Management Briefing for Kerndt Brothers Savings Bank

CliftonLarsonAllen
IT ENHANCED MANAGED SERVICES

Bryan Reynolds, Technical Director
Bryan.Reynolds@CLAconnect.com
John Moeller, Principal
John.Moeller@CLAconnect.com

Current Technology Environment

- Legacy Network Technology Based Upon Design Strategies from early 2000s.
  - VMWare ESX Servers, NetApp SAN, Server 2008 R2, Citrix, Mixed desktop environment, and Microsoft Office.
- Fiserv Precision is In House.
- Do Not Have a 3-Year Strategic Technology Plan.
  - Risk of continuing outdated design strategies leading to performance and reliability issues, cybersecurity breaches, and decline in employee productivity.
- Lack of Comprehensive of Cybersecurity Strategy.
- Some Basic (significant) Information Security Controls are Lacking (10-D report).

Current Technology Environment

- Comparison to Peers ($250M-$300M asset size)
  - Current Technology is About Average (50th percentile).
  - Lack of a Strategic Technology Plan (50th percentile).
  - Lack of a Cybersecurity Strategy (50th percentile).
  - Lacking Some Basic Information Security Controls is less than Average (35th percentile).
- Comparison to IT EMS Peers ($250M-$300M asset size)
  - Current Technology is Less than Average (35th percentile).
  - Lack of a Strategic Technology Plan (25th percentile).
  - Lack of a Cybersecurity Strategy (35th percentile).
  - Lacking Some Basic IS Security Controls (10th percentile).

Current Technology Support Environment

- Use RSM IT-Vision for Network Support
  - Break/Fix – reactive not proactive.
  - Like Knowledgeable Support Staff – do not want to take a step back in knowledge.
- Peggy Provides First Line Support and Core Banking Application Support.
  - Would like to do more and is willing to learn.
- Various Vendors for Phone, Printer, WAN Communications.
  - Can Lead to Some Finger Pointing. Need Outside IT Support Involvement in Many Cases.

CLA Advantage – Philosophical Change

- CLA Client Relationship Begins With Focusing on Your Daily Support Needs.
  - IT Enhanced Managed Services.
    - ◊ We Are FI Industry Focused.
    - ◊ Hire Experienced Professionals – no entry level hires.
    - ◊ Hire Bankers and Banking Consultants.
    - ◊ Low Turnover – Builds Relationships.
    - ◊ Hire People That Value Long Term Relationships.
    - ◊ 1 Service Desk Analyst For Every 5 FI Clients. 1 Director/Manager for every 6 FI Clients. Industry Ratio is Over 1:50.

CLA Advantage – Philosophical Change

- IT Enhanced Managed Services.
  - ◊ Obsessive Focus on Melding Strategic Technology Planning with Cybersecurity Strategy:
    - Vulnerability Management Process, Quarterly Network Scans,
    - All Scans Reviewed by CISSP,
    - Progressive Patching Methodology.
  - ◊ Requirement to Meet the Evolving Maturity Level in all Categories Within the 5 Cybersecurity Framework Domains – 12 months.
  - ◊ Focused on Simplifying Networks and Making Them Less Complex – Complexity = More Costly to Support, More Technology That Breaks, Frustrated Employees, Diminished Confidence in Management.

Proactive Approach

- Named Client Engagement Team
  - John Moeller (Relationship, Strategy, Cybersecurity).
  - Bryan Reynolds (Relationship, Strategy, & Design).
  - Jeff Mathews (Strategy & Design).
  - Desi Wren (Service Desk Supervisor).
  - Primary Service Desk Analysts (To Be Named).
  - Amy McHugh (IT Policies, Risk Assessment, ISO Advisory).
- Technology Advisory & Strategy (TAS).
  - Strategic Technology Assessments.
  - Core System Selection, Contract Review & Negotiation.
  - Outsourced CIO.

Proactive Approach

- Strategic Technology Plan That Integrates Cybersecurity Plan.
  - Expand to Include Telecommunications, Core Banking Applications, Physical Security, and Other Technology.
- Educate Executive Manage and the Board of Directors on Their Responsibilities to Oversee the Bank's Cybersecurity Program.
  - Employee Cybersecurity Training.
- Find Better and More Efficient Ways To Work By Analyzing Monthly Service Requests.

Proactive Approach

- National Service Desk
  - Monitor Alerts from N-Able Managed Services Software.
  - Open Tickets Online, Email or by Phone.
  - Proactive Fix instead of Break/Fix.
  - Weekly Ticket Aging.
  - Follow Service Desk Best Practices.
- Monthly Reports on IT EMS Activities.
  - Executive Summary Report, Patch Management Report, Remote Control Log Report, Antivirus Report, Hardware Inventory Report, Software Inventory Report and Custom Reports.
  - Review of Monthly IT EMS Invoice and Work in Process (WIP). Identify Trends and Opportunities to Reduce Support Time.

