All the latest technology trends and topical issues

ISSUE 1 - 2017

technology times

Could One Tiny Leak Wipe Out Your Entire Computer

Why Physical Security of your IT Equipment Remains Important

Go Mobile - Without Killing your Data

PASSWORD FATIGUE

Velocity
Technology

Contents Issue 1- 2017

STUART'S CORNER

> “As a business owner, you don't have time to waste on technical and operational issues. That's where we shine!”

Welcome to the first edition of our Tech News newsletter for 2017. I can say that as we approach the end of our financial year, that this has been our best year ever. Velocity continues to expand the teams across our offices and the service offering enhancements that we are planning for this year are both exciting and sweeping. Stay tuned for announcements in the coming months.

One of the concerns I have as 2017 begins, is that I get a sense that there is a feeling of saturation and fatigue around cybersecurity. In particular, this applies to the fund industry. While everyone understands it is important, the constant barrage of sales calls and emails from every firm selling the latest cybersecurity “fix-it” is tiring. Some of my clients are getting a constant barrage of calls and emails – I know as they forward them to me.

Why does this concern me? History is full of examples where industries and fads go from one extreme to the other. Cybersecurity is a real issue, but it is important to take a holistic and top-down approach. No single solution is the be-all and end-all, and what is appropriate very much depends on the nature and size of the fund or business. So while I certainly have strong opinions regarding some vendors, in general, I try to take a vendor neutral or agnostic approach.

This corner piece tends to be the last thing written for the newsletter, so what I can say is that next issue will have an in-depth article on what should be a guide for appropriate systems.

STUART SANDERS
Managing Director
Velocity Technology Ltd

✉ stuart.sanders@velocity-technology.com
Velocity Technology Limited
Velocity Technology Limited
VelocityTechnologyLimited
@velocitytechhk

All the latest technology trends and topical issues
ISSUE 1 - 2017
technology times
Could One Tiny Leak Wipe Out Your Entire Computer
Why Physical Security of your IT Equipment Remains Important
Go Mobile - Without Killing your Data
PASSWORD FATIGUE
Velocity Technology

HK Newsletter Team

Stuart Sanders
EDITOR

Michael Early
EDITOR IN CHIEF

Cristina Caratao
ART EDITOR

Newsletter Contact

✉ newsletter@velocity-technology.com
☎ +852 2915.5096
🖷 +852 2834.8852

Could One Tiny Leak Wipe Out Your Entire Company?

Things were going great at Michael Daugherty's up-and-coming $4 million medical-testing company.

He was a happy man. He ran a good business in a nice place. His Atlanta-based LabMD had about 30 employees and tested blood, urine and tissue samples for urologists. Life was good for this middle-aged businessman from Detroit.

Then, one Tuesday afternoon in May 2008, the phone call came that changed his life. His general manager came in to tell Daugherty about a call he'd just fielded from a man claiming to have nabbed a file full of LabMD patient documents. For a medical business that had to comply with strict federal rules on privacy, this was bad. Very bad.

It turned out that LabMD's billing manager had been using LimeWire file-sharing software to download music. In the process, she'd unwittingly left her documents folder containing the medical records exposed to a public network.

A hacker easily found and downloaded LabMD's patient records. And now the fate of Michael's life – and his business – were drastically altered.

What followed was a nightmarish downward spiral for LabMD. Not one to go down without a fight, Michael found himself mired in an escalating number of multiple lawsuits and legal battles with the Federal Trade Commission and other regulators investigating the leak.

Finally, in January 2014, exhausted and out of funds, his business cratering under constant pressure, he gave up the fight and shuttered his company.

One tiny leak that could have easily been prevented took his entire company down. Could this happen to you and your business? Let's take a look at four fatal errors you MUST avoid, to make sure it never does:

Have you developed a false sense of security?

Please, please, please do NOT think you are immune to a cyberattack simply because you are not a big company. The fact is, whether you have 12 clients, or 12,000 clients, your data has value to hackers. A simple client profile with name, address and phone number sells for as little as $1 on the black market. Yet add a few details, like credit card and Social Security numbers, and the price can skyrocket – $300 per record is not uncommon. Being small doesn't mean you are immune.

