Complete Security
Secure Network
Secure Data
Secure Identities and Access
Secure Mobile Environment
Secure Apps

Where do you begin if you currently have little to no Cybersecurity Protection? Common Sense IT Security Measures Could Help

According to Verizon Data Breach Investigation report, 61% of breaches hit small businesses, up from the previous year's 53% (2017).

Small Businesses A Criminal's Target, Consequences are High

Studies continue to reveal and confirm alarming facts about attacks and consequences on small businesses when security measures are inadequate:

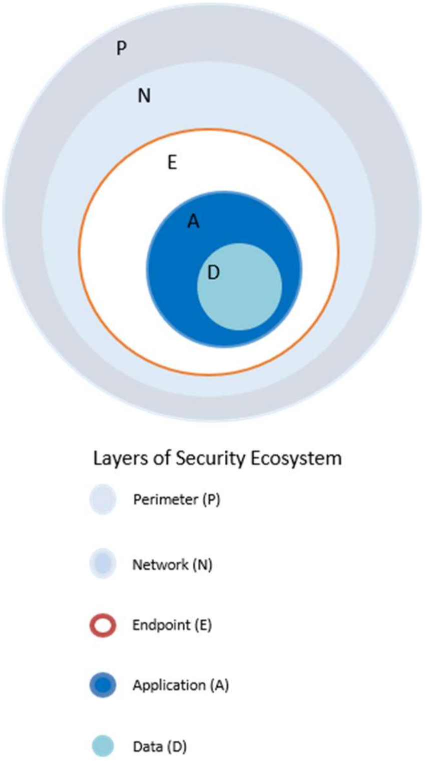
- 1 in every 2 small businesses were cyber attacked, hacked or experienced a data breach in the last 12 months (Ponemon Study[1], 2016)
- The **average cost** of **a single** cybercrime **incident** for a small to med-sized business (<1000 employees) is **$40,000** (National SBA Estimate) to close to **$2 Million** (Ponemon Study[1], 2016)
- Nearly 60% of small businesses that are hacked ultimately go out of business within half a year of the attack according to a study cited by the subcommittee chairman Rep. Chris Collins, (R-NY) (Fox Business, 2013)

Common and Impending Cyberattack Threats

There is a significant number and a broad range of cyberattack types. However, the internet crime report (2017) published by the FBI this past May reveals the biggest threats to include Business Email Compromise (also known as Phishing, Whaling and Spearphishing), Advanced Persistent Threats, Ransomware, Malware and Zero-day attacks. Others cited by a recent panel of cybersecurity experts including the Co-Chair of the National Advisory for the FBI Director include DDoS (Distributed Denial of

Service), Internal Attacks (Disgruntled or terminated employees, administrators, etc.) and Password Attacks. Visit the following URL for additional insights recently shared by cybersecurity experts about Cybersecurity Threats

https://www.areteadvisorsltd.com/cfolceventmaterials



So where do you begin?

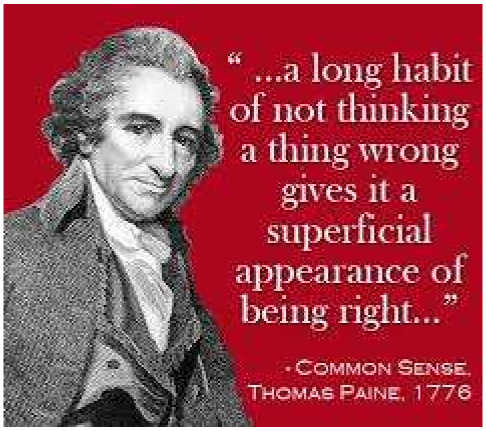
If you are a small enterprise with limited resources and currently have zero (i.e. nada, little) Cybersecurity Protection, where should you begin, and how do you maximize the investment of your limited resources on cybersecurity protection?

First, recognize that there is no silver bullet solution. The security ecosystem is complex and broad. Any vendor that promises they can solve all your cybersecurity risks and issues with a single product or solution is likely a fraud.

Second, every organization that uses any technology or IT systems, applications or the internet to support their business in any manner, will by using technology and the internet, be vulnerable to cybersecurity attacks. Each of these organizations must protect their company's users, data, IP, digital assets and systems at various layers of the security ecosystem (illustrated in the diagram on the left).

