GLASSWALL

Silxo

Cybersecurity Crisis Response and Recovery
Respond, Contain, Remediation

Even with major investment in cybersecurity technologies, extensive user training and constant vigilance, no organization is 100% safe from a serious incident or breach. Cybercriminals have become increasingly sophisticated, quickly exploiting new vulnerabilities or taking advantage of users who simply cannot be expected to spot every fake email, link or attachment.

Across the world, the problems have become so serious that it's no longer a question of if organizations will be targeted, but when. As a result, the way leadership, IT and security teams respond to a cybersecurity breach is just as important as how hard they work to prevent them.

From crisis response to business as usual

That's why Silxo and Glasswall have combined to deliver a cybersecurity crisis response service and solutions portfolio. Combining years of technical insight and product development, they enable cybercrime victims to mitigate the impact of an attack, repair the damage to their systems and data, and quickly return to business as usual. Here's how:

Silxo

Silxo is a technology services company that specialises in supporting businesses to achieve accelerated growth and success. Their portfolio includes crisis management services and solutions that have enabled organizations around the world to address, mitigate and recover from a wide range of major cybersecurity incidents.

Silxo have an incident assessment team and individual roles identified from the outset and create focused action plans and communicate with stakeholders swiftly, allowing the process to start as soon as possible.

Silxo's solutions are delivered by a team of experienced professionals who bring intuitive knowledge and a track record of success across a diverse range of technology environments and crisis scenarios.

Their response typically focuses on three core areas:

Silxo minimise and mitigate the business impact of a cyber breach, by tailoring and adapting their processes to each unique crisis situation.

While traditional detection-based security methods play catch up with new threats, businesses are at risk from popular file formats (such as PDFs, Word and Excel files) that offer many places for malware to hide. In 2020, for instance, ransomware attacks increased by 66% to 304.6 million.

As part of a cybersecurity crisis response solution, Glasswall's patented CDR technology instantly cleans and rebuilds files to match their known good industry specification – automatically removing potential threats. In the event of a cybersecurity breach, files can easily and quickly be bulk sanitized, meaning the Glasswalled files are quickly disarmed of potential threats, giving users the freedom to open any document or attachment without further delay.

Bulk File Sanitization

Problem

- Large government agency
- TBs of important data
- Believed could contain unknown malicious content

Solution

- Battle hardened SDK engine
- Combined with highly scalable, flexible, Compliant Kubernetes architecture.

Results

- Trusted files in secure location
- Files processed within days
- Full audit trail with risk mitigation details

That means organisations can confidently remove malware from every file and document in on-premise or cloud-based networks to quickly return to business as usual.

Key benefits

- ✓ Focused incident action plans
- ✓ Stakeholder communication plans
- ✓ Remediation plan to mitigate future risk
- ✓ Bulk file sanitization to disarm potential threats
- ✓ Secure and optimised files and documents
- ✓ De-risk documents without users even noticing
- ✓ Return to business as usual state in days not months

glasswall.com
info@glasswall.com

silxo.com
information@silxo.com