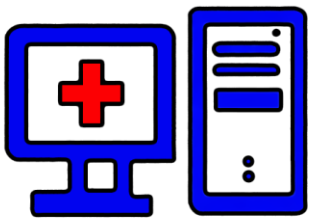


SNECS, LLC

A Guide to Cyber Security

601 Great Rd.
North Smithfield RI 02896

p. 401-762-0660
w. snecsllc.com

39 Greenville Ave.
Johnston RI 02919

Table of Contents

Description of SNECS, LLC.

SNECS, LLC has been in business since May, 2002. We offer fast, reliable and affordable IT services to businesses in Southern New England. With multiple locations, emergency contact numbers and dedicated departments for business needs, we are able to respond and resolve many issues with ease. We offer in-store, on-site and remote service for all of our clients.

Locations

North Smithfield (Headquarters): 601 Great Rd. North Smithfield, RI 02896

Johnston: 39 Greenville Ave. Johnston, RI 02919

Hours of Operation

North Smithfield:	Johnston:
Monday – Friday: 9am – 6pm	**Monday – Friday: 9am – 6pm**
Saturday: 10am – 5pm	**Saturday: 9am – 5pm**
Sunday: Closed	**Sunday: Closed**

Products and Services

The following are just a few services we offer. We offer many additional services that are not listed. If you are interested in a service that is not listed, please contact our business department for further information.

- Flat Rate Managed IT Services
- Sales and Service of IT Equipment including Servers, Workstations, Printers and Networking Equipment
- 24/7 OS Updates and Patch Maintenance
- Anti-Virus
- Local and Offsite Backups
- Virus and Malware Removal
- Software and Hardware installation

Contact Information

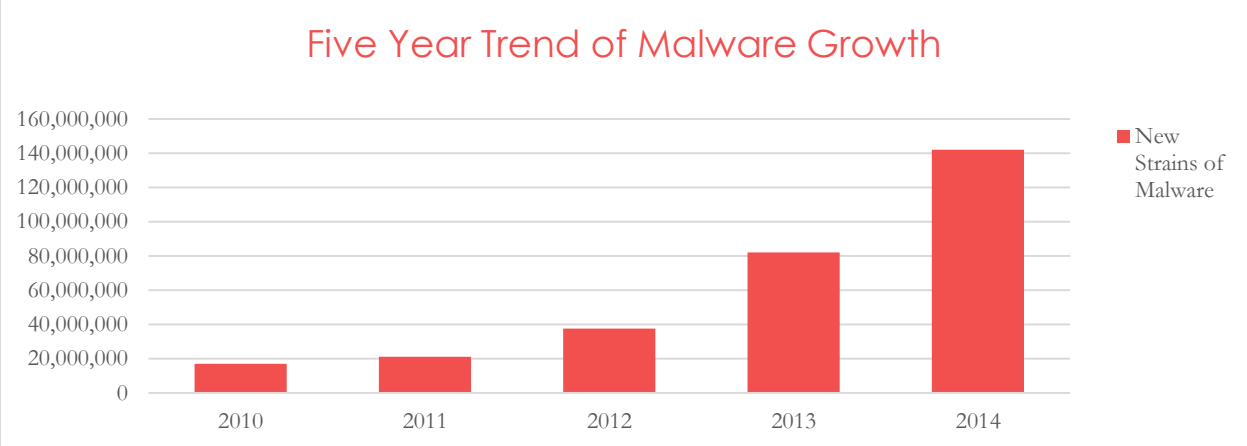
If you are have a question or issue regarding your business's IT, please contact us via email or phone support.

- Email: support@filetobackup.com
- Phone: 401-522-5200

You may also contact your account manager directly via email or extension. Please refer to your onboarding packet for additional contact information.

Cyber Security Summary

All companies should develop and maintain clear and robust policies for safeguarding critical business data and sensitive information, protecting their reputation and discouraging inappropriate behavior by employees. Many new viruses and types of malware are developed daily. With this rising trend, we exercise more of a proactive approach to external dangers like viruses and network intrusion attacks. You may already have other policies in place for procedures specific to your business. We encourage you to incorporate this guide into your business plan for Cyber Security. In the following outline, many topics will be covered as well as general best practice guidelines for the IT security of your business.



Highlights

In the following sections we will cover topics such as Privacy and Data Security, Scams and Fraud, Network & Website Security, Email, Mobile Devices, Employees, Facility and Operational Security, Payment Cards, Incident Response and Reporting, and Policy Development & Management.

Objectives

Our main objective is to inform and educate you and your employees on Cyber Security. Our long term goal is to keep your business safe from the rising trend of malicious attacks.

Mission Statement

Our mission is to provide you with the best security and preventive maintenance around. We will incorporate many avenues of protection including anti-virus, security firewalls/routers, backups and best practice guidelines to follow.

