Velocity Technology

E-book

STOP! YOU MIGHT BE THE NEXT TARGET!

INCIDENT RESPONSE PLAN

BUSINESS CONTINUITY SOLUTION

CYBERSECURITY TIPS FOR WORKING REMOTELY

HOW SECURE IS YOUR BUSINESS?

All sizes of business need a cybersecurity plan so that they can be prepared for cyber-attacks

CYBERSECURITY

Cybersecurity, Ransomware and Cyber Hygiene

Cyber threats and hacks have made headlines now on every major news organisation. This is no longer a niche for the IT security news sites and blogs. Hospitals, pipelines, insurance companies, hedge funds and probably someone you personally know has had some form of cyber security event over the last few years.

Threat actors steal or encrypt company data, personal photos, bank records and its common place now to receive phishing attempts to get the unsuspecting to cough up their user name and password to all sort of email accounts and websites. The attackers may try to trick you into voluntarily sending them money or they may try to extort you or your company into paying a ransom for access to your own data, or perhaps even they will threaten to release confidential data onto the internet unless you pay them money.

Money… Money… Money. That's what its all about. These are modern day thugs and extortionists that do anything to unlawfully get money from digital crime.

Often its not some highly skilled hacker that's managed to break through all your security like you might see on some TV drama show. Often its simple cyber hygiene or training that prevents an attack. Criminals may share breached user names and passwords they find or buy on the dark web (look at our dark web monitoring), maybe a firewall, server or desktop hasn't been patched (look at our IT Risk and Review, Penetration Testing and Continuous Vulnerability Scanning services) or users may have given away their corporate password to a phishing email (look at our Security Awareness Training).

Even if an attacker does get inside a network, most damage can easily be reversed with good backups and a well thought out Business Continuity Plan (look at our Distaster Recovery as a Service offering and Business Continuity Consulting) and maybe even thwarted with the appropriate security measures (look at our Breach Detection and Endpoint Detection and Response)

Of course we can also manage your network and systems too.

TABLE OF
CONTENTS

Velocity Technology

sales@velocity-technology.com
+852 2915-5096
www.velocity-technology.com
7th Floor Golden Star Building
20-24 Lockhart Road
Wanchai, Hong Kong

Don’t let hackers get into your network!

How secure is your business from Cyber-attacks?

Most small/medium businesses do not take the threat of cyber-attack seriously. Most people think “I would not be a target”. The reality is that all businesses are potential targets as hackers will send many thousands of phishing emails to large lists of email accounts that they buy from the dark web. Phishing emails are the most efficient way to infiltrate a company with ransomware, key loggers, remote control malware and other malicious software that can be downloaded by clicking a link or attachment within a phishing email.

Any businesses that get infected with ransomware on one computer could have it spread to all their computers including servers and even to their backups. This will force them to pay a ransom to the hackers unless they have a very recent backup and decide to rebuild their critical workstations and servers from backups.

All sizes of business need a cybersecurity plan so that they can be prepared for these type of cyber-attacks. The cybersecurity plan should feature best practices and detail exactly what should be done in the event of a cybersecurity incident. Failure to do this may lead to the business failing a short time after a serious cybersecurity attack.

The importance of an IT Infrastructure and Risk Review

An IT Infrastructure and Risk Review is vital to an organization to be protected from cybersecurity threats. This will help your organization to identify how your computer network is from attack and provide you with the best solutions to improve your current state of cyber-preparedness. This will include running different software tools to test your computer network and gather all the information needed. This will also include analyzing the current IT policies and procedures of your physical network. A comprehensive report will be discussed with you in detail that includes recommendations to improve the security and functionality of your computer network.

IT Infrastructure and Risk Review

- Provides you with an independent report on the state of your computer network.
- IT experts will examine the current state of your network and document the hardware and software on your network using specialist software tools.

The aim of this type of review is to identify any areas that will affect the security and reliability of your computer network and provide you with an independent review of your IT systems. A Cybersecurity review should be conducted in accordance with best practices and consist of the following phases:

Information gathering

Engineers use a range of software tools during an initial site visit to gather the details required. Your current IT policies, procedures and conduct will be examined and documented. Your physical network and any current IT issues that are present will also be documented.

Data Aggregation and Report Preparation

All of the information collected will be analysed and summarised in a report that will detail areas that require attention.

Presentation of report

The IT Infrastructure and Risk Review report should be discussed with you in detail. The report should include recommendations to improve the security of your network. After the recommendations are discussed with you, the solutions to these issues should be presented in a proposal.

Penetration Testing

Cybersecurity is a must for one of the following reasons: investors, regulators and your own peace of mind.

