Suriname Banking & Finance Summit · LAUNCH 2026

BASELINE CYBERSECURITY PROTOCOL

An initiative of the Suriname Bankers Association

Sandeep Gangaram Panday – Brightlyn

sandeep@brightlyn.nl

17 October 2026

Nice to meet you!

Sandeep Gangaram Panday, MSc RE CISA

Co-founder & security advisor @ **Brightlyn**

Chair Regulatory Taskforce @ NOREA
Chair DevOps Working Group @ NOREA

(Co-) author of:

- DevOps in Control
- Ransomware in Control
- DORA in Control
- NIS2/Cbw in Control

sandeep@brightlyn.nl

Slides can be downloaded

The gap between attackers and defenders is widening

Attackers are accelerating

+11%

Exploitation of vulnerabilities
Up from last year, now the leading initial-access vector

48%

of breaches involve ransomware
Up from prior year; impact is operational, not just data

+60%

Breaches via third parties
Supply chain is now a primary attack path

Defenders are falling behind

26%

of critical vulnerabilities fully remediated in 2025
A drop from last year

43 days

Median time to resolve
Up from 32 days last year

+50%

More critical vulnerabilities to patch in 2025
Backlog grows faster than capacity

Source: Verizon DBIR 2026

Small and public-sector organizations under pressure

5% → 35%

Small organizations
report insufficient cyber resilience
Up from 5% in 2022 to 35% in 2025 — a seven-fold jump.

38%

Public-sector organizations
say their resilience is insufficient
Up from 36%; the gap is widening, not closing.

