Productivity Enhancement and Protection
Improving Business IT Resilience
Graduated Benefits

2024-09-01

We understand that relatively recently a large Christchurch (NZ) Law Firm had its IT system made unusable for many days by computer malware.

It's clear to us that you're all doing the best possible with the defensive technologies available to you. But the continuing plague of malware outbreaks shows that those technologies are nowhere near effective enough.

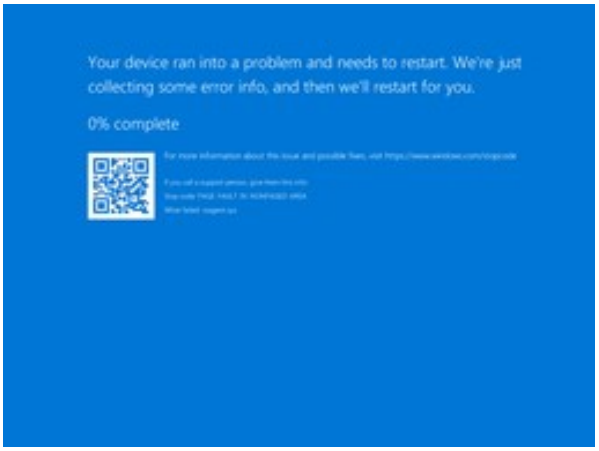
A reliable source has stated that only around 10% of invasions get publicly reported, so the risk is much higher than generally realised. Most victims apparently think it won't happen to them or that the effects will be minor. By the time they realise how disruptive it is it's too late to prevent major damage.

If you are another of the businesses that realise the true seriousness of the situation, the following 2 images and their accompanying text will resonate with you, and you will appreciate the business benefits of our insight and innnovation.

When malware invades a typical business IT system every desktop and server machine rapidly becomes disabled, and all data becomes unusable.

It's been likened to having a sudden heart attack followed by needing open-heart surgery.

The full effects of such sudden disruption are underestimated by most. Problems can easily persist for months, and the total cost is much higher than generally realised.



On 19th July 2024 a software update distributed by CrowdStrike resulted in boot-failure on a huge number of business Windows-running machines worldwide. Recovery took many days in many cases.

The risk of major disruption from security software is underestimated by most because it's not generally understood that it needs to be given privileged access. Which enables it to be as disruptive as malware.

As you know, maintaining your business's operational flow is what really matters, and our scheme can deliver that for you.

One unique aspect is that we assume that disruptive software will invade a business's IT system, and so our scheme has appropriate adaption capabilities.

It involves a more resilient way of organising and operating your existing IT system. Enabling your business to continue to operate regardless. One key aspect of it is the IT equivalent of the principle that biological diversity is good because it prevents a disease wiping out an entire species.

Our resilience scheme gives you control. You decide how much benefit to get, and how much downtime there'll be when disruptive software invades. It gives you competitive advantage via publicising your exceptional commitment to system resilience and safety.

Imagine how comfortable you and the rest of your staff will feel once you all know how little effect a disruptive-software outbreak can have with the things below in play.

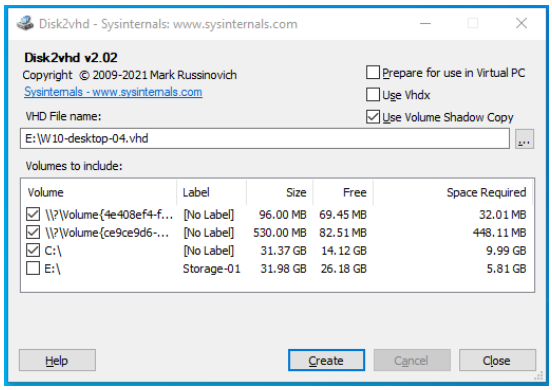
You're free to implement as much of the scheme as you wish yourselves, or to enlist the help of us or appropriate other companies for parts of it.

The following are the major components of our approach. The technical aspects of the descriptions are intended for your IT support people :

Using Virtual Machines

Typically businesses have MS-Windows installed directly on machines. So when Windows-targeted malware or faulty security software invades, all of a machine's software functionality is disabled.