Keys to Success

By working together, we strive to keep your business running without downtime caused by viruses and network intrusions. Since many people rely on the internet for their daily routine, we hope to encourage you and your employees to practice safe Cyber Security habits in day-to-day situations.

Privacy and Data Security

Establish Security Roles and Responsibilities

Clearly identify company data ownership and employee roles for security oversight and their inherit privileges, including:

- Necessary roles, and the privileges and constraints accorded to those roles.
- The types of employees who should be allowed to assume the various roles.
- How long an employee may hold a role before access rights must be reviewed.
- If employees may hold multiple roles, the circumstances defining when to adopt one role over another.

Depending on the types of data regularly handled by your business, it may also make sense to create separate policies governing who is responsible for certain types of data.

Establish an Employee Internet Usage Policy

The limits on employee Internet usage in the workplace vary widely from business to business. Your guidelines should allow employees the maximum degree of freedom they require to be productive. Rules of behavior are necessary to ensure that all employees are aware of boundaries, both to keep them safe and to keep your company successful.

- Personal breaks to surf the web should be limited to a reasonable amount of time and to certain types of activities.
- If you use a web filtering system, employees should have clear knowledge of how and why their web activities will be monitored, and what types of sites are deemed unacceptable by your policy.
- Workplace rules of behavior should be clear, concise and easy to follow. Businesses may want to include an Internet usage policy during initial hiring so that all new employees are aware of this policy.

Establish a Social Media Policy

Social networking applications present a number of risks that are difficult to address using technical or procedural solutions. A strong social media policy is crucial for any business that seeks to use social networking to promote its activities and communicate with its customers. At a minimum, a social media policy should clearly include the following:

- Specific guidance on when to disclose company activities using social media, and what kinds of details can be discussed in a public forum.
- Additional rules of behavior for employees using personal social networking accounts to make clear what kinds of discussion topics or posts could cause risk for the company.
- Guidance on the acceptability of using a company email address to register for, or get notices from, social media sites.
- Guidance on selecting long and strong passwords for social networking accounts, since very few social media sites enforce strong authentication policies for users.

Identify Potential Reputation Risks

All organizations should take the time to identify potential risks to their reputation and develop a strategy to mitigate those risks via policies or other measures as available. Specific types of reputation risks include:

- Being impersonated online by a criminal organization (e.g., an illegitimate website spoofing your business name and copying your site design, then attempting to defraud potential customers via phishing scams).
- Having sensitive company or customer information leaked to the public via the web.
- Having sensitive or inappropriate employee actions made public via the web or social media sites.

All businesses should set a policy for managing these types of risks and plans to address such incidents if and when they occur. Such a policy should cover a regular process for identifying potential risks to the company's reputation in cyberspace, practical measures to prevent those risks from materializing and reference plans to respond and recover from potential incidents as soon as they occur.

Scams and Fraud

Steps to Prevent Becoming a Victim

New telecommunication technologies may offer countless opportunities for small businesses, but they also offer cyber criminals many new ways to victimize your business, scam your customers and hurt your reputation. Businesses of all sizes should be aware of the most common scams perpetrated online.

Train Employees to Recognize Social Engineering

Many criminals use social engineering tactics to get individuals to voluntarily install malicious computer software such as fake antivirus, thinking they are doing something that will help make them more secure. Users who are tricked into loading malicious programs on their computers may be providing remote control capabilities to an attacker, unwittingly installing software that can steal financial information or simply try to sell them fake security software.

Protect Against Online Fraud

Be sure to never request personal information or account details through email, social networking or other online messages. Let your customers know you will never request this kind of information through such channels and instruct them to contact you directly should they have any concerns.

Protect Against Phishing

Employee awareness is your best defense against your users being tricked into handing over their usernames and passwords to cyber criminals. Explain to everyone that they should never respond to incoming messages requesting private information. Also, to avoid being led to a fake site, they should know to never click on a link sent by email from an untrustworthy source. Employees needing to access a website link sent from a questionable source should open an Internet browser window and manually type in the site's web address to make sure the emailed link is not maliciously redirecting to a dangerous site. This advice is especially critical for protecting online banking accounts belonging to your organization. Criminals are targeting small business banking accounts more than any other sector.

Don't Fall for Fake Anti-Virus Offers

Fake antivirus, "scareware" and other rogue online security scams have been behind some of the most successful online frauds in recent times. If your computer becomes infected with a virus, shut down the infected machine and call us immediately.

Develop a Layered Approach to Guard Against Malicious Software

Combining the use of web filtering, antivirus signature protection, proactive malware protection, firewalls, strong security policies and employee training significantly lowers the risk of infection. Keeping protection software up to date along with your operating system and applications increases the safety of your systems.

Verify the Identity of Information Seekers

Most offline social engineering occurs over the telephone. Information gathered through social networks and information posted on websites can be enough to create a convincing ruse to trick your employees. Ensure that you train employees to never disclose customer information, usernames, passwords or other sensitive details to incoming callers. When someone requests information, always contact the person back using a known phone number or email account to verify the identity and validity of the individual and their requests.

