

Executive Leadership of Cybersecurity ELOC Best Practices

Questions Community Bank Directors Should Ask:

(Cybersecurity has to be on the agenda.)

- 1) Can you put that in laymen's terms? Can you explain what that means?
 - This is a serious question. Technology has a language of its own that few of us can be 100% fluent in. Directors must insist on briefings in plain language.
- 2) Are we getting into the weeds?
 - Again, a serious question. Cyber is not an IT issue, but a risk management issue.
- 3) Do we need a cybersecurity committee to have the time to become educated?
- 4) How do we determine how much to spend on cybersecurity?
- 5) What are our greatest weaknesses and what events are most likely to happen?
 - Do we have incident response plans for these and when were they last tested / updated?
 - Explain the legal implications and financial risks if XYZ should happen to us?
 - What are the most sophisticated types of cyber threats that you are monitoring against?
- 6) How would the latest threat reported in the news (such as a DDoS attack, an ATM Cash Out, Open SSL Vulnerability, Cryptolocker) attack affect us? And, what steps have been taken to minimize those risks?
- 7) What incidents require customer notification and which ones don't?
- 8) What are we looking for when we run penetration tests and perform vulnerability scans? How often are we scanning?
- 9) How do we move away from security checklists and focus on addressing the risk identified in our risk assessment?
- 10) What are some contract terms you (CEO) look for in contracts (cyber security practiced by the vendor, requirement to be notified of a vendor breach, restrictions on vendor's use of subcontractors, requirement's for vendor's security testing, access to vendor audits, etc.)?
- 11) Do we have an education / training incentive program for our IT security professionals?