

ANDERSON MORGAN PRESENTS

SERVER

**DISASTER
RECOVERY**

VS

**BUSINESS
CONTINUITY**



**OCT 17
WEDNESDAY**

WILL YOUR COUNCIL SURVIVE WITHOUT IT?

OPEN 5PM | **ENTRY** \$10 | **FIRST FIGHT** 8PM

FOR MORE INFORMATION: 555-555-5555 / YOUREMAIL@EMAIL.COM

102 BOXING STREET, DEVONPORT, TAS 7320

PARNAPLE



Anderson Morgan
BUSINESS ENABLED

Andrew Roberts

Sales & Marketing Manager

andrew.roberts@andersonmorgan.com.au

Nic Paley

Account Manager

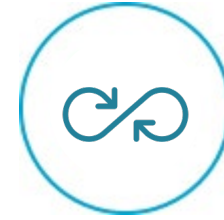
Nicholas.paley@andersonmorgan.com.au



**Managed
IT Support**



**Digital
Security**



**Disaster
Recovery**



**Hardware &
Software Sales**



**Cloud,
SAAS & IAAS**



**Strategic ICT
Consulting**

HOBART | LAUNCESTON | ULVERSTONE
andersonmorgan.com.au
1300 557 312

A decorative background on the left side of the slide consisting of a complex, low-poly geometric pattern in various shades of blue, ranging from light sky blue to a deeper cerulean.

Disaster Recovery vs Business Continuity

What's the Difference?

Abstract, flowing shapes in light blue and cyan colors located in the bottom right corner of the slide, resembling stylized waves or smoke.



Kultar Khatra

Sr. Channel Manager – VIC/SA/TAS

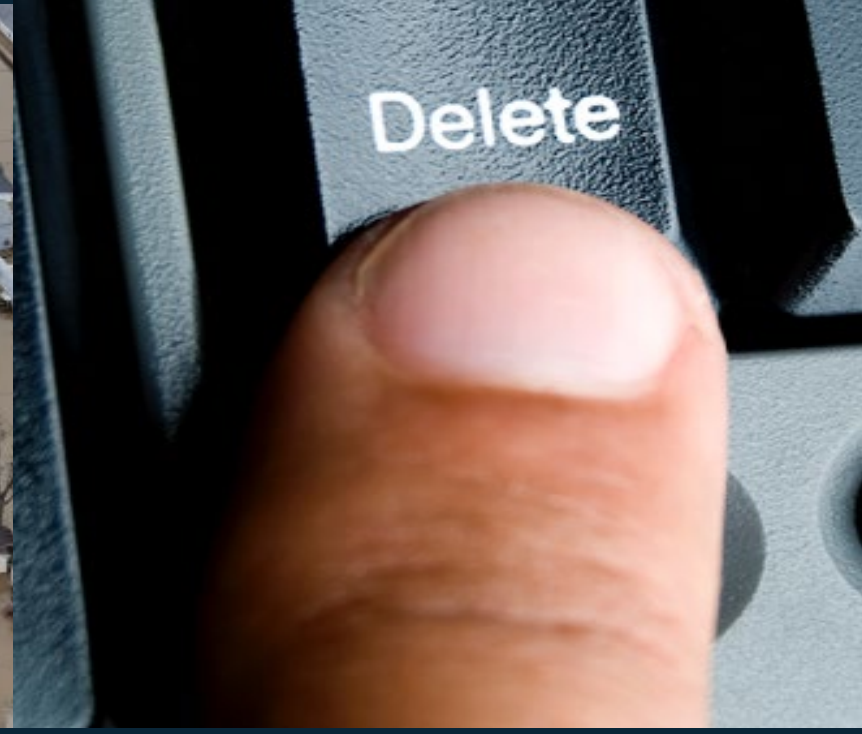
kkhatra@datto.com

[linkedin.com/in/kultarkhatra](https://www.linkedin.com/in/kultarkhatra)

A photograph of a city street completely flooded with water. In the background, there are several buildings: a modern glass-fronted building on the left, a multi-story brick building in the center, and a tall blue and white checkered skyscraper on the right. Lush green trees line the right side of the street. The water in the foreground is dark and reflects the surrounding buildings and trees, with ripples visible. The text "This isn't the only disaster..." is overlaid in white with a black outline across the middle of the image.

This isn't the only disaster...

HOW MANY PEOPLE HAVE EXPERIENCED THESE DISASTERS?



Most Commonly Seen

68% of downtime incidents

HUMAN
ERROR

RANSOMWARE

Booming
threat

One of the
most common

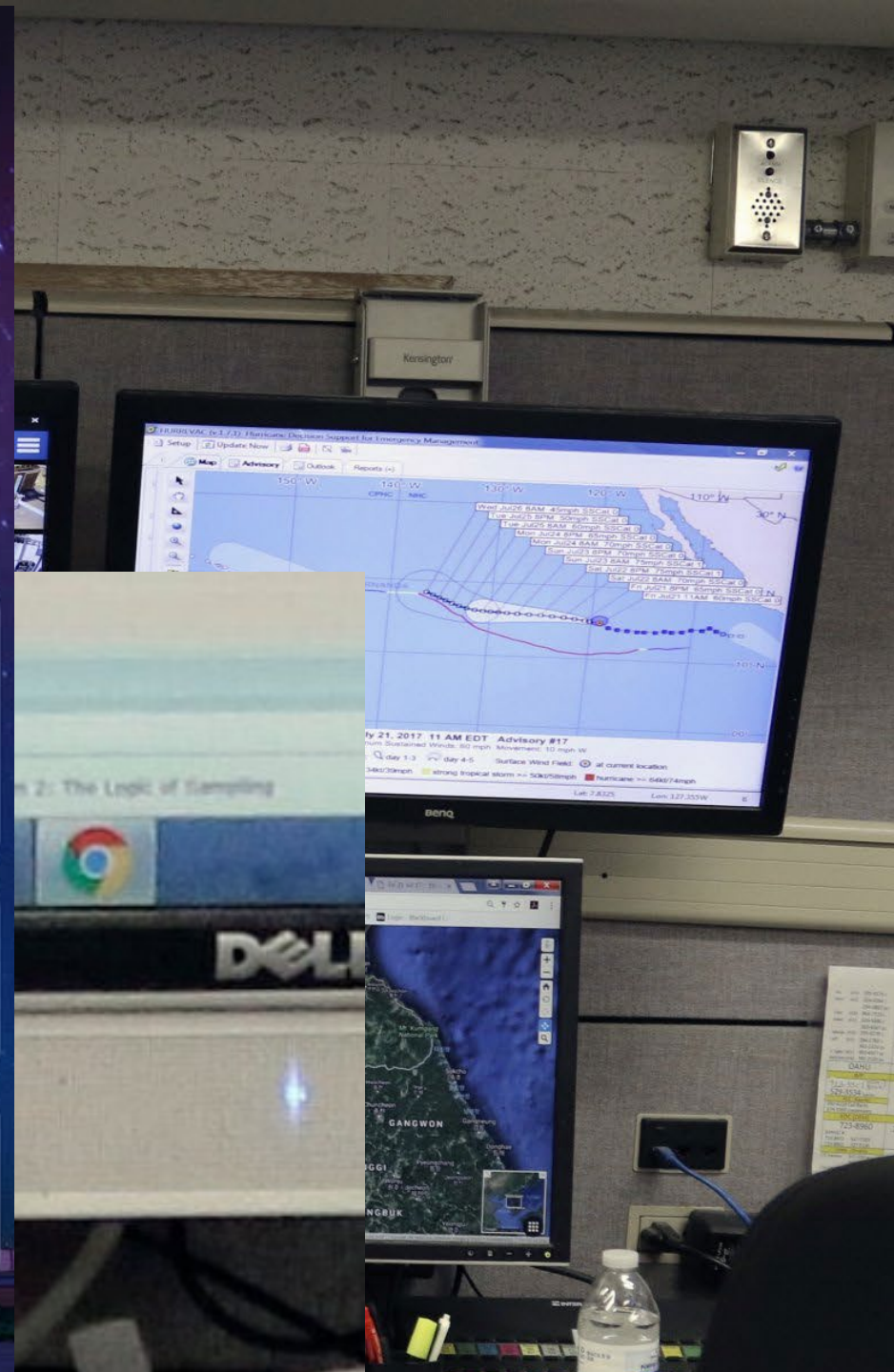
HARDWARE
FAILURE

SECURITY
INCIDENTS

Consistent Threats

NATURAL
DISASTER

<10% of downtime
incidents



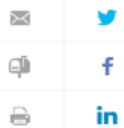
Crypto/Ransomware

www.abc.net.au/news/2014-01-16/australian-pharmacies-targeted-in-ransomware-attacks/5203970

