

BULLETPROOFING YOUR NETWORK

Mitigating cyber issues from the top down



CYBERSECURITY IN THE MEDIA

- Persistent threats
- Growing losses
- Even the largest enterprises being hit

WHAT CHANCE DO WE EVEN HAVE?

MOST CYBERCRIMES REPEAT THE SAME PATTERNS

- There is very little new under the sun
- Criminal groups have gotten really good at perfecting one pattern that works reliably and scaling it up.
- This means we have good intelligence about what's happening...and how we can prevent it

INFORMATION SECURITY IS NOT ROCKET SCIENCE

- Instead, good information security is about better - more consistent application of basic fundamentals.
- But, there exists a knowledge gap.

WHAT ARE THE CONTROLS THAT
MATTER?

MULTIFACTOR AUTHENTICATION

- Hands down – the single most effective control you can use in 2019
- Absolves a multitude of sins
- Mail, banking, and social media should absolutely have it enabled. If your provider doesn't use it – switch.

PASSWORD MANAGEMENT

- Strong, unique passwords are critical
- Use a password manager – even the best of us need one
- Make sure you're using unique passwords for email, banking, social media, and critical apps

DATA INVENTORY

- You cannot protect data that you don't know about!
- Go through the inventory process with your stakeholders
- Have the hard conversations about getting rid of stuff

REDUCE ACCESS TO INFORMATION

- Limit access to data to need-to-know
- Lead by example
- Monitor access – and pay attention when people exceed limits

WHOLE DISK ENCRYPTION

- WDE is cheap insurance against lost or stolen devices
- In 2019 – this isn't something you need to buy – it simply needs to be enabled.
- Bitlocker on Windows / FileVault on Macs / Passcodes on mobile devices

VULNERABILITY MANAGEMENT

- Know your vulnerabilities – scan on a regular basis
- Most technical hacks have had patches available for 12-18 months
- Patching should largely be automated – and scheduled

LIMIT DAMAGE POTENTIAL

- We need to remove the channels via which malware spread
 - Remove local administrative access
 - Keep antivirus up-to-date
 - Pay attention to technical debt (stuff that can't be updated)

INCIDENT RESPONSE

- We need to be able to respond better - faster
- You will not rise to the occasion – you will default to your level of training
- Cyber insurance makes a world of difference when something happens

BACKUPS

- You don't have backups until you've successfully restored from them!
- Test, and revisit scope on a periodic basis
- Consider cloud options

BRYAN F. THORNTON

615.346.9209 – office

615.207.0414 – mobile

bthornton@risksentry.com