Why do we need Penetration Testing?

Running penetration tests will help your company to identify your network's weaknesses and make sure that your cybersecurity systems are actually working.

Sophisticated investors are now asking about penetration testing in Due Diligence Questionnaires. Industry regulators can ask about penetration tests in their questionnaires and audits. Your business needs peace of mind to know what security issues are present within your network, and if they can be used by a hacker to gain entry and remove sensitive information or hold you to ransom. Your company's reputation should not suffer by letting cybercriminals get into your network and exploit your important information in what is commonly known as a "data breach".

Penetration testing will help you to moderate the threats that your business may encounter. This testing should be conducted by security experts that hold internationally recognized security certifications such as CISSP, CISA, GCIA, GSNA, GWAPT, and CEH.

What are the different types of Penetration testing?

- Remote Network Analysis
- Exploiting Network Vulnerabilities
- Wifi Network Testing
- Microsoft/Office 365 security testing
- Internal vulnerability scans
- Remote Website Analysis
- Exploiting website vulnerabilities
- Phishing Attacks
- Physical Access Test
- USB Key Attack
- Phone Call Attack

The objective of running penetration tests on your network is to determine, and potentially exploit, the vulnerabilities discovered within your computer network.

Breach Detection Solution

A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment. Individuals and organizations are being attacked on a daily basis by cybercriminals and hackers. How will you know if an intruder is already inside your network? Will you be ready for this kind of incident? This is why it is so important to have a Breach Detection Solution to get protected from this type of threat. This will not only help your organization protect your confidential information but also protect your time, money and reputation.

A Breach Detection solution provides a managed appliance that appears like a server on your network. One of the first steps a hacker or malicious insider takes is to probe your network and attempt to learn what is connected and how. When an intruder probes the appliance, you will receive an alert that someone is trying to access files on your network.

If you do not have a breach detection solution you will not know if there is an intruder on your network until it's too late.

Noticing an Intruder

In a recent report from Mandiant (a global consulting firm) they stated that while businesses in the United States will detect a hacker in their networks within 4 months (which is in line with the global average), it takes 17 months for companies in the Asia Pacific region to notice they have an intruder.

The Velocity Breach Detection solution provides high quality, actionable alerts on where a breach has taken place on your network.

Velocity provides 24x7 monitoring via our helpdesk and you will be alerted if there are any attempts to probe the Breach Detection appliance.

Security Awareness Training

ARE YOUR EMPLOYEES CYBER-READY?

Cybercrime has turned professional. Now more than ever, your users are the weakest link in your network security. Your users need to be trained and then stay on their toes, keeping security top of mind or else your company will become a victim of ransomware and/or your company's data will be stolen, altered or deleted.

Effective security awareness training is usually hard. Today internal IT teams don't have the support, time, or resources they need to be successful and/or are missing the required skills and experience to effectively engage and train their organization.

A good Security Awareness Training program will include live training, online training and ongoing testing and reporting.

What's Typically Included?

- **Baseline Testing**
  A baseline test will assess the initial Phishing-prone percentage of your users through a simulated phishing attack.

- **Train Your Users**
  Live training, On-demand, interactive, and engaging training that explain the common traps.

- **Phish Your Users**
  Fully automated simulated phishing attacks will test your users on a huge variety of subjects.

- **See The Results**
  Reporting that includes stats and graphs for both training and phishing, ready for presentation to management.

- **Discussion of Results**
  The results of the training program should be discussed in an annual review meeting.

Security Awareness Training Program Features:

- **Training Campaigns**
  Automated Training Campaigns do the heavy lifting for you, saving you the hassle associated with setup and chasing down users to complete their training.

- **Custom Phishing Templates**
  The best training programs include hundreds of easy-to-use existing templates, and should have customizable scenarios based on personal information, creating targeted spear-phishing campaigns.

- **Custom Landing Pages**
  Each Phishing Email Template can have its own Custom Landing Page, which allows for point-of-failure education and landing pages that specifically phish for sensitive information.

- **Simulated Attachments**
  Your customized Phishing Templates can also include simulated attachments in the following formats: Word, Excel, PowerPoint and PDF, (also zipped versions of these files).

- **Detailed Reporting**
  Reporting for phishing campaigns will include a general overview, and you should be able to drill-down into one-time and recurring campaigns for more detail.

Cybersecurity tips for working remotely

Remote work policies have become a necessity not just because of the current coronavirus crisis, but also for the ways they improve a company's bottom line and efficiency. Yet despite remote work's benefits, it leaves you and your company exposed to online scams and other cybersecurity threats. To defend your company and your remote workers, make sure to heed the following tips.

