2022 CIRSA

GENERAL MEMBERSHIP MEETING

WEDNESDAY JUNE 22, 2022

Breckenridge

CIRSA SAFERTOGETHER

CIRSA

Demystifying Cyber Security

A Practical Approach for Non-Technical Administrators to Improve Cyber Readiness

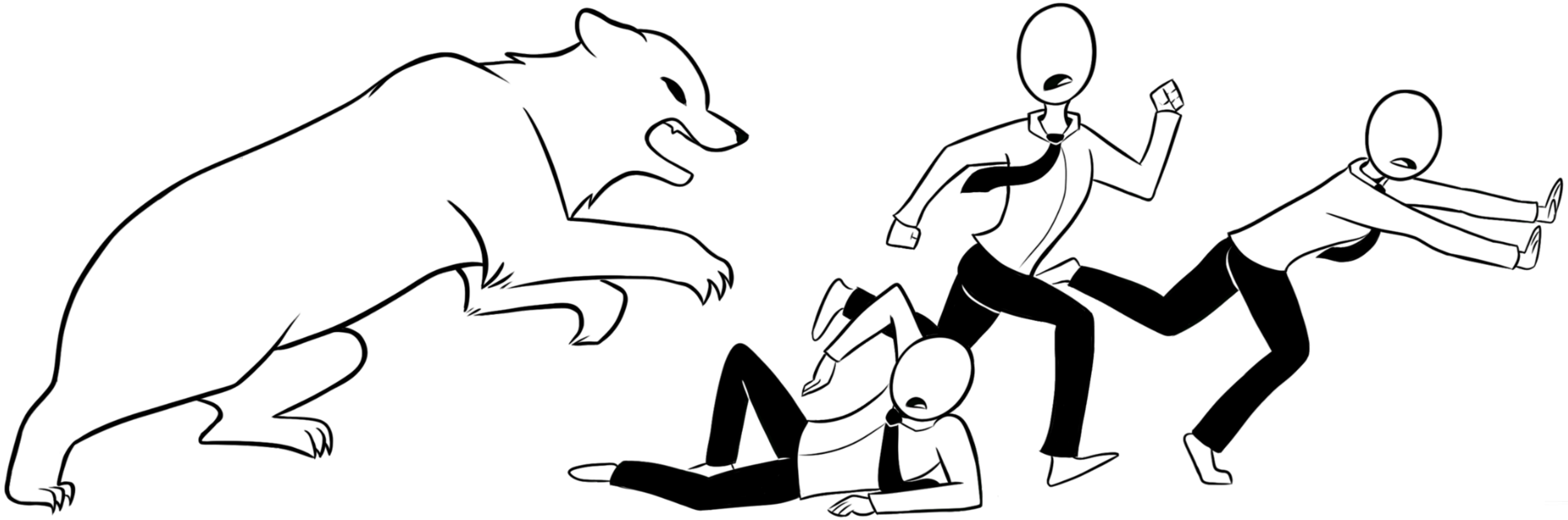
Presented by Jim Kilmer, The OPAL Group

About Me

- MSE Computer Engineering
- Research Lab@ Case Western Reserve University on Human Genetic Analysis Software & Data, 1995-1999
- Consulting Associates International; Global Business Analyst, 1999-2001
- Founder of Tech Division/Partner; The OPAL Group, 2000 – Present

