VERITAS REPUTATION PR

FUTURE GENERALI
TOTAL INSURANCE SOLUTIONS

Monthly Coverage Dossier

January 2020

Future Generali India Life Insurance Company Limited

SR NO.	OVERVIEW OF ACTIVITIES	KEY PUBLICATIONS
1	Authored Article: - Creating a cyber secure organisation	• Silicon India Magazine (Print and online)
	Spokesperson: Mr. Pawan Chawla	
2	Industry story participation - About Insurance	• Financial Express (print)
	Spokesperson: Mr. Shreeraj Deshpande	
3	Industry story participation - Post-budget reaction	• Deccan Herald (online) • Top News (online) • City Air News (online)
	Spokesperson: Ms. Jyoti Vaswani	

Sr. no	Publication	Headline	Date	Coverage appeared
Spokesperson – Pawan Chawla				
Authored Article				
1	Silicon India Magazine	Creating a cyber secure organisation	Jan 2020 edition	Print and Online
Spokesperson – Mr. Shreeraj Deshpande				
Industry Story Participation (About Insurance)				
1	Financial Express	On health Insurance	15-Jan-20	Print
Spokesperson – Ms. Jyoti Vaswani				
Industry Story Participation (Post-budget reaction)				
1	Deccan Herald	Nirmala Sitharaman chose to be prudent in Budget	02-Feb-20	Online
2	Top News	Union Budget 2020 Reactions by Jyoti Vaswani Future Generali India Life Insurance	01-Feb-20	Online
3	City Air News	Industry reactions on Union Budget 2020-21	01-Feb-20	Online

Published Date:	January 2020 edition	Publication:	Silicon India Magazine
Edition:	Bangalore	Page No:	
Circulation:			

CIO INSIGHTS

CREATING A CYBER SECURE ORGANIZATION

By Pawan Chawla, CIO, Future Generali

An Information Security & Technology Professional with 18+ years of experience in Cyber Security, Pawan is ensuring optimal utilization of resources

Is technology becomes more important in our Lives,no data is safe. Cybersecurity awareness training is essential to a platform to share the knowledge that organizations can't afford to overlook.

Organization data is at risk. Organization employees may be hostages in the next threat from a highly skilled hacktivist or criminal. For several years now, most of the digital attacks to exploit the human factor is through phishing attempts and related efforts.

Malicious hackers and attackers seek to trick users into granting them access to a digital resource, long before they will try to hack their way in. To Simply put: People are the weakest link in any organization's cyber security defenses. And that's why employees are usually the first targets of cyber-attackers who use tactics and tools such as ransomware, spear phishing, malware, and social engineering.

Understanding the importance of Information Security Awareness in an Organization

The organization relies on employees as their primary resource for conducting business and interacting with customers. Of course, simple, repetitive tasks can be automated. But people will always be behind every automated task and on the other end of every phone call, email and chat session. And people represent the "human factor" in the cross hackle of cyber attackers. The only defense against such attacks is education.

Pawan Chawla, CIO

Important to note, cybersecurity training must be repetitive, updated and constantly tested. Because of the rapidly changing environment and a long list of vulnerabilities, security awareness training also cannot involve a one-shot approach or a "set it and forget it" program.

Let us understand the Relevance of Information Security Awareness Training

Information Security Awareness training must start with the organization acknowledgment that its employees are the weakest cybersecurity link. Employees in an organization are the first line of defense against cyber-attack.

Information Security Awareness shall consist of areas of exploitation, few of them are listed below

1. Spam – Spam is the main method of attack, not limited to direct email.

2. Social Engineering – Social engineering uses a variety of tools and recourses to gain access to targeted resources, it occurs when one person fools another into giving up access to a resource.

