WHITE PAPER

Your Business Cybersecurity Plan:

From Assessments to Implementation to Management

THRIVE℠

Introduction

The frequency of news reports about cyber hacks and data breaches demonstrates that the threats to your IT infrastructure are never-ending—and that IT security is a moving target.

IT security must be a priority for every business leader, no matter the size of their organization.

But when was the last time you took a step back to look at what you and your organization are doing to address IT security today? And how well are you prepared for the future?

This white paper will provide you with an overview of the major areas that must be assessed when reviewing your Cybersecurity Plan. While IT security is never "one size fits all," you'll see where you're most vulnerable—and what you can do.

Welcome to a Shifting Landscape

Years ago, the scope of IT security normally was limited to a company's physical office locations — because that's where all the IT infrastructure was located. Most companies today no longer fit this mold. That means when looking at your security plan you need to know where your data and end users reside.

Two major aspects have changed the IT landscape significantly over the last 10 to 15 years:

1. The number of remote workers has risen dramatically. According to globalworkplaceanalytics.com, "regular work-at-home, among the non-self-employed population, has grown by 115% since 2005, nearly 10x faster than the rest of the workforce."
2. Everyone is using the Cloud. A recent survey by RightScale revealed that the average organization uses five clouds. Examples of these include hyper-scaler cloud providers like Amazon AWS, Microsoft Azure, and Google GCP (Google Cloud Platform), as well as the SaaS (Software as a Service) providers like Box and Salesforce.

Why have these changes had such drastic impacts on how businesses are approaching their IT Security plan?

The days of walking down the hall to access the server room, where you can install one device to solve a security gap, are long over. With servers and applications living in multiple clouds, you can no longer rely on installing software on user's laptops via GPO (Group Policy Object), because they might never connect to your corporate environment.

A Security Plan for today's IT landscape must account for every location your data and users reside in.

Advanced Email Security, Security Awareness Training, and RMM

According to Mimecast, 91% of all cyber attacks start with a phishing email. This means that if you want to protect your company, you're going to need a best-of-breed email security provider to stop harmful malware before it even gets to your users' inboxes. Regardless of where your users are located, making sure all emails flow in and out of an email security provider should be a top priority when making your Security Plan.

Security Awareness Training is just as important. You may be asking why you need to conduct training if you're paying for an email security provider that's supposed to be stopping malware in its tracks. The harsh reality is that in today's fast-moving world, the "bad guys" are constantly working on ways to get around all the security measures being deployed. So, it pays to be extra cautious. Training your users to know when an email looks malicious and to ignore it—without clicking on the link—is how you add that extra, security blanket layer of protection to your email security framework.

As employees are increasingly working from home, you'll also need to make sure that their systems are always up-to-date. Otherwise they risk becoming a major vector for hackers attempting to exploit your IT infrastructure. **RMM (Remote Management and Monitoring)** gives you the ability to patch, deploy new software, and keep an inventory of what's been installed on all of your endpoints regardless of their location.

Next Generation Firewalls

The firewalls in your environment are your first line of defense against malware attacks. In a way, it's similar to the way airport security works.

Years ago, when you arrived at the airport to check in for an international flight you'd have to show your passport and ticket to get through security. This is analogous to a basic stateful packet inspection firewall.

Today, when you show your ticket or open a mobile app for your airline, you are issued a bar code to be scanned at security. When that ticket is scanned by the security personnel, there are multiple checks happening in the background—i.e. seeing that your information matches your passport—to ensure your approval to proceed through security and to your terminal.

So, what's the connection?

Those multiple checks going on as you go through airport security are analogous to the advanced NGFW (Next Generation Firewall) features of many 5th generation firewalls, like Fortinet. In both cases the ideal outcome is that only approved travelers—or data—may proceed on their journey.

Web Application Firewalls (WAF)

If you are unfamiliar with what a WAF is, think of it as a firewall that is specifically built to protect your critical HTTP web applications. WAFs can protect your applications from sophisticated threats like:

- **SQL injection**
- **Cross-site scripting**
- **Buffer overflows**
- **Cookie poisoning**

Next Generation Firewall Capabilities Can Include:

- Advanced Threat Protection
- Application Control
- Device Identity & Authentication
- User Entity Behavior Analysis (UEBA)
- IP Reputation
- SSL Inspection. NSS Labs predicts that 75% of all web traffic will be encrypted by 2019. This should matter to you because the SSL encryption makes it more difficult to know what's happening in your environment. Having a NGFW that lets you see encrypted traffic—the good, bad, and ugly—is something that you should have high on your security plan list.
- IPsec/SSL VPN
- Sandboxing

Denial of Service (DoS) and Distributed Denial of Service (DDoS)

If you are hosting any critical infrastructure you must have a **DoS mitigation plan** in place. The speed and bandwidth that these attacks are consuming are beyond what any single human can keep up with. A recent Memcached DDoS attack was recorded at 1.7Tbps—a staggering amount of bandwidth. If you take a step back and look at the bandwidth in your data center, in most cases you probably don't have more than 1Gbps.

