The Boards Role in Cybersecurity Risks

Phil Kenkel
Bill Fitzwater Cooperative Chair

Cybersecurity is an increasingly important risk for all firms. I would be the first to say that I am no expert in cybersecurity. Most cooperative board members are also not experts. Our natural tendency is to avoid areas where we are unfamiliar. However, the board has the responsibility of monitoring and safeguarding the cooperative's assets. That includes monitoring the risk management plan and cyber risk are one of the types of risks that the cooperative faces.. That implies that the board should ensure that the firm has a set of cyber risk management policies and procedures consistent with its situation and risk appetite. The board is not responsible for the mechanics of cyber risk management, but rather in insuring that procedures are in place.

That raises the question as to how a board member can know if the cyber risk management practices are sufficient. A general guideline for the board is to consider what a reasonable and prudent person would do when faced with a similar situation. The board can also generally rely on information provided by the CEO and/or outside consultants. A good approach might be having the CEO or an outside consultant prepare an assessment of the possible cyber risks facing the firm. That assessment might consider the member information that the cooperative maintains and the implications of a breach. It might also consider the types of authorized actions that could be perpetuated and the impacts. After reviewing the risks, the board should ensure that the cooperative has policies and procedures designed to prevent foreseeable security breaches and is reasonably prepared to recover from a cyber-security breach. A good reality check is to ask whether the cooperative is taking the steps that other similar size businesses with similar risks are taking.

All risks change over time and cyber risks are particularly volatile. The board should periodically re-evaluate their cyber risk management plan. Again, the standard of the reasonable person comes into play. For example, we have all encountered two-step verification where after providing a password the user is sent a security token via email or phone. If two-step verification were to become the norm, the cooperative should consider adopting it. Otherwise, the board would stand the risk of being scolded for not taking the precautions that a reasonable person would employ.

As a final piece of advice: Don't use the word "beef stew" as a computer password. It's not stroganoff!