Amplify Intelligence

About Amplify Intelligence

Amplify Intelligence is a Cyber Security company looking to empower all businesses to understand and manage their Cyber Risks. Our vision is for everyone to have access to world-class security. Currently, cyber safety is too complicated and costly, particularly for small business. Our service integrates into your IT network and identifies your cybersecurity risks to your business. We communicate these in a way that everyone understands and give simple, actionable steps to help you remediate these.

For further details about this customer experience or the services provided by Amplify Intelligence, please contact **info@amplifyintelligence.com** or visit our customer reference portal at **www.amplifyintelligence.com**.

Expert Visibility Helped Us Avoid Dangerous Security Risks

83% Improvement in their Cyber Risk

Case Study Overview

Amplify Intelligence

Customer issue: Direct Hacking
Who (Threat Actor): Ukrainian Cybercriminals
Problem Recurrence: None
Number of Attacks seen: **1944** in 2 hours
Improvement in Overall Cyber Risk: 83%
Percentage of Remote hacking attacks stopped: 100%
Customer Benefits: Reduced Risk, demonstration of proper security management, preventing business interruption and members' impact

This small business can feel proud that they thwarted a severe cyber threat from Ukrainian cybercriminals. Chief Financial Officer, Michael, states “For a nominal fee, Amplify Intelligence’s service added a level of security that makes a difference”.

Michael consulted his IT provider on how they would administer and manage his computers. They decided to use the built-in features from Microsoft Windows. He was not sufficiently technical to appreciate the risks that this would pose.

> **“When we did the RDP *[Remote Login for Windows]*, the IT provider and I had a conversation about the risk, and we knew that it would expose us and some people would try to get in. We decided together that this was a manageable risk.”**

As part of normal business operations, Michael has broad insurance cover. Approaching insurance renewal, Michael’s Insurance broker suggested the ‘Amplify Intelligence -- Companion to Insurance Cyber Safety service’. The insurance broker was keen to assist their policyholders to manage their cyber risks more effectively.

Michael was already concerned about the growing number of press reports of compromised businesses – with over 50% of small and medium businesses hacked annually. He was worried that everyone’s insurance premiums would start rising as a consequence. It is not uncommon for insurance premiums to double after a claim. Michael happily accepted the opportunity to demonstrate his good risk intentions, so as not to have his insurance premiums increased

An innovative service executed professionally in a matter of minutes

Unlike traditional approaches, Amplify Intelligence’s service was fast to install and cost-effective. Michael was surprised at how simple it was to get started. After receiving Amplify Intelligence’s innovative brAIn-box, he was able to follow the instructions and install it himself in less than 5 minutes. Alternative security approaches have required Michael to engage his IT provider to install specialist software on all their computers. These changes can cost thousands in IT service fees.

Amplify Intelligence’s Cyber Safety Solution for loss reduction

Within 15 minutes of Michael installing the brAIn-box, it identified a severe targeted attack. The target was the computer on which the organisation conducted its online business banking, a high-value target for a cyber-criminal. The brAIn-box detected multiple suspicious connections, originating in Ukraine to Michael’s computer, who is the CFO. Michael and his IT provider had considered that others might try to connect to his network. He was still startled by the volume of attacks on his personal computer (1944 in just two hours). Michael and his IT provider had always thought that these attacks would be at only a public website. It was clear that neither Michael or his IT provider had deep expertise in the continually evolving world of cyber attack and defense.

> **Michael said, “I saw the reports and the sheer volume of attacks directly on us. To see it as a quantifiable measure of the exposure we had and the intensity of the attacks, made me uncomfortable.”**

Michael had put his trust in his firewall, antivirus software, and IT provider to manage the security risks for him. He did not realise that specialist Cybersecurity skills are extremely scarce.

A cost effective evidence trail for compliance

Michael and his IT provider made the changes recommended by Amplify Intelligence by adding a VPN (Virtual Private Network). By implementing the advice provided, Michael was able to demonstrate to his insurer his changes in cyber resilience and the constant drive to reduce risk by his organisation.

> **Michael said “We used to just install our anti-virus and thought that would be enough. Now it is clear that it was not enough. We found that the service has raised our level of awareness. It helped us make a practical change in our IT setup by highlighting the risks.”**

The service model offered by Amplify Intelligence is simple and does not include any hidden costs that so many providers do.

> **Michael agrees “it is a small cost and helps us demonstrate how we are proactively taking steps to be more secure. This, I believe, will be important for when we have a claim or are required to demonstrate actions by a regulator like the Privacy Commissioner.”**

Bringing bank-like cybersecurity for everyone

Amplify Intelligence focuses on bringing bank-like security techniques to organisations like Michael’s. They enable organisations and their supporting IT teams to utilise scarce cybersecurity expertise clearly and cost-effectively.

> **Michael concurred “your service added a level of security that makes a difference. Being able to see our risks allows us to set a benchmark and measure them over time.”**

The “Highlighted Risks” show Michael a prioritised list of what actionable steps he can make to provide a measurable change in their cyber risk. He can use these reports to demonstrate progress to both insurers -- for better coverage and premiums; and to regulators -- like the privacy commissioner who wants to see proper guardianship of an individual’s information.