Network Security

Secure Internal Network and Cloud Services

Your company's network should be separated from the public Internet by strong user authentication mechanisms and policy enforcement systems such as firewalls and web filtering proxies. Additional monitoring and security solutions, such as anti-virus software and intrusion detection systems, should also be employed to identify and stop malicious code or unauthorized access attempts.

Internal networks should be evaluated to determine what types of security controls are necessary and how they can be best deployed. Border routers should be configured to only route traffic to and from your company's public IP addresses, firewalls should be deployed to restrict traffic only to and from the minimum set of necessary services, and intrusion prevention systems should be configured to monitor for suspicious activity crossing your network perimeter. In order to prevent bottlenecks, all security systems you deploy to your company's network perimeter should be capable of handling the bandwidth that your carrier provides.

Cloud based services should ensure that your company's information and activities are protected with the same degree of security you would intend to provide on your own. Request security and auditing from your cloud service providers as applicable to your company's needs and concerns. Review and understand service level agreements, or SLAs, for system restoration and reconstitution time.

Develop Strong Password Policies

Generally speaking, two-factor authentication methods, which require two types of evidence that you are who you claim to be, are safer than using just static passwords for authentication. One common example is a personal security token that displays changing passcodes to be used in conjunction with an established password. However, two-factor systems may not always be possible or practical for your company. Password policies should encourage your employees to employ the strongest passwords possible without creating the need or temptation to reuse passwords or write them down. That means passwords that are random, complex and long (at least 10 characters), that are changed regularly, and that are closely guarded by those who know them.

Secure and Segregate Your Wi-Fi

Your company may choose to operate a Wireless Local Area Network (WLAN) for the use of customers, guests and visitors. If so, it is important that such a WLAN be kept separate from the main company network so that traffic from the public network cannot traverse the company's internal systems at any point.

Encrypt Sensitive Company Data

Encryption should be employed to protect any data that your company considers sensitive, in addition to meeting applicable regulatory requirements on information safeguarding. Different encryption schemes are appropriate under different circumstances. If you choose to offer secure transactions via your company's website, consult with your service provider about available options for an SSL certificate for your site.

Set Safe Web Browsing Rules

Your company's internal network should only be able to access those services and resources on the Internet that are essential to the business and the needs of your employees. Use the safe browsing features included with modern web browsing software to ensure that malicious or unauthorized sites cannot be accessed from your internal network.

Website Security

Website security is more important than ever. Web servers, which host the data and other content available to your customers on the Internet, are often the most targeted and attacked components of a company's network. Cyber criminals are constantly looking for improperly secured websites to attack, while many customers say website security is a top consideration when they choose to shop online. As a result, it is essential to secure servers and the network infrastructure that supports them. The consequences of a security breach are great: loss of revenues, damage to credibility, legal liability and loss of customer trust. The following are examples of specific security threats to web servers:

- Cyber criminals may exploit software bugs in the web server, underlying operating system, or active content to gain unauthorized access to the web server. Examples of unauthorized access include gaining access to files or folders that were not meant to be publicly accessible and being able to execute commands and/or install malicious software on the web server.
- Denial-of-service attacks may be directed at the web server or its supporting network infrastructure to prevent or hinder your website users from making use of its services.
- Sensitive information on the web server may be read or modified without authorization.
- Sensitive information on backend databases that are used to support interactive elements of a web application may be compromised through the injection of unauthorized software commands. Examples include Structured Query Language (SQL) injection, Lightweight Directory Access Protocol (LDAP) injection and cross-site scripting (XSS).
- Sensitive unencrypted information transmitted between the web server and the browser may be intercepted.
- Information on the web server may be changed for malicious purposes. Website defacement is a commonly reported example of this threat.
- Cyber criminals may gain unauthorized access to resources elsewhere in the organization's network via a successful attack on the web server.
- Cyber criminals may also attack external entities after compromising a web server. These attacks can be launched directly (e.g., from the compromised server against an external server) or indirectly (e.g., placing malicious content on the compromised web server that attempts to exploit vulnerabilities in the web browsers of users visiting the site).
- The server may be used as a distribution point for attack tools, pornography or illegally copied software.

Because of the network traffic and high liability your business could be held accountable for due to improper Website Security, we strongly recommend having a third party host and maintain your website(s). Please contact your website host for any additional information regarding their security practices. If you currently host your website in-house, we urge you to have a third party take over the hosting and upkeep of the website. Many webhosts are available and are relatively cheap for the amount of time saved in maintaining your own website security.

If you are interested in switching to a third party host, we recommend ProProducts Web Design. They are located in Smithfield, RI and their website is www.proproductswebdesign.com. They offer many services including web design, web hosting, e-Commerce, and so much more. Additional contact information can be found at the end of this guide.

