avast business

GUIDE

Embracing the New Normal

SMB Guide to a Secure Digital Transformation

Introduction

Digital transformation has exploded in popularity over the past few years and is now a buzzword for business leaders in nearly every industry. Improved user experience, agility, convenience, and lower overhead costs make it particularly attractive to small and mid-sized businesses. SMBs are embracing digital transformation in increasing numbers to improve their business and prevent a more massive transition as their organizations grow.

Digital transformation will always be a delicate balance of improved processes and increased risk. SMBs are at particular risk for data breaches and compromised information during their digital transformation if they fail to increase their security in tandem. Managed security services provide an opportunity to protect sensitive information with top-level solutions delivered from the cloud with total protection.

The first step in delivering complete security is to pinpoint the inherent weaknesses in traditional security methods to address their planned digital transformation. Once the potential issues have been identified, the next step is finding the best tools that will provide the optimal level of protection. The right amount of protection will largely mitigate vulnerability, while still working in the budget and processes of a smaller organization.

This whitepaper will discuss the current risks in digital transformation that make SMBs particularly vulnerable to attack, as well as the three essential steps of managed security services to mitigate them. The appropriate level of proactive security and monitoring will keep customers from overspending on security, or the steep cost of a data breach. In particular, this paper will cover:

- Why a digital transformation makes SMBs an attractive target to bad players
- Critical vulnerabilities of the various aspects of expanded technology
- How to protect your customer's data, as well as your devices and people

Contents

Why a Digital Transformation Makes Businesses Vulnerable

Each year, more and more businesses pour their resources and large portions of their budget into digital transformation. It often fails to make the impact that leaders hope to achieve, though; research shows that 70% of all digital transformations do not reach their intended goals.

While some articles like to point to organizational issues or employee mindsets as the reason for their failures, companies themselves report that it is security that presents many of their challenges. In one study of over 270 businesses, leaders pointed to security issues as their most significant barrier to a successful digital transformation. However, only 34% of these organizations stated that they considered cybersecurity issues during the development stage. Organizations that fail to take security into account during their digital transformation risk having the entire plan compromised before reaching the intended goals.

Cybercriminals tend to strike SMBs because they typically have lax security standards and less budget for protecting their data than enterprises. They can target a large number of them at once, leading to exploitable data that is often just as valuable as that of larger companies. While SMBs turn to digital transformation to be more cost-effective, it can turn out to be more costly if they fall victim to a data breach. IBM's "Cost of a Data Breach" report found that the average cost of a data breach was $8.19 million in the United States. They also discovered that SMBs end up paying more on average than enterprises: Organizations between 500-1000 employees paid $3,533 per employee for a data breach, as opposed to $204 per employee for enterprises with more than 25,000.[1]

SMBs that undergo digital transformation are particularly vulnerable to attack because their security may not always match their expansion in technology. Also, attacks continue to become more sophisticated, which SMBs might not be prepared to defend against. SMBs fall victim to ransomware, phishing, distributed denial-of-service, and social engineering attacks. The evolving attacks and subsequent financial consequences should cause any SMB alarm.

Risks Involved in the Digital Transformation

The term "digital transformation" has been maligned by experts and leaders because it is a vague and broad term, encompassing a wide range of technologies. In this whitepaper, we will touch on the most common technology adopted in the digital transformation for SMBs.

The common aspects of digital transformation for SMBs include:

IoT

Internet of Things provides significant advantages to SMBs. The ability of sensors to complete tasks, analyze, and communicate without human intervention offers companies ways to create value for their customers. However, many are not designed with security in mind and leave organizations open to potential data breaches.

IoT's ability to connect low-risk and high-risk devices can cause significant cybersecurity issues for businesses that have not adapted their security accordingly. What was now once a low-risk part of your system is now linked with your most sensitive data. Hackers only need to find one entry point to get access to everything.

According to the National Institute of Standards and Technology,[2] the three largest security issues for IoTs are:

- IoT devices interact with each other to make changes to physical systems in ways that traditional technology does not.
- IoT can't be accessed or controlled the same way as traditional technology.
- Availability, efficiency, and effectiveness of cybersecurity are different for IoT than traditional IT.

Because IoT doesn't operate the same as IT, it requires a different approach to cybersecurity. Unless SMBs adjust their security accordingly, they face a potential breach in their data.

BYOD

In an attempt to reduce overhead costs and improve employee satisfaction, BYOD (or Bring Your Own Device) is an increasing practice for SMBs. It allows employees to work from their personal devices, such as smartphones, tablets, or laptops.

Businesses that have not established an official BYOD policy may find that their employees are using personal devices anyways. With the proliferation of internet devices, a company would be hard-pressed to find employees that don't bring their cell phone into work. While phones that are only used for personal reasons don't pose a security threat, conducting work from their devices can compromise the security of your entire company.

BYOD leaves organizations particularly vulnerable to DDoS attacks. Data theft is another risk associated with BYOD. If an employee sends a file over an insecure network, such as at a coffee shop or airport, it is easy for bad players to compromise the information. Malware infiltration is also a problem. Employees can download a mobile game with malware attached to it and attack your information through their device.

Disgruntled former employees can also pose a problem for company security. They can use the information loaded on their device to wreak havoc and destruction for both your customers and company reputation.

Remote Work

Even before remote work became mandatory in some areas, it was exploding in popularity. In today's current environment, though, remote work is a necessity. Organizations that previously resisted remote work find themselves forced to develop methods that allow their employees to work from home.

