INTRODUCTIONS

Rich Eckstein
CCSP, ISGR, CIH, Security+, CCIDS-IPS, CCIDS-CPS,
CCIDS-CVPNs, CEHVA, MCSE, MSEP-L, XRM, CS2, VCP

THE EVOLVING LANDSCAPE OF CYBERSECURITY

Attacks will happen
no matter how big...
or small...
your company.

The world is filled with those companies that have been hacked and those that are about to be hacked.

Think you are not a target?

1 in 5 Small businesses will suffer a cyber breach this year.

81% of all breaches happen to small/medium sized businesses.

97% of breaches could have prevented with today's technology.

Hacking continues to grow at an alarming rate.
Do you have bitcoin?

How to protect your business from Cyber Attack!

1. Security Assessment
2. SAM (Email)
3. Password
4. Security Awareness and Training
5. Endpoint Security
6. Multi-factor Authentication
7. Computer Updates
8. Dark Web Research
9. Next gen Firewall
10. Encryption
11. Backup
12. Cyber Insurance
13. Legal Counsel
1. Security Assessment

2. Spam Email

3. Passwords
Bad password practices that lead to breaches:
1) Lack of MFA
2) Lack of brute-force password guessing protection
3) Use open RDP
4) Reuse of passwords

Users tend to choose weaker memorized secrets when they know that they will have to change them in the near future. When those changes do occur, the often select a secret that is similar to their old memorized secret by applying a set of common transformations such as increasing a number in the password.

Latest recommendations are to NOT force password changes unless their has been a suspected BEC or OPC.
How long to crack online? 7.92 minutes
How long to crack OFFLINE? 0.0000475 seconds
Cracking array OFFLINE? 0.0000000475 seconds

How long to crack online? 2.07 hours
How long to crack OFFLINE? 0.000745 seconds
Cracking array OFFLINE? 0.00000074 seconds

How long to crack online? 14.67 hours
How long to crack OFFLINE? 0.000528 seconds
Cracking array OFFLINE? 0.000000528 seconds
How long to crack online?  **22.87 hours**
How long to crack OFFLINE?  **0.000823 seconds**
Cracking array OFFLINE?  **0.000000823 seconds**

Which of the following two passwords is stronger, more secure and more difficult to crack?

**D0g................ (has 25 characters)**

**PrXyc.N(n4k77#L!eVdAfp9 (has 24 characters)**

Who knows why?
Since the first password is one character longer and contains uppercase, lowercase, number and special characters, the first password would take

95 times longer find

So go tell that client or coworker the WHY the next time they resist.

Then be a hero – solve the problem and tell them it’s easy with a password manager and BTW – 2FA!
Evaluation of Risk

...And repeat

PICK A STANDARD
ISO 27001:2013
Nist csf 800-53
Cobit

CONDUCT AN ASSESSMENT
ADMINISTRATIVE CONTROLS
PHYSICAL CONTROLS
TECHNICAL CONTROLS

MAKE A PLAN
ACCEPT
MITIGATE
AVOID

WORK THE PLAN
Due Care, due diligence
Measurable improvement

What controls are currently in place to mitigate risk?
Prioritize

1. What are your critical business systems?
2. Where is your most critical data?
3. What are your key line-of-business applications?
4. Have you protected your intellectual property?
5. What systems keep operations going?
6. What tools do your employees need to do their work?

You are not going to button up all your risk

1. I have not seen one small business with an unlimited budget.
2. There will always be some level of exposure you will be willing to live with
Get a clear Understanding of where you stand