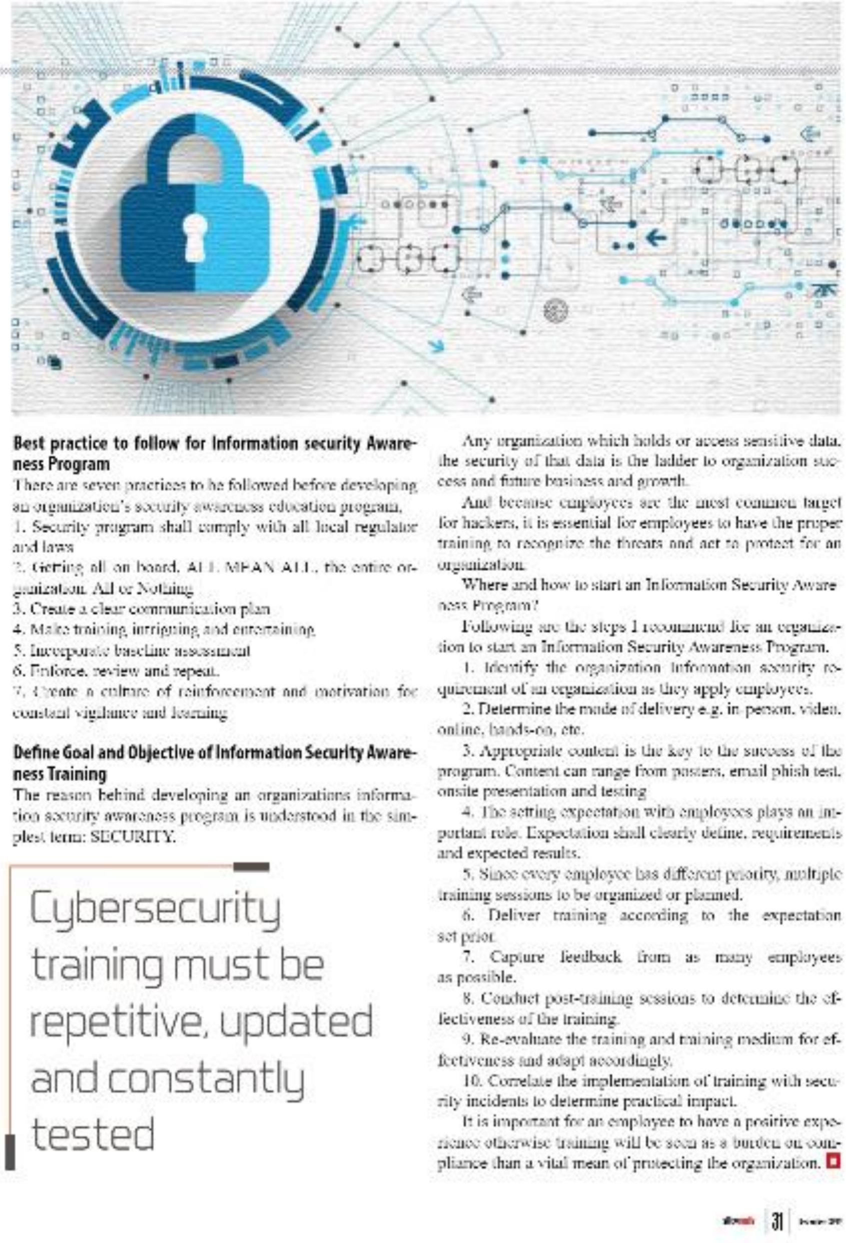
3. Phishing–Phishing intends to lead the uneducated user to click on dangerous links to gain access to employees' usernames, passwords, personally identifiable information, even financial information.

4. Vishing A vishing is conducted by Voice email, VOIP (Voice over IP), or landline or cellular telephone.

5. Spear phishing Spear phishing target high-profile individuals or people with access to valuable digital assets.

6. Advance Malware Advance malware is a specific target mission attack typically aimed at an enterprise.

7. Ransomware Ransomware attempts to steal credentials in the memory and attempts to propagate through the network using stolen credential or exploits.



Best practice to follow for Information security Awareness Program

There are seven practices to be followed before developing an organization's security awareness education program.

1. Security program shall comply with all local regulator and laws

2. Getting all on board. ALL MEAN ALL, the entire organization. All or Nothing

3. Create a clear communication plan

4. Make training intriguing and entertaining

5. Incorporate baseline assessment

6. Enforce, review and repeat.

7. Create a culture of reinforcement and motivation for constant vigilance and learning

Define Goal and Objective of Information Security Awareness Training

The reason behind developing an organizations information security awareness program is understood in the simplest term: SECURITY.