Email Security

Email has become a critical part of our everyday business, from internal management to direct customer support. The benefits associated with email as a primary business tool far outweigh the negatives. However, businesses must be mindful that a successful email platform starts with basic principles of email security to ensure the privacy and protection of customer and business information.

Setup a Spam Filter

It has been well documented that spam, phishing attempts and otherwise unsolicited and unwelcome email often accounts for more than 60 percent of all email that an individual or business receives. Email is the primary method for spreading viruses and malware and it is one of the easiest to defend against. Consider using email-filtering services that your email service, hosting provider or other cloud providers offer. Ensure that filters are reviewed regularly so that important email and/or domains are not blocked in error.

Train Your Employees in Responsible Email Usage

The last line of defense for all of your cyber risk efforts lies with the employees who use tools such as email and their responsible and appropriate use and management of the information under their control. Technology alone cannot make a business secure. Employees must be trained to identify risks associated with email use, how and when to use email appropriate to their work, and when to seek assistance of professionals. Employee awareness training is available in many forms, including printed media, videos and online training.

Protect Sensitive Information Sent via Email

Since email in its native form is not designed to be secure, incidents of misaddressing or other common accidental forwarding can lead to data leakage. Businesses that handle this type of information should consider whether such information should be sent via email. Never send credit card information, social security numbers or other information that may lead to a data breach or identity theft.

Set a Sensible Email Retention Policy

Many industries have specific rules that dictate how long emails can or should be retained, but the basic rule of thumb is only as long as it supports your business efforts. Many companies implement a 60-90 day retention standard if not compelled by law to another retention period. To ensure compliance, companies should consider mandatory archiving at a chosen retention cycle end date and automatic permanent email removal after another set point, such as 180-360 days in archives. In addition, organizations should discourage the use of personal folders on employee computers as this will make it more difficult to manage company standards.

Develop an Email Usage Policy

Your policies should be easy to read, understand, define and enforce. Key areas to address include what the company email system should and should not be used for, and what data are allowed to be transmitted. Other policy areas should address retention, privacy and acceptable use. Depending on your business and jurisdiction, you may have a need for email monitoring. The rights of the business and the user should be documented in the policy as well. The policy should be part of your general end user awareness training and reviewed for updates on a yearly basis.

Mobile Devices

If your company uses mobile devices to conduct company business, such as accessing company email or sensitive data, pay close attention to mobile security and the potential threats that can expose and compromise your overall business networks. This section describes the mobile threat environment and the practices that small businesses can use to help secure devices such as smartphones, tablets and Wi-Fi enabled laptops.

Many organizations are finding that employees are most productive when using mobile devices, and the benefits are too great to ignore. But while mobility can increase workplace productivity, allowing employees to bring their own mobile devices into the enterprise can create significant security and management challenges.

Data loss and data breaches caused by lost or stolen phones create big challenges, as mobile devices are now used to store confidential business information and access the corporate network. It is important to remember that while the individual employee may be liable for a device, the company is still liable for the data.

Top Threats Targeting Mobile Devices

- Data Loss – An employee or hacker accesses sensitive information from device or network. This can be unintentional or malicious, and is considered the biggest threat to mobile devices
- Social Engineering Attacks – A cyber-criminal attempts to trick users to disclose sensitive information or install malware. Methods include phishing and targeted attacks.
- Malware – Malicious software that includes traditional computer viruses, computer worms and Trojan horse programs. Specific examples include the Ikee worm, targeting iOS-based devices; and Pjapps malware that can enroll infected Android devices in a collection of hacker-controlled "zombie" devices known as a "botnet."
- Data Integrity Threats – Attempts to corrupt or modify data in order to disrupt operations of a business for financial gain. These can also occur unintentionally.
- Resource Abuse – Attempts to misuse network, device or identity resources. Examples include sending spam from compromised devices or denial of service attacks using computing resources of compromised devices.
- Web and Network-based Attacks – Launched by malicious websites or compromised legitimate sites, these target a device's browser and attempt to install malware or steal confidential data that flows through it.

Steps to Protect Your Mobile Devices

- Use Security Software on All Smartphones - It can detect and remove viruses and other mobile threats before they cause you problems. It can also eliminate annoying text and multimedia spam messages.
- Make Sure All Software is Up-to-Date - Mobile devices must be treated like personal computers in that all software on the devices should be kept current, especially the security software.
- Encrypt the Data on Mobile Devices - If a device is lost and the SIM card stolen, the thief will not be able to access the data if the proper encryption technology is loaded on the device.
- Have Users Password Protect Access to Mobile Devices - It is important to use strong passwords and lock screen patterns to protect data stored on mobile devices.
- Urge Users to be Aware of Their Surroundings - Whether entering passwords or viewing sensitive or confidential data, users should be cautious of who might be looking over their shoulder.
- Apply Safe Procedure Strategies for PCs to Mobile Devices - Email, Texting and Social Networking on Mobile Devices should be treated the same as if it was on a stationary PC. This includes avoid opening unexpected text messages from unknown senders, don't be lured in by spammers and phishers and to "click with caution".
- Set Reporting Procedure for Lost or Stolen Equipment - Processes to deactivate the device and protect its information from intrusion should be in place. We also offer the automation of such processes, allowing small businesses to breathe easier after such incidents.
- Ensure All Devices are Wiped Clean Prior to Disposal – Perform a Factory Reset and destroy the SIM card.

