envision
IT PARTNERS

You are being hacked. What are you doing about it?

Why you should be asking about cyber security
and the steps you can take to help keep you & your comany safe

In many businesses cyber security is often a misunderstood topic. Given the current business climate, and the seemingly unending news of cyber security attacks and breaches, it sometimes seems strange that the simple question still needs to be asked:

Why do you need to know about cyber security?

Cyber security at its root is about protecting your computer-based equipment and information from unintended or unauthorized access, change, theft or destruction.

But even more than that, good cyber security can enhance the reputation of your business and open up new commercial opportunities.

Today most companies now use the internet to do business, to advertise and sell, find new markets, customers and staff, communicate with customers and suppliers, and carry out financial transactions. The internet brings huge business opportunities and benefits. But with those benefits it also brings risks. Every day there are attacks on the IT systems of companies like yours attempting to steal your information and money, or disrupt your business.

Unfortunately you can never be totally safe, but most online attacks can be prevented or detected with basic security practices for your staff, processes and IT systems. These security practices are as important as locking your doors or putting your cash in a safe. You can manage your online security in the same way you would protect any other aspect of your business. With more customers demanding that their suppliers are secure, this is becoming a business necessity.

One of the major things you can begin doing is attacking the problem of cyber security in a business centric way. In other words take a risk management approach to how you look at cyber security and understand the risks to your business.

The following details 4 major steps organizations should be constantly cycling through on a yearly basis (or more often) to answer this question:

1. Define and Understand
   How to think about the problem of cyber security and what the risks may be to your business

2. Focus on the planning aspect of business risk management
   Ensuring a strategy and roadmap exists in line with your business goals to tackle cyber security

3. Implementation
   It’s time to take action by putting in place measures to mitigate risk

4. Review
   Ongoing review of plans and measures to ensure efficacy

1. Define and Understand

The first step is to ask yourself a number of simple, but crucial, questions in order to define and understand how to think about the problem of cyber security.

What is directly at risk in the event of a cyber security attack or breach?

Broadly answered, things such as your money, your information, your reputation, your IT equipment and your IT-based services. Information is an asset that can take many forms: client lists, customer databases, your financial details, your customers' financial details, deals you are making or considering, your pricing information, product designs or manufacturing processes. There is a risk to your IT services and information wherever they are stored, whether held on your own systems and devices, or on third-party hosted systems (i.e. 'in the cloud').

Who could potentially pose a threat to these assets?

Current or former employees, or people you do business with, compromising your information by accident, through negligence, or with malicious intent. Criminals, out to steal from you, compromise your valuable information or disrupt your business because they don't like what you do. Or perhaps business competitors, wanting to gain an economic advantage.

What form could the threat take?

- Theft or unauthorized access of computers, laptops, tablets, mobiles.
- A remote attack on your IT systems or website.
- Attacks to information held in third party systems e.g. your hosted services or company bank account.
- Gaining access to information through your staff via social engineering.

What impact could an attack have?

- Financial losses from theft of information, financial and bank details or money. The average cost of the worst kinds of security breach is between $94,000 and $165,000.
- Financial losses from disruption to trading and doing business – especially if you are depen dent on doing business online. The worst breaches can result in a business being out of action for up to 10 days.
- Losing business from bad publicity & damage to your reputation & customer base.
- Costs from cleaning up affected systems and getting them up and running.
- Costs of fines if personal data is lost or compromised.
- Damage to other companies that you supply or are connected to.

2. Focus on the planning aspect of business risk management

We've gone over why do you need to know about cyber security and what you need to ask, now let's take a deeper dive... The second step is focusing on the planning aspect of business risk management.

Consider using these steps to make information security part of your normal business risk management procedures.

1. Consider whether your business could be a target- this will indicate the level of risk your business is exposed to. Ask around to see whether any of your suppliers, major customers or similar businesses in your area have been attacked, so you can learn from their experiences.

2. Know whether you need to comply with personal data protection legislation and Payment Card Industry compliance (PCI).

3. Identify the financial and information assets that are critical to your business, and the IT services you rely on, such as the ability to take payments via your website.