> Cybersecurity training must be repetitive, updated and constantly tested

Any organization which holds or access sensitive data, the security of that data is the ladder to organization success and future business and growth.

And because employees are the most common target for hackers, it is essential for employees to have the proper training to recognize the threats and act to protect for an organization.

Where and how to start an Information Security Awareness Program?

Following are the steps I recommend for an organization to start an Information Security Awareness Program.

1. Identify the organization Information security requirement of an organization as they apply employees.

2. Determine the mode of delivery e.g. in person, video, online, hands-on, etc.

3. Appropriate content is the key to the success of the program. Content can range from posters, email phish test, onsite presentation and testing

4. The setting expectation with employees plays an important role. Expectation shall clearly define, requirements and expected results.

5. Since every employee has different priority, multiple training sessions to be organized or planned.

6. Deliver training according to the expectation set prior.

7. Capture feedback from as many employees as possible.

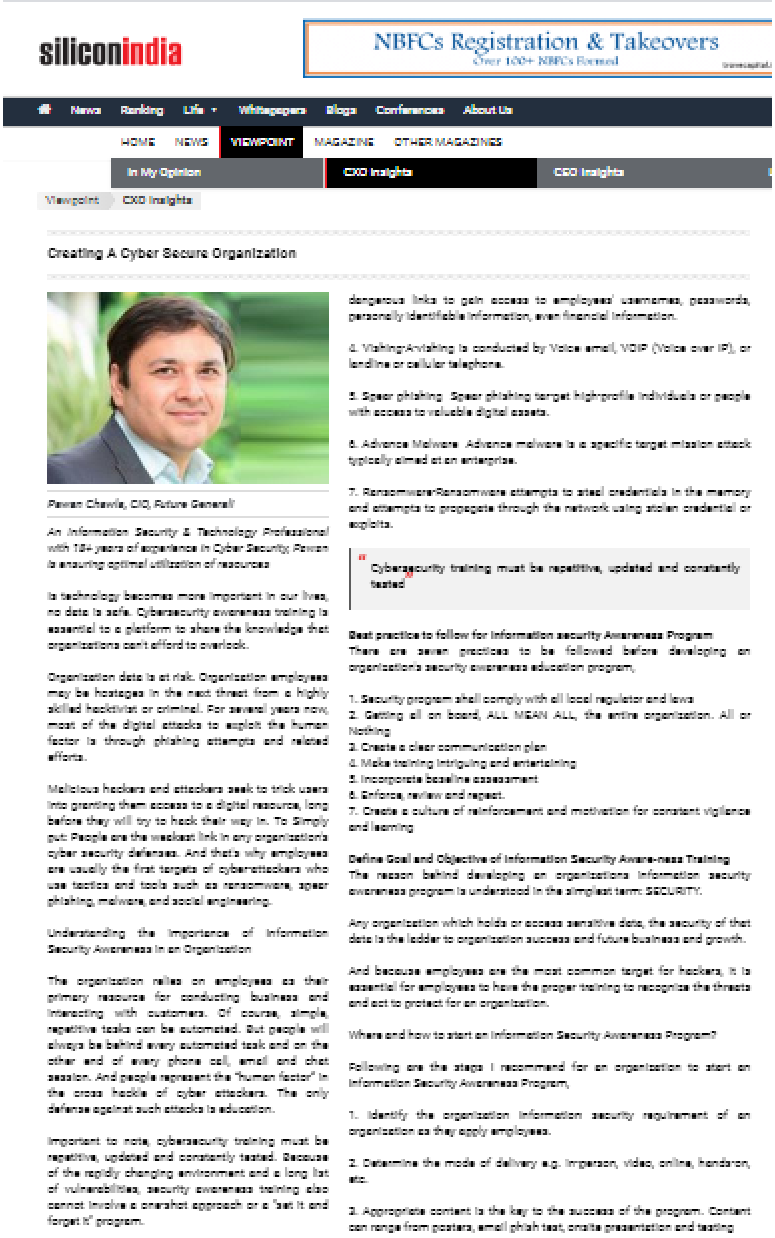
8. Conduct post-training sessions to determine the effectiveness of the training.

