WHITEPAPER

Building Successful Cybersecurity Defenses for SMBs

As technology plays a larger role in the work and culture of small and midsize businesses, so does the threat of cyberattack. This paper will examine how companies can develop and implement a security strategy to mitigate risk and defend against the latest threats.

Presented By:

Manhattan TechSupport.com

Sales: 212-299-7673

sales@manhattantechsupport.com

TABLE OF CONTENTS

ManhattanTechSupport.com, 55 W 39th St,12th Floor, New York, NY 10018
Sales: 212-299-7673 sales@manhattantechsupport.com

THE NEW CYBERSECURITY TARGET: VULNERABLE SMBS

It is well-known that the threat of cyberattack is growing more serious for businesses. According to Ponemon Institute, one of the leading researchers in the cybersecurity field, 54% of businesses were victims of an attack that compromised their data or infrastructure in 2017[1], while less than one-quarter of those same businesses consider their ability to defend against cyber threats as highly effective or better.

The increased risk of attack has compelled larger businesses and institutions to make considerable investments in cyber defense. JP Morgan Chase now spends approximately $500 million per year on cyber security[2], while institutions like Bank of America have said they're willing to spend unlimited financial resources to protect their business against cyberattack. To clarify, that's a completely blank check for cybersecurity spending.

An unintended consequence of improved security at large organizations is that the threat to small- and medium-businesses (SMBs) has grown. Hackers and cybercriminals, eager for an easy target, are now taking aim at the relatively undefended SMB sector as a new and easy source of revenue. According to the Ponemon Institute's 2017 report, *the State of Cybersecurity in SMBs*, 60% of small business owners say that cybersecurity threats are becoming more targeted and more sophisticated[3].

THE CHALLENGES OF AN EVOLVING THREAT LANDSCAPE

Along with regulatory pressure from federal and state agencies, new and evolving cyber threats are another factor which makes SMB security an urgent matter. While ransomware and traditional denial of service (DoS) attacks still pose a significant problem, there are new and more insidious threats emerging daily. Countering these new threats often demands cybersecurity expertise beyond what's available at most SMBs.

1 Ponemon Institute, "2017 State of Endpoint Security Risk Report," https://www.barkly.com/ponemon-2018-endpoint-security-statistics-trends, (Nov, 2018).
2 Forbes Magazine "A Lack of Cybersecurity Funding and Expertise Threatens U.S. Infrastructure" https://www.forbes.com/sites/ellistalton/2018/04/23/the-u-s-governments-lack-of-cybersecurity-expertise-threatens-our-infrastructure/, (April 23rd, 2018).
3 Ponemon Institute, "2017 State of Cybersecurity in SMBs" https://keepersecurity.com/2017-State-Cybersecurity-Small-Medium-Businesses-SMB.html, (Sept, 2017).

Meanwhile, there's a national lack of competent cybersecurity specialists. Cybersecurity professionals, according to a variety of industry sources, are going to grow increasingly scarce as government agencies and large companies attract an outsize proportion of the top-tier talent. According to a report by Frost & Sullivan, there could be as many as 1.8 *million* unfilled jobs in the cybersecurity sector by 2020[4], which presents a serious issue, especially for smaller companies that don't have the money to lure experienced security analysts and engineers away from large organizations.

Here are some of the threats that are currently posing the greatest cybersecurity challenge to SMBs.

ADVANCED MALWARE THREATS

By now, everyone has heard of ransomware. Ransomware made global headlines in 2017 by striking computer networks of high-profile organizations like shipping giant Maersk, the National Health Service of the UK, municipal agencies across the United States, and many other high-profile targets. Since then, ransomware attacks have declined in frequency while increasing in sophistication. For SMBs, the threat of ransomware is still very real, and companies must continue to be vigilant.

But unfortunately, ransomware is just the beginning of the malware threat now facing SMBs. According to leading anti-virus provider Kaspersky Labs, there are over 360k new malware variants *every day*[5]. This enormous number of new variants makes reliably detecting malware with traditional anti-virus solutions a challenge. The rapid increase in malware is driven in part by the rise of "single-use" malware, programs designed to last just hours – or even minutes, before being replaced by newer, harder to detect variations.

