Protecting ourselves from Cyber Terrorism

SGSecure@Workplaces Workshop 2020
18 Nov 2020

Topics

1. What are the cyber terror threats
2. What will be the new cyberspace
3. Exercise
4. Key Takeaways

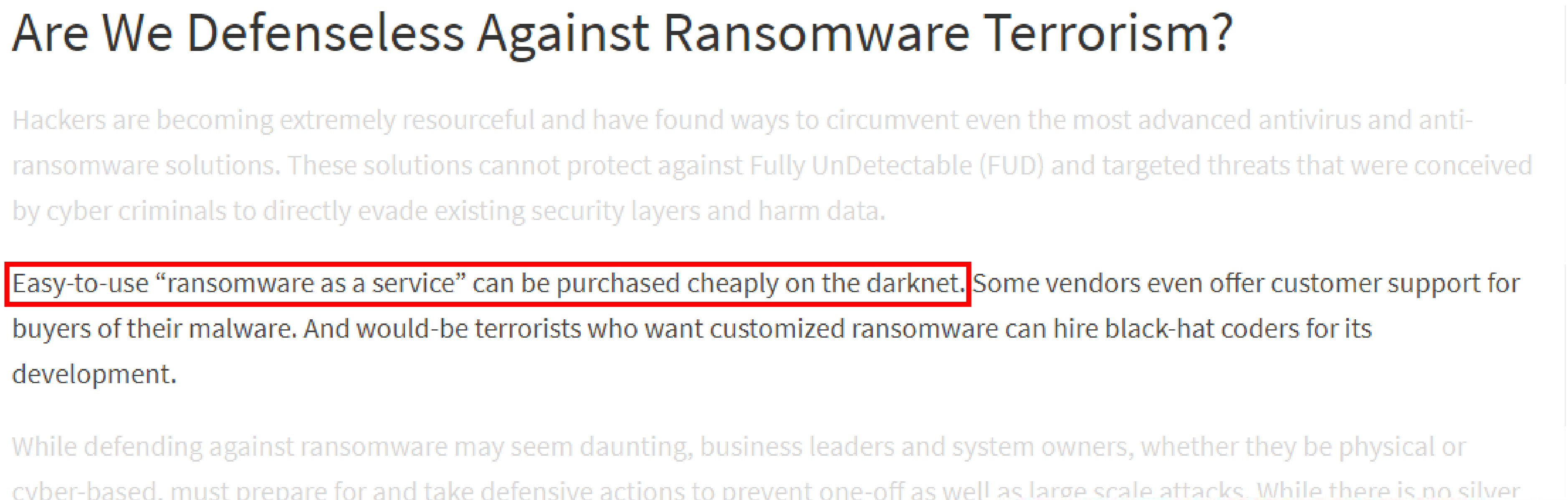
What are the cyber terror threats

Poll #1

Which do you think are related to cyber terrorism? Can choose more than one.

1. Hotel data breach
2. Ransomware attack on MNC
3. Ransomware attacks on hospitals
4. Asymptomatic COVID19 super spreader
5. Person died in ambulance on the way to hospital

Ransomware as a Service



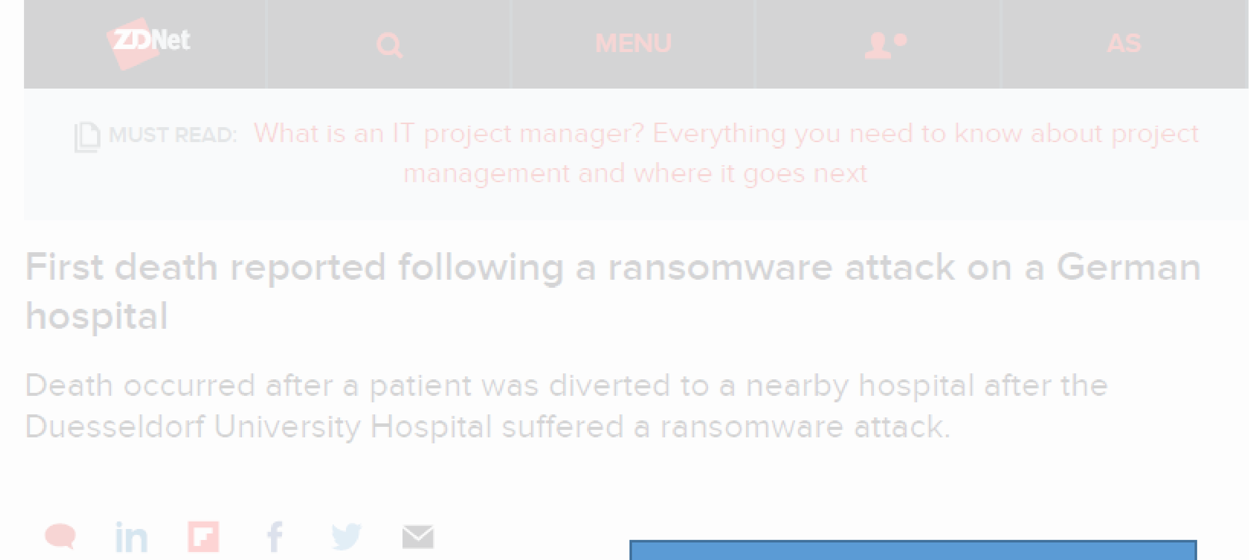
Are We Defenseless Against Ransomware Terrorism?

Hackers are becoming extremely resourceful and have found ways to circumvent even the most advanced antivirus and anti-ransomware solutions. These solutions cannot protect against Fully UnDetectable (FUD) and targeted threats that were conceived by cyber criminals to directly evade existing security layers and harm data.

Easy-to-use "ransomware as a service" can be purchased cheaply on the darknet. Some vendors even offer customer support for buyers of their malware. And would-be terrorists who want customized ransomware can hire black-hat coders for its development.

While defending against ransomware may seem daunting, business leaders and system owners, whether they be physical or cyber-based, must prepare for and take defensive actions to prevent one-off as well as large scale attacks. While there is no silver bullet ransomware solution, the following are some of the most important actions

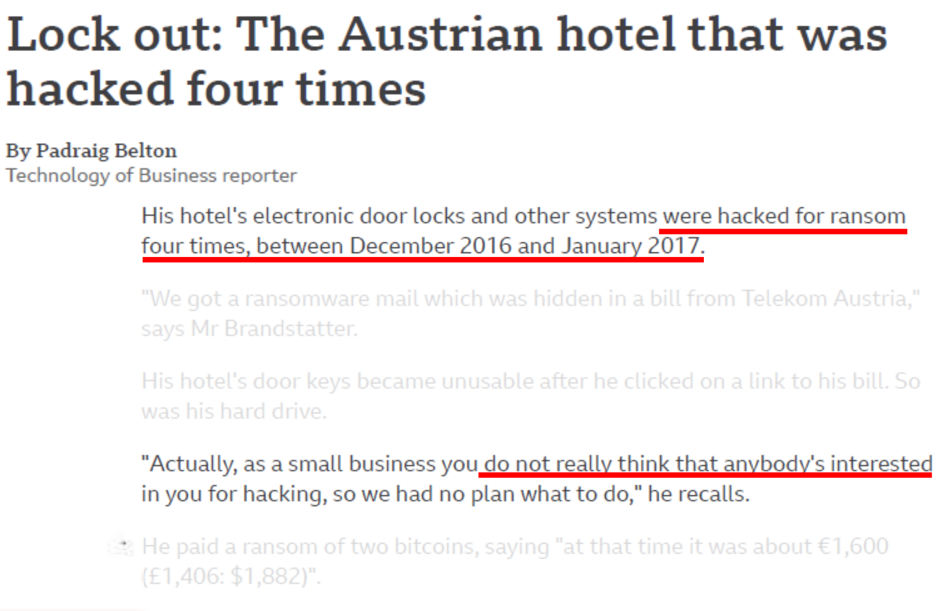
Cases of Cyber Attack of severe impact



MUST READ: What is an IT project manager? Everything you need to know about project management and where it goes next

First death reported following a ransomware attack on a German hospital

Death occurred after a patient was diverted to a nearby hospital after the Duesseldorf University Hospital suffered a ransomware attack.



