Beyond Scattergun: The new face of ransomware

The war on digital security is being fought on different fronts. Cyberattacks themselves are more common, and the type and impact has changed. Viruses used to focus on system damage and data destruction, typically randomly infecting as many systems as possible. Now, ransomware attacks are more carefully considered to maximize the hackers' return.

Cyber-crime is big business

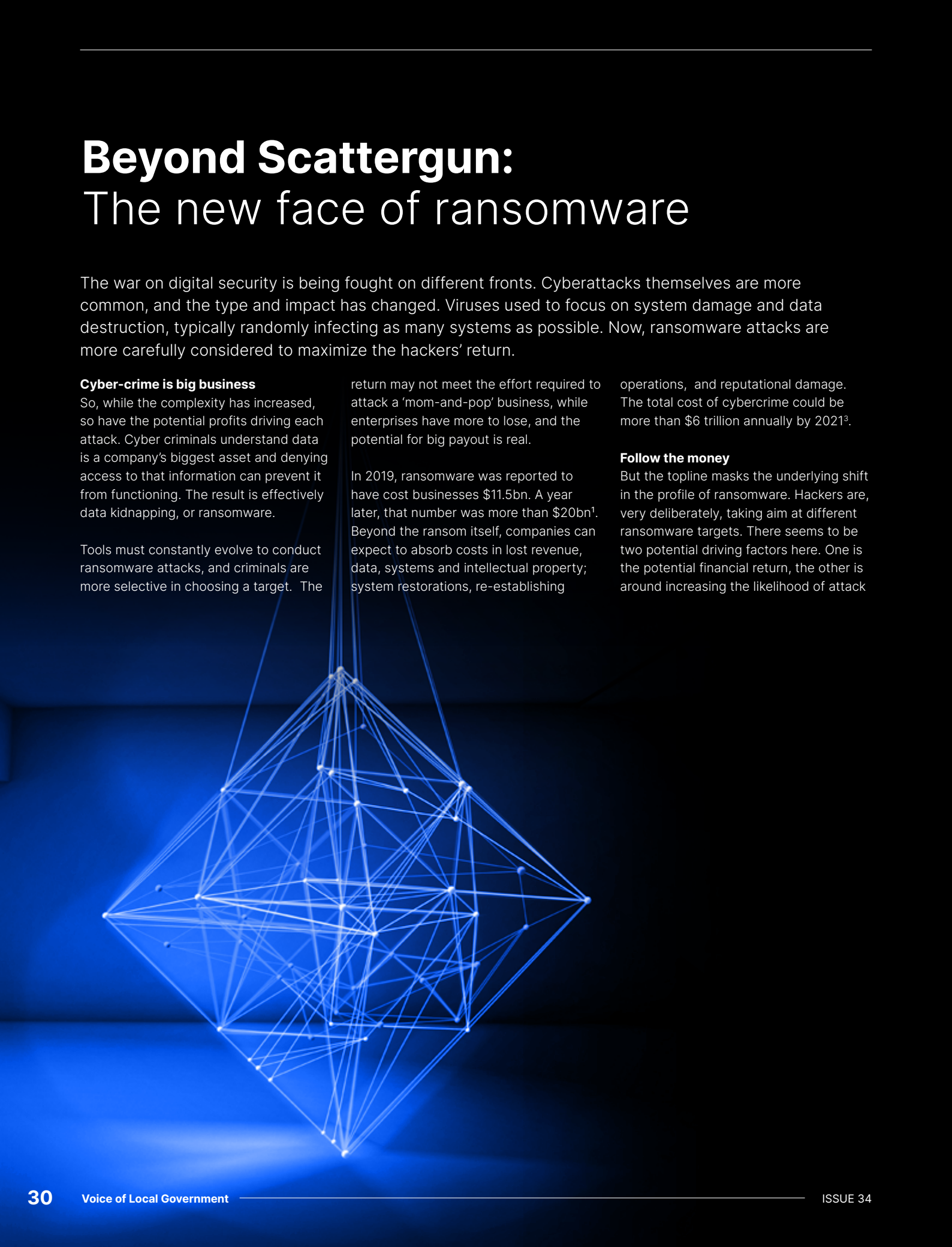
So, while the complexity has increased, so have the potential profits driving each attack. Cyber criminals understand data is a company's biggest asset and denying access to that information can prevent it from functioning. The result is effectively data kidnapping, or ransomware.

Tools must constantly evolve to conduct ransomware attacks, and criminals are more selective in choosing a target. The return may not meet the effort required to attack a 'mom-and-pop' business, while enterprises have more to lose, and the potential for big payout is real.

