HELICAL

THE 2020

Small and Mid Sized Business Cybersecurity Outlook

The SMB Guide to Cybersecurity – Risks and Solutions

The 2020 Small and Mid Sized Business Cybersecurity Outlook

Small to Mid Sized businesses need quality information to assist them in making important security decisions. With this in mind, Helical hopes that you will use this summary to assist you in understanding the threat landscape and how your business should be responding. Helical's solutions provide the proper protection for the SMB marketplace in a simple single-screen interface bringing together the security essentials required to protect an SMB's valuable digital assets.

The document is broken into the following categories:

1 Part	Understanding SMB Security Risks & Costs	01 – 04
2 Part	COVID-19 Cybersecurity Risks	05
3 Part	Protecting your SMB	06 – 08
4 Part	Overcoming Resource Limitations	09 – 13

The Helical Team is ready to assist in providing a simple, easy to manage, level of protection to assist you if you want to **manage your own security**, or provide a simple level of **overwatch** to ensure your Managed Services Provider (MSP) is meeting your expectations. Please reach out to us at Sales@helical-inc.com to schedule a 30 minute briefing on our solutions.

HELICAL

Understanding SMB Security Risks & Costs

Introduction – The SMB Appeal to Attackers

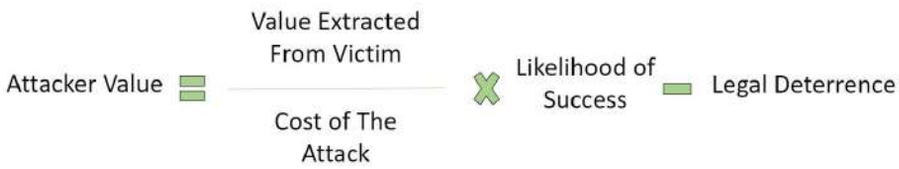
Small and Medium Sized Business (SMB's) are the lifeblood of the American economy. Making up **44%** of all economic activity[1], SMB's draw the attention of cyber criminals.

In 2019, firms with less than 250 employees **reported** the greatest annual increase in cyber-attacks[2].

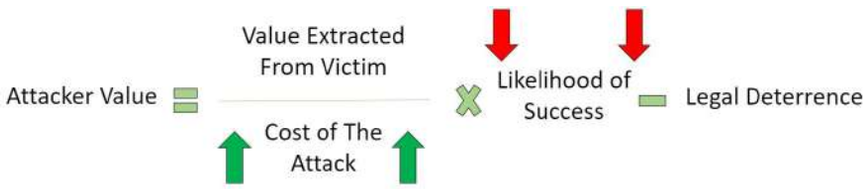
Like legitimate businesss, cyber criminals are cost conscious and their ROI is important!

Large firms with big security budgets will cost more $$ to breach than a resource constrained SMB.

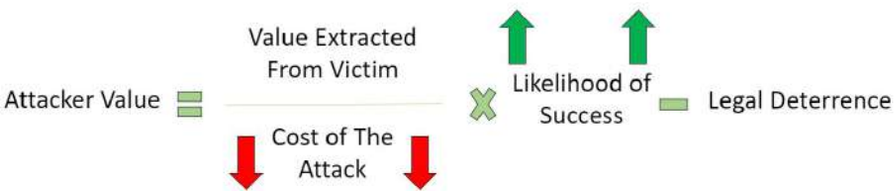
Criminal ROI



Large Firm Criminal ROI



SMB Criminal ROI



Understanding SMB Security Risks & Costs

The first step towards protecting an SMB is understanding the nature of threats they face. Attackers maximizing ROI will resort to the methods with a proven record of success, and SMB's must be ready to defend against them.
The 2020 Verizon Data Breach Investigations Report (DBIR) identified the most breach causes among Small to Mid-Size Businesses to be[3]

- **Phishing**
- **Use of Stolen Credentials**
- **Password Dumpers**
- **Misconfiguration**
- **Ransomware**

These top threats represent the main weaknesses of organizational security that does not properly layer protections. Problems start small, then become big...fast!