Employees

Businesses must establish formal recruitment and employment processes to control and preserve the quality of their employees. Many employers have learned the hard way that hiring someone with a criminal record, falsified credentials or undesirable background can create a legal and financial nightmare. Without exercising due diligence in hiring, employers run the risk of making unwise hiring choices that can lead to workplace violence, theft, embezzlement, lawsuits for negligent hiring and numerous other workplace problems.

Develop a Hiring Process that Properly Vets Candidates

The hiring process should be a collaborative effort among different groups of your organization, including recruitment, human resources, security, legal and management teams. It is important to have a solid application, resume, interview and reference-checking process to identify potential gaps and issues that may appear in a background check.

Perform Background Checks and Credentialing

Background checks are essential and must be consistent. Using a background screening company is highly recommended. The standard background screening should include the following checks:

- Employment verification
- Education verification
- Criminal records
- Drug testing
- The U.S. Treasury Office of Foreign Affairs and Control
- Sex offender registries
- Social Security traces and validation

For professional background checks, we use and recommend Hire Image, a local RI company that does nationwide and international screenings. Visit their website at www.hireimage.com. Additional contact information can be found at the end of this guide.

Set Appropriate Access Controls for Employees

Both client data and internal company data are considered confidential and need particular care when viewed, stored, used, transmitted or disposed. It is important to analyze the role of each employee and set data access control based upon the role. If the organization does not have a system in place to control data access, the following precautions are strongly recommended. Every employee should:

- Never access or view client data without a valid business reason. Access should be on a need-to-know basis.
- Never provide confidential data to anyone – client representatives, business partners or even other employees – unless you are sure of the identity and authority of that person.
- Never use client data for development, testing, training presentations or any purpose other than providing production service, client-specific testing or production diagnostics. Only properly sanitized data that cannot be traced to a client, client employee, customer or your organization's employee should be used for such purposes.
- Always use secure transmission methods such as secure email, secure file transfer (from application to application) and encrypted electronic media (e.g., CDs, USB drives or tapes).
- Always keep confidential data (hard copy and electronic) only as long as it is needed.
- Follow a "clean desk" policy, keeping workspaces uncluttered and securing sensitive documents so that confidential information does not get into the wrong hands.

- Always use only approved document disposal services or shred all hardcopy documents containing confidential information when finished using them. Similarly, use only approved methods that fully remove all data when disposing of, sending out for repair or preparing to reuse electronic media.

Provide Security Training for Employees

Security awareness training teaches employees to understand system vulnerabilities and threats to business operations that are present when using a computer on a business network.

A strong IT security program must include training IT users on security policy, procedures and techniques, as well as the various management, operational and technical controls necessary and available to keep IT resources secure. In addition, IT infrastructure managers must have the skills necessary to carry out their assigned duties effectively. Failure to give attention to the area of security training puts an enterprise at great risk because security of business resources is as much a human issue as it is a technology issue.

Technology users are the largest audience in any organization and are the single most important group of people who can help to reduce unintentional errors and IT vulnerabilities. Users may include employees, contractors, foreign or domestic guest researchers, other personnel, visitors, guests and other collaborators or associates requiring access. Users must:

- Understand and comply with security policies and procedures.
- Be appropriately trained in the rules of behavior for the systems and applications to which they have access.
- Work with management to meet training needs.
- Keep software and applications updated with security patches.
- Be aware of actions they can take to better protect company information. These actions include: proper password usage, data backup, proper antivirus protection, reporting any suspected incidents or violations of security policy, and following rules established to avoid social engineering attacks and deter the spread of spam or viruses and worms.

A clear categorization of what is considered sensitive data versus non-sensitive data is also needed. Typically, the following data are considered sensitive information that should be handled with precaution:

- Government issued identification numbers (e.g., Social Security numbers, driver's license numbers)
- Financial account information (bank account numbers, credit card numbers)
- Medical records
- Health insurance information
- Salary information
- Passwords

The training should cover security policies for all means of access and transmission methods, including secure databases, email, file transfer, encrypted electronic media and hard copies. Employers should constantly emphasize the critical nature of data security.

Regularly scheduled refresher training courses should be established in order to instill the data security culture of your organization. Additionally, distribute data privacy and security related news articles in your training, and send organization-wide communication on notable data privacy related news as reminders to your employees.

Facility Security

Protecting employees and members of the public who visit your facility is a complex and challenging responsibility. It should also be one of your company's top priorities.