Lock out: The Austrian hotel that was hacked four times

By Padraig Belton
Technology of Business reporter

His hotel's electronic door locks and other systems were hacked for ransom four times, between December 2016 and January 2017.

"We got a ransomware mail which was hidden in a bill from Telekom Austria," says Mr Brandstatter.

His hotel's door keys became unusable after he clicked on a link to his bill. So was his hard drive.

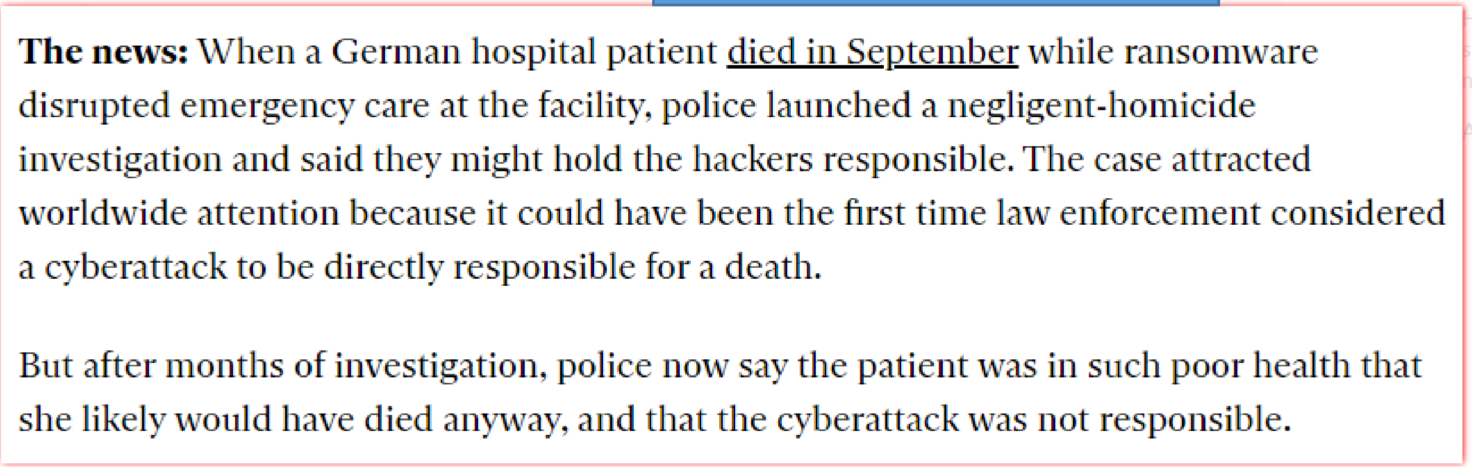
"Actually, as a small business you do not really think that anybody's interested in you for hacking, so we had no plan what to do," he recalls.

He paid a ransom of two bitcoins, saying "at that time it was about €1,600 (£1,406: $1,882)".

He has now installed firewalls and new antivirus software, and has trained his staff to recognise phishing emails that may seem genuine but actually contain malware.

And he's moved back to traditional metal keys.

Correction

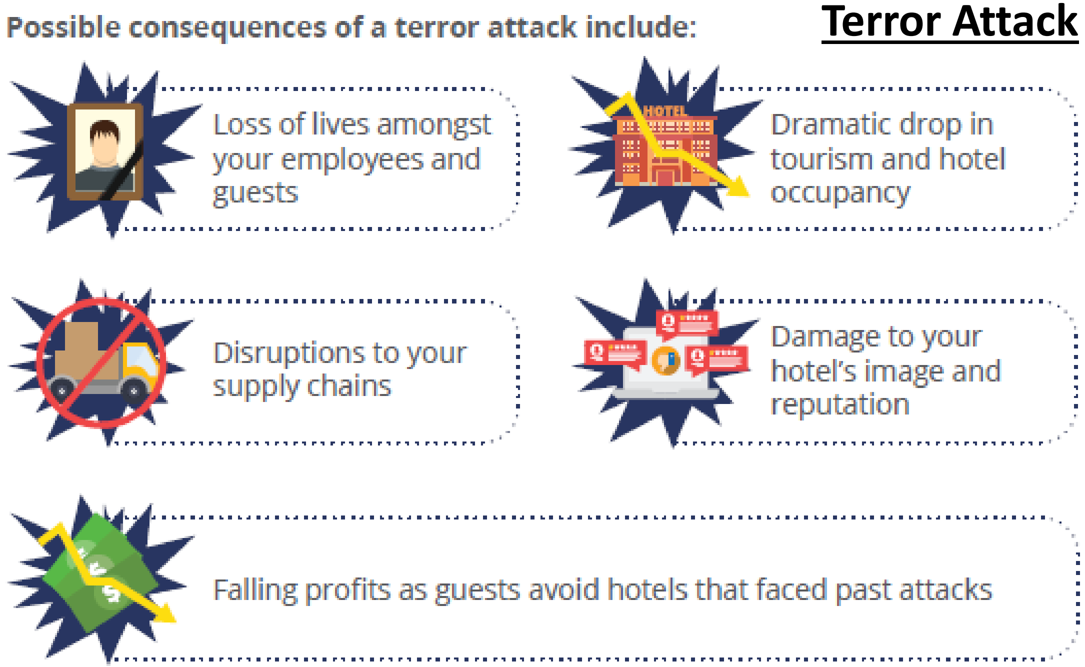


The news: When a German hospital patient died in September while ransomware disrupted emergency care at the facility, police launched a negligent-homicide investigation and said they might hold the hackers responsible. The case attracted worldwide attention because it could have been the first time law enforcement considered a cyberattack to be directly responsible for a death.

But after months of investigation, police now say the patient was in such poor health that she likely would have died anyway, and that the cyberattack was not responsible.