Proactive Approach

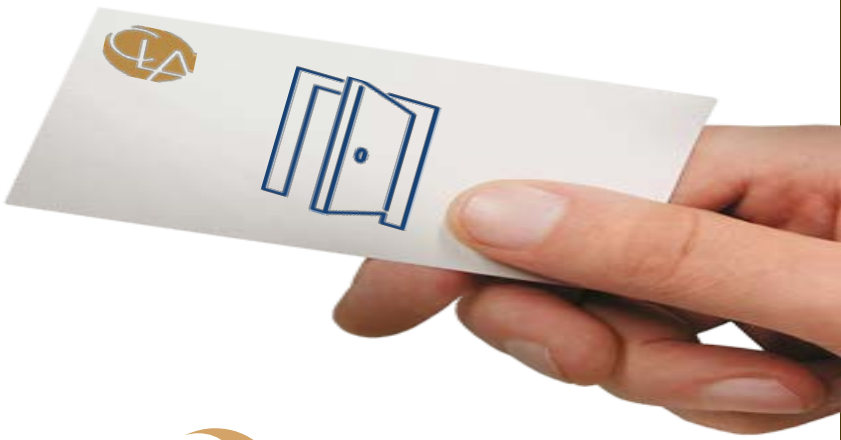
- Named Client Engagement Team.
  - John Moeller (Relationship, Strategy, Cybersecurity).
  - Bryan Reynolds (Relationship, Strategy, & Design).
  - Jeff Mathews (Strategy & Design).
  - Desi Wren (Service Desk Supervisor).
  - Primary Service Desk Analysts (To Be Named).
  - Amy McHugh (IT Policies, Risk Assessment, ISO Advisory).
- Technology Advisory & Strategy (TAS).
  - Strategic Technology Assessments.
  - Core System Selection, Contract Review & Negotiation.
  - Outsourced CIO.

Our Recommendations

- Begin the Kerndt Brothers Savings Bank and CLA with IT Enhanced Managed Services.
- After the First Month of Support Conclude a Strategic Technology Assessment in At Least the Following Areas:
  - Backup/Disaster Recovery
  - Data Circuits and Voice Circuits
  - Remote Network Access.
  - Mobile Device Management.
  - Remote Desktop
  - Server/Thin Client Strategy
  - Hyper-Convergence
  - Private Cloud (Data Center)
  - Overall System Performance and Capacity
  - Cybersecurity

Network Design Considerations

- Cloud Computing
- High Availability
- Performance Enhancements
- Reduce Complexity
- User Perceived Network Speed Improvement
- Ability to Identify Local Area Network Congestion
- Network Resiliency
- Shorten Recovery Times from Malware, Disaster, etc…
- Scalable for Business Growth
- Support Core System Changes
- Cybersecurity Framework Expectations



Cloud Computing – High Availability Observations

- The cloud is the hot “new” technology.
- The cloud is nothing more than a data center somewhere within the continental United States with software provided as a service (SaaS).
- The cloud can be used to host applications (SaaS) or hardware as a service (HaaS) that the bank’s servers run on.
- Sold as a way for Banks to shift technology responsibilities to the cloud provider.
- The bank pays a monthly invoice and all of their IT issues go away or so you are told.
- The cloud provider becomes the “one stop shop” for the bank.

Cloud Computing – High Availability Reality

- The cloud is expensive.
  - Moving all network servers and storage to the cloud can be 1.5 to 3X more expensive compared to bank owned hardware and software.
  - Unpredicted costs – adding/changing servers, increasing resource requirements.
  - May have to pay for software subscriptions on software the bank already owns such as MS Office, MS Outlook and server OS.
- Performance Inconsistencies.
  - Shared resources with other companies whose needs are fluctuating constantly can result in performance inconsistencies.
  - Downtime due to technical outages and support of many customers.
  - Downtime and performance issues due to equipment the bank does not have access to.

Cloud Computing – High Availability Reality

- Lack of options and inflexibility.
  - Forces the bank to fit into a one size fits all environment.
  - Industry ratio for staff to customers is 3:500.
  - Switching from one cloud environment to another is hard to do.
- Limited control and support.
  - The bank has some access to CPU and RAM but cannot get to the underlying virtualization layer and hardware.
  - Significantly lengthens troubleshooting time.
  - Can have more support issues than traditional environment
  - Cannot control restoration of backups.
  - Cannot “spin up” a new server without a new agreement which increases costs.

Cloud Computing – High Availability Reality

- Does not relieve the bank of their IT compliance responsibilities.
  - Must maintain information security and cybersecurity program.
  - Must maintain information security risk assessment.
  - Must maintain and test business continuity plan.
  - Must have annual information security testing.
- Does not resolve bank of cybersecurity responsibilities.
  - Must maintain cybersecurity self assessment.
  - Must maintain and test incident response plan.
  - The Board of Directors must provide oversight of the bank's cybersecurity program.
  - The bank does not have control over network security best practices.
  - Cannot confirm information security practices of the cloud provider.

Cloud Computing – High Availability Reality

- Information Security.
  - Cloud service providers implement the best security standards and industry certifications.
  - Using cloud-powered technologies means you need to provide your service provider with access to important business data.
  - Being a public service opens up cloud service providers to security challenges on a routine basis.
  - In a multi-tenant cloud architecture where multiple users are hosted on the same server, a hacker might try to break into the data of other users hosted and stored on the same server.
- Increases vendor management oversight responsibilities.