Are you skimping on security to save money?

Sure, of course you have a tight budget... So you cut a deal with your marketing manager, who wants to work from home at times. He links into the company network with a VPN. If configured properly, your VPN creates a secure and encrypted tunnel into your network. So his device now links his home network into the company network. The problem is, his home cable modem may be vulnerable to attack, an all-too-common issue with consumer devices. Now you have an open tunnel for malware and viruses to attack your network.

Could lack of an off-boarding process put your company at risk?

It's crucial to keep a record of user accounts for each employee with security privileges. When an employee leaves, you MUST remove those accounts without delay. An internal attack by a disgruntled worker could do serious harm to your business. Be sure to close this loop.

Have you been lax about implementing security policies for desktop computers, mobile devices and the Internet?

The greatest threat to your company's data originates not in technology, but in human behavior. It starts before you boot up a single device. In an era of BYOD (bring your own device), for instance, lax behavior by anyone connecting to your network weakens its security. Your team love their smartphones, and with good reason. So it's tough sticking with strict rules about BYOD. But without absolute adherence to a clear policy, you might as well sell your company's secrets on eBay.

Why Physical Security of your IT Equipment Remains Important

Words: STUART SANDERS

Physical security of IT infrastructure has always been important. While server rooms tend to provide cooling to keep the equipment running at a lower temperature to preserve longevity they are also secured to protect what is increasingly one of the most important assets a company has. There is an old adage that if I can get physical access to some equipment its mine! I can personally vouch for this, as I have been asked to reset passwords on servers and other equipment over the years when a vendor has disappeared or staff left without providing necessary credentials. With a CDROM or bootable USB, it's a matter of a few minutes in most cases to reset the administrator password and have full unrestricted access to key equipment. This includes servers, firewalls, and workstations.

So securing your equipment is important.

Larger corporations sometimes take this a step further and lock down peripheral equipment on even desktops and notebooks. Ever worked for a company where the IT department blocks the use of USB devices (except maybe a mouse and keyboard)? It is much for the same reason. If they don't block this, then someone who is IT savvy can reset the local admin account, which then gives them the ability to control the device in question and it's a step to further infiltrate the company network.

Now there are other things to worry about. In September, it was announced that a company (China based) was offering USB devices that would literally destroy the equipment it was plugged into. The concept is fairly simple. USB provides power. That's why you can charge your phone or run external USB equipment. Well, this particularly enterprising company have come up with a USB that uses the power to charge some capacitors and then fire the electric charge down the data ports on the USB. If the USB data channel is not electrically isolated or protected then that electric charge can burn out the systems its attached to. Like, for example, the motherboard of a server or notebook. Of course, the manufacturer says this is designed for "testing purposes" only, but with reports discussing this on mainstream tech news sites, knowledge of the availability is now widespread.

Do you keep your equipment in an unlocked cabinet or room? You might want to rethink this.

Another enterprising security researcher has come up with a USB that pretends it's a network USB connector. Apparently, both Mac and Windows will happily give the logged on user credentials and password hash to any device that is a network adaptor when plugged in. Even when the screen is locked. This takes less than 30 seconds to accomplish, and the password hash can be cracked fairly easily to obtain the full username and network password for any user so logged in.

It may be time to review the physical security of your IT equipment, both for core infrastructures like servers and network gear, but also for standard desktops and notebooks.

PASSWORD FATIGUE

Words: STUART SANDERS

Many of us suffer from password fatigue. Every website you visit requires a user name (often your email address) and password. They want it to be secure which means you end up either reusing the same password for everything or juggle with trying to remember which password is for what site and may end up using a sticky note on your screen or something similar.

A recent survey by NIST (the National Institute of Science and Technology) had a result that they weren't expecting when interviewing non-technical people about cybersecurity. The study found that a majority of the typical computer users they interviewed experienced security fatigue that often leads users to risky computing behaviour at work and in their personal lives. There was an overwhelming sense of giving up and fatalism.