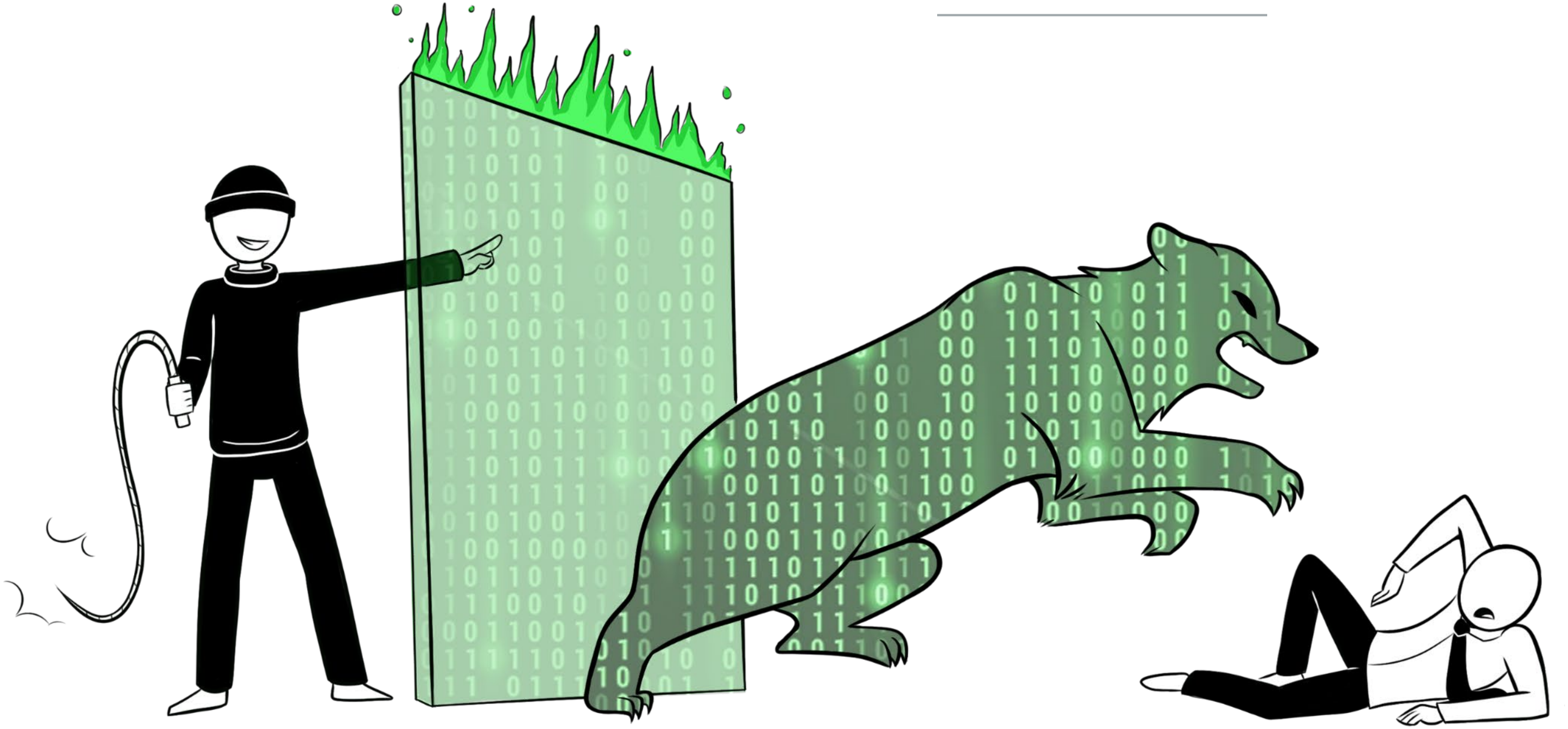
- OPAL is a Managed Services Outsourcing & Consulting Firm
- Technology Division focused on systems modernization & best practices for Small-to-Medium Enterprise
- Partnered with Enquiron & Zywave since 2010, focusing on cybersecurity for small and mid-sized organizations.

How Do You Avoid a Cyber Attack?



How Do You Avoid a Cyber Attack?

How Do You Avoid a Cyber Attack?



CIRSA SAFERTOGETHER

Scope of This Presentation

- Large Municipalities may already have some or all of these in place
- Smaller Municipalities may worry about cost – we'll talk about that a bit, and put this in perspective
- None of these techniques are "Government Specific". (Any IT vendor or contractor could assist)
- Not comprehensive. Other more advanced techniques are advisable, but definitely require strong IT support.

CIRSA SAFERTOGETHER

Cybersecurity is a Human Problem Pretending to be an IT Problem

- Primary threats now come from Social Engineering, Account Compromise and Opportunity, not “Hacking”

- Primary damages come from:
  - Loss of productivity and services
  - Reputational / Consequential Damage
  - Self-inflicted wounds during response
  - … NOT technology failures.