Fortify user accounts

When everyone is working remotely, user accounts must be properly secured. One way to achieve this is by setting at least 12-character long passwords with numbers and special characters mixed in to make them more difficult to guess. More importantly, these passwords must be unique to each account, to minimize the damage if hackers do manage to compromise one set of credentials. If you find it difficult to generate and remember login details for all your accounts, consider password managers like LastPass, Dashlane, and Keeper.

To further strengthen your accounts, however, you'll also need to enable multifactor authentication (MFA). This adds another layer of identity verification — like fingerprint scans or one-time activation codes generated by SMS — to make it more difficult for cybercriminals to hijack your accounts.

Use a virtual private network (VPN)

VPNs are primarily known for circumventing geographic restrictions on location-specific websites and streaming services, but they're also a crucial tool for remote workers. A reliable VPN creates secure connections between devices and networks by encrypting

internet traffic. This hides web activity from prying eyes, protecting your employees' online privacy, and mitigating the risk of hackers stealing company information.

Patch your software regularly

Although installing software updates can be a major nuisance, they cover critical weaknesses and protect your systems from the latest threats. Most apps now offer an automatic update feature so you don't have to manually patch your software.

Another option for your business is patch management software. These track the patches on employee devices and distribute the most recent updates on a company-wide scale.

Set up firewalls and antivirus software

Make sure to enable firewalls in your operating systems and hardware. These provide a strong layer of protection between your device and the internet, preventing malicious programs and other network threats from reaching your device. Your managed IT services provider (MSP) may also provide third-party firewalls in case your computers don't have any built in by default.

In addition to firewalls, you'll also want to implement antivirus software to detect and remove any malicious programs that do manage to find their way onto your device. Just remember to constantly update the software so it can effectively detect the newest malware.

Watch out for online scams

The biggest threat remote workers face is online scams. Phishing emails may entice you with free coronavirus test kits in exchange for personal information. Some cybercriminals may even masquerade as legitimate companies, CEOs, or friends to trick you into clicking on dangerous links and attachments.

To avoid these threats, you must be critical of everything you see online. Look for any suspicious links and attachments, grammatical errors in the email body, and misspelled email addresses. Plus, never give out sensitive information to an unsolicited email, text message, or phone call.

Working from home poses many cybersecurity challenges for businesses, but you don't have to address them alone. If you need guidance with setting up firewalls, avoiding scams, and even enabling MFA, we can provide the IT support you need in this difficult time. *Call us now.*

Published with permission from TechAdvisory.org.

"Cyber security is everyone's responsibility!"

Fully Managed Firewall Service

“Having a poorly configured or out of date firewall is the equivalent of leaving your office door unlocked.”

A firewall is a vital part of your computer network and is your defence from Internet attack. A firewall system is an item that cannot just be installed and then forgotten about. Customers that do this “set and forget” approach are exposing their network to a multitude of hacker attacks from the Internet.

Protect Your Network

A Fully Managed Firewall Service is designed to protect your network with a solution that provides the latest firewall equipment, is monitored 24 x7 and continually updated by an engineering team.

Badly configured and non-updated firewalls are some of the most common vulnerabilities that appear in penetration tests of networks. Having a poorly configured or out of date firewall is the equivalent of leaving your office door unlocked.

For more information on firewalls and network security, check out this video:

The security features provided by a fully managed firewall service include:

- Gateway Antivirus to examine incoming traffic for viruses and malware
- Intrusion Prevention to protect against known threats and zero-day attacks including malware and underlying vulnerabilities
- Application control to prioritise specific application traffic and block or throttle traffic from some sources (eg. BitTorrent, Spotify, Youtube etc.)
- Web search filtering to filter out offensive websites and search results
- Antispam - provides a comprehensive and multi-layered approach to detect and filter spam
- Sandboxing to safely examine potential threats before they pass through the firewall

Business Continuity Solution

There are a number of disasters such as major computer hardware failures, office fires, water leaks etc. that can have a massive impact on your business. Your business could be exposed to days of downtime for your computer systems if you have to rely on conventional backup solutions. If you are still using tape backups, there are statistics showing that 50% of all tapes fail when you try to restore from them.

- A Business Continuity solution for your servers and critical workstations will enable you to be back up and running quickly after most disaster scenarios.

- A good Business Continuity solution will enable you to launch a virtual server or workstation from a recent backup (as recent as 5 minutes ago). A Virtual Machine should be able to be launched from a backup appliance or from a regional secure cloud service.

- Having a good Business Continuity solution means that even if you have a major computer hardware failure, an office fire or other disaster, you will still be able to access your data.

Being prepared when disaster strikes will mean the difference between staying in business or having to shut down your operations due to non-functioning computer systems.

