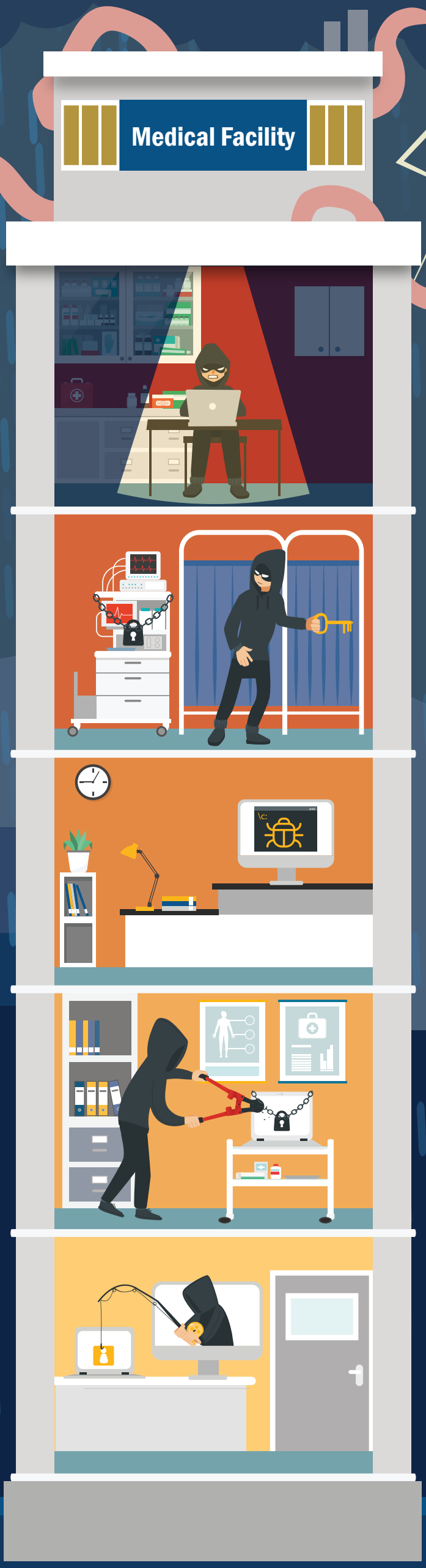
Healthcare Threat Identification

Many threats exist at some level for all healthcare organizations. Threats may be internal or external, natural, or manmade, malicious, or accidental. The impact of these threats to your organization depends on the ability of the threat to exploit existing vulnerabilities. It is imperative that you are aware of the threats that can impact your environment in-order to protect your valuable PHI.



THREAT

Ransomware Attack

Ransomware is a type of malware (malicious software) who's defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the attacker who deployed the malware, until a ransom is paid.

Denial of Service Attack

Once a virus has infected your network, an attacker can implement a denial-of-service attack, which makes resources on your network completely unavailable. This can impact patient care and disrupt service to all of your network, medical records, and medical devices.

Virus Attack

Once a virus is injected into your environment, it can be detrimental to your network by corrupting the system or destroying valuable healthcare data.

Brute Force Attack

An attacker can use a brute force attack to gain access to your network through attempting multiple combinations of numeric passwords until a match is found. This will allow them permission into your environment where all your valuable PHI data is stored.

Social Engineering

Many attacks begin with a phishing email containing a malicious link and if clicked can create serious cybersecurity risks to the network and organization. The attacker could potentially gain access to sensitive patient data the organization maintains.

REMEDIATION

Audit your software applications at each endpoint. Maintain a list of approved software applications. Remove unauthorized software applications as soon as they are detected

Create a baseline for your network and monitor unusual network activity. If there is a huge spike in traffic, that could indicate volumetric denial of service (DoS) attack. Any kind of traffic that deviates too far from the norm should lead to the quarantining of an endpoint. This can help mitigate the damage when a breach occurs.

Organizations should ensure that basic spam/ anitvirus software solutions are installed, active, and automatically updated wherever possible

Limit the rate at which authentication attempts can occur. Try spacing out each password attempt by a second or two which can severely limit the ability of systems to brute force the password.

Multi-Factor Authentication (MFA) should be implemented on remote-access technologies to limit the value of password credentials that could be compromised through phishing or malware attacks. MFA is an incredibly impactful method for limiting an attacker's ability to compromise your organization's environment.

HHS 405(d)
Aligning Health Care Industry Security Approaches

To learn more about how you can protect your patients from cyber threats check out the **Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients** publication. Check out the available resources 405(d) has to offer by visiting our social media pages: **@ask405d** on **Facebook**, **Twitter**, **LinkedIn** and **Instagram**!