

# SCVINSIGHT

NOVEMBER 2020

SCV & Co. LLP  
Chartered Accountants



## CYBER SECURITY BULLETIN



## **PREFACE**

In new digital world, Industries and Users with data-driven digital approach in their business world, find increased Cyber-attacks, breach incidents of sensitive data leaks and critical intellectual property, due to various reasons like —unknown application vulnerabilities, weak access controls or poor configuration of network security systems, advanced cyber-attacks in their Computer Systems, Network, Web and Software applications and Data storage which do not safeguard user business interests in a secure environment,

## **TODAY'S INDUSTRY CHALLENGE**

In new digital world, when organizations are adopting emerging and disruptive technologies in their decision-making and business strategies to retain their competitive edge, Industry still face unprecedented cybersecurity challenges as they modernize their infrastructure and rely increasingly on digital processes.

Cybercriminals are constantly looking for fresh exploits and coming up with advanced strategies to defraud and damage institutions and organizations.

With the data-driven digital approach, Increased Cyber-attacks in the business world have crippled Business growth with breach of sensitive data and critical intellectual property, a constant threat to them.

With rising digitization and IoT, the surface of threat vectors are increasing, and the complexity of the security threat landscape in the industry.

Despite organization's efforts to deploy the latest security measures and data leak-prevention tools, there are an increasing number of lethal cyber-attacks, incidents of sensitive data leaks due to various reasons—unknown vulnerability, weak access controls or poor configuration of security systems. Additionally, there are zero-day attacks where malwares are configured to 'exfiltrate' a company's sensitive data.

Email Phishing attacks, Password attacks, Denial of Service (DoS) attacks on Business websites, Man in the Middle (MITM) Attacks in Banking transactions, Advertising, Rogue Software's are very common routine in the Computer Applications, Business Network and Web Application without strong Cyberspace Security and Data protection regulations.

# Latest IT Security Threats in Digital World

## 1. Phishing Scams



“Phishing” is a spin on the word fishing. Cybercriminals are dangling a fake “lure” in the email or website that appears legitimate, hoping users will “bite” by providing the information the criminals have requested (bank account numbers, credit card details, handphone numbers). If you encounter such tactics, do not click on the link provided and type in the company’s name in the search engine. It will direct you to the legitimate website.

## 2. Cloud Jacking



In 2020, cloud jacking is likely to become a more prominent cybersecurity threat due to the increased use of cloud computing. With more businesses migrating their data to the cloud, cybercriminals will focus on hacking the servers used by cloud computing providers. Hackers are able to infiltrate cloud computing infrastructure and steal the stored data. That being said, it is important to select reputable cloud providers that can offer the best security measures.

## 3. Mobile Malware

Mobile malware targets mobile devices to gain access to your private data. As many companies allow employees to access corporate networks using their personal devices, it potentially brings unknown threats to the companies’ stored data. Mobile malware commonly comes in the form of ransomware, advertising clicks, and others.



## MARKET'S EVIDENCE & IMPACTS

### **Cyberattacks hit almost every business, survey finds**

Security personnel and executives from 94% of companies asked saw a cyberattack affect their business in the past year, finds a report from Forrester Consulting. Nearly half of personnel surveyed worldwide said their company was the target of five or more attacks.

**Full Story:** [Intelligent CIO](#)    

### **How criminals are harnessing artificial intelligence**

Just as artificial intelligence is being used to thwart cyberattacks, criminals are also learning to employ it, panelists noted at an event sponsored by the US National Cyber Security Alliance and Nasdaq. "Attackers can use AI to evade detections, to hide where they can't be found, and automatically adapt to counter measures," said Elham Tabassi of the US National Institute of Standards and Technology.

**Full Story:** [TechRepublic](#)    

### **As bitcoin rises, so does hard-to-detect cryptojacking**

Cryptojacking has been around for a while but remains underreported because the malware involved is "incredibly lightweight, elegant, and easily changed," writes Matthew Honea of Guidewire Software. As might be expected, activity ebbs and flows, closely tracking the price of bitcoin, Honea points out.

**Full Story:** [Dark Reading \(free registration\)](#)    

## Cloud Security Breaches: Who is ultimately responsible?

Cloud security breaches consistently make news headlines, yet the stories of these breaches are often framed with vague explanations—a "misconfigured database" or mismanagement by an unnamed third party. Concerns about security have led some CIOs to limit their organizational use of public cloud services. However, the challenge exists not in the security of the cloud itself, but in the policies and technologies for security and control of the technology. **Full Story:** [ISACA](#)    

## Failing to secure data costs Morgan Stanley US \$60M fine

US regulators have hit Morgan Stanley with a \$60 million fine for failing to oversee the third party tearing down two data centers that once served the bank's wealth management unit. Morgan Stanley says it believes no customer data were accessed or misused from the data centers, which went out of service in 2016.