Exploiting Legitimate Access Points – The Easiest Way to Breakthrough

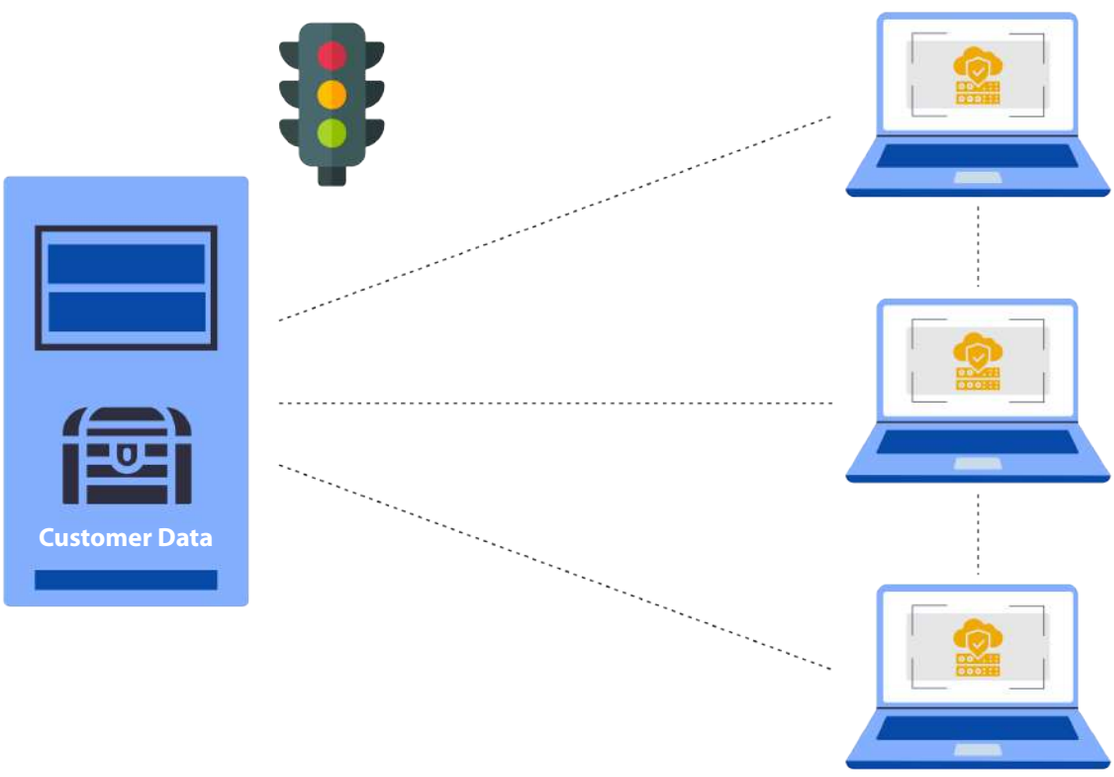
Phishing, stolen credentials, and password dumpers are consistently the top threats faced by any organization. Attackers favor them because they do not require a complicated approach. It is much easier to send out a phishing campaign and wait for a bite than it is to break the encryption on a password safe. Attackers will also be less likely to set off alarm bells by using legitimate access points. They simply slip through an open door while no one is looking.

Understanding SMB Security Risks & Costs

Exploiting Network Vulnerabilities – Turning Small Faults into Colossal Damage

Misconfiguration and Ransomware are threats that are seeing a rise in prominence from year to year.

SMB Attackers favor these methods because they rely on a failure to detect and mitigate before theyspread. Resource constrained SMB's are less likely to have the proper protections in place, resulting in larger paydays.



