SECURITY IN A SMALL COMPANY

CASE STUDY

CATE DILLON, DEV DEVENDRA, BENJAMIN YANKSON, MOAZ AL BADAWI

AGENDA

- Definition of a Small Business
- Security Challenges of a Small Business
- Case Study – Introduction
- Case Study – Existing Security Measures
- Recommended Security Measures
- Closing Review

DEFINITION OF A SMALL BUSINESS

As per Industry Canada –

"A business being carried on in Canada for gain or profit, with estimated gross annual revenue of not more than $5 million. It does not include the business of farming or a business having its principal object, the furtherance of a charitable or religious purpose."

As per Statistics Canada - it is a business with $30,000 to $5 million of annual revenue and less than 500 employees

SECURITY CHALLENGES OF SMALL BUSINESS

Q. What are the top five challenges of a small business

A. As per the white paper by Cisco Systems, “Top Five Security Challenges of Small and Medium Sized Businesses” –

i. Worms and Viruses
ii. Information Theft
iii. Business Availability
iv. The Unknown
v. Security Legislation

CASE STUDY - INTRODUCTION

Introduction to the small business we interviewed

- We met with the founders of young stylish branding and marketing communications business based in the west end of GTA. The company has 6-7 employees (including 4 partners). The core business of the company is its creativity and ideas to promote its clients brand, services and products.

⏳ From the type of the business, what do you think must be protected?

CASE STUDY – IT SCOPE

Information Technology Setup

- All employees use laptops that are personally owned by them for business purposes.
- There is one server that is used to hold the client confidential information and company's information assets. This server is also remotely accessible.
- There is no IT professional on staff, and neither is there is a plan or budget to hire one in near future. One of the partner's is tech savvy and performing the IT role.

CASE STUDY – SECURITY MEASURES

Physical Security

- The office is a single dedicated room within a one level building shared with another company.
- The building has 3 exit doors with alarm system.
- The office has a coded entry and motion sensor installed.
- The office has a single server locked in a wooden cabinet hidden from view.
- One paper filing cabinet (with lock) is located in the office.

⌛ What are the additional Physical Security measures you would recommend to this business?

CASE STUDY – SECURITY MEASURES

Business Confidentiality

- The business signs Non-Disclosure Agreements with clients, which varies from one client to another.
- The employees and contractors/suppliers of the company are required to sign confidentiality agreement.
- There is an informal policy that employees should not disclose the marketing plans of their clients (e.g. advertisements and promotions)
- The company hires employees and contractors only by networking and word of mouth. They do not advertise for the positions.

⌛ Has the business done enough to protect themselves?

CASE STUDY – SECURITY MEASURES

Internet and Email Use

- All confidential client information distributed by email is explicitly noted with instructions not to disclose the content outside the company.
- There is no formal or informal internet or social media policy.

Virus Protection

- The company does not have any measures for virus protection.

⏳ Considering the size of the organization, what else would you recommend?

CASE STUDY – SECURITY MEASURES

Remote Access

- Due to small employee base and nature of the business, all employees have remote access.
- The enrolment to remote access is distributed with validity set to 24 hours by which time employees have to login and create credentials.
- There is a separate remote access for clients through 'WD My Book Live' where they have access only to specific drop box with no ability to change. All clients have their own separate designated folder.

Data Encryption

- None of the computing devices (laptops, smart phones and other portable devices) are protected.

CASE STUDY – SECURITY MEASURES

Password Management for Remote Access

- All connection to company network resources requires a password.
- Initial password setup to access server resources expires within 24 hours.
- Company does not have formal policy; dictated by the remote access application rules.

⏳ What is a cost effective measure this company can take to protect against Viruses?

CASE STUDY – SECURITY MEASURES

Data Backup and Recovery

- Manual Backup is done by employees on removable media and stored at home.
- Automatic Backup is done on company server when the user logs into the company network.
- Data Recovery is done through backups stored at home.

⏳ What do you think about the company Data Backup and Recovery policy? Is it sufficient?

RECOMMENDED SECURITY MEASURES

- ✓ **Periodic Formal Risk Assessment and Management**
- ✓ **Data Protection**
  - ❖ **Virus Protection**
  - ❖ **Data Encryption**
  - ❖ **Backup Management**
- ✓ **Access Control**
  - ❖ Password Management
  - ❖ Access as per "Need-to-Know"
- ✓ **Physical Security**
  - ❖ Automatic Access Door Lock
  - ❖ Protect Windows from potential Break-in

CLOSING REVIEW

What did we do well

- ✓ We reviewed the company business, size, corporate website and NDA documents prior to the interview.
- ✓ We prepared interview questions ahead of the time.
- ✓ We oriented the company prior to the start of interview and used layman terms to explain the intent of our questions.
- ✓ We encouraged the company representatives to think deeper when answering our questions.
- ✓ We had lots of fun!

What did we learn

- ❑ Gained awareness that implementing security measures requires resources and funds that may be expensive for small businesses, so be creative when suggesting solutions.

RECOMMENDED TOP 3 SECURITY MEASURES, AND WHY?

TOP 3 RECOMMENDATIONS, AND WHY?

(1) PERIODIC FORMAL RISK ASSESSMENT AND MANAGEMENT

- Currently the company holds formal strategy planning sessions on an annual basis with quarterly status updates, review and plan adjustments led by the senior partner and founder.

