Scott Klososky
Founder, Future Point of View
Technology Speaker

COMPLIMENTARY
CYBERSECURITY RISK EVALUATION

Developed with
FUTURE POINT OF VIEW

Exclusively for clients, SpeakersOffice is offering Scott's checklist tool to you. We think you will find the latest thinking around cybersecurity to be extremely valuable to your own organization.

The risks from cybersecurity attacks, whether external or internal, continue to grow. Leaders must make thoughtful and informed decisions as to the level of risk they are willing to accept on behalf of the organization. This risk decision cannot be outsourced to IT people; it must be made by the executive level leaders responsible for organizational policies and controls. This document is meant to be a very abbreviated checklist of sorts that leaders can use to assure they are proactive when addressing cyber risk.

SPEAKERSOFFICE

scott klososky @sklososky /sklososky

CYBERSECURITY CHECKLIST EXCERPT

- [ ] Are you educating employees around types of common cyber-attacks as well as protection tactics?
  Most need a blend of periodic instructor led sessions and eLearning modules for new team members.

- [ ] Are you following cybersecurity training with employee testing scenarios covered in cybersecurity training?
  (e.g., social engineering attempts, emails with suspicious links, dropping storage devices around your building, etc.) to make sure all employees are following protection advice?

- [ ] Do you enforce password policy setting requirements for the amount and types of characters used as well as the frequency with which new passwords are created?

- [ ] Do you enforce a screen saver policy detailing the situations in which a screen saver must be in use and that a password is required to unlock?

- [ ] Do you develop and constantly improve infection and incident response plans? Do you also conduct practice “drills” to play out these plans?
  In the case of a major breach it is a best practice to have a third party do the forensics to understand what led to the incident (we can help you create incident response plan and can do the post breach forensics if needed).

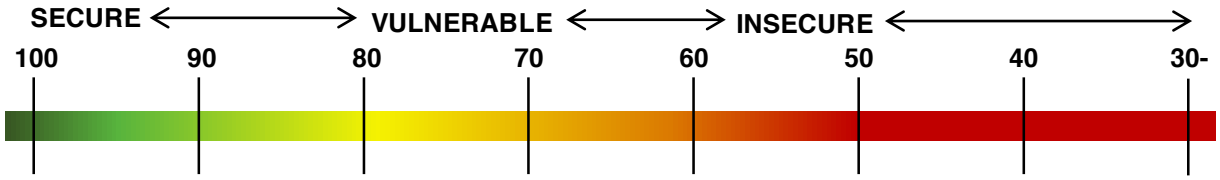
- [ ] Do you have a policy for changing login credentials on all network hardware and software whenever any IT employee or contractor who has worked with these systems leaves your organization?

- [ ] Do you have email security gateway to protect corporate users from spammers and malware?

This simplified checklist represents only a fraction of our complete checklist and generally it serves as an eye-opener to begin understanding what holes you might have in your cybersecurity.

For your Technology Professionals- Scott would love to send you his comprehensive Checklist. Email clientservices@fpov.com to request the full checklist!

If you have any concerns about the state of your organization's cybersecurity Scott's team can walk you through some deeper assessments help you build a remediation plan to shore up your networks, your employees, your data and more. They use a very simple framework to illustrate the most critical areas to address for your immediate safety.



100-91: Only Low Vulnerabilities – Simple adjustments necessary

90-76: Medium and Low Vulnerabilities – Remediation recommended

75-60: High Vulnerabilities – Immediate remediation recommended

59-0: Extreme Vulnerabilities – Immediate remediation required

WHAT NOW?

For more information on a keynote or cybersecurity workshop, please call 760-603-8110 or email info@speakersoffice.com.

SPEAKERSOFFICE