This is the sixth of a series of documents created by St. Andrew's parishioner Kelly Bourne, a retired computer security professional.

Cyber-safety Article #6 Ransomware

Ransomware is a cybercrime that encrypts files and devices, preventing them from being used. Desktop computers, laptops, smart phones, servers, entire networks and other electronic devices can be locked up by a ransomware attack. Ransomware attacks have been launched against individuals, small businesses, large corporations, government institutions, non-profits, schools and hospitals.

To regain access to their files or devices victims must pay a ransom. Ransom payments must be made in cryptocurrency like Bitcoin, so the criminals remain anonymous. Victims expect that after paying the ransom the criminals will provide a key to unlock the files or devices. Unfortunately, there is no guarantee that the key will be provided. Sources differ widely, but some say as many as 35% of victims who pay the ransom never receive a decryption key.

Ransomware is expensive for corporations and other victims. Wired magazine reported that over one billion dollars was paid in ransom in 2023. For large organizations the average ransom in 2024 was almost 2.75 million dollars according to several sources. Whether or not the ransom is paid, victims can spend millions on related costs like restoring the data, consultant fees, lawyers, new security software, fines and PR costs. Money spent on ransom isn't available for salaries, raises, bonuses, expansion, or new technology. A business that experiences ransomware-related losses won't grow as much and could even go bankrupt.

The majority of ransomware attacks begin in the following ways:

- Phishing emails that have an infected attachment or a dangerous link in the email's body.
- Pop-ups ads seen in Internet browsers can install malware, including ransomware, if clicked.
- Many individuals and organizations have installed remote access tools on computers so work can be done remotely. These access methods can be exploited by criminals.
- Users or employees viewing websites that have malware on them. In many cases legitimate websites have been infected.
- Installing pirated software or infected applications onto their computer or smart phone.

To pay the ransom or not to pay it is a critical decision. Some factors that must be considered before deciding are:

- Law enforcement agencies advise victims not to pay because doing so encourages criminal activity.
- There's no guarantee that paying the ransom will get your files or computers unlocked.
- If computer files weren't previously backed up it might be impossible to recover without paying the ransom.
- Time critical situations like hospitals or production facilities may require that the systems be restored as quickly as possible even if it means paying a criminal.
- In some countries it's illegal to pay ransom to get files unlocked.
- Organizations that pay ransom are likely to be targeted again. One source says 80% of organizations that pay ransoms are hit with another attack.

Recovering from a ransomware attack can be time-consuming and expensive. Actions that are typically taken include:

- Ensuring that all malware, not just the ransomware, gets removed from the system is critical. It's common for ransomware to be accompanied by other malicious software.
- Rebuilding a computer or entire network takes time. Recently created backups can speed up the process significantly.
- Breach notifications to customers, clients, patients, etc. may be required if personally identifiable information (PII) has been compromised.
- Expose of PII may result in lawsuits from affected individuals or fines from government agencies.

- The organization must identify how the ransomware got onto the system so future similar attacks can be avoided.

Some steps that can help avoid becoming a victim of ransomware are:
- Keep all software updated since updates frequently contain security fixes. This includes operating systems, smart phones, browsers, applications and anti-virus tools. If possible, have updates installed automatically.
- Install reputable anti-virus software onto computers and phones.
- Install firewalls to protect computers from suspicious activity to and from the Internet.
- Install email filtering so users see fewer spam and phishing emails.
- Activate pop-up blockers in browsers so users aren't bothered by pop-up ads.
- User training can teach employees not to open phishing email attachments or click on suspicious links.
- Limit access and permissions that users have. This can prevent ransomware from spreading from one computer to every device on the network.
- Regularly backing up data won't prevent ransomware attacks but will make recovering from them easier.

Even people that aren't the direct target of ransomware can still be affected by it.
- Some ransomware attacks disclose individuals' personal data like social security numbers, account numbers, passwords and email addresses. This can result in becoming the victim of identity theft or account takeover attacks.
- When businesses are attacked it threatens their health or survival. The worst scenario could shut the company down. Less severe scenarios could result in employees being laid off. One study showed that almost 40% of organizations let some employees go after a ransomware attack.
- Hospitals, schools and local governments are frequent targets of ransomware. Patients, students and citizens depending on them for services are impacted.
- Companies that provide goods and services to individuals and other organizations can be crippled by ransomware attacks. The impact on the supply chain attacks can impact thousands.
- Businesses like retailers, airlines, hotels, casinos and entertainment venues can't operate normally during an attack or while recovering from one. This can impact consumers throughout the country.

The future of Ransomware
- Some cybercriminals are applying artificial intelligence (AI) to make their attacks more likely to succeed and more damaging to victims.
- Internet of Things (IoT) devices like smart TVs, HVAC systems, printers, security cameras have been impacted by ransomware and other types of attacks. As more IoT devices come online this threat is certain to increase.
- A new variation of ransomware called multi-extortion ransomware also steals an organization's data. Unless a second ransom is paid the stolen data is sold or exposed publicly.
- Ransomware as a Service (RaaS) is a business model where the creators of ransomware allow other criminals to use it in return for a share of the profits. This results in the ransomware attacking a greater number of victims.

Ransomware is a threat to computers and smart phones around the world. The most important steps that people can take to protect themselves are to keep your computers, including smart phones, updated. Another important protection is to be extremely cautious when opening email attachments or clicking on links in emails.

- Kelly Bourne