starport
MANAGED SERVICES

Cyber Protection

6 Reasons WHY

and

7 Steps HOW

Cyber724.com

The risk of cyber threats is not new, but the level of sophistication, the speed of attacks and the severity of damage that can be inflicted by cyber thieves and hackers are alarmingly new.

Here are just a few organizations that have recently been attacked:

- ✓ University of Calgary
- ✓ Home Depot
- ✓ Equifax
- ✓ Target
- ✓ Uber
- ✓ Deloitte
- ✓ DNC

Large corporations and government aren't the only targets of cyber thieves. Small and midsized businesses (SMBs) must also make data and network protection a top priority. We hear news of destructive breaches almost daily. Boards, investors, clients and suppliers are all demanding that action be taken to bolster defenses; they are realizing the time to act is now.

If you still haven't developed a plan to safeguard your company's information assets, here are the top 6 reasons cyber security matters for SMBs, and the 7 steps you can take to keep them more secure.

6 Reasons WHY Cyber Protection is an Essential Business Activity

1. Your Reputation could be at Risk

- SMBs are learning that the consequences of cyber theft, such as extortion, data theft and data exposure can lead to serious reputational damage.
- The repercussions of a breach can be devastating. Customers or business partners may doubt that their data is safe with your company, potentially prompting them to reduce, even discontinue business relations with you.
- Not every breach makes headlines like Uber's or Equifax's, but if your business has an exposure, people will find it.

2. Breaches are a Financial Burden

- When a breach is discovered, systems are taken offline to recover encrypted data, or to patch a security hole. During that time, you may not be able to process customers' orders or continue operations.
- Consulting fees for technology and investor relations specialists will be incurred as part of the recovery process.

- Following a data breach organizations will likely incur higher cyber insurance deductibles and potential premium increases.

3. Not a Matter of "If," but "When"

- With the pace of breaches ever increasing in our connected data-intensive world, no business, industry or region is immune. Cyber criminals have discovered that smaller organizations also have valuable data and that they've lagged larger corporations in defending themselves.
- Consequently, SMBs are increasingly becoming targets. Rather than hoping to simply avoid a data exposure, small businesses are learning it's smarter to protect themselves and be prepared to do battle with hackers and cyber thieves.

> "I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."
>
> Robert S. Mueller, III, Past Director FBI

4. Insider Threats are Real

- Cyber-attacks can originate from within an organization. Disgruntled employees can take revenge or divulge sensitive information for financial gain.
- Employees can inadvertently grant cyber thieves access by opening emails containing viruses or links that lead to the exposure of confidential information or passwords.

5. Supply Chain Risk

- Some of the largest security breaches have been due to SMBs serving as vendors to larger companies. SMBs have to ensure that they are not putting their business partners at risk.
- SMBs are increasingly being scrutinized for their cyber security processes by their supply chain partners who are seeking to identify and eliminate the weakest links.

6. Identity Theft

- Victims of identity theft fall prey to fraud when criminals use personal information to commit crimes in their name.
- Given the danger of identity theft and fraud, putting in place defenses to protect customers' data should be a priority business item.

7 Steps that show HOW you can Improve your Cyber Protection

1. Conduct an IT Cyber Security Audit to Identify Security Gaps

- Conduct a CyberAudit of existing IT defences and procedures to understand your current ability to protect information assets and defend against cyber threats.
- A CyberAudit must take a rounded view of people, processes and technology to enable you to understand areas of vulnerability, to identify and prioritize areas for remediation and to demonstrate compliance.
- Upon completion of a CyberAudit, you should have a comprehensive view of your organization's level of cyber maturity. You should know where you are, where you need to be and the areas that need to be updated, changed or improved.

2. Deploy Cyber Security Tools as a First Line of Defence

A) Install a Specialized Network Audit and Monitoring Appliance

- Security breaches may happen from outside the organization or from within. Damage can be limited with early detection and swift corrective action
- A network Audit and Monitoring Appliance is a specialized server that is configured to run inside your IT environment, watching for security events and anomalous user behaviour.