Cyber Terrorism VS Cyber Attack

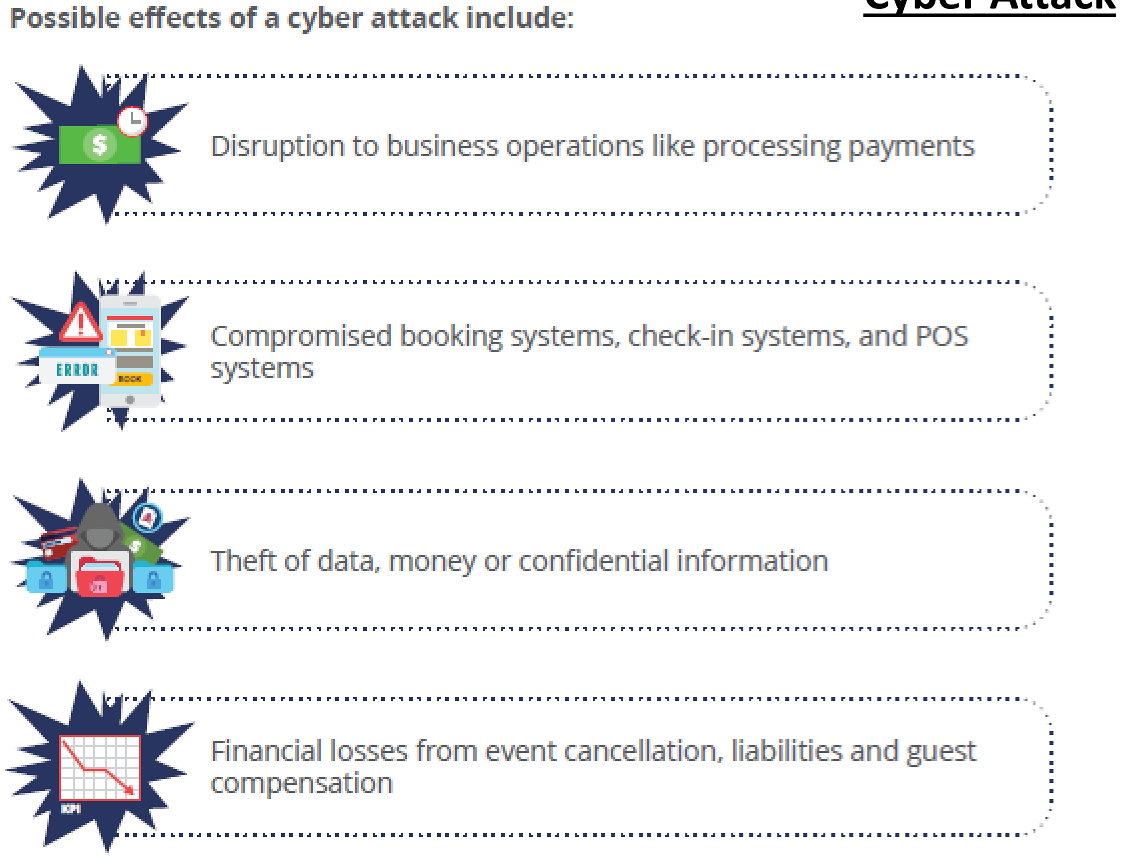
Terror Attack



Possible consequences of a terror attack include:

- Loss of lives amongst your employees and guests
- Dramatic drop in tourism and hotel occupancy
- Disruptions to your supply chains
- Damage to your hotel's image and reputation
- Falling profits as guests avoid hotels that faced past attacks

Cyber Attack



Possible effects of a cyber attack include:

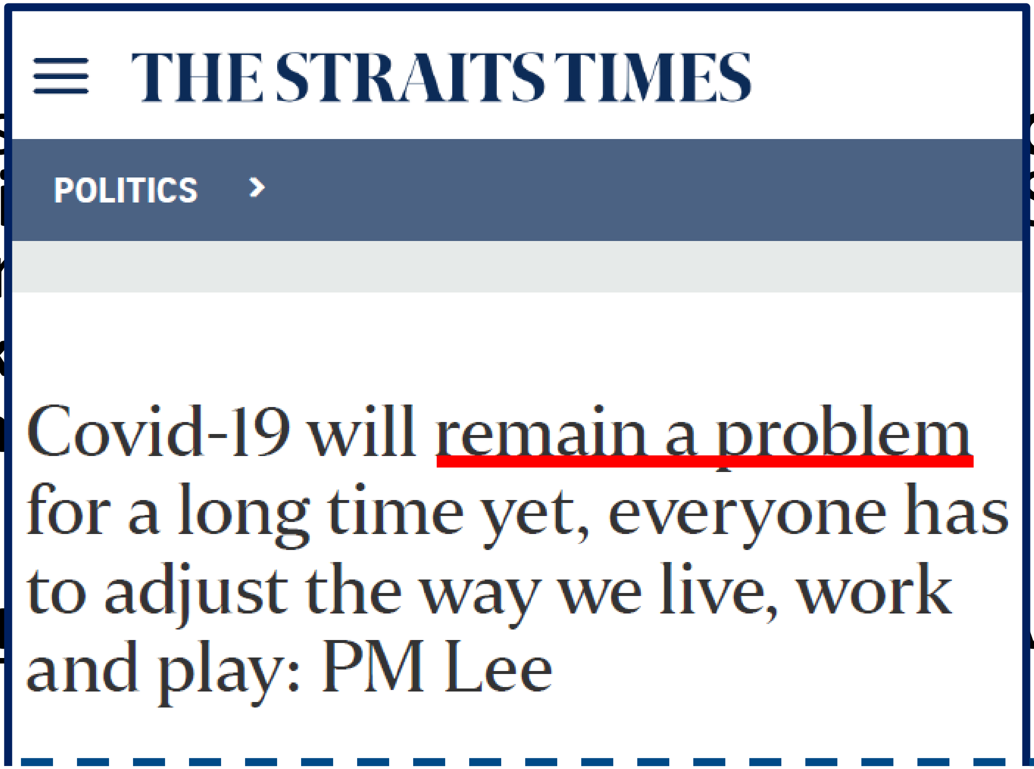
- Disruption to business operations like processing payments
- Compromised booking systems, check-in systems, and POS systems
- Theft of data, money or confidential information
- Financial losses from event cancellation, liabilities and guest compensation

Cyber Terrorism

What will be the new cyberspace

What will be the Covid-19 New Normal?

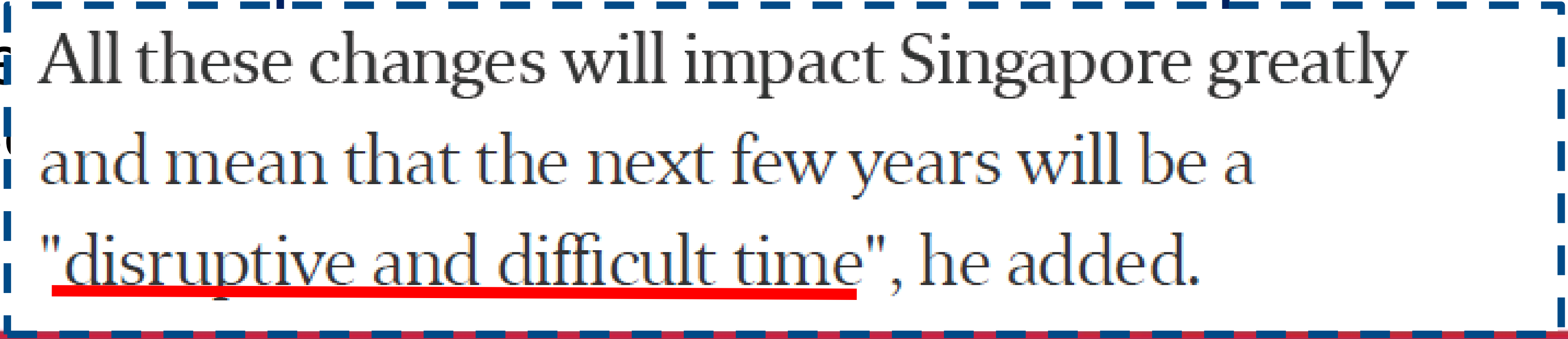
- Covid-19 has **on and transformati** Singapore and all over the wor
  - **More work**
  - **More onlin**
- **Digitalizatio** ve
- Leve
  - B



THE STRAITS TIMES

POLITICS

Covid-19 will remain a problem for a long time yet, everyone has to adjust the way we live, work and play: PM Lee



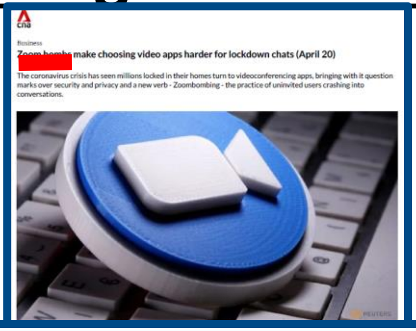
All these changes will impact Singapore greatly and mean that the next few years will be a "disruptive and difficult time", he added.