4. Assess all the IT equipment within your business, including mobile and personal IT devices. Understand the risks to all of these things by considering how they are currently managed and stored, and who has access to them.

5. Assess the level of password protection required to access your equipment and/or online services by your staff, third parties and customers, and whether it is enough to protect them.

6. Ensure that your staff have appropriate awareness training, so that everyone understands their role in keeping the business secure. Decide whether you need to make an investment, or seek expert advice, to get the right security controls in place for your business. You could seek advice from accredited security consultants, internet and managed service providers or even your web designer if they have the capability.

7. Consider who you could turn to for support if you are attacked, or if your online services are disrupted in some way. Define what your recovery procedures would be, and how you could keep your business running, particularly if you trade online.

8. You may like to consider whether cyber insurance could protect your business against any impacts resulting from a cyber-attack.

With cyber security risks increasing year-on-year establishing cyber security best practices via detailed planning is not only useful; ***it's a necessity***.

Cyber security is a complex web and as such there are many areas to consider. The best place for any manager to start is to take a step back and assess the risk of their overall business environment.

3. Implementation

Having explored the topic of planning your organization's cyber security approach through using a business centric model (performing a risk management analysis) the next step to take is to take action.

When it comes to planning how your organization will deal with the cyber security problem your organization can have the best formulated plans, but even the best laid plans need to be executed well in order for them to provide the value and protection they are designed to provide.

Take these steps to put the right security controls in place for your business.

- If you use third-party managed IT services, check your contracts and service level agreements, and ensure that whoever handles your systems and data has security controls in place.
- Malware protection: install anti-virus solutions on all systems, and keep your software and web browsers up to date. Consider restricting access to inappropriate websites to lessen the risk of being exposed to malware. Create a policy governing when and how security updates should be installed.
- Network security: increase protection of your networks, including wireless networks, against external attacks through the use of firewalls, proxies, access lists and other measures.
- Secure configuration: maintain an inventory of all IT equipment and software. Identify a secure standard configuration for all existing and future IT equipment used by your business. Change any default passwords.
- Managing user privileges: restrict staff and third-party access to IT equipment, systems and information to the minimum required. Keep items physically secure to prevent unauthorized access.
- Home and mobile working, including use of personal devices for work: ensure that sensitive data is encrypted when stored or transmitted online so that data can only be accessed by authorized users.
- Removable media: restrict the use of removable media such as USB drives, CDs, DVDs and secure digital cards, and protect any data stored on such media to prevent data being lost and malware from being installed.
- Monitoring: monitor use of all equipment and IT systems, collect activity logs, and ensure that you have the capability to identify any unauthorized or malicious activity.

4. Review

Every year (and generally more often) organizations should be going over their cyber security plan and cybersecurity implementations thoroughly in order to ensure the plan and measures they have taken still align with organizational goal and requirements. It is not uncommon for businesses to change rapidly or for consumer requirements to alter to such an extent that what was previously adequate is no longer sufficient to support the business needs of a company.

To this end it is crucial for an organization to have a review process by which they can evaluate systematically both the cyber security plan and the technical and policy measures currently in place.

Organizations should take the following steps to review their security and respond to any changes or problems they identify, including attacks or disruption to business.

- Test, monitor and improve your security controls on a regular basis to manage any change in the level of risk to your IT equipment, services and information.

- Remove any software or equipment that you no longer need, ensuring that no sensitive information is stored on it when disposed of. Review and manage any change in user access, such as the creation of accounts when staff arrive and deletion of accounts when they leave.

- If your business is disrupted or attacked, ensure that the response includes removing any ongoing threat such as malware, understanding the cause of the incident and, if appropriate, addressing any gaps in your security that have been identified following the incident.

- If you fall victim to online fraud or attack, you should report the incident. You may need to notify your customers and suppliers if their data has been compromised or lost.

Once you have your plan in place, a strategy for implementing and a schedule for review, make sure to stick to it and ***repeat yearly*** if not more often!

Envision IT Partners brings you a simplified IT world that will get you out of the IT support business. We provide all-inclusive support and complete accountability for your technology under one management plan. We have developed specific personnel, skills, technology and experience to provide that support to mid-sized organizations.

Contact info@envisionitpartners.com to learn more about manged IT support.