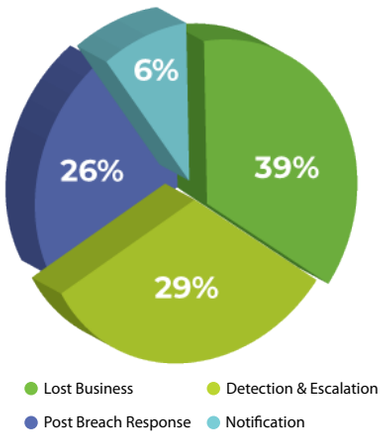
Understanding the relationships between your endpoints is essential towards understanding the routes attackers are likely to take and putting up the roadblocks to stop them.

Understanding SMB Security Risks & Costs

Breach Costs

A recent report by IBM and The Ponemon Institute revealed that, on the average, a successful breach will cost a minimum of **$146** per lost record for large firms and that per record costs sharply scale up for SMB's[4].

IBM categorizes the average breach cost as the following:



The Single Biggest Cost: Lost Business.

85% of customers say they will NOT DO BUSINESS with a company if they have concerns about its security[5]!

IBM highlights how steps your business takes now WILL impact the cost to your business of a breach.

When a Breach Occurred
The Average Firm
Lost $3.86 million

Firms with these security measures in place realized reduced costs

- Security Training - 6.2%
- Extensive Encrypting - 6.1%
- Security Analytics - 6.1%
- Vulnerability Testing - 4.5%
- Security Management - 2%

Firms with these issues saw increased costs

- Complex Security Systems- 7.5%
- Lack of security skills - 6.7%
- Poor Internal Compliance - 6.6%
- Lost Devices - 5%
- Remote Workforces - 3.5%

COVID-19 Cybersecurity Risks

Cyber criminals thrive in chaos because chaos breeds mistakes.

83% of businesses are reporting a significant shift in workers to home environments...a disruption that is creating a new threat landscape[6].

Personal Security Impacting Company Security More Than Before

60% of employees do company work on personal devices, increasing business security risk[7].

41% of security staff report that they are struggling to keep up with all the new devices connected to their company's network[8].

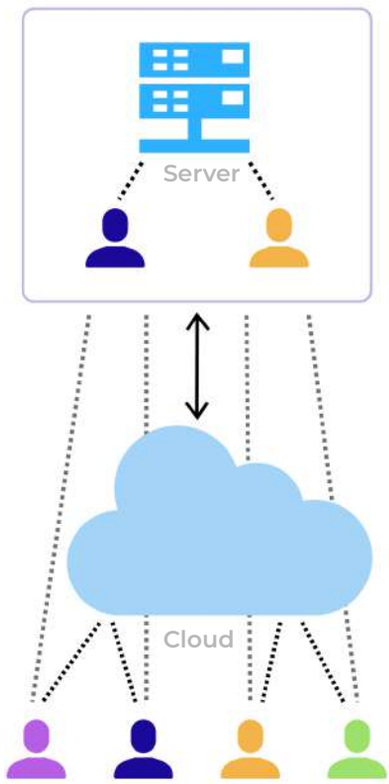
Internal Operation Disruptions

Transitioning to a work from home environment has caused centrally managed processes to become decentralized. This has, in turn, led to communication and performances issues.

37% of security staff report that collaborating and communicating with IT teams suffers in a work from home environment.

38% of security staff report it being harder to get visibility of remote assets and systems with the increase in working from home... making it easier for vulnerabilities to be exploited by attackers.

SMB's that don't have an ongoing scanning program will miss gaps in their patch programs in addition to other exploitable vulnerabilities.



Protecting Your SMB

COVID-19 induced disruption will continue to increase NOT reduce cyber threats.

Endpoints, Endpoints, Endpoints!

Everyday cyber threats to SMB's did not disappear with COVID-19 ....they accelerated.

If endpoint security was not already a top priority, a remote workforce makes it essential.

