



The Game Has Changed

Why Today's Security Strategy May Not Be Enough

Compliments of:



Introduction:

The world loves racing - whether it's NASCAR, IndyCar or Formula 1; the speed, the adrenaline, the crashes! Racing, however, is a very dangerous sport. Safety is a subject that is always on everyone's mind, but when a fatal accident occurs, the safety topic becomes center-stage. The tragic death of British driver Justin Wilson in an August 2015 race at Pocono, (the ninth IndyCar driver to perish since 1992) again brought focus to the safety measures being taken on the IndyCar circuit.

Compared to racing 25 years ago, **the game has changed** dramatically. Cars are faster, lighter, and the danger to drivers has increased. There have been marked improvements in safety to both tracks and cars, in an effort to keep drivers safe. Much like the airline industry, those safety improvements often result from tragedy. For instance, it was the tragic death of Dale Earnhardt Sr. in 2001 that prompted structural changes in cars and tougher standards for driver safety equipment, including the HANS device (a full-face helmet with head and neck support). These technology enhancements, though costly, are a requirement to keep more tragedies from happening.

Though the stakes aren't as high, cyber-security, much like car racing, has changed significantly over the past several years. Unfortunately the pattern continues: corporations often forgo the necessary safety mechanisms until a breach has occurred. In the Small-to-medium business (SMB) space, this could mean the end of the business.



Emerson Fittipaldi said he would have not survived this 1996 crash at Michigan had it not been for safety advances in the construction of open-wheel race cars.

The SMB has invested in what has been billed as an adequate security posture. There are five ways the cyber-security game has changed and why the current strategy, particularly in the SMB, may not be enough.

“ Though the stakes aren't as high, cyber-security, much like car racing, has changed significantly ”

1.

The Growth of Cyber-Crime

Cyber-crime has increased exponentially in three major areas: volume, complexity and vectors.

- Symantec saw over 317 million new malware variants released into the threat landscape.¹
- Intel saw over 1.1 million mobile malware samples in the first quarter of 2015.²
- Kaspersky Lab saw 4 million attempted MAC infections.³
- In 2014, 3.9 million web attacks were blocked daily.³
- Just shy of 2 million bots were reported.¹

The complexity of attacks on organizations has also increased. Traditional online attacks have become less effective, so cyber-criminals are finding ways to combine strike methods to get through corporate firewalls. As these attacks become more complex, they are much more difficult to detect. Cyber-criminals are highly skilled and well-funded, and instead of generically spraying their malicious code to indiscriminate victims, they're now specifically targeting corporations based on the type of data or financial accounts that can be hacked.

Targeted attacks and Advanced Persistent Threats have broadened the number of vectors used by cyber-criminals to gain access to proprietary data and company bank accounts. Social engineering, spear-phishing, water-holes and drive-by-downloads are only a few of these methods – all with one goal in mind: to deliver malware un-detected, within a company perimeter, “up-level” their access privileges and gain entry to company data or bank accounts.

This growth in attack volume, complexity and vectors has created a no-win scenario in many SMB organizations. Why? Because it's easy. Small and medium-sized businesses (and some public sector entities as well) tend to be well behind the security curve, making the organization an easy target of cybercrime⁴. It is too difficult for them to keep up with the amount of vulnerabilities that exist in the company's network and systems. It is no longer a matter of if a breach will occur, but when, as cybercrime has become a highly-lucrative business.



2014 Non Targeted
317M new

Targeted Attacks

- ENT: 5 in 6
- MED: 30%
- SMALL: 26%

KASPERSKY Lab

4M

attempted Mac
infections

123M unique
samples



1.1M

MOBILE

samples Q1 '15

2.

The Target of Cyber-Crime

Who has not seen stories in the weekly news about high-profile companies that have been breached due to Targeted and Advanced Persistent attacks? Target, Home Depot, Anthem Healthcare, OPM, Michael's – corporate and government entities alike have been showcased. What do they all have in common? Millions of lost records, millions of lost dollars, damage to company brand and loss of customers. Clearly the stories that make the nightly news are about large, high-profile targets.

The real target of cyber-crime, however, is not those companies that make the news because of their size. The real target is the SMB! The reality is that in 2014, 60% of all known successful attacks were against small and medium businesses. And of those that were breached, 60% go out of business within 6 months.⁵ The Targets and Home Depots of the world can weather an attack financially and survive. The SMB, who often lacks the financial resources required, cannot. A successful attack can cost hundreds of thousands, even millions of dollars, not to mention the damage done to the company brand. The prudent business manager should be asking whether their company could survive a successful breach.

“The real target of cyber-crime, however, is not those companies that make the news because of their size”



3.