9. Re-evaluate the training and training medium for effectiveness and adapt accordingly.

10. Correlate the implementation of training with security incidents to determine practical impact.

It is important for an employee to have a positive experience otherwise training will be seen as a burden on compliance than a vital mean of protecting the organization. □

Date	Jan 2020
Publication	Silicon India Magazine
Headline	Creating a cyber secure organisation
Link	https://finance.siliconindia.com/viewpoint/cxoinsights/creating-a-cyber-secure-organization-nwid-21266.html



Creating A Cyber Secure Organization

Pawan Chawla, CIO, Future Generali

An Information Security & Technology Professional with 18+ years of experience in Cyber Security, Pawan is ensuring optimal utilization of resources

Is technology becomes more important in our lives, no data is safe. Cybersecurity awareness training is essential to a platform to share the knowledge that organizations can't afford to overlook.

Organization data is at risk. Organization employees may be hostages in the next threat from a highly skilled hacktivist or criminal. For several years now, most of the digital attacks to exploit the human factor is through phishing attempts and related efforts.

Malicious hackers and attackers seek to trick users into granting them access to a digital resource, long before they will try to hack their way in. To Simply put: People are the weakest link in any organization's cyber security defenses. And that's why employees are usually the first targets of cyberattackers who use tactics and tools such as ransomware, spear phishing, malware, and social engineering.

Understanding the Importance of Information Security Awareness in an Organization

The organization relies on employees as their primary resource for conducting business and interacting with customers. Of course, simple, repetitive tasks can be automated. But people will always be behind every automated task and on the other end of every phone call, email and chat session. And people represent the "human factor" in the cross hackle of cyber attackers. The only defense against such attacks is education.

Important to note, cybersecurity training must be repetitive, updated and constantly tested. Because of the rapidly changing environment and a long list of vulnerabilities, security awareness training also cannot involve a oneshot approach or a "set it and forget it" program.

dangerous links to gain access to employees' usernames, passwords, personally identifiable information, even financial information.

4. Vishing:Avishing is conducted by Voice email, VOIP (Voice over IP), or landline or cellular telephone.

5. Spear phishing: Spear phishing target high-profile individuals or people with access to valuable digital assets.

6. Advance Malware: Advance malware is a specific target mission attack typically aimed at an enterprise.

7. Ransomware:Ransomware attempts to steal credentials in the memory and attempts to propagate through the network using stolen credential or exploits.

> " Cybersecurity training must be repetitive, updated and constantly tested "

Best practice to follow for Information security Awareness Program
There are seven practices to be followed before developing an organization's security awareness education program,

1. Security program shall comply with all local regulator and laws
2. Getting all on board, ALL MEAN ALL, the entire organization. All or Nothing
3. Create a clear communication plan
4. Make training intriguing and entertaining
5. Incorporate baseline assessment
6. Enforce, review and repeat.
7. Create a culture of reinforcement and motivation for constant vigilance and learning

Define Goal and Objective of Information Security Aware-ness Training
The reason behind developing an organizations information security awareness program is understood in the simplest term: SECURITY.

Any organization which holds or access sensitive data, the security of that data is the ladder to organization success and future business and growth.

And because employees are the most common target for hackers, it is essential for employees to have the proper training to recognize the threats and act to protect for an organization.

Where and how to start an Information Security Awareness Program?