CIRSA SAFERTOGETHER

5 Simple Things Non-Technical Managers Can Implement

- Password Managers
- Anti-Phishing Testing & Training
- **Multi-Factor Authentication**
- **Endpoint Protection**
- **Off-site (Cloud) Backups**

CIRSA **SAFER**TOGETHER

GETTING TO YES: Passing a Cyber Insurance Audit

Will cover these in greater detail…
Generally these do require some level of IT support,
but not as much as you think!

- **Multi-Factor Authentication**
- **Endpoint Protection**
- **Off-site (Cloud) Backups**

CIRSA SAFERTOGETHER

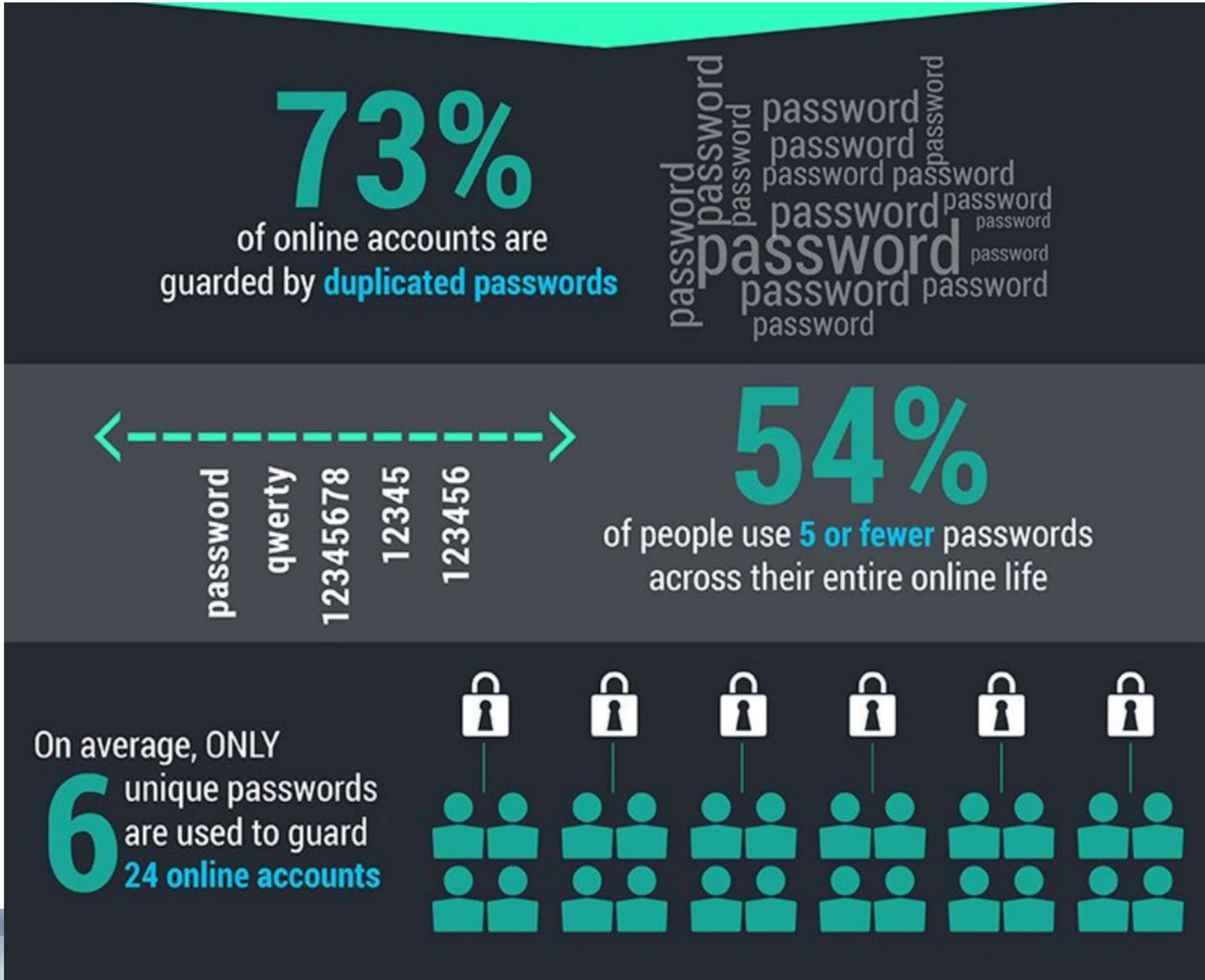
Password Managers

- Create strong, unique passwords for every site/service
- Reduce changes of fraudulent password entry
- Actually makes account management *easier* for staff

