CYBERSCOUT®
A Sontiq™ Brand

SMALL BUSINESS, HUGE RISKS

2020 SMB Cyberscurity Survey

Cyberattacks among largest risks SMBs face today

INTRODUCTION

2020 has been a record year for cyberattacks on consumers, public institutions and businesses of all size. Small and medium size businesses (SMBs) have seen some relief in 2020 as hackers switch focus to large organizations with remote workforces during the pandemic.

When you consider that the average cost of an insider-related cyber incident is $7.68 million for small businesses with less than 500 employees[1], cyberattacks are undoubtedly one of the largest risks SMBs face today.

Small business leaders must begin prioritizing the protection of their business networks and digital assets as well as the security and privacy of their customer data.

With more than 31.7 million small businesses, and 60.6 million small business employees, in the U.S.[2], it is imperative that business leaders, cybersecurity experts and the government work together to prevent fraud and business disruption from hurting our economy and siphoning billions in funds and valuable private personal information to hackers and dark web forums across the globe.

In honor of National Cybersecurity Awareness Month, Cyberscout, a global leader in cybersecurity and identity theft resolution services, has released the findings of a 2020 survey of 2,055 small and medium-sized (SMB) U.S. business owners. The survey sought to understand SMB leader's awareness, knowledge and concern about top cybersecurity issues facing businesses today.

51% of U.S. companies **DO NOT HAVE AN ONGOING TRAINING PROGRAM** on cybersecurity best practices. While most respondents (76 %) felt secure about their company's cybersecurity infrastructure, the survey found that several training, cybersecurity and insurance best practices still have not been widely adopted by U.S. SMBs.

[1] https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#/

[2] https://cdn.advocacy.sba.gov/wp-content/uploads/2020/0 6/04144224/2020-Small-Business-Economic-Profile-US.pdf

TOP CYBERSECURITY CONCERNS

Ransomware attacks continue to pose a significant threat to SMBs

Ransomware is one of the most sophisticated and harmful cyber threats businesses face today, and small to medium-sized businesses are most frequently affected by these attacks. According to insurer Beazley Group, nearly 70 percent of ransomware attacks in 2018 targeted small businesses.

Cyberscout's survey found that 16 percent of surveyed SMBs reported having already fallen victim to a ransomware attack.

With proper incident response being a key element of mitigating the damage of any cyberattack, Cyberscout posed a series of questions to SMB leaders about how they would respond to a ransomware attack which could result in permanent loss of business data, reputation destroying exposure of sensitive customer data and not being able to continue conducting business during the attack.

Top Cybersecurity Concerns:

30%	DATA BREACH
17%	MALWARE
10%	RANSOMWARE
10%	PHISHING

Insurance reality:
4-IN-5 managed service providers (MSPs) identified **RANSOMWARE ATTACKS** as the leading malware threat to SMBs[3].

[3] https://www.datto.com/resources/dattos-global-state-of-the-channel-ransomware-report

What SMB's would do if they fell victim to a ransomware attack:	Cyberscout offers these Do's and Don'ts for responding to a ransomware attack:
45% Would run existing anti-virus software	**DO** Contact IT support before doing anything
22% Would purchase upgraded anti-virus software	**DON'T** Click anything or respond to the demand message
40% Didn't know who to contact if they fell victim	**DON'T** Run anti-virus software — it will eliminate the hacker's trail
12% Would contact their IT team first	**DO** Let your insurance company know about the incident

PANDEMIC HIGHLIGHTS LACK OF PLANNING FOR BUSINESS CONTINUITY

With shelter-in-place orders shocking businesses across the country in early March, the survey found that **more than a quarter (29 percent) of U.S. SMBs went into the pandemic operating without a business continuity plan**.

Hopefully not too little too late, another **30 percent of SMBs created their first business continuity plan in response to the crisis**. This demonstrates that SMB leaders know the importance of having a plan but lack the resources to prioritize crisis planning for their business.

However, nearly one-in-four businesses have not taken any steps to prepare or amend their business continuity plans despite the significant changes the pandemic has made to the way Americans are doing business.

29% of U.S. SMBs went into the pandemic operating **WITHOUT** a business **CONTINUITY PLAN**

CYBERSECURITY BEST PRACTICES NOT BEING ADOPTED DESPITE REMOTE WORK RISKS

The survey found that some fundamental cybersecurity best practices are still not being widely adopted among U.S. SMBs, even in the face of the heightened cybersecurity risks of remote work.

While a majority of companies regularly scan for vulnerabilities (66 percent), a quarter of respondents (25 percent) either do not conduct network vulnerability testing or weren't aware of their company policy.

After most companies shifted to remote working arrangements due to shelter-in-place orders, SMB leaders reported the following:

REMOTE WORK FINDINGS

Only 17% established or reinterated their **IT PROTOCOL** for remote work

34% required a **VPN CONNECTION** to log in to business systems

14% do not follow any **CYBER SECURITY** measures for remote work

Backup Behaviors

With system network backups being a critical element of ensuring business continuity, the survey found that **nearly 16 percent of respondent do not conduct any type of regular system backups**.

Less than a quarter (22 percent) of U.S. SMBs have a backup plan in place in their organization.

Of those companies that do perform regular system backups, 40 percent maintain on-premise and remote back-ups, while 33 percent backup to the cloud only.

Cyberscout empowers people and businesses to take control of their cybersecurity through digital tools and real-life experts that address the increasing threats of online scams and cyberattacks.

FOR MORE INFORMATION call 877-432-7463 or visit us at www.cyberscout.com

CYBERATTACK RECOVERY

Cyber insurance, policies that cover financial losses and offer crisis response services and expert assistance with cyberattack recovery, are becoming more commonplace. Currently, 192 US insurers offered cyber insurance policies in 2019 with both package and standalone cyber products available across insurers[4]. The market for insurance policies may still be concentrated, insurers and cybersecurity services firms are innovating around the clock to create risk mitigation policies and procedures that can provide peace of mind to SMB leaders.

The Role of Cyber Insurance and Cybersecurity Education and Response Services

64% of U.S. SMBs reported **NOT HAVING CYBER INSURANCE** coverage for their business and

5% DIDN'T KNOW if they have any cyber coverage in their current policy.

While the headlines focus on big business breaches, every business leader should be concerned about cybercrime. Business leaders need to look at their own cyber practices to protect critical data and employee information. Leaders must also prioritize workforce education to reduce the chance that hackers can infiltrate the business through an unsuspecting employee.

In addition, todays SMBs should have an integrated cyber insurance policy that includes cybersecurity education services, cyber incident response services such as breach consultation and forensic services with incident response expense coverages that help protect the business from the potentially devastating impacts that can result from a cyberattack.

The landscape of cybercrime is ever changing, and attacks are becoming more sophisticated, but like so many things in life, knowledge is power and the best approach to empowering yourself against cyberattacks is staying informed.

The key to coming out of the pandemic remote work transition stronger, is to embrace that the future of work is digital, and business plans must therefore prioritize cybersecurity as a top business objective.

[4] Aon—US Cyber Market Update: 2019 US Cyber Insurance Profits and Performance