hararei areté

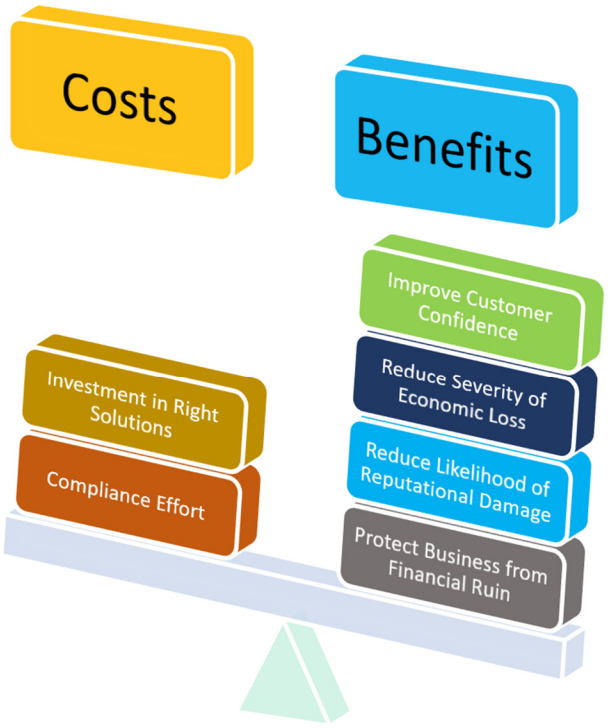
Article

Are you compliant with the new Cybersecurity law? Common Sense IT Security Measures Could Help

The deadline for federal contractors to comply with DFARS **clause** 252.204-**7012** (Safeguarding covered defense information and cyber incident reporting) is drawing near. Small and large companies alike who do business with the Department of Defense and wish to continue doing business with the agency are required to implement NIST SP 800-171 standards, as soon as practical, but not later than December 31, 2017. NIST SP 800-171 is a directive for *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.* This clause flows down to all subcontractors and teammates so any vendor that does business with the federal agency directly or through their primes must demonstrate compliance with the requirements.

Government's Cybersecurity Law a Pain but Ultimately Benefits You

While the NIST SP 800-171 regulatory requirements are laced with lots of technical jargon and terms that may be foreign, you will be surprised to find that a lot of it can be boiled down to common sense and basic IT security measures that are necessary to protect your systems and data. Amid the rise of cyberattacks, many of the requirements force businesses to practice good security hygiene which ultimately benefits companies. Adopting good security practices will not only enable your business to comply with the regulations but it will also protect your valuable digital assets.

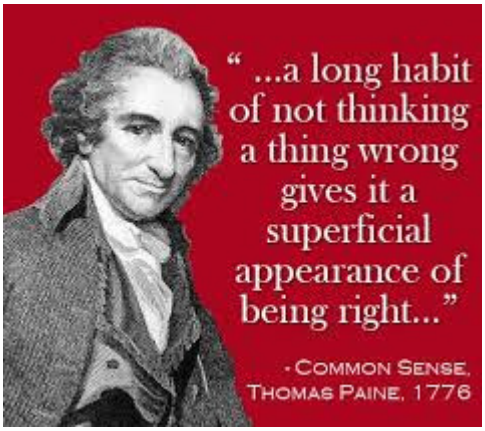


Small Businesses A Criminal's Target, Consequences are High

For small businesses, complying with the laws could help protect you from being financially ruined by a cyberattack. Studies reveal 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)

© 2017 Arete Advisors LLC and Hararei, Inc.
All Rights Reserved. Copying, reproduction, and distribution without written permission are strictly prohibited.



