allot
See. Control. Secure.

Addressing Cybersecurity for Small & Medium Businesses

June 2023

Contents

1. Introduction

Due to the rise in the use of ransomware, the business world has been compelled to protect their valuable data from cyberattacks. Large enterprises have a lot to lose and therefore have dedicated teams in place when it comes to security. But it is the small and medium businesses who lack the resources to protect the company data that can lose everything they have created with just one breach.

Market data clearly shows that small businesses are not prepared to handle cyberattacks but these attacks can easily put them out of business. ***This creates a clear and present danger to small and midsize businesses who***, ACCORDING TO MARKET STUDIES, ***suffer the vast majority of cyberattacks.***

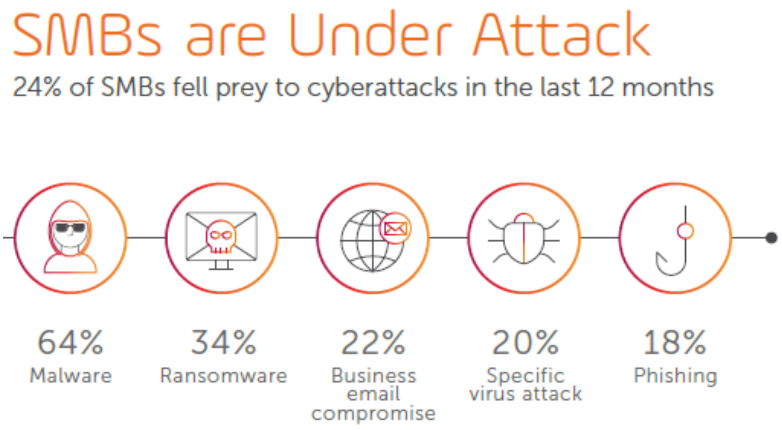
However, because SMBs need to have a communication service provider (CSP) in place for their connection to the internet, they can rely on those CSPs to provide a security solution. SECaaS (Security as a Service) is now being offered by some CSPs to SMBs, providing a robust cybersecurity solution that any business can afford without the need for them to have internal IT personnel in place.

2. SMBs are Easy Targets for Cyberattacks

As SMBs increasingly move to digitization to realize maximum potential for their businesses, reliance on information technology, mobility, IoT and the internet becomes a standard practice. Because larger enterprises understand the need for dedicated cybersecurity personnel or a Security Operations Center (SOC), they have budgeted the resources to create and run such a team. For SMBs that might not have the ability to adequately support the security function, the consequences of a security breach can be devastating.

RESEARCH IN JANUARY 2020 BY BULLGUARD shows that small companies are poorly prepared when it comes to cybersecurity defense. According to the report, more than two in five companies that have 50 or fewer employees in the US and UK don't have any type of cybersecurity defense plan in place. Research collaboration between Cisco and the NATIONAL CENTER FOR THE MIDDLE MARKET based on data from 1,377 CEOs of small and midsize businesses showed that 62% of these firms do not have an up to date or active cybersecurity strategy or any strategy at all.

This makes SMBs an attractive target. ACCORDING TO INC., the vast majority of cyberattacks happen to small and midsize businesses. Cybercriminals are looking for fast profits.



Source: Telcos: Protect Your SMB Customers, SMB Security Survey, Allot Q4 2021

Once bad actors have an entry into the network, they are either looking to sell valuable personal identifiable information (PII) or lock up the company data for ransom. Instead of trying to take down a major corporation for a big pay day, it is easier to go after the many smaller companies worldwide.

And this isn't a theoretical threat. Data from an **OCTOBER 2020 STUDY BY KEEPER SECURITY AND THE PONEMAN INSTITUTE** shows that fifty-eight percent (58%) of respondents say their organizations experienced a compromise that damaged IT infrastructure or stole IT assets.

In an extensive survey of 8,000 consumers around the world undertaken by Allot and conducted by London-based Coleman Parkes Research, a quarter of respondents said they experienced a cyberattack in the past 12 months! The cost of such an attack might run more than $200,000, which can shut down the company completely. In addition to the threat of attack, the loss of work hours while systems are being restored costs money, too. According to CISCO'S 2020 CISO BENCHMARK STUDY, 46% of SMBs with fewer than 1000 employees had 5-16 hours of breach-related downtime in 2019.

Source: Telcos: Protect Your SMB Customers, SMB Security Survey, Allot Q4 2021

With the stakes so high, these companies have plenty to lose, and, as reported in Inc., quoting a widely circulated statistic, the price to be paid can be devastating - *fully 60% of small businesses fold within six months of a cyberattack!*

The owner of a small company can try and take the risk of avoiding a breach until they have a better solution in place, but they are risking the very future of their companies and taking chances with the livelihood of their employees.

.