Recognize the Importance of Securing Your Company Facilities

It is easy to think about physical security of your company's facility as merely an exercise in maintaining control of access points and ensuring there is complete visibility in areas that are determined to be of high-risk – either because of the threat of easy public access or because of the value of information located nearby. However, maintaining security of your company's facility also includes the physical environment of public spaces. For instance:

- Employees whose computers have access to sensitive information should not have their computer monitors oriented toward publicly accessible spaces such as reception areas, check-in desks and waiting rooms.
- Employees should be trained to not write out logins and passwords on small pieces of paper affixed to computer equipment viewable in public spaces.
- Easy-to-grab equipment that could contain sensitive or personally identifiable information – such as laptops, electronic tablets and cell phones – should be located away from public areas.
- Consider implementing a badge identification system for all employees, and train employees to stop and question anyone in the operational business area without a badge or who appears to be an unescorted visitor.

Minimize and Safeguard Printed Materials with Sensitive Information

Safeguard copies of material containing sensitive information by providing employees with locking file cabinets or safes. Make it a standard operating procedure to lock up important information. Train employees to understand that leaving the wrong material in view of the general public can result in consequences that impact the company and its customers.

Dispose of Trash Securely

Too often, sensitive information – including customers' personally identifiable information, business financial and other data, and company system access information – is available for anyone to find in the trash. Invest in business grade shredders and buy enough of them to make it convenient for employees. Alternatively, subscribe to a trusted shredding company that will provide locked containers for storage until documents are shredded. Develop standard procedures and employee training programs to ensure that everyone is aware of what types of information need to be shredded.

Dispose of Electronic Equipment Securely

Be aware that emptying the recycle bin on your desktop or deleting documents from folders on your computer or other electronic device may not delete information forever. Disposing of electronic equipment (such as hard drives, CDs and USB drives) requires specialists in order to ensure the security of sensitive information contained within that equipment. We use Big Brothers Big Sisters of the Ocean State to donate our older electronic equipment. You can find them at www.bbbsos.org. As for certified hard drive data destruction, we use Data Medics located in Cranston, RI and on the web at www.data-medics.com. Additional contact information can be found at the end of this guide.

Train your Employees in Facility Security Procedures

A security breach of customer information or a breach of internal company information can result in a public loss of confidence in your company and can be as devastating for your business as a natural disaster. In order to address such risks, you must devote your time, attention and resources to the potential vulnerabilities in your business environment and the procedures and practices that must be a standard part of each employee's workday.

Operational Security

Operational Security, or OPSEC, is the process of denying hackers access to any information about the capabilities or intentions of a business by identifying, controlling and protecting evidence of the planning and execution of activities that are essential the success of operations. OPSEC is a continuous process that consists of five distinct actions:

- Identify information that is critical to your business.
- Analyze the threat to that critical information.
- Analyze the vulnerabilities to your business that would allow a cyber-criminal to access critical information.
- Assess the risk to your business if the vulnerabilities are exploited.
- Apply countermeasures to mitigate the risk factors.

In addition to being a five-step process, OPSEC is also a mindset that all business employees should embrace. By educating oneself on OPSEC risks and methodologies, protecting sensitive information that is critical to the success of your business becomes second nature.

Identity of Critical Information

Given that any business has limited time, personnel and money for developing secure business practices, it is essential to focus those limited resources on protecting information that is most critical to successful business operations. Examples of critical information include, but should not be limited to, the following:

- Customer lists and contact information
- Contracts
- Patents and intellectual property
- Leases and deeds
- Policy manuals
- Articles of incorporation
- Corporate papers
- Laboratory notebooks
- Audio tapes
- Video tapes
- Photographs and slides
- Strategic plans and board meeting minutes

Importantly, what is critical information for one business may not be critical for another. Use your company's mission as a guide for determining what data are truly vital.

Analyze Threats

This action involves research and analysis to identify likely cyber criminals who may attempt to obtain critical information regarding your company's operations. OPSEC planners in your business should answer the following critical information questions:

- Who might be a cyber-criminal (e.g. competitors, politically motivated hackers, etc.)?
- What are cyber criminal's goals?
- What actions might the cyber-criminal take?
- What critical information does the cyber-criminal already have on your company's operations? (i.e., what is already publicly available?)

Analyze Vulnerabilities

The purpose of this action is to identify the vulnerabilities of your business in protecting critical information. It requires examining each aspect of security that seeks to protect your critical information and then comparing those indicators with the threats identified in the previous step. Common vulnerabilities for small businesses include the following:

- Poorly secured mobile devices that have access to critical information.
- Lack of policy on what information and networked equipment can be taken home from work or taken abroad on travel.
- Storage of critical information on personal email accounts or other non-company networks.
- Lack of policy on what business information can be posted to or accessed by social network sites.