What I'd like to discuss in this article is one way to claim back some control over this and improve your security in the process. It is generally recommended to use a different password for every service. Many of the public breaches that occurred earlier this year were due to people reusing their passwords across multiple sites and services including work. Unless you are a savant, it is not feasible to be expected to remember dozens or hundreds of complex passwords ... so don't.

There are a number of services now that offer secure password management. You remember one master password and then it remembers the rest. The one I generally recommend to clients is LastPass (www.lastpass.com). They have a free version, a paid premium version that allows you to sync across multiple devices and computers and an enterprise version if you want all of your corporate web and application login information to be stored securely. You can also store notes securely and other information you may not want to put in a document called passwords.doc. They use current best practices for encryption and security including 2-factor authentication.

Many of the password management services are cloud based services, but there are non-cloud services available as well. These will allow passwords to be stored securely on corporate servers, but will not then sync to a mobile device.

Using a password manager like LastPass or one of the other commonly used services allows you to take control back of your password fatigue and protect both yourself and your business better in the process.

If you have any questions about password managers, feel free to reach out to me at stuart.sanders@velocity-solutions.com

$1.5M Cyber-Heist Typifies Growing Threat

Efficient Escrow of California was forced to close its doors and lay off its entire staff when cybercriminals nabbed $1.5 million from its bank account. The thieves gained access to the Escrow Company's bank data using a form of "Trojan horse" malware.

Once the hackers broke in, they wired $432,215 from the firm's bank to an account in Moscow. That was followed by two more transfers totaling $1.1 million, this time to banks in Heilongjiang Province in China, near the Russian border.

The company recovered the first transfer, but not the next two. They were shocked to discover that, unlike with consumer accounts, banks are under no obligation to recoup losses in a cybertheft against a commercial account. That meant a loss of $1.1 million, in a year when they expected to clear less than half that. Unable to replace the funds, they were shut down by state regulators just three days after reporting the loss.

Net result? The two brothers who owned the firm lost their nine-person staff and faced mounting attorneys' fees nearing the total amount of the funds recovered, with no immediate way to return their customers' money.

Avoid Getting Blindsided
While hacks against the big boys like Target, Home Depot, and Sony get more than their share of public attention, cyberattacks on small and medium-sized companies often go unreported, and rarely make national headlines.

Don't let this lull you into a false sense of security. The number of crippling attacks against everyday businesses is growing. Cybersecurity Company Symantec reports, for example, that 52.4% of "phishing" attacks last December were against SMEs – with a massive spike in November.

Here are just a few examples out of thousands that you'll probably never hear about:

- Green Ford Sales, a car dealership in Kansas, lost $23,000 when hackers broke into their network and swiped bank account info. They added nine fake employees to the company payroll in less than 24 hours and paid them a total of $63,000 before the company caught on. Only some of the transfers could be canceled in time.
- Wright Hotels, a real estate development firm, had $1 million drained from their bank account after thieves gained access to a company e-mail account. Information gleaned from e-mails allowed the thieves to impersonate the owner and convince the bookkeeper to wire money to an account in China.
- Maine-based PATCO Construction lost $588,000 in a Trojan horse cyber-heist. They managed to reclaim some of it, but that was offset by interest on thousands of dollars in overdraft loans from their bank.

Why You're A Target – And How to Fight Back!
Increasingly, cyberthieves view SMEs like yours and mine as easy "soft targets." That's because all too often we have:

1. Bank accounts with thousands of dollars.
2. A false sense of security about not being targeted.
3. Our customers' credit card information, social security numbers and other vital data that hackers can easily sell on the black market.

If you don't want your company to become yet another statistic in today's cyberwar against smaller companies, and your business doesn't currently have a "bullet-proof" security shield, **you MUST take action without delay – or put everything you've worked for at risk. The choice is yours.**

Here are three things you can do right away:

1. Remove software that you don't need from any systems linked to your bank account.
2. Make sure everyone with a device in your network NEVER opens an attachment in an unexpected e-mail.
3. Require two people to sign off on every transaction.

