Easy ways to DOMINATE the Security-as-a-Service Game

RapidFireTools®
A Kaseya COMPANY

Cybercrime

is expected to cost companies

$6 TRILLION

worldwide by 2021.*

This presents managed service providers (MSPs) with a **huge** opportunity to build monthly recurring revenue by delivering comprehensive security solutions designed to thwart these attacks.

Among those at risk of being targeted by cybercriminals, small and medium businesses (SMBs) are particularly vulnerable. In fact, **43% of all data breaches target SMBs.**

*2019 Official Annual Cybercrime Report conducted by Cybersecurity Ventures

**Verizon 2019 Data Breach Investigations Report

Identifying the *BIGGEST* Security Threat

Most MSPs deliver antivirus and anti-malware as part of a standard security offering. Doing so is generally acknowledged to be a best practice among industry professionals. However, these solutions fail to take into account one big variable:
your customer's employees.

Did you know ***70% of companies*** are more worried about an ***inadvertent insider breach*** than one caused by malicious intent?*

*2019 Insider Threat Report conducted by Cybersecurity Insider

Take Action

Consider making internal network security part of your comprehensive Security-as-a-Service offering. Adding this service is affordable and easy when you use a tool like **RapidFire Tool's Cyber Hawk.™**

Up Next:
Discover the state of SMB security

Known Issues

The state of SMB security is poor, with only 12% of SMBs rating their ability to monitor, detect, and respond to insider threats as extremely effective.*

Even more astonishing is the fact that **63% of SMBs have experienced a data breach within the past 12 months,** and only 33% of SMBs surveyed by the Ponemon Institute reported having intrusion detection systems in place.**

These security gaps present an opportunity for MSPs to expand their Security-as-a-Service offerings and include more comprehensive support—especially against internal vulnerabilities.

*2019 Insider Threat Report conducted by Cybersecurity Insider

**2019 Global State of Cybersecurity in Small and Medium-Sized Businesses conducted by Ponemon Institute LLC

Misconceptions

While most SMBs understand the need for, and are willing to invest in, basic security solutions to minimize external security vulnerabilities, few feel the same way about investing in solutions to reduce internal security gaps.

Educating your customers about the risks surrounding internal vulnerabilities is an important first-step when trying to upgrade existing customers to a more comprehensive plan that includes additional internal threat-detection measures.

Take Action

Find resources you can brand as your own, and use them to educate your customers about the need to protect against internal vulnerabilities.

Up Next:
Steering the Security Conversation with SMBs

Capture Their *ATTENTION*

Even compelling sales pitches fall flat if listeners fail to pay attention. The first step in starting a productive conversation around a more comprehensive security solution involves capturing your SMB customer's attention.

Keep in mind that the calls-to-action (CTAs) you use may vary depending on the vertical, industry, or job title being targeted. Make sure your CTAs clearly address the biggest business-related security fears your target audience is likely to face.

Take Action

3 Attention-Grabbing SMB Security Statistics:

1. The average cost of a security compromise over a 12-month period is $1.24 million.*
2. While 80% of SMBs rate IT security as a top priority, almost 30% invest less than $1,000 a year.**
3. 69% of SMBs report cyber threats are becoming more targeted.***

Bonus Tip:

Timely messages that acknowledge recent security incidents can also help you grab your audience's attention. For a list of the most recent data breaches, click here.

Up Next:
Create Interest

*2019 Global State of Cybersecurity in Small and Medium-Sized Businesses conducted by Ponemon Institute LLC
**2019 SMB IT Security Report conducted by Untangle, Inc.
***2019 Global State of Cybersecurity in Small and Medium-Sized Businesses conducted by Ponemon Institute LLC

Create *INTEREST*

Once you have the attention of your audience, it's time to go from gaining their attention—which might only span a few seconds—to building long-term interest.

To achieve this, you could introduce a core issue. In the case of a data breach, the core issue could be something as simple as a user plugging a compromised USB drive into your customer's network.

Take Action

What makes detection and prevention of insider attacks increasingly difficult?

1. Insiders already have privileged access to sensitive data.*

2. More end-user devices capable of theft.*

3. Difficulty in detecting rogue devices introduced into the network.*

Bonus Tip:

Cyber Hawk keeps you posted of any potential internal security issues going on inside your client's network. The daily alerts aggregate the issues that were detected during the past 24 hours and can be sorted either by priority/severity or by the type of issue.

Up Next:

Drive Action

*2019 Insider Threat Report conducted by Cybersecurity Insider

Drive ACTION

Now that the underlying problem has been identified, it's time to **drive action by introducing the solution to the painful problem you've just presented.**

In the case of SMB security, the problem is that most companies are not taking measures to protect against internal vulnerabilities, and the solution for these companies is to subscribe to your comprehensive Security-as-a-Service offering that minimizes internal vulnerabilities.

Essential Elements of a Comprehensive Security Offering

A comprehensive security solution—which detects internal and external vulnerabilities—should include these 11 elements:

1. **Evaluation of inbound firewall configuration**
2. **Review of outbound firewall configuration**
3. **Inspection of current patch-management tool effectiveness**
4. **Examination of antivirus and anti-spyware deployment**
5. **Permission review**
6. **Physical security walk-through**
7. **Internal vulnerability scan**
8. **Anomalous login detection**
9. **Security policy assessment**
10. **IT administrator review**
11. **Compliance-level auditing**

For a more comprehensive look at each of these elements, along with pricing suggestions, download our whitepaper: How to Sell and Deliver Internal Threat Detection with Cyber Hawk.

Next Steps

If you do not currently provide a solution that identifies and remediates internal data vulnerabilities, consider adding one to your Security-as-a-Service offering to capitalize on monthly recurring revenue.

Cyber Hawk is purpose-built to help MSPs create their own branded cybersecurity offering. To learn more about this revolutionary tool, click here.

RapidFire Tools a Kaseya company, creates innovative business-building technology tools for Managed Service Providers (MSPs). More than 8,000 technology service professionals worldwide use our products to close more business, offer more services, keep more customers, and make more money. Our offerings include Network Detective®, Compliance Manager™, and Cyber Hawk.™

Network Detective is the #1 non-intrusive IT assessment and reporting tool. With it, MSPs can quickly and easily capture a vast amount of network assets, users, configurations, and vulnerabilities without installing any software, probes, or agents. Our proprietary algorithm analyzes the data to generate dozens of professionally designed, completely brandable reports in minutes.

Cyber Hawk detects insider cybersecurity threats and generates daily alerts of suspicious network changes and anomalous end-user behaviors. Cyber Hawk empowers MSPs to create custom, brandable, and unique cybersecurity services at an affordable rate.

Compliance Manager is a unique compliance process automation tool with built-in modules to support the delivery of Compliance-as-a-Service solutions for HIPAA, GDPR, the NIST Cybersecurity Framework, as well as for most cyber liability insurance policies. MSPs use Compliance Manager to ensure that the IT policies and procedures required by industry or government regulations are being followed and, critically important, documented.

To learn more, visit www.rapidfiretools.com or call 678-323-1300.