accenture

THEY WHO SLEEP CATCH NO PHISH

AUDIO TRANSCRIPT

A wake up call for India Inc. to restore 'trust' in digital economy and build resilient businesses

Siddhi Miglani, a 25-year-old digital native, works as an executive with a technology company. Siddhi spends most of her free time online—connecting with friends, making purchases, paying her bills and more. The digital trail of online activities she leaves behind is easily tracked by social media platforms, advertisers… and, unfortunately, threat actors. As is commonplace in the digital space these days, Siddhi falls prey to an e-mail phishing scam, losing all her savings in a matter of seconds. Siddhi and hundreds of unsuspecting online users are at risk from hackers today. As the Internet continues to change the way we live and work, online users need a more secure, safe and trustworthy experience—every step of their digital trail!

India is taking a huge digital leap. With its Internet user base set to reach 627 million by end-2019, the country is the second-largest market for digital consumers—and growing fast.

Having reaped significant value from developing its core digital sectors, such as IT and business process management, the country is now exploring the digital opportunity in energy, financial services and healthcare, to name a few. The potential is huge.

Government estimates show that digital can unlock economic value worth US$1 trillion in India by 2025. While digital promises to be one of the most inclusive drivers of India's growth, a real risk exists that Siddhi and millions of millennials like her will lose "trust" in the digital economy.

The last couple of years have seen a dramatic surge in cyberattacks in the country. In fact, India was the second-most affected by cyberattacks globally, between 2016 and 2018, according to the Data Security Council of India (DSCI)3. While a regulatory framework in the form of the Information Technology Act 2000 exists, the absence of well-defined cybersecurity laws continues to be a challenge for India.

In the European Union, the General Data Protection Regulation (GDPR) established a global benchmark in personal data protection in May 2018. In India, the Personal Data Protection Bill Law, while still a work in progress, is a positive step in helping the country chart a clear path toward data sovereignty.

Indeed, "trust" is at the center of the digital economy. After all, when people create online accounts to make purchases, they don't just engage in the exchange of data, but also transact in the ultimate currency of "trust." This trust stems from the confidence they have in organizations' ability and foresight to create a secure digital experience.

According to Accenture research, a "trusted" digital economy has the potential to stimulate US$5.2 trillion in value creation opportunities for society.

Unless business leaders take concrete action, lack of safeguards could hurt both individual companies and the economy, and derail the growth of India's digital economy.

MAKE A WISE SECURITY PIVOT
Cybercrime defense and mitigation is a continuous journey and not a one-time event—necessitating the need for commitment to quickly turn to conclusive action.

It's true that just as one loophole is blocked, cybercriminals will try everything possible in their might to move to another, more advanced way to breach security.

A double whammy stares India in the face as cyberattacks continue to rise and cybercriminals get smarter and quicker. Attackers are adopting novel ways and emerging technologies to target cyber systems, leaving India's cyber future hanging in the balance.

How can Indian businesses successfully tackle cybercrime, build trust, and prepare to fight and win tomorrow's cybersecurity wars?

The answer lies in staying one step ahead of cybercriminals while continuing to use breakthrough technologies such as artificial intelligence (AI) and blockchain to secure the future. Our 2019 Cyber Threatscape report underscores the need for businesses to continue investing in digital trust.

Do remember that:

• Communications targeting the global stage may not be all they seem. With rising geopolitical tensions, cyberthreat actors are using high-profile global events, such as sporting events, to influence mass opinion. Using emerging technologies such as AI and 5G communications, along with social media, they explore new ways of breaching security and influencing the geopolitical landscape. Businesses must become ever-more vigilant and realize that global events are often a target—with phishing scams that use lures to influence outcomes.

• Cybercriminals are shifting—and so should you. Cyber criminals are changing tactics to reduce the risk of detection and disruption. They favour close-knit syndicates instead of partnerships. This aids in taking advantage of the familiarity with the local environment and enhances the precision of targeting by using legitimate documents to identify likely victims before delivering malware. Meanwhile, new tactics, techniques and procedures (TTPs) such as "big game hunting" and hack 'n' hustle network access intrusions are on the rise.

• The mixed motives behind ransomware are making it more destructive. The drivers behind ransomware attacks may go beyond financial motives to also serve hybrid motives, such as ideological or political. For example, they could be led by a geopolitical motive aimed at paralyzing a government or a business in a specific country or region.

The reality is that ransomware can disrupt operations, leading to high costs for repairing or restoring systems, and, more importantly, adversely impact the brand and its trust. Since a ransom payment may not guarantee the restoration of company data, companies must have a contingency plan in place for the recovery of operations.

• This is no time for splendid isolation—your ecosystem needs you. Cyber threat actors, especially those who are part of politically motivated groups, continue to favour creating third-party compromises. To safeguard their supply chain, reduce third-party risk and insulate merger and acquisition functions, organizations should embrace proactive, intelligence-driven approaches to cybersecurity.

• Beware of opening more than the back door. Side channel CPU vulnerabilities inevitably pose a high risk to organizations running their compute infrastructure in the public cloud. Adversaries can use such side-channel vulnerabilities to read sensitive data from other hosts on the same physical server. Although mitigations are available for most platforms, cloud deployments and software, they come at a cost of reduced performance, which may lead to an increase in compute costs. Organizations should understand the threats posed by CPU vulnerabilities and then design a robust risk mitigation strategy that suits their needs.

CENTRALIZING SECURITY OPERATIONS THROUGH MANAGED SECURITY SERVICES

With the move to digital and an industry-wide increase in cyber attacks, a global food manufacturer needed to safeguard its customer and employee data, intellectual property and operations. However, several acquisitions had resulted in the company's security being highly distributed and siloed, making it challenging to drive these business objectives. Accenture quickly established processes and metrics, and launched the company's first centralized security operations using existing tools and new technologies.

As the client's trusted security partner, we provide 24/7 end-to-end managed security services. These include monitoring, investigation and response for the client's network across the value chain spanning manufacturing, applications and data. With clearly defined processes and metrics, and a standardized approach, the company has completely transformed its security program. The CISO and executive team now have access to monthly dashboards that provide visibility into key metrics, trends and risks to drive informed decision-making regarding risk and investments. In addition, a highly scalable operating model has helped improve the coverage of critical assets, processing 2+ TB of traffic per day from thousands of log sources.

With clearly defined processes and metrics, and a standardized approach, the company has completely transformed its security program. The CISO and executive team now have access to monthly dashboards that provide visibility into key metrics, trends and risks to drive informed decision-making regarding risk and investments. In addition, a highly scalable operating model has helped improve the coverage of critical assets, processing 2+ TB of traffic per day from thousands of log sources.

Moreover, a phased prioritization approach will not only help in achieving cost optimization and faster RoI but will also reduce risk and generate better insights on business value-chain protection.

Matching pace with their global counterparts, Indian companies are embarking on their digital journeys, with some leading the digital transformation curve. As cyberthreats and attacks become more rampant, the need to protect the value chain of businesses is ever more pronounced.

For example, manufacturing needs the protection of IT and operational technology (OT), with rampant attacks on OT systems.

Indian enterprises must continue to rise to the challenge of putting "digital trust" and security at the center of business strategy. Else, in the not-so-distant future, it may become harder to engage consumers such as Siddhi, who may start taking back control of their online time and reducing the amount of data they share on the internet—a not-so-desirable state for one of the world's fastest-growing digital economies!

This article is written by

KANWAR SINGH, Managing Director and Lead – Technology, Accenture in India