According to Verizon’s 2019 Data Breach Investigations Report, 43 percent of reported breaches affected small businesses. There are more than 30 million small businesses across the United States, and tens of thousands of them perform work for federal, state and local government agencies. The requirement to diversify the size mix on most federal and state contracts has increased over the past 10 years, and many of the smaller companies struggle with information technology (IT) security regulatory and statutory requirements.

Rapid changes in technology create new security vulnerabilities that require small businesses to expend resources to remain compliant. Lack of guidance, definitions or policy place small businesses in positions requiring them to make security investments without fully understanding the need or outcome of the resources they expend. While companies that provide IT services to the government are better staffed from a security perspective, those that provide other services often do not have the staff or expertise to operate their internal computer systems at a high level of security, making them ideal targets for adversaries. While the U.S. Defense Department and some federal agencies have strong information security compliance policies that their contractors must comply with, other government agencies may not have such policies.
The fundamental problem is twofold: increasing technology complexity and competition for trained security professionals. Unlike other critical systems a business owner must maintain such as the plumbing, air conditioning or electrical wiring in the building, skilled maintainers of information systems are hired at salaries that small businesses often cannot afford. This leads many small businesses to hire junior personnel and make additional investments in their training and education to maintain competency in rapidly changing technology. Once trained, many are hired away by larger companies offering opportunities that the small business cannot offer, leaving small businesses to start the training process over again.

AFCEA’s Small Business and Cyber committees present best practices, recommendations and information resources for small businesses. This paper is intended to support training and increase awareness for small businesses within local AFCEA chapters.
Some small businesses struggle with cybersecurity because they cannot afford an expensive solution, have limited time to devote to it or simply just do not know where to start. A small business is an organization defined by the North American Industry Classification System (NAICS) codes that stipulate revenue ceilings or employee numbers. Small business employee numbers are different in every case, but more importantly, most of these companies have a small or nonexistent security team.

Small businesses are structured to be efficient in delivering their products or services to the government customer and to place the majority of their labor in direct support to the customer; consequently, they minimize the overhead staff. As such, only one to five employees handle general IT services such as managing hardware and software to support business needs or contracting for external IT services.

In some cases, IT security is often an additional duty assigned to an IT staff member and rarely does that person coordinate with the person responsible for physical security such as keys, locks and badges. Human security, including health, safety and identity theft, is unfortunately not a major focus for most small businesses.
Relying on a single security person to protect a company, or a fraction of one person’s time if it’s an additional assigned duty, places a small business at high risk of becoming a victim of a range of security issues. From lowest to highest business impact, some of these problems include:

- Website defacements or phishing against customers resulting in reputation damage.
- Viruses and malware entering the company’s network causing work disruptions.
- Data breaches resulting in the theft of intellectual property such as employee or customer data or other sensitive corporate information.
- Ransomware that encrypts sensitive data and bad actors who demand a payment for decryption of this information.
- Direct manipulation of machinery, control systems or other connected devices that results in business disruptions.
- Mechanical or logical damage that could destroy a critical system or lead to human injury or loss of life.

For businesses contracting with the government, a minor security incident could lead to the loss of a major contract and even a restriction to bid on future work. For businesses that deal with consumers and the public, a security incident could lead to expensive lawsuits or loss of customer confidence. Major security incidents could put a company out of business virtually overnight. Some small businesses have Employee Errors and Omissions insurance, but it’s expensive. Lack of a comprehensive insurance strategy to cover liability when dealing with the government may lead to significant business losses.