The Number of Security Solutions

With the increase in attack vectors, security vendors are creating solutions that deal with these different approaches. One thing is clear, there are a plethora of vendors out there in the security world. IT security is a \$70+ billion dollar market⁶ – and every week a new vendor emerges and claims to have the hardware or software that is going to solve every security problem on the vulnerable network.

While most SMBs install the typical security measures – firewalls, IDS/IPS (Intrusion Detection/Prevention Systems), AV, etc., improper configuration and management of those tools often leaves them with more risk. By nature of their size, it's unlikely they have the resources or expertise to know what to do if those tools alert them of a problem.

Despite this situation, with so many vendors and so many solutions –the name of the game appears to be “sell more product” in response to the volume and complexity of threats. Therefore, more and more point products are introduced to an already complex environment. Though well-meaning, it could be argued that this approach has created a real problem in the typical SMB business.

“One thing is clear, there are a plethora of vendors out there in the security world”



4.

The Lack of Expertise

Too many security solutions tackling several different problems under one roof is the recipe for complexity. And - the more complex the environment, the harder it is to manage. ISACA (the Information Systems Audit and Control Association) in a 2015 study entitled “The State of Cybersecurity: Implications for 2015,” provides a view into this reality. This survey of over 600 cybersecurity and IT professionals revealed that 52 percent of those surveyed say less than 20% of applicants for cybersecurity jobs have the skills required for the open position.⁷ Is it possible the lack of readiness is because of a poor education, or the job at hand has become more complex? Either way, a lack of knowledge about the product and threat-scape leads to misconfigurations and ineffective use.

“
...the more complex
the environment,
the harder it is to
manage.”

Configuration is important, but so is the task of monitoring these devices. The most effective way to listen to these devices is to observe their every action and the patterns of communication between each other. Because these actions and “event logs” occur several times per second, many companies turn to a Security Information and Event Management tool (SIEM) to help make sense of the vast amount of machine data being generated. A SIEM product, out of the box, can be a highly *ineffective* tool at identifying and alerting to threats. For optimal results, SIEMs must be honed and fine-tuned with intelligent rulesets and knowledgebase updates. A robust knowledgebase that feeds the SIEM is a must-have in order to keep up with current threats and threat vectors. The SIEM must know how to weed through the millions of events that it gets per day, remove the false positives, and identify real malicious activity that threatens the company. In order to accomplish all of this, the SIEM must be monitored 24/7 by engineers who have security analysis experience to know and implement remediation steps before the damage occurs.

Often in the SMB, the IT Administrator doesn't possess this advanced expertise that is required to analyze and remediate events in their environment – with or without a SIEM. They simply cannot keep up with the ever-growing threat landscape, nor with the training needed to properly consume the security products they have in house. The result is increased risk that an attack will be successful.



5.

The Lack of Resources

Again, for a security product to be effective it must be constantly monitored and maintained so that threats are detected and responded to immediately. Not an easy task for the typical SMB company that cannot afford the 24x7 resources required to monitor the security infrastructure.

But the lack of resources extends to more than just money. The cyber security workforce is not increasing in size to meet the demand. Symantec's CEO, Michael Brown said, "The demand for cybersecurity workers is expected to rise to 6 million by 2019, with a projected shortfall of 1.5 million."⁸ Cisco, in their 2014 Annual Security Report, agreed that "the worldwide shortage of information security professionals is at 1 million openings, even as cyberattacks and data breaches increase each year."⁹ This has resulted in an increase in the average annual salary of a trained security professional, making it even more difficult for an SMB to attract and retain these resources.

And, according to the 2015 (ISC)2 Global Information Security Workforce Study, almost 20% of all security workers changed jobs last year¹⁰. This means that even if the SMB has the budget to hire 24x7 security professionals, retaining those employees will be a major challenge as the market becomes even more competitive.

“...the typical SMB company cannot afford the 24x7 resources required to monitor the security infrastructure.”

In 2014
Nearly one in 5 Security
Professionals Changed Jobs.



Source: 2015 (ISC)2 Global Information Security Workforce Study

The Game Has Changed

The volume, complexity and vectors have increased. The market is overloaded with security products that are ineffective because the expertise and resources to properly manage, maintain and monitor them is often lacking. And, as a result, the SMB is an easy target, consistently and increasingly targeted by well-funded and highly skilled cyber criminals. Is there an effective solution in sight? Is the “keep throwing money at the problem” mentality going to persist? Will the effects on the SMB be marginalized until the next big incident?

Because the security game has changed, so must the strategy and investment to effectively deal with the threat. Security products are critical to protect against vulnerabilities, but if those products are not being monitored 24/7 by trained security professionals that can analyze, triage and remediate security events, the investment in those products will be only partially realized.