Current cyber landscape related to COVID19

- More online activities attracted more cyber attacks

- More phishing attacks using COVD19 baits/lures

- **WFH includes learning from home**
  - **Leverage video conferencing systems**

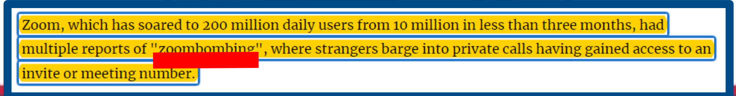


cna

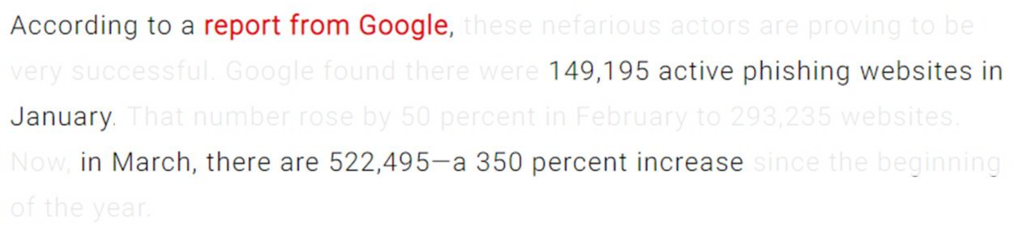
Business

Zoom bombs make choosing video apps harder for lockdown chats (April 20)

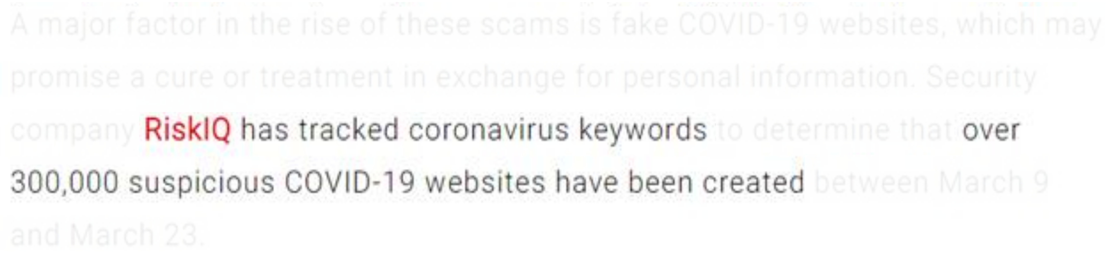
The coronavirus crisis has seen millions locked in their homes turn to videoconferencing apps, bringing with it question marks over security and privacy and a new verb - Zoombombing - the practice of uninvited users crashing into conversations.



Zoom, which has soared to 200 million daily users from 10 million in less than three months, had multiple reports of "zoombombing", where strangers barge into private calls having gained access to an invite or meeting number.

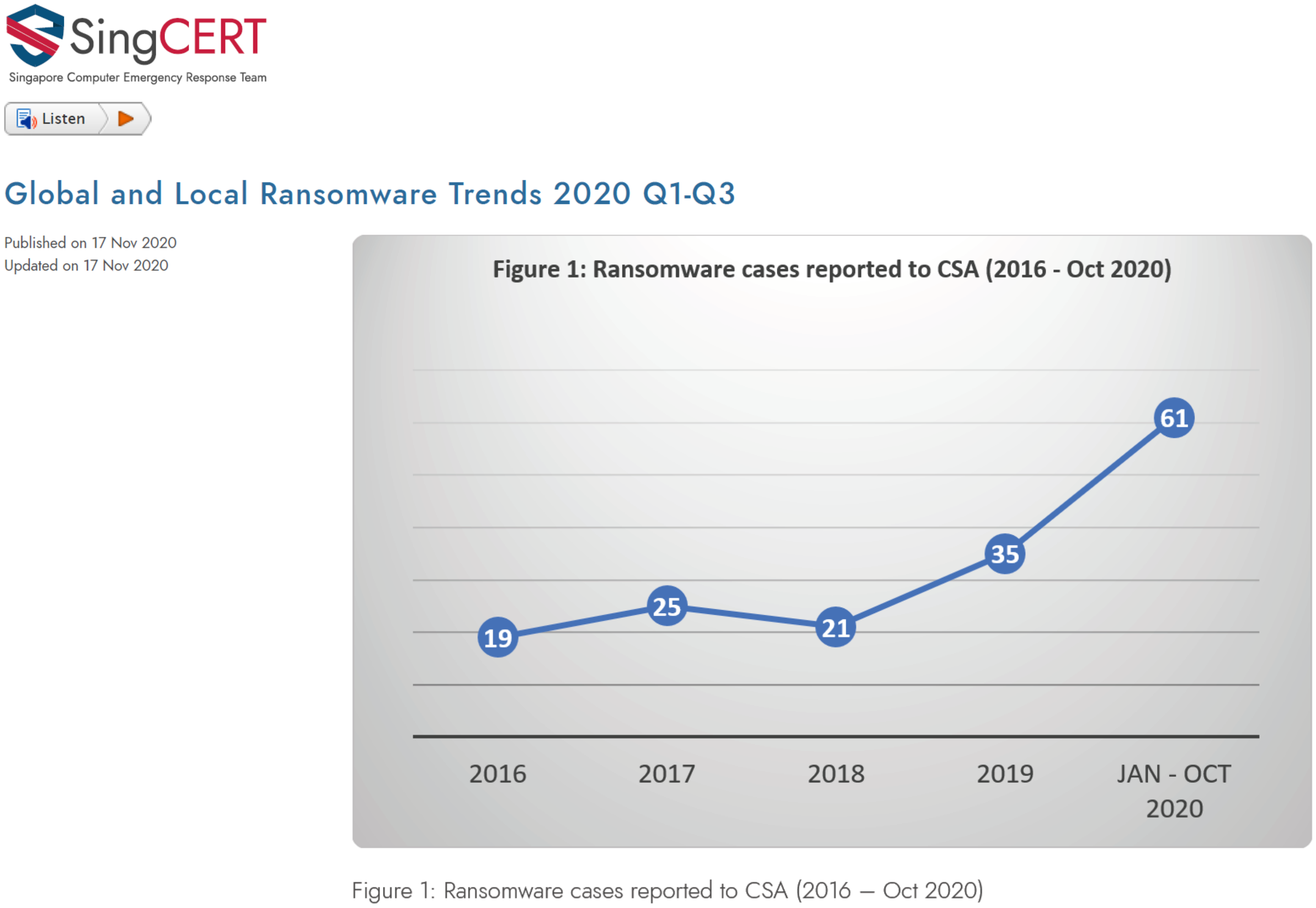


According to a report from Google, these nefarious actors are proving to be very successful. Google found there were 149,195 active phishing websites in January. That number rose by 50 percent in February to 293,235 websites. Now, in March, there are 522,495—a 350 percent increase since the beginning of the year.



A major factor in the rise of these scams is fake COVID-19 websites, which may promise a cure or treatment in exchange for personal information. Security company RiskIQ has tracked coronavirus keywords to determine that over 300,000 suspicious COVID-19 websites have been created between March 9 and March 23.