Fake Aussie AGL bill phishing continues

By Michael Jenkin
Oct 20 2014
7:00AM

0 Comments



RELATED ARTICLES

10,000 Australians hit by energy bill ransomware

Ransomware offers live chat 'help'

Crysis ransomware attacking Australian businesses

Australians continue to be targeted by email-enabled ransomware ploys, with renewed reports of malware being spread by posing as energy provider AGL's bills.

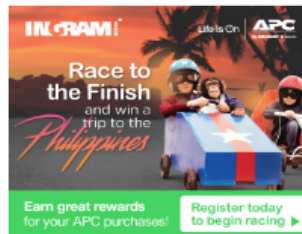
An alert provided by the government's Stay Smart Online website marks the second time in recent memory a ransomware campaign has struck under the guise of an energy bill.

In June at least 10,000 people had reported being scammed by emails looking like AGL bills.

According to a blog post on Aussie cloud security provider Mailguard's website, the newest phishing attempt includes references to recent storms and flooding.

"In an effort to appear legitimate, the email says flooding victims may receive additional support to help pay their bill," poster Jaclyn McRae wrote.

"Those who make the mistake of clicking a link on the fake invoice



Crysis ransomware now attacking businesses in Australia and New Zealand

by Greg Masters | Wednesday 21 September 2016 | 1 Comment



The Sydney Morning Herald

Digital Life

Latest News Gadgets Science Innovation Web Culture Gaming Security IT Pro

You are here: Home » Technology »

'Locky' ransomware scam hits tens of thousands of Australian computers

March 11, 2016

NEWS

Cyber attacks: pharmacies, patient records targeted 'ransomware' attacks

By technology reporter Jake Sturmer and Alison McClymont

Updated 17 Jan 2014, 5:27pm

Pharmacists have become the latest targets of sophisticated computer hacks known as ransomware attacks, which lock up PCs until victims pay up.

Once the hackers plant the virus, the files on a computer become encrypted and unable to be accessed.

Sorry, this video has expired

VIDEO: Ransomware attacks target pharmacies (ABC News)



Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

CMT from Mondays to Fridays

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

Autotask

Your personal files are encrypted



Info

Your **important files were encrypted** on this computer: photos, videos, documents, etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key **RSA-4096** generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption**

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

If you see the main locker window, follow the instructions on the locker. Otherwise, it's seems that you or your antivirus deleted the locker program. Now you have the last chance to decrypt your files.

Open <http://jssestaew3e7ao3q.onion.cab> or <http://jssestaew3e7ao3q.tor2web.org> in your browser. They are public gates to the secret server.

If you have problems with gates, use direct connection:

1. Download Tor Browser from <http://torproject.org/>
2. In the Tor Browser open the <http://jssestaew3e7ao3q.onion/>
Note that this server is available via Tor Browser only. Retry in 1 hour if site is not reachable.

← → ↺ www.cso.com.au/article/562658/over-9-000-pcs-australia-infected-by-torrentlocker-ransomware/

prints.

Restoring your files - The fast and easy way

To get your files fast, please transfer **1.0 Bitcoin** to our wallet address **1LEiPgvh6S9VEXWV2dZTytSRd7e9B1bWt3**. When we will get the money, we will immediately give you your private decryption key. Payment should be confirmed in about 2 hours after payment made.

Restoring your files - The nasty way

Send the link below to other people, if two or more people will install this file and pay, we will decrypt your files for free.

<https://3hnuhydu4pd247qb.onion.to/r/0e72bfe849c71dec4a867fe60c78ffa5>

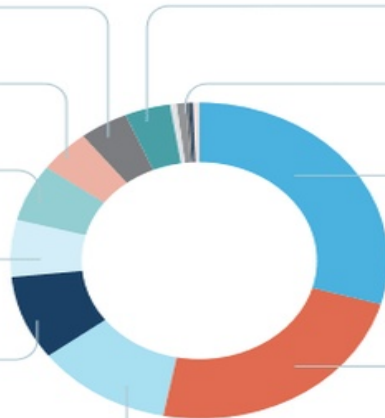
1,683
SPAIN

1,777
UNKNOWN

2,287
NETHERLANDS

2,329
UNITED KINGDOM

3,420
CZECH REPUBLIC



1,504
AUSTRIA

11,700
TURKEY

9,415
AUSTRALIA

314
FRANCE
240
GERMANY
180
NEW ZEALAND
133
CANADA
112
IRELAND

CHINA NEWS

Alleged Chinese Hacking: Alcoa Breach Relied on Simple Phishing Scam

“...At least one employee will click on anything.”

Alcoa Inc. AA -2.92% board member.

But Mr. Ghosn's name was slightly misspelled, and the attachment, billed as the agenda to a 2008 shareholders' meeting, actually held a computer virus that allowed Chinese hackers to allegedly steal nearly 3,000 emails, according to a federal indictment unsealed Monday.

The indictment makes the case, with an unusual level of detail, that many foreign cyberattacks often don't rely on sophisticated hacking technology. Rather, it says, the hackers primarily used an old trick, known as phishing—baiting a user to download malicious code allowing outsiders to spy on the machine. The charges illustrate an age-old security problem for U.S. companies: At least one employee will click on anything.

The latest ransomware is pure evil genius

Popcorn Time ransomware melds social engineering with technology to spread itself faster than ever



Credit: [Dbreen via Pixabay](#)

Ransomware is always nasty business, but the latest variant discovered by the [MalwareHunterTeam](#) takes the nastiness to a whole 'nother level.

Turning victims into criminals

Apparently, [the latest Popcorn Time ransomware adds a new twist to the standard M.O.](#) of demanding payment from their victims or permanently lose access to their

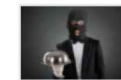
RELATED



Much ado about the ransomware scourge



Stupid encryption mistakes criminals make



Ransomware as a Service fuels explosive growth



VIDEO
Setting up DLP features for email security.

