In this tutorial we will introduce important elements of a small business cyber security plan. These elements include physical, network and data security. In addition to discussing these elements in this tutorial, more detail on each of these security measures can be found in a very approachable document prepared by the Federal Communications Commission or FCC called Cyber Security Planning Guide.

**ELEMENTS OF A CYBERSECURITY PLAN**

**With respect to physical security,** the building and/or the room(s) where computer and network equipment are located should have some level of access control to prevent unauthorized access and use. These measures may include perimeter security such as building alarms, security cameras, and/or badge-controlled access to interior areas requiring control or storage of sensitive operations and/or data.

With respect to network security, there are many actions that one can take to enhance this. Computers and their associated networks should be protected against cyberattacks. Protection strategies may include installation of firewalls for internet connections to prevent outside access to internal data; secure Wi-Fi networks; storage of archived data off-site or in the cloud; a clear policy on mobile device security used for company business; and additional authentication requirements for network operators and administrators. Now if your business is short-staffed in terms of security expertise, it is recommended that you seek outside technical support under a managed security services arrangement. Some of the services commonly provided by a managed service provider or MSP include computer and server support, data backup and disaster recovery, network security, and remote network monitoring. Please remember that important items that are part of the cost of doing business can be included as part of your indirect costs, discussed previously in the accounting course.

**With data security** there are many considerations that should be made. Small businesses have considerable data that are proprietary in nature, such as personnel and payroll information, bank and financial information and in many cases, data regarding larger firms that may be customers or suppliers. “All of this information is often impossible to replace if lost and dangerous in the hands of criminals.” The FCC recommends that you consider the following when developing a data security plan:

**What kind of data do you have in your business?** Your business data may include account records, customer data,
transactions; bank accounts and financial information; intellec-
tual property and sensitive business data such as marketing
plans, product designs; and employee personal information,
such as social security numbers, addresses, payroll and other
personal identifying information.

How are data handled and protected? If your data resides
on a server or computer that is not connected to the internet,
then it is probably secure - that is unless it is on a laptop which
you inadvertently leave in the back of a cab on the way to the
airport. When data move they are exposed to different threats.
Your data may move throughout the company between em-
ployees via your company network, via the internet, via email
and your website, on laptops and cellphones as you and your
employees travel, and over Wi-Fi nets, both secured and unse-
cured. When data moves, it’s vulnerable. Every business should
know what data it has; how it moves and is handled, and have
the appropriate guidelines and polices in place to protect it and
minimize the risk of inadvertent loss or disclosure.

Who has access to company data and under what
circumstances? Not everyone in the company needs access
to everything. As part of the data inventory, access and privi-
leges to that data should be identified. Assigning access rights
is an important step toward securing your data. Establishing
policies and guidelines about how data are handled, validated,
protected and who has access based on its use and where it
goes, are essential steps in data security. Other access protec-
tion considerations may include: (1) use of advance authenti-
cation such as one-time passwords and hardware tokens; (2)
cloud-base authentication platforms; and (3) two-factor au-
thentication that often combine a password with another veri-
fication method for those employees with access to networks
and data.

Employ best practices for financial and banking activities.
Businesses should work with their banks and other financial
institutions to ensure that best practices and up-to-date fraud
prevention tools are being utilized. Other protection strategies to
consider include the following: (1) isolation of business financial
systems from other network systems; and (2) using separate
computers for payment processing and web surfing the internet.
Apart from physical, network, and data security it is important
that every small business establish clear policies and guidelines
for use of computers, protection of data, and employee respon-
sibilities. Topics for consideration include proper use of compa-
y computers and networks; mobile device action plans and
policies; prohibited computing activities; and password and au-
thentication policies. Once the policies are in place this should
be coupled with staff training. The first line of cyber protection is
an adequately trained staff that is well versed and knowled-
geable in security principles. It is recommended that companies
establish basic security practices, policies and training for em-
ployees regarding password protection requirements; mobile
device use; protection of company and client data; and penal-
ties for violation of company cybersecurity guidelines.

An additional form of protection that some companies
implement to mitigate the impacts of a possible cyberattack is
the purchase of cybersecurity insurance. PwC reports that the
global cyberinsurance market will grow to $7.5 billion in annual
sales by 2020, up from $2.5 billion in 2015. Cyberinsurance can
cover: (1) data destruction, denial of service attacks; (2) theft
and extortion; (3) incident response and remediation, (4) crisis
management; and many other risks associated with cybertheft
of company information.

In closing, it is recommended that you review what you are
doing now within your firm to protect your network and data.
If you find that your plan has gaps - consider implementing the
risk based Cybersecurity Framework developed by the Na-
tional Institute of Standards and Technology, most commonly
known as NIST. This Framework enables organizations – re-
gardless of size, degree of cybersecurity risk, or cybersecurity
sophistication – to apply the principles and best practices of
risk management to improve the security and resilience of
critical infrastructure. The Framework assembles standards,
guidelines, and practices that are working effectively in indus-
try today such as those developed by NIST and the Interna-
tional Standardization Organization (ISO). The framework pro-
motes five core functions: Identify, Detect, Protect, Respond,
and Recover.
The NIST Framework will help an organization to better understand, manage, and reduce its cybersecurity risks and can assist organizations determine which activities are most important to maintain critical business operations and service delivery, while providing a common language to address cybersecurity risk management.

ENDNOTES


