor authentication on everywhere possible.
- Also, identify where ftp is enabled and disable it wherever possible (e.g., ShareFile).

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

14) Hardware and Software Inventories

- In some automated manner, maintain an inventory of current hardware and software, beyond what is provided by your network support vendor.
  - **PDQ inventory**
  - Vulnerability scanning, if scanning the whole subnet, is another method

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

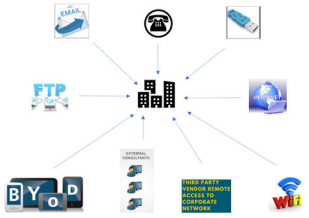
Secure Guard Consulting

Cybersecurity versus IT

(515) 229-5674
kkothari@sgcsecure.com

15) Bank's Attack Surface

- Show your Board all of the bank's external points of connectivity.



(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

16) Incident Response Testing

- Incident response roundtable (e.g., FS-ISAC CAPS Exercises, FDIC vignettes – Cyber Challenges, other testing)
  - FS-ISAC Cyber-Attack Against Payment Systems (CAPS) Exercises
    - https://www.fsisac.com/events/caps-na19-1
    - Next one appears to be 1-2 October 2019
  - FDIC Cyber Challenges – Vignettes: https://www.fdic.gov/regulations/resources/director/technical/cyber/purpose.html
  - Other testing
    - It's 8:30am, Jim has just clicked a link in an email. What actions should Jim take?
      - Unplug ethernet on devices when there's something suspicious.
        - Label ethernet cables with some type of bright electrical colored tape.
      - Leaving devices powered on.
      - Employees should know precisely who they should contact and what actions they should take.

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

17) Security Information and Event Management

- How do we know if we've been hacked?
- Implement Security Information and Event Management (SIEM) solution on internal critical servers.
- If costs are an issue, then implement, at a minimum, basic Log Event Monitoring (LEM) on your own.
  - ManageEngine – LogAnalyzer
- If you have a SIEM implemented, make sure to understand what is being monitored and what escalation procedures are in place.
- Research what else might need to be monitored.
  - https://www.beyondtrust.com/blog/entry/windows-server-events-monitor

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

18) Know How You Will Respond

- How do you remove a device connected to the network?
  - If you're small enough, you might have inventories in place such that you know where each IP is at.
  - If not, how are you going to do it? More importantly, how will your network support vendor do it?
- Based on subnet, identify switch(s), obtain MAC, obtain Port, Shut off Port
- Block all incoming and outgoing traffic related to offending device.

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

19) Rogue Device Detection

- How do you detect when rogue IP's are on the network?
  - Using PDQ Inventory, Nessus, or similar – this might be too late
  - Implementing full Network Access Control
  - Scope Level Link Layer Filtering
    - https://blogs.technet.microsoft.com/teamdhcp/2012/09/15/scope-level-link-layer-filtering-using-dhcp-policies-in-windows-server-2012/
  - Using solution like ARP Watch to catch static IP assignments

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting

20) IT / IS Succession and Strategic Plans

- Don't forget the IS portion in Succession Planning.
  - Risk Assessment
    - IT
    - CAT
  - Policies
  - Annual GLBA report
  - Vendor Management
  - Oversight of ISP
- Strategic Planning
  - Employee IS training – 5 years
  - IT / IS staff training – 5 years

(515) 229-5674
kkothari@sgcsecure.com

Secure Guard Consulting


Secure Guard Consulting
Subscribe to Internet Storm Center
(515) 225-5674
kkothari@sgsecure.com