Terrifying 'Popcorn Time' computer virus can only be removed by infecting **TWO FRIENDS** or paying a ransom

- Access to decryption key given after paying in Bitcoin or nominating two others
- Ransomware shares a name with programme that downloads and streams films
- Hackers claim to be using proceeds for 'food, medicine and shelter to those in need'

By [LIBBY PLUMMER FOR MAILONLINE](#)

PUBLISHED: 10:16 EDT, 12 December 2016 | **UPDATED:** 18:28 EDT, 12 December 2016



78
shares

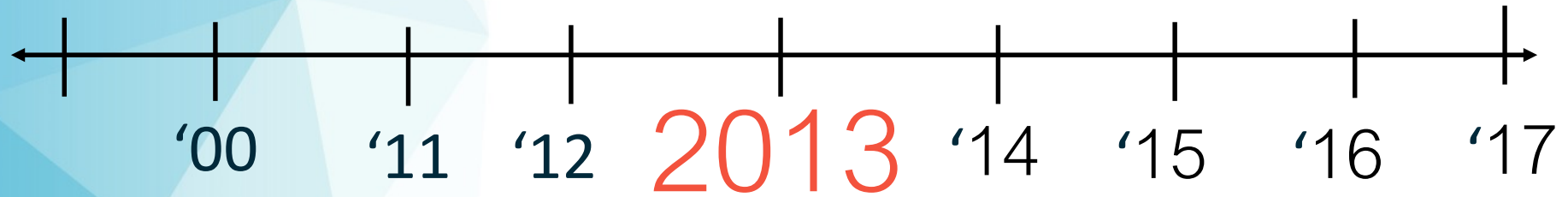
 **21**
[View comments](#)

A menacing new computer virus leaves victims with a choice between paying hackers a ransom and infecting two friends' computers.

BC



AC



VIC/TAS is under attack

Petya cyber attack: Cadbury ch

<https://www.abc.net.au/news/2017-06-28/cadbury-chocolate-factory-tasmania-hit-by-ransomware>

Petya cyber attack: Cadbury chocolate Tasmania hit by ransomware

ABC Radio Hobart

Updated 28 Jun 2017, 4:55pm



PHOTO: A Cadbury computer under ransomware attack. (Twitter: Leon Compton)

The Tasmanian Cadbury chocolate factory has been targeted by a ransomware attack which is affecting the company's IT system.

RELATED STORY: [Global ransomware attacks](#)

Production at the company's Claremont facility was halted when the computer system went down at 9:30pm on Tuesday in what was described as a "cyber attack".

The incident comes as a [global malware attack is rolling out across the globe](#), with Russia's biggest oil company, disrupting operations at Ukrainian banks and sh

<https://www.examiner.com.au/story/6421785/newstead-hair-systems-hacked-bookings-lost/>

Home / News / Local News

OCTOBER 4 2019 - 4:00PM

Newstead Hair systems hacked, bookings lost



Kasey Wilkins

Local News

[f SHARE](#) [TWEET](#) [Email](#)



Newstead Hair stylist Caitlin Harback and manager Gabby Gibbons. Picture: Paul Scambler

Patrons of Newstead Hair are asked to get in touch with the salon.

The salon has been experiencing technical difficulties since Thursday after their systems were hacked.

Ad closed by Google

datto

The Nation – is at risk

12:51 31 4G 67%

← Google News

≡ **NEWS** → SHARE

IMAGE: Scott Morrison said a "sophisticated state actor" was behind the breaches earlier this month.
(ABC News: Jed Cooper)

Prime Minister Scott Morrison has said the computer servers of Australia's major political parties were hit by a recent cyber attack.

He updated the House of Representatives on the issue this morning, saying there was no evidence of electoral interference.

Mr Morrison said the nation's cyber security agencies believed a "sophisticated state actor" was behind the attacks.

The impact to political parties was uncovered during an investigation of a breach of Parliament House's computer servers earlier this month.

More to come.

betootaadvocate

≡ The  BETOOTA ADVOCATE 🔍



PM Reveals Parliament Cyber Attack Happened Because Nobody Updated Norton Internet Security

Ransomware attack hit San Francisco train system



Elizabeth Weise, USATODAY

11:29 a.m. EST November 29, 2016



The San Francisco Municipal Transportation Agency has contained a cyber attack that disrupted its ticketing systems over the Thanksgiving weekend. USA TODAY



SAN FRANCISCO — A ransomware attack took ticket machines for San Francisco's light rail transit system offline all day Saturday during one of the busiest shopping weekends of the year, but rather than shutting down, the agency decided instead to let users ride for free. By Sunday the system was once again running normally.

Kenmore.
Be Amazing™

come home to Kenmore® for
**reliability, service
and performance**

shop Kenmore laundry

Trusted by American families for over 100 years.



HOW MUCH DID IT COST...

- ▶ They did not pay the \$73k in ransom (100 bitcoins) because they had proper backups
- ▶ However....
 - ▶ They did not have a continuity solution
 - ▶ Down 2 days (Friday & Saturday)
 - ▶ 735,000 rides a day offered for free
 - ▶ \$2.25 per ride

Lost \$1.65 million per day in revenue

A decorative background on the left side of the slide consisting of overlapping, semi-transparent blue triangles of various shades, creating a low-poly or mosaic effect.

BEYOND THE NUMBERS

- ▶ Reputation and Brand Damage
- ▶ Compliance and legal Implications
- ▶ Notifiable Data Breach Act (oaic.gov.au)
- ▶ Customer Retention
- ▶ Employee Productivity/Retention
- ▶ Peace Of Mind

NDBA - Background

- Came into effect on February 22, 2018
- Conducted by the Office of the Australian Information Commissioner (OAIC)
- Strengthens Australia's privacy laws
- 812 data breach notifications reported in 2018
 - 33% Human Error – 64% Malicious Attacks



Australian Government

**Office of the Australian
Information Commissioner**

Notifiable Data Breaches Quarterly Statistics Report

1 April – 30 June 2018

oaic.gov.au

NDBs 2018/2019

Quarter	Number of Notified Breaches	Human Error	Malicious/ Criminal Attacks	System Error
Q3 2018	245	37%	57%	6%
Q4 2018	262	33%	64%	3%
Q1 2019	215	35%	61%	4%
Q2 2019	245	34%	62%	4%

= 812 notified breaches in 2018

= 460 in Q1 + Q2 in 2019

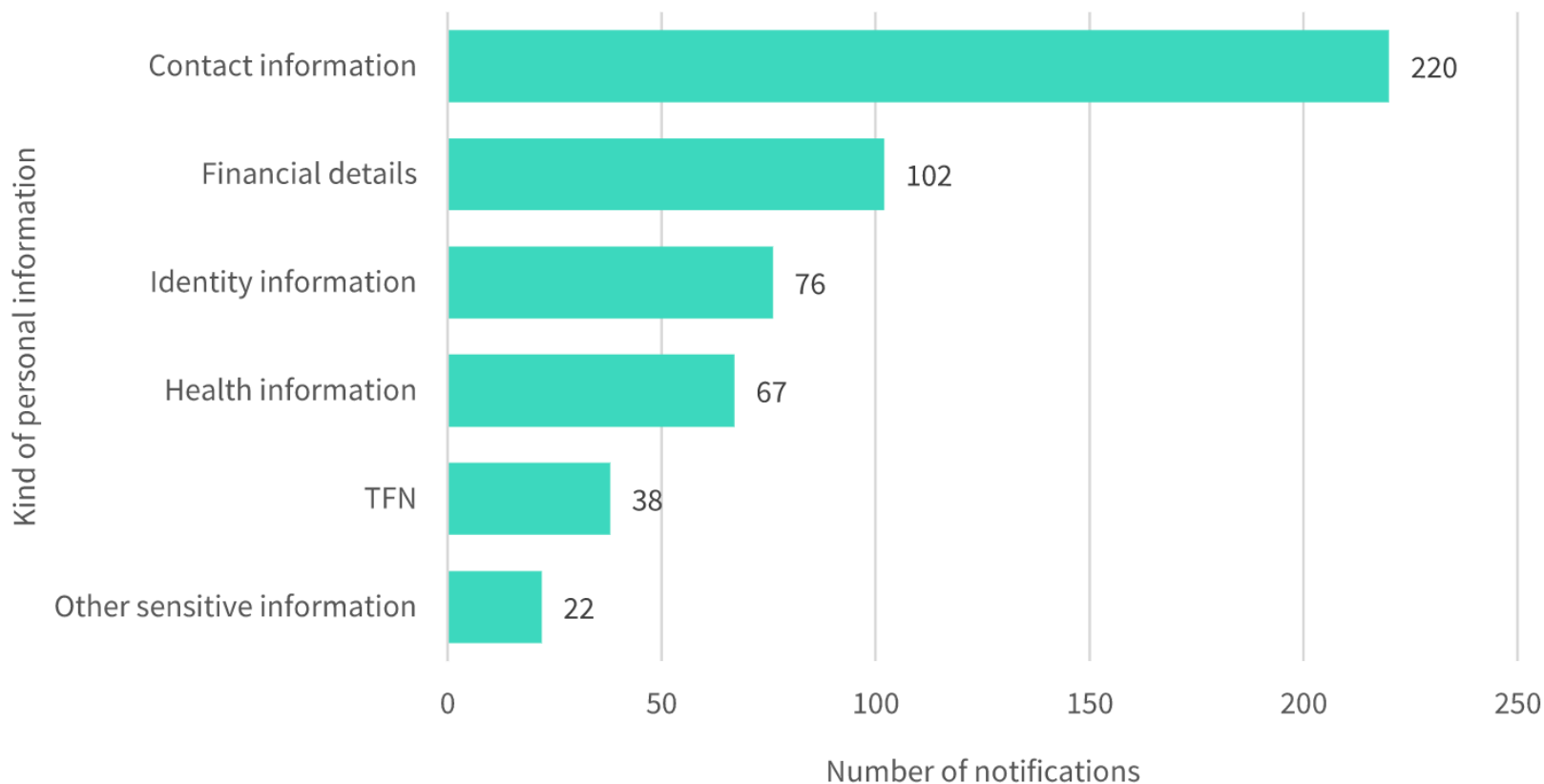
(On average 18 reported breaches p/week to OAIC)

