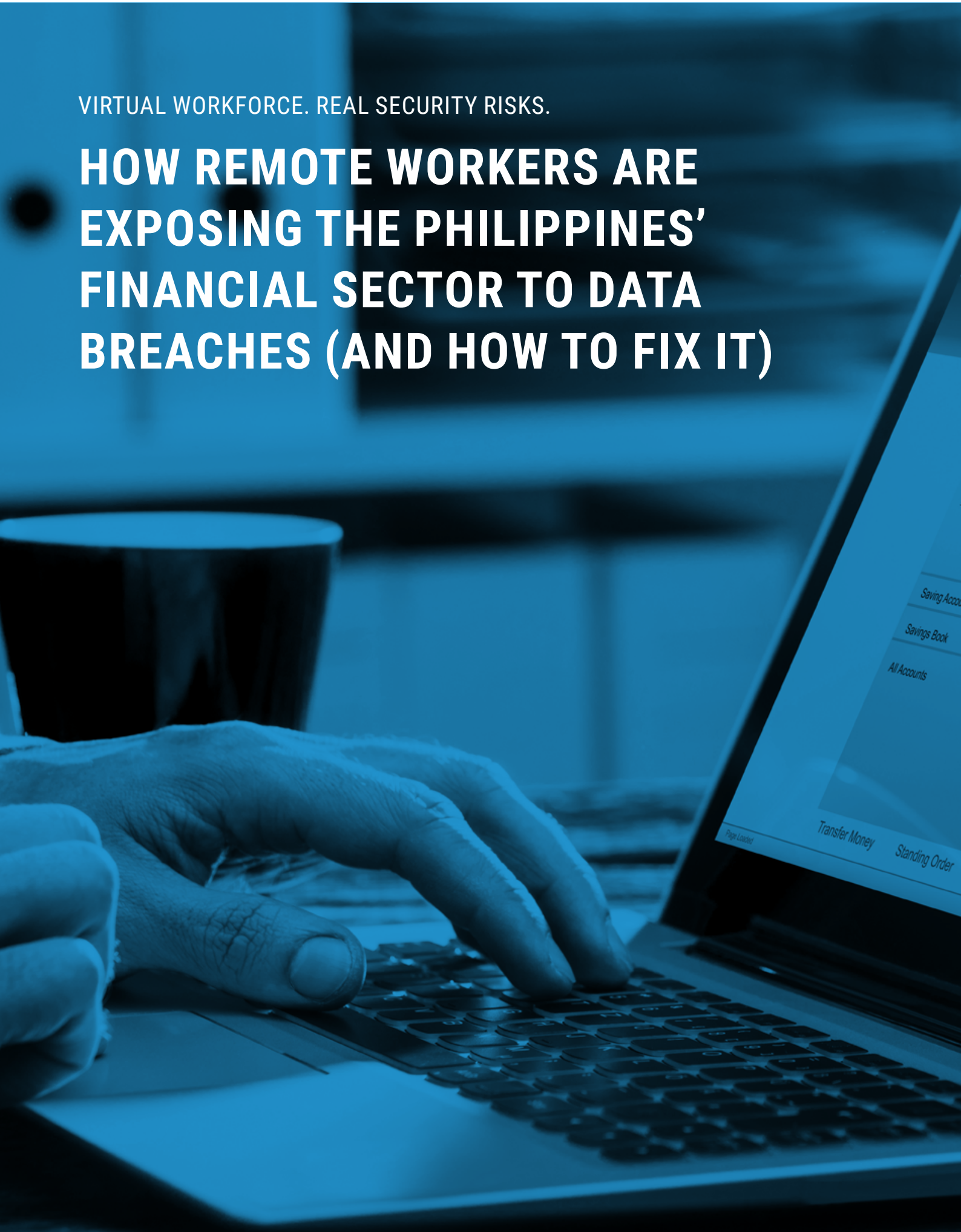
APPISTOKI
Virtualise Your Techscape

VIRTUAL WORKFORCE. REAL SECURITY RISKS.

# HOW REMOTE WORKERS ARE EXPOSING THE PHILIPPINES' FINANCIAL SECTOR TO DATA BREACHES (AND HOW TO FIX IT)

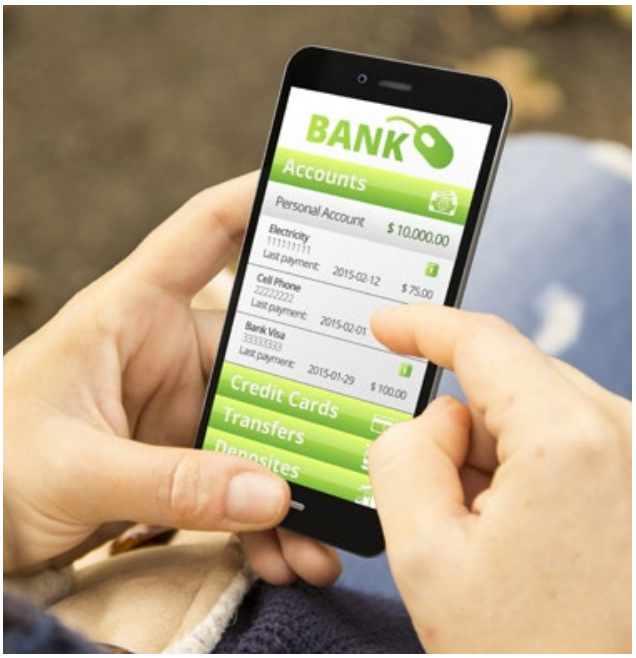


**The impact of COVID-19 has accelerated the growing trend towards working from home. While it has helped keep the economy open, and been embraced by many, the sudden shift has left financial institutions vulnerable to security breaches.**

Most of the data collected by banks, insurers and financial services firms is regulated, sensitive, confidential or personally identifiable information (PII), which requires flawless security at every level – infrastructure, network and application – inside and outside of the office.