Not only is there more malware, but it's getting smarter too. Polymorphic viruses, bots, trojans, and keyloggers are a new breed of malware that's able to change the identifiable parts of

4 CSO Magazine "Statement of Issue with the Cybersecurity Jobs Gap" https://www.csoonline.com/article/3258746/hiring-and-staffing/statement-of-issue-with-the-cybersecurity-jobs-gap.html (Feb 26th, 2018).
5 Kaspersky Labs "Numbers of the Year" https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-number-of-the-year (Dec, 2017).

their makeup to avoid detection by traditional anti-virus solutions. Because anti-virus software detects malware based on a known "signature" in its code, polymorphic malware only needs to make a slight change from an identifiable signature to make itself invisible. Defending against polymorphic malware and its cousin metamorphic malware requires that SMBs expand their security tools beyond traditional anti-virus.

the cost of a single insider attack reached $8.7 million dollars, an increase from just over $4 million dollars only two years ago

ManhattanTechSupport.com has you covered with advanced anti-malware detection that covers both traditional definition-based detection and a heuristic analysis. We can help you identify zero-day threats and the dynamic variants of the polymorphic and metamorphic malware.

THE INSIDER THREAT

Insider threats are a cybersecurity threat that originate from inside your business or organization. An insider threat can be a disgruntled employee or a staff member who becomes influenced or bribed. They may even come from a nonmalicious employee who unwittingly leaks their login, password, or data to a third party.

Different institutions will have their own unique vulnerability to insider threats. Banks must contend with disgruntled tellers who are willing to trade valuable credentials for personal gain. Companies that employ temporary workers or have a complex supply chain, such as manufacturers or distributers, must ensure their cybersecurity systems protect data from the many people that access their network in a single day. Organizations in the healthcare industry, where the risk of insider attack is higher than the risk of attack from external sources, must pay particular attention to these threats.

The general trend is that these insider threats are becoming more damaging. According to a 2018 study by the Ponemon Institute called, *2018 Cost of Insider Threats: Global Organizations*[6], the cost of a single insider attack reached $8.7 million dollars, an increase from just over $4 million dollars only two years ago.

ManhattanTechSupport.com's security services focus on a risk-based architecture and a layered approach that includes secure configurations, training, and data loss prevention. This,

6 Ponemon Institute "2018 Cost of Insider Threats: Global Organizations" https://securityintelligence.com/news/the-average-cost-of-an-insider-threat-hits-8-7-million/ (May 1st, 2018).

combined with our advanced risk analysis and security information and event management (SIEM) solutions, can detect indications of data theft or risky behavior before it's too late.

ADVANCED PERSISTENT THREAT

An advanced persistent threat (APT) is a type of cyberattack in which an intruder maintains a long-term, undetected presence in your network. When an attacker gains access to your systems, they'll opportunistically seek greater network access and evade detection while they surreptitiously encrypt and harvest your data. The goal of an APT attack is to exfiltrate high-value data, so they're often used against financial firms, hospitals, or other businesses which possess information the hackers can sell or hold for ransom.

Although these attacks were once the province of the most elite hacking groups working at the nation-state level, in the last several years mid-level criminals have started to adopt APT techniques. Take for example DarkHotel campaign[7], which uses unsecured hotel WiFi connections to hack into the laptops and mobile devices of traveling business executives. The attack has been successfully operating for over a decade, and over that time has infected the devices of thousands, perhaps tens of thousands of business people as they travel the world.

Because APT attacks happen over months or years, and don't leave behind obvious signs of intrusion, they're very difficult to detect. Locating an APT includes carefully examining network traffic, deep analysis of network log files, and inspecting suspicious data transmissions to look for possible data exfiltration.

ManhattanTechSupport.com's managed security offering provides options to mitigate and detect these slow, low profile attacks. The correlation of network, application, and device log data through a SIEM platform, combined with advanced detection that utilizes real-time global intelligence, can help stop insidious APTs in their tracks.

AN UNPREPARED WORKFORCE

One of the most pressing threats facing today's SMB is an uneducated workforce. According

7 SecureList "The DarkHotel APT" https://securelist.com/the-darkhotel-apt/66779/ (Nov, 2014).

ManhattanTechSupport.com, 55 W 39th St,12th Floor, New York, NY 10018
Sales: 212-299-7673 sales@manhattantechsupport.com

to Wombat Security's 2018 State of the Phish report, over 74% of businesses were the target of some form of phishing attack in 2017, an attack that manipulates authorized network users into sending confidential information outside the network. Phishing attacks can be used to steal passwords, bank account information, or other user data that's then used to launch a more lucrative second-stage attack.

The need for better workforce training has been publicly endorsed by several prominent cybersecurity leaders, including the nation's first Chief Information Security Officer (CISO) Gregg Touhill[8], who during an interview with the Information Security Media Group, called it "priority number 1" for improving cybersecurity at businesses.

To prevent human error from creating dangerous security vulnerabilities, it's important that employees are educated not only about the basics of digital hygiene, such as password maintenance and regularly updating applications, but also in more advanced topics. This should include what a phishing attack looks like and how to identify the tell-tale signs of fraudulent, potentially dangerous communication.