Current cyber landscape related to COVID19



SingCERT

Singapore Computer Emergency Response Team

Listen

Global and Local Ransomware Trends 2020 Q1-Q3

Published on 17 Nov 2020
Updated on 17 Nov 2020

Figure 1: Ransomware cases reported to CSA (2016 - Oct 2020)

Figure 1: Ransomware cases reported to CSA (2016 – Oct 2020)

https://go.gov.sg/csa-global-local-ransomware-trends-2020-q1-q3

Common Cyber Attacks

- Ransomware; Also involves data leaks
- Data breaches (APTs and insider threats)
- Financial frauds (Business Email Compromise- BEC)
- Denial of Service (DOS & DDOS)

S’pore SME Cyber Preparedness 2019

The key findings from Chubb S’pore SME Cyber Preparedness Report for 2019 are:

- 65% SME had one cyber incident
- 54% of these incidents – SME bosses already knew of the risks
- 53% cyber incidents caused by employees
- Most commonly breached data files – email traffic of Snr Teams
- Main concerns after a cyber incident:
    - Relationship with customers (55%)
    - Revenue and sales (51%)
    - Public reputation (49%)
    - Cost of the incident (from 46%)

Poll #2

Which problem statements are your concerns?
Can choose more than 1

1) SMEs lack cyber defence and digital risk management capabilities to protect themselves against the increasing frequency and sophistication of cyber-attacks
2) SMEs lack a cost effective solution to safeguard themselves against the increasing frequency and sophistication of cyber-attacks and insider threats
3) SMEs lack IT security support staff to support their daily business.
4) The incident response is too “slow” – manual processes;
   - Incident response and digital forensic are not integrated into a single solution

Be Safe Online

ESSENTIAL

7

Encrypt Your Crown Jewels
Encrypt classified or sensitive information to prevent exfiltrated data to be accessible by adversaries.

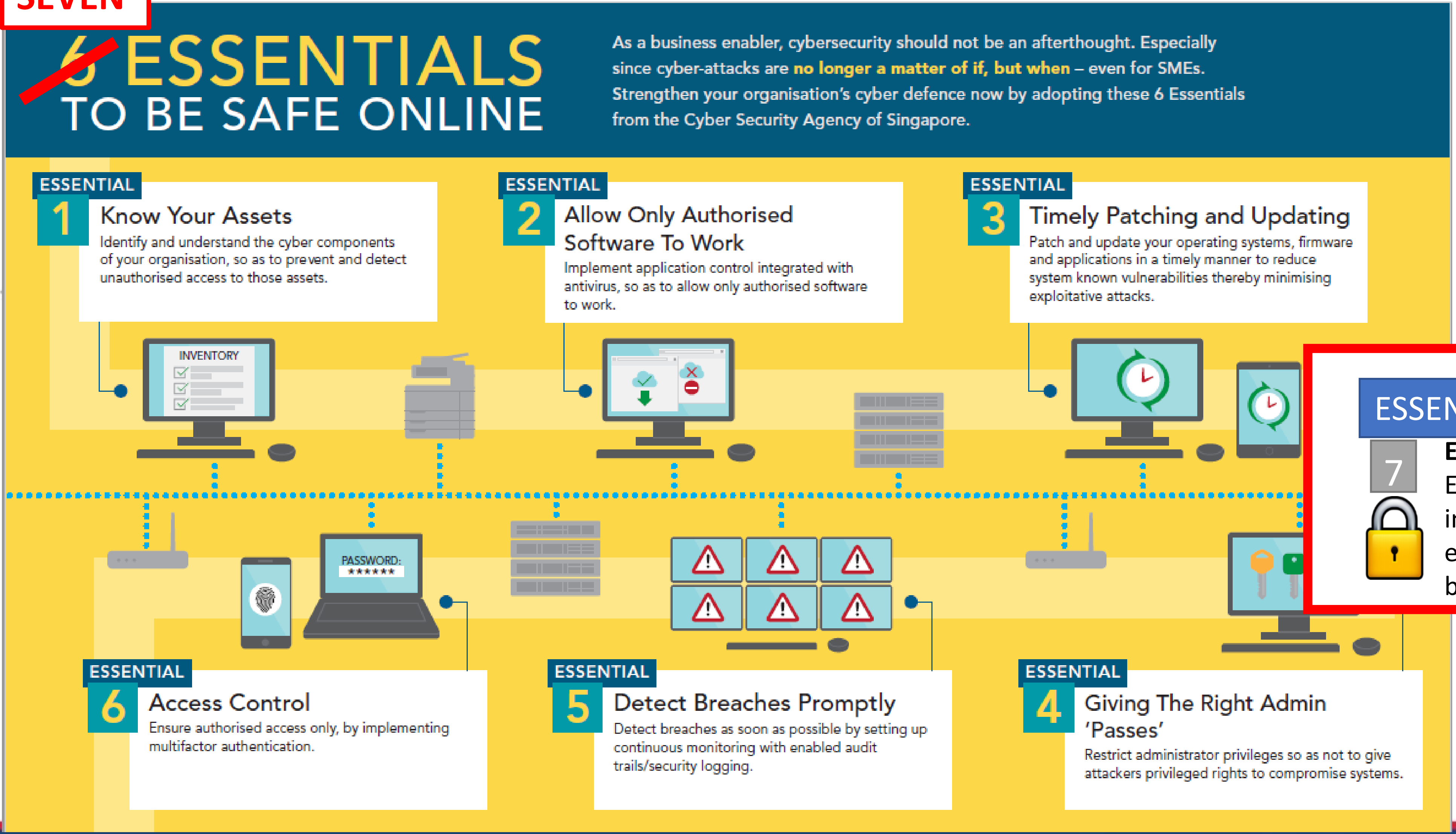
- Security principles remain relevant in the 'new' cyberspace
- CSA Be Safe Online (BSOL) guidelines and its Six Essentials still relevant
- Trends of **bigger data leaks** promoting 7th BSOL measure to Essential
- The Magnificent 7s – new backbone of Be Safe Online
- New technologies means BSOL measures done in different ways
  - Fully integrated
  - Co-operative security – cybersecurity is a **TEAM WORK**

They were seven... THEY FOUGHT LIKE SEVEN HUNDRED!
THE MIRISCH COMPANY
YUL BRYNNER
"THE MAGNIFICENT SEVEN"
ELI WALLACH · STEVE McQUEEN
CHARLES BRONSON · ROBERT VAUGHN · HORST BUCHOLZ

Team Work is Key

Security In The Covid-19 New Normal

SEVEN



~~6~~ ESSENTIALS TO BE SAFE ONLINE

As a business enabler, cybersecurity should not be an afterthought. Especially since cyber-attacks are **no longer a matter of if, but when** – even for SMEs. Strengthen your organisation's cyber defence now by adopting these 6 Essentials from the Cyber Security Agency of Singapore.

ESSENTIAL 1 **Know Your Assets**

Identify and understand the cyber components of your organisation, so as to prevent and detect unauthorised access to those assets.

ESSENTIAL 2 **Allow Only Authorised Software To Work**

Implement application control integrated with antivirus, so as to allow only authorised software to work.

ESSENTIAL 3 **Timely Patching and Updating**

Patch and update your operating systems, firmware and applications in a timely manner to reduce system known vulnerabilities thereby minimising exploitative attacks.

ESSENTIAL 6 **Access Control**

Ensure authorised access only, by implementing multifactor authentication.

ESSENTIAL 5 **Detect Breaches Promptly**

Detect breaches as soon as possible by setting up continuous monitoring with enabled audit trails/security logging.

ESSENTIAL 4 **Giving The Right Admin 'Passes'**

Restrict administrator privileges so as not to give attackers privileged rights to compromise systems.

