FINANCIAL SERVICES

Now more than ever, “follow the money” is the guiding principle for cyber criminals the world over. Financial Service companies are their major targets. But not just criminals. Disgruntled employees, hacktivists and increasingly nation states pose serious cyber threats. Cyber attacks against the financial services industry are increasingly sophisticated and frequent. As providers shift to digital channels like mobile banking the attack surface grows. Fund managers, financial information suppliers, commercial banking services, broking services and even share markets have been the focus of sophisticated attacks. Financial Service companies collect, store and process huge amounts of personally identifiable information (PII), credit card data and financial transactions. Consequently they face a growing number of stringent industry and government regulations for secure data protection and privacy such as PCI, SOX, MAS-TRM and the EU GDPR.

Digital security has also opened up new opportunities for serving clients. USB and Australia Post are among a group of consumer-facing institutions that offer digital safety deposit boxes for their customers. Turn cyber risks into a revenue line with STASH’s secure digital safety deposit box application developed for large-scale deployment.

STASH is a key partner for financial services companies to keep data at rest and back-up databases securely stored and shared. STASH is the perfect partner for sharing secure deal data, as well intellectual property, administrative, HR and other data secure. Keeping data very securely on separate networks diminishes the risks of infection from email, operational systems and other attack vectors on your present networks. STASH’s unique authentication and encryption processes slash the risk of insider access to key data. Its secure data repositories are not vulnerable to ransomware. STASH has developed trustworthy digital repository technology and processes to ensure the storage and retrieval of viable data over many decades. Your compliance and business needs for storing data for the long-term is safe with STASH.

STASH is also perfectly suited to meet the data retention and encryption requirements of the New York Department of Financial Services (DFS) cybersecurity rules (23 N.Y.C.R.R. Part 500) for New York-licensed insurance companies and banks, as well as other financial services companies regulated by DFS, including, agents, brokers, adjusters, registered service contract providers, licensed reinsurance intermediaries, licensed life settlement providers, licensed life settlement brokers and licensed insurance consultants.

.

"Files were literally disappearing from our server... We don’t know how much was actually taken... They were clearly letting us know that the files were gone... It took about a week of rebuilding and diagnosing everything... We had to order new servers, we had to write everything and then we had to reload everything...”
– ***(Confidential) Rights Group***

"Governor Andrew Cuomo announced [a new] regulation on Thursday, describing it as the first of its kind in the nation. The rule will require banks, insurance companies, and other entities regulated by the state's Department of Financial Services to establish cybersecurity programs to protect consumers' sensitive data and secure the financial services industry. "New York is the financial capital of the world, and it is critical that we do everything in our power to protect consumers and our financial system from the ever increasing threat of cyber-attacks," Cuomo said in a statement on Thursday. "These strong, first-in-the-nation protections will help ensure this industry has the necessary safeguards in place in order to protect themselves and the New Yorkers they serve from the serious economic harm caused by these devastating cyber-crimes," the governor added. The rule will take effect on March 1, 2017. "

– ***The Hill, 16 February 2017***

"The prospect of direct access to money with a capitalisation expected to have exceed $143 trillion worldwide in 2014 has resulted in the financial services industry becoming a prime target for cybercrime — such as financial fraud, identity theft, unauthorised access, or loss of data and denial of service attacks. Hackers and organised criminal groups with potential government funding have been constantly developing and improving techniques to circumvent information security controls and safeguards in order to commit fraud, financial theft and other cybercrimes with advanced capabilities to execute persistent and targeted attacks."

– ***Cybersecurity in Financial Services, CSC***

Whether you want to keep things to yourself or share with others, STASH delivers DSECaaS™ (data-security-as-a-service) to meet your needs. In a world of Open Networks and Bring Your Own Device, we focus on the crown jewels. On the data. On what really matters to your business.

STASH Data Protection for everyday valuable data and STASH HIBERNATE® for very long term data protection with data integrity for decades are the most impactful encryption and privacy Solutions ever developed to protect the actual data bytes themselves. STASH doesn't analyze, predict, try to defend, or react to data compromise after the fact like 99.99% of all other security options. When data is protected with STASH, it has a statistical probability of nil to breach, manipulation, loss, harm, or ransomware.

Data, network, and infrastructure agnostic, STASH is completely automated and simple to deploy, without changing anything about how you do business. Activated via SAAS, Secure Backup, & API

AICPA | NIST | SOC 1 | SOC 2 | SOC 3 | ISO 27001 | Privacy Shield (Safe Harbor) | PCI- DSS | HIPAA

Digital Confetti® • Keys-on-the-Fly® • Data Integrity & Resilience for Decades • Cost Effective