Annual training simply isn't enough. It provides too much information in one session for anyone to retain, while failing to supply the up-to-date instruction that employees need to stay ahead of threats. That's why ManhattanTechSupport.com's security services offer a training package that includes a monthly newsletter, and proactive notifications when we notice a significant increase in malicious activity.

DEFINING "RIGHT-SIZED" CYBERSECURITY FOR YOUR ORGANIZATION

The confidentiality, integrity, availability (CIA) model is one of the most widely-accepted frameworks for developing a good overall security policy. Defenders can use the CIA model to ensure the administrative, technological, and physical controls in their cybersecurity strategy are balanced to meet all the security needs of the organization.

8 BankInfoSecurity "Former US CISO on Why Awareness Training Is Priority Number 1" https://www.bankinfosecurity.com/interviews/former-us-ciso-on-awareness-training-priority-1-i-3815 (Dec 22nd, 2017).

Confidentiality – Securing access to information and company assets by granting permission on a need to know basis. This is done by restricting access rights to those a user or application needs to function, a concept known as "least privilege."

Integrity – Ensuring data is not tampered with during storage or transmission. This also includes protecting the accuracy and authenticity of data. Integrity is often achieved using file permission policies and user access controls.

Availability – Providing consistent access to data and services. This may include developing systems that are fault tolerant through redundancy, and a robust backup and disaster recovery plan to ensure that sensitive data is always available to authorized users.

The CIA model is a time-tested guideline for securing any network or system and a useful reference for performing cybersecurity assessments.

RISK ASSESSMENT

A first step in practical cybersecurity is to dispel the notion of a "perfect cybersecurity" strategy that provides absolute protection against all threats. That's not a realistic goal in any situation, especially for SMBs on a limited budget. Instead, the goal should be to mitigate the threat of cybersecurity to the largest degree possible while minimizing the harm an attack would do if it bypasses your security.

Today, most experts agree that a risk-based approach is the best way to build a sound cybersecurity strategy. A risk-based approach identifies and scores each potential risk, then prioritizes them along a scale so that the most damaging risks with the highest probability of occurring are addressed first, followed by the second most damaging and likely, and so on until all risks have been accounted for.

Risk-based strategies not only ensure that each risk receives the proper attention, but also that your security budget is spent in areas that will have the greatest impact.

ManhattanTechSupport.com, 55 W 39th St,12th Floor, New York, NY 10018
Sales: 212-299-7673 sales@manhattantechsupport.com

The process of performing a risk assessment has four stages.

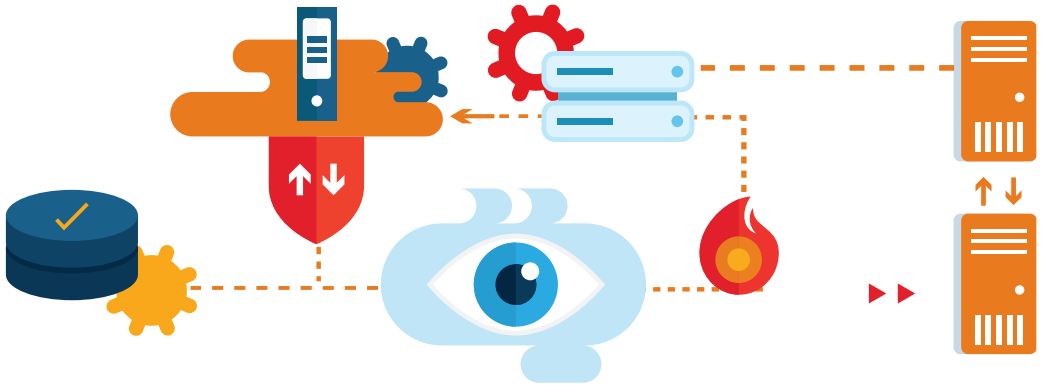
When formulating a risk-based security strategy, it's likely you'll want the help of an expert, whether internal or hired as an external contractor. After all, cybersecurity risks are not purely technical problems, but are deeply rooted in the operations of your company. A trusted expert can help you identify the root cause of all your cybersecurity risks, whether they be technical or operational in origin, and provide a clearly articulated strategy for comprehensively managing those risks, without leaving behind any loose ends.

VULNERABILITY ASSESSMENT AND PENETRATION TESTING

After the risk assessment, your organization should also run a vulnerability assessment, which is a targeted scan that looks for weaknesses in your cybersecurity defenses. Vulnerability assessments use specialized tools to draw from a database of known weaknesses and probe your systems in search of potential areas of exposure, like out-of-date or poorly-patched software and firmware. Regular vulnerability assessments might have helped prevent the "NotPetya" attack of last year, which did widespread financial damage to over 65 countries by exploiting unpatched software.