<https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/>

Kinds of Personal Information Involved in Breaches

Q2 2019

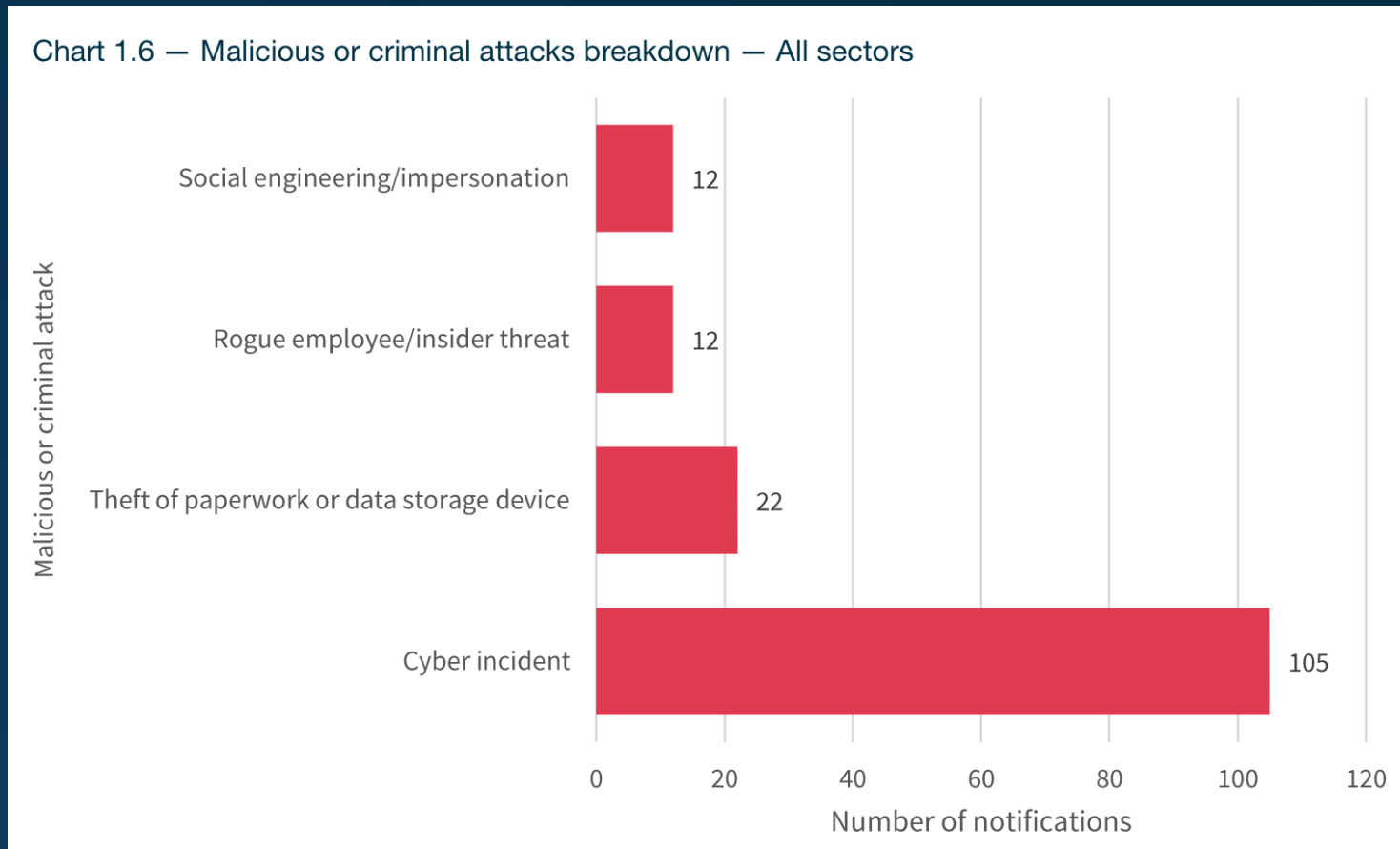
Chart 1.3 — Kinds of personal information involved in data breaches by number of notifications — All sectors



Note: Data breaches may involve one or more kinds of personal information.