3. The Main Attack Vectors

Phishing, or leveraging social engineering techniques to get one person to click on the wrong link, is the most popular way to get to Personal Identifiable Information (PII – phone numbers, emails, etc.). The breached data then gets sold for cheap on the dark web, creating opportunities for attacks from many other bad actors. **Malware** can also be used to enter the network, allowing the attacker to move laterally until they find the critical information they are looking for. Small companies are also susceptible to **ransomware**, where attackers basically stop the small business from continuing to work by locking up their files.

Companies that make it harder for bad actors to enter their networks will see fewer attempts made to compromise their data. Yet, criminals are always inventing new ways to infiltrate organizations. The top reasons cyber-attacks such as ransomware and data breaches have been increasing for SMBs in the past 3 years are due to:

- Remote working and Work from Home (WFH) becoming popular with employees
- Many small companies have a non-functional security system in place and no dedicated personnel to oversee the security situation
- Easy access to DIY criminal tools and PII for sale on the dark web
- Companies have been willing to pay the criminals in their currency of choice (usually Bitcoin) to get on with business by experiencing success and profits with very little chance for repercussions, bad actors have every reason to continue to attack these easy targets

Smaller businesses have simply become low-hanging fruit for cybercriminals. So why aren't the smaller companies focused on better network security?

Companies with less than 50 employees do not usually have a dedicated IT person, sometimes relying on an antivirus or an off-the-shelf solution for their security needs. Even this type of software needs to be installed correctly and must be updated and maintained to be effective. If an IoT device is introduced to the network by an employee, it wouldn't be covered by the antivirus. There are simply too many entry points that could possibly fail for an organization that doesn't have the bandwidth to oversee and react to potential breaches.

If financial loss and the many hours of downtime aren't enough incentive to develop greater security measures, sometimes it is demanded by the SMB's customers. A small company that is a partner or customer of a supplier can be used by a hacker as a backdoor into that supplier, exploiting the implicit level of trust held between the two companies. While the supplier will have a security system in place, this can be evaded by infiltrating the less secure smaller company.

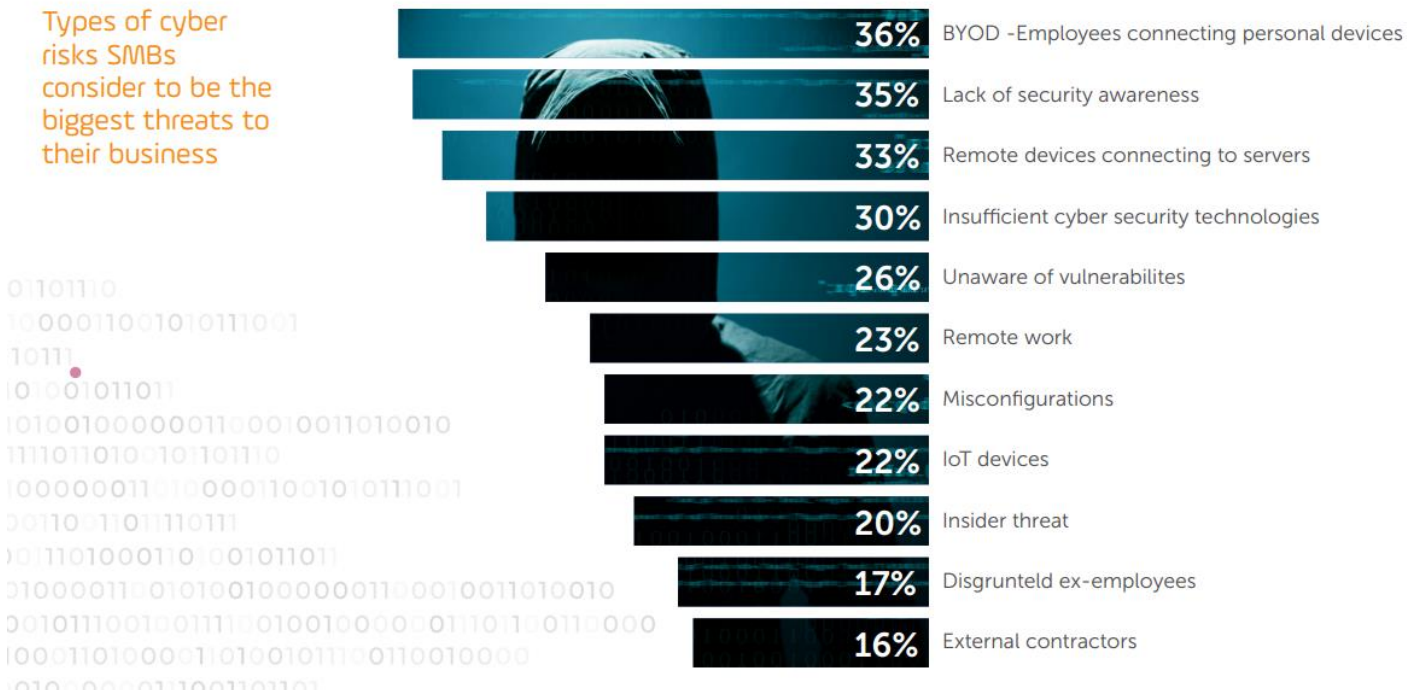
Another attack vector utilized by cybercriminals is **Distributed Denial-of-Service (DDoS)** attacks. DDoS attacks occur when cybercriminals recruit millions of connected devices and have them simultaneously attack an online service or website. Cybercriminals can infect and recruit devices on the business network and use them to launch an outbound DDoS attack that goes out through the SMB's connection to the CSP network. These outbound attacks decrease the SMBs network performance and services as well as generate large amount of traffic which could clog the network, negatively affecting communication of other devices on the network.