Traditionally, it was cost-prohibitive to provide even the most basic security. With the advent of next generation technologies and tools, small enterprises today benefit because these tools are not only readily available and simple to deploy but they are also amazingly affordable. Companies with as few as 10 users/employees can implement basic security tools for the price of a cup of Starbucks coffee per employee, per month.

If you are just starting to implement a cybersecurity program and currently have zero protection, you should take measures to, at minimum, address your known highest risk vulnerabilities, as well as known vulnerabilities that could cause severe adverse impact on your business (even if the likelihood of occurrence is low).


"...a long habit of not thinking a thing wrong gives it a superficial appearance of being right..."
- Common Sense, Thomas Paine, 1776

A Common-Sense and Pragmatic Approach on a Shoe-String Budget

What security measures and actions can small businesses take immediately on a shoe-string budget that is practical and will yield maximum benefit to safeguard against cybercrime? Well, there are several of what we call **Common Sense Security Measures** that you, your team or consultants can start implementing right away. These measures encompass policy, procedures, training, basic tools and risk mitigation techniques.

Policy, Procedures, Training and Education

1. Define and adopt a strong password security policy. As much as you love your child or wife, using their first name as a password should be strictly prohibited on all work and business systems, computers and devices. Convenience should not be equated with good policy. Try using a short phrase you love but difficult for others to guess and one that uses a combination of alphanumeric and symbols instead. e.g." My1stdoglovesicecream!"
2. Keep your systems up to date by applying security patches. A key speaker who spoke at an agency event earlier this year regarding cybersecurity and who requested anonymity (for this publication) reminds us the reason Russia and China are the biggest victims of widespread worms and malicious code (think "Wannacry") is because they allow large numbers of their systems to remain unpatched. According to Osterman Research (reported by CNN Tech on July 27, 2017), about 22% of 1,000 businesses with less than 1,000 employees randomly selected for the study, 22% had to cease business operations immediately because of a cyberattack, and 15% loss revenue because of it. If you are a federal contractor, you know that stopping business means you cannot fulfill your contract obligations, and this would hurt your past performance or your supplier risk system ratings. And for those who failed or were negligent to protect against the crime in the first place because of lack of adequate security measures would be further penalized by being with an issued **Corrective Action Request (CAR)** for contractual non-conformance.
3. Adopt good "cyber hygiene". e.g. Evaluate and check for security patches on a periodic basis, at minimum, monthly. Change your passwords and scan for viruses. Do these things regularly or periodically based on business need, scheduled vendor releases of patches and other factors. For example, if Microsoft releases its patches every first Tuesday of the month, incorporate into your SOP (Standard Operating Procedure), a policy to evaluate and deploy these updates in your production environment by timing these tasks to occur after each of those Tuesday releases.
4. Thumb drives. Don't use unauthorized thumb drives at work and do not permit personal thumb drives to be used on business laptops, work computers or equipment, or allow work authorized thumb drives to be used at home or on unauthorized personal PCs.
5. Make sure you don't just have good security policies. Be certain to train your people on those policies based on their roles.

6. Foster a security resilient culture where all employees are trained to recognize, identify and report suspicious cybersecurity activities.
7. Enforce your policies. Make sure your people follow the rules. Conduct random audits to ensure compliance to identify areas for remediation and employee training needs.
8. Like number five and six above. Define good security management processes, then train and have people follow those processes.
9. Grant user access to only those who need it, applying what security experts call the “principle of least privilege”. Grant minimum access needed to enable users to do their jobs. If they only need X access to do their jobs, don’t give them X and Y access.
10. Realize that the number one IT security threat lies in your organization. That’s right. It’s your people. An authority on IT security once said, “CEOs to secretaries, they all peruse websites they should not”. Awareness training and education is necessary to prevent behaviors that could inadvertently harm your network and shut down your business. Tools like Varonis that deploy artificial Intelligence and behavioral analytics could also be used to prevent and mitigate risks of insider threats (internal employees stealing sensitive data).
11. Don’t conduct high risk activities (e.g. online business banking) on unsecured or public Wi-Fi
12. Check for the lock symbol in the browser to make sure it’s secure before using it. Make sure there is an ‘s’ at the end of http. E.g. Https://
13. Public Wi-Fi are easily available, and many are free these days. Don’t be quick to connect your work devices or laptops to them for speed and convenience without thinking of what-ifs. These little convenient luxuries are the perfect means for a dishonest person and cyber criminals to hack your systems, steal your digital credentials and exploit your devices’ vulnerabilities.