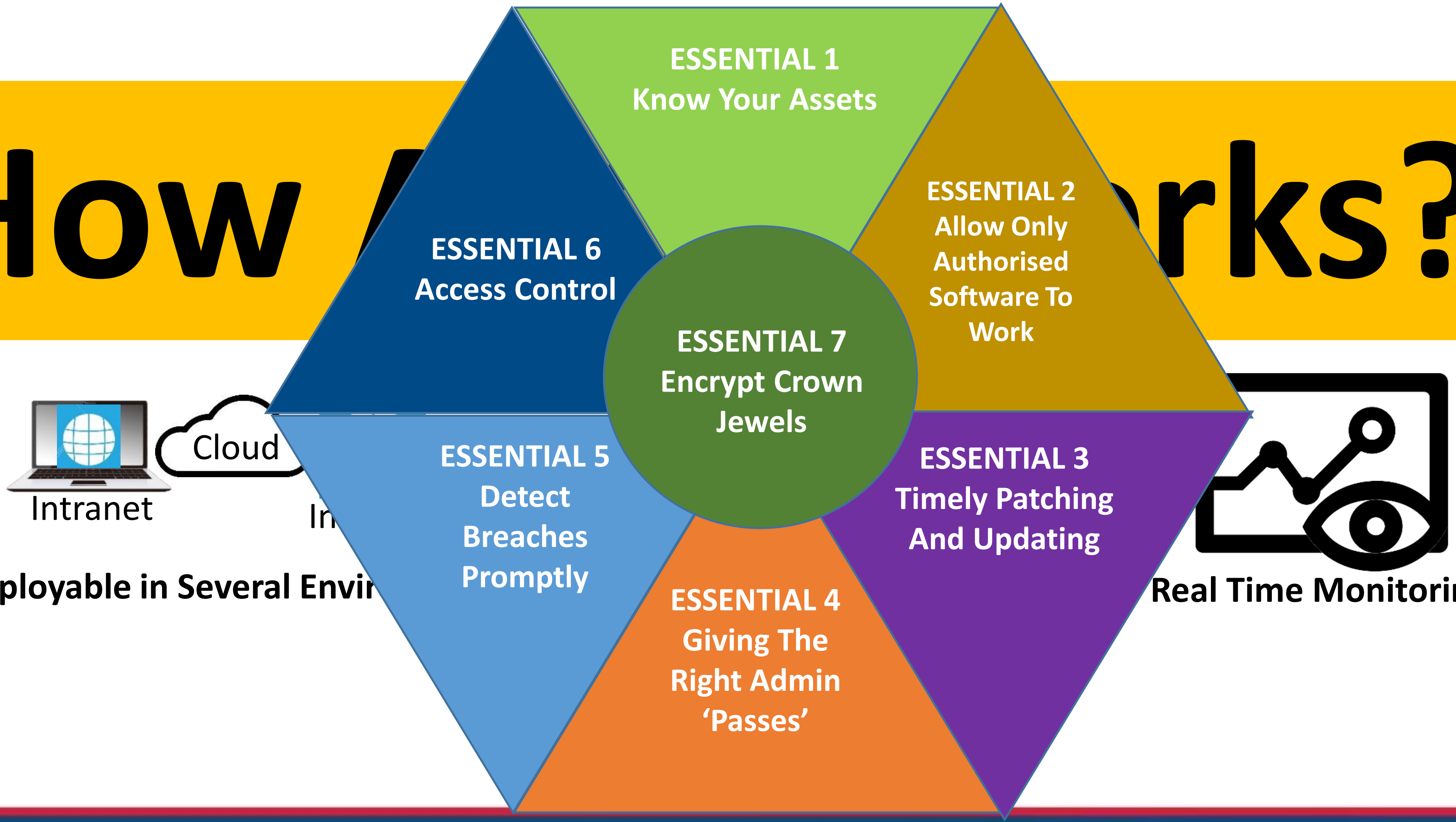
ESSENTIAL 7 **Encrypt Your Crown Jewels**

Encrypt classified or sensitive information to prevent exfiltrated data to be accessible by adversaries.

Asset Based Cyber Defence (ABCD) of BSOL

How

rks?



ESSENTIAL 1
Know Your Assets

ESSENTIAL 2
Allow Only Authorised Software To Work

ESSENTIAL 3
Timely Patching And Updating

ESSENTIAL 4
Giving The Right Admin 'Passes'

ESSENTIAL 5
Detect Breaches Promptly

ESSENTIAL 6
Access Control

ESSENTIAL 7
Encrypt Crown Jewels

Deployable in Several Envir

Real Time Monitoring

Secure Conferencing In The Covid-19 New Normal

CSA suggests three requirements for secure conferencing

1. Secure your endpoints used for communications and conferencing
2. Allow only authorized participants in the conference Or control Participants
3. Encrypt conference information from participants to participants

Our current assessment of many video conference systems:

- Most do not have True E2E Encryption
  - Have to trust vendors to protect contents in VC server
- Look for VC that has Lobby/Waiting Room which can control user access

Plan to develop secure VC within VPN for sensitive discussions

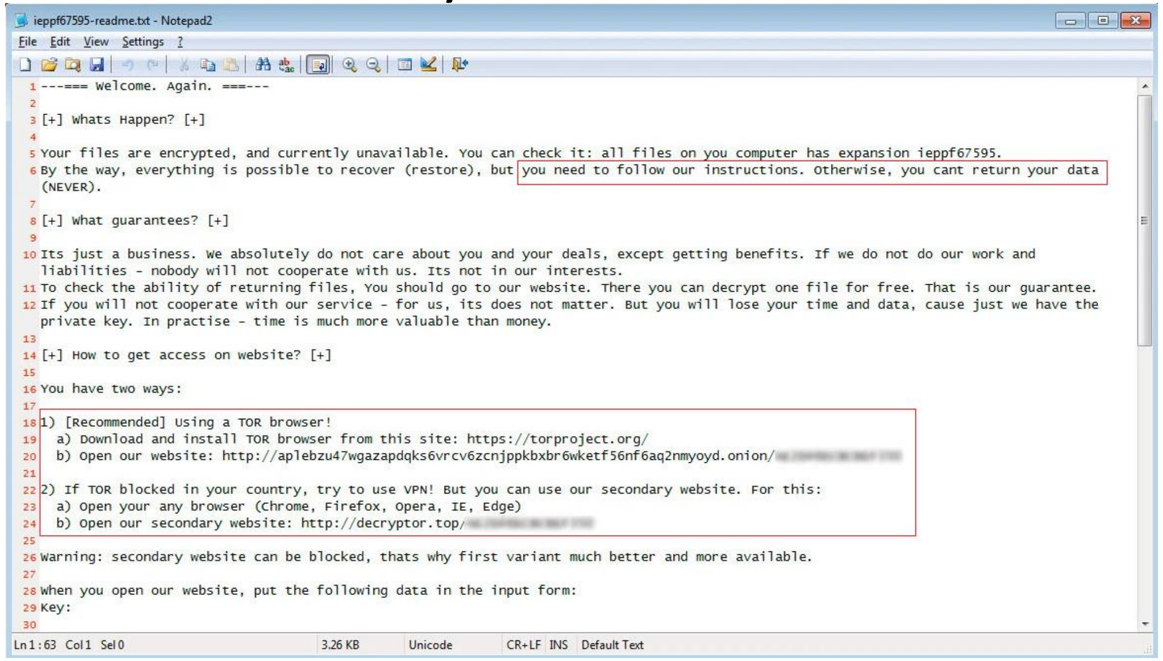
- Nothing is recorded at service provider’s servers

