



E-Commerce & E-Service Security

What is Included in E-commerce Services?

- Services that are Internet based and performed by the member. Some examples are;
 - Internet Banking
 - Bill Payment
 - E-Statements
 - Check Requests & Re-orders
 - Investment Services

What Falls under Electronic Data Systems or E-Services?

- Services that involve the electronic storage & transmission of membership data.
- This transmission does not have to be via the Internet.
- It could be via;
 - Frame Relay
 - FTP
 - VPN
 - Direct Dial

Some Examples of E-Services

- Credit Card Programs
 - May allow Vendor remote access to pull or send files.
 - System being accessed may be on the same network as your Data Processor.

Some Examples cont.

- Loan Processing Workstations
 - Allow Vendor remote access for support.
 - Software & Servers may be installed and on the same network as your Data Processor.

What do E-Commerce and Electronic Data Services have in common?

- Security Risks due to potential access to large amounts of membership data.



When do you need a Security Policy?

- Every credit union needs a Security policy & program for your physical & electronic data systems.

When do you need an E-Commerce Policy?

- A policy is needed if you have a web site of any kind.
- If you do not have a web site but have Internet access you need to include the controls and procedures as part of your Security policy.



For Those Without a Web Site

Identify Your Access Points

- Do you have dial up or DSL to access to the Internet? If so;
 - Purchase, install and document controls for Anti-virus & Firewall software.
 - Implement a Maintenance program for the software to ensure it is kept up to date.



For Those Preparing to Implement a Web Site

Create an E-Commerce Committee

- Review E-Commerce activities & reports.
- Review/monitor vendors and their security policies.
- Perform risk analysis for new E-Commerce products.
- Responsible to come up with methods to monitor activities and reporting back to the board.

Identify Your Services

- Identify and summarize your E-Commerce products.
 - Internet Banking
 - Bill Payment
 - On-line Applications & Forms
 - Third Party Links

Risk Assessment

- Perform a Risk Assessment for the web site and related services previously summarized.

Look at:

- Transaction Risk
- Posting of invalid text
- Reputation Risk
- Compliance/Legal Risk



Some Questions to Ask During the Risk Assessment

Internet Banking

- Will your membership data be accessed directly? An example is;

Will it be On-line or Batch Internet Banking?

- Who is responsible for security?
- What type of firewall is in place and how is it maintained?
- Where does the membership information and PIN reside?

Internet Banking Applications

- Will you allow membership to sign-up via the Internet or require a signature?
 - Assess & Prepare your strategy before implementing the service.
 - Keep in mind you will need:
 - Applications and a process to accept, implement and retain the applications.
 - Determine employee access, training and responsibilities.
 - Retain appropriate disclosures and legal advise.

What Transactions Will You Allow?

- Does your Vendor allow members to transfer within or outside their accounts?
 - Identify what security is in place to avoid errors.
 - PIN considerations

Under Compliance/Legal Risk

- Be aware of your responsibilities and risks when selecting a third party web relationship.
 - Is the link passive or framed?
 - Make sure to include all disclaimers.
 - Review contracts – make sure you can terminate if their practices are not in line with the credit union.
 - Review Security & Privacy Policies.



How do you Identify and Document Security Controls?



First Five Steps

- For each E-Commerce or E-service start with these five steps.....

Protecting your E-Systems #1

1. First, identify the means of data communication/transfer
 - Internet
 - Direct Dial
 - Frame relay
 - Wireless

Protecting your E-Systems # 2

2. Identify & document what is in place to protect the data on both sides.

- Logins and Passwords
- Digital certificates
- Smart Keys
- Firewalls

Protecting your E-Systems # 3

3. Identify & document who has access to the system and what controls are in place.
 - Remote access support
 - Login & Password controls
 - Employee termination/leave procedures
 - For you and the vendor!

Protecting your E-Systems # 4

4. Develop a management control & maintenance program for each service to;

- Identify who within the credit union is responsible for the service.

This person will then be able to;

- Ensure the latest software is in place
- Track incidents and complaints
- Ensure the controls are truly working

Protecting your E-Systems # 5

5. Diagram (Topography) each service and the flow of information. Some examples are;

- Home Banking transactions
- Bill Payment
- Applications
- Internal Network
- Web site



How to Secure your Network and Data access

Develop Strong Passwords

- Unique
- Alphanumeric
- @ least six digit minimum
- Expire
- Can't be re-used



Implement Screen Savers

- Protect your member data from unauthorized viewing.

Restrict Employee Access

- Lock down Data Processing menu options by implementing security program for tellers, etc.
- Check for remote access options to system and PC's
 - What is the login and password policy for remote logins?
 - Ask yourself, what else can they access over your network?
 - Be careful of file sharing and older versions of Windows.

Restrict Employee Access cont.

- Remove internal modems from PC's that are not being used.
 - Note, Identify and retain specific modems for your disaster recovery plan in the situation your Internet access fails.

Implement Virus protection

- E-mail
 - Turn on e-mail scanning & live update
 - Perform daily scans
- Windows and Browser updates
 - Take advantage of Microsoft free downloads.

Third Party Assessments & Monitoring

- Utilize Third Parties for;
 - Vulnerability Assessments
 - Security Reviews & Policies
 - Firewalls & Intrusion Detection
 - Penetration Testing

Continuity Plan

- E-Systems should be included in Business Impact Analysis and Recovery Plans.

Required Employees Policies

- Employee Internet Usage Policy
- Employee Software Policy

Web site General Maintenance

- Retain an annual copy of the web site.
- All web revisions should be documented.
- All member e-mail correspondence retained.
- All member applications retained.

Membership Data Backups

- Network & Data processing backups are performed and safeguarded.
- Log and secure all Membership electronic data stored at the credit union.
- Log all media containing membership data that leaves the credit union.

Buckley Technology Group

- Please visit our web site @ www.buckleytechgroup.com
- We have recently moved our office so please refer below for our latest contact information:
 - Buckley Technology Group, 130 Till Rock Lane, Norwell MA. 02061
 - Phone: 1 (781) 829-9934
 - Fax: 1 (781) 829-4407
 - Email: kmb@buckleytechgroup.com



Thank You!