An important note: “Investment” doesn’t always mean throwing out what’s in place and buying more and newer products. Technology abounds and, as said earlier, most companies have made adequate investments in their infrastructure with firewalls, high-quality anti-virus, IDS/IPS or perhaps even Anti-APT mechanisms. The sensible evolution in security is to optimize the existing infrastructure with 24/7 intelligent monitoring and remediation using enterprise-class technology and human expertise.

“
The sensible
evolution in security
is to optimize
the existing
infrastructure ...
”



What Options Does the SMB Have?

The SMB needs to re-evaluate the current methods of approaching the risks to their business. There are a few options that the IT manager can choose from:

Ignore: The ostrich approach is appealing because the investment in this model is completely free, but the risks of an attack are significantly higher.

Build: One solution that the SMB can invest in is to build a 24x7 Security Operations Center (SOC). Such a strategy requires capital investments that many SMBs just don't have.

- A robust and redundant infrastructure can run into the high six if not, seven figures.
- The SOC must then be staffed around-the-clock with highly trained, often hard to find security engineers.
- Expertise in detecting and remediating cyber-threats cannot be built overnight.

The truth is, creation of such a service delivery mechanism is typically beyond the capability of the SMB. Surely, there is another option.

“Expertise in detecting and remediating cyber-threats cannot be built overnight”

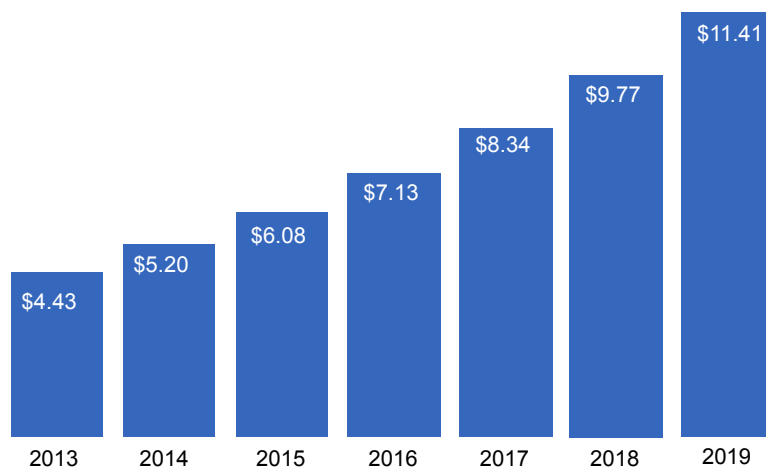
The Managed Security Services Option

Of course ignoring the situation or spending millions on a SOC are out of the question, the best option for the SMB is leave the security function to an expert in the field. This leads the SMB decision maker to the 3rd option:

Outsource: Because of the continued and escalating onslaught of cybercrime today, many companies, are turning towards outsourced Managed Security Services Providers (MSSP's) for help. This solution allows the SMB to immediately implement the intelligence and expert resources required without the capital outlay (and time) required to build it.

Due to the appealing nature of this option, the Managed Security Services market is expected to grow significantly over the next several years (see graph below). The SMB who chooses to outsource is not alone.

SECURITY OUTSOURCING MARKET (Billions)



Gartner Forecast: Information Security, Worldwide, 2013-2019, 2Q15 Update

How to Select a Managed Services Provider

Once the decision is made to outsource. The next step is the arduous task of choosing the right MSP. Here are a few DO's and DON'Ts that a prudent business should consider in their selection process:

- Stay away from automated alerting services. These services force the SMB to analyze and remediate threats themselves rather than solving problems. This leaves the SMB exactly where they started.
- Seek expertise. Effective 24/7 Managed Services Providers have employed (or have immediate access to) security engineers that can remediate security threats, not just inform the business there is a problem.
- Steer clear of vendors and providers who “dabble” in services, only to sell more product. If the Solution Provider's main offering is a product, or if the service offering depends exclusively on the SMB rebuilding their infrastructure, that is a red flag. The goal is to optimize the SMB's existing tools as much as possible.
- Choose a vendor that has a history of Security Intelligence. Of course, that is not something a Managed Services Provider who is in the process of growing their business can offer. In these cases, ensure the provider is partnered with a vendor that can readily provide this security expertise in the form of a service. The goal is to make sure the person watching the alerts knows what they are doing.