4. IoT and BYOD

As IoT and connected devices proliferate, network management and cybersecurity become ever more critical for SMBs. The growing prevalence of Bring Your Own Device (BYOD) practices further increases the risk of infected business networks. Employees who are using devices with access to the company network while at their house or at a coffee shop or on the road instead of within the office are exposing the company to potential infiltrations. If they experience a Man in the Middle attack (MitM) or pick up a malicious software from an unsecured site, they simply bring the problem back to the company.

Just because the resources available to small businesses for security may be slim, it doesn't mean that there is a lack of awareness as to the importance of handling these issues. Every week there is another headline involving major cyberattacks, either business-related or politically motivated. There is clearly a need for protection in the following areas:

- **Keeping employees off dangerous or inappropriate sites**
- **Protecting employees from malware, phishing, and other cyber attacks**
- **Extending protection to fixed and mobile devices when employees are connected outside the corporate network**



Source: Telcos: Protect Your SMB Customers, SMB Security Survey, Allot Q4 2021

5. An Effective Solution for SMB Security

Eager for security solutions without complexity and without the need to invest large amounts of resources in both time and money, many small businesses are turning to service providers for their cybersecurity needs. Service providers are in a unique position in the market because they can touch all network traffic in and out of increasingly complex SMB environments, on fixed and mobile, ensuring that workers' devices stay safe, whether at the office, home or on the road.

Such security services can include:

- Threat protection against phishing, malware, and viruses
- Content filtering of inappropriate internet content
- Network Firewall functionality to prevent unwanted connections and communication

Threat Protection:

Viruses, ransomware, phishing, crypto-jacking, and spyware are among the many threats businesses face every day. Network-based threat protection can keep the small business safe against all kinds of malware and online threats. These threats can cause major disruption to business operations, financial loss, compromise customer data, and damage the company's reputation. The security protection services would:

- Protect all on-premises PCs and devices instantly against malicious sites
- Check every website request for threats
- Offer Zero-touch deployment delivers protection via the network
- Not require IT expertise or management
- Provide reports of security level and threats blocked
- Automatically learn and protect against new attacks

Content Filtering:

Internet connectivity is vital to any business, but it can also seriously damage productivity. Employees can be easily distracted and waste time and network bandwidth. Employees and the business itself can be protected by having access to inappropriate and offensive content automatically limited or blocked. Content filtering services that can be defined by the business owner would:

- Restrict content access by blocking employees from visiting offensive or inappropriate websites that damage productivity and put the company at risk. It would filter requests from all PCs and devices according to the categories selected (i.e. gambling, pornography, ecommerce, social media)
- Increase productivity and reduce risk of inappropriate behavior
- Block or allow specific sites, listing websites that the business wants to always block or allow, that override the category definitions. For example, allow specific ecommerce sites used for business procurements.
- Provide notifications when an employee attempts to access restricted content

Network Firewall:

A Network Firewall service gives small businesses additional visibility and control over their Internet traffic, complementing the threat protection and content filtering services. These services should include:

- Rules based on source, destination, service, and action.
- Pre-configured rules for typical use cases
- A GUI suitable for small businesses without firewall expertise, including wizard-driven rule creation

6. Conclusion

SMBs do not have the resources to adequately secure their networks from the increasing wave of cybercrime. To be effective, there should be 24/7 protection, and this is beyond the reach of all but the largest companies. Cybercriminals understand this concept, which is why they target the SMBs on a constant basis with phishing, malware, and ransomware. The most effective way for these smaller businesses to protect their data assets is through the connection to the internet as provided by their communications service provider. CSPs around the world have started offering Security as a Service to small and medium-sized businesses, as a flexible and affordable solution that does not require cybersecurity expertise. This is the least expensive, most comprehensive and expeditious way for SMBs to get protection against the increased cybercriminal activities and continue to focus on their core business.