So, if you were to get hit with a DDoS attack at 1.7Tbps, your applications would shut down until the DDoS attack was over. Using a DDoS mitigation service allows you to offload the DDoS traffic and call in experts to assist in shutting down the DDoS attempt on your digital environment.

Advanced Endpoint Protection

When people hear "antivirus," most think of veteran vendors like Symantec and McAfee. Let's talk about how these traditional antivirus softwares function when installed on an endpoint (laptop, desktop, server, or mobile device).

These solutions were all founded on a simple idea that involves installing software that scans endpoint files and compares them to the signatures of known bad files. If a file matches the signature of a known bad file, then it's quarantined to keep the endpoint safe. If you're unfamiliar with advanced endpoint protection, you're not alone. At its core, this type of protection is more sophisticated than traditional antivirus software.

The best protection softwares that incorporate an advanced endpoint protection approach will typically include the following functions:

- **Endpoint Detection and Response (EDR).** This defines a category of tools and solutions that focus on detecting, investigating, and mitigating suspicious activities and issues on hosts and endpoints. In some cases, these tools give you a clear path to determining what was affected in a security breach and where it spread.
- **Advanced Threat Protection**, by Microsoft. Windows Defender Advanced Threat Protection is powered by a combination of Windows behavioral sensors, cloud-based security analytics, and threat intelligence, as well as by tapping into Microsoft's intelligent security graph.
- **Vulnerability Scanning**
- **Application Usage Reporting**

Security Information and Events Management (SIEM)

A Security Information and Events Management (SIEM) system aggregates logs from many (or all) of the critical devices and services (Cloud, SaaS, etc.) within your environment. Many of the SIEM products on the market today go a step further and aggregate events that are related into a single event. Some of the more powerful SIEM products also incorporate Performance and Availability Monitoring (PAM) into the aggregation of logs.

Security Operation Center (SOC)

Your Security Operation Center (SOC) should be staffed 24/7/365 with trained security professionals who are equipped to interpret and respond to the alerts that are generated from a SIEM or other security-specific tools. These individuals can assist with remediation steps when a security incident is detected. While it is possible to employ individuals within a company to fulfill these roles, it is increasingly more cost effective to outsource this function to a third party.

SOC In Action

A simple example of a company that ties these concepts together is one that has a firewall, switch, and a few servers, of which one is a Microsoft SQL (database) server, all sending their respective logs to a SIEM, which is being monitored by a SOC.

Imagine a case where an attacker from a foreign country has gained access to the SQL server and just performed a query which dumped a table containing all the Social Security Numbers of your customers. In performing this query, the SQL server CPU spiked to a high level that is not normal for that time of day. The SIEM could potentially throw up multiple alerts in this case. When the SOC personnel responded to the alert,

- They would see all the logs related to this incident in a single place
- They would see logs from the firewall proving that the SQL server has an open connection to a foreign country
- They would see that the SQL server service was the reason the CPU spiked
- They would also see a query was run that dumped all the SSNs

Having all this information in one place now allows the SOC to contact the appropriate personnel and discuss intervention and mitigation possibilities with a full explanation of what happened. An SIEM can be a highly cost-effective component of your Security Plan; the SOC component can be added at later date.

Conclusion

Every day a new Internet threat or virus emerges to become an imposing menace to your business. Developing, managing and optimizing the internal systems, tools and personnel to properly mitigate these risks alone is an overwhelming task for most companies.

Thrive's Managed Security Platform has been developed from decades of experience troubleshooting, halting, and remediating online security vulnerabilities. Our engineering team works 24/7/365 with the most advanced partners, software, and systems available to support or augment your organization's network security demands.

This process doesn't have to be overwhelming—Thrive can be there every step of the way.

Thrivenextgen.com

Contact the Thrive Team

To Learn More, Contact Us Today, or Give Us a Call At:

thrivenextgen.com | info@thrivenetworks.com

1-866-205-2810

About Thrive

Thrive is a leading provider of NextGen managed services designed to drive business outcomes through application enablement and optimization. The company's Thrive5 Methodology utilizes a unique combination of its Application Performance Platform and strategic services to ensure each business application takes advantage of technology that enables peak performance, scale, and the highest level of security.