5 KEY MESSAGES ON CYBERSECURITY

FROM MICROSOFT CEO, SATYA NADELLA

Brought to you by

mailguard

Gold
Microsoft Partner
Microsoft

Fuelling tech intensity and transformation. That was the theme of Microsoft CEO, Satya Nadella's Keynote address at Microsoft Innovate, and within that address he spent some time talking about trust, privacy and in particular cybersecurity.

One of the biggest challenges is breaking through the inertia of businesses settling for the status quo and simply accepting the reassurances that they are doing enough to defend against cybersecurity risks. You may have a robust cybersecurity strategy, but as 2020 begins, it's key to review that strategy, enhance your defences, and ensure you're doing everything you can to protect your business, and your professional reputation against cybercrime.

As you look forward and review your cybersecurity readiness, here are the **5 key messages from Nadella's address.**

1

UNDERSTAND THE COST AND IMPACT

"US$1 TRILLION is lost every year because of cyber issues" was the first message from Microsoft CEO, Satya Nadella, as he turned his attention to the perils of cybercrime. Expanding his point, he said that "the impact of cyber is disproportionately borne by small business and ordinary individuals" who may not have the necessary tools and resources to defend themselves.

The message here is clear, you need to prepare for the inevitable. The scale of the problem is immense, and it is impacting thousands of businesses around the world – regardless of size. The statistics tell us that as many as nine out of every 10 businesses are impacted by cybercrime. It would be foolish and unwise to think that it won't happen to you and your business.

Cybercrime is a global epidemic that is crippling businesses, destroying reputations and having devastating economic repercussions.

5 key messages on cybersecurity from Microsoft CEO, Satya Nadella | Brought to you by MailGuard

2

THINK ABOUT YOUR END-TO-END SECURITY

Nadella explained that this is the approach that Microsoft has taken to resolve the problem. **"The issue with security is, you can't just secure one room in the house. You have to have end-to-end security. Starting with identity, to devices, to applications to information and data, as well as your infrastructure. It needs to be one chain."**

The saying goes that 'you are only as strong as your weakest link,' and that is certainly true with respect to cybersecurity. Considering your people, processes, assets and infrastructure, a single vulnerability could lead to the downfall of your business. Email is the number one threat vector, which can include business and personal email use, but the proliferation of risks is vast when you begin to consider the diversity of devices and services that are interacting with your people and your network, and the breadth of access points for data in and out.

3

REAL-TIME MONITORING

Continuing with the message about the need for end-to-end security, Nadella said that **"This is not about just having the locks in the house, it's about the ability to monitor what's happening in real-time."**

It's one thing to put in place a plethora of defences, but if you assume that your system will be breached, will you be able to detect that incident as it occurs? Do you have the tools and processes in place that will provide real-time intelligence about a breach of your system?

Set in place solutions and processes to alert the right people immediately, so that your organisation can quickly respond and mitigate the impact of any threat.

4

SPEED: "MOVE FASTER THAN THE ADVERSARY"

"That ability to move faster than the adversary is going to be so important," remarked Nadella.

In the realm of cybercrime, things are moving at warp speed. That means that what you set in place to defend your business yesterday, is likely not enough to keep it safe today or tomorrow. Your business must continue to challenge its readiness, and question if vendors are still fit for purpose. You must iterate on your plans and processes to adapt to new innovations, because that's precisely what cybercriminals are doing. The NIST framework consists of five functions – identify, protect, detect, respond and recover. Speed is vital throughout.

5

SEEK NEW INNOVATIONS TO KEEP SAFE

Talking about the end-to-end infrastructure that Microsoft has built, Nadella said **"We have done this with openness. That means all of what we see, the trillions of signals are in a graph, that is available in fact to ISVs. I had a chance to learn about an ISV doing fantastic work, especially around creating threat protection around social engineering. That's the type of innovation we want to see, where we share the signal and we allow for defence in depth."**

He was talking about innovation from MailGuard.

Want to know more about what Satya said at Microsoft Innovate? You can watch the full Keynote here.

Ready to start your cyber review and learn more about MailGuard?

START YOUR CYBER REVIEW