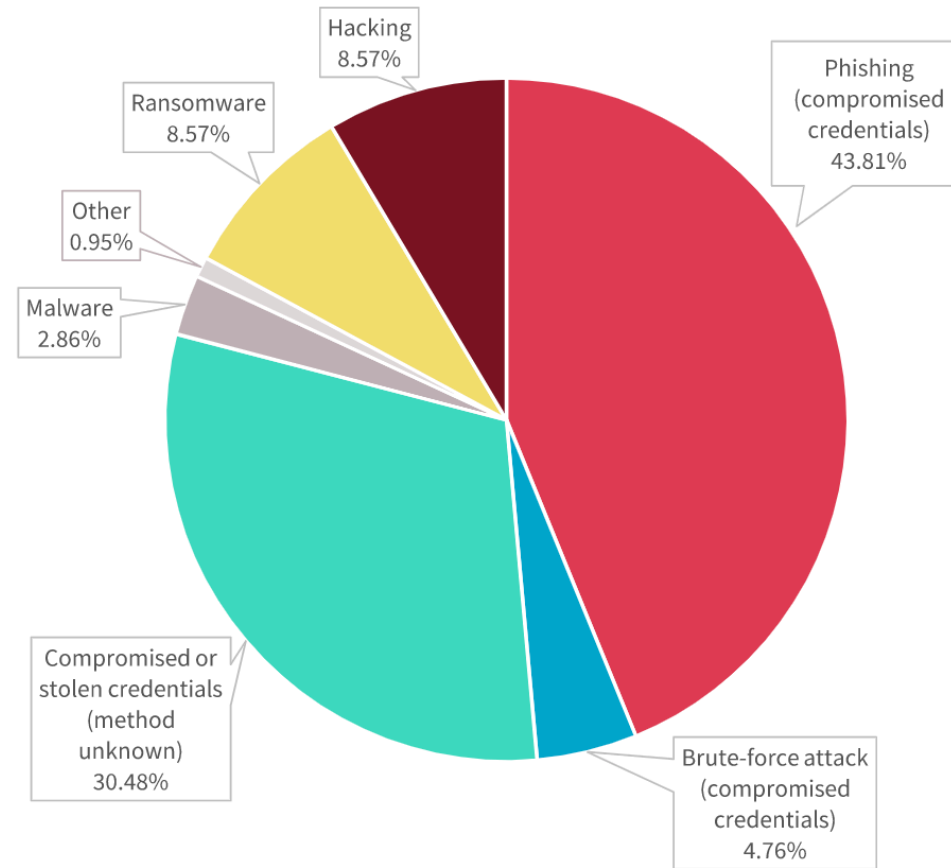
Q2 2019 - Cyber Incident Breaches

Malicious/Criminal Attack breakdown



Q2 2019 - Cyber Incident Breaches

Chart 1.7 — Cyber incident breakdown — All sectors



[Chart 1.7: Long text description](#)



Essential Eight Maturity Model

FEBRUARY 2019

Introduction

The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies, in the form of the ***Strategies to Mitigate Cyber Security Incidents***, to help organisations mitigate cyber security incidents caused by various cyber threats. The most effective of these mitigation strategies are known as the Essential Eight.

Maturity levels

To assist organisations in determining the maturity of their implementation of the Essential Eight, three maturity levels have been defined for each mitigation strategy. The maturity levels are defined as:

- Maturity Level One: Partly aligned with intent of mitigation strategy
- Maturity Level Two: Mostly aligned with intent of mitigation strategy
- Maturity Level Three: Fully aligned with intent of mitigation strategy.

Essential Eight Maturity Model

Mitigation Strategies to Prevent Malware Delivery and Execution

Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.

Why: All non-approved applications (including malicious code) are prevented from executing.

Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.

Why: Microsoft Office macros can be used to deliver and execute malicious code on systems.

Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.

Why: Security vulnerabilities in applications can be used to execute malicious code on systems.

User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.

Why: Flash, ads and Java are popular ways to deliver and execute malicious code on systems.

Mitigation Strategies to Limit the Extent of Cyber Security Incidents

Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.

Why: Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems.

Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.

Why: Security vulnerabilities in operating systems can be used to further the compromise of systems.

Multi-factor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.

Why: Stronger user authentication makes it harder for adversaries to access sensitive information and systems.

Mitigation Strategies to Recover Data and System Availability

Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.

Why: To ensure information can be accessed following a cyber security incident (e.g. a ransomware incident).

Essential Eight Maturity Model

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Application whitelisting	An application whitelisting solution is implemented on all workstations to restrict the execution of executables to an approved set. An application whitelisting solution is implemented on Active Directory servers, email servers and other servers handling user authentication to restrict the execution of executables to an approved set.	An application whitelisting solution is implemented on all workstations to restrict the execution of executables and software libraries to an approved set. An application whitelisting solution is implemented on Active Directory servers, email servers and other servers handling user authentication to restrict the execution of executables and software libraries to an approved set.	An application whitelisting solution is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set. An application whitelisting solution is implemented on Active Directory servers, email servers and other servers handling user authentication to restrict the execution of executables, software libraries, scripts and installers to an approved set.
Patch applications	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within two weeks of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. An automated mechanism is used to confirm and record that deployed application and driver patches or updates have been installed, applied successfully and remain in place. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.
Configure Microsoft Office macro settings	Microsoft Office macros are allowed to execute, but only after prompting users for approval. Microsoft Office macro security settings cannot be changed by users.	Only signed Microsoft Office macros are allowed to execute. Microsoft Office macros in documents originating from the Internet are blocked. Microsoft Office macro security settings cannot be changed by users.	Microsoft Office macros are only allowed to execute in documents from Trusted Locations where write access is limited to personnel whose role is to vet and approve macros. Microsoft Office macros in documents originating from the Internet are blocked. Microsoft Office macro security settings cannot be changed by users.
User application hardening	Web browsers are configured to block or disable support for Flash content. Web browsers are configured to block or disable support for Flash content. Web browsers are configured to block web advertisements.	Web browsers are configured to block or disable support for Flash content. Web browsers are configured to block or disable support for Flash content. Web browsers are configured to block web advertisements.	Web browsers are configured to block or disable support for Flash content. Web browsers are configured to block or disable support for Flash content. Web browsers are configured to block web advertisements.
Restrict administrative privileges	Backups of important information, software and configuration settings are performed at least daily. Backups are stored offline, or online but in a non-rewritable and non-erasable manner. Backups are stored for three months or greater.		
Patch operating systems	Full backup and restoration processes are tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.		
Multi-factor authentication	Partial backup and restoration processes are tested on an annual or more frequent basis.		
	software certificates.	six or more characters, Universal 2nd Factor (U2F) security keys, physical one-time password (OTP) tokens, biometrics, smartcards or mobile app OTP tokens.	repositories. Multi-factor authentication uses at least two of the following authentication factors: passwords with six or more characters, Universal 2nd Factor (U2F) security keys, physical one-time password (OTP) tokens, biometrics or smartcards.
Daily backups	Backups of important information, software and configuration settings are performed monthly. Backups are stored for between one to three months. Full backup and restoration processes are tested at least once.	Backups of important information, software and configuration settings are performed weekly. Backups are stored offline, or online but in a non-rewritable and non-erasable manner. Backups are stored for between one to three months. Full backup and restoration processes are tested at least once. Partial backup and restoration processes are tested on an annual or more frequent basis.	Backups of important information, software and configuration settings are performed at least daily. Backups are stored offline, or online but in a non-rewritable and non-erasable manner. Backups are stored for three months or greater. Full backup and restoration processes are tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur. Partial backup and restoration processes are tested on an annual or more frequent basis.

WHY SaaS PROTECTION?



**1 in 3 COMPANIES
HAVE EXPERIENCED
DATA LOSS IN SaaS
APPS**

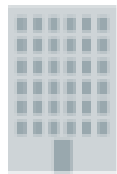


THE SHARED RESPONSIBILITY MODEL

Microsoft provides for the security of the cloud, and the tenant (partner) provides the security in their cloud.

SaaS VENDORS DON'T PROTECT USER DATA

Data Protection Responsibilities



Microsoft

Application • OS • Virtualization
Hardware • Network



MSP

Users • Data • App Admin



Hardware
Failure



Software
Failure



Natural
Disaster



Power
Outage



Human
Error



Programmatic
Errors



Malicious
Insiders



External
Hackers

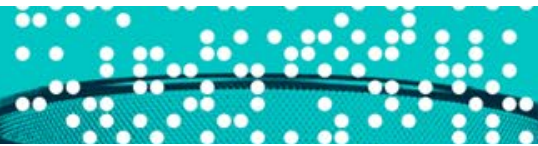


Viruses/
Malware



Step 1: Make sure you have a backup of your files

We cannot guarantee that you will be able to recover your data.



As recommended by the Microsoft Malware Protection Center (MMPC) in their “Backup the best defense against (Cri)locked files” blog post, you should back up your files on a regular basis by enabling System Restore, using manual syncing methods, or even by manually moving your files to a separate drive.

