

Executive Leadership of Cybersecurity
ELOC Best Practices
Texas Bankers Electronic Crimes Task Force

Leadership Steps Every CEO Should Take:

1) Commit to establish a Cybersecurity strategy and give it broad staff and Board visibility.

- Put cyber on agendas at least monthly for staff and quarterly for Board meetings.

2) Commit to develop a corporate culture of security and cyber literacy.

- Evaluate where you spend your time, as that conveys what you value;
- Protecting your customers and your bank's reputation is everyone's responsibility;
- Shift focus to security and away from compliance checklists;
- Use Safety & Soundness reasons to protect your bank; don't focus on GLBA requirements, as that is a compliance mentality;
- Incorporate cybersecurity into routine and recurring bank-wide training; and
- Establish continuing education hours for directors, similar to BSA training.

3) Adopt sound management practices.

- Practices to prevent cyber incidents are not enough. Regularly update your cyber incident response plans, as threats change regularly;
- Personally study the cyber elements of your risk assessment and understand:
 - How are you protecting your high value assets?
 - Where are your soft spots?
- Establish a reliable method (or person) to prioritize incoming cyber issues;
- Obtain regular threat updates (and provide to Board) to help stay engaged;
- Be willing to write the check for protection, especially if you want to roll out cutting edge technology. Acquisition is just the down payment;
- Don't rely on contracts with borrowers and depositors - it doesn't work;
- Actively work with trade associations and groups to identify trusted vendors and other third-party providers in your market(s); and
- File SARs to help law enforcement build a large case to shut down an operation.

4) Cybersecurity messages must regularly come from the CEO / Executive management. The tone is set at the top; not from the "IT guy."

- But, the IT security officer must also be an upper level employee to demonstrate to your entire organization how importantly you view this issue;
- Carry the message to your community. Lead cyber education in your community, especially for small/midsize businesses or industries:
 - Talk about threats they are unaware of and that they need to protect against at their own business; and
 - Put on short training session during a "lunch & learn" for the Chamber of Commerce or other civic organizations, such as Rotary Clubs, churches, nonprofits, schools, etc.