While fighting external hackers can dominate headlines and budgets, insider threats are just as pervasive. Verizon's Data Breach Investigations Report[1] found that 30% of breaches were caused either intentionally or accidentally by insiders. In an infamous case at Capital One in Canada, an employee exposed personal data of 100 million clients in a breach estimated to cost the bank in excess of $100 million to fix.[2]

Having large numbers of people working remotely amplifies this threat, whether it's malicious theft, disgruntled employees, careless errors, weak passwords, lost devices or competitor leaks.




## The stakes are higher than ever

The intense media scrutiny, strict regulations, harsh penalties in the Philippines, and added complexity of virtual workforces has heightened the risks.

### Reputational risk

If you expose private data - no matter how it happened – the damage to your brand and customer trust is severe, resulting in immediate financial losses and loss of long-term value.

### Regulatory risk

In a highly regulated market like the Philippines, there are serious fines and legal consequences – personal and corporate – if you're found to be negligent in data security.

### Competitor risk

Whether through malicious acts, internal theft or innocent mistakes, if commercially sensitive data gets in the wrong hands the results can be disastrous.

To mitigate this and comply with regulations, intelligent monitoring tools have become critical for automating compliance, governance and security protocols at a massive scale.

---

### Yesterday's systems facing tomorrow's challenges

Until recently, financial institutions primarily protected their core platforms and data in the fortress of the office, but the pandemic is stretching legacy security protocols to the limit:

- You may have governance frameworks in place, but how can you be sure they are followed by every staff member, every time, wherever they are based?
- With thousands of devices, transactions, interactions and remote staff members, how do you individually monitor, track, detect and prevent breaches at massive scale?
- Discovering breaches after the problem is no longer good enough. How are you proactively finding potential risks, anomalies and vulnerabilities before there is a problem?

**Protection you can bank on**

To comply with regulations, finance companies must proactively monitor, sift through and analyse millions of data points, detect vulnerabilities, block breaches and maintain transparent reporting.

Fortunately, innovative tools like Salesforce Shield for Financial Services are now equipped to streamline and automate the compliance process so IT and business leaders can focus on their core business.

**1. Monitor & Detect**

The first step is to get detailed visibility of your system. Monitoring who is accessing critical data and systems and what they are doing, when and where, right down to pages and documents viewed, downloaded, printed and shared. Set up alerts for suspicious activity and automatic real-time blocks if usage patterns exceed what is expected.

**2. Protect & Control**

Ensure end-to-end platform protection of data in transit and for the end user. For sensitive data such as PII, extra protection may be required to encrypt the data at rest while still enabling critical functionality such as search, workflow and validations rules.

**3. Maintain & Audit**

In the Philippines and other markets, the banking, finance and insurance industry has regulations that require customer data to be retained for a set period of time, as well as any changes. It's essential to maintain a searchable field audit trail and archive capability to manage the lifecycle of regulated data.

**4. Visibility & Reporting**

If there is suspicious activity or a breach, you need to rapidly analyse and eliminate the threat and report the incident with full transparency. Forget wading through thousands of rows of log data, the latest tools deploy visual dashboards that integrate with reporting software to deliver actionable insights.

## Case in point

Using Salesforce Shield, Appistoki helped two ASEAN-based unicorns securely navigate COVID-19. One is a major eCommerce website and the other a multi-service and digital payments leader.

**Challenge: Pandemic sends workers home**

- Surge in home-based workers due to COVID-19
- Spike in online orders meant thousands of transactions to monitor
- Strict compliance, governance and security requirements

**Solution: Rapid scope definition**

- Appistoki works with the clients and Salesforce to define, goals, KPIs and use cases
- Rapid implement of Salesforce Shield using pre-configured templates
- Threshold-driven alerts, automated protections secure data at scale

**Result: Protection activated within 4-weeks**

- Urgent security, control and governance fully enabled
- Equipped to trade through COVID-19 and emerge stronger

## Switch on security at scale

In the Philippines, the remote working genie is out of the bottle and here to stay, so it's critical to embrace security solutions that work today and equip you to thrive in the new normal.

Salesforce Shield for Financial Services is a powerful tool to secure customer data, improve governance and protect you against reputational, regulatory and competitor risk.

As a Salesforce Silver Consulting Partner with proven results on 50+ Salesforce projects in the APAC region, you can trust Appistoki to help you secure your platforms fast and at scale. We have a growing team of 150 consultants available in the Philippines, Singapore, India and Europe.

If you're already a Salesforce user, our fully customised implementation framework can have you up and running with events monitoring within 4 weeks.

**To arrange a confidential, no obligation discussion, contact the Appistoki team at abhijeet.kulkarni@appistoki.com**

*1. Verizon's Data Breach Investigations Report 2019*

*2. The Wall Street Journal: Capital One Breach Highlights Dangers of Insider Threats, July 2019*