Go Mobile - Without Killing Your Data

What if you could tap into the top talent in your industry, no matter where in the world they are? With the power of the mobile web, your all-star team is now – literally – at your fingertips.

Consider this: 83% of workers report that they prefer using cloud apps over those deployed on-premise. Millennials, who will make up almost 50% of the available workforce by 2020, are "digital natives." And don't forget how much money remote workers allow you to save on real estate and office equipment.

Yet there are risks. Spreading your network around the world on a variety of devices you don't control can expose your data in more ways than ever before. The key is to find the right balance between protection and productivity. Here, then, are five ways to effectively "mobilize" your workforce – without endangering your data:

1 Collaborate In The Cloud

A plethora of online collaboration tools have sprung up that make it easy for a geographically dispersed team to access and share the same files in real time. These tools not only make sharing easy and instantaneous, they help your team communicate quickly and effectively. Tools like Slack, HipChat, Asana, Podio and Trello – to mention just a few of the most popular options – are proving to make teams more productive. And that includes keeping critical data safe and secure.

2 Expand Elastically

In-house investments in IT hardware, software and staff can lock you into a rigid structure that can't easily adapt to changes in demand. A cloud-based mobile workforce is able to contract and expand more easily as needs arise, and with very little loss of capital. Bottom line: use a VPN (virtual private network) and cloud-based collaboration tools to remain agile, flexible and competitive.

3 Cut Costs Dramatically

Physical work areas, equipment, software and on-site security expenses can add up. Instead of spending money on office space, equipment and infrastructure, invest it in innovation and refinement. Combine the power of the cloud with a well-designed workflow to reduce the number of people needed to get things done. That will free up your key players to focus on more important tasks – the ones that boost productivity and ROI.

4 Deal With BYOD

Let's face it, BYOD (bring your own device) can be your greatest IT security threat. Yet, like it or not, workers will use their own devices on the job. Foisting strict controls without buy-in will just backfire. Yet doing nothing simply makes you a sitting duck for a cyberattack. Solution? First, audit how your employees use their devices. Note the data they access and the apps they rely on. Group them by the levels of security and compliance they need to be governed by. A CEO, for example, may need to abide by financial regulations. An HR manager must deal with employment laws. Armed with information from your audit, you can roll out new policies as well as technical and process controls. Train your team in safe practices. And be sure to contact us for help in getting all this done securely and effectively.

5 Go Remote Without Risk

Whether you want to cut commuting time for your team, tap into the talents of experts outside your locale or simply accommodate a worker caring for family members, mobilizing your workforce can have big benefits. The trick is defending it at all points. Make sure remote workers share files and communicate with other employees only via a secured network. Make sure they use adequate virus protection. And, if they are using WiFi, either at home or on the road, make sure they do it safely. For instance, ensure that their tablet isn't set to automatically connect to the default wireless network. That's often an easy access point for hackers.

Which Flavor Of The Cloud Is Right For You?

Secure data backup, greater reliability, better resource and growth management options, and improved collaboration are just a few of the reasons to take full advantage of cloud computing today.

Yet understanding the choices you have can help you avoid some VERY costly mistakes you could wind up seriously regretting later. To help you move forward with confidence, here are some important points to consider.

Three "Flavors" Of The Cloud

Not all cloud models are the same. A cloud environment that works for a dental practice with a half dozen locations may not be entirely suitable for a new law firm with just a single office. In determining what the best cloud model is for your organization, it's important to know how cloud services are structured.

Basically, there are three types of cloud: public, private and hybrid.

1 Public Cloud Services Offer Flexibility And Lower Cost

A public cloud comprises a collection of data storage and software services that can be accessed on an as-needed monthly basis, somewhat like an electric utility or fitness club. It houses data facilities outside the corporate firewall that you access through an Internet browser without having to make any initial or ongoing capital investment.

Well-known examples of public cloud services include Google Drive, Microsoft Office Online, Apple iCloud and Amazon Cloud Drive. They provide data storage and, in many cases, web apps.