Cloud Computing – High Availability Recommendations

- Recommend creation of the bank's own Private Cloud environment.
  - Combines advantages of a data center without the cloud issues.
  - Mover servers and associated network hardware to the Enseva Data Center (tier 4 DC in Hiawatha, IA).
  - Improved uptime (reliability & availability) through redundant infrastructure backed by service level agreements.
  - Increased efficiency & performance through purpose-built design (environmental monitoring and controls, electrical monitoring and controls, etc…).
  - Risk mitigation through onsite security, video surveillance and other measures.
- Identify applications that make sense to host from the public cloud (Exchange365, Office365, etc…).

Performance, Complexity, Speed, Congestion

- Current server infrastructure was installed several years ago and built upon leading technologies from the late 2000s.
- Overall network speed is unacceptable.
- Performance was improved by moving from physical servers with internal storage to virtual servers connected to a storage area network (SAN).
- Redundant gigabit switches were installed between servers and SAN for performance improvements.
- Added gigabit Power over Ethernet (PoE) switches to offices for improved speed and Voice over Internet Protocol (VoIP).
- Server technology is out of warranty and at end of life for production systems.
- SAN is at ¾ life.

New Technology Recommendations

- Hyper-Convergence with Scale Computing HC3.
- Meraki core network switch.
- Server 2012.
- Office365/Exchage365 or Update Office and Exchange to Latest Versions.
- Replace Citrix with Remote Desktop Server.

Performance, Complexity, Speed, Congestion Recommendations

- Install Scale Computing servers and Meraki core switch to improve overall network performance/speed, reduce complexity, aid troubleshooting, reduce network congestion
  - Replace current physical hosts, switch, and SAN with Scale Computing solution – warranty extended to 5 years
  - Scale Computing eliminates complexity by integrating virtualization, storage, and servers into expandable modules
    - ◊ Eliminates separate SAN
    - ◊ Eliminates switches between hosts and SAN
    - ◊ Eliminated VMWare
  - Replace core network switch with Meraki 48 port layer 2 switch
    - ◊ Can manage each port and identify performance issues
    - ◊ Provides foundation for network segmentation in 2017
  - Upgrade 2008 servers to 2012 servers
    - ◊ Improved performance & Compatibility

Network Resiliency and Shorten Recovery Times from Malware, Disaster, etc…

- Current server infrastructure was designed with maximum hardware redundancy.
- Current servers are backed up daily to local storage and to the cloud.
- Cannot replicate frequently during the day without affecting the network performance.
- Would take at least one day (likely more) to recover network head to Disaster Recovery site in Lansing.
- Even with hardware redundancy there has been downtime due to technology system issues.

Network Resiliency and Shorten Recovery Times Recommendations

- Implement site to site replication between Scale Computing systems in Enseva and Lansing (existing production site).
- Replication intervals can be as short as every 15 minutes.
  - Ransomware: recover to last known good recovery point and restore in minutes instead of days.
- Launch last good recovery point for each server from replication site/DR site (Lansing).
  - Bring servers up within minutes, entire network in less than one hour with proper WAN failover.
- Windows server issues that caused downtime can now be recovered in minutes from last good recovery point.

Scalable for Business Growth & Core System Changes Recommendations

- Scale Computing hardware is modular and can be expanded to accommodate future acquisitions.
- Sized to support new windows servers required for the core system changes.
- Sized for 5 year production life based upon current network and applications.

Cybersecurity Framework Expectations

- Currently the bank is at the Baseline rating level in most of the 5 cybersecurity domains.
- The regulatory agencies are expecting banks to implement cybersecurity strategies that are overseen by the Board of Directors.
- The bank is weak in several areas within the 5 cybersecurity domains.
  - Monitoring & Analyzing, Infrastructure Management, Access & Data Management, Device/Endpoint Security, Threat & Vulnerability Detection, Remediation, Patch Management, Connections, Incident Resilience Planning & Strategy, and Testing

Cybersecurity Framework Expectations Recommendations

- Monitoring & Analyzing.
  - Setup windows server auditing for success, failure in all audit categories.
  - Setup server log archiving.
- Infrastructure Management.
  - Establish configuration standards.
  - Disable unneeded protocols and ports.
- Access & Data Management.
  - Develop data classification program for network files.
  - Review and modify security groups based upon information sensitivity.

Cybersecurity Framework Expectations Recommendations

- Device/Endpoint Security.
  - Restrict use of removable media.
- Threat & Vulnerability Detection.
  - Develop vulnerability management process.
  - Quarterly internal network scans.
- Remediation.
  - Quarterly remediation of vulnerabilities.
- Patch Management.
  - Automate 3rd party patches.
  - Implement timely firmware update process.

Cybersecurity Framework Expectations Recommendations

- Incident Resilience Planning & Strategy.
  - Update Business Impact Analysis to include cybersecurity threats.
  - Scale Computing hardware supports incident resilience.
- Testing.
  - Implement quarterly incident response/business continuity testing plan.
  - Run network from disaster recovery site (Lansing).

End of Presentation

- Thank You –

Questions