Exercise

Exercise 1 (Ransomware Attack)

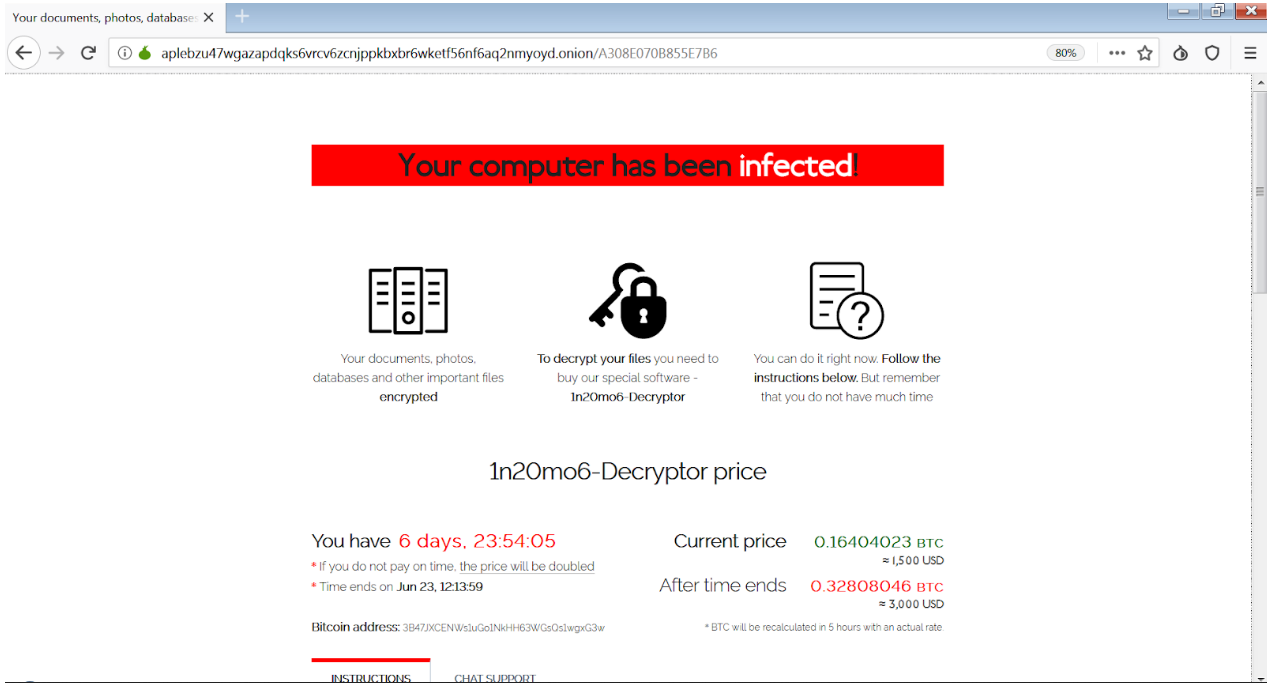
Scenario: You downloaded an attachment from your business partner. After opening it, you noticed your computer became slower than usual and noticed a ransom note demanding payment and files on your desktop were encrypted.

What should you do?



```
---=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has expansion ieppf67595.
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data
(NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and
liabilities - nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the
private key. In practise - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/[redacted]

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://decryptor.top/[redacted]

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:
```

Ln 1 : 63 Col 1 Sel 0
3.26 KB
Unicode
CR+LF INS Default Text



Your documents, photos, database
aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/A308E070B855E7B6
80%

Your computer has been infected!

Your documents, photos, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - **1n20mo6-Decryptor**

You can do it right now. **Follow the instructions below.** But remember that you do not have much time

1n20mo6-Decryptor price

You have 6 days, 23:54:05

* If you do not pay on time, the price will be doubled

* Time ends on Jun 23, 12:13:59

Current price	0.16404023 BTC ≈ 1,500 USD
After time ends	0.32808046 BTC ≈ 3,000 USD

Bitcoin address: 3B47JXCENWs1uGo1NkHH63WGsQs1wgxG3w

* BTC will be recalculated in 5 hours with an actual rate.

Exercise 1 (Ransomware Attack)

Scenario: You downloaded an attachment from your business partner. After opening it, you noticed your computer became slower than usual and noticed a ransom note demanding payment and files on your desktop were encrypted.

What should you do?

A. Ignore it and continue to work without your computer and report to manager

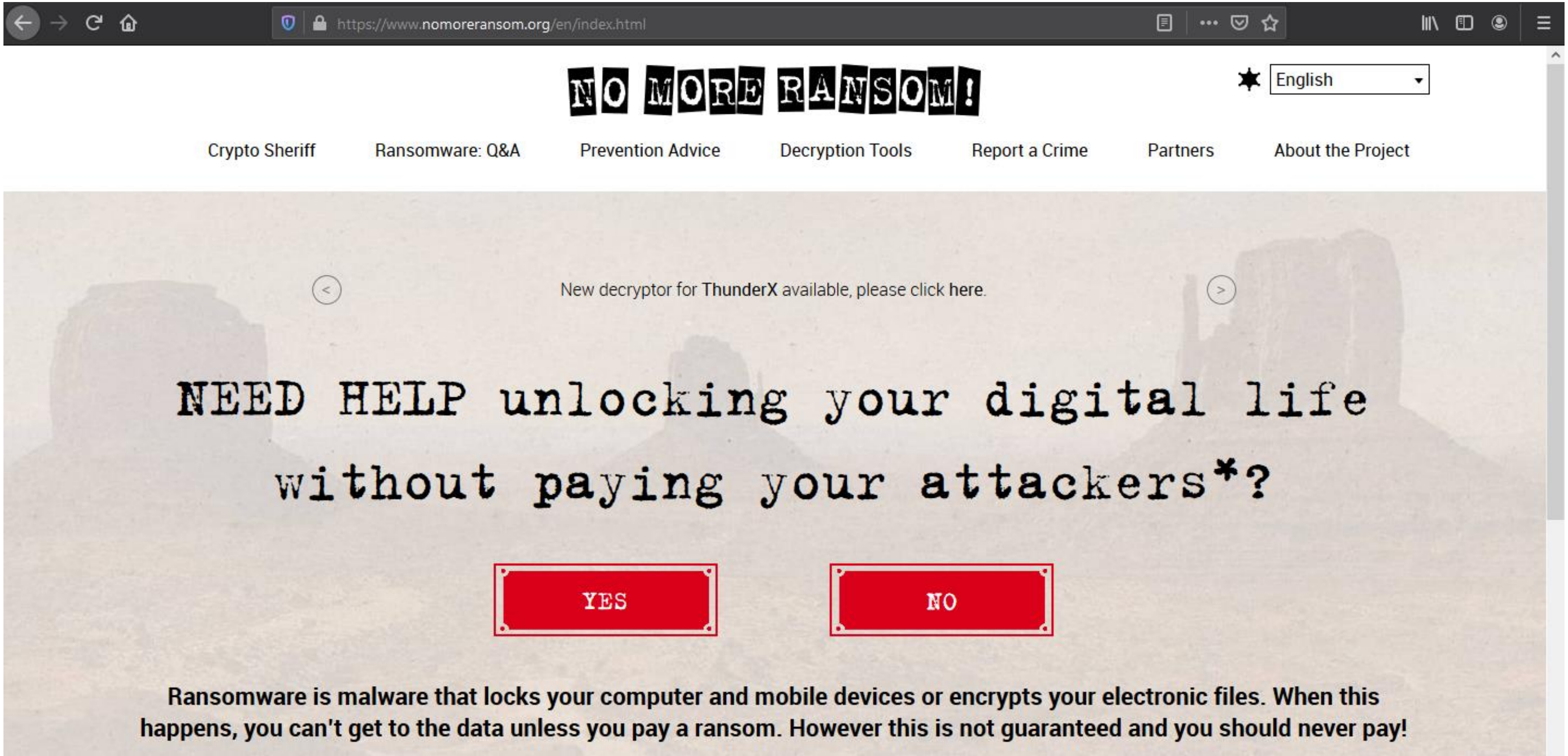
B. Shutdown or restart your computer and report to manager

C. Disconnect the computer from the network including pulling out the network cable and call IT Team or Vendor and report to manager

What can be done?

