SMALL & MEDIUM BUSINESS THE NEW TARGET

Small and Medium Businesses (SMB) are great targets for cybercriminals. They have sufficiently valuable information to make it worth an attacker's time and the organizations protection level is weaker than that of a large organization. Yet, SMB's do not have the resources to buy the tools or hire the staff to protect their organizations. What can they do?

62% of Cyber Attacks are aimed at SMB -- Verizon Cyber Crime Survey

>50% of small-to-medium sized businesses had experienced at least one data breach -- Ponemon Institute

87% of SMB's have not written a formal security policy for employees

83% lack a security blueprint

59% have no plan in place to respond to a security incident -- NCSA and Symantec "National Small Business" survey

INFO@DEFENSATIVE.COM

SMB's - Behind in Their Understanding of the Problem

- ✓ *86% of businesses 250 employees or fewer said they are "satisfied" with the level of security they have in place to defend customer or employee data*
- ✓ *87% of respondents have not written a formal security policy for employees*
- ✓ *83% lack any security blueprint at all*
- ✓ *59% have no plan in place to respond to a security incident*

[National Cyber Security Alliance (NCSA) and Symantec "National Small Business" survey]

Companies that have to deal with compliance concerns such as Healthcare with HIPAA, Financial Services with FINRA or Retail with PCI-DSS have had to deal with security concerns for years. However, industries such as legal, manufacturing, real estate and others are woefully behind.

Fortune 1000 companies in all verticals have had the luxury of many vendors that offer security services calling on them and educating them of the issues their corporations are facing in regards to cyber security. However, those vendors' solutions cost hundreds of thousands of dollars to deploy and require a specialized skill set to operate that is very hard to hire in today's market.

Even companies that have dealt with compliance for years do not necessarily understand the true threat to their companies and they are getting fined continually. Many of these companies think that if they scan for issues once a year or quarter they are fine. They might pass as compliant but they are not secure… Here are just a few examples:

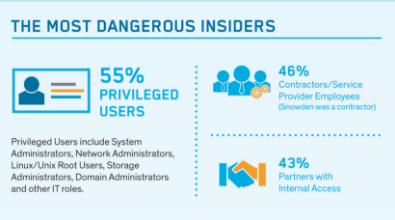
- ✓ HIPAA example
- ✓ PCI-DSS example
- ✓ FINRA example

Threat vector has shifted to the SMB

- ✓ *Target Hackers Broke in Via HVAC Company* [Krebs on Security]

- ✓ *"CVS, Rite-Aid, Sam's Club, Walmart Canada and other large retail chains have suspended their online photo services following a suspected hack attack against **a third-party service provider** that may, in some cases, have resulted in the compromise of payment card data."* [BankInfoSecurity]

Bad actors know that the SMB has much lower security protections than the larger firms and they are using this soft underbelly to infiltrate critical systems. They also know that these SMBs are easy ways into big companies. How? Just follow any companies supply chain—for example, take a large aircraft manufacturer building the next jet liner and you will find more than 2,000 suppliers in over 20 countries delivering the components, parts, systems and hardware that is required to assemble the aircraft. If you look at some of those suppliers you will find the same thing (they each have several suppliers and so on…). This corporate to corporate commerce is what keeps our global economy going and growing. The problem is that all of these supplier companies do not have the same emphasis on securing their networks as the large aircraft manufacturer—that creates a big hole and one that a bad actor can exploit. If the bad actor can compromise the big company (aircraft manufacturer) via one of the suppliers in their supply chain they will easily do it. **This is why your customers may ask to audit your security infrastructure/policies if you want to continue supplying them with products/services.**



[Vormetric]

The Insider Threat

Many SMB executive still believe that a firewall and Anti-virus software will protect them from a bad actor exploiting their company—what they don't understand is that the biggest issue is not a bad actor 'breaking in' it's their employees unintentionally letting the bad actor through the firewall without knowing they did…

SMB's - NOT Prepared

- ✓ *"92% of infosec professionals have totally lost confidence in antivirus"* Bromium

- ✓ *"Once, firewalls were useful for certain types of attacks. Now they're more trouble than they're worth -- and create a false sense of security into the bargain"* Infoworld

Top Attack Vectors

- ✓ *Employees clicking on links and attachments in email*
- ✓ *Employees downloading files on the internet*
- ✓ *Unmanaged BYOD*
- ✓ *Employees not keeping software up to date*
- ✓ *Employees sending PII over the internet in clear text*
- ✓ *Employees running risky software*
- ✓ *Employees visiting explicit websites*

What will a cyber breach cost?