Combination of Risk Mitigation, Tools, Controls, and Policy

14. There is an overwhelming number of cybersecurity tools and products in the marketplace today, all touting to have the best technology and capabilities to provide maximum protection for the least amount of investment. It is difficult even for experts to sift through the rapidly growing market of cybersecurity products to differentiate what are legitimate claims from pure marketing ingenuity. To this end, we recommend getting a combination of professional cybersecurity expert advice and fact-checking with sources like Gartner, an independent

research consulting company to ensure the product does what it says it does, and that the product is also appropriate for your environment.

15. What tools should you consider?
At a minimum, consider having a tool that protects each layer of the security ecosystem: Protect your
    a. Network and perimeter
    b. Internet users
    c. Users and root-users (privileged) access to systems, application and devices
    d. Business applications
    e. Devices (all end-points) including laptops, PCs, Macs, iPhone, Tablets, Androids that are allowed at work and for your users to access company's email and systems
    f. Data
16. Implement two-factor (2FA) user authentications. Effective two-factor authentication tools like Duo or TokenOne can be inexpensively deployed on all devices. Don't be penny wise and pound foolish about security. 2FA tools are considered basic controls and strongly advocated by both public and private security experts alike for small enterprises
17. Do not connect your outdated systems that are on corporate networks directly to the internet. Outdated systems are vulnerable to malware and ransomware and could provide hackers with easy access to your networks and critical systems. Systems with outdated versions of operating system are found to be almost three times as likely to experience a breach, according to research (HelpNetSecurity, June 9, 2017). Implement hardware firewall or next-gen solutions like Zscaler that are software defined or Cloud-based.
18. Make sure your systems are protected from Zero-day and known malware attacks. Not all tools and technologies protect both, and not all tools protect all types of devices or various layers of the ecosystem. So, be clear about which ones you need, and seek professional advice that can provide product, technology and cybersecurity business knowledge and expertise to ensure you are comparing apples with apples and not apples with oranges. As an example, Cylance is a tool that provides Zero-day and malware protection, effectively providing anti-virus protection using Artificial Intelligence/Machine Learning algorithms to detect, predict and prevent Zero-day attacks on devices such as PC and Mac, even when they are not connected to the Internet. However, it does not protect malware at the network level, and a separate tool such as Zscaler is necessary to prevent malware from accessing through the network perimeter. Having one however does not replace the other.
19. Backup and Recovery – Take measures to make sure you have a sound and secure backup and recovery policy and process. Backups provide "point in time" protection, which means you can restore data should it be lost through Ransomware, or simple human error. Today, you can store and recover data easily, securely and cost-efficiently using cloud solutions. Tools like Druva provide automatic data back and recovery to and/from the Cloud.
20. Mitigate risks and deploy more stringent security measures based on security risks. Classify your systems and data. If you have voluminous unstructured and structured data, tools like Varonis can help automate and classify data easier. Don't keep mission-critical data on networks or systems that are "online" and "available" 24/7 if you don't need to. Segregate your mission-critical systems and data from those that contain mostly general non-sensitive data for which the latter may not require as stringent a security policy.

For those who are concerned about being compliant with the law, it is worth keeping in mind that security requirements haven't changed that much in a decade. As an agency representative was once heard saying, the biggest change (in requirements) lies in the need for contractors to a) demonstrate compliance and b) self-report security deficiencies to the authorized DoD CIO in a timely manner as specified by the law.

Conclusion

As investors, senior management and owners of small businesses, you do want to act and act quickly to both protect your business and investment, as well as comply with the law. If you have not started evaluating your IT security risks or identified the gaps between your existing security environment and the requirements of the law, you need to start immediately. If you do have a good understanding of your gaps but haven't remediated those gaps, you probably want to start developing an action and remediation plan quickly. Rest assured the Agency you do business with will be enforcing these cybersecurity laws because if they didn't our nation's systems and sensitive data could be put in danger.