- Actually once ransomware hit you, it’s Game Over if you don’t have any backups. Therefore Prevention and ‘off-line’ Backup is essential
- Prevent
  - ABCD (7 CSA Essentials) or other integrated security solutions
  - Secure Backups
- Respond (this is included in ABCD Sec-aaS)
  - Contain the infection; find and isolate infected computers
  - Report and seek assistance from relevant authorities and follow their advice e.g. SingCert, PDPC Identify ransomware’s entry point(s) and rectify
- Recover
  - Clean infected devices
  - Restore data through backups or recovered keys (No More Ransoms project)

No More Ransom!



New decryptor for ThunderX available, please click here.

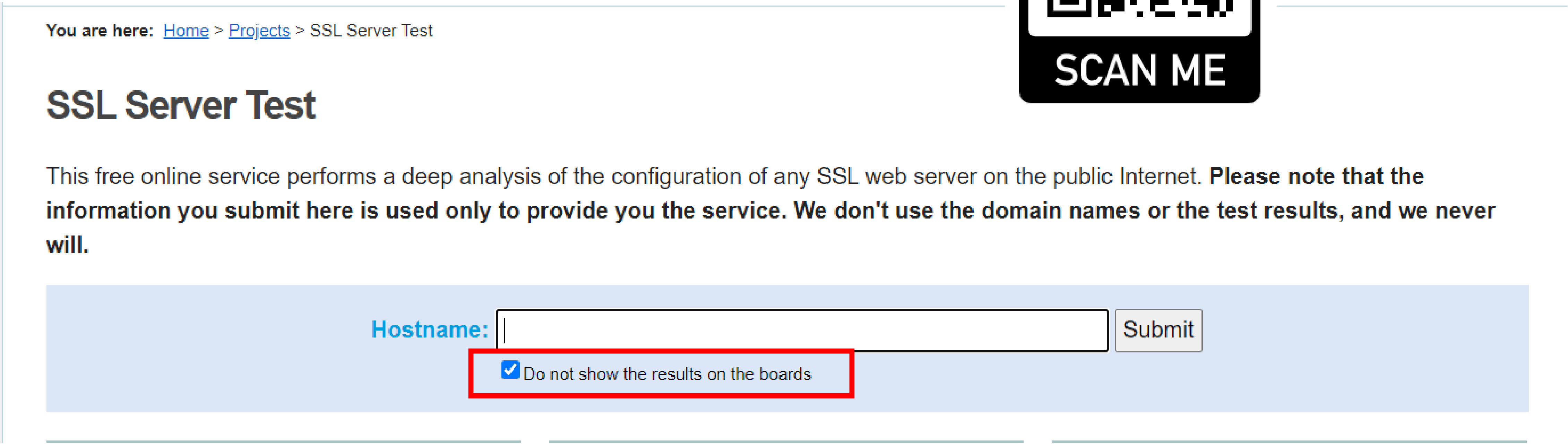
NEED HELP unlocking your digital life without paying your attackers*?

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!

Poll #3 (Website Test)

- Go to https://www.ssllabs.com/ssltest/index.htm
- Type in your companies website address

SCAN ME



You are here: Home > Projects > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname: |

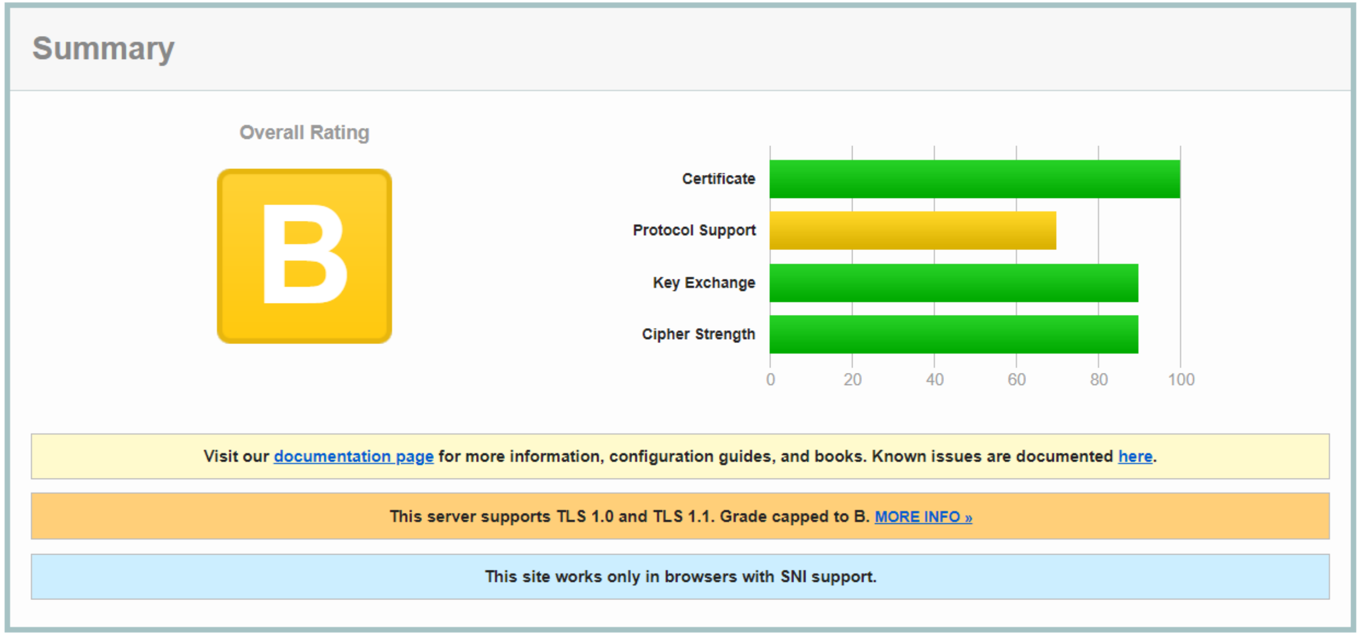
☑ Do not show the results on the boards

Poll #3 (Website Test)

- Go to https://www.ssllabs.com/ssltest/index.htm
- Type in your companies website address
- Provide the Overall Rating in the Poll

SCAN ME

- A
- B
- C and below
- Others



Summary

Overall Rating

B

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

This site works only in browsers with SNI support.

Summary - Key Takeaways

Summary - Key Takeaways

- Cyber Attack attempts has increase during Covid-19
- CSA’s Be Safe Online relevant to defend your business
  - https://go.gov.sg/csa-be-safe-online
- Leverage on trusted advisor and MSSPs
- Leverage on IMDA Grants to enhance Security
  - https://go.gov.sg/imda-psg-itsolution

https://go.gov.sg/csa-be-safe-online

https://go.gov.sg/imda-psg-itsolutio
n

Thank You for attending