Of course, security issues are not only limited to cyber risks but also to physical and human risks. Many businesses rarely coordinate security across all three risk areas, and in general only deploy the minimum number of controls needed to “feel secure” or to comply with a specific customer’s contracted requirements. For small businesses supporting the Defense Department, this will change with the requirement to comply with the Cybersecurity Maturity Model Certification (CMMC) process. This is the Defense Department’s effort to provide a unified cybersecurity standard to protect Controlled Unclassified Information (CUI) data on contractor networks and reduce the risk against a specific set of cyber threats.
The increasing complexity of technology supporting businesses requires the development of a new workforce that can install, maintain and secure it. Most of the common enterprise IT systems like desktop and laptop computers are designed to work out of the box with minimal expertise by the owner. Internet of Things (IoT) devices also are designed to be self-configuring and easy to install. Manufacturers of enterprise IT systems and developers of their accompanying operating systems and application software have dramatically improved the way these systems can update themselves and detect known problems. But beyond the desktop or IoT, installing and maintaining the IT infrastructure such as routers, WiFi gateways, servers and security event monitoring requires specialized skills and training. Some infrastructure devices can automatically detect and repair problems, but most require human control for proper operation.

A small business with an in-house enterprise IT staff may typically devote less than 5 percent of its total employee count to that function. Finding and retaining an employee with a decade or more of IT experience is difficult. A rare employee with high levels of competence and training will be difficult to retain unless the business can offer a compensation plan that goes well beyond salary. Some companies may retain an outside network/security consultant to periodically review policies and procedures; that consultant also can assist in-house staff who are working toward certification.

A sample of the IT-related infrastructure a small business must operate, maintain and secure includes:

- The internal office Local Area Network (LAN), which could be wired or wireless.
- Gateways, routers, modems or other devices that connect the internal LAN to the Internet.
- Internal and external websites, including both content as well as back-end connections to data servers.
• Security systems such as firewalls, Intrusion Detection Systems (IDS), and Security Information and Event Management (SIEM) tools.
• Domain names and accompanying Domain Name System (DNS) configurations.
• Email and other business servers.
• Data storage and backup capabilities.
• Cloud services such as Amazon Web Services or Microsoft Office 365; this includes all instances of Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).
• Remote access for teleworking employees.

A small business that is not a technology company will likely outsource the operation, maintenance and security of most of these systems to one or more vendors, anticipating that the vendors will protect them at a sufficient level. When outsourcing is used, a company employee must manage the contract and have the competence and skills to know if the vendors are performing properly. This is an aspect that is frequently overlooked.
Some businesses will retain a small internal IT staff for essential functions such as troubleshooting Microsoft Office applications, configuring new computers and replacing printer toner. These support employees normally will not have the advanced training or skills needed to secure the company’s website, network infrastructure, databases or other resources that are prime targets for adversaries. Outsourced technical support is often used to fill this gap, as are hosted email and web services.

Beyond IT staff, many small businesses struggle with the security competency of the regular employee. For example, do all employees know how to recognize and respond to a phishing email or a tech support phone call scam? Even worse, do all employees know what information is on their computer systems and the impact to the company should that data be stolen, modified or destroyed with no backup available?

Some businesses may find benefit in hosting their networks and servers in an offsite co-location or data facility. This allows the facility to handle physical security, power and environmental systems. Personnel who enter the facility must be vetted and badged, their entry and exit are usually recorded on camera, and the small business is not absorbing the overhead costs of the employees. Small businesses also will not have separate bills for uninterruptible power supplies (UPS) or worry about weather or local construction affecting building power, will not need separate/additional air conditioning for the server room, and will not have to monitor heat, humidity or flooding.
All businesses, whether they have a full in-house IT and security team or everything is outsourced, should at a minimum follow these principles:

Business considerations:

• Properly vet employees’ education and certifications and perform a pre-hire background check.
• Properly insure the company with coverage for all aspects of operations, including people, process and tools.
• Know what IT resources are owned or used by the business; know which resources are outsourced.
• Ensure that all employees understand the need for protecting information systems and understand their individual role with respect to security, as well as that an Acceptable Use Policy is in place and is enforced.
• Document the company’s security policies and train employees on their use.
• Develop policies for the use of personally owned devices in the office, as well as the processing of company information on personally owned computers.
• Engage the business’s legal staff to ensure compliance with any applicable laws, regulations or standards.
• Consider retaining a senior network/security consultant to periodically review policies and procedures.
Technology considerations:

- Separate IoT devices such as cameras, voice-activated assistants and smart appliances, from enterprise systems by putting them on a different physical LAN or WiFi network with no cross-connections.
- Encrypt everything, including hard drives, removable media, WiFi access points and website transactions.
- Have a plan for the protection of company assets when employees work remotely.
- Provide a mechanism for backing up critical business information.
- Ensure that all endpoints use security software.
- Keep all software updated and patched.
- Enforce a strong password policy.
- Limit access to resources to only those who have a need to know.
- Develop and practice an incident response plan for a cybersecurity crisis.
- Don’t forget about physical security.
Often a small business with no security expertise on its staff struggles with the problem: “Where do I start?” A business that has been in operation for more than a year has most likely developed a basic cybersecurity understanding and has developed initial policies such as keeping systems updated or using anti-virus software. But a startup or a business that has not given much thought to security may need a starting point.

A great way to begin is to follow an existing cybersecurity model for building a security plan. The Small Business Administration offers a wealth of information for small business owners online at https://www.sba.gov/business-guide/manage-your-business/small-business-cybersecurity.

The FCC has a Cyber Planner located online at https://www.fcc.gov/cyberplanner for developing a small business cybersecurity plan.

DHS also has a Cybersecurity Road Map on the CERT website at https://www.us-cert.gov/sites/default/files/c3vp/smb/DHS-SMB-Road-Map.pdf to help companies get started.

Small and large companies supporting the Defense Department will need to comply with the CMMC, and according to Katie Arrington, chief information security officer, Defense Department, most are required to comply at level 1. There are five maturity levels ranging from basic hygiene to advanced security. The CMMC effort builds upon existing regulations (DFARS 252.204-7012) and will require contractors’ internal networks and systems to be audited by a third party and receive an official level of security, which is expected to be a consideration during the acquisition process in the future. There are 17 security controls for the first level of the CMMC. Consider approaching the CMMC in a step-by-step process by addressing level 1 first and then moving on to the next levels. Most of the first-level items are nontechnical and only require changes or updates to corporate policies.
Businesses that don’t have a road map from a supported agency to follow should consider doing the following:

**Step 1: Conduct inventories.** Any company, whether new or old, cannot have a working security program if the business does not know what assets or resources it owns. The first step in any cybersecurity plan is to inventory the business’s hardware, software, databases, domain names, email accounts, cloud services, access points and anything else related to information technology. Analysis of data breaches by Verizon over the past several years reveals that most attackers either access an unknown resource or breach the business’s perimeter by a previously unknown access point. Eliminating those unknowns is part of this first step. The inventory should include model numbers and software version so the equipment can be sorted and tracked for end-of-life/end-of-service dates. Once a manufacturer stops patching an outdated system, it can be vulnerable to a cyber attack.

**Step 2: Manage configurations.** Secure configuration of these assets is the next move. Most systems come from the manufacturer with default usernames, passwords and configurations. Consequently, unnecessary software features may be active, passwords are weak or guessable or remote access capabilities are enabled. Numerous guides for securely configuring various products are available. This mindset applies to cloud services just as much as physical systems.

In addition, before putting sensitive company data into the cloud, ensure that the company’s cloud is configured securely. It is imperative to update these configurations regularly and maintain the latest security software, web browser and operation systems to defend against common threats such as malware and viruses.

**Step 3: Secure the work environment.** Control physical access to company equipment. Today’s work environment is no longer just the office; it extends into the home, car, hotel room, café and many other places. Begin by securing what is close at hand such as desktop or laptop computers, office networks and software systems used in the office. Then extend the policies and action to mobile devices and remote or home offices. Finally, develop policies and
protocols for resources outside of the company’s control such as outsourced websites, email or other systems. If employees work from home, ensure the business has VPN access and a firewall. Limit employee access to back-office functions to only those required to use them and limit the authority to install software. Consider using a multifactor authentication approach instead of just username and password.

**Step 4: Secure employees.** Probably the most overlooked initial step for any small business is education and awareness training for employees, staff and everyone handling company information. Nobody is expected to be a security expert, but all employees should be expected to know the company’s security policies, to follow basic security hygiene principles, and to complete security training on an annual basis. Steps like choosing complex passwords, knowing how to react to phishing or scam calls, and knowing how to report an incident are a great starting point.