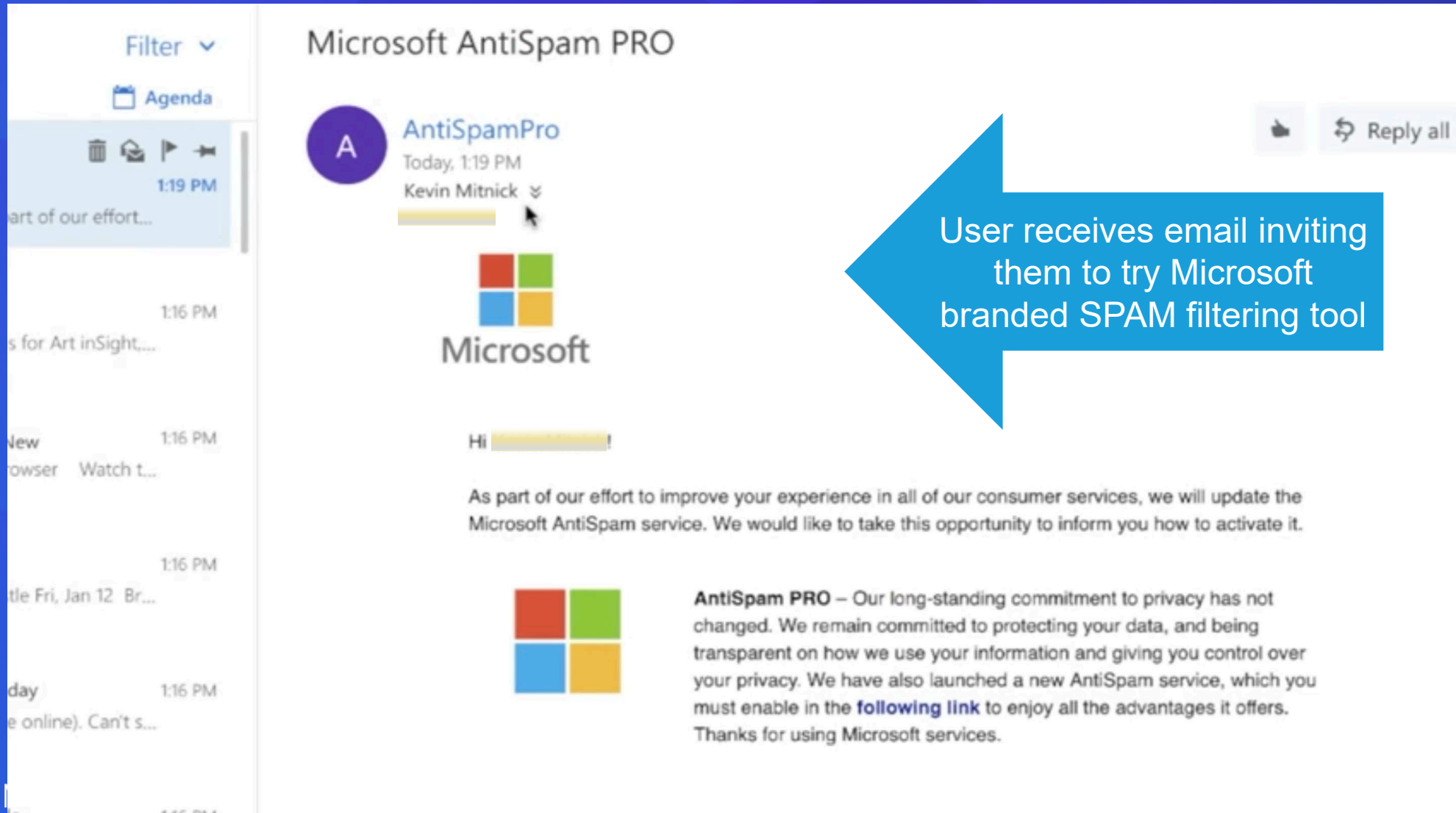
We recommend that your backups are kept in an external, non-mapped or not synced storage.



