CrowdStrike Products

CROWDSTRIKE

RANSOMWARE REALITIES FOR SMALL AND MEDIUM-SIZED BUSINESSES

All organizations can be the target of ransomware, where users' files or computers are taken hostage or system access is hindered until a ransom demand is met. And although **big game hunting** is on the rise — where ransomware operators target large enterprise organizations to gain huge payouts — ransomware is frequently aimed at small and medium-sized organizations, including state and local governments, which are often more vulnerable to attacks. Organizations of all shapes and sizes should continue to stay alert and on top of their security. This paper explains the impact of ransomware on small and medium-sized organizations, explores factors that lead to increased vulnerability and offers advice on how to protect and secure your organization.

Verizon reported in its 2019 Data Breach Investigations Report that 43% of breaches involved small business victims. And unfortunately, only 30% of small businesses believe their IT security posture is strong against threats.

RANSOMWARE ATTACKS: SIZE DOES NOT ENSURE SAFETY

Small and medium-sized businesses (SMBs) fuel the economy, contributing to growth and innovation, but they often trail behind their larger counterparts when it comes to cybersecurity, leaving them vulnerable to malicious attacks. A cybersecurity lag had not worried SMBs in the past, as many believed their organizations fell under the radar for attacks and ransomware. While that attitude appears to continue for some businesses, recent studies suggest that times may be changing.

A study conducted by **Paychex** in 2017 reported that 68% of SMB owners were not worried about being hacked. That mindset was confirmed in a more recent **study** from 2019, where 66% of SMB decision-makers believed they were not a likely target. But another 2019 study suggested that awareness and concern may be changing. A **report** released in late 2019 by the National Cyber Security Alliance (NCSA) noted that 88% of the smaller-sized organizations it polled believed that they are at least a "somewhat likely" target for cybercriminals, including almost half (46%) who believe they are "very likely" a target.

While risk perception may vary, as different studies suggest, there is good reason for growing concern: Verizon reported in its **2019 Data Breach Investigations Report** that 43% of breaches involved small business victims. And unfortunately, only **30%** of small businesses believe their IT security posture is strong against threats.

SMBs HAVE WHAT ADVERSARIES WANT

Small businesses are targeted for a number of reasons, from money and intellectual property (IP) to customer data and access.

In fact, access may be a primary driver because an SMB can be used as a vector to attack a larger parent organization or the supply chain of a larger target. Small business owners may not realize their value to attackers, as many news reports involving ransomware highlight attacks on larger organizations more often than smaller ones, perpetuating a false sense of security that ransomware attacks are related to size and profitability.

SMALL SIZE, BIG LOSS: SMBs HAVE A LOT TO LOSE

Cybercriminals have a lot to gain by targeting SMBs, and unfortunately, SMBs have even more to lose. According to **KnowBe4**, the average ransom requested from SMBs is about $4,300 USD. While that amount may seem insignificant, the same report noted that the average cost of downtime related to a ransomware incident is much higher, at about $46,800 USD.

Some ransomware attacks encrypt computer files and hard drives, locking users out of their devices and data, while other variants of ransomware can access user data and release or sell it to third parties, leading to data breaches and higher losses.

While larger organizations — including **FedEx**, which was hit by NotPetya ransomware and attributes the attack to $300 million in losses — are better equipped to absorb huge losses and continue to prosper, that is not the reality for many small businesses. Smaller organizations can lose more than just money in a ransomware attack — the attack can damage their reputation and diminish their chance of survival. Research indicates that **60%** of SMBs in the U.S. that experience cyberattacks go out of business within six months.

Due to their smaller size and limited resources, SMBs have a harder time absorbing the extra cost of a ransomware attack and the strain on customer relationships. And the perception that they are not a target means smaller businesses often don't have the personnel or cybersecurity budget in place to protect themselves, making a bad situation even worse. The **Ponemon Institute** study noted that 77% of small businesses said they didn't have the personnel to mitigate cyber risks and breaches, 55% didn't have the budget and 45% didn't know how to protect themselves against attacks.

The idea of a ransomware attack shutting down a business may seem unrealistic, but unfortunately, it is a real risk.

COMMON VULNERABILITIES

The success of ransomware attacks on small businesses can be attributed to the unique challenges associated with smaller size and also the more ubiquitous challenges faced by organizations of any size: the human element.

While a work-issued computer is common and even expected in larger organizations, smaller organizations do not always provide work computers and instead can rely on employees using their personal devices. These devices are used both for work-related purposes, including accessing and storing privileged documents and information, along with personal activities such as browsing and searching. These dual-purpose machines contain high volumes of both business and personal information, including credit card information, email accounts, social media platforms, and personal photos and content. **AppRiver's 2019 survey** discovered that 48% of SMBs do not store their most important and confidential data exclusively on a secure network and instead disperse it across multiple unsecure locations or are unsure of where the data is stored. Data access and storage blind spots along with inconsistent or inadequate security coverage quickly lead to gaps in cyber protection, increasing risk.