Employees that are not aware of safe remote work practices can leave a company vulnerable to a data breach. Sharing devices with non-authorized people, accessing information through unsafe networks, such as public Wi-Fi, and carelessness in opening emails can also compromise sensitive information and leave your organization at risk.

Cloud Applications

Cloud apps provide SMBs with more access to their data.It allows them to make data-driven decisions and gain critical insights to grow their business. Organizations can be vulnerable to attacks, though, when they fail to take proper precautions.

Cloud apps leave companies at risk for account hijacking, where attackers can access sensitive information using stolen credentials. Advanced, persistent threat groups target cloud environments and use public cloud services to operate their attacks. Insecure APIs can also create an entry point for attackers to exploit.

Data loss can also provide a significant issue for SMBs. An accident or catastrophe can mean that customer information is permanently lost without the right backups in place. Google and Amazon are both examples of how even the most technically-advanced companies can lose data by failing to back it up.

How to Protect Your Business For a Digital Transformation

A managed security service that understands the complexities of both a digital transformation and SMBs should be able to pinpoint potential vulnerabilities, provide the security level needed to account for any changes to technology, and continue to provide monitoring for your organization.

Identify Vulnerabilities in Your Digital Transformation Plan

Cybersecurity begins as soon as the plan for a digital transformation starts to form. It needs to be a part of the initial plan considered each step of the way. SMBs are a particular target because their security does not always evenly match their growth, leaving gaps and vulnerability. Digital transformation and security must be coordinated in tandem to avoid this potentially catastrophic mistake.

IBM conducted a study of the most successful transformations, and found that those who had a greater appreciation and emphasis on the importance of security ended up with a more successful outcome.[3] These "high performers," as the research paper referred to them, were less likely to suffer a data breach during their process.

Identify what digital transformations your organization hopes to accomplish. Note where you would like to expand into IoT, BYOD, remote work, or more cloud apps. Be sure to include the details of your plans to see where the potential vulnerabilities might be.

Also, make a list of the physical and virtual computing devices in the company. Workstations, laptops, printers, mobile devices, network application servers, corporate firewalls, and network file servers should be included in the assessment.

Determine the Level of Security Needed

Once you understand what you want to accomplish and the potential vulnerabilities, you can determine what level of security is needed. Below are the vital security services for a successful digital transformation.

Continuous Monitoring

A serious mistake made by many SMBs is to overspend on prevention to the detriment of detection and response capabilities. While prevention is a vital aspect of protecting sensitive information, attacks change and can strike at any moment. The faster a company can respond to an attack, the easier it will be to contain and reduce the amount of damage that can be done.

Maintain a solid foundation of security with ongoing remote monitoring and management. Finding and maintaining new software patches and updates, as well as updating security measures based on new threats, will ensure continuous protection against cyber criminals.

IOT	BYOD	REMOTE WORK	CLOUD APPS
ANTIVIRUS Installing and monitoring antivirus on all devices to secure every point of entry.	**EMAIL ENCRYPTION** End-to-end encryption directly on user devices ensures information only ends up in the right hands.	**SECURE EMPLOYEES ANYTIME, ANYWHERE** Provide a VPN connection to remote workers to secure access to company data and applications.	**BACKUP AND DISASTER RECOVERY** Prevents you from losing sensitive and valuable data in case of accident or emergency.
REGULAR VULNERABILITY SCANS Regular scans ensure that antivirus, passwords, and any other software is up to date.	**SSL DECRYPTION** Secure Internet Gateway inspects all ports and protocols to ensure threats can't make it to your network, and fills gaps in security left by traditional appliances.	**SECURITY AWARENESS AND TRAINING** Educate employees on practices that protect themselves and your company, such as recognizing scams and creating strong passwords.	**SECURE WEB GATEWAY** Acting as a virtual security guard, any detection from the cloud immediately blocks all threats for all customers within the network.
DATA LOSS PREVENTION Prevents users from sharing sensitive data and regulates what data can be transferred.	**SECURE AUTHENTICATION** There are several ways to achieve this, but password policies and multi-factor authentication (MFA) are some first steps.	**ENFORCEABLE PROCESSES AND POLICIES** Make sure everyone knows how to keep the company safe. Establish clear direction regarding what data needs protecting and how.	**PATCH MANAGEMENT** Installing patches and keeping them up-to-date can help resolve the inherent vulnerabilities of cloud apps.

Summary

Digital transformations are an inevitable change for SMBs. However, it leaves organizations vulnerable to newer and more sophisticated threats. IoT, BYOD, remote work, and cloud applications all have unique challenges that businesses must be aware of. Managed security services can help SMBs identify potential compromises and reduce vulnerabilities while improving their processes for a stronger business. These services can help you embrace change and technology, knowing that you have protection for both you and your customers.

1 Ponemon Institute. 2019 Cost of a Data Breach Report July 2019.

2 National Institute of Standards and Technology (NIST). Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. June 2019.

3 Ponemon Institute. Bridging the Digital Transformation Divide: Leaders Must Balance Risk and Growth. March 2018.

About Avast Business

Avast Business provides integrated, enterprise-grade endpoint and network security solutions for SMBs and IT service providers Backed by the largest, most globally dispersed threat detection network, the Avast Business security portfolio makes it easy and affordable to secure, manage, and monitor complex networks. The result is superior protection that businesses can count on. For more information about our managed services and cybersecurity solutions, visit **www.avast.com/business**.

WP-ENN-08-20