Public clouds are best used where a high level of privacy is not required. They can provide access to a growing pool of newer technologies that would not be affordable if developed individually.

2 Private Clouds Support Highly Specialized Apps

A private cloud resides within an organization's firewall, and is typically owned, managed and supported by that business. IT resources are available to members of the organization from their own data center.

Private clouds can support highly specialized and/or privacy-restricted applications, like medical-records software for a health-care organization concerned about HIPPA requirements, for example.

And, while it can be more expensive to set up initially, a private cloud may deliver a higher ROI in the long run since you're not paying for ongoing shared services.

3 Hybrid Clouds: Balancing Complexity With Flexibility

Merging the flexibility of public cloud services with the control of a private cloud, a hybrid cloud can provide the ideal infrastructure for some organizations. A hybrid cloud enables you to put some of your apps and data – archives and e-mail, for instance – in a public cloud, and the remainder in your private cloud. This provides the cost savings and benefits of the public cloud while retaining the customization and security advantages of a private cloud.

While it can be more complex to deploy and manage than a pure public or private cloud, a hybrid cloud may deliver the best blend of control, flexibility and cost-effectiveness for some organizations.

So Which "Flavor" Is Right For You?

There is no perfect solution – each type of cloud has its own pros and cons. That being said, here are a few key factors to consider when determining the best approach for your particular business:

Public cloud solutions are best suited to the flexibility and budget requirements of smaller businesses that want access to the kind of IT resources that bigger organizations can afford, without the cost of development and ongoing support and management.

A private cloud, managed and supported by an in-house IT team, may be ideal for your organization if control and privacy are of paramount concern.

A hybrid cloud could be the ideal solution for any enterprise that wants to manage sensitive data in-house while availing itself of third-party software and data storage for uses where the data involved isn't as sensitive.

10 FEATURED PRODUCTS

THE LATEST TECHNOLOGIES

HP Power Back Pack can recharge your laptop on the go. The canvas bag has a 22,400mAh battery inside that provides a full charge to most HP laptops up to 17.3 inches, charges a tablet up to three times, and a smartphone up to 10 times.

The Power Backpack also lets you control the order in which your devices charge. There's also a built-in heat sensor that monitors the temperature to make sure the bag doesn't get too hot. A side-pocket plug-in makes the backpack easy to recharge.

The HP Power Backpack features ventilated and organized cable routing and meets security requirements for in-flight carry-ons.

http://store.hp.com/us/en/pdp/hp-powerup-backpack

Zillion the world's smartest and slimmest wallet that has Tile's location technology built right into its sleek design and a power bank which features a 2,500mAh battery and built-in cable, capable of fully charging your smartphone.

Tile is an application and RFID hardware device package, for Android (Google) and iOS (Apple) platforms that allow users to locate lost items via Bluetooth 4.0 radio technology.

https://www.zillionwallets.com/

Surface Studio is Microsoft's first desktop PC designed for the creative process. Featuring an adjustable 28-inch PixelSense™ Display with 13.5 million pixels to bring your ideas, images and drawing to life. Studio has a Zero Gravity Hinge that moves the display weightlessly from an upright angle, down to 20 degrees. It has an i5/i7 Intel® Core™ processors, up to 4GB NVIDIA® GeForce® dGPU and up to 32GB RAM. The studio comes with a keyboard, mouse, Surface Pen and an add-on Surface Dial.

https://www.microsoft.com/en-us/surface/devices/surface-studio/overview

SanDisk Ultra Dual USB Type-C Flash Drive features USB-C and USB-A connectors allowing easy and quick transfers between smartphones, tablets, and computer. The new SanDisk Ultra Dual-Drive USB Type-C Flash Drive can read speeds of up to 150 MB/s and comes in four different capacities: 16 GB, 32 GB, 64 GB and 128 GB.