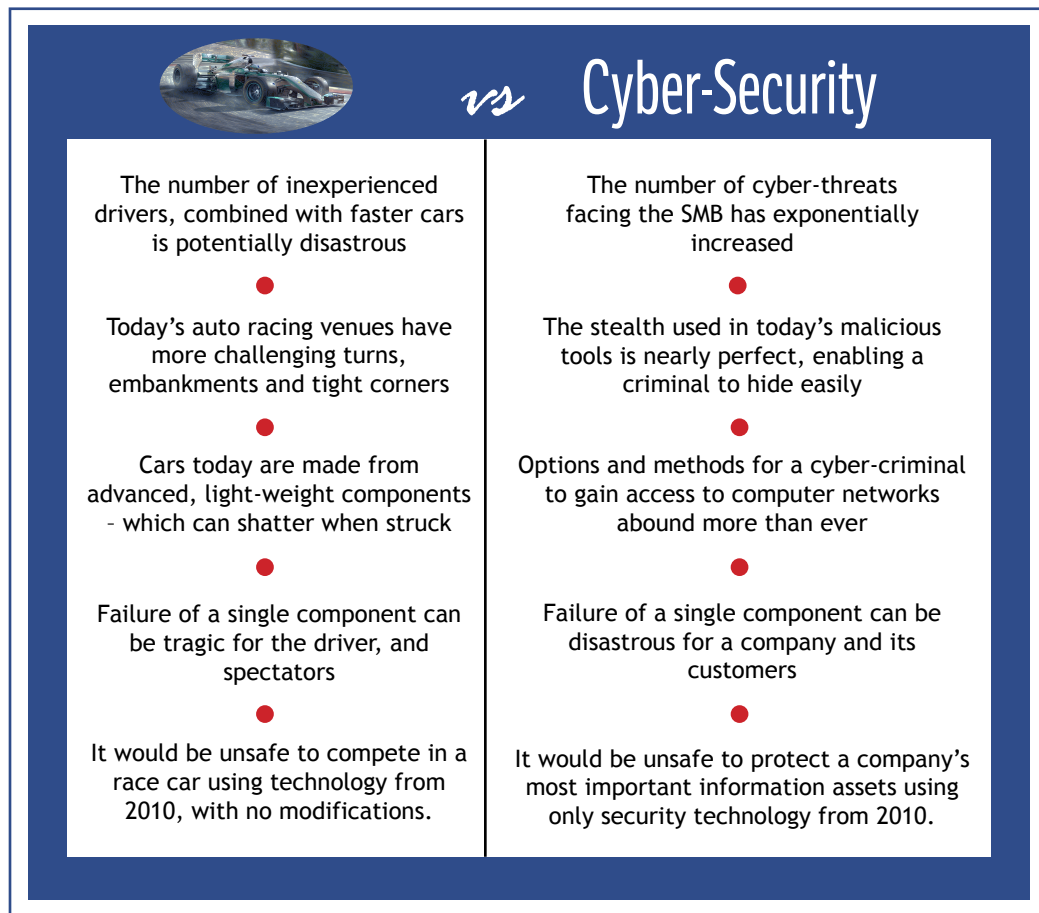
“Here are a few DO's and DON'Ts”

Summary:

While auto racing has considerably higher stakes than does SMB cyber-security, there are some parallels that can be observed in order to illustrate how a revised investment strategy is required.

A failure to realize that “the game has changed” could have tragic results.

“
A failure to realize
that “the game has
changed” could have
tragic results.”



From a racing perspective, the changing environment means additional measures must be added to the cars. Better safety is going to cost more money and there's no way around it.

Likewise, what a Managed Services Provider sold to an SMB for protection yesterday was all that was required. A changing threat landscape has demanded a new level of vigilance and increased investment to avoid risk.

Following some simple guidelines to ensure organizations are selecting the best Managed Service Provider can help them optimize their existing security infrastructure, and prevent risk to their environment.

Corporate Headquarters:

3625 NW 82 Avenue | Suite 407

Miami, FL 33166

(786) 375-9020

www.johnstek.com

1. Symantec Corporation, *2015 Internet Security Threat Report*, April 2015
2. Intel Security, *McAfee Labs Threats Report*, May 2015
3. Kaspersky Lab, *Kaspersky Security Bulletin 2014*, December 2014
4. Harris Interactive, "Fighting Fraud: Small Business Owner Attitudes about Fraud Prevention and Security", September 2013
5. 2013 National Small Business Association Survey, September 2013
6. Gartner, Inc. *Forecast Analysis: Information Security, Worldwide, Q2 2015 Update*, September 2015
7. ISACA and RSA, *Implications for 2015, An ISACA and RSA Conference Survey*, April 2015
8. Morgan, Steve. *Cybersecurity Business Report*, CSO Online. July 28, 2015
9. Frost & Sullivan / Booz Allen Hamilton. 2013 (ISC)2 Global Information Security Workforce Study, February, 2013
10. Frost & Sullivan / Booz Allen Hamilton. 2013 (ISC)2 Global Information Security Workforce Study, February, 2013