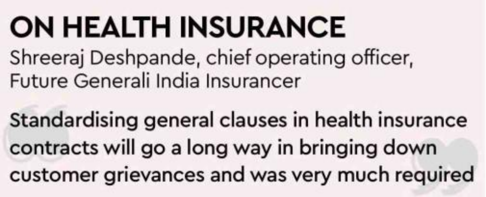
Following are the stage I recommend for an organization to start an Information Security Awareness Program,

1. Identify the organization information security requirement of an organization as they apply employees.

2. Determine the mode of delivery e.g. Inperson, video, online, handson, etc.

3. Appropriate content is the key to the success of the program. Content can range from posters, email phish test, onsite presentation and testing

Published Date:	15 Jan 2020	Publication:	The Financial Express
Edition:	Mumbai, New Delhi, Bangalore, Kolkata, Hyderabad, Chennai	Page No:	13
Circulation:	15000		

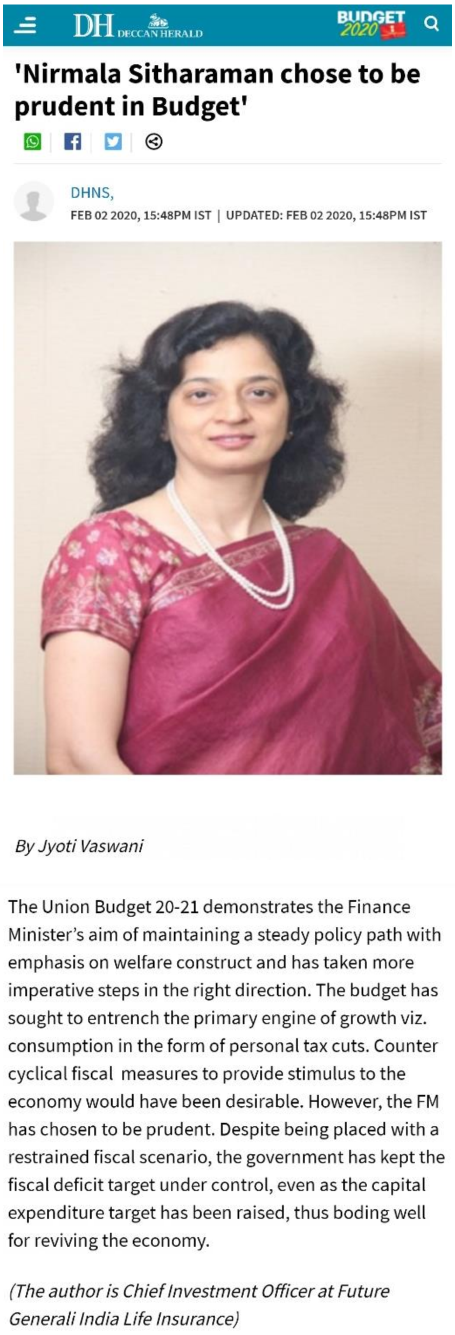


ON HEALTH INSURANCE

Shreeraj Deshpande, chief operating officer, Future Generali India Insurancer

“Standardising general clauses in health insurance contracts will go a long way in bringing down customer grievances and was very much required”

Date	02 February 2020
Publication	Deccan Herald
Headline	'Nirmala Sitharaman chose to be prudent in Budget'
Link	https://www.deccanherald.com/business/budget-2020/nirmala-sitharaman-chose-to-be-prudent-in-budget-800803.html



'Nirmala Sitharaman chose to be prudent in Budget'