- Money
  - *Attorney fees*
  - *Plaintiff demands*
  - *Forensics*
  - *PR response*
  - *Fines (FTC, SLG, PCI-DSS…)*
- Reputation
  - *Employees*
  - *Customers*
  - *Suppliers*
- Your customers
- **Your business...**

Firewall and Anti-Virus protection are still necessary but they are not enough in today's cyber threat landscape. The Fortune 1000 have Intrusion Detection Systems (IDS), Intrusion Protection Systems (IPS), Security information and event management Systems (SIEM), Threat Intelligence and End Point technologies… On top of all of that they have many security analysts using the data and tools to weed out the bad actors from their infrastructure. They also have corporate employee policy documents that contain cyber security provisions, cyber insurance, employee cyber training etc..

The SMB cannot afford this type of protection however they need to do more than a firewall and anti-virus or they will be the next victim.

Policies? Insurance? Training? Technology?

The first step in securing your environment should start with good corporate employee cyber security policies with controls, enforcement and consequences. These policies should include the use of social networking, personal email, mobile phones etc. on the corporate network as well as many additional items. (more)

The second step is training your employees, contractors and even vendors on both the policies as well as general security protections such as understanding how a Phishing attack occurs. Here are a few good slide decks for you to use to train end users and executives… The training goes into how a bad actor will exploit an end user that does not keep software up to date (such as Java, Flash and Windows security patches), an end user that uses insecure mobile applications on Android phones, a user running risky software such as TOR and Bit Torrent and a user that clicks on attachments, links and unsafe websites—all of these scenarios invite an exploit!

The third step is to ensure you have a cyber-liability insurance policy in place. These are not expensive and should be a part of every businesses insurance portfolio.

The fourth step--use a managed security services provider to offer low cost security services such as Defensative's **NetWatcher** service that can keep an eye on your network and look for anomalous behavior 24x7 365 days a year.

Your Customers Requiring Security Audits

Given the very publicized break-ins at Target Inc. and The US Office of Personnel Management (OPM) occurred due to subcontractors being compromised and infecting their customers --most large organizations are now requiring audits of their vendors policies, insurance and cyber security infrastructure support. If you don't pass you lose their business!

The Result

According to the National Cyber Security Alliance, one in five small businesses falls victim to cybercrime each year. And of those, some 60 percent go out of business within six months after an attack.

How Defensative Can Help

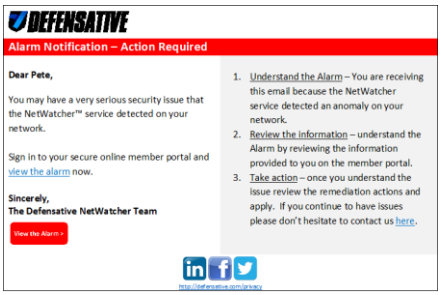
Defensative is a Managed Security Service Provider, focused on providing enterprise-level security management services, which only the Fortune 500 could afford in the past, to Small and Medium (SMB) organizations at a very low rate.

Defensative's **NetWatcher**™ Managed Security Service is similar to the services offered by physical security company's (ADT & Alarm.com) and Identity Management companies (Identity Guard) – **it warns you when someone is trying to break into your companies networks (and much more).**

Continuously Monitor for Exploits & Security Hygiene

In today's environment of widespread cyber-intrusions, advanced persistent threats, and insider threats, it is essential for SMB's to have real-time accurate knowledge of their enterprise network security posture so that responses to external and internal threats can be made swiftly.

Continuous monitoring is a risk management approach to cybersecurity that maintains an accurate picture of a SMB's security risk posture, provides visibility into assets, and leverages use of automated data feeds to quantify risk, ensure effectiveness of security controls, and enable you to remediate the issues quickly. A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status.


DEFENSATIVE

Alarm Notification – Action Required

Dear Pete,

You may have a very serious security issue that the NetWatcher™ service detected on your network.

Sign in to your secure online member portal and view the alarm now.

Sincerely,
The Defensative NetWatcher Team

View the Alarm >

1. Understand the Alarm – You are receiving this email because the NetWatcher service detected an anomaly on your network.
2. Review the information – understand the Alarm by reviewing the information provided to you on the member portal.
3. Take action – once you understand the issue review the remediation actions and apply. If you continue to have issues please don't hesitate to contact us here.

Steps to Protection

1. Install a sensor on the network
2. If you are exploited you will receive Alarms via email, SMS or via our customer portal – start your remediation process **
3. Log in to view your customer network security score – plug the holes in your network

Coming Soon

- ✓ Bandwidth monitoring and analytics
- ✓ SIEM and Log retention

Pricing

- ✓ $399/month (paid monthly) or **$299/month** (1 year paid up front)
- ✓ 30% discount on sensors 2+
- ✓ $37/helpdesk tickets (sold in 5 pack bundles)

***we offer Triumfant end-point remediation software as an add-on for up to 50 endpoints for an additional $229/month*