To assist with retention, a company should build and execute an employee training program that aligns with your business needs by:

- Training and certifying the IT workforce in areas needed by customers and the business.
- Provide a career progression for these employees.
- Pay them market price for what they know and the responsibilities they perform.

**Step 5: Backup critical data.** A major security incident can largely be avoided by having and following a good security plan, but because of the complexity of IT systems and the skills of criminals and other adversaries, incidents will occur. The worst that could happen to many small businesses is the loss of critical data tied to revenue-generating projects. This could be databases, human resources data, software code under development, accumulated research or papers underway, financial records or testing results that cannot be easily reproduced. Data backup systems, along with regular exercises to restore from backup, will help a business recover from ransomware attacks, theft or failure of hardware devices. In addition, organizations must store backups either offsite or in the cloud.
Step 6: Establish policies. At a minimum, businesses should have the following cybersecurity policy topics and procedures in place as either separate policies or as part of the Employee Handbook.

- Acceptable Use of Information Technology containing guidelines for the use of computers, telephones, the Internet, email and voicemail.
- Information security: Guidelines for passwords and levels of access to the network, virus protection, confidentiality and use of data.
- Security awareness: Training employees must complete.
- Physical security.
- Technology standards: Security baseline for company-owned PCs/mobile devices and information about what is prohibited, for example use of peer-to-peer software.
- Continuity of operations and disaster recovery, including data backup methods.
- Media destruction.
- Mobile device/BYOD guidance.
- Telework/remote access.
- Incident response, including cyber incidents and procedures to report lost or stolen equipment.
The following are several tools small businesses can use to improve their cybersecurity status:

Center for Internet Security: Contains a small subset of the CIS Controls specifically selected to help protect small businesses. [https://www.cisecurity.org/white-papers/cis-controls-sme-guide/](https://www.cisecurity.org/white-papers/cis-controls-sme-guide/)

Cybersecurity Collaborative: Provides webinars on best practices focused on unique security challenges. [https://cyberleadersunite.com/upcoming-webinars/](https://cyberleadersunite.com/upcoming-webinars/)

DHS: The Cybersecurity Resources Road Map is designed to help critical infrastructure small and midsize businesses identify useful cybersecurity resources to meet their needs. [https://www.us-cert.gov/resources/smb](https://www.us-cert.gov/resources/smb)


FCC: The Small Biz Cyber Planner 2.0 is an online resource to help small businesses create customized cybersecurity plans. [https://transition.fcc.gov/cyber/cyberplanner.pdf](https://transition.fcc.gov/cyber/cyberplanner.pdf)


FBI: Contains FBI best practices to protect your computer and employees from Internet fraud. [https://www.fbi.gov/scams-and-safety/on-the-internet](https://www.fbi.gov/scams-and-safety/on-the-internet)

GCA: Contains free tools to inventory and update defenses and authentication; prevent phishing and viruses; defend against ransomware; and protect email. [https://gcatoolkit.org/smallbusiness/](https://gcatoolkit.org/smallbusiness/)
NIST: Provides guidance on how small businesses can provide basic security for their information, networks and systems. [https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf](https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf)


Sharing groups: [https://www.isao.org/information-sharing-groups/](https://www.isao.org/information-sharing-groups/)


---

1. [https://enterprise.verizon.com/resources/reports/dbir/](https://enterprise.verizon.com/resources/reports/dbir/)
The AFCEA Cyber Committee is a volunteer group of public and private sector information technology professionals that oversees AFCEA's outreach and helps ensure open lines of communication between the government and industry. It provides an active focal point within AFCEA for encouraging the exchange of ideas and coordinating AFCEA's cyber-related activities.

The AFCEA Small Business Committee helps shape the association’s small business benefits and provides an active focal point for the coordination of the association’s small business programs. Its purpose is to enhance AFCEA’s outreach to the small business community, grow company memberships and cultivate partnerships among government, industry and academic leaders, investing time and resources for such endeavors.