DHNS,

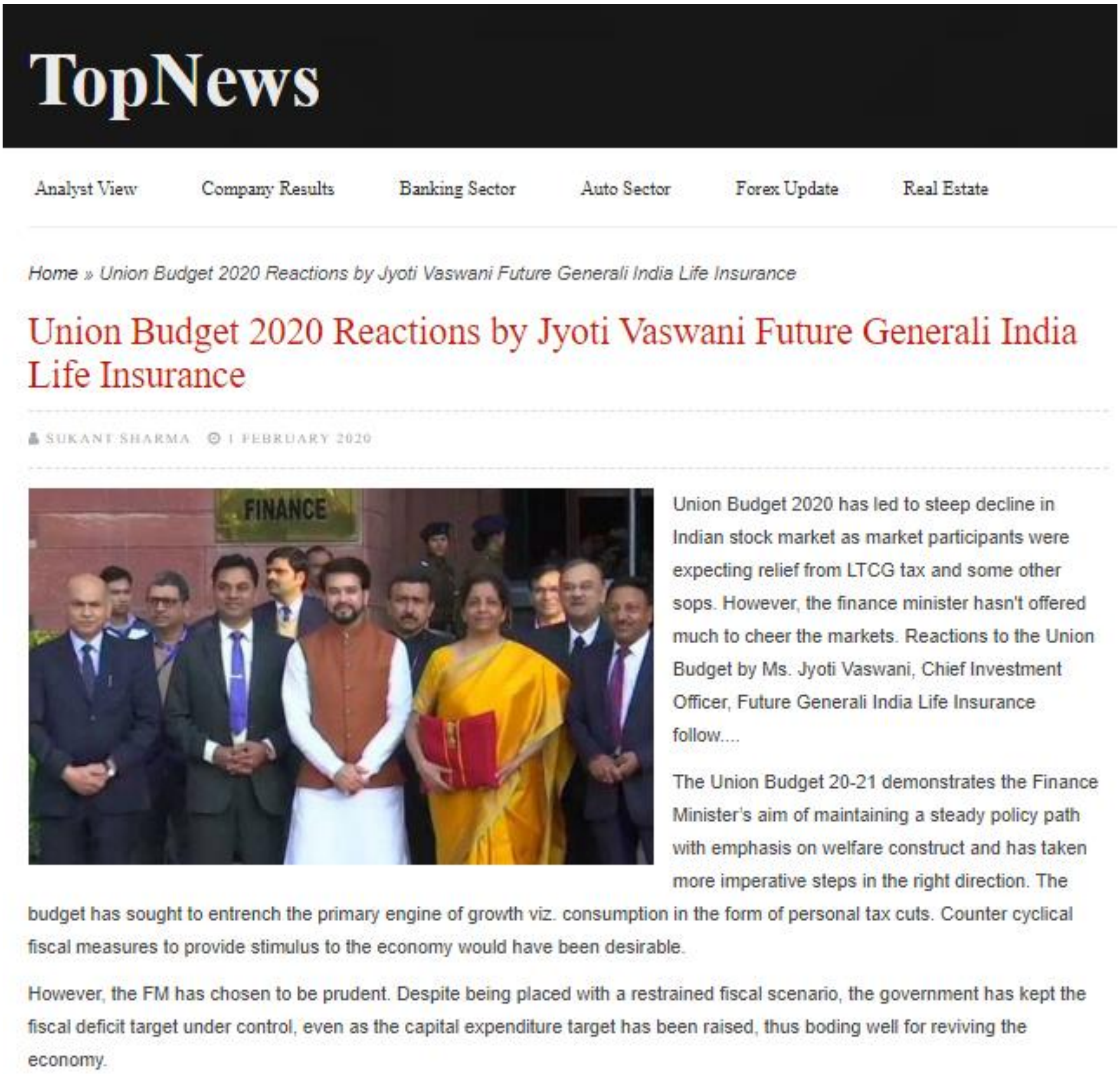
FEB 02 2020, 15:48PM IST | UPDATED: FEB 02 2020, 15:48PM IST

By Jyoti Vaswani

The Union Budget 20-21 demonstrates the Finance Minister's aim of maintaining a steady policy path with emphasis on welfare construct and has taken more imperative steps in the right direction. The budget has sought to entrench the primary engine of growth viz. consumption in the form of personal tax cuts. Counter cyclical fiscal measures to provide stimulus to the economy would have been desirable. However, the FM has chosen to be prudent. Despite being placed with a restrained fiscal scenario, the government has kept the fiscal deficit target under control, even as the capital expenditure target has been raised, thus boding well for reviving the economy.