You may also consider a deeper, more involved test called a penetration test or "pen test." The goal of the penetration test isn't to merely locate vulnerabilities, but to exploit those weaknesses just as a hacker would during a real-life attack. While a vulnerability assessment is a largely automated process, penetration testing is conducted by a skilled security professional with the expertise and creativity to mimic a real-world hacker.

High-profile organizations should perform monthly vulnerability testing to ensure that changes in their technology don't create a hole in their cyber defenses. As a bare minimum, smaller businesses should conduct vulnerability and penetration testing after new security patches have been applied, or after significant alternations have been made to their network infrastructure or applications.



GOVERNMENT REGULATORY COMPLIANCE

A major focus for organizations, especially those in regulated industries like finance and healthcare, is to stay compliant with government regulations. Some of the regulations that SMBs must adopt most often include HIPAA, PCI-DSS, FINRA/SEC, GDPR, FAR/DFAR & NIST SP 800-171, NYS-DFS part 500, and others.

While it's extremely important to make certain you meet or exceed all the regulatory compliance standards for your industry, you shouldn't let regulatory requirements dictate your entire security posture. New threats emerge quickly, yet it can take regulatory agencies up to 24 months to identify changes, update existing guidelines, and publish those requirements to the public. Because government regulations tend to be so far behind the latest cyber threats, organizations with a security strategy that's based solely on compliance standards open themselves up to new threats the regulatory bodies haven't accounted for.

In the complicated realm of cybersecurity compliance, many businesses and organizations find it beneficial to seek the assistance of an experienced technology services firm. Enlisting the assistance of a partner can help you clarify your organization's regulatory requirements, ensure that those needs are consistently met, and help you apply for exemptions or waivers in situations where your security already exceeds a specific standard.

DISASTER RESPONSE AND BUSINESS CONTINUITY PLANNING

As we've established, in cybersecurity there is no absolute prevention. Even an isolated system with no connection to the Internet or other computers has vulnerabilities. Based on the assumption that serious problems will *inevitably* occur, businesses should have a strategy to mitigate the impact of these events. This should include a business continuity plan supported by a very proactive disaster recovery effort.

Though the two concepts are often conflated, important differences exist between the two. Disaster recovery means having the ability to restore your data and applications after something seriously damages your infrastructure. Good disaster recovery starts with backing up critical data so it's always available from a secure, off-site location. You'll also want to define your tolerance for downtime of each system and document a process for the recovery of sensitive information in your disaster recovery plan.

Business continuity is a larger concept that describes the speed at which your business can recover to full operations after a catastrophe. As opposed to disaster recovery, business continuity addresses the overall security of your business operations, from defining alternate work locations, to supplying battery backups that keep on-premise servers and critical workstations online. To make sure your disaster recovery and business continuity plans provide comprehensive protection, both should be well-documented and shared throughout your organization, and revisited and updated on a regular basis.

CONCLUSION

What we've provided here is an overview of the cybersecurity and compliance challenges facing today's SMBs, and the steps businesses need to take to mitigate those challenges. Although we touched on many of the major points that an SMB will want to address, there are countless, more complex elements that were beyond the scope of this white paper. We encourage any small- or medium-sized company that's eager to improve their cyber defenses to contact us at 212-299-7673 with any questions they might have. We're happy to use our experience to level the playing field, help the good guys win, and keep the bad guys from doing any more damage than they've already done to this vital sector of the economy.

ManhattanTechSupport.com, 55 W 39th St,12th Floor, New York, NY 10018
Sales: 212-299-7673 sales@manhattantechsupport.com

ABOUT ManhattanTechSupport.com

ManhattanTechSupport.com is a recognized leader in providing SMBs in New York City with cybersecurity strategies and solutions that optimize their defenses and minimize the chance of disaster. For over 20 years, ManhattanTechSupport.com has been providing bespoke cybersecurity services that cover each aspect of our clients' technology, from cloud and mobile computing, to servers and workstations.

Our team of security and network experts will help you build and manage a risk-based security strategy that keeps your business or organization safe, while minimizing its impact on productivity and making the most of your security budget.

Learn more about cybersecurity services from ManhattanTechSupport.com:

Call Us

212-299-7673

Email Us

sales@manhattantechsupport.com

Visit us on the web

www.ManhattanTechSupport.com

ManhattanTechSupport.com, 55 W 39th St,12th Floor, New York, NY 10018
Sales: 212-299-7673 sales@manhattantechsupport.com