

How are you Responding to today's CYBER THREAT LANDSCAPE?

RANSOMWARE IS NOT going away. Too many bad actors have found that crime does pay, and it costs its victims in dollars, time, and reputation.

- Ransomware attacks are not just a big business and government problem. While Colonial Pipeline and JBS Meat Packing make the news, the proliferation of attacks means smaller and smaller businesses and municipalities are being targeted. 2020 was the worst year for cyberattacks and 2021 is seeing an attack every 14 seconds.
- Stand-alone organizations make their living by producing and selling the tools others need to commit cybersecurity crimes.
- As fast as many insurance companies entered the cyber threat market, many are leaving again. Those staying are scaling back coverage leaving clients with a larger liability for payment and requirements to meet more stringent qualifications to keep a policy in force.



The **5**-Step Response Process...

IDENTIFY Know your environment, your assets, your current state of security, your current ability to respond to an incident.

PROTECT Safeguard your critical assets and make sure your policies and procedures are designed to reduce risk.

DETECT Security and continuous monitoring, investigate anomalies and events, put in place processes that let you know a breach is occurring as soon as possible.

RESPOND Develop and implement appropriate procedures to act when a cybersecurity incident is detected and communicate the part that all play in that response.

RECOVER When an incident does occur, have resilience and restoration capabilities ready to reduce impact and return to normal operations.

Learn, assess, implement the best policy, procedure, and technology you can and then reassess as your environment changes. It seems a daunting task, but you do not have to go it alone. A good first-start is a conversation with **McMahon Technology Consultants** to see how we can help.

We can perform a cybersecurity assessment that is tailored to your needs and recommend solutions that are respective of your time, budget, and personnel. Improving your ability to **Identify, Protect, Detect, Respond and Recover** does not have to monopolize your time, break your budget, or overwhelm limited personnel with yet more job responsibilities.

Whether it is a one-time assessment that lets you know your security posture and you take it from there, to becoming a partner who you can turn to for help and advice on a regular basis, we do what you need, not sell you solutions you do not. That is not how we work.

TO DISCUSS FURTHER HOW McMAHON
TECHNOLOGY CONSULTANTS CAN HELP, CONTACT
Andrew J. Westphal
Public Management Specialist / IT Specialist
awestphal@mcmgrp.com
920.751.4200 ext. 405