Some points to remember:

- ✓ These appliances are a core defence for cyber security.
  They look for unusual activity such as:
  - Unusual login times
  - Users logging in from new equipment or new locations
  - Failed attempts to access restricted data
  - Unsuccessful login attempts
- ✓ Alerts regarding any user rights changes, such as privilege escalation,
- ✓ Notification of new account creation

B) Deploy Software and Hardware tools to Guard your Network

- As cyber thieves improve their capabilities, companies must also improve their ability to protect themselves from attacks.
- The following lists some of the cyber security tools that are commonly put in place to combat cyber thieves;

  ✓ Enterprise grade firewalls (including IDS/IPS)
  ✓ Antivirus, anti-malware
  ✓ Email, spam and phishing protection
  ✓ Web blocking of malicious or infected web sites
  ✓ Follow rigorous IT policies (robust passwords, remote access, acceptable use policies)
  ✓ 2 factor authentication as a double check for authorized access

3. Conduct Rigorous Software Maintenance, Patching and Updates

- Viruses and malware are under continuous refinement by cyber- thieves in their search for security holes to exploit and gain entry to your data.
- The purpose of software updates and patching is to install fixes for known vulnerabilities, to correct problems and to create a safer computing environment. Software patches must be kept up to date at two levels, to keep your company safe.

  ✓ In your organization's in-house and/or cloud based servers and firewalls
  ✓ On your PCs, notebooks, tablets, cell phones and mobile devices

- The back-office infrastructure is typically managed by the IT department or by your managed IT services provider. Of equal importance is the responsibility of everyone to keep his or her personal IT devices up-to-date, patched and protected.

  Some points to remember:

  ✓ Turn on automatic updates for your operating system
  ✓ Make sure to keep browser plug-ins (i.e. Java) up to date
  ✓ Disable plug-ins you do not use (e.g. Flash)

- Patching is preventative rather than curative.
  Simply put, software updates whether big or small are important.

4. Implement 3 Levels of Backups

- Data backup is one of the most important yet overlooked areas of IT. Backups are vital for recovery from disasters such as fire, theft or flood and as a defence to combat the actions of cyber thieves.
- These criminals know that many companies are poorly backed up and have found that if they can gain access to your systems, then they can encrypt your data, and hold you ransom for a payment.
- If you aren't backed up and ready for a recovery, you'll have no choice but to negotiate with the cyber thieves. In many cases, they don't deliver the decryption key.
- Organizations should use 3 levels of backup:

  ✓ Onsite server imaging (e.g. Network Attached Storage Device)
  ✓ Offsite server imaging (typically cloud)
  ✓ Long term file archive (separate from the first two backups and never overwritten)

5. Maintain a Disaster Recovery Plan and Test it

- Organizations should have a disaster recovery plan in place that is tested annually to make sure that all tiers of data backup are working correctly, that all required directories and data are being correctly backed up and that staff are aware of the processes they must follow in the event of the declaration of a disaster.
- Organizations are under severe stress during a recovery. An actual disaster is NOT the time to be trying a recovery for the first time.

  Some points to remember:

  ✓ Regularly test the plan – including tests after major system upgrades
  ✓ Confirm both how long it takes to recover and any issues with the recovered systems
  ✓ Have a plan that is understood and available to all relevant staff

6. Conduct Regular Security Testing

- Security testing is the process of testing your IT infrastructure for vulnerabilities, identifying harm a hacker could do to applications and data.
- Penetration tests are at the centre of security testing and will usually involve a certified ethical hacker who purposefully and anonymously attempts to gain unauthorized access to your company's confidential data.
- Important tests include:

  ✓ Penetration Testing
  ✓ Social Engineering testing
  ✓ Vulnerability testing
  ✓ Phishing campaigns

7. Conduct Security Awareness Training for All Staff

- The role that staff and insiders play in the vulnerability of corporations of all sizes is alarming.
- Industry estimates are that up to 80% of cyber-attacks originate from staff and insiders; sometimes maliciously, but often inadvertently.

A well-educated workforce is a critical component of any comprehensive cyber-security policy.

- Every organization, no matter its size, should require all employees—even its management, directors and key executives—to learn how cyber-attack schemes work, to sense potential threats, and to learn the measures they can each take to reduce the risk of an attack and to protect the data on their computers and networks.
- Companies should consider requiring staff to attend a class, in person or online, and pass a test on the basic steps to identify and prevent cyber security breaches.
- As a matter of HR policy, companies should consider cyber awareness training as part of new staff orientation.

starport MANAGED SERVICES

Your Organization is an Attractive Target to Cyber Thieves

Don't ever Say

"It Won't Happen to Us"

Email us today at: cyber724@starport.ca

or call

1-888-435-7320 x 724

because a cyber defense strategy based on hope is just wishful thinking

Cyber724.com

Cyber Security Services