A Hypervisor is software that virtualises computer hardware to create Virtual Machines (VMs). Installing Windows on a VM works the same as installing it on actual hardware, as does using it. Typical modern machines can run multiple VMs simultaneously.



Conversion of installed Windows systems to VMs is straightforward using the free program Disk2VHD which can be downloaded from Microsoft.

It's much easier to manage Windows that's running on a VM rather than on the actual hardware.

When disruptive software invades Windows that's running on a VM, only that VM is affected.

To speed up recovery from invasion you can set up replacement Windows VMs ahead of time and under low pressure. Then copy each to the relevant machine at the appropriate time later. Preferably prepare them on isolated VM Maintenance Machines so that malware or disruptive updates can't get to them.

So just changing to using VMs can reduce downtime. But with Windows VMs you have to wait until Windows malware is definitely gone from the entire business IT system before trying to resume operations.

Also note that if you use MS's Hyper-V it's possible that Windows malware or faulty security software will affect it too. Meaning that for safety all the software that runs directly on the machine should be reinstalled, further delaying resumption of operations.

Or you can enjoy the benefits of using an Enterprise-Linux-based Hypervisor, which is naturally immune to Windows malware. The component parts are free to download and use, and you can install and customise them. As an alternative we offer a service that creates customised versions and installs them remotely.

Further information : https://iopen.co.nz/docs/virtual_machines.pdf

Desktop Fallback

With a VM-based system, on desktop machines have available an additional VM that runs an Alternative Desktop system which is immune to Windows malware and which can also keep operational data flowing.

The desktop that we use and recommend is as easy to get to grips with as a new car is.

So when Windows-disruptive software invades your desktop Windows VM you can switch to the Alt-Desktop VM and continue working, even with the disrupt still around.

If a desktop machine has enough memory (RAM) you can run both VMs simultaneously, and easily switch between them using keyboard hot-keys.

Which enables work to be done routinely on the Alternative Desktop, and reduces the amount of work-switching that has to be done when Windows-disruption happens.

We recommend Fedora Linux MATE (mah-tay) for the Alternative Desktop, since it comes with the superb SELinux security module enabled. You can download and install and customise it. Again as an alternative, our service offerings include supplying customised VMs that run it.

Further information : https://iopen.co.nz/docs/desktop-fallback.pdf

Malware Defeating File Sharer

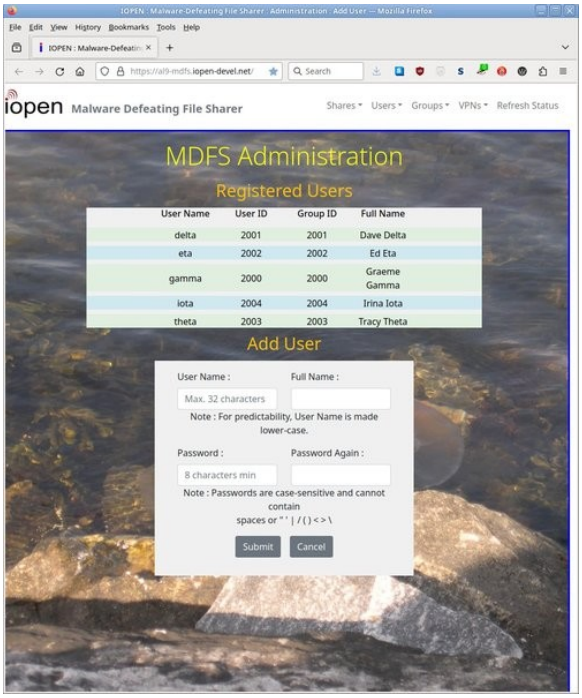
A Windows-compatible file sharer. Supplied as a VM.

MDFS complements Desktop Fallback by remaining operational and thus able to provide Alternative Desktops with operational data.

Malware on Windows desktops can attack files in shares that the desktops are connected to, so MDFS runs software developed by us that defeats such attacks.