(The author is Chief Investment Officer at Future Generali India Life Insurance)

Date	01 February 2020
Publication	Top News
Headline	Union Budget 2020 Reactions by Jyoti Vaswani Future Generali India Life Insurance
Link	https://www.topnews.in/union-budget-2020-reactions-jyoti-vaswani-future-generali-india-life-insurance-2411129



Home » Union Budget 2020 Reactions by Jyoti Vaswani Future Generali India Life Insurance

Union Budget 2020 Reactions by Jyoti Vaswani Future Generali India Life Insurance

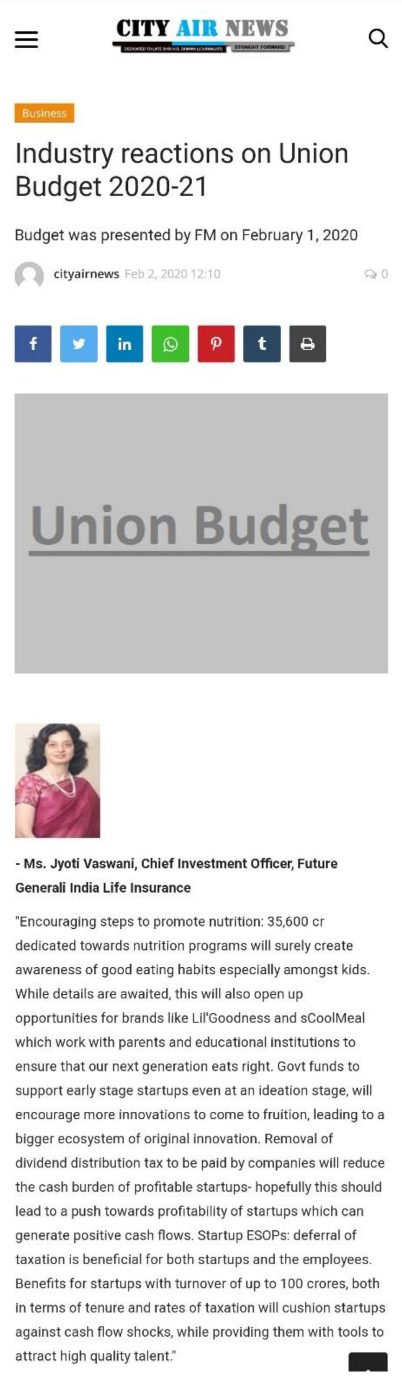
SUKANT SHARMA 1 FEBRUARY 2020

Union Budget 2020 has led to steep decline in Indian stock market as market participants were expecting relief from LTCG tax and some other sops. However, the finance minister hasn't offered much to cheer the markets. Reactions to the Union Budget by Ms. Jyoti Vaswani, Chief Investment Officer, Future Generali India Life Insurance follow....

The Union Budget 20-21 demonstrates the Finance Minister's aim of maintaining a steady policy path with emphasis on welfare construct and has taken more imperative steps in the right direction. The budget has sought to entrench the primary engine of growth viz. consumption in the form of personal tax cuts. Counter cyclical fiscal measures to provide stimulus to the economy would have been desirable.

However, the FM has chosen to be prudent. Despite being placed with a restrained fiscal scenario, the government has kept the fiscal deficit target under control, even as the capital expenditure target has been raised, thus boding well for reviving the economy.

Date	01 February 2020
Publication	City Air News
Headline	Industry reactions on Union Budget 2020-21
Link	https://www.cityairnews.com/content/industry-reactions-on-union-budget-2020-21



Industry reactions on Union Budget 2020-21

Budget was presented by FM on February 1, 2020

cityairnews Feb 2, 2020 12:10 0

- Ms. Jyoti Vaswani, Chief Investment Officer, Future Generali India Life Insurance

"Encouraging steps to promote nutrition: 35,600 cr dedicated towards nutrition programs will surely create awareness of good eating habits especially amongst kids. While details are awaited, this will also open up opportunities for brands like Lil'Goodness and sCoolMeal which work with parents and educational institutions to ensure that our next generation eats right. Govt funds to support early stage startups even at an ideation stage, will encourage more innovations to come to fruition, leading to a bigger ecosystem of original innovation. Removal of dividend distribution tax to be paid by companies will reduce the cash burden of profitable startups- hopefully this should lead to a push towards profitability of startups which can generate positive cash flows. Startup ESOPs: deferral of taxation is beneficial for both startups and the employees. Benefits for startups with turnover of up to 100 crores, both in terms of tenure and rates of taxation will cushion startups against cash flow shocks, while providing them with tools to attract high quality talent."