CYBER THREAT
PREPAREDNESS ACTION PLAN

DATE	ACTIONS
1	**Assess your Digital Infrastructure** — are you leaving your gates unlocked and the keys in the forklift?
2	**Assess the Human Factor** — are your employees aware of phishing schemes, are they clicking on links from unknown senders, is their password strong enough, what are they to do when they spot something wrong?
3	**Encrypt remote devices** — including those utilizing business email and file access, on laptops and phones.
4	**Discuss authority, authentication, and "regular business practices" with your bank** — if you don't usually send wire transfers out of your bank, then confirm with your bank that this would not be allowed without phone or in-person confirmation.
5	**Use multi factor authentication** — include on all remote email and system access.
6	**Use the Cyber Application provided as a checklist** — if you can answer yes to these questions then you'll not only be better prepared, but also lower your premium.
7	**Conduct a tabletop exercise** — what would happen in the event of a system lockdown — no email, no share drives?
8	**Share the results of the tabletop exercise with all staff**
9	**Deliver expectations for everyone** — instruct to alert IT, or Accounting, or whomever you designate, when they see something amiss.
10	**Train Employees as your front-line defense** — conduct threat awareness training quarterly or at minimum annually for all employees with access to company devices; these can be as easy as a 5 minute video which raises awareness

Want to understand if your organization is prepared for cyber threats?

We are happy to answer any questions.

TRAVIS DAVIS
TTDavis@PayneWest.com
(541) 306-2081

PayneWest INSURANCE

A Marsh & McLennan Agency LLC company

PayneWest.com