CIRSA SAFERTOGETHER

Password Managers

- Prevent sideways attacks
- Securely provide and monitor passwords for teams
- Warn of compromises and old passwords



73% of online accounts are guarded by duplicated passwords

54% of people use 5 or fewer passwords across their entire online life

On average, ONLY 6 unique passwords are used to guard 24 online accounts

Source: TeleSign Consumer Account Activity Report

Password Managers

- $3-$5 per month, per user.
- Easily installed and set up by non-technical users
- Strong online training and how-to videos

1Password

KEEPER
Cybersecurity Starts Here

LastPass

DASHLANE

Anti-Phishing Testing and Training

- Get to your staff before the bad guys do!
- Early warning of the latest frauds and attack techniques
- Know where to target your re-training efforts

Anti-Phishing Testing and Training

- Can do fully-random testing with a variety of messages, or targeted testing to “dry run” response procedures

- Use as a mechanism to train and test your Incident Response Plan

A Quick Note on Incident Response Plans

- You do have one… right?

- Your incident "play book"
- Don't make decisions in the heat of the moment.
- Everyone from the Mayor to the Maintenance staff have a role
- Train, train, train… and test!

Anti-Phishing Testing and Training

- Offered through your membership in CIRSA!
- Can run ongoing automated after initial setup

KnowBe4
Human error. Conquered.

Multi-Factor Authentication

- Also referred to as Two-Factor Authentication (MFA or 2FA)
- “Something you Know” + “Something you Have”
- Prevent Account Takeover
- Widely Supported

Multi-Factor Authentication

- Security Questions – Terrible
- SMS (Text Message) – Bad but better than nothing
- Authenticator App – Good but harder for users
- **Push Notification & Approval – Best all-around option!**
- Hardware Token – Best but not yet widely supported and $$

Multi-Factor Authentication

- In most cases, FREE!
- Hardware Tokens ~$50 each

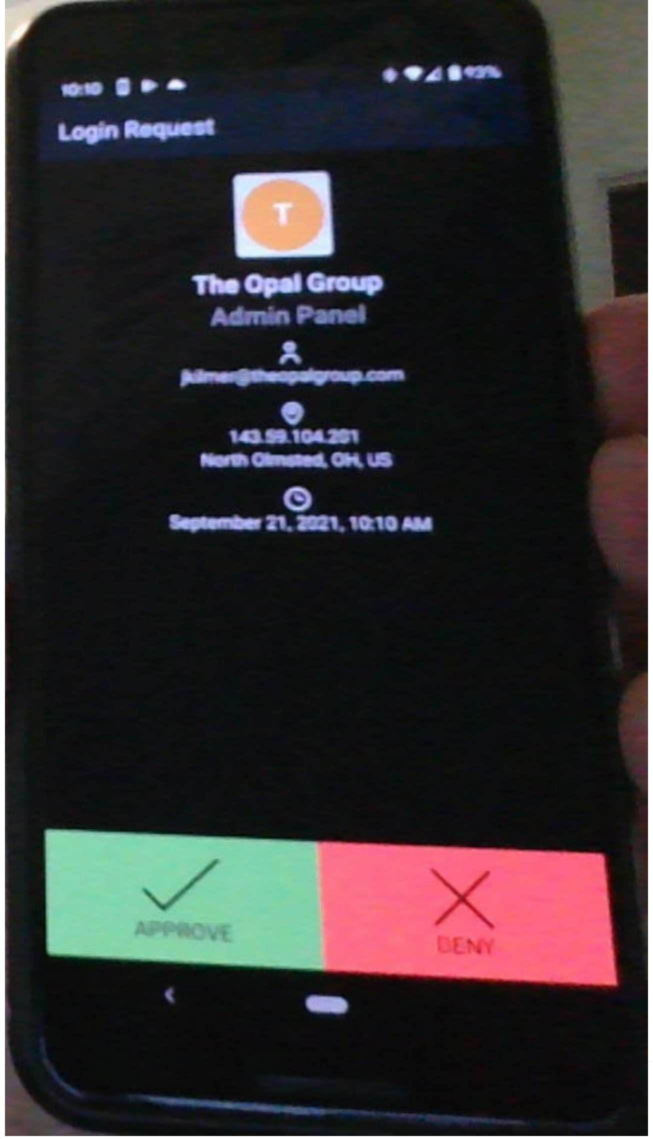
Examples:

App-Based	Push-Based	Hardware
AUTHY	DUO	yubico
Google Authenticator	Microsoft Authenticator	fido U2F™ Ready

How does Push Notification work?

- Push prompt to your Android or iPhone device
- 6-digit SMS Code sent to your phone
- Hardware token that must be plugged into USB port

- Upon Desktop Login
- Upon Remote login to RDP Server
- Can work w/ remote login to VPN

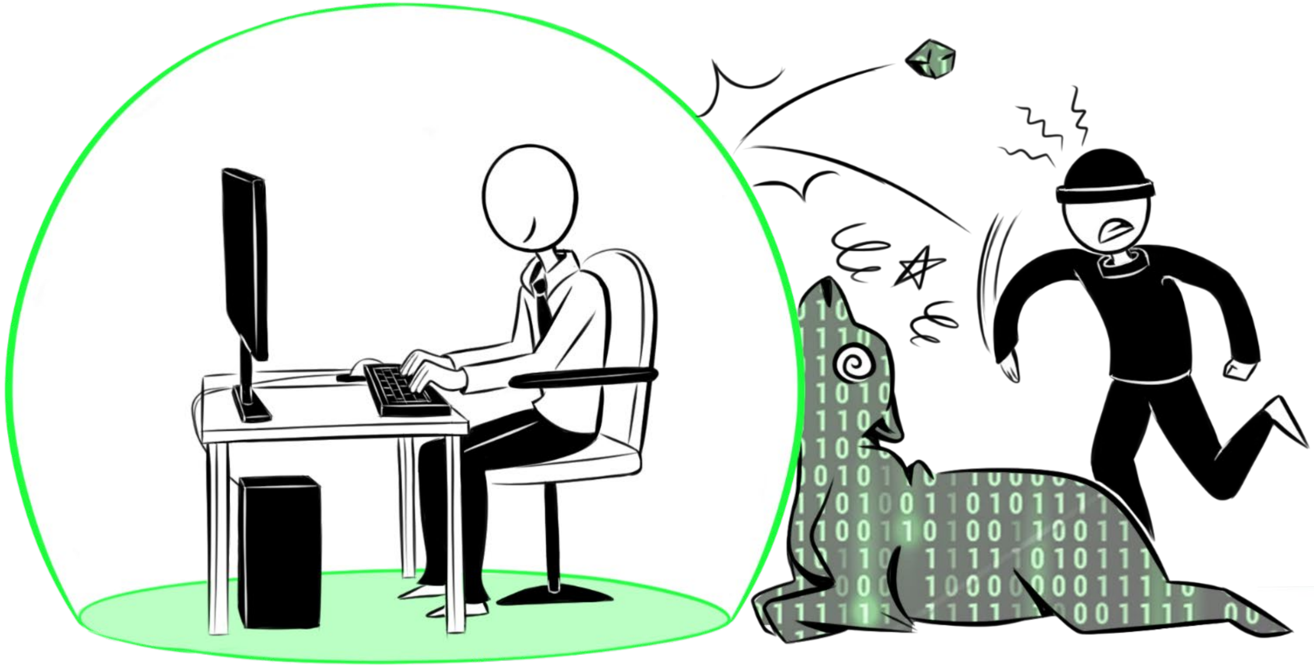


The Opal Group
Admin Panel
jkilmer@theopalgroup.com
143.59.104.201
North Olmsted, OH, US
September 21, 2021, 10:10 AM

What is Endpoint Protection?

- A Protective Bubble around your PCs and Servers

- Anti-Virus +
- Firewall +
- Network Threat Protection +
- Ransomware Protection +
- Fraud Detection +
- Security Restrictions +
- …



Endpoint Protection

- Can be installed and managed from a central server, OR deployed individually to stand-alone desktop computers (cloud managed)

- Most vendors offer Government / Nonprofit discounts

- EDR (Endpoint Detection and Response) is Endpoint Protection plus an “always on” network component that provides advanced monitoring, for larger organizations

What is an “Endpoint”?