Click the video below to watch Stuart Sanders (Chief Technology and Security Officer at Velocity Technology) and Tom Fernandez (General Manager) of ASEAN Datto speak about - Cyber Resiliency: the last line of defence - DRaaS What you need to know about Disaster Recovery as a Service.

Calculate the cost of your downtime! CALCULATE DOWNTIME

Did you know that Microsoft 365 is Not Automatically Protected?

As organizations increasingly move data into cloud-based applications, many believe that traditional best practices such as data backup are outdated. After all, SaaS applications are always available, accessible from anywhere, and highly redundant, so why is backup necessary?

An astonishing 1 in 3 companies report losing data stored in cloud-based applications. The single leading cause of this data loss? End-user error. Other common culprits include:

- Malware or ransomware attacks
- Malicious end-user activity
- Accidental data overwrites
- Canceled account subscriptions

With more and more companies depending on Microsoft 365 for collaboration and business operations, these risks are impossible to ignore. Backup is just as important in the cloud as in traditional on-premises IT systems. An independent, third-party, SaaS backup solution is the best way to protect organizations against the most common data loss pitfalls.

Watch our Microsoft 365 Data Protection webinar

Did you know that 47% of data loss is caused by accidental deletions? In the event of such an incident, Microsoft is not liable nor responsible for restoring lost documents.

The Shared Responsibility Model was created by Microsoft to outline who is responsible for data in different scenarios of data loss. Is your team aware of which scenarios you are responsible for protecting your own data?

Watch our webinar titled "**Cyber Resiliency for Microsoft 365 - What you need to know?**", to find out what the shared responsibility model is and how you can protect your workforce from facing permanent data loss issues.

Other items to covered:

- What is Cyber Resilience
- Changing threat landscape for Microsoft 365
- What is the true cost of a cyberattack
- Product demonstration - Datto SAAS for Microsoft/Office 365

Our Speakers:
Stuart Sanders, Chief Technology & Security Officer at Velocity Technology and Daniel Nguyen, Regional Channel Manager of ASEAN Datto

WATCH NOW

Endpoint Detection & Response

This type of cybersecurity solution installs an agent that inventories each of your applications that are scheduled to automatically start at boot-time or on user login (persistent applications). Metadata on these applications are sent to an Analysis Engine for inspection.

The Analysis Engine aggregates data from the installed agents and uses algorithms to discover malicious outliers (footholds) in the dataset. Each persistent application is evaluated using a combination of file reputation, frequency analysis, and other proprietary algorithms.

When an anomaly is detected this solution delivers prioritised remediation recommendations – not alerts – to you and all other affected members within this solution's community.

Application Whitelisting

An Application Whitelist is a list of applications and application components that are authorized for use within an organization.

Application whitelisting technologies use whitelists to control which applications are permitted to execute on a host.

This helps to stop the execution of malware, unlicensed software, and other unauthorized software.

Incident Response Plan

An Incident response plan helps the IT team to be prepared, identify, eliminate the malware and recover from cyber attacks. This will also help the organization to prevent follow on attacks or similar incident in the future.

A good Incident response plan should be recommended by a respected organization, which provides research and education on information security such as the SANS Institute. The SANS Institute is the world's largest provider of security training and certification, and maintains the largest collection of research about cybersecurity.

Below are the 6 steps of a good Incident Response Plan:

Preparation—review and codify an organizational security policy, perform a risk assessment, identify sensitive assets, define which are critical security incidents the team should focus on, and build a Computer Security Incident Response Team (CSIRT).

Identification—monitor IT systems and detect deviations from normal operations, and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything.

Containment—perform short-term containment, for example by isolating the network segment that is under attack. Then focus on long-term containment, which involves temporary fixes to allow systems to be used in production, while rebuilding clean systems.

Eradication—remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.

Recovery—bring affected production systems back online carefully, to prevent additional attacks. Test, verify and monitor affected systems to ensure they are back to normal activity.

Lessons learned—no later than two weeks from the end of the incident, perform a retrospective of the incident. Prepare complete documentation of the incident, investigate the incident further, understand what was done to contain it and whether anything in the incident response process could be improved.

GET IN TOUCH WITH US!

Velocity Technology is the right choice as your technology partner as we cover all areas from secure computer network design through to implementation and managed support services.

As new technologies are established, Velocity Technology will design IT systems that enable you to leverage technology to make your business perform better and enhance productivity for all your staff, wherever they are located.

Contact us today to find out how we can help your company to be more secure and effective.

CONTACT US!

consulting@velocity-technology.com | +852 2915-5096 | www.velocity-technology.com