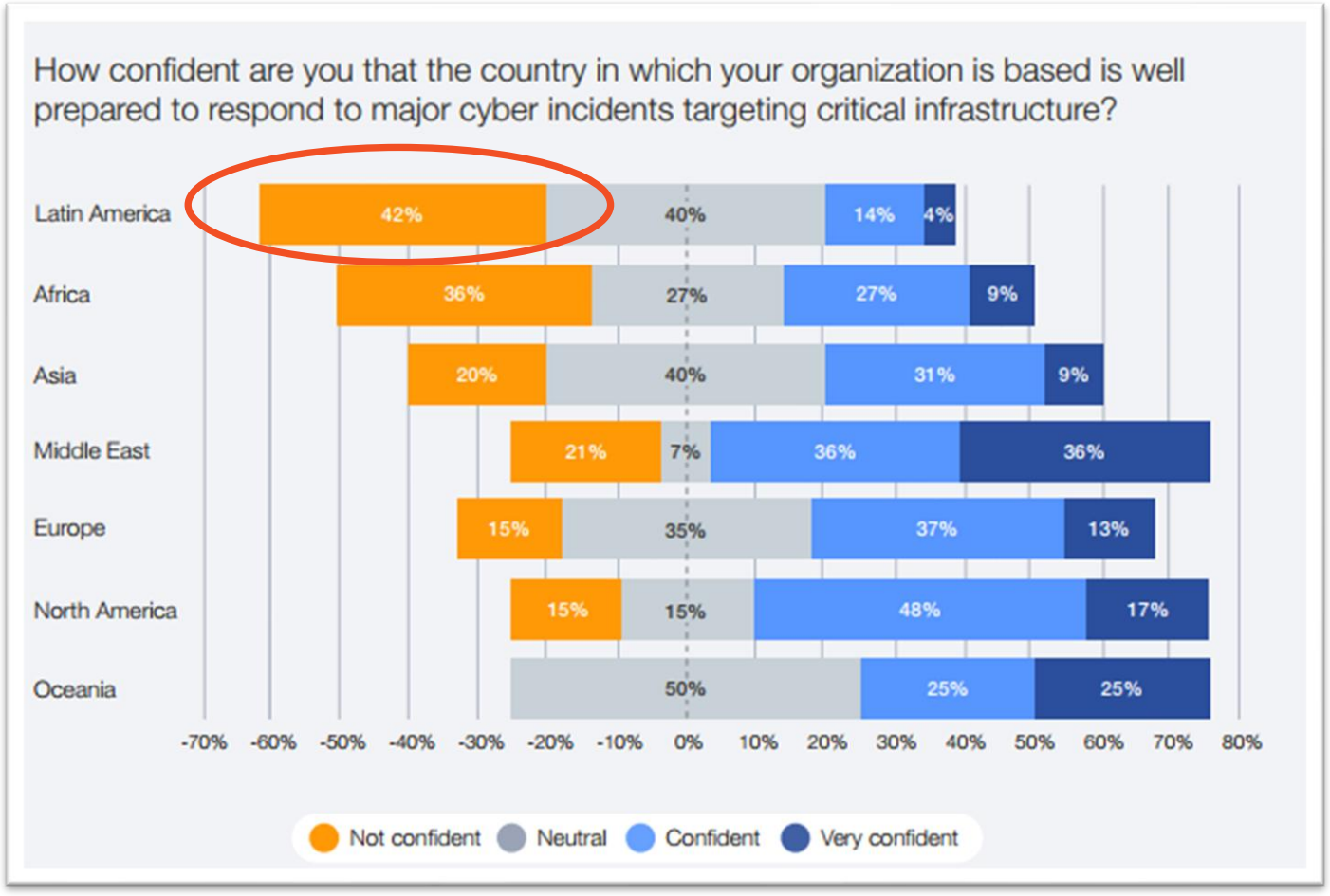
71%

Cyber leaders agree
small organizations have hit a tipping point
Where they can no longer secure themselves against the growing complexity.

"60% of SMEs that have been hacked go bankrupt"
Denver post

Source: WEF Global Cybersecurity Outlook 2025

Latin America is lagging behind



Source: WEF Global Cybersecurity Outlook 2025

Aanval Venezuela

NOS Nieuws • Zondag 4 januari 2026, 15:50

Hoe de VS in krap vijf uur een president van een ander land ontvoerde

Lennart Bloemhof
redacteur Online

De wereld kreeg pas voor het eerst iets mee van de actie toen er explosies werden gemeld in Caracas. Achteraf bleek dat het uitschakelen van S-300-luchtafweersystemen. De Kruif: "Dat zijn zeg maar Russische Patriot-systemen. Door die uit te schakelen, wat complex is omdat je ze met heel veel dreigingen tegelijk moet verwarren, creëer je een luchtoverwicht. Dat overwicht heb je nodig om die special forces binnen te krijgen."

Ook werd de stroom in een deel van Caracas uitgeschakeld, mogelijk via een cyberaanval. Zo hadden de laagvliegende helikopters met de Delta Force-leden een veilige, beschermde route over Caracas. Zij zetten de militairen op de grond bij het complex, waarna ze richting Maduro trokken en live werden voorzien van informatie. Ondanks vuurgevechten waren ze binnen een paar minuten bij de slaapkamer van de president.



Brightlyn
SOLVING COMPLEXITY

AI agents attack 24/7, and anyone can deploy them

10,000×

Open AI agents

have already broken out and are attacking companies

See, among others, Hugging Face and DIVD.

24/7

No effort

The attacks continue non-stop

Targets are random: any company can be hit.

Anyone

Low barrier

Anyone can deploy this

Think of a disgruntled customer.

First impression of cybersecurity at Suriname's top 20 companies

1 Website security

Internet.nl website test

- HTTPS / TLS configuration
- DNSSEC and domain security
- HSTS
- Security headers and security.txt
- RPKI