**Full Story:** [BankInfoSecurity](#)    

## Weak passwords put telecom sector at risk, report states

SpyCloud examined more than 100 billion accounts involved in data breaches that affected Fortune 1000 companies and determined that the telecom sector's executives represent the weakest link. About three-fourths of workers, including top executives, are reusing passwords across work and personal accounts, researchers say.

**Full Story:** [CPO Magazine \(Singapore\)](#)    

## Report: Unnecessary data access leads to breaches

More than 6 in 10 companies allow employees to access data that isn't integral to their job functions, and such companies are more than twice as likely to experience a breach, GetApp's annual report states. The report identified remote work as the top trend to watch, with companies advised to institute formal policies and use software to guard data.

**Full Story:** [TechRepublic](#)    

## Ransomware makes a lasting impression, Sophos finds

IT managers whose employers suffer ransomware attacks are more likely to feel unprepared for addressing cyberthreats, states a report from UK security company Sophos. "Whatever the reasons, it is clear that when it comes to security, an organization is never the same again after being hit by ransomware," says Chester Wisniewski of Sophos.

**Full Story:** [TechRadar SecurityBrief Europe](#)    

## What challenges face CISOs as work changes?

Frameworks such as secure access service edge and zero trust will take on more importance as chief information security officers adjust to employees working from home, writes Raif Mehmet of cloud security company Bitglass. CISOs must determine the new risks and how they can adapt without additional resources, among other concerns, Mehmet writes.

**Full Story:** [IDG Connect](#)    

## Young workers see automation as a threat, survey finds

More than half of 350 professionals under age 45 surveyed in the UK, US, Australia, Germany and Singapore say they view artificial intelligence and machine learning as a threat to their jobs, security advisory firm Exabeam reports. The results were a contrast to the 2019 survey, in which only 1 in 10 respondents viewed automation as job-threatening.

**Full Story:** [TechRepublic](#)    

## CYBER REMEDIES

### Why companies should develop cyberresilience plans

It's wise to formulate a resilience plan on the assumption that a company's cyberdefenses will break down eventually, writes consultant Bernard Marr. In this analysis, Marr offers a seven-step plan, including a process by which data can be regenerated—because anything can be lost, even if it is backed up.

**Full Story:** [Forbes](#)    

## Visa: Powerful tools can help small businesses fight fraud

The growth of e-commerce is getting attention from cybercriminals, but a "pretty powerful" bright spot has emerged for small businesses, says Michele Herron, a senior vice president at Visa. Herron says more businesses are adopting sophisticated anti-fraud tools "to fend off scams as they're happening, in real time."

**Full Story:** [CNET](#)    

## Q&A: Why medical devices should be more secure

Makers of medical devices must "take security seriously or be pushed out of the market by competitors who do take it seriously," says Christopher Gates of Velentium, co-author of a manual for engineers and manufacturers. In this Q&A, Gates cites recent nation-state attacks and wonders "if these same actors have been exploring medical devices as a way to inhibit our medical response in an emergency."

**Full Story:** [Help Net Security](#)    

## Survey looks at trends in data protection

The health care and software industries have more mature procedures for protecting data than do other fields, finds FairWarning research based on a survey of more than 550 professionals from around the world. About one-quarter of respondents reported at least 30 attacks over the past three years.

**Full Story:** [Help Net Security](#)    

## Make security awareness an experience

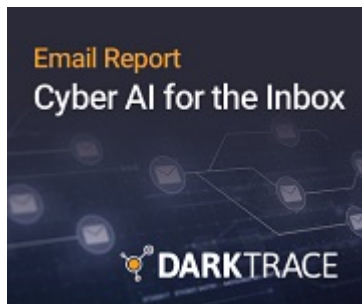
October is Cybersecurity Awareness Month, a common time for organizations to consider their security awareness training and how best to engage employees. Users should be trained regularly to improve their security awareness levels to prevent and detect cyberattacks. But continuous improvement and keeping security awareness at a high level are not easy tasks.

