PARTNER EMAIL:

Subject: 2025 Cybersecurity Budget Ready? Essential Steps to Protect Your Clients

[Partner Name],

As we wrap up 2024, it's time to position your clients for a secure and resilient 2025. Now is the time to engage your clients in budget discussions around cybersecurity, conversations that will protect their businesses and give them a realistic look at what's at stake.

Start with our targeted checklist and sample client email that I've attached. These tools will help you build compelling conversations around cybersecurity ROI, risk mitigation, and proactive defense that will ultimately lead your clients to a safer 2025.

[signature]

Subject: 2025 Cybersecurity Budget Ready? Essential Steps to Protect Your Clients

[Partner Name],

As we wrap up 2024 and look ahead to 2025, it's important for you to proactively engage with your clients about their cybersecurity budget planning, brainstorm strategies and explain investment in cybersecurity.

Now is the time to have these discussions. To get you started we've created a checklist of key points and topics to aid with the discussion. Click here to view the document and a sample email you can send to your clients.

[signature]

CLIENT EMAIL:

Subject: **Urgent: Is Your 2025 Cybersecurity Budget Ready to Face the Storm?**

Hi [Client's Name],

I know the holidays are approaching, and things are getting hectic, but we can't afford to let cybersecurity planning fall to the bottom of the list. As we move into 2025, the risks are intensifying. Cyberattacks are no longer a question of *if* but *when*. The financial and legal fallout from a breach could be catastrophic if your budget isn't aligned with the threats ahead.

Before we wrap up the year, we need to discuss your 2025 cybersecurity budget. Waiting until next year could expose you to risks that aren't just about lost revenue, but also compliance fines and potential legal liabilities. We need to take action now to protect your business from being the next headline.

I understand your time is tight, but a quick call now could save you from serious trouble in 2025. Let me know when we can connect.

==

Checklist:

- Emerging threats and their potential impact on budgets
    - Ransomware
    - IoT Vulnerabilities
    - Supply Chain Attacks
- Best practices for allocating resources effectively
    - High-Risk Areas
    - Employee Training
- Innovative solutions that could enhance their security posture
    - AI-Driven Threat Detection
    - Zero-Trust Architectures
- Collaborative approaches to support client needs
    - Sharing Best Practices

==

Simple explanations (do we need these??):

Ransomware
Ransomware is a bad type of software that locks up your computer files and asks for money to unlock them. If someone falls for this, it can cost a lot to fix the computer and get everything back.

IoT Vulnerabilities
IoT vulnerabilities are problems with smart devices, like those in homes that connect to the internet, which can be hacked by bad people. If these devices aren't secure, it can lead to privacy issues and extra costs to protect them.

Supply Chain Attacks
Supply chain attacks happen when bad actors target the companies that supply goods or services to bigger businesses. If a supplier gets hacked, it can put everyone at risk and cost a lot to fix the problems that arise.

High-Risk Areas

High-risk areas are parts of a business that are more likely to be targeted by bad actors, like sensitive customer information or financial data. It's important to focus resources on these areas to keep them safe and prevent costly problems.

Employee Training
Employee training teaches staff how to recognize and avoid cyber threats, like phishing emails or suspicious links. Investing in training helps everyone stay alert and reduces the chances of making mistakes that could lead to security issues.

AI-Driven Threat Detection
AI-driven threat detection uses smart computer programs to identify and respond to cyber threats faster than humans can. This technology helps catch problems early, keeping the business safer from attacks.

Zero-Trust Architectures
Zero-trust architectures are security systems that assume no one, inside or outside the company, can be trusted by default. This means everyone must prove they are safe before accessing sensitive information, which helps protect against breaches.

Sharing Best Practices
Sharing best practices means discussing and using proven methods that work well in keeping businesses secure. When everyone shares what they know, it helps improve safety for everyone involved.