MDFS is based on an Enterprise Linux (EL) and so it is naturally immune to Windows malware. It's protected from other malware by security sub-system SELinux that, amongst its many capabilities, defeats unknown threats. There's also a highly capable firewall. It doesn't need other security software and so is not vulnerable to the sort of event which caused the major outage of 19th July 2024.

MDFS also enables having file shares that only Alternative Desktops can access. Perhaps store critical or ultra-sensitive data in such shares, so Windows malware can't access or affect it in any way.



You can gradually evolve your use of our scheme under low pressure so when an invasion happens your staff can make a smooth and rapid transition to full-Fallback.

Furthermore, if on your network you organise machine addresses appropriately, then it's straightforward for us to make the MDFS firewall able to deny access from Windows machines whilst allowing access from Alternative Desktop machines.

So that during a Windows malware outbreak it's possible to prevent the malware interfering in any way with the continuing operations.

Further information : https://iopen.co.nz/docs/mdfs-client-experience.pdf
https://iopen.co.nz/docs/mdfs-structure.pdf
https://iopen.co.nz/ws_opdataflow.html

Data Backups with Maximum Safety and Availability

Although MDFS effectively defends your data, there's always the possibility of hardware failure, so frequent automatic backups are vital.

In making backups we use the safer 'pull' method.

See : https://iopen.co.nz/docs/backup_overview.pdf

We think it's vital for businesses to retain control of their operational data, meaning keeping it, and backups of it, on hardware that they own. Keep your operating data close and your backups of it safely-close.

Thus we recommend in-house backing-up to at least 2 devices located in the homes of managers or executives, or in other offices of the business. Those devices automatically pull data from MDFS and other office servers via a dedicated VPN.

We also offer a service that does secure backing-up to our backup servers in case a business wants extra assurance. It can be used in addition to the in-house variant.

See : https://iopen.co.nz/docs/backup_options.pdf

Note that our MDFS has a dedicated backup channel (a dedicated VPN), which improves security and also avoids legitimate backup runs degrading the checking for signs of malware doing file exfiltration.

For VM-based systems there's a backup option called a warm-spare VM, and we've documented how to create and maintain them.

See : https://iopen.co.nz/docs/vm-warm-spare.pdf

Linux

You and your IT support people need not be concerned about the introduction of Linux into your business. It's simpler and can be used much more securely than Windows, and even Microsoft are promoting its use.

It also runs many devices, including ones in motor vehicles, and very likely you have devices that use it.

Your IT support people will benefit from learning how Linux can boost system security. Especially via security module SELinux, with its ability to defeat unknown threats when operating in Enforcing mode.

We use and provide Enterprise Linux variants AlmaLinux or Rocky Linux for all server-like situations because by default they have SELinux:Enforcing. For desktops it's either Fedora Linux MATE or Rocky Linux MATE. Both have SELinux:Enforcing.

MS-Windows doesn't have anything even close to SELinux's capabilities, and it shows.

Basis Of Our Charges

Almost all of the software involved in this scheme has a Free Software licence. Free as in freedom to copy and install and use. As with all IT systems there is a need to select the appropriate software packages and configure them appropriately after installation.

Thus the basis of our charging is similar to that of lawyers and accountants. In principle your business can do all its legal and accounting work itself, but you outsource the work to them in order to benefit from expertise and reduce the risk of mistakes, and pay the resulting significant fees.

If you use this operational-flow-maintaining scheme at close to maximum benefit you can expect very rapid payback after a Windows malware outbreak starts.

At an appropriate point we will commence donating a percentage of our profits to relevant Free Software projects.

If you decide to do some of the work yourselves it's vital to download Free Software packages from official servers. Some packages downloadable from non-official servers have been modified in unacceptable ways.

When we're involved there's 3 levels of users for our Resilience Improvement scheme components. Enquire for details : https://iopen.co.nz/ws_contact.html

Software that we develop which has security implications is licenced to individual clients, and we provide them with a copy directly. To prevent the distribution of corrupted or backdoored copies.

Our Motivation For Producing This

We want businesses to achieve better outcomes, regardless of whether we're directly involved in making them happen. Such outcomes can produce effects that benefit many, including ourselves.