INFORMATION TECHNOLOGY SECURITY

Purpose: Organizations (and individuals) should assess and minimize their technology risk profile, which includes developing a security plan. Given limited resources, the most challenging part is getting started, especially when an organization lacks someone with a strong Information Technology (IT) background. Below is an overview of some security considerations as well as practical steps for developing a basic security plan. This is not intended to be an exhaustive list of security measure, but should provide starting points and structure to discussions regarding security.

1. **What to Secure:** For most individuals and organizations, two main things need to be secured:
   a. Data: protect data an organization collects from unauthorized access by employees and others.
   b. Devices: protect computers, phones, etc. from unauthorized logical (hacking) and physical access.

2. **Risk Assessment:** To begin assessing risk, organizations need to know what type of data they are collecting and why. If an organization is collecting private and/or sensitive data – personally identifiable information (PII), payment card information (PCI), etc. – it is obviously incurring more risk. Reducing that risk requires more security. Optionally, an organization may decide to not collect private information in the first place.

Risk Factors	Risk Level (potential)		
	Low	Moderate	High
Type of Data Collected	Public	Private	PII, PCI, HIPAA
Organization Size	Small	Medium	Large
Staff Turnover	Low	Moderate	High
Access Policy (as-needed basis, tracked)	Yes	Yes	No
Security Staff (even part-time role)	Yes	Yes	No
Security Budget (funding and time)	Yes	Yes	No

While much focus is on data security, device security should not be ignored. As a starting point, organizations should inventory devices and users with access to each device. If a device is compromised, keystroke loggers or other malware could be installed and put individual and organizational accounts and data at risk. A thief may be able to access any data stored on a stolen device, and even online accounts if a person had passwords stored within applications or browsers.

3. **Security Components:** Security should be implemented at both technical and non-technical levels.

Plan Component	Plan Actor	Potential Action(s)
Service Providers (i.e. cloud)	You	Work with reputable vendors. Know what data is stored where.
Network	Consultant	Firewall, VPN. Other steps depending on network.
Device	You, Consultant	Anti-virus. Password protected. Hard drive encryption.
Application	You, Consultant	Approved applications. Frequent updates.
Access	You, Consultant	Limit access appropriately. Track access.
Password	You	Strong. Limited re-use. Change periodically. Password management tools. Multi-factor authentication.
Behavioral	You	Education about phishing, social engineering, etc.

Depending on an organization's work flows, employee skill sets, resources, etc., it may choose to focus on developing different aspects of a security program.

Foundant Technologies, Inc. | P.O. Box 11888 | Bozeman, MT 59719 | toll free 877.297.0043 | direct 406.585.1221

Service Provider: Determining how secure a provider is can be challenging. At a minimum, a reputable provider should be running their services over an SSL connection. They should have other clients with similar or more stringent security requirements, and they should be responsive and transparent about any inquiries regarding security, as well as data ownership. In most cases, organizations want to retain "ownership" of their data.

Network: This more technical component of security may require some consulting to most effectively implement. Best practices for most networks include having a firewall in place and correctly configured. Depending on how the network is accessed, a VPN (virtual private network) may be used to provide additional security during remote access. Protocols such as FTP (file transfer protocol) should not be allowed by default.

Device: At a minimum, devices – including smart phones – should be password-protected. Devices should be running antivirus software configured for automatic updates. If sensitive data will be stored on them, hard drive encryption should be considered. Disabling USB port access, or appropriately securing USB ports, is important to prevent the spread of malware via flash drives. Running a host-based firewall on devices may provide an additional layer of security. Finally, if a device is lost or stolen, it should be possible to remotely disable it.

Application: Applications should be kept up-to-date; unused ones should be uninstalled. Older applications, like Internet Explorer 6, have known security issues that have been widely exploited. In addition, only approved applications should be installed on devices that are used to access an organization's network and accounts.

Access: At a minimum, a list of who (employees, contractors, etc.) has access to what (devices, data, vendor accounts, etc.) should be maintained. In general, access should only be granted on an as-needed basis, and a clear process for handling employee turnover should be in place.

Password / Behavioral: Improving password management is an important step in increasing security. However, even more important is education to increase awareness of risks such as phishing and social engineering. Having the best password policy in place will not help if an employee clicks a link in a malicious email.

Other

Auditing: Having a basic security plan in place is one thing; ensuring it is changing behaviors is another. While full-scale audits can be time and resource intensive, having some kind of periodic review of the implementation of a security plan is important in ensuring long-term success. The extensiveness of an audit may depend on the size of an organization, but even spending a few hours every quarter reviewing a particular employee's devices and access can be a good start.

Disaster Recovery: If security is compromised and data is corrupted or a device is lost or stolen, having an up-to-date backup of important information is critical. There are many backup options available with various features at a variety of price points. Backups should be periodically restored to ensure that they are up-to-date and that the restoration process is functional and well understood.

Summary: Security is an ongoing effort, and plans need to be kept up-to-date to reflect the evolution of various threats and technologies. Auditing and testing of a plan should be done periodically to verify its effectiveness. Start today!

Other Resources:
http://www.sans.org/critical-security-controls – a more technical and in-depth overview of security measures