In a nutshell, some of the best security measures are those that are basic, practical and common-sense. Small and larger businesses are reminded to take these precautions. Before you rush into creating complex security programs or purchasing expensive security technologies, you should first ensure you understand where your biggest risks lie and, prioritize remediation needs to protect your business. When addressing gaps, ensure the basics, highest risk areas, low-hanging fruit opportunities and those remediation issues that take a long time to resolve are tackled first. You may be surprised to find that many of those gaps can be easily addressed by implementing common sense IT security measures discussed in this article.

Finally, if you don't have internal IT security expertise, seek professional or consulting assistance from the experts. Don't throw good money away on bad decisions or buy security products you don't need or do little to help you defend your systems or comply with the law. There is no silver bullet that will allow companies to address all your IT security needs. No one product is designed to address the range of cyber security threats. Anyone who promises you their product will do so is a fraud. Google 'cybersecurity products' and you will find no less than 22 million search results. An expert can help you narrow down the list to a handful of products that work best for your needs or environment. Also bear in mind that a reasonable solution should encompass training for your people, adequate policies, procedures, and processes, and configuration of the right mix of tools to protect your network, data, systems, devices, users and customers. Real-time monitoring, reporting and analytics are also necessary to ensure anything that is broken can be quickly identified, reported, assessed and fixed in a timely manner.

The following are additional resources you may wish to use as a guidance for defining your IT security plans, policies or programs:

https://www.areteadvisorsltd.com/cybersecurityresources

https://www.cisecurity.org/

https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

Resources:

1. Ponemon Institute is the pre-eminent research center and thought leader dedicated to privacy, data protection and information security.
2. Fox Business, "Most Small Businesses Don't Recover from Cybercrime", Karol, G., March 2013
3. https://www.fcc.gov/general/cybersecurity-small-business
4. https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework
5. https://www.cisecurity.org/

This Publication
This publication is written by Arete Advisors LLC, (“Areté”), in collaboration with Hararei, Inc., a strategic alliance and joint venture partner.

About Hararei, Inc.
Hararei is a strategic IT and infrastructure boutique consultancy firm and channel partner for leading-edge cloud, cybersecurity, network and data management solutions and services. Visit www.Hararei.com

Disclaimer
This publication does not constitute professional advice and you should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, Hararei, Inc. does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

areté Achieve more with *less*

Arete Advisors is a boutique management and technology consultancy. Areté (pronounced ah-ree-tay) specializes in helping small businesses address IT security risk assessment, cybersecurity, cloud, policy, process, compliance, governance, training, quality management (ISO) and risk management challenges.

Website: www.areteadvisorsltd.com

Visit the following URLs to learn more about cybersecurity solutions and resources:

https://www.areteadvisorsltd.com/smallbusinesscybersecurity

https://www.areteadvisorsltd.com/cybersecurityresources

For Small Business Consulting Services, contact:
Lilian Snodgrass
Managing Director
(917) 288-4756
ls@areteadvisorsltd.com

General Inquiries
Phone: +1 (862) 295-1488
Email: contact@areteadvisorsltd.com

Product Channel Partner

Hararei, Inc. is a proud channel partner and value-add reseller of leading cyber-security products that are cost-effective solutions for small businesses. Contact us to schedule a free assessment and demonstration of these and other products.

Zscaler enables secure, policy-based access to the Internet. Block attacks are in real time with network security that is always inline, cost-effective and easy to deploy. Protect your employees from malware (including Ransomware), viruses and other internet threats, blocking attacks in real time. Zscaler security services scan and filter every byte of your network traffic, *including SSL-encrypted sessions*, as it passes to and from the internet.

Varonis is the only company that can monitor, manage and protect human–generated data in critical file systems, email, intranets, and file shares, while at the same time increasing employee productivity and reducing costs, and only Varonis have proven that they can do it at scale

DB Networks next generation technology is based on database infrastructure sensors, deep protocol extraction, machine learning, and behavioral analysis. The technology is foundational to achieving the ultimate vision of autonomous cybersecurity.

Druva is a Cloud Native data protection technology that can protect your data whether it is on-premise, or in the Cloud. The technology is data protection technology that was "born in the cloud" to address the unique challenges of protecting your sensitive data wherever it may reside.

Duo Security implements two-factor authentication (2FA) which strengthens access security by requiring two methods (also referred to as factors) to verify your identity. These factors can include something you know — like a username and password, plus something you have — like a smartphone app to approve authentication requests.