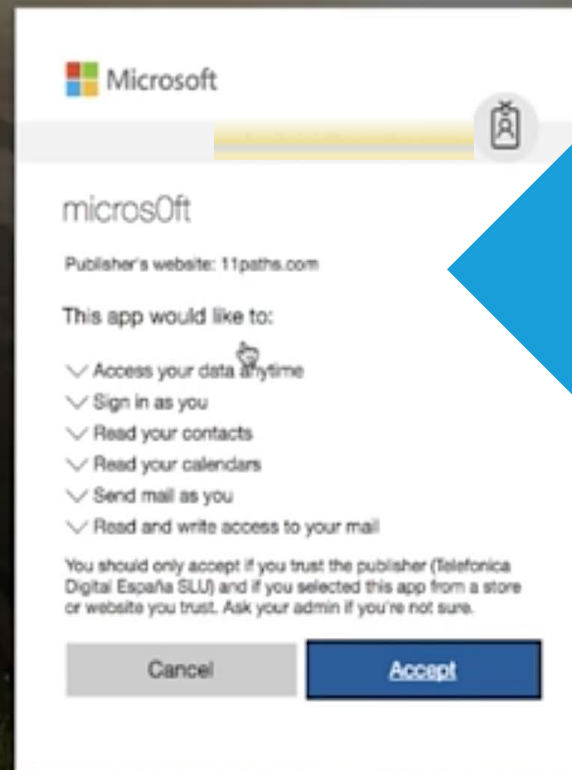
RANSOMCLOUD



HOW HACKERS INFECT OFFICE 365 WITH RANSOMWARE

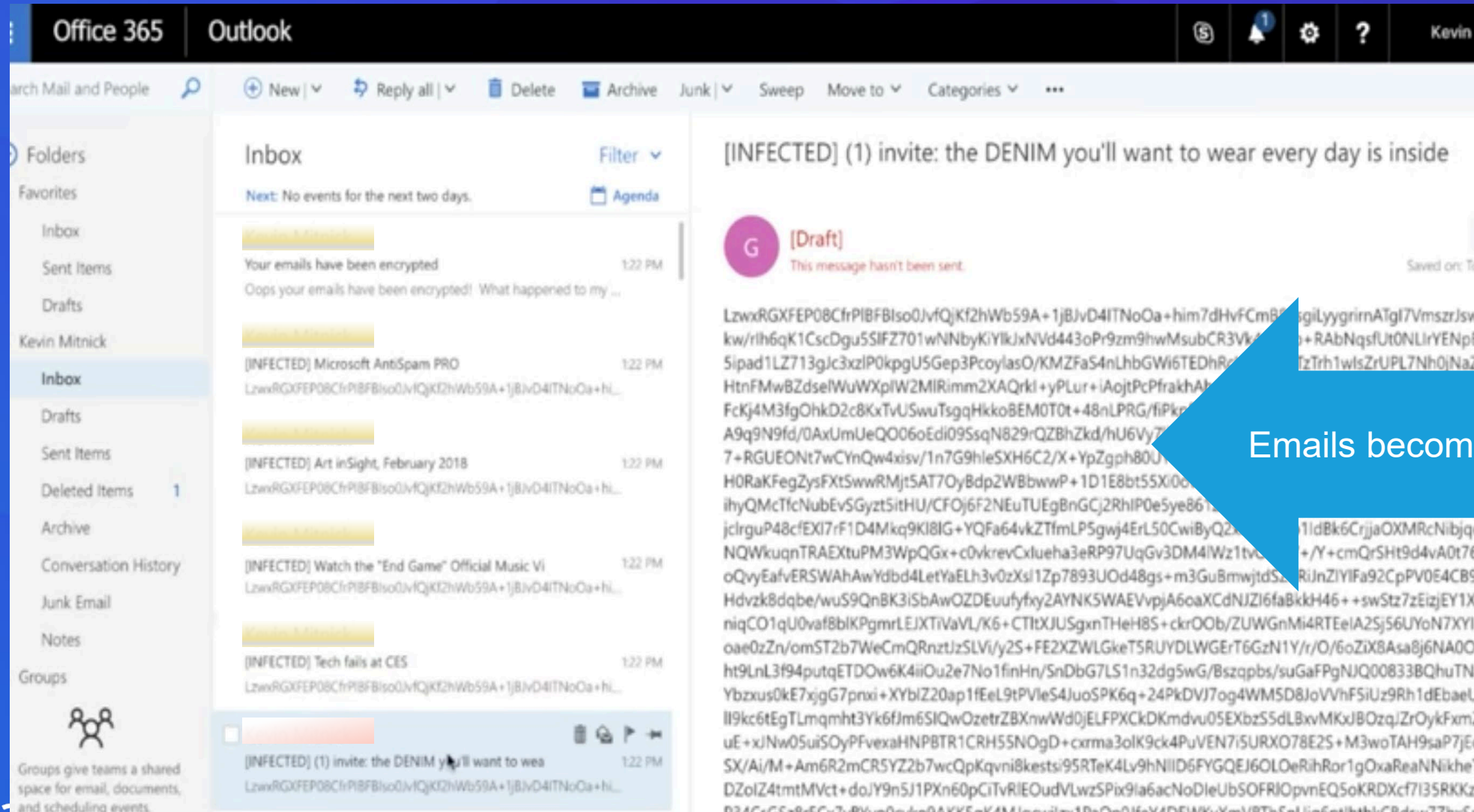


HOW HACKERS INFECT OFFICE 365 WITH RANSOMWARE



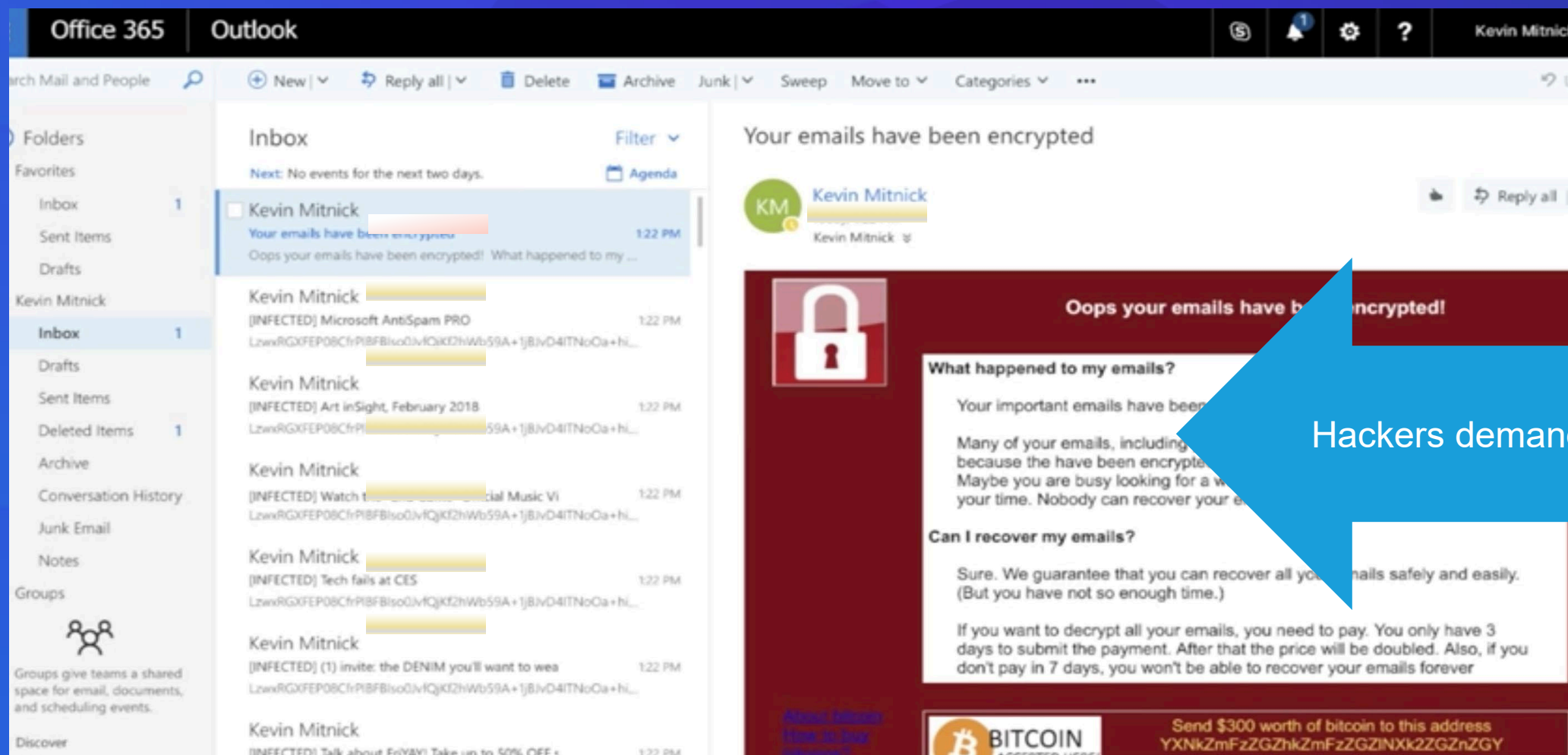
User authorizes the tool to
access their Office365
account

HOW HACKERS INFECT OFFICE 365 WITH RANSOMWARE



Emails become encrypted

HOW HACKERS INFECT OFFICE 365 WITH RANSOMWARE



Hackers demand a ransom



More data, more threats

Understanding the risk

Rethink backup!

Rethink DR!

Move to Continuity!

DR → BC



“...At least one employee will click on anything.”

It's not a matter of
if...

It's a matter of when..

BACKUP = SPARE TYRE



- Rusty Dusty Spare in the boot
- Is the spare still inflated?
- Is it good to use?
- No way to check if it is working before you need it
- Get out of car & get hands dirty
- Disruptive

DISASTER RECOVERY = RACT MEMBERSHIP



- Procedure in place
- Could take a while for RACT to arrive
- A lift to the mechanic
- You are going to be late (Downtime)
- Left waiting in the car
- Disruptive

BUSINESS CONTINUITY = RUN FLAT TYRES



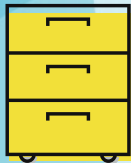
- Run Flat tyres
- You do not have to stop
- Continue on your journey
- May need to slow down slightly
- Safe, and saves time
- Automatic notification if there is a problem
- Minimal disruption
- Gives you continuity

WHY BUSINESS CONTINUITY?

