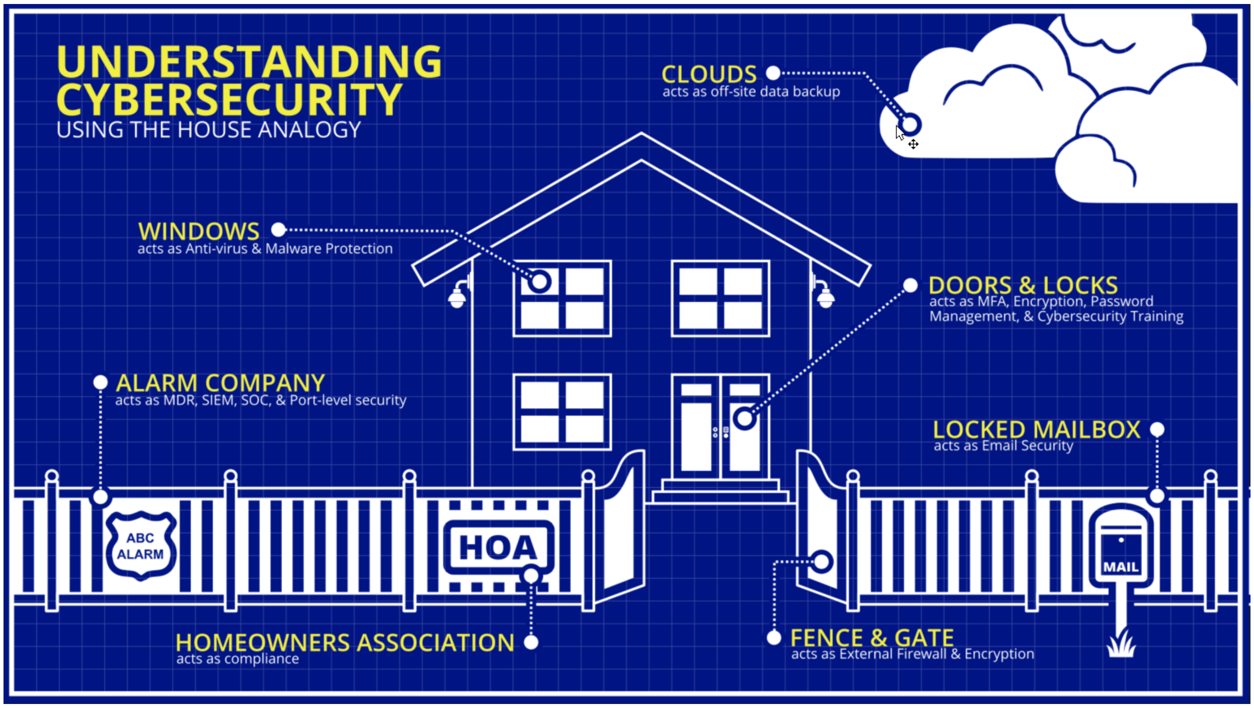
Cybersecurity Important:

Multilayered security will help limit threats to your organization from malware, phishing, and other more sophisticated attacks. When you think about home security, it is easy to relate to the prevent, detect, and respond methods in action.


UNDERSTANDING CYBERSECURITY
USING THE HOUSE ANALOGY
CLOUDS
acts as off-site data backup
WINDOWS
acts as Anti-virus & Malware Protection
DOORS & LOCKS
acts as MFA, Encryption, Password Management, & Cybersecurity Training
ALARM COMPANY
acts as MDR, SIEM, SOC, & Port-level security
LOCKED MAILBOX
acts as Email Security
ABC ALARM
HOA
MAIL
HOMEOWNERS ASSOCIATION
acts as compliance
FENCE & GATE
acts as External Firewall & Encryption

Fence & Gate:

A Firewall acts as your fence and gate, your first line of defense. A VPN makes it possible to securely access applications and resources remotely that would otherwise be inaccessible from offsite locations, while also encrypting connections and providing some access control for corporate networks.

Locked Mailbox:

Email content control and data leak prevention (DLP) scans subject, body, and attachments to detect, encrypt, or block the sending or receiving of sensitive information.

Door Locks:

Multi-Factor Authentication (MFA) is a security enhancement that uses multiple barriers to entry to prevent hackers from gaining access to personal information and sensitive corporate data. Encryption protects digital data stored on computer systems and as it is transmitted using the internet or privately to other computer networks. Password management keeps login and password credentials private. Security awareness training equips everyone in an organization with the information they need to protect themselves and their organization’s assets from loss or harm.

Windows:

Anti-Virus and Malware prevention utilities handle Trojans, rootkits, spyware, adware, ransomware, and more.

Clouds:

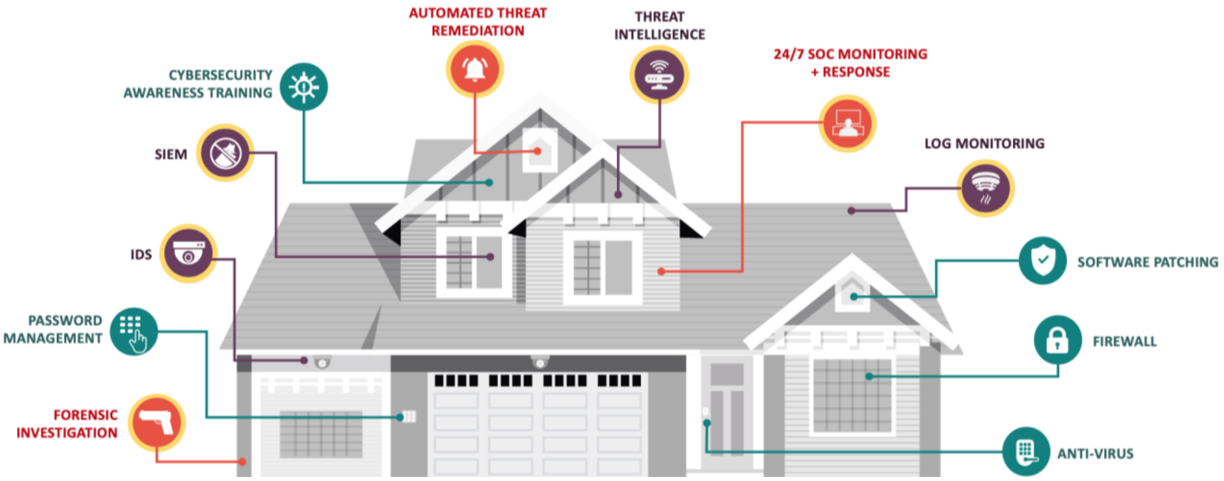
Off-Site data backup is essential in today's world of ransomware attacks to help recover stolen data, continue working and prevent further revenue loss.

Alarm Company:

MDR, SIEM, SOC, and port-level security features monitor activity on a network. When unauthorized activity is detected, protections can automatically be invoked and IT teams notified.

HOA:

Compliance mandated by government agencies and industry groups provides incentives (like avoiding fines and other punishments) for proving the use of cybersecurity best practices.



Here are some important security questions to consider:

Are you assuming your Perimeter Defense is perfect?
What if the attack gets past your Firewall and Anti-Virus?
Are you confident that every endpoint is always patched perfectly?
Are you confident that every user on your network is safe from phishing scams?
If an employee's network login credentials are compromised, how would you know?
If an IT Admin abused their privileges, how would you know?
How valuable is your sensitive company data? What risk do you face if it is lost or held ransom?
What was the last security incident in your network? How was it found? Fixed? How long had it been in the network? What were lessons learned?
When was your last Audit? How easy was it to demonstrate compliance?