**Full Story:** [ISACA](#)    

## 4 steps for securing your cloud data

Securing data in the cloud begins with "strong encryption and local authentication, as well as the native capabilities of leading cloud storage solutions," writes Russ Kennedy, Nasuni's chief product officer. In this commentary, Kennedy lays out a four-step plan for cloud security, concluding with making sure vendors "have geo-redundant storage and possess complete industry security and compliance certifications."

**Full Story:** [CPO Magazine \(Singapore\)](#)    



### Email Security Threat Report 2020

As a human-driven medium, email often represents the 'weakest link' in an organization's security strategy. By learning the normal 'pattern of life' for every user and correspondent, AI technology builds an evolving understanding of the 'human' within email communications.

[Download the report.](#)

## Your security can be scalable?

When building or upgrading enterprise cryptographic infrastructure in particular, organizations must prioritize scalable architectures and systems as a critical requirement for growing business environments. These principles are applicable to virtually all businesses, but, in particular, they apply to the "always on, always available" needs of financial institutions, retailers and Internet of Things (IoT) device manufacturers. Whether it involves high-volume financial transaction processing or issuing hundreds of millions of certificates, these organizations require security and an nth degree of throughput scalability—essentially, a high availability infrastructure—to handle the volume. **Full Story:** [ISACA](#)





## Basic Prevention Steps for Organisations

### 1. Keep Your Software Up-To-Date

Updating patches and security updates are key to ensure online security. They mend previous security flaws and bugs to create a safe computer environment. They may also be built-in as regular schedule updates. Keeping all of your software and handheld devices up-to-date will give hackers a harder time to work on their end.

### 2. Backup Your Systems and SaaS App Data

Software-as-a-service (SaaS) is a convenient cloud service in which a service provider hosts applications for customers and makes them available to these customers via the Internet. Examples of SaaS applications are Google GSuite (apps), Dropbox, MailChimp, and Hubspot. Cloud services are popular tools used by many companies, which is why hackers aim to exploit all forms of cloud computing to steal stored private data. Backup your systems and SaaS app data from time to time to ensure efficient and quick recovery from cyberattacks.

### 3. Have a Full Suite of IT Security Services for Company Laptops

For high-risk businesses, invest in robust antivirus software and security applications for every company-owned electronic device to prevent possible security breaches. Lower-risk businesses may opt for more affordable security software that provides the amount of protection needed.

### 4. Prepare an Emergency Management Plan

Sometimes, the efforts you put into IT security monitoring may not be enough to prevent company information theft. When hackers are good at what they do, you will have to think a few steps ahead of them. Organise your IT team, communication department and the rest of your company to draw out a contingency plan in the event of a security breach. Although the company suffers a loss of data and profit, the quick rate of recovery will make up the losses in good time.

***Happy reading, stay safe and vigilant***

The summary of IT risks compiled above and more so during Covid, is to make the business entities vigilant about the hidden enemy behind our computer screen!

For any clarifications or queries you may reach out to:

**Piyush Chaturvedi**

**Director – Risk Advisory**

**[piyush.chaturvedi@scvindia.com](mailto:piyush.chaturvedi@scvindia.com)**

## CONNECT WITH US



### Delhi

B-41, Panchsheel Enclave,  
New Delhi -110 017  
T: +91-11-26499111  
F: +91-11-41749444

4/18, Asaf Ali Road,  
New Delhi -110 002  
T: +91-11-23274888  
F: +91-11-23272805  
Email:  
[delhi@scvindia.com](mailto:delhi@scvindia.com)

### Noida

5th Floor  
(Unit No. 505)  
World Trade Tower,  
C -1, Sector- 16,  
Noida -201 301  
Uttar Pradesh  
T: +91-120-4814400


Email:  
[delhi@scvindia.com](mailto:delhi@scvindia.com)

### Ludhiana

B-XIX-220,  
Rani Jhansi Road,  
Near SBI Treasury  
Branch  
Ghumar Mandi,  
Ludhiana -141 001  
Punjab  
T: +91-161-2774527

Email:  
[ludhiana@scvindia.com](mailto:ludhiana@scvindia.com)

Website: [www.scvindia.com](http://www.scvindia.com)

 [www.facebook.com/scvandco/](https://www.facebook.com/scvandco/)  
 [www.linkedin.com/company/scv&co/](https://www.linkedin.com/company/scv&co/)

### **Disclaimer:**

*This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, SCV & Co. LLP, its employees and partners accept no liability, and disclaim all responsibility, for the consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.*

*This publication is solely for the purposes of knowledge dissemination.*