Backup Software

Copies/backup of your data

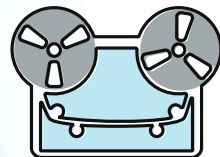
Filing Cabinet



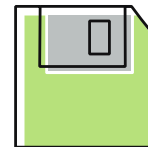
Disaster Recovery

Disaster recovery (DR) focuses on the policies, procedures & technology to enable the recovery of I.T

Tape Storage



File Based



Business Continuity

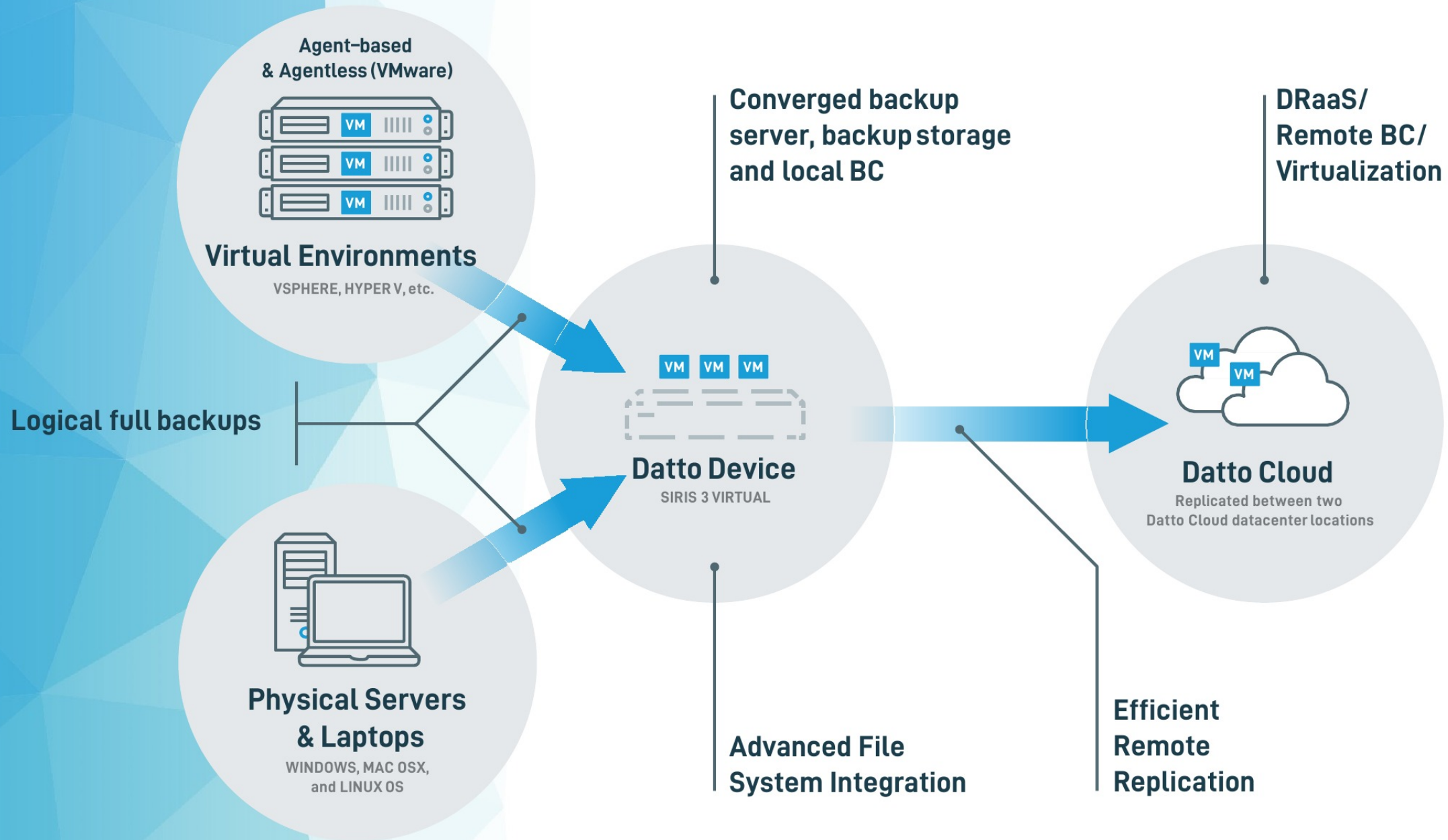
Next evolution of technology and is focused on minimizing downtime

Image Based/USB

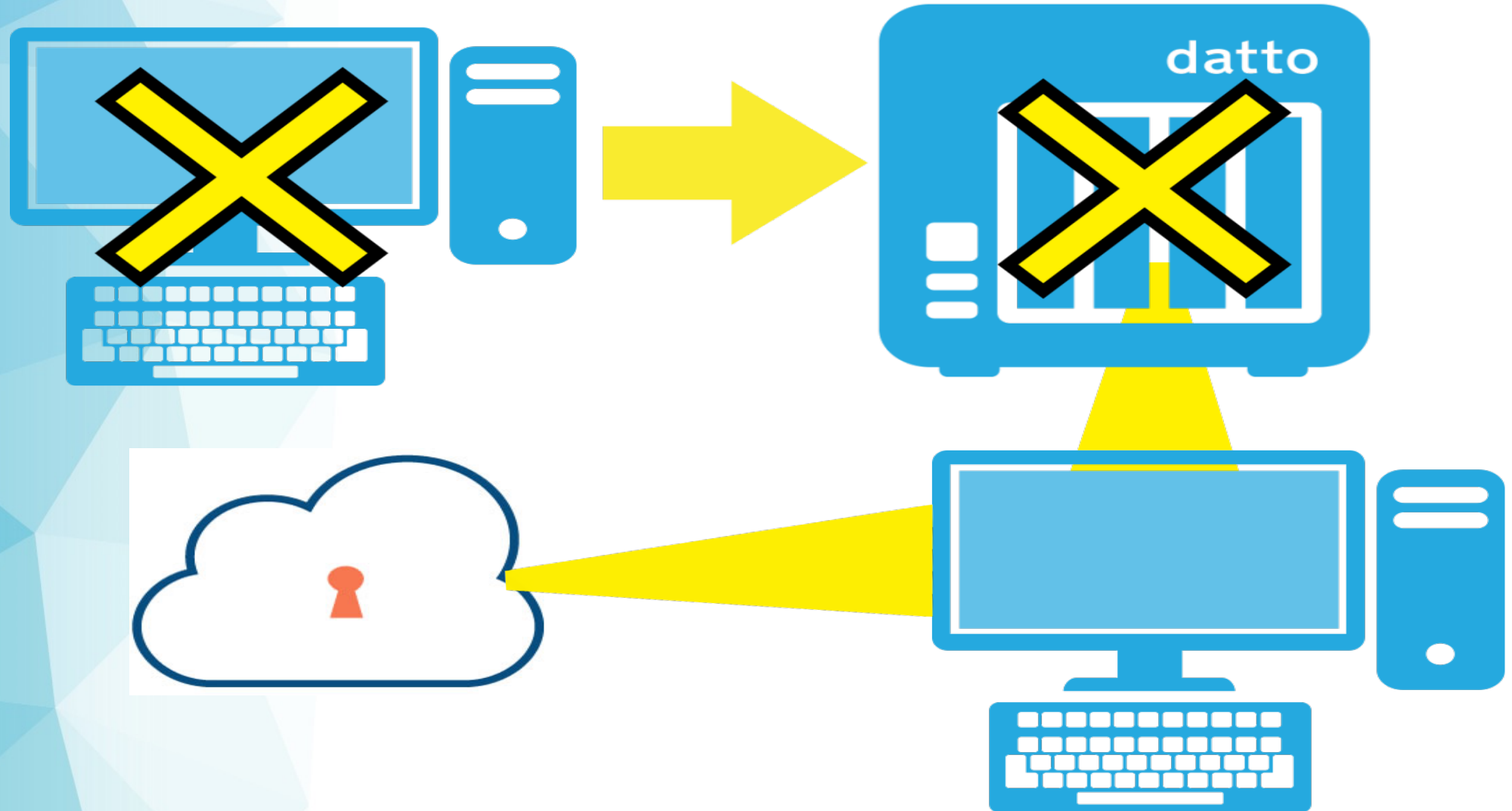



Continuity





Instant Virtualization – Local & Off-Site/Cloud





Thank you.
Any questions?

Kultar Khatra
kkhatra@datto.com
[linkedin.com/in/kultarkhatra](https://www.linkedin.com/in/kultarkhatra)





datto

CERTIFIED

PARTNER

Anderson Morgan
BUSINESS ENABLED

HOBART | LAUNCESTON | ULVERSTONE

andersonmorgan.com.au

1300 557 312