In 2019, ransomware was reported to have cost businesses $11.5bn. A year later, that number was more than $20bn[1]. Beyond the ransom itself, companies can expect to absorb costs in lost revenue, data, systems and intellectual property; system restorations, re-establishing operations, and reputational damage. The total cost of cybercrime could be more than $6 trillion annually by 2021[3].

Follow the money

But the topline masks the underlying shift in the profile of ransomware. Hackers are, very deliberately, taking aim at different ransomware targets. There seems to be two potential driving factors here. One is the potential financial return, the other is around increasing the likelihood of attack



success.The US and Europe have always been priority targets, but the scatter-gun approach hits everyone indiscriminately. This Sophos report[2] shows a marked shift to wealthier, more stable countries and those with poor cyber-defenses. Well-resourced countries are better prepared to combat ransomware and are therefore less likely to be targeted.

Their lower GDP may have put South Africa, Poland and Philippines further down the list of organizations most recently hit by ransomware, with South Africa falling from a previous incidence rate of 54%, to 24% in the most recent report[2]. Public sector organizations are least likely to be targeted, with 45% of respondents reporting an attack, however, this is only 6% below the average of 51%2.

Consequences and the Covid effect

But no country or organization can afford to be complacent. The threat is real, as the WannaCry ransomware attack on the UK's National Health Service (NHS) in 2017 proved. The UK government had to make up £19m in lost output and £73m in IT costs.

The DarkSide ransomware gang attack on the US's Colonial Pipeline in May of 2021 shut down one of the East Coast's main oil supply lines, affecting multiple states for five days. Many garages ran out of fuel, sparking panic buying and triggering a state of emergency in several locations. News outlets report that the company paid $5,000,000 in bitcoin to the hackers.

Both examples prove ransomware attacks are not 'just' a business issue, but can easily become public emergencies affecting healthcare, communications, transport, and other critical infrastructure. Despite increased protection, the attack froze the core operations of Colonial Pipeline. The initial, but unproven belief is that hackers gained access through phishing emails and the personal equipment of home workers. The pandemic has created new hacking opportunities as workers access systems through less secure methods.

Ransomware recommendations

Ransomware attack prevention is multi-faceted; each element must be thorough, and maintained. The first step is to ensure systems and software are updated with the latest versions and all security patches applied. The WannaCry worm exploited a Windows vulnerability for which a patch had already been issued, but not applied by many organizations.

Updated systems need defending by anti-virus and anti-phishing software. Again, these must be updated regularly to keep up with constantly-evolving hacker efforts to find and exploit new vulnerabilities. Deploying analysis software to monitor systems, data, and networks for unusual behavior can indicate an attack is in progress and attempt to stop it.

While electronic defenses will prevent many problems, the major attack route remains employee behavior, with 45% of organizations reporting ransomware accessed their system either as a file download or via email[2]. Educating the workforce will reduce the incidence of ransomware ingress by increasing and maintaining awareness.

Ultimately, it is wise to assume an attack will occur, and organizations will be compromised. A robust backup process is needed. Hiding data in the cloud does not makes it safe from attack and subsequent encryption, as almost six in 10 ransomware attacks encrypted data in the public cloud[2].

OpenText Data Protector is a comprehensive backup solution that supports the 3-2-1 rule for backup. The rule requires three backup copies of the data to be made and held on at least two different media types such as tape, disk, cloud, virtual, or physical, with at least one copy held in an off-site location, detached from the network. A comprehensive and integrated management and reporting capability ensures backups are completing on schedule and within their SLAs.

A single backup software tool, protecting all data is the simplest and most cost-effective solution. It will back up everything from lower importance data on older servers, to mission-critical applications and data running on the latest storage infrastructure or virtual machines. Being able to direct backup to different locations and media types, and move them when required, offers the best protection. Regularly testing restore operations will ensure quick and efficient data restoration should the worst happen.

Reverting to backups following an attack is not ideal. It takes time and causes disruption, but is far less costly in money and resources than paying a ransom, hoping the data is encrypted and then rebuilding the systems to get them operational again. It is a lesson businesses would do well to not learn the hard way.

References:

[1] Coveware 2020 Ransomware Marketplace Report

https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report#1

[2] Sophos: The State of Ransomware 2020

https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

[3] Cybersecurity Ventures: 2019 Official Annual Cybercrime Report

https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

opentext™

44-1635-565-784

OpenText.com

The Lawn 22-30 Old Bath Road
Newbury, Berkshire