A Common Sense Approach

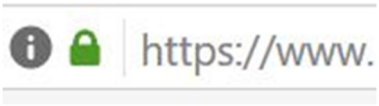
What security measures and actions can small businesses take immediately not only to safeguard against cybercrime but also start complying with the federal law? Well, there are several of what we call **Common Sense IT Security Measures** that you, your team or consultants can start implementing right away. These measures encompass policy, procedures, training, automation 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 had to cease business operations immediately because of a cyberattack, and 15% lost revenue because of it. If you are a federal contractor, you know that stopping business means you cannot fulfill your contract obligations. And for those who failed or were negligent to protect against the crime in the first place because of lack of adequate security measures, you would be further penalized. The Agency would issue a **Corrective Action Request (CAR)** against you for contractual non-conformance, and this would hurt your past performance or your supplier risk system ratings.
3. Adopt good "cyber hygiene". E.g. Change your passwords regularly and scan for viruses. Evaluate and check for security patches on a periodic basis, at minimum, monthly. 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. Don't just have good security policies. Be certain to train your people on those policies.
6. Enforce your policies. Make your people follow the rules. Conduct random audits to ensure compliance to identify areas for remediation and employee training needs.

© 2017 Arete Advisors LLC and Hararei, Inc.
All Rights Reserved. Copying, reproduction, and distribution without written permission are strictly prohibited.

7. Similar to number five and six above. Define good security management processes, train and have people follow those processes. This will prevent bad decisions during the "fog of war" that often accompanies chaos that occurs when an attack is discovered.
8. If your systems do get compromised, self-report and get covered. Fail to report and you would be in violation of the clause, and could lose your contract.
9. You must be prepared to show or supply documentation that shows evidence that you are in compliant with the NIST SP 800-171 security requirements. Proper documentation and electronic filing is necessary to ensure that you can quickly retrieve the relevant documentation in response to an agency's audit, request or inquiry for evidence of compliance. Such documentation includes but is not limited to your company's IT security policy and plan.
10. Grant user access to only those who need it. 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. This is what security professionals call the principle of "least privilege".
11. 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 be used to prevent and mitigate risks of insider threats (internal employees stealing sensitive data). Note: Varonis is also used by Federal Agencies like the Defense Logistic Agency.
12. Don't conduct high risk activities (e.g. online business banking) on unsecured or public WiFi. Majority of small businesses do not realize that *business checking accounts are not protected by banks if their bank accounts are hacked,* according to Molly Brogan, Director at National Small Business Association (FoxBusiness, September, 2013)
13. 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://



14. Public Wi-Fi is easily available and many hotspots 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.

© 2017 Arete Advisors LLC and Hararei, Inc.
All Rights Reserved. Copying, reproduction, and distribution without written permission are strictly prohibited.

15. Implement two-factor authentications where possible. 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.

16. 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.
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.

Conclusion

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 said earlier in the year, "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

© 2017 Arete Advisors LLC and Hararei, Inc.
All Rights Reserved. Copying, reproduction, and distribution without written permission are strictly prohibited.

specified by the law. Recognize two other differences; a) there is a rapid and aggressive rise of cybercrimes and b) scrutiny for suppliers to adopt proper company IT security measures is heightened by both federal agencies as well as end-user and business customers.

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, prioritize remediation needs to protect your business and comply with NIST SP 800-171 requirements. 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.

Last but not least, 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 comply with NIST SP 800-171 requirements or 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 and 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 guidance for defining your IT security plans, policies or programs:

https://dibnet.dod.mil/
http://dodprocurementtoolbox.com/faqs/cybersecurity

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. Fox Business, "Cyberattacks costs small business…", Karol, G., September, 2013

© 2017 Arete Advisors LLC and Hararei, Inc.
All Rights Reserved. Copying, reproduction, and distribution without written permission are strictly prohibited.

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

This Publication
This publication is written as a collaboration between Hararei, Inc., and Arete Advisors LLC, ("Areté"), a strategic alliance.

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

© 2017 Arete Advisors LLC and Hararei, Inc.
All Rights Reserved. Copying, reproduction, and distribution without written permission are strictly prohibited.

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.

© 2017 Arete Advisors LLC and Hararei, Inc.
All Rights Reserved. Copying, reproduction, and distribution without written permission are strictly prohibited.