HEALTH HORRORS

In April 2019, Brookside ENT and Hearing Services, a small medical practice run by two doctors in Michigan, was hit with a **ransomware attack** that deleted and overwrote every medical appointment, bill and patient record. It also deleted the backups and left behind a duplicate of the deleted files that could be unlocked if they paid $6,500 USD in ransom. The doctors refused to pay the ransom and continued to show up to the office to assist patients. Because the files and records were deleted, they had no way of contacting the patients to cancel or reschedule appointments. After a few grueling weeks, the practice was forced to shut down, and the doctors settled for an early retirement.

This is the first case in which a medical practice had to shut down due to a ransomware attack. In this case, like many others, having backups in place was not enough to protect against a ransomware attack, and the small practice was forced to shut down because it was not able to absorb both the financial and time-consuming burdens necessary for remediation.

THE HUMAN FACTOR

For organizations of any size, employee behavior — from oversharing on social media to clicking any link that comes their way — is a concern, and it is a definite risk factor for smaller organizations. In fact, **77%** of SMBs are concerned about social media use as a cybersecurity risk, highlighting Facebook as a major concern for employees. Social media platforms are hubs for spam accounts, and while many can be harmless, certain accounts contain well-disguised pop-ups and web links that lead to ransomware. Employees may also overshare on Facebook and attract potential scammers that can conduct research on the business and launch social engineering efforts. Social engineering can take many forms, including simple fake accounts gathering information to full-blown spear-phishing attacks claiming to be an employee's boss or colleague. Spear-phishing via compromised emails is the primary point of entry for many ransomware attacks. Victims more often fall prey to opening these emails and clicking the links within since the sender appears to be a known entity from a trusted source, colleague or manager.

KnowBe4 released results of its phishing email testing services and revealed that of the users that clicked on the phishing email tests, 56% were related to LinkedIn messages. Social media platforms such as LinkedIn and Facebook are generally trusted by users, making those channels prime sources for collecting information and fueling phishing campaigns.

In fact, 77% of SMBs are concerned about social media use as a cybersecurity risk, highlighting Facebook as a major concern for employees. Social media platforms are hubs for spam accounts, and while many can be harmless, certain accounts contain well-disguised pop-ups and web links that lead to ransomware.

HOW TO PROTECT AGAINST RANSOMWARE

In September 2019, the **U.S. Department of Homeland Security** published an article outlining measures organizations should take to handle the threat of ransomware. The article provides advice on how to protect against ransomware, how to prepare for a potential incident, how to recover and where to find help. It includes practical recommendations ranging from keeping systems patched and up to date to training end users and creating and executing an incident response plan.

Keep in mind, while backups are a good defense, they must be protected as well, as they are often the first targets attackers prohibit access to or try to destroy in an environment. Making sure files are backed up, are properly secured and can be accessed separately, even in a compromised environment, is a standard precautionary measure and also effective for faster remediation in the event of a ransomware attack.

Implementing proper employee training is also an essential practice to help keep your brand and your business secure. Keeping employees up to date on awareness practices — including not clicking links or downloading attachments from suspicious emails and checking email addresses of senders — is essential for reducing phishing entry attempts.

Adopting an effective endpoint protection solution is another key method to defend your organization. Fortunately, CrowdStrike provides next-generation endpoint protection to help SMBs flourish.

CROWDSTRIKE SOLUTIONS FOR SMALL AND MEDIUM-SIZED ORGANIZATIONS

CrowdStrike® security experts understand that smaller organizations face different challenges than larger ones, and they also know that smaller organizations often face the same threats and need the same standard of protection.

The CrowdStrike Falcon® next-generation endpoint protection platform uses an array of complementary prevention and detection methods to fight against constantly shifting ransomware techniques. The Falcon platform includes the following:

- **Machine learning** for the prevention of both known and previously unknown or "zero-day" ransomware, without requiring updates
- **Exploit blocking** to stop the execution and spread of ransomware via unpatched vulnerabilities
- **Indicators of attack (IOAs)** to identify and block additional ransomware behaviors and protect against fileless attacks and new categories of ransomware
- **Automated threat analysis** to immediately obtain all details about the ransomware found, including origin, attribution, similar families and IOCs (indicators of compromise)

CrowdStrike offers various endpoint protection packages to provide you with the right solution to match your security needs, ranging from **Falcon Pro** with next-generation antivirus to **Falcon Complete**™, where all of your endpoint security needs are handled by CrowdStrike's experienced team.

As headlines continue to remind us, ransomware remains a significant threat. CrowdStrike is committed to defending against ransomware by evolving and innovating its security technology to stay a step ahead of the most determined adversaries. A combination of elements is required to adequately protect your organization, including taking practical steps to align your security strategy with sound practices, and deploying the innovative, cloud-native, next-generation prevention and detection technology provided by the CrowdStrike Falcon platform.

Start Free Trial
of Next-Gen AV

Learn more at **www.crowdstrike.com**

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the organization, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches.

Speak to a representative to learn more about how CrowdStrike can help you protect your environment:

Phone: 1.888.512.8906
Email: sales@crowdstrike.com
Web: www.crowdstrike.com