It is also compatible with SanDisk's Memory Zone app available as a free download from Google Play™ store. It lets you view, access, and backup all the files from your phone's memory in one location.

https://www.sandisk.com/home/mobile-device-storage/ultra-dual-drive-usb-type-c

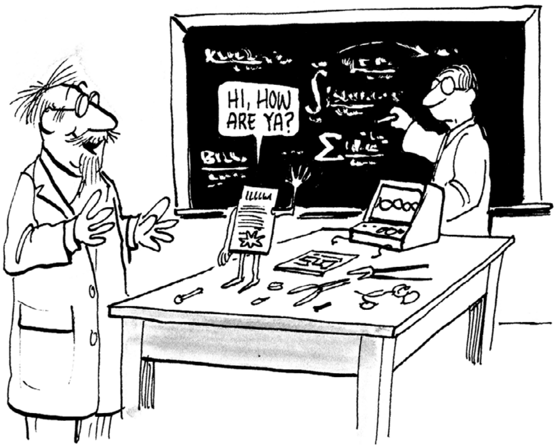
FREE 1 Hour IT Review for Your Business

Velocity Technology can provide qualifying businesses with a free 1 hour initial consultation to assess your current IT systems. We can examine your current IT systems and highlight any areas that could affect your business continuity or the productivity of your staff.

This is the perfect time to evaluate the state of your IT systems and position your company for increased efficiency and effectiveness in 2017!

Contact us today by emailing: **itreview@velocity-technology.com**

Or call us on **+852 2915 5096**



"At last, a fully interactive mailer."

"We do it to keep people from surfing all day."

Swimming with Alligators

A CEO throwing a party takes his executives on a tour of his opulent mansion. In the back of the property, the CEO has the largest swimming pool any of them has ever seen. The huge pool, however, is filled with hungry alligators. .

The CEO says to his executives "I think an executive should be measured by courage. Courage is what made me CEO. So this is my challenge to each of you: if anyone has enough courage to dive into the pool, swim through those alligators, and make it to the other side, I will give that person anything they desire. My job, my money, my house, anything!"

Everyone laughs at the outrageous offer and proceeds to follow the CEO on the tour of the estate. Suddenly, they hear a loud splash. Everyone turns around and sees the CFO in the pool, swimming for his life. He dodges the alligators left and right and makes it to the edge of the pool with seconds to spare. He pulls himself out just as a huge alligator snaps at his shoes.

The flabbergasted CEO approaches the CFO and says, "You are amazing. I've never seen anything like it in my life. You are brave beyond measure and anything I own is yours. Tell me what I can do for you.

The CFO, panting for breath, looks up and says, "You can tell me who pushed me in the pool!"

Have a Chance to Win a HK$200 Starbucks Gift Voucher

For this issue of the newsletter we will give away a HK$200 Starbucks Gift Voucher to the first correct email sent to **trivia@velocity-technology.com**.

The question for this issue is: **As an independent nation in the 2012 London Olympic Games, Hong Kong won a bronze medal in which event?**

Email us now with your answer!

Ransomware Is a Serious Threat to Your Business!

Ransomware comes in many forms. It is mostly spread by very clever and tricky emails but can also be spread by social media. A ransomware attack can happen to any business, and all it takes is a single employee to click on an attachment in an email or a link to an email or website, and your company can have at least one computer and possibly your server and backups encrypted. To get your files unencrypted will require you to pay a ransom.

Billions of dollars have been paid to ransomware criminals and billions more lost from downtime and impaired business function.

To protect your business from the threat of ransomware there are 3 things you must do!

1. Protect your network with technical security measures
2. Train yourself and your staff to be very, very careful about clicking anything in any email or social media contact, even if it looks like it is internal or an acquaintance.
3. Provide adequate backup for all your data. In the event of an attack you can quickly recover without paying a ransom or suffering much loss.

It is possible to be safe, but it requires expertise. We are here to help.

Act now and call us on **+852 2915 5096** or
email **security@velocity-technology.com**
to arrange a meeting time

Velocity Technology

Velocity Technology Limited
1802 Wan Chai Commercial Centre
194 Johnston Road
Wanchai, Hong Kong
(Hong Kong HQ since 1998)

www.velocity-technology.com