2 Email resilience

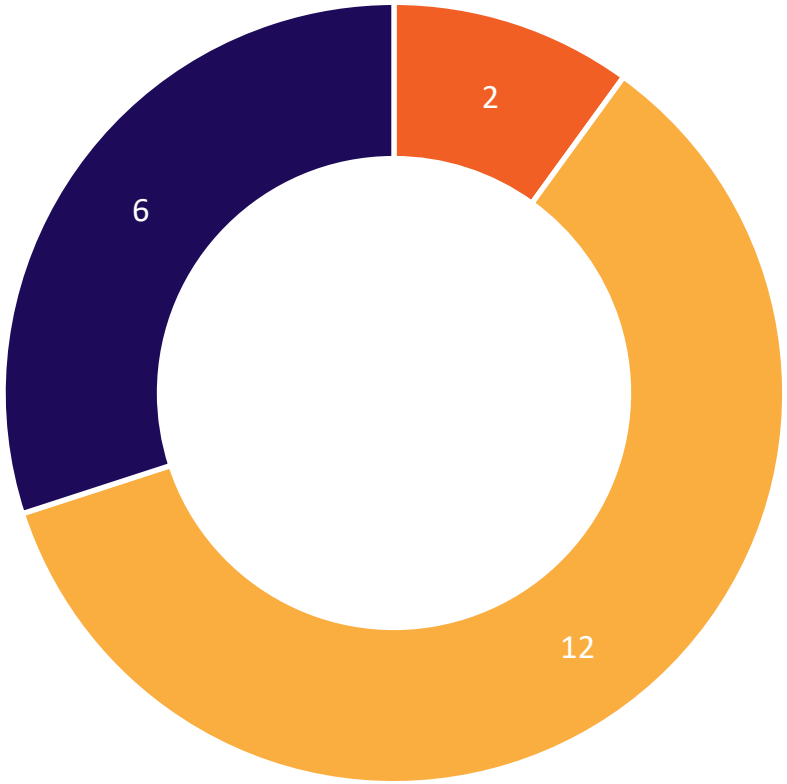
Internet.nl email test — basis for spoofing risk

- SPF
- DKIM
- DMARC
- STARTTLS

Note: this measures publicly observable baseline technical controls — it is not a penetration test. The results say nothing about internal security or staff.

Website security: only 3 in 10 have a solid baseline

Distribution of Internet.nl website scores across 20 organizations



2 of 20

Insufficient baseline — score 0–39%

12 of 20

Partly in place — score 40–69%

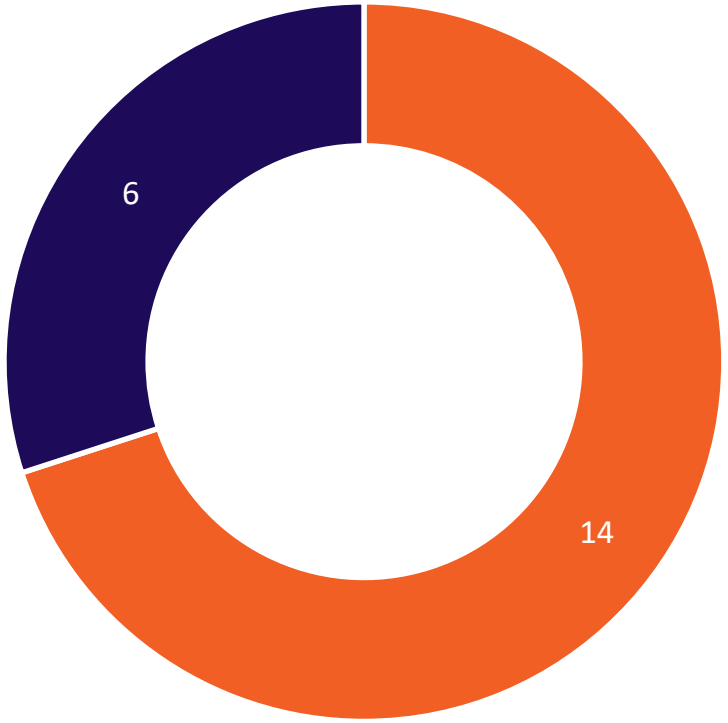
6 of 20

Solid baseline — score 70%+

Measured on HTTPS/TLS, DNSSEC, HSTS and security headers, among others. A low score increases the risk that traffic is intercepted or manipulated, or that a domain is impersonated.

Email spoofing: the most tangible risk

Presence of SPF, DKIM and DMARC — the baseline defense against email spoofing



14 of 20

organizations (70%) do not have all three of SPF, DKIM and DMARC in place.

What does this mean in practice?

Without a complete SPF/DKIM/DMARC configuration, an attacker can fairly easily send emails that appear to come from the company itself. This is the main entry point for convincing phishing emails and brand abuse aimed at customers and partners.

