TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Evolving TERRAIN OF CYBERSECURITY FOR SMBs

www.tataadvancedsystems.com

TATA ADVANCED SYSTEMS
CYBER SECURITY PRACTICE

"No businesses are trivial for cyber-attacks."

We often see small businesses falling victim to cyber-attacks as a majority of them feel that they will not face any such incident and hence do not adopt a proactive approach when it comes to cybersecurity. As a result, the number of cyber-attacks targeting SMBs has seen consistent growth in the last few years. And, this is one of the reasons why around 60% of small organizations fail to recover and go out of business within six months after falling victim to cyber-attacks.

Common Security Strategies Followed by SMBs

SMBs often follow different cybersecurity practices to protect their confidential data and brand reputation, most of which are economical and simple to apply. As per the industry reports, some most common cybersecurity approaches followed by small businesses include the usage of strong passwords, implementation of data encryption techniques, limiting employee access to data, 2-factor authentication, etc.

Security Threats Faced by SMBs

Unlike large organizations, SMBs face a lot of complex cyber threats. Phishing emails are the top and most damaging threats faced by small and medium-sized organizations. They are accounted for a majority of cyber-attacks as such emails are highly difficult to recognize. As per Verizon's 2020 DBIR report, phishing accounted for 30% of breaches encountered by small organizations, accompanied by more key threats such as stolen credentials (27%) and password dumpers (16%).

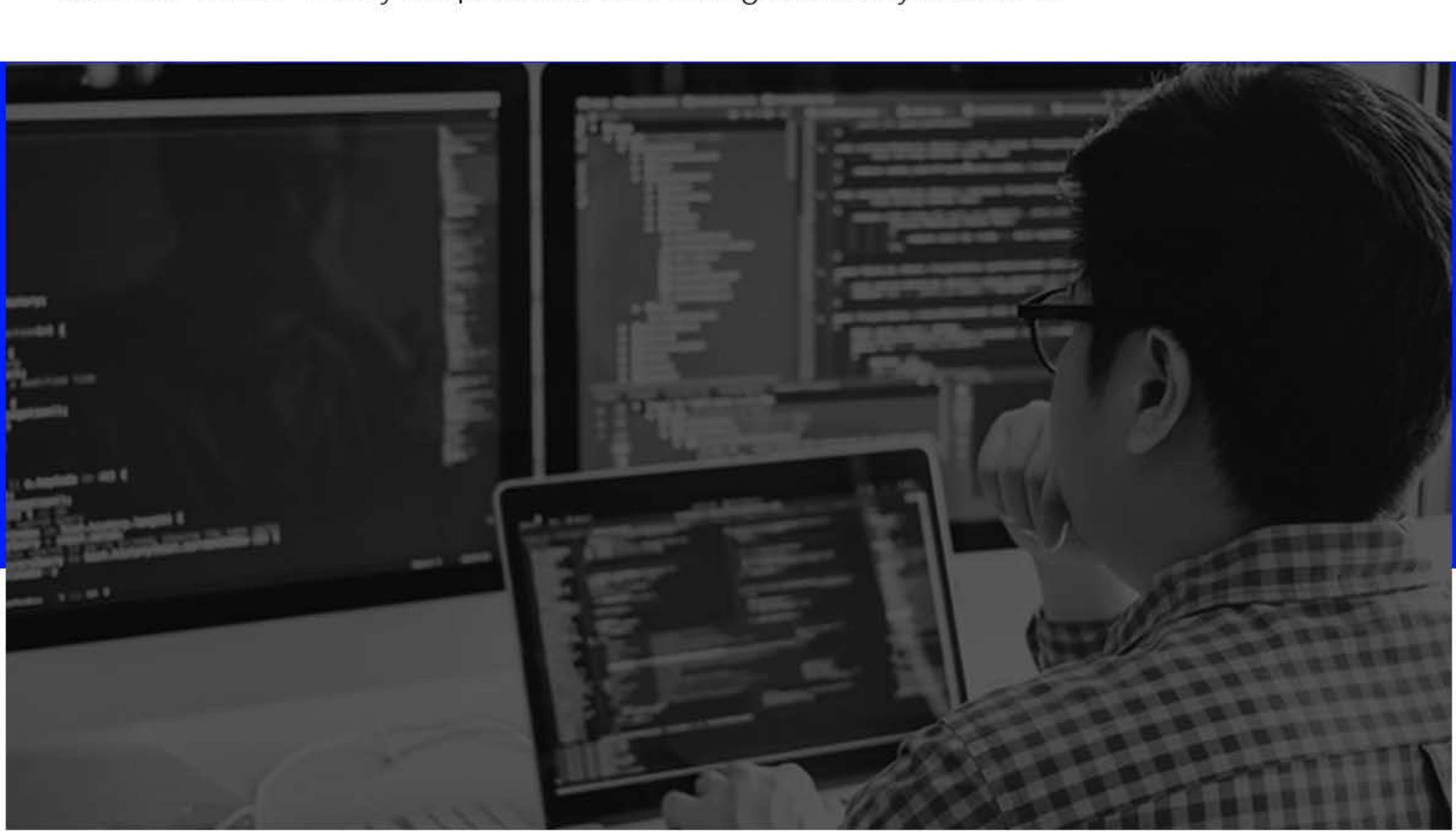
Some other leading threat actions involved in SMBs' breaches include:

- **Exploiting Vulnerabilities**
- **Skimming**
- **Ransomware**
- **Brute Force**
- **Misconfigurations**
- **Data Mishandling**

In addition to the above-listed threats, SQL injection has now become a popular attack vector as companies of all sizes have started developing and utilizing data-driven websites. These attacks, if executed successfully, can allow threat actors to steal, alter or delete business-critical information. Also, Denial-of-Service (DoS) and Man-in-the-Middle (MiTM) can never be placed out of the list when it comes to attacking an organization, particularly, SMBs.

Revamping Security in 2021

SMBs are turning their attention towards cybersecurity after a significant increase in the number of reported frauds and cyber-attacks. As per the 2020 State of SMB Cybersecurity report, 77% of SMBs are worried about cyber-attacks within the next six months, while 73% plan to invest more in cybersecurity in the next 12 months. The report also highlighted that more than half (52%) of SMBs surveyed lack the in-house skills required to effectively address security problems, and 57% lack cybersecurity professionals in their organization. It is important to notice that only 43% of SMBs are currently outsourcing all or the majority of their cybersecurity requirements. But then, 91% responded that they would consider moving to a new "MSSP" if they are provided with the right security solutions.



Let's now glance through some effective methods that can help SMBs to ensure a safe working environment in 2021.

TATA ADVANCED SYSTEMS
CYBER SECURITY PRACTICE

Perform Regular Audits

SMBs should conduct security audits at particular intervals to look for red flags, which indicates your systems have been compromised. It helps security teams to fix and remediate the loopholes and prevent future cyber-attacks. Also, conducting security audits helps in maintaining compliance with different industry regulations like PCI-DSS, HIPAA, etc.

Ensure Cloud Security

SMBs are swiftly turning to the cloud to grow their business and welcome benefits like easy access to resources, increased productivity and greater flexibility. They must choose cloud platforms and applications that offer the maximum level of security and have in-built defences to protect against vulnerabilities.

Investment in VPNs & Firewalls

SMBs should consider implementing more security products like VPNs and advanced Firewalls. Firewalls are generally considered as the first line of defence. VPNs have also played a critical role in allowing employees to safely connect to critical networks during the pandemic. Now, organizations must re-assess their VPN solutions and resolve issues which may have surfaced during the remote work.

Cybersecurity Training

Not every attack is a result of brute force attempts; instead human errors are accounted for a majority of cyber-attacks. SMBs should conduct training sessions to promote cybersecurity awareness and encourage employees to follow safe practices like using strong passwords, paying attention to anonymous emails, installing the latest system/application updates, etc.

Look For Mobile Malware

As cyber-attacks targeting mobile devices are increasingly becoming popular, SMBs need to draft mobile usage policies and security solutions like Mobile Device Management (MDM) to protect their critical data, internal systems, software and networks.

Towards The End...

As we move forward into 2021, the priorities to ensure a cyber-safe working culture will evolve. SMBs need to recognise the threats emerging in modern cyberspace. Tackling cybersecurity challenges can be daunting for SMBs but they can keep their infrastructure safe from cybercriminals by using advanced security controls, or outsourcing MSSPs. With support from MSSPs, SMBs can successfully address potential cyber threats and maintain their business continuity.