AFCEA Paper
Small Business Cyber Security

Introduction

According to Verizon's 2019 Data Breach Investigations Report[1], 43% of reported breaches affected small businesses. There are over 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 last 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 Department of Defense (DoD) and some Federal agencies have strong information security policies that must be complied with by their contractors, other government agencies may not have such policies.

The fundamental problem is two-fold: 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 business 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 businesses offering opportunities that the small business cannot, leaving small businesses to start the training process over again.

The purpose of this paper is to provide 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.

Security Issues Faced by Small Businesses

Some small businesses struggle with cybersecurity because they cannot afford an expensive solution, have limited time to devote to it or they simply just do not know where to start. A "small business" in the context of this paper is an organization defined by North American Industry Classification System (NAICS)[2] codes that stipulate revenue ceilings or employee numbers. Small business employee numbers are different in every case, but more importantly most have a small or non-existent security team. Small businesses are structured to be efficient in delivering their products or services to the government customer and place the majority of their labor in direct support to the customer and minimize the overhead staff. As such, there may be one to five employees who handle general IT services like the management of hardware and software that support business needs, or the contracting for external IT

[1] https://enterprise.verizon.com/resources/reports/dbir/

[2] https://www.census.gov/eos/www/naics/ and https://www.sba.gov/federal-contracting/contracting-guide/size-standards

services. 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 (keys, locks, badges, etc.) Human security (health, safety, identity theft, etc.) is unfortunately not a major focus for most small businesses.

Relying on a single security person to protect a company, or a fractional person 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 breach resulting in the theft of intellectual property such as employee or customer data, or other sensitive corporate information
- Ransomware that encrypts sensitive data then demands a payment for decryption
- 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 the business out of business virtually overnight. Some small businesses have Employee Errors and Omissions (EEO) 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 limited to just 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 DoD this will change with the requirement to comply with the Cybersecurity Maturity Model Certification (CMMC) process[3]. This is an effort by DoD 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 Challenges of Keeping a Small Business Secure

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 are also 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 (routers, WiFi gateways, servers, security event monitoring, etc.) requires specialized skills and training. Some infrastructure devices can automatically detect and repair problems, but most require human control for proper operation.

[3] https://www.acq.osd.mil/cmmc/

A small business with an in-house enterprise IT staff may typically devote less than 5% 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 can also assist in-house staff who are working towards 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 (AWS) 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 business will retain a small internal IT staff for essential functions such as troubleshooting Microsoft Office applications, configuring new computers, replacing printer toner, etc. 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 phishing email or a tech support phone scam call? 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 or have to monitor heat, humidity or water on the floor.

Best Security Practices for Small Business

All businesses, whether they have a full in-house IT and security team or if 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 (people, process and tools)
- Know what IT resources are owned or used by the business; know what is in-sourced and what is out-sourced
- Ensure that all employees understand the need for protecting information systems, that they understand their individual role with respect to security, and 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 your 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 (cameras, voice-activated assistants, smart appliances, etc.) from enterprise systems – put them on a different physical LAN or different 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 cyber security crisis
- Don't forget about physical security

Recommended Initial First Steps

Often a small business with no security expertise on its staff struggles with the "where do I start?" problem. A business that has been in operation for more than a year has most likely developed a basic cyber security 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 your security plan. The Small Business Administration offers a wealth of information for small business owners here: https://www.sba.gov/business-guide/manage-your-business/small-business-cybersecurity

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

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

As noted earlier, small and large businesses supporting the DoD will need to comply with CMMC and according to DoD CISO, Katie Arrington, most are required to comply at level 1.[4] There are five maturity levels ranging from basic hygiene to advanced. 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. The "level" of security a business has is expected to be a consideration during the acquisition process in the future. There are 17 security controls for Level 1 CMMC. Consider approaching CMMC in a step by step process by addressing level 1 first and then move on to 2 and 3. Most of level 1 are non-technical and only require changes or updates to corporate policies.

Businesses that don't have a roadmap from a supported agency to follow should consider doing the following:

Step 1 – Inventories. Any business, whether new or old, cannot have a working security program if the business does not know what assets or resources it owns. So, the first step in any cyber security plan is to inventory the business' 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' 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 – Configuration Management. Secure configuration of the assets identified in Step 1 comes next. Out of the box, most systems come from the manufacturer with default usernames, passwords, and configurations. This means that unnecessary software features may be turned on, that passwords are weak or guessable, or that remote access capabilities are enabled. There are numerous guides for securely configuring various products and some of them can be found in the resources section below. This mindset applies to cloud services just as much as physical systems. Before putting sensitive company data "into the cloud" ensure that your 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 Work Environment. Control physical access to your equipment. Today's work environment is no longer just the office, but 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.

[4] https://www.meritalk.com/articles/cmmc-aims-for-global-standard-in-cybersecurity-arrington-says/

Step 4 – Secure Employees. Probably the most overlooked initial step for any small business is education and awareness training for employees, staff, and anybody 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.

Build and execute an employee training program that aligns with your business needs by:

- Training and certifying your IT workforce in areas needed by your customers and the business
- Provide a career progression for these employees
- Pay them market price for what they know and the responsibilities they perform
- Each of these items will assist with retention (more of a comment than bullet point).

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 thing 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 being written, 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. Ensure to 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 included in the Employee Handbook.

- Acceptable Use of Information Technology containing guidelines for the use of computers, telephones, internet, email, voicemail
- Information Security: Guidelines for passwords. Levels of access to the network, virus protection, confidentiality and use of data
- Security Awareness: Training that employees must complete
- Physical Security
- Technology Standards: security baseline for company-owned PCs/mobile devices and what is prohibited, i.e. use of peer to peer software, pornography, etc.
- Continuity of Operations and Disaster Recovery to include data backup methods
- Media destruction
- Mobile Device/BYOD guidance
- Telework/Remote Access
- Incident response to include cyber incidents and procedures to report lost or stolen equipment

Contributors

Marc Sachs (primary), Hee Ahn, Dr. Tony Barber, Claire Cuccio, Tom DeWitt, Noel Henry, Les Owens, Steve Shirley, and Tan Wilson

Resources

Center for Internet Security: Contains a small sub-set of the CIS Controls specifically selected to help protect small businesses. 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/

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

DoD: Information on CMMC. https://www.acq.osd.mil/cmmc/

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

FCC: Tips on selecting a cyber insurance policy. https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/cyber-insurance

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

GCA: Contains free tools to inventory, update defenses, authentication, prevent phishing and viruses, defend against ransomware, and protect your email. 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

SANS Security Awareness: Requires a subscription. Provides a toolkit and security resources. https://www.sans.org/security-awareness-training/resources/security-awareness-planning-toolkit

SBA: Contains best practices. https://www.sba.gov/business-guide/manage-your-business/small-business-cybersecurity

Sharing groups: https://www.isao.org/information-sharing-groups/

Vendor presentation:

https://www.checkpoint.com/downloads/products/small-business-top-10-security-best-practices.pdf