- Desktop PCs
- Servers
- Laptops
- Tablets
- Mobile Devices
- Printers
- Networked Devices (Kiosks, POS systems, etc…)
- IoT Devices

* Covered by Endpoint Detection and Response

Endpoint Protection Software

- $15-$35 per year, per device
- Can run with or without an on-premise server

Bitdefender® GravityZone

TREND MICRO™

McAfee Enhanced Remediation

Apex One

Endpoint Detection and Response

- $20-$45 per year, per device
- Requires an on-premise server
- Sometimes needs dedicated hardware

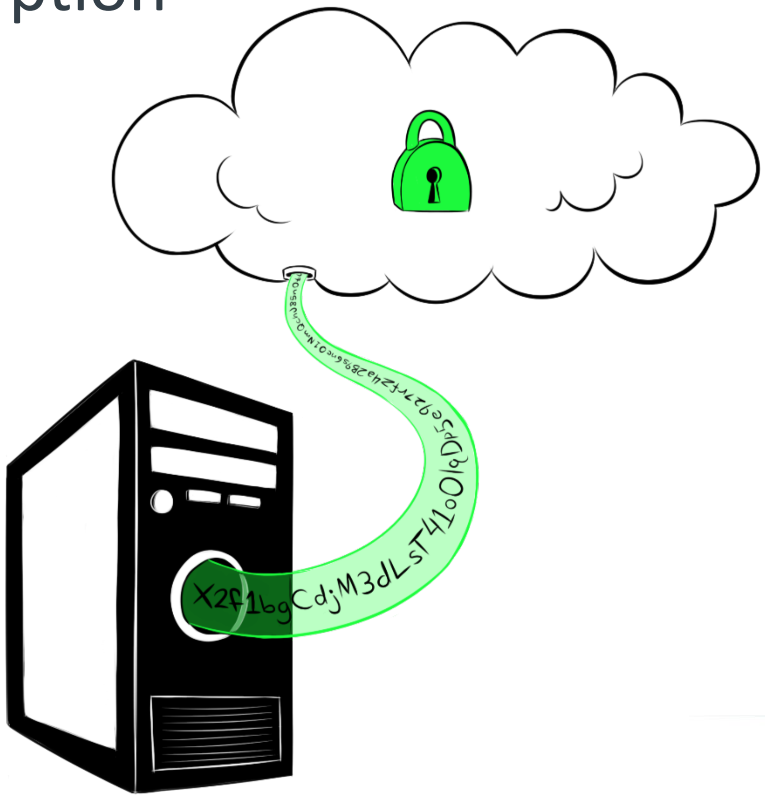
Bitdefender®
EDR

McAfee
Enhanced Remediation

CROWDSTRIKE
FALCON INSIGHT

Cloud Backups

- Simultaneously provides off-site backup AND encryption
- Best chance of recovery from Ransomware
- Appropriate for sensitive information
  (If provider offers strong encryption)
- Most modern platforms run unattended
  and can be managed & tested by
  non-technical users.



Cloud Backups

- Suitable for Servers and Desktops
  … BUT – you should not store sensitive data on desktop/laptop machines unless no other option is feasibly available!

- Essentially required to receive insurance coverage these days

- Easy to set up, but most services offer guided setup as a service.

- Offered/Supported by effectively ANY IT Support shop as a basic service.

CIRSA SAFERTOGETHER

Cloud Backups

- Priced by amount of data backed up and retention period.
- Generally anywhere from $50-$250 per month
- Cost is effectively negligible compared to recovering from a major data loss or ransomware attack.

IDrive

BACKBLAZE

CARBONITE
an opentext company

It’s a new dawn… to think about your organization’s security

Don’t Ignore the Human Factor

- It’s not just an “IT Problem”
- Treat Cyber hygiene just like any other HR Compliance issue
- Train, Train, Train
- Become a harder target

Thank You!

Q & A

Thanks to CIRSA for their Support!

CIRSA SAFERTOGETHER