CEO fraud at Pathé: €19 million lost without a single hack

Spoofing in practice — Dutch branch of the cinema chain, 2018



Source: Het Parool, ‘CEO-fraude kostte Pathé 19 miljoen euro’ · incident 2018

€19.2 million

lost to fraudulent payment orders

0 technical hacks

no malware or intrusion — purely deceiving people

2 executives

CEO and CFO departed

No DMARC

Email sent from the @pathe.com domain

CEO fraud at Intesa Sanpaolo – Italy’s biggest bank

AI impersonation in practice — Fideuram, private banking arm of Italy’s largest bank, 2026



€95 million

stolen through urgent transfers ordered by the bank’s own chairman

AI voice clone

a fake lawyer’s call made the WhatsApp request look genuine

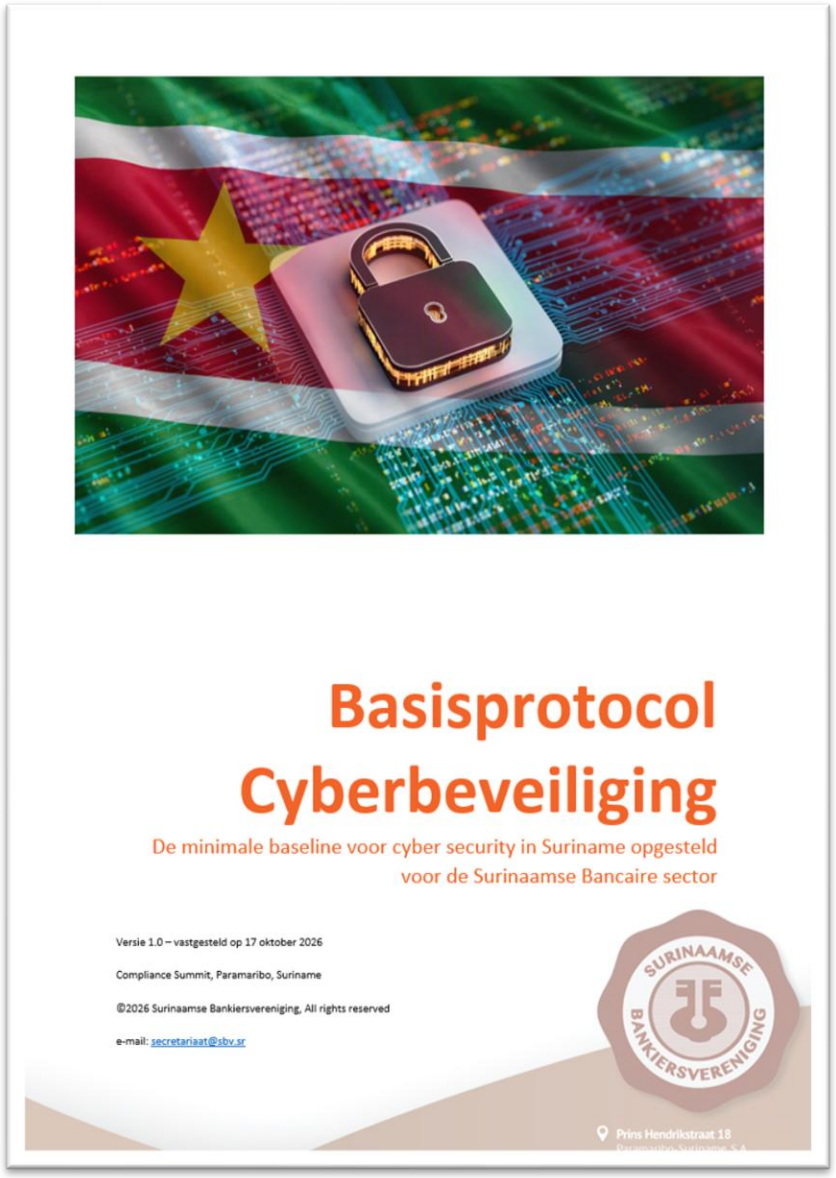
€36 million

still untraced; about €53 million recovered via China, Portugal and Italy

1 executive

Fideuram’s chairman stepped down in March

Source: NU.nl, based on Corriere della Sera and Reuters · incident February 2026



OFFICIAL SIGNING · 17 OCTOBER 2026

BASELINE CYBERSECURITY PROTOCOL

One shared minimum standard

Ten core principles, a common floor for all ten signing banks

Built on international frameworks

Based on the Dutch NCSC duty-of-care measures (NIS2) and the Cyber Security Council's KCIs