How to protect your endpoints:

- Know the devices on your network – Get a clear picture of the endpoints you are responsible for.
- Recognize that personal device security risks are company risks - Of organizations that allow workers to connect to their network on personal devices, **30%** of companies do nothing to protect against malware at all on those devices. Have a layer of protection on as many devices as possible[9].
- Use the cloud, but monitor cloud security – The cloud is built to ease scaling, but does not resolve all security issues. Those who believe it does may actually increase their security risk.
- Stay informed of threats – Threats are constantly evolving, and security decision makers must remain on top of them.
- Automate security – Automated alerting will free up staff to manage security.
- Encrypt Everything – Ensure encryption on all devices, as well as encryption at-rest and in-transit.

Protecting Your SMB

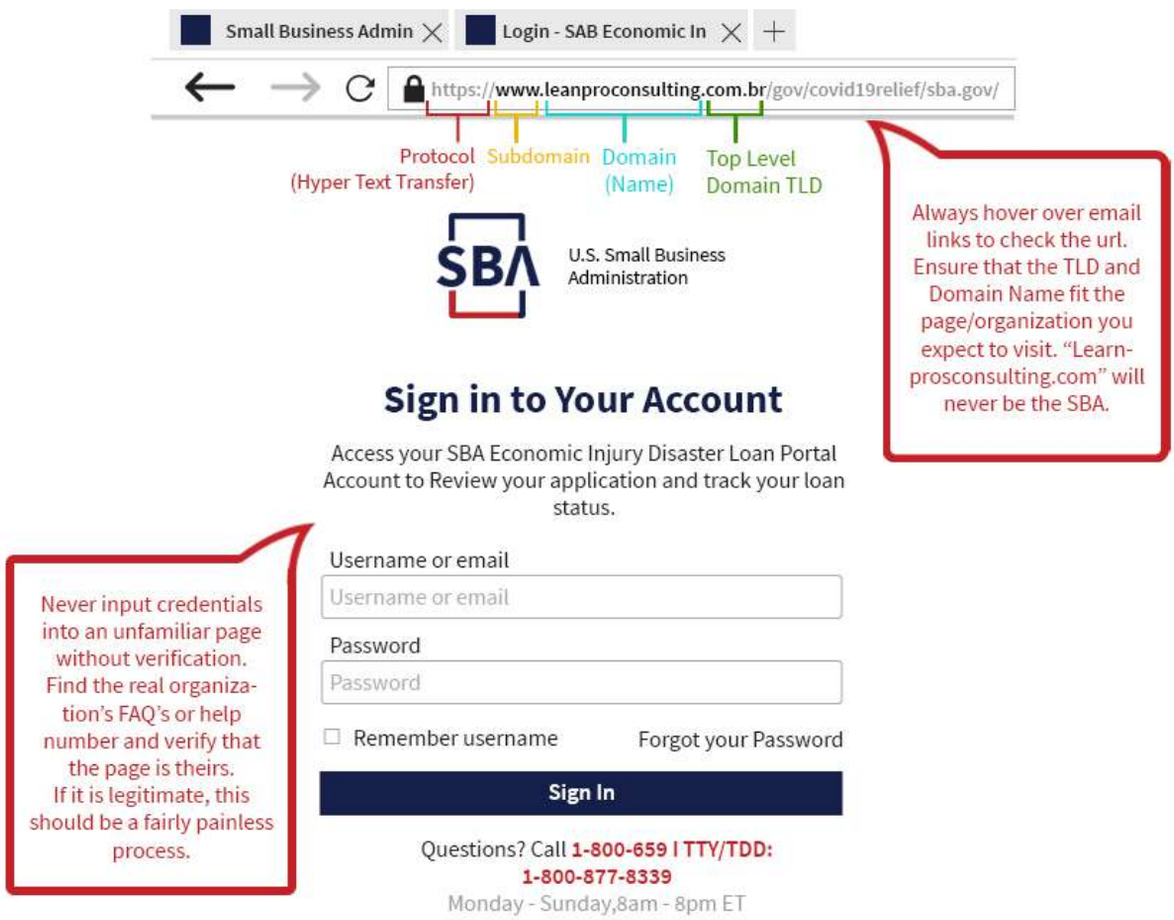
Security tools and talent cannot be maximized, unless security awareness exists throughout an organization. Take the proper steps to building this awareness.