Assess Risk

This action has two components. First, OPSEC managers must analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures to mitigate each one. Second, specific OPSEC measures must be selected for execution based upon a risk assessment done by your company's senior leadership. Risk assessment requires comparing the estimated cost associated with implementing each possible OPSEC measure to the potential harmful effects on business operations resulting from the exploitation of a particular vulnerability.

OPSEC measures may entail some cost in time, resources, personnel or interference with normal operations. If the cost to achieve OPSEC protection exceeds the cost of the harm that an intruder could inflict, then the application of the measure may be circumvented. Because the decision not to implement a particular OPSEC measure entails security risks, this step requires your company's leadership approval.

Apply Appropriate OPSEC Measures

In this action, your company's leadership reviews and implements the OPSEC measures selected in the assessment of risk action. Before OPSEC measures can be selected, security objectives and critical information must be known, indicators identified and vulnerabilities assessed.

Payment Cards

If your business accepts payment by credit or debit cards, it is important to have security steps in place to ensure your customer information is safe. You also may have security obligations pursuant to agreements with your bank or payment services processor. These entities can help you prevent fraud.

Understand and Catalog Customer and Card Data Kept

- Make a list of the type of customer and card information you collect and keep – names, addresses, identification information, payment card numbers, magnetic stripe data, bank account details and Social Security numbers. It's not only card numbers criminals want; they're looking for all types of personal information, especially if it helps them commit identity fraud.
- Understand where you keep such information and how it is protected.
- Determine who has access to this data and if they need to have access.

Evaluate Whether You need to Keep All the Data Stored

Once you know what information you collect and store, evaluate whether you really need to keep it. Often businesses may not realize they're logging or otherwise keeping unnecessary data until they conduct an audit. Not keeping sensitive data in storage makes it harder for criminals to steal it. If you've been using card numbers for purposes other than payment transactions, such as a customer loyalty program, ask your merchant processor if you can use alternative data instead. Tokenization, for example, is technology that masks card numbers and replaces it with an alternate number that can't be used for fraud.

Use Secure Tools and Services

The payments industry maintains lists of hardware, software and service providers who have been validated against industry security requirements. Small businesses that use integrated payment systems, in which the card terminal is connected to a larger computer system, can check the list of validated payment applications to make sure any software they employ has been tested. If you have questions, have a conversation about security with your credit merchant provider if the products or services you are currently using are not on the lists.

Control Access to Payment Systems

Whether you use a more complicated payment system or a simple standalone terminal, make sure you carefully control access. Isolate payment systems from other, less secure programs, especially those connected to the Internet. For example, don't use the same computer to process payments and surf the Internet. Control or limit access to payment systems to only employees who need access. Make sure you use a secure system for remote access or eliminate remote access if you don't need it so that criminals cannot infiltrate your system from the Internet.

Use Security Tools and Resources

Work with your bank or processor and ask about the anti-fraud measures, tools and services you can use to ensure criminals cannot use stolen card information at your business. For e-commerce retailers, you can verify the customer by having them provide the CVV2 code, billing address or personal password of the payment method being used. For brick and mortar retailers, you can swipe the card, match the card signature to receipt and use a dedicated payment terminal.

Remember the Security Basics

When using your terminal, use strong, unique passwords and change them frequently, use an up-to-date firewall and anti-virus and do not click on suspicious links you may receive by email or encounter online.

Incident Response and Reporting

Even well-implemented cyber security structures and plans may not prevent all breaches of your business' data defenses, so be sure to have procedures in place to respond to security breaches when they occur.

Types of Breaches

Physical breaches include real-world crimes such as burglaries and equipment theft, as well as any event when your company's equipment is misplaced or lost in transit. Unauthorized devices may be installed on a system or network, permitting further compromises of data confidentiality and integrity. Physical breaches can also result from reselling, donating or recycling old equipment that has not been properly cleansed of potentially sensitive information.

Network and system security breaches include events when computers become infected with malicious code, are accessed by unauthorized individuals remotely or are used by authorized individuals to perform malicious activity. This can also include breaches to network routers and firewalls, both within and outside your organization's boundary and control.

Data breaches, meaning the leakage or spillage of sensitive information into insecure channels, can result from any of the types of events described above. Data breaches can also occur if sensitive information is left improperly exposed by mistake.

Steps to Take if a Breach Occurs

- Work cohesively across technical and leadership teams to limit the damage - Once your company becomes aware that a breach has occurred, technical personnel and business decision makers should work together to decide on the most practical and effective containment plan. Containment plans will vary from one set of circumstances to the next, and they may quickly become intensive in terms of time and resources from both the technological and business impact perspectives
- Begin Recovery Effort - After a containment plan has been established and execution has begun, get started on eradication and recovery efforts. In the case of network and system security breaches, eradication usually means removing all instances of unauthorized software from the network and disabling all access privileges associated with users who have committed malicious activity. Cleaning a network or system of all traces of malicious code can often entail having to completely wipe all storage media and perform a "clean install." Therefore, recovery from such a breach may be resource intensive and require careful restoration of data from backups. Bear in mind that backups may also contain malicious code and should be carefully checked for compromise; otherwise, the security breach will be perpetuated after the recovery phase.