Stronger together as a sector

Banks share incidents, threat information and lessons learned

A starting point, not an end point

Reviewed annually and developed further, where possible with the Central Bank of Suriname

Support: getting started together

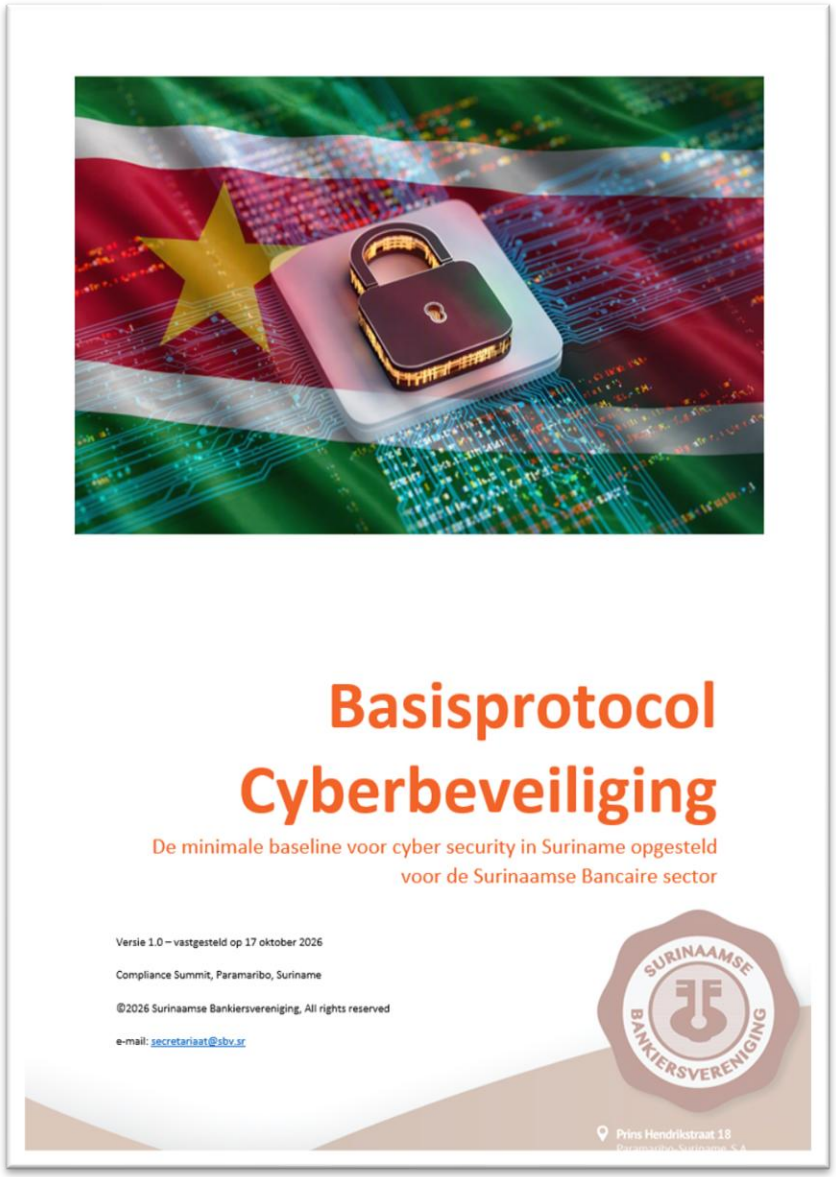
17 November

Online seminar — getting started with the protocol
From baseline assessment to the first concrete measures in your organization.

21 Januari

Online seminar — first practical experiences
What works in practice, where people run into problems, and how others approach it.

You are not on your own: both sessions are online and free of charge. An invitation and registration link will follow by email. Questions in the meantime? Contact the Suriname Bankers Association.



Download here

CYBER RESILIENCE SURINAME · LAUNCH 2026

THANK YOU

For more information see: https://www.sbv.sr/