- The annual strategy planning forum would be a good opportunity for the partners to conduct a formal or facilitated Enterprise Risk Assessment for the company. This will help the management team identify the “top priority” information security risks for the company by formally identifying risks, and then “quantifying” the probability of risk materialization, and business impacts should the risk materialize.

TOP 3 RECOMMENDATIONS, AND WHY?

(1) PERIODIC FORMAL RISK ASSESSMENT AND MANAGEMENT

- The high priority security risk items should then be managed though appropriate mitigation plans, and in addition contingency plans should be developed (in the event the risk materializes).

- The management team can also use the identified “top priority” information security risks to:
  - prioritize security policy development activities for the company.
  - Develop employee security risk awareness, education and training programs.

TOP 3 RECOMMENDATIONS, AND WHY?

(2) VIRUS PROTECTION

- Currently each employee owns a personal Macintosh computer used for business. None of the employees have virus protection installed on their computers.
- Furthermore these laptops are sometimes used by family members of the employees who may use the devices to access personal emails or internet websites.
- This presents an increased risk of the devices becoming infected with virus software which may in turn may lead to compromise of confidential company data.
- **Recommendation**: The company should implement virus protection software for servers, and all laptops and work stations.

TOP 3 RECOMMENDATIONS, AND WHY?

(3) DATA ENCRYPTION

- Currently each employee owns his or her own laptop, and stores company data on their hard disk without any encryption. Each staff also backup their computer data at home on a removable storage without any encryption.
- Furthermore, these laptops are sometimes used by family members of the employees who use the devices for personal use. The employees also travel to client sites with their laptops for meetings.
- It is therefore imperative to protect the loss and compromise of "confidential" company and client data in the event a laptop or mobile device is lost or stolen.
- **Recommendation**: The company should implement data encryption for servers, and all laptops, mobile devices and work stations.

ADDITIONAL RECOMMENDATIONS, AND WHY?

(4) DATA BACKUP AND RECOVERY

- "All" company data are only backed-up on one of the senior partners computer, and removable media . There is medium risk probability that critical company information may be lost due to storage and hardware failure or corruption.
- Loss of critical company and client information (without proper backup and recovery) could seriously jeopardize the daily business operations and competitive position, and the viability of the company as going concern.
- **Recommendation**: Company needs to implement more robust and formal data backup measures, and formal policy to mitigate risk to loss of critical company data.

RECOMMENDED POLICIES FOR A SMALL BUSINESS, INTERVIEW RESPONSE & FINDINGS

RECOMMENDED POLICIES – INTERVIEW RESPONSE

Policy	Y/ N	What measures are in place currently to protect the company interests and assets with respect to the following:
Confidentiality Policy	Y	• Formal Non Disclosure Agreement (NDA) / Confidentiality Agreement in place for all company employees, consultants and suppliers. • The business signs Non-Disclosure Agreements with clients, which varies from one client to another. • There is an informal policy that employees should not disclose the marketing plans of their clients (e.g. advertisements and promotions) • The company only hires employees and contractors by networking and word of mouth. They do not advertise for the positions.
Acceptable Use Policy	Y	• Informal measures and rules in place.
Internet Use Policy	N	• There is no formal or informal internet or social media policy. • **<u>Recommendation</u>: company should implement a formal policy (low priority).**
E-mail Use Policy	Y	• Informal measures and rules are in place. • All confidential client information distributed by email is explicitly noted with instructions not to disclose the content outside the company. • **<u>Recommendation</u>: company should implement a formal policy (low priority).**

RECOMMENDED POLICIES - SMALL BUSINESS

Policy	Y/ N	What measures are in place currently to protect the company interests and assets with respect to the following:
Incident Reporting & Response Policy	N	No formal policy or informal measures and rules in place. There needs to be better employee awareness through security risk education and training.
Password Management Policy	Y	Informal measures and rules in place. All connection to company network resources requires a password. Initial password setup to access server resources expires within 24 hours. Recommendation: • **company should implement a formal policy (medium priority).**
Information Protection Policy	Y	Informal measures and rules in place. However none of the business computing devices (laptops, smart phones and other portable devices) are protected with data encryption. Recommendation: • **company should implement a formal policy (high priority).** • Implement **data encryption** for servers, laptops, mobile devices and work stations.
Virus Protection Policy	N	No formal policy or informal measures and rules in place. The company does not have any measures for virus protection. Recommendation: • **company should implement a formal policy (high priority).** • Implement robust virus protection for all company servers, laptops and desktops.

RECOMMENDED POLICIES - SMALL BUSINESS

Policy	Y/ N	What measures are in place currently to protect the company interests and assets with respect to the following:
Remote Access Policy	Y	Informal measures and rules in place. Due to small employee base and nature of the business, all employees have remote access. The enrolment to remote access is distributed with validity set to 24 hours, by which time employees have to login and create credentials. There is a separate remote access for clients through 'WD My Book Live' where they have access only to specific drop box with no ability to change. All clients have their own separate designated folder. <u>Recommendation</u>: • **company should implement a formal policy (medium priority).**
Change Control Policy	N	No formal policy or informal measures and rules in place. Not applicable. / relevant at this stage.
Data Backup & Recovery Policy	Y	The company is using WD My Book Live for backups. Manual Backup is done by employees on removable media and stored at home. Automatic Backup is done on company server when the user logs into the company network. Data Recovery is done through backups stored at home. <u>Recommendation</u>: • **company should implement a formal policy (high / medium priority).** • .Implement formal regular back-up and recovery measures.