Key Disaster Recovery Principles

- Don't wait until it's too late – Small businesses should not wait until after a disaster to think about what should have been done to protect their data. Not only is downtime costly from a financial perspective, but it could mean the complete demise of the business. Small businesses should map out disaster preparedness plans ahead of time, including the identification of key systems, data and other resources that are critical to running the business.
- Protect information completely – To reduce the risk of losing critical business information, small businesses must implement the appropriate security and backup solutions to archive important files, such as customer records and financial information for the long term. Natural disasters, theft and cyber-attacks can all result in data and financial loss, so small businesses need to make sure important files are saved not only on an external hard drive and/or company network, but in a safe, off-site location.
- Get employees involved – Employees play a key role in helping to prevent downtime. They should be educated on computer security best practices and what to do if information is accidentally deleted or cannot easily be

found in their files. Since small businesses often have limited resources, all employees should know how to retrieve the businesses' information in times of disaster.

- Test frequently – After a disaster hits is the worst time to learn that critical files were not backed up as planned. Regular disaster recovery testing is invaluable. Test your plan anytime anything changes in your environment.
- Review your plan – If frequent testing is not feasible due to resources and bandwidth, small businesses should at least review disaster preparedness plan on a quarterly basis.
- Be prepared – It is always better and less costly to invest in adequate security up-front rather than going through a costly incident response which could result in rebuilding your entire network infrastructure.

Hold a "Lessons Learned" Meeting

Lastly, your company should always perform a "lessons learned" meeting after the recovery phase has been successfully completed to discover, document and refine the knowledge gained during the incident handling process.

Policy Development and Management

All companies should develop and maintain clear and robust policies for safeguarding critical business data and sensitive information, protecting their reputation and discouraging inappropriate behavior by employees. As with any other business document, cyber security policies should follow good design and governance practices -- not so long that they become unusable, not so vague that they become meaningless, and reviewed on a regular basis to ensure that they stay pertinent as your business needs change.

The best thing a business can do is create and enforce an Acceptable Users Policy (AUP). An AUP is a written document stating exactly what your employees can and cannot do with company Internet access, computers, and e-mail. As we touched upon these topics earlier, it is time for them to come together into a coherent and understandable document that will be easily available for your employees.

An AUP should also educate your employees on the appropriate use of your company's resources. If you don't want your employees to download pornographic material and send racist jokes with a company e-mail account, you have to communicate this information to them in an acceptable user's policy and have them acknowledge in writing that they have read and understood it. There are countless stories of companies being sued for sexual harassment because one employee walked by another employee's desk and saw something offensive on their computer screen. Creating an acceptable user's policy not only ensures your employees know what behavior is acceptable, but it will also help in the prevention of spyware and malware. For example, employees should not be allowed to download programs, screen savers, pictures, music files, or access file sharing networks (like peer-to-peer file sharing sites). This will save precious bandwidth and prevent them from downloading files and programs that contain viruses and spyware. We suggest an overview during their initial introduction to the company as a new employee and a yearly meeting to serve as a refresher course to all employees.

We strongly suggest incorporating additional policies based on the type of business you have (such as a "Clean Desk Policy" for healthcare providers or a "Password Construction/Protection Policy" for those who access sensitive data located online). Many policy templates are available online at http://www.sans.org/security-resources/policies and can be customized for your business needs. Using this guide as a tool, you can create your own policies and guidelines with ease.

Reference Information

We sincerely hope you have enjoyed this guide on Cyber Security. We encourage you will incorporate all of the knowledge we shared here into your own Cyber Security policy for your business.

SNECS Recommended and Trusted Companies

Web Hosting:

ProProducts Web Design
9 Thurber Blvd. Smithfield RI 02917
1-401-231-PPWD (7793)
http://www.proproductswebdesign.com/

Background Checks:

Hire Image, LLC.
6 Alcazar Ave. Johnston RI 02919
1-888-720- HIRE (4473)
http://www.hireimage.com/

Donation of Old I.T. Equipment:

Big Brothers Big Sisters of the Ocean State
1540 Pontiac Ave. Cranston RI 02920
1-401-921-2434
www.bbbsos.org

Hard Drive Data Destruction (or Recovery) and Disposal:

Data Medics
1215 Reservoir Ave. Cranston RI 02920
1-844-4-MY-DATA (1-844-469-3282)
www.data-medics.com

Sample Templates and Workplace Materials

Informational and Security Policy Templates: http://www.sans.org/security-resources/policies

Distributable Materials for Cyber Security: https://www.us-cert.gov/publications/distributable-materials

Social Networking: https://www.us-cert.gov/sites/default/files/publications/safe_social_networking.pdf