Communication is key - Before adopting a policy, be prepared to justify it to the people you expect to follow.

Skills Training – A great way to take a burden off the security team is to ensure that all staff have minimum security skills.

Phishing – COVID-related phishing is on the rise. Give employees tips on how to spot it and what to do when they suspect it.

One **CISA alert** warned that SMB's were being targeted by attackers posing as the SBA seeking loan applications[10].



Protecting Your SMB

Manage BYOD Risks

Vulnerability Scanning and Patch Compliance

Most organizations endeavor to manage patching but often fail to ensure compliance. Maintain an ongoing vulnerability scanning program to ensure patches are up to date.

Configuration Status

Proper device management requires an active profile of endpoints that are/are not compliant with configuration standards. If organizations lose sight of this, they will be open to exploitation from threats they believed were remediated.

Network Discovery

With an expanded number of connections, organizations cannot afford to lose sight of what devices are connecting and disconnecting from their network. Are all these devices approved?

Overcoming Resource Limitations

What stops SMB's from being proactive?

Simple, resources. Many SMB's believe they cannot afford to spend on security and that view can put their entire business at risk. In other cases, the issue is a lack of in-house expertise. For most, the issue is a combination of both.

How can they overcome these limitations?

- **Build Smarter not Larger**

The optimal SMB solution is one that layers strength in each of the three pillars of cybersecurity : People, Process, and Technology.

SMB's will never have access to the same tools as large enterprises but layering their protection will drive up attack costs and dissuade criminals.

- **Strategize**

Before determining the cybersecurity budget, or deciding what tools to buy, SMB's should take a step back and assess their situation. Answer a series of questions internally before seeking external support.

Generic Security Questions

1. What are our current security strengths & weaknesses?
2. What are our regulatory requirements?
3. What level of risk are we comfortable with?
4. What are our most sensitive data assets?
5. How highly do we prioritize security?
6. What is our Security culture like?

Overcoming Resource Limitations

Remote Workforce Specific Questions


How many employees work from home?


Do we lose visibility with remote workers?


How many employees use personal devices?


Do we currently take any steps to secure business emails?


Do we currently take any steps to secure remote workers?


Are we accurately tracking access to sensitive information?

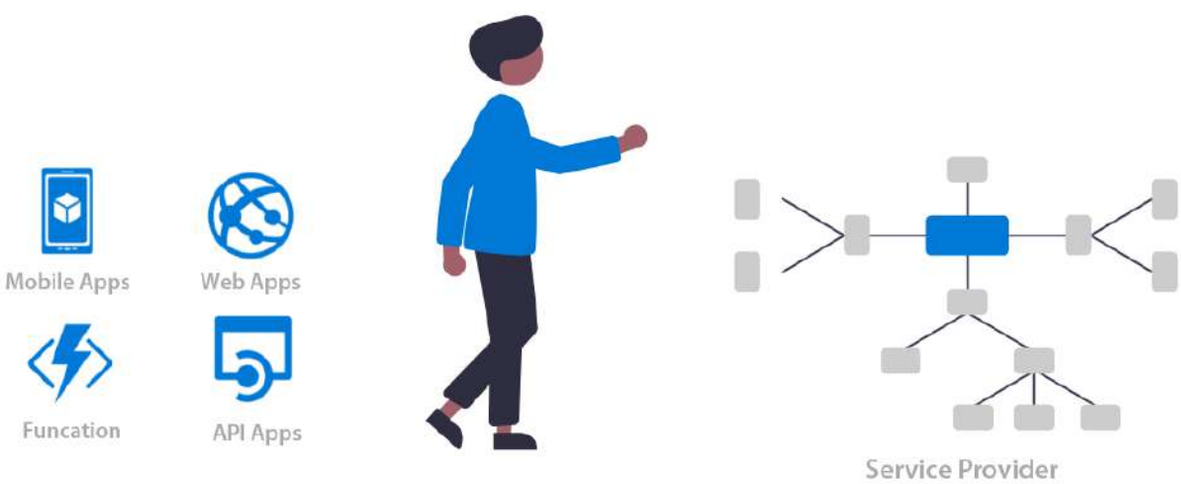
- **Keep it simple**

One of the best things an SMB can do to maximize protection is simplify their strategy. Adding layers without a plan or the ability to monitor all layers is just as effective as doing nothing at all. Ensure that your solution fits your management capabilities.

- **Products and focused consulting expertise**

As more strict privacy regulations like GDPR and CCPA come into play, and attackers innovate their strategies, organizations across the globe are increasingly turning to security services to help simplify and manage security. Leveraging the expertise of a solution provider like Helical can help plug the gaps left by a patchwork solution.

Overcoming Resource Limitations



Helical understands the multi-layered process of securing an organization. That's why we made it our specialty.

• Helical Security Essentials

The **Helical's Security Essentials Solution or Platform (Essentials)** will navigate you through the building and implementation of a program that protects all three cybersecurity pillars.

Essentials' modules will account for the level of protection your organization requires in light of its business, risk priorities, and regulatory obligations.

People: Phishing and Training

Phishing vulnerability is a symptom of poor security culture. To combat this, we offer a comprehensive simulation and training module that will strengthen your culture.

Process: Risk Assessment

We build the foundation of your solution by assessing your goals and vulnerabilities to identify where you can improve. Our risk assessment module automates the collection of the information highlighted on pages 09 and 10.

Overcoming Resource Limitations

Technology: Vulnerability Scanning

We scan your systems and offer a multi-layered reporting tool that lets you manage remediation by identifying the most critical vulnerabilities and tracking work-in-progress solutions.

Technology: Endpoint Protection

When it comes to endpoint security, Helical integrates next generation protection bringing lightweight high-level performance to your organization.

Technology: Ransomware Protection

Helical provides its own unique ransomware protection configuration alerts and we are so confident in our solution that we offer a financial guarantee against attacks.

Essentials will help you put the right tools and policies in place.

The next SMB challenge is managing it all. That is where Helical's OverWatch Technology comes in.

We ensure that your devices and cloud environments are compliant with IT policies in the most important areas.

- Network Access
- User Authentication
- Secure Configuration
- Vulnerability Scanning
- Patch Management
- Endpoint Security
- Device Encryption
- Cloud Port Monitoring
- Asset Management

Overcoming Resource Limitations

Helical's OverWatch Solution or Platform (OverWatch) continuously monitors system components to present you with a clear picture of your network and empower decision making. You control the compliance rules, risk and remediation priorities, work in progress status and more from Helical's unified management interface.

SMB's cannot afford to wait for a breach to occur before taking command of their cybersecurity

Helical's holistic solution provides the expertise and tools you require to build a resilient program, and the compliance monitoring necessary to manage it.

Simple Dashboard for Your Security Essentials

Automated IT Security Policy Auditing

Every organization has IT security policies, whether they are written down or not. **OverWatch** empowers you to know whether the security you have deployed on your endpoints and throughout your cloud infrastructure is consistently deployed and in alignment with those IT security policies. This level of policy auditing is valuable if you are using it to audit your in-house activities, and equally of value if you have outsourced your endpoint security to a Managed Services Provider (MSP).

The Helical Team is ready to assist in providing a simple, easy to manage, level of protection to assist you if you want to manage your own security, or provide a simple level of **OverWatch** to ensure your MSP is meeting your expectations.
